

HP 5500 EI & 5500 SI Switch Series

Layer 3 - IP Routing

Command Reference

Part number: 5998-1717

Software version: Release 2220

Document version: 6W100-20130810



Legal and notice information

© Copyright 2013 Hewlett-Packard Development Company, L.P.

No part of this documentation may be reproduced or transmitted in any form or by any means without prior written consent of Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Contents

Basic IP routing commands	1
display ip routing-table	1
display ip routing-table acl	5
display ip routing-table <i>ip-address</i>	8
display ip routing-table ip-prefix	11
display ip routing-table protocol	12
display ip routing-table statistics	14
display ipv6 routing-table	15
display ipv6 routing-table acl	17
display ipv6 routing-table <i>ipv6-address</i>	18
display ipv6 routing-table ipv6-prefix	20
display ipv6 routing-table protocol	21
display ipv6 routing-table statistics	22
reset ip routing-table statistics protocol	23
reset ipv6 routing-table statistics	23
Static routing configuration commands	25
delete static-routes all	25
ip route-static	25
ip route-static default-preference	28
ip route-static fast-reroute	28
RIP configuration commands	30
checkzero	30
default cost (RIP view)	30
default-route	31
display rip	32
display rip database	34
display rip interface	35
display rip route	36
dscp (RIP view)	38
fast-reroute	38
filter-policy export (RIP view)	39
filter-policy import (RIP view)	41
host-route	42
import-route (RIP view)	42
maximum load-balancing (RIP view)	44
network	44
output-delay	45
peer	45
preference	46
reset rip process	47
reset rip statistics	47
rip	48
rip authentication-mode	48
rip bfd enable	49
rip default-route	50
rip input	51
rip metricin	51
rip metricout	52

rip mib-binding	53
rip output	54
rip poison-reverse	54
rip split-horizon	55
rip summary-address	55
rip version	56
silent-interface (RIP view)	57
summary	57
timers	58
validate-source-address	59
version	60

OSPF configuration commands	61
abr-summary (OSPF area view)	61
area (OSPF view)	62
asbr-summary	62
authentication-mode	63
bandwidth-reference (OSPF view)	64
default	65
default-cost (OSPF area view)	65
default-route-advertise (OSPF view)	66
description (OSPF/OSPF area view)	67
display ospf abr-asbr	68
display ospf asbr-summary	69
display ospf brief	70
display ospf cumulative	73
display ospf error	75
display ospf interface	77
display ospf lsdb	79
display ospf nexthop	81
display ospf peer	82
display ospf peer statistics	85
display ospf request-queue	86
display ospf retrans-queue	87
display ospf routing	89
display ospf vlink	90
display router id	91
dscp (OSPF view)	92
enable link-local-signaling	92
enable log	93
enable out-of-band-resynchronization	93
fast-reroute	94
filter	95
filter-policy export (OSPF view)	96
filter-policy import (OSPF view)	97
graceful-restart (OSPF view)	98
graceful-restart help	99
graceful-restart interval (OSPF view)	100
host-advertise	100
import-route (OSPF view)	101
ispf enable	102
log-peer-change	103
lsa-arrival-interval	103
lsa-generation-interval	104
lsdb-overflow-limit	105

maximum load-balancing (OSPF view).....	105
maximum-routes.....	106
network (OSPF area view).....	107
nssa.....	107
opaque-capability enable.....	108
ospf.....	109
ospf authentication-mode.....	110
ospf bfd enable.....	111
ospf cost.....	112
ospf dr-priority.....	112
ospf mib-binding.....	113
ospf mtu-enable.....	113
ospf network-type.....	114
ospf packet-process prioritized-treatment.....	115
ospf timer dead.....	116
ospf timer hello.....	116
ospf timer poll.....	117
ospf timer retransmit.....	118
ospf trans-delay.....	118
peer.....	119
preference.....	120
reset ospf counters.....	120
reset ospf process.....	121
reset ospf redistribution.....	122
rfc1583 compatible.....	122
router id.....	123
silent-interface (OSPF view).....	123
snmp-agent trap enable ospf.....	124
spf-schedule-interval.....	125
stub (OSPF area view).....	126
stub-router.....	127
transmit-pacing.....	127
vlink-peer (OSPF area view).....	128

IS-IS configuration commands.....	130
area-authentication-mode.....	130
auto-cost enable.....	131
bandwidth-reference (IS-IS view).....	132
circuit-cost.....	132
cost-style.....	133
default-route-advertise (IS-IS view).....	134
display isis brief.....	135
display isis debug-switches.....	136
display isis graceful-restart status.....	137
display isis interface.....	138
display isis lsdb.....	142
display isis name-table.....	145
display isis peer.....	146
display isis route.....	148
display isis spf-log.....	151
display isis statistics.....	153
domain-authentication-mode.....	155
fast-reroute.....	156
filter-policy export (IS-IS view).....	157
filter-policy import (IS-IS view).....	158

flash-flood	159
graceful-restart (IS-IS view)	160
graceful-restart interval (IS-IS view)	161
graceful-restart suppress-sa	161
import-route (IS-IS view)	162
import-route isis level-2 into level-1	163
import-route limit (IS-IS view)	164
isis	164
isis authentication-mode	165
isis bfd enable	166
isis circuit-level	167
isis circuit-type p2p	167
isis cost	168
isis dis-name	169
isis dis-priority	170
isis enable	170
isis mib-binding	171
isis silent	172
isis small-hello	172
isis timer csnp	173
isis timer hello	174
isis timer holding-multiplier	174
isis timer lsp	175
isis timer retransmit	176
is-level	177
is-name	178
is-name map	178
is-snmp-traps enable	179
log-peer-change (IS-IS view)	179
lsp-fragments-extend	180
lsp-length originate	180
lsp-length receive	181
maximum load-balancing (IS-IS view)	182
network-entity	182
non-stop-routing	183
non-stop-routing interval	184
preference (IS-IS view)	184
priority high	185
reset isis all	186
reset isis peer	186
set-overload	187
summary (IS-IS view)	188
timer lsp-generation	189
timer lsp-max-age	190
timer lsp-refresh	190
timer spf	191
virtual-system	192
BGP configuration commands	193
aggregate	193
balance (BGP/BGP-VPN instance view)	194
bestroute as-path-neglect (BGP/BGP-VPN instance view)	195
bestroute compare-med (BGP/BGP-VPN instance view)	196
bestroute med-confederation (BGP/BGP-VPN instance view)	196
bgp	197

compare-different-as-med (BGP/BGP-VPN instance view).....	198
confederation id	198
confederation nonstandard	199
confederation peer-as	200
dampening (BGP/BGP-VPN instance view)	201
default ipv4-unicast	202
default local-preference (BGP/BGP-VPN instance view).....	202
default med (BGP/BGP-VPN instance view).....	203
default-route imported (BGP/BGP-VPN instance view)	204
display bgp group.....	205
display bgp network	206
display bgp paths.....	207
display bgp peer	208
display bgp peer received ip-prefix	211
display bgp routing-table.....	212
display bgp routing-table as-path-acl	214
display bgp routing-table cidr.....	215
display bgp routing-table community	216
display bgp routing-table community-list.....	217
display bgp routing-table dampened.....	218
display bgp routing-table dampening parameter	219
display bgp routing-table different-origin-as.....	220
display bgp routing-table flap-info	220
display bgp routing-table label.....	222
display bgp routing-table peer.....	222
display bgp routing-table regular-expression	223
display bgp routing-table statistic	224
display router id	225
ebgp-interface-sensitive	225
filter-policy export (BGP/BGP-VPN instance view)	226
filter-policy import (BGP/BGP-VPN instance view)	227
graceful-restart (BGP view).....	228
graceful-restart timer restart.....	229
graceful-restart timer wait-for-rib	230
group (BGP/BGP-VPN instance view).....	230
ignore-first-as	231
import-route (BGP/BGP-VPN instance view).....	232
log-peer-change	233
network (BGP/BGP-VPN instance view)	233
network short-cut (BGP/BGP-VPN instance view)	234
peer advertise-community (BGP/BGP-VPN instance view)	235
peer advertise-ext-community (BGP/BGP-VPN instance view).....	236
peer allow-as-loop (BGP/BGP-VPN instance view)	236
peer as-number (BGP/BGP-VPN instance view)	237
peer as-path-acl (BGP/BGP-VPN instance view).....	238
peer bfd.....	239
peer capability-advertise conventional	240
peer capability-advertise orf	240
peer capability-advertise orf non-standard	241
peer capability-advertise route-refresh	242
peer capability-advertise suppress-4-byte-as	243
peer connect-interface (BGP/BGP-VPN instance view).....	244
peer default-route-advertise (BGP/BGP-VPN instance view).....	245
peer description (BGP/BGP-VPN instance view).....	246

peer dscp (BGP/BGP-VPN instance view).....	246
peer ebgp-max-hop (BGP/BGP-VPN instance view)	247
peer enable (BGP/BGP-VPN instance view)	248
peer fake-as (BGP/BGP-VPN instance view).....	249
peer filter-policy (BGP/BGP-VPN instance view)	249
peer group (BGP/BGP-VPN instance view).....	250
peer ignore (BGP/BGP-VPN instance view).....	251
peer ip-prefix.....	252
peer keep-all-routes (BGP/BGP-VPN instance view).....	253
peer log-change (BGP/BGP-VPN instance view).....	253
peer next-hop-local (BGP/BGP-VPN instance view)	254
peer password.....	255
peer preferred-value (BGP/BGP-VPN instance view)	256
peer public-as-only (BGP/BGP-VPN instance view).....	257
peer reflect-client (BGP/BGP-VPN instance view).....	258
peer route-limit (BGP/BGP-VPN instance view)	258
peer route-policy (BGP/BGP-VPN instance view).....	259
peer route-update-interval (BGP/BGP-VPN instance view)	260
peer timer (BGP/BGP-VPN instance view)	261
preference (BGP/BGP-VPN instance view).....	262
reflect between-clients (BGP view/BGP-VPN instance view)	263
reflector cluster-id (BGP view/BGP-VPN instance view).....	264
refresh bgp.....	265
reset bgp	265
reset bgp dampening.....	266
reset bgp flap-info	266
reset bgp ipv4 all	267
router id.....	267
router-id	268
summary automatic	269
synchronization (BGP view)	269
timer (BGP/BGP-VPN instance view)	270
IPv6 static routing configuration commands	272
delete ipv6 static-routes all	272
ipv6 route-static.....	272
RIPng configuration commands.....	274
checkzero.....	274
default cost (RIPng view).....	274
display ripng.....	275
display ripng database.....	276
display ripng interface.....	278
display ripng route	279
enable ipsec-policy (RIPng view)	281
filter-policy export (RIPng view).....	281
filter-policy import (RIPng view).....	282
import-route.....	283
maximum load-balancing (RIPng view).....	284
preference	285
reset ripng process	285
reset ripng statistics	286
ripng	286
ripng default-route	287
ripng enable	288

ripng ipsec-policy	288
ripng metricin	289
ripng metricout	290
ripng poison-reverse	290
ripng split-horizon	291
ripng summary-address	291
timers	292

OSPFv3 configuration commands..... 294

abr-summary (OSPFv3 area view)	294
area (OSPFv3 view)	294
bandwidth-reference	295
default cost	296
default-cost (OSPFv3 area view)	296
default-route-advertise	297
display ospfv3	298
display ospfv3 graceful-restart status	300
display ospfv3 interface	301
display ospfv3 lsdb	303
display ospfv3 lsdb statistic	307
display ospfv3 next-hop	308
display ospfv3 peer	309
display ospfv3 peer statistics	311
display ospfv3 request-list	312
display ospfv3 retrans-list	313
display ospfv3 routing	315
display ospfv3 statistics	317
display ospfv3 topology	318
display ospfv3 vlink	319
enable ipsec-policy (OSPFv3 area view)	320
filter-policy export (OSPFv3 view)	321
filter-policy import (OSPFv3 view)	322
graceful-restart enable	323
graceful-restart helper enable	324
graceful-restart helper strict-lsa-checking	324
graceful-restart interval	325
import-route (OSPFv3 view)	325
log-peer-change	326
maximum load-balancing (OSPFv3 view)	327
ospfv3	327
ospfv3 area	328
ospfv3 bfd enable	329
ospfv3 cost	329
ospfv3 dr-priority	330
ospfv3 ipsec-policy	331
ospfv3 mtu-ignore	331
ospfv3 network-type	332
ospfv3 peer	332
ospfv3 timer dead	333
ospfv3 timer hello	334
ospfv3 timer retransmit	334
ospfv3 timer poll	335
ospfv3 trans-delay	336
preference	336
router-id	337

silent-interface(OSPFv3 view).....	338
spf timers	338
stub (OSPFv3 area view).....	339
vlink-peer (OSPFv3 area view).....	340
IPv6 IS-IS configuration commands.....	342
display isis route ipv6	342
ipv6 default-route-advertise	345
ipv6 enable.....	345
ipv6 filter-policy export.....	346
ipv6 filter-policy import.....	347
ipv6 import-route	348
ipv6 import-route isisv6 level-2 into level-1	349
ipv6 import-route limit	350
ipv6 maximum load-balancing	351
ipv6 preference	351
ipv6 summary	352
isis ipv6 bfd enable.....	353
isis ipv6 enable	353
multiple-topology ipv6-unicast.....	354
IPv6 BGP configuration commands.....	356
aggregate (IPv6 address family view).....	356
balance (IPv6 address family view/IPv6 BGP-VPN instance view).....	357
bestroute as-path-neglect (IPv6 address family view)	358
bestroute compare-med (IPv6 address family view)	358
bestroute med-confederation (IPv6 address family view).....	359
compare-different-as-med (IPv6 address family view).....	360
dampening (IPv6 address family view).....	360
default local-preference (IPv6 address family view/IPv6 BGP-VPN instance view)	361
default med (IPv6 address family view/IPv6 BGP-VPN instance view)	362
default-route imported (IPv6 address family view/IPv6 BGP-VPN instance view).....	363
display bgp ipv6 group.....	363
display bgp ipv6 network	365
display bgp ipv6 paths.....	366
display bgp ipv6 peer	367
display bgp ipv6 peer received ipv6-prefix	371
display bgp ipv6 routing-table.....	372
display bgp ipv6 routing-table as-path-acl	374
display bgp ipv6 routing-table community	375
display bgp ipv6 routing-table community-list.....	376
display bgp ipv6 routing-table dampened	377
display bgp ipv6 routing-table dampening parameter	378
display bgp ipv6 routing-table different-origin-as	379
display bgp ipv6 routing-table flap-info.....	380
display bgp ipv6 routing-table peer.....	381
display bgp ipv6 routing-table regular-expression	382
display bgp ipv6 routing-table statistic	383
filter-policy export (IPv6 address family view/IPv6 BGP-VPN instance view).....	384
filter-policy import (IPv6 address family view/IPv6 BGP-VPN instance view).....	385
group (IPv6 address family view)	386
import-route (IPv6 address family view/IPv6 BGP-VPN instance view).....	386
ipv6-family.....	387
network (IPv6 address family view/IPv6 BGP-VPN instance view).....	388
peer advertise-community (IPv6 address family view).....	389

peer advertise-ext-community (IPv6 address family view)	389
peer allow-as-loop (IPv6 address family view)	390
peer as-number (IPv6 address family view)	391
peer as-number (IPv6 BGP-VPN instance view)	391
peer as-path-acl (IPv6 address family view)	392
peer bfd (IPv6 address family view/IPv6 BGP-VPN instance view)	393
peer capability-advertise orf	393
peer capability-advertise orf non-standard (IPv6 address family view)	394
peer capability-advertise route-refresh	395
peer capability-advertise suppress-4-byte-as (IPv6 address family view)	396
peer capability-advertise suppress-4-byte-as (IPv6 BGP-VPN instance view)	397
peer connect-interface (IPv6 address family view)	397
peer default-route-advertise	398
peer description (IPv6 address family view)	399
peer dscp (IPv6 address family view)	399
peer ebgp-max-hop (IPv6 address family view)	400
peer enable (IPv6 address family view)	401
peer fake-as (IPv6 address family view)	402
peer filter-policy (IPv6 address family view)	402
peer group (IPv6 address family view)	403
peer ignore (IPv6 address family view)	404
peer ipv6-prefix	404
peer ipsec-policy (IPv6 address family view)	405
peer keep-all-routes (IPv6 address family view)	406
peer log-change (IPv6 address family view)	406
peer next-hop-local (IPv6 address family view)	407
peer password	408
peer preferred-value (IPv6 address family view)	409
peer preferred-value (IPv6 BGP-VPN instance view)	409
peer public-as-only (IPv6 address family view)	410
peer reflect-client (IPv6 address family view)	411
peer route-limit (IPv6 address family view)	411
peer route-policy (IPv6 address family view)	412
peer route-policy (IPv6 BGP-VPN instance view)	413
peer route-update-interval (IPv6 address family view)	414
peer substitute-as (IPv6 address family view)	415
peer timer (IPv6 address family view)	415
preference (IPv6 address family view/IPv6 BGP-VPN instance view)	416
reflect between-clients (IPv6 address family view)	417
reflector cluster-id (IPv6 address family view)	418
refresh bgp ipv6	418
reset bgp ipv6	419
reset bgp ipv6 dampening	420
reset bgp ipv6 flap-info	420
router-id	421
synchronization (IPv6 address family view)	422
timer (IPv6 address family view)	422

Routing policy configuration commands 424

Common routing policy configuration commands	424
apply as-path	424
apply comm-list delete	424
apply community	425
apply cost	426
apply cost-type	427

apply extcommunity	428
apply isis	428
apply local-preference	429
apply origin	430
apply preference	430
apply preferred-value	431
apply tag	431
continue	432
display ip as-path	433
display ip community-list	433
display ip extcommunity-list	434
display route-policy	435
if-match as-path	436
if-match community	436
if-match cost	437
if-match extcommunity	438
if-match interface	438
if-match route-type	439
if-match tag	440
ip as-path	440
ip community-list	441
ip extcommunity-list	442
route-policy	443
IPv4 routing policy configuration commands	444
apply fast-reroute	444
apply ip-address next-hop	445
display ip ip-prefix	445
if-match acl	446
if-match ip	447
if-match ip-prefix	448
ip ip-prefix	448
reset ip ip-prefix	449
IPv6 routing policy configuration commands	450
apply ipv6 next-hop	450
display ip ipv6-prefix	450
if-match ipv6	451
ip ipv6-prefix	452
reset ip ipv6-prefix	453
Policy-based routing configuration commands	455
apply ip-address default next-hop	455
apply ip-address next-hop	455
apply ip-precedence	456
display ip policy-based-route	457
display ip policy-based-route setup	458
display policy-based-route	459
if-match acl	460
ip local policy-based-route	461
ip policy-based-route	461
policy-based-route	462
MCE configuration commands	463
description	463
display bgp vpnv4 vpn-instance group	463
display bgp vpnv4 vpn-instance network	465

display bgp vpnv4 vpn-instance paths	466
display bgp vpnv4 vpn-instance peer	467
display bgp vpnv4 vpn-instance routing-table	470
display fib vpn-instance	472
display fib vpn-instance <i>ip-address</i>	474
display ip vpn-instance	475
domain-id	477
export route-policy	478
ext-community-type	479
filter-policy export	480
filter-policy import	480
import route-policy	481
ip binding vpn-instance	482
ip vpn-instance	482
ipv4-family	483
ipv4-family vpn-instance	484
peer allow-as-loop	484
refresh bgp vpn-instance	485
reset bgp vpn-instance	485
reset bgp vpn-instance dampening	486
reset bgp vpn-instance flap-info	487
route-distinguisher	487
routing-table limit	488
vpn-instance-capability simple	489
vpn-target	489
IPv6 MCE configuration commands	491
display bgp vpnv6 vpn-instance peer	491
display bgp vpnv6 vpn-instance routing-table	494
display ipv6 fib vpn-instance	495
display ipv6 fib vpn-instance <i>ipv6-address</i>	496
export route-policy	498
filter-policy export	499
filter-policy import	500
import route-policy	500
ipv6-family	501
ipv6-family vpn-instance	502
refresh bgp ipv6 vpn-instance	502
reset bgp ipv6 vpn-instance	503
routing-table limit	503
vpn-target	504
Support and other resources	506
Contacting HP	506
Subscription service	506
Related information	506
Documents	506
Websites	506
Conventions	507
Index	509

Basic IP routing commands

The term "router" in this chapter refers to both routers and Layer 3 switches.

The term "interface" in the routing features collectively refers to Layer 3 interfaces, including VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

The A5500 SI Switch Series does not support VPN-related parameters.

The A5500 SI Switch Series does not support OSPF, BGP, IS-IS, OSPFv3, IPv6 BGP, or IPv6 IS-IS.

display ip routing-table

Syntax

```
display ip routing-table [ vpn-instance vpn-instance-name ] [ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

verbose: Displays detailed routing table information, including inactive routes. Without this keyword, the command displays only brief information about active routes.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip routing-table** to display brief information about active routes in the routing table.

This command displays brief information about a routing table, with a routing entry contained in one line. The information displayed includes destination IP address/mask length, protocol, priority, cost, next hop, and outbound interface. This command displays only the optimal routes in use.

Use **display ip routing-table verbose** to display detailed information about all routes in the routing table.

This command displays detailed information about all active and inactive routes, including the statistics of the entire routing table and information for each route.

Examples

Display brief information about active routes in the routing table.

```
<Sysname> display ip routing-table
```

```
Routing Tables: Public
```

```
Destinations : 7      Routes : 7
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
1.1.2.0/24	Direct	0	0	1.1.2.1	Vlan11
1.1.2.1/32	Direct	0	0	127.0.0.1	InLoop0
2.2.2.0/24	OSPF	10	2	1.1.2.2	Vlan12
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	Vlan1
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0

Table 1 Command output

Field	Description
Destinations	Number of destination addresses
Routes	Number of routes
Destination/Mask	Destination address/mask length
Proto	Protocol that presents the route
Pre	Priority of the route
Cost	Cost of the route
NextHop	Address of the next hop on the route
Interface	Outbound interface for packets to be forwarded along the route

Display detailed information about all routes in the routing table.

```
<Sysname> display ip routing-table verbose
```

```
Routing Tables: Public
```

```
Destinations : 7      Routes : 7
```

```
Destination: 1.1.2.0/24
  Protocol: Direct          Process ID: 0
  Preference: 0            Cost: 0
  IpPrecedence:           QoSLeId:
  NextHop: 1.1.2.1        Interface: Vlan-interfaces11
  BkNextHop: 0.0.0.0     BkInterface:
  RelyNextHop: 0.0.0.0   Neighbor : 0.0.0.0
  Tunnel ID: 0x0         Label: NULL
  BKTunnel ID: 0x0      BKLabel: NULL
  State: Active Adv      Age: 06h46m22s
  Tag: 0

Destination: 1.1.2.1/32
```

```

    Protocol: Direct          Process ID: 0
    Preference: 0            Cost: 0
    IpPrecedence:           QoS LcId:
    NextHop: 127.0.0.1      Interface: InLoopBack0
    BkNextHop: 0.0.0.0     BkInterface:
    RelyNextHop: 0.0.0.0   Neighbor : 0.0.0.0
    Tunnel ID: 0x0         Label: NULL
    BKTunnel ID: 0x0      BKLabel: NULL
    State: Active NoAdv    Age: 06h46m22s
    Tag: 0

Destination: 2.2.2.0/24
    Protocol: OSPF          Process ID: 1
    Preference: 10         Cost: 2
    IpPrecedence:         QoS LcId:
    NextHop: 1.1.2.2      Interface: Vlan-interface12
    BkNextHop: 0.0.0.0   BkInterface:
    RelyNextHop: 0.0.0.0 Neighbor : 0.0.0.0
    Tunnel ID: 0x0         Label: NULL
    BKTunnel ID: 0x0      BKLabel: NULL
    State: Active Adv     Age: 00h00m53s
    Tag: 0

Destination: 127.0.0.0/8
    Protocol: Direct       Process ID: 0
    Preference: 0          Cost: 0
    IpPrecedence:         QoS LcId:
    NextHop: 127.0.0.1    Interface: InLoopBack0
    BkNextHop: 0.0.0.0   BkInterface:
    RelyNextHop: 0.0.0.0 Neighbor : 0.0.0.0
    Tunnel ID: 0x0         Label: NULL
    BKTunnel ID: 0x0      BKLabel: NULL
    State: Active NoAdv   Age: 06h46m36s
    Tag: 0

Destination: 127.0.0.1/32
    Protocol: Direct       Process ID: 0
    Preference: 0          Cost: 0
    IpPrecedence:         QoS LcId:
    NextHop: 127.0.0.1    Interface: InLoopBack0
    BkNextHop: 0.0.0.0   BkInterface:
    RelyNextHop: 0.0.0.0 Neighbor : 0.0.0.0
    Tunnel ID: 0x0         Label: NULL
    BKTunnel ID: 0x0      BKLabel: NULL
    State: Active NoAdv   Age: 06h46m37s
    Tag: 0

Destination: 192.168.0.0/24

```



```

    Protocol: Direct          Process ID: 0
  Preference: 0              Cost: 0
IpPrecedence:                QoSLocalId:
    NextHop: 192.168.0.1     Interface: Vlan-interface1
    BkNextHop: 0.0.0.0       BkInterface:
  RelyNextHop: 0.0.0.0       Neighbor : 0.0.0.0
    Tunnel ID: 0x0           Label: NULL
  BKTunnel ID: 0x0           BKLabel: NULL
    State: Active Adv        Age: 06h46m35s
    Tag: 0

```

```

Destination: 192.168.0.1/32
  Protocol: Direct          Process ID: 0
  Preference: 0              Cost: 0
IpPrecedence:                QoSLocalId:
    NextHop: 127.0.0.1      Interface: InLoopBack0
    BkNextHop: 0.0.0.0       BkInterface:
  RelyNextHop: 0.0.0.0       Neighbor : 0.0.0.0
    Tunnel ID: 0x0           Label: NULL
  BKTunnel ID: 0x0           BKLabel: NULL
    State: Active NoAdv     Age: 06h46m35s
    Tag: 0

```

Displayed first are statistics for the whole routing table, followed by a detailed description of each route (in sequence).

Table 2 Command output

Field	Description
Destination	Destination address/mask length.
Protocol	Protocol that presents the route.
Process ID	Process ID.
Preference	Priority of the route.
Cost	Cost of the route.
IpPrecedence	IP precedence.
QoSLocalId	QoS-local ID.
NextHop	Address of the next hop on the route.
Interface	Outbound interface for packets to be forwarded along the route.
BkNextHop	Backup next hop.
BkInterface	Backup outbound interface.
RelyNextHop	Next hop address obtained through routing recursion.
Neighbor	Neighboring address determined by routing protocol.
Tunnel ID	Tunnel ID.
Label	Label.
BKTunnel ID	Backup tunnel ID.

Field	Description
BKLabel	Backup label.
State	<p>Route status:</p> <ul style="list-style-type: none"> • Active—This is an active unicast route. • Adv—This route can be advertised. • Delete—This route is deleted. • Gateway—This is an indirect route. • Holddown—Number of holddown routes. Holddown is a route advertisement policy used in some distance vector (D-V) routing protocols, such as RIP, to avoid the propagation of some incorrect routes. It distributes a Holddown route during a period regardless of whether a new route to the same destination is found. For more information, refer to relevant routing protocols. • Int—The route was discovered by an Interior Gateway Protocol (IGP). • NoAdv—The route is not advertised when the router advertises routes based on policies. • NotInstall—Among routes to a destination, the route with the highest priority is installed into the core routing table and advertised. A NotInstall route cannot be installed into the core routing table but can be advertised. • Reject—The packets matching a Reject route will be dropped. Besides, the router sends ICMP unreachable messages to the sources of the dropped packets. The Reject routes are usually used for network testing. • Static—A static route is not lost when you perform the save operation and then restart the router. Routes configured manually are marked as static. • Unicast—Unicast routes. • Inactive—Inactive routes. • Invalid—Invalid routes. • WaitQ—The route is the WaitQ during route recursion. • TunE—Tunnel. • GotQ—The route is in the GotQ during route recursion.
Age	Time for which the route has been in the routing table, in the sequence of hour, minute, and second from left to right.
Tag	Route tag.

display ip routing-table acl

Syntax

```
display ip routing-table [ vpn-instance vpn-instance-name ] acl acl-number [ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

acl-number: Specifies the basic ACL number, in the range of 2000 to 2999.

verbose: Displays detailed routing table information, including inactive routes. Without this argument, the command displays only brief information about active routes.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip routing-table acl** to display information about routes permitted by a specified basic ACL.

For more information about routing policy, see *Layer 3—IP Routing Configuration Guide*.

This command is usually used together with routing policy display commands.

If the specified ACL does not exist or it has no rules configured, the entire routing table is displayed.

Examples

Define basic ACL 2000 and set the route filtering rules.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule deny source any
```

Display brief information about active routes permitted by basic ACL 2000.

```
[Sysname-acl-basic-2000] display ip routing-table acl 2000
Routes Matched by Access list : 2000
Summary Count : 6
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	Direct	0	0	10.1.1.2	Vlan1
10.1.1.2/32	Direct	0	0	127.0.0.1	InLoop0
10.1.2.0/24	Direct	0	0	10.1.2.1	Vlan12
10.1.2.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.3.0/24	Direct	0	0	10.1.3.1	Vlan11
10.1.3.1/32	Direct	0	0	127.0.0.1	InLoop0

For command output, see [Table 1](#).

Display detailed information about both active and inactive routes permitted by basic ACL 2000.

```
<Sysname> display ip routing-table acl 2000 verbose
Routes Matched by Access list : 2000
Summary Count: 6
```

Destination: 10.1.1.0/24
Protocol: Direct Process ID: 0
Preference: 0 Cost: 0
IpPrecedence: QoSLeId:
NextHop: 10.1.1.2 Interface: Vlan-interfacel
BkNextHop: 0.0.0.0 BkInterface:
RelyNextHop: 0.0.0.0 Neighbor: 0.0.0.0
Tunnel ID: 0x0 Label: NULL
BKTunnel ID: 0x0 BKLabel: NULL
State: Active Adv Age: 1d00h25m32s
Tag: 0

Destination: 10.1.1.2/32
Protocol: Direct Process ID: 0
Preference: 0 Cost: 0
IpPrecedence: QoSLeId:
NextHop: 127.0.0.1 Interface: InLoopBack0
BkNextHop: 0.0.0.0 BkInterface:
RelyNextHop: 0.0.0.0 Neighbor: 0.0.0.0
Tunnel ID: 0x0 Label: NULL
BKTunnel ID: 0x0 BKLabel: NULL
State: Active NoAdv Age: 1d00h41m34s
Tag: 0

Destination: 10.1.2.0/24
Protocol: Direct Process ID: 0
Preference: 0 Cost: 0
IpPrecedence: QoSLeId:
NextHop: 10.1.2.1 Interface: Vlan-interfacel2
BkNextHop: 0.0.0.0 BkInterface:
RelyNextHop: 0.0.0.0 Neighbor: 0.0.0.0
Tunnel ID: 0x0 Label: NULL
BKTunnel ID: 0x0 BKLabel: NULL
State: Active Adv Age: 1d00h05m42s
Tag: 0

Destination: 10.1.2.1/32
Protocol: Direct Process ID: 0
Preference: 0 Cost: 0
IpPrecedence: QoSLeId:
NextHop: 127.0.0.1 Interface: InLoopBack0
BkNextHop: 0.0.0.0 BkInterface:
RelyNextHop: 0.0.0.0 Neighbor: 0.0.0.0
Tunnel ID: 0x0 Label: NULL
BKTunnel ID: 0x0 BKLabel: NULL
State: Active NoAdv Age: 1d00h05m42s
Tag: 0

```

Destination: 10.1.3.0/24
  Protocol: Direct          Process ID: 0
  Preference: 0            Cost: 0
  IpPrecedence:           QoSLeId:
  NextHop: 10.1.3.1       Interface: Vlan-interface1
  BkNextHop: 0.0.0.0     BkInterface:
  RelyNextHop: 0.0.0.0   Neighbor: 0.0.0.0
  Tunnel ID: 0x0         Label: NULL
  BKTunnel ID: 0x0      BKLabel: NULL
  State: Active Adv      Age: 1d00h05m31s
  Tag: 0

```

```

Destination: 10.1.3.1/32
  Protocol: Direct          Process ID: 0
  Preference: 0            Cost: 0
  IpPrecedence:           QoSLeId:
  NextHop: 127.0.0.1     Interface: InLoopBack0
  BkNextHop: 0.0.0.0     BkInterface:
  RelyNextHop: 0.0.0.0   Neighbor: 0.0.0.0
  Tunnel ID: 0x0         Label: NULL
  BKTunnel ID: 0x0      BKLabel: NULL
  State: Active NoAdv    Age: 1d00h05m32s
  Tag: 0

```

For command output, see [Table 2](#).

display ip routing-table *ip-address*

Syntax

```
display ip routing-table [ vpn-instance vpn-instance-name ] ip-address [ mask | mask-length ]
[ longer-match ] [ verbose ] [ | { begin | exclude | include } regular-expression ]
```

```
display ip routing-table [ vpn-instance vpn-instance-name ] ip-address1 { mask | mask-length }
ip-address2 { mask | mask-length } [ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

ip-address: Specifies the destination IP address, in dotted decimal format.

mask | *mask-length*: Specifies the IP address mask, in dotted decimal format or represented by an integer in the range of 0 to 32.

longer-match: Displays the route with the longest mask.

verbose: Displays detailed routing table information, including both active and inactive routes. Without this argument, the command displays only brief information about active routes.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip routing-table ip-address** to display information about routes to a specified destination address.

Executing the command with different parameters yields different output:

- **display ip routing-table ip-address:**
 - The system ANDs the input destination IP address with the subnet mask in each route entry.
 - The system ANDs the destination IP address in each route entry with its own subnet mask.If the two operations yield the same result for an entry and this entry is active, it is displayed.
- **display ip routing-table ip-address mask:**
 - The system ANDs the input destination IP address with the input subnet mask.
 - The system ANDs the destination IP address in each route entry with the input subnet mask.If the two operations yield the same result for an entry and the entry is active with a subnet mask less than or equal to the input subnet mask, the entry is displayed.
Only route entries that exactly match the input destination address and mask are displayed.
- **display ip routing-table ip-address longer-match:**
 - The system ANDs the input destination IP address with the subnet mask in each route entry.
 - The system ANDs the destination IP address in each route entry with its own subnet mask.If the two operations yield the same result for multiple entries that are active, the one with the longest mask length is displayed.
- **display ip routing-table ip-address mask longer-match:**
 - The system ANDs the input destination IP address with the input subnet mask.
 - The system ANDs the destination IP address in each route entry with the input subnet mask.If the two operations yield the same result for multiple entries with a mask less than or equal to the input subnet mask, the one that is active with longest mask length is displayed.

Use **display ip routing-table ip-address1 { mask-length | mask } ip-address2 { mask-length | mask }** to display route entries with destination addresses within a specified range.

Examples

```
# Display route entries for the destination IP address 11.1.1.1.
```

```
<Sysname> display ip routing-table 11.1.1.1
```

```
Routing Table : Public
```

```
Summary Count : 4
```

```
Destination/Mask    Proto  Pre  Cost           NextHop           Interface
```

```

0.0.0.0/0          Static 60 0          0.0.0.0          NULL0
11.0.0.0/8        Static 60 0          0.0.0.0          NULL0
11.1.0.0/16       Static 60 0          0.0.0.0          NULL0
11.1.1.0/24       Static 60 0          0.0.0.0          NULL0

```

Display route entries by specifying a destination IP address and the **longer-match** keyword.

```

<Sysname> display ip routing-table 11.1.1.1 longer-match
Routing Table : Public
Summary Count : 1

```

```

Destination/Mask  Proto  Pre  Cost          NextHop          Interface
11.1.1.0/24      Static 60  0          0.0.0.0          NULL0

```

Display route entries by specifying a destination IP address and mask.

```

<Sysname> display ip routing-table 11.1.1.1 24
Routing Table : Public
Summary Count : 1

```

```

Destination/Mask  Proto  Pre  Cost          NextHop          Interface
11.1.1.0/24      Static 60  0          0.0.0.0          NULL0

```

Display route entries by specifying a destination IP address and mask and the **longer-match** keyword.

```

<Sysname> display ip routing-table 11.1.1.1 24 longer-match
Routing Table : Public
Summary Count : 1

```

```

Destination/Mask  Proto  Pre  Cost          NextHop          Interface
11.1.1.0/24      Static 60  0          0.0.0.0          NULL0

```

Display route entries for destination addresses in the range of 1.1.1.0 to 5.5.5.0.

```

<Sysname> display ip routing-table 1.1.1.0 24 5.5.5.0 24
Routing Table : Public

```

```

Destination/Mask  Proto  Pre  Cost          NextHop          Interface
1.1.1.0/24        Direct 0    0          1.1.1.1          Vlan1
1.1.1.1/32        Direct 0    0          127.0.0.1         InLoop0
2.2.2.0/24        Direct 0    0          2.2.2.1          Vlan2
3.3.3.0/24        Direct 0    0          3.3.3.1          Vlan12
3.3.3.1/32        Direct 0    0          127.0.0.1         InLoop0
4.4.4.0/24        Direct 0    0          4.4.4.1          Vlan11
4.4.4.1/32        Direct 0    0          127.0.0.1         InLoop0

```

For command output, see [Table 1](#).

display ip routing-table ip-prefix

Syntax

```
display ip routing-table [ vpn-instance vpn-instance-name ] ip-prefix ip-prefix-name [ verbose ] [ |  
{ begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

ip-prefix-name: Specifies the IP prefix list name, a string of 1 to 19 characters.

verbose: Displays detailed routing table information, including inactive routes. Without this argument, the command displays only brief information about active routes.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip routing-table ip-prefix** to display information about routes permitted by a specified prefix list.

This command is usually used together with routing policy display commands. If the specified prefix list is not configured, detailed information about all routes (with the **verbose** keyword) or brief information about all active routes (without the **verbose** keyword) is displayed.

Examples

Configure a prefix list named **test**, permitting routes with a prefix of 2.2.2.0 and a mask length between 24 and 32.

```
<Sysname> system-view  
[Sysname] ip ip-prefix test permit 2.2.2.0 24 less-equal 32
```

Display brief information about active routes permitted by the prefix list **test**.

```
[Sysname] display ip routing-table ip-prefix test  
Routes Matched by Prefix list : test  
Summary Count : 2  
Destination/Mask  Proto  Pre  Cost           NextHop           Interface  
2.2.2.0/24         Direct  0    0             2.2.2.1           Vlan2  
2.2.2.1/32         Direct  0    0             127.0.0.1         InLoop0
```

For command output, see [Table 1](#).

Display detailed information about both active and inactive routes permitted by IP prefix list **test**.


```
[Sysname] display ip routing-table ip-prefix test verbose
Routes Matched by Prefix list test :
Summary Count : 2

Destination: 2.2.2.0/24
  Protocol: Direct          Process ID: 0
  Preference: 0            Cost: 0
  IpPrecedence:           QoSLeId:
  NextHop: 2.2.2.1        Interface: Vlan-interface2
  BkNextHop: 0.0.0.0      BkInterface:
  RelyNextHop: 0.0.0.0    Neighbor : 0.0.0.0
  Tunnel ID: 0x0          Label: NULL
  BKTunnel ID: 0x0        BKLabel: NULL
  State: Active Adv      Age: 1d00h20m52s
  Tag: 0
```

```
Destination: 2.2.2.1/32
  Protocol: Direct          Process ID: 0
  Preference: 0            Cost: 0
  IpPrecedence:           QoSLeId:
  NextHop: 127.0.0.1      Interface: InLoopBack0
  BkNextHop: 0.0.0.0      BkInterface:
  RelyNextHop: 0.0.0.0    Neighbor : 0.0.0.0
  Tunnel ID: 0x0          Label: NULL
  BKTunnel ID: 0x0        BKLabel: NULL
  State: Active NoAdv     Age: 1d00h20m52s
  Tag: 0
```

For command output, see [Table 2](#).

display ip routing-table protocol

Syntax

```
display ip routing-table [ vpn-instance vpn-instance-name ] protocol protocol [ inactive | verbose ] [ [ begin | exclude | include ] regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

protocol: Specifies the routing protocol. It can be **bgp**, **direct**, **isis**, **nat**, **ospf**, **rip**, and **static**.

inactive: Displays information about only inactive routes. Without this argument, the command displays information about both active and inactive routes.

verbose: Displays detailed routing table information. Without this argument, the command displays brief routing table information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip routing-table protocol** to display routing information of a specified routing protocol.

Examples

Display brief information about direct routes.

```
<Sysname> display ip routing-table protocol direct
```

```
Public Routing Table : Direct
```

```
Summary Count : 6
```

```
Direct Routing Table Status : <Active>
```

```
Summary Count : 6
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
2.2.2.0/24	Direct	0	0	2.2.2.1	Vlan2
2.2.2.2/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.80.0/24	Direct	0	0	192.168.80.10	Vlan11
192.168.80.10/32	Direct	0	0	127.0.0.1	InLoop0

```
Direct Routing Table Status : <Inactive>
```

```
Summary Count : 0
```

Display brief information about static routes.

```
<Sysname> display ip routing-table protocol static
```

```
Public Routing Table : Static
```

```
Summary Count : 2
```

```
Static Routing Table Status : <Active>
```

```
Summary Count : 0
```

```
Static Routing Table Status : <Inactive>
```

```
Summary Count : 2
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
1.2.3.0/24	Static	60	0	1.2.4.5	Vlan10
3.0.0.0/8	Static	60	0	2.2.2.2	Vlan11

For command output, see [Table 1](#).

display ip routing-table statistics

Syntax

```
display ip routing-table [ vpn-instance vpn-instance-name ] statistics [ | { begin | exclude | include }  
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip routing-table statistics** to display the route statistics of the routing table.

Examples

```
# Display route statistics in the routing table.
```

```
<Sysname> display ip routing-table statistics
```

Proto	route	active	added	deleted	freed
DIRECT	24	4	25	1	0
STATIC	4	1	4	0	0
RIP	0	0	0	0	0
OSPF	0	0	0	0	0
IS-IS	0	0	0	0	0
BGP	0	0	0	0	0
Total	28	5	29	1	0

Table 3 Command output

Field	Description
Proto	Origin of the routes
route	Number of routes from the origin
active	Number of active routes from the origin
added	Number of routes added into the routing table since the router started up or the routing table was last cleared
deleted	Number of routes marked as deleted, which will be freed after a period
freed	Number of routes that got freed (got removed permanently)

Field	Description
Total	Total number

display ipv6 routing-table

Syntax

```
display ipv6 routing-table [ vpn-instance vpn-instance-name ] [ verbose ] [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

verbose: Displays detailed information about both active and inactive routes. Without this keyword, only brief information about active routes is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 routing-table** to display brief IPv6 routing information, including destination IP address and prefix, protocol type, priority, metric, next hop, and outbound interface.

The command displays only active routes (the brief information about the current optimal routes).

Use **display ipv6 routing-table verbose** to display detailed information about all IPv6 routes, including both active and inactive routes. The output shows the statistics of the entire routing table, and then the detailed information of each route.

Examples

```
# Display brief routing table information
<Sysname> display ipv6 routing-table
Routing Table : Public
      Destinations : 1          Routes : 1
Destination: ::1/128          Protocol : Direct
NextHop      : ::1            Preference: 0
Interface    : InLoop0        Cost       : 0
```

Table 4 Command output

Field	Description
Destination	IPv6 address of the destination network/host
NextHop	Next hop address
Preference	Route priority
Interface	Outbound interface
Protocol	Routing protocol
Cost	Route cost

Display detailed routing table information.

```
<Sysname> display ipv6 routing-table verbose
```

```
Routing Table : Public
```

```
Destinations : 1      Routes : 1
```

```

Destination : ::1          PrefixLength : 128
NextHop      : ::1          Preference    : 0
IpPrecedence :              QoSLocalId    :
RelayNextHop : ::          Tag           : 0H
Neighbor     : ::          ProcessID     : 0
Interface    : InLoopBack0 Protocol      : Direct
State        : Active NoAdv Cost           : 0
Tunnel ID    : 0x0         Label         : NULL
Age          : 22161sec

```

Table 5 Command output

Field	Description
Destination	IPv6 address of the destination network/host
PrefixLength	Prefix length of the address
NextHop	Next hop
Preference	Route priority
IpPrecedence	IP precedence
QoSLocalId	QoS-local ID
RelayNextHop	Recursive next hop
Tag	Tag of the route
Neighbor	Neighbor address
ProcessID	Process ID
Interface	Outbound interface
Protocol	Routing protocol
State	State of the route, Active, Inactive, Adv (advertised), or NoAdv (not advertised)
Cost	Cost of the route

Field	Description
Tunnel ID	Tunnel ID
Label	Label
Age	Time that has elapsed since the route was generated

display ipv6 routing-table acl

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **acl** *acl6-number* [**verbose**] [|] { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

acl6-number: Specifies the basic IPv6 ACL number, in the range of 2000 to 2999.

verbose: Displays both active and inactive verbose routing information permitted by the ACL. Without this keyword, only brief active routing information is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 routing-table acl** to display routing information permitted by the IPv6 ACL.

If the specified IPv6 ACL is not available, all routing information is displayed.

Examples

```
# Display brief routing information permitted by ACL 2000.
<Sysname> display ipv6 routing-table acl 2000
Routes Matched by Access list 2000 :
Summary Count : 2
Destination : ::1/128                Protocol : Direct
NextHop      : ::1                    Preference: 0
Interface    : InLoop0                Cost      : 0

Destination : 1:1::/64                Protocol : Static
NextHop      : ::                      Preference: 60
```

Interface : NULL0

Cost : 0

For command output, see [Table 4](#).

display ipv6 routing-table ipv6-address

Syntax

```
display ipv6 routing-table [ vpn-instance vpn-instance-name ] ipv6-address prefix-length [ longer-match ]  
[ verbose ] [ | { begin | exclude | include } regular-expression ]
```

```
display ipv6 routing-table [ vpn-instance vpn-instance-name ] ipv6-address1 prefix-length1  
ipv6-address2 prefix-length2 [ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

ipv6-address: Specifies the destination IPv6 address.

prefix-length: Specifies the prefix length, in the range of 0 to 128.

longer-match: Displays the matched route having the longest prefix length.

ipv6-address1/ipv6-address2: Specifies the an IPv6 address range from IPv6 address1 to IPv6 address2.

prefix-length1/prefix-length2: Specifies the prefix length, in the range of 0 to 128.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 routing-table** *ipv6-address* to display routing information about the specified destination IPv6 address.

Executing the command with different parameters yields different output:

- **display ipv6 routing-table** *ipv6-address prefix-length*:
 - The system ANDs the input destination IPv6 address with the input prefix length.
 - The system ANDs the destination IPv6 address in each route entry with the input prefix length.If the two operations yield the same result for an entry and the entry is active with a prefix length less than or equal to the input prefix length, the entry is displayed.

- Only route entries that exactly match the input destination address and prefix length are displayed.
- **display ipv6 routing-table *ipv6-address prefix-length longer-match*:**
 - The system ANDs the input destination IPv6 address with the input prefix length.
 - The system ANDs the destination IPv6 address in each route entry with the input prefix length. If the two operations yield the same result for multiple entries with a prefix length less than or equal to the input prefix length, the one that is active with the longest prefix length is displayed.

Use **display ipv6 routing-table *ipv6-address1 ipv6-address2*** to display routes whose destinations fall into the specified IPv6 address range.

Examples

Display brief information about the route matching the specified destination IPv6 address.

```
<Sysname> display ipv6 routing-table 10::1 127
```

```
Routing Table: Public
```

```
Summary Count: 3
```

```
Destination: 10::/64                                Protocol : Static
NextHop      : ::                                    Preference: 60
Interface   : NULL0                                 Cost      : 0
```

```
Destination: 10::/68                                Protocol : Static
NextHop      : ::                                    Preference: 60
Interface   : NULL0                                 Cost      : 0
```

```
Destination: 10::/120                                Protocol : Static
NextHop      : ::                                    Preference: 60
Interface   : NULL0                                 Cost      : 0
```

Display brief information about the matched route with the longest prefix length.

```
<Sysname> display ipv6 routing-table 10:: 127 longer-match
```

```
Routing Tables: Public
```

```
Summary Count : 1
```

```
Destination: 10::/120                                Protocol : Static
NextHop      : ::                                    Preference: 60
Interface   : NULL0                                 Cost      : 0
```

Display routes whose destinations fall into the specified IPv6 address range.

```
<Sysname> display ipv6 routing-table 100:: 64 300:: 64
```

```
Routing Table : Public
```

```
Summary Count : 3
```

```
Destination: 100::/64                                Protocol : Static
NextHop      : ::                                    Preference: 60
Interface   : NULL0                                 Cost      : 0
```

```
Destination: 200::/64                                Protocol : Static
NextHop      : ::                                    Preference: 60
Interface   : NULL0                                 Cost      : 0
```



```

Destination: 300::/64
NextHop      : ::
Interface    : NULL0
              Cost      : 0
Protocol     : Static
Preference   : 60
Cost         : 0

```

For command output, see [Table 4](#) .

display ipv6 routing-table ipv6-prefix

Syntax

```

display ipv6 routing-table [ vpn-instance vpn-instance-name ] ipv6-prefix ipv6-prefix-name [ verbose ]
[ | { begin | exclude | include } regular-expression ]

```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

ipv6-prefix-name: Specifies the name of the IPv6 prefix list, in the range of 1 to 19 characters.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 routing-table ipv6-prefix** to display routes permitted by the IPv6 prefix list.

Examples

Display brief active routing information permitted by the IPv6 prefix list **test2**.

```
<Sysname> display ipv6 routing-table ipv6-prefix test2
```

```
Routes Matched by Prefix list test2 :
```

```
Summary Count : 1
```

```

Destination: 100::/64
NextHop      : ::
Interface    : NULL0
              Cost      : 0
Protocol     : Static
Preference   : 60
Cost         : 0

```

For command output, see [Table 4](#).

display ipv6 routing-table protocol

Syntax

```
display ipv6 routing-table [ vpn-instance vpn-instance-name ] protocol protocol [ inactive | verbose ] [ |  
{ begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

protocol: Displays routes of a routing protocol, which can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, and **static**.

inactive: Displays only inactive routes. Without this keyword, all active and inactive routes are displayed.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 routing-table protocol** to display IPv6 routes of a specified routing protocol.

Examples

```
# Display brief information about all direct routes.
```

```
<Sysname> display ipv6 routing-table protocol direct
```

```
Public Routing Table : Direct
```

```
Summary Count : 1
```

```
Direct Routing Table Status : <Active>
```

```
Summary Count : 1
```

```
Destination: ::1/128
```

```
Protocol : Direct
```

```
NextHop : ::1
```

```
Preference: 0
```

```
Interface : InLoop0
```

```
Cost : 0
```

```
Direct Routing Table Status : <Inactive>
```

```
Summary Count : 0
```

For command output, see [Table 4](#).

display ipv6 routing-table statistics

Syntax

```
display ipv6 routing-table [ vpn-instance vpn-instance-name ] statistics [ | { begin | exclude | include }  
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 routing-table statistics** to display IPv6 routing statistics, including total route number, added route number, and deleted route number.

Examples

```
# Display IPv6 routing statistics.
```

```
<Sysname> display ipv6 routing-table statistics
```

Protocol	route	active	added	deleted	freed
DIRECT	1	1	1	0	0
STATIC	3	0	3	0	0
RIPng	0	0	0	0	0
OSPFv3	0	0	0	0	0
IS-ISv6	0	0	0	0	0
BGP4+	0	0	0	0	0
Total	4	1	4	0	0

Table 6 Command output

Field	Description
Protocol	Routing protocol
route	Route number of the protocol
active	Number of active routes
added	Routes added after the last startup of the router
deleted	Deleted routes, which will be released after a specified time
freed	Released (totally removed from the routing table) route number

Field	Description
Total	Total number of routes

reset ip routing-table statistics protocol

Syntax

```
reset ip routing-table statistics protocol [ vpn-instance vpn-instance-name ] { protocol | all }
```

View

User view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the routing statistics of the public network is cleared.

protocol: Clears statistics for the IPv4 routing protocol, which can be **bgp**, **direct**, **isis**, **ospf**, **rip**, or **static**.

all: Clears statistics for all IPv4 routing protocols.

Description

Use **reset ip routing-table statistics protocol** to clear routing statistics for the routing table.

Examples

Clear routing statistics in the routing table of VPN instance **Sysname1**.

```
<Sysname> reset ip routing-table statistics protocol vpn-instance Sysname1 all
```

reset ipv6 routing-table statistics

Syntax

```
reset ipv6 routing-table statistics protocol [ vpn-instance vpn-instance-name ] { protocol | all }
```

View

User view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

protocol: Clears statistics for the routing protocol, which can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

all: Clears statistics for all IPv6 routing protocols.

Description

Use **reset ipv6 routing-table statistics** to clear the route statistics of the routing table.

Examples

Clear statistics for all routing protocols.

```
<Sysname> reset ipv6 routing-table statistics protocol all
```

Static routing configuration commands

The term "router" in this chapter refers to both routers and Layer 3 switches.

The A5500 SI Switch Series does not support VPN and BFD related parameters or FRR.

delete static-routes all

Syntax

```
delete [ vpn-instance vpn-instance-name ] static-routes all
```

View

System view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, all static routes on the public network are deleted.

Description

Use **delete static-routes all** to delete all static routes.

When you use this command to delete static routes, the system will prompt you to confirm the operation before deleting all the static routes.

Related commands: **display ip routing-table** and **ip route-static**.

Examples

```
# Delete all static routes on the router.
```

```
<Sysname> system-view
```

```
[Sysname] delete static-routes all
```

```
This will erase all ipv4 static routes and their configurations, you must reconfigure all static routes
```

```
Are you sure?[Y/N]:Y
```

ip route-static

Syntax

```
ip route-static dest-address { mask | mask-length } { next-hop-address [ bfd control-packet [ bfd-source ip-address ] | track track-entry-number ] | interface-type interface-number [ next-hop-address ] [ bfd { control-packet [ bfd-source ip-address ] | echo-packet } ] | vpn-instance d-vpn-instance-name next-hop-address [ bfd control-packet bfd-source ip-address | track track-entry-number ] } [ preference preference-value ] [ tag tag-value ] [ permanent ] [ description description-text ]
```

```
undo ip route-static dest-address { mask | mask-length } [ next-hop-address | interface-type interface-number [ next-hop-address ] | vpn-instance d-vpn-instance-name next-hop-address ] [ preference preference-value ]
```

```
ip route-static vpn-instance s-vpn-instance-name&<1-6> dest-address { mask | mask-length }  
{ next-hop-address [ public ] [ bfd control-packet [ bfd-source ip-address ] | track track-entry-number ] |  
interface-type interface-number [ next-hop-address ] [ bfd { control-packet [ bfd-source ip-address ] |  
echo-packet } ] | vpn-instance d-vpn-instance-name next-hop-address [ bfd control-packet bfd-source  
ip-address | track track-entry-number ] } [ preference preference-value ] [ tag tag-value ] [ permanent ]  
[ description description-text ]
```

```
undo ip route-static vpn-instance s-vpn-instance-name&<1-6> dest-address { mask | mask-length }  
[ next-hop-address [ public ] | interface-type interface-number [ next-hop-address ] | vpn-instance  
d-vpn-instance-name next-hop-address ] [ preference preference-value ]
```

View

System view

Default level

2: System level

Parameters

vpn-instance *s-vpn-instance-name*&<1-6>: Specifies a source MPLS L3VPN. *s-vpn-instance-name* is a case-sensitive string of 1 to 31 characters. &<1-6> indicates the argument before it can be entered up to 6 times. Each VPN has its own routing table, and the configured static route is installed in the routing tables of the specified VPNs.

dest-address: Specifies the destination IP address of the static route, in dotted decimal notation.

mask: Specifies the mask of the IP address, in dotted decimal notation.

mask-length: Specifies the mask length, in the range of 0 to 32.

next-hop-address: Specifies the IP address of the next hop, in dotted decimal notation.

interface-type interface-number: Specifies the output interface by its type and number. If the output interface is a broadcast interface, such as an Ethernet interface or a VLAN interface, the next hop address must be specified.

vpn-instance *d-vpn-instance-name*: Specifies a destination MPLS L3VPN. *d-vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If a destination VPN is specified, the router will search the output interface in the destination VPN based on the configured *next-hop-address*.

next-hop-address **public**: Indicates that the specified *next-hop-address* is a public network address, rather than a VPN instance address.

preference *preference-value* : Specifies the preference of the static route, in the range of 1 to 255 and defaults to 60.

tag *tag-value*: Sets a tag value for the static route from 1 to 4294967295. The default is 0. Tags of routes are used in routing policies to control routing. For more information about routing policies, see "[Routing policy configuration commands](#)."

permanent: Specifies the route as a permanent static route. If the output interface is down, the permanent static route is still active.

description *description-text*: Configures a description for the static route, which consists of 1 to 60 characters, including special characters like space, but excluding question marks (?).

bfd: Enable the bidirectional forwarding detection (BFD) function to detect reachability of the static route's next hop. Once the next hop is unreachable, the system will switch to a backup route.

control-packet: Implements BFD in the control mode.

echo-packet: Implements BFD in the echo mode.

bfd-source ip-address: Specifies the source address of BFD packets. HP recommends you configure loopback interface address.

track track-entry-number: Associates the static route with a track entry. Use the *track-entry-number* argument to specify a track entry number, in the range of 1 to 1024.

Description

Use **ip route-static** to configure a unicast static route.

Use **undo ip route-static** to delete a unicast static route.

When you configure a unicast static route, follow these guidelines:

- If the destination IP address and the mask are both 0.0.0.0 (or 0), the configured route is a default route. The default route will be used for forwarding a packet if no route is available for the packet in the routing table.
- Implement different routing policies by tuning route preference. For example, to enable multiple routes to the same destination address to share load, assign the same preference to the routes; to enable them to back up one another, assign different preferences to them.
- Specify the output interface or the next hop address of the static route as needed.
 - If the output interface supports network address-to-link layer address resolution or is a point-to-point interface, you may specify only the interface or the next hop address.
 - If the output interface is a Null 0 interface, no next hop address is required.
 - If you specify a broadcast interface (such as an Ethernet interface or a VLAN interface) as the output interface for a static route, you must specify the corresponding next hop of the interface at the same time.
 - To implement BFD with the **control-packet** mode, the remote end must create a BFD session; otherwise the BFD function cannot work. To implement BFD with the **echo-packet** mode, the BFD function can work without the remote end needing to create any BFD session.
 - To configure a static route and enable BFD control packet mode for it, specify an output interface and a direct next hop—BFD establishes a direct session, or specify an indirect next hop and a specific BFD packet source address—BFD establishes an indirect session—for the static route.
- The next hop address cannot be the IP address of a local interface (such as an Ethernet interface and VLAN interface). Otherwise, the static route does not take effect.
- Enabling BFD for a flapping route could worsen the situation. Therefore, use it with caution. For more information about BFD, see *High Availability Configuration Guide*.
- If the track module uses NQA to detect the reachability of the private network static route's next hop, the VPN instance number of the static route's next hop must be identical to that configured in the NQA test group.
- If a static route needs route recursion, the associated track entry must monitor the next hop of the recursive route instead of that of the static route. Otherwise, a valid route may be mistakenly considered invalid.
- Do not specify the **permanent** keyword together with the **bfd** or **track** keyword.

Related commands: **display ip routing-table** and **ip route-static default-preference**.

Examples

Configure a static route, whose destination address is 1.1.1.1/24, next hop address is 2.2.2.2, tag value is 45, and description information is **for internet & intranet**.


```

<Sysname> system-view
[Sysname] ip route-static 1.1.1.1 24 2.2.2.2 tag 45 description for internet & intranet
# Configure a static route for a VPN instance named vpn1: the destination address is 1.1.1.1/16 and the
next hop address is 1.1.1.2, which is the address of this VPN instance.
<Sysname> system-view
[Sysname] ip route-static vpn-instance vpn1 1.1.1.1 16 vpn-instance vpn1 1.1.1.2
# Configure a static route: the destination address is 1.1.1.1/24, the output interface is Vlan-interface11,
and the next hop address is 2.2.2.2, and enable BFD with the echo packet mode.
<Sysname> system-view
[Sysname] ip route-static 1.1.1.1 24 Vlan-interface 11 2.2.2.2 bfd echo-packet

```

ip route-static default-preference

Syntax

```

ip route-static default-preference default-preference-value
undo ip route-static default-preference

```

View

System view

Default level

2: System level

Parameters

default-preference-value: Specifies the default preference for static routes, in the range of 1 to 255.

Description

Use **ip route-static default-preference** to configure the default preference for static routes.

Use **undo ip route-static default-preference** to restore the default.

By default, the default preference of static routes is 60.

If no preference is specified when configuring a static route, the default preference is used.

When the default preference is re-configured, it applies only to newly added static routes.

Related commands: **display ip routing-table** and **ip route-static**.

Examples

```

# Set the default preference of static routes to 120.
<Sysname> system-view
[Sysname] ip route-static default-preference 120

```

ip route-static fast-reroute

Syntax

```

ip route-static [ vpn-instance vpn-instance-name ] fast-reroute route-policy route-policy-name
undo ip route-static [ vpn-instance vpn-instance-name ] fast-reroute

```

View

System view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN to configure FRR for all matching static routes in it. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, FRR is configured for all static routes on the public network.

route-policy *route-policy-name*: References a routing policy. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

Description

Use **ip route-static fast-reroute** to configure static route fast reroute (FRR).

Use **undo ip route-static fast-reroute** to restore the default.

By default, static route FRR is not configured.

Configuring static route FRR needs to reference a routing policy, which specifies a backup next hop with the **apply fast-reroute backup-interface** command. For more information about the command and routing policy configurations, see *Layer 3—IP Routing Configuration Guide*.

Static route FRR takes effect only for static routes that have both the output interface and next hop specified.

Do not use static route FRR and BFD (for static route) at the same time.

Example

Enable static route FRR to designate a backup next hop using routing policy **frr**.

```
<Sysname> system-view
[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] ip ip-prefix abc index 10 permit 100.1.1.0 24
[Sysname] route-policy frr permit node 10
[Sysname-route-policy] if-match ip-prefix abc
[Sysname-route-policy] apply fast-reroute backup-interface vlan-interface 1
backup-nexthop 193.1.1.8
[Sysname-route-policy] quit
[Sysname] ip route-static fast-reroute route-policy frr
```

RIP configuration commands

The term "router" in this chapter refers to both routers and Layer 3 switches.

The A5500 SI Switch Series does not support VPN and BFD related parameters or FRR.

checkzero

Syntax

```
checkzero  
undo checkzero
```

View

RIP view

Default level

2: System level

Parameters

None

Description

Use **checkzero** to enable zero field check on RIPv1 messages.

Use **undo checkzero** to disable zero field check.

The zero field check function is enabled by default.

After the zero field check is enabled, the router discards RIPv1 messages in which zero fields are non-zero. If all messages are trusty, disable this feature to reduce the processing time of the CPU.

Examples

```
# Disable the zero field check on RIPv1 messages for RIP process 100.  
<Sysname> system-view  
[Sysname] rip 100  
[Sysname-rip-100] undo checkzero
```

default cost (RIP view)

Syntax

```
default cost value  
undo default cost
```

View

RIP view

Default level

2: System level

Parameters

value: Default metric of redistributed routes, in the range of 0 to 16.

Description

Use **default cost** to configure the default metric for redistributed routes.

Use **undo default cost** to restore the default.

By default, the default metric of redistributed routes is 0.

When you use the **import-route** command to redistribute routes from other protocols without specifying a metric, the metric specified by the **default cost** command applies.

Related command: **import-route**.

Examples

```
# Configure the default metric for redistributed routes as 3.
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] default cost 3
```

default-route

Syntax

default-route { **only** | **originate** } [**cost** *cost*]

undo default-route

View

RIP view

Default level

2: System level

Parameters

only: Advertises only a default route.

originate: Advertises both a default route and other routes.

cost: Cost of the default route, in the range of 1 to 15. The default is 1.

Description

Use **default-route** to configure all the interfaces under the RIP process to advertise a default route with the specified metric to RIP neighbors.

Use **undo default-route** to disable all the interfaces under the RIP process from sending a default route.

By default, no default route is sent to RIP neighbors.

The RIP router with this feature configured will not receive any default routes from RIP neighbors.

Related commands: **rip default-route**.

Examples

```
# Configure all the interfaces under RIP process 100 to send only a default route with a metric of 2 to RIP neighbors.
<Sysname> system-view
```

```
[Sysname] rip 100
[Sysname-rip-100] default-route only cost 2
```

display rip

Syntax

```
display rip [ process-id | vpn-instance vpn-instance-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: RIP process ID, in the range of 1 to 65535. If no process ID is specified, information about all configured RIP processes is displayed.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the information of the public network is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rip** to display the current status and configuration information of the specified RIP process.

Examples

```
# Display the current status and configuration information of all configured RIP processes.
```

```
<Sysname> display rip
Public VPN-instance name :

RIP process : 1
RIP version : 1
Preference : 100
Checkzero : Enabled
Default-cost : 0
Summary : Enabled
Hostroutes : Enabled
Maximum number of balanced paths : 8
Update time : 30 sec(s) Timeout time : 180 sec(s)
Suppress time : 120 sec(s) Garbage-collect time : 120 sec(s)
update output delay : 20(ms) output count : 3
TRIP retransmit time : 5 sec(s)
TRIP response packets retransmit count : 36
```

```

Silent interfaces : None
Default routes : Only Default route cost : 3
Verify-source : Enabled
Networks :
    192.168.1.0
Configured peers : None
Triggered updates sent : 0
Number of routes changes : 0
Number of replies to queries : 0

```

Table 7 Command output

Field	Description
Public VPN-instance name (or Private VPN-instance name)	The RIP process runs under a public VPN instance./The RIP process runs under a private VPN instance.
RIP process	RIP process ID.
RIP version	RIP version 1 or 2.
Preference	RIP route priority.
Checkzero	Indicates whether the zero field check is enabled for RIPv1 messages.
Default-cost	Default cost of the redistributed routes.
Summary	Indicates whether route summarization is enabled.
Hostroutes	Indicates whether to receive host routes.
Maximum number of balanced paths	Maximum number of load balanced routes.
Update time	RIP update interval.
Timeout time	RIP timeout time.
Suppress time	RIP suppress interval.
update output delay	RIP packet sending interval.
output count	Maximum number of RIP packets sent at each interval.
Garbage-collect time	RIP garbage collection interval.
TRIP retransmit time	TRIP retransmit interval for sending update requests and responses.
TRIP response packets retransmit count	Maximum retransmit times for update requests and responses.
Silent interfaces	Number of silent interfaces, which do not periodically send updates.
Default routes	Indicates whether a default route is sent to RIP neighbors: <ul style="list-style-type: none"> • only—Means only a default route is advertised. • originate—Means a default route is advertised along with other routes. • disable—Means no default route is advertised.
Default route cost	Cost of the default route.

Field	Description
Verify-source	Indicates whether the source IP address is checked on the received RIP routing updates.
Networks	Networks enabled with RIP.
Configured peers	Configured neighbors.
Triggered updates sent	Number of sent triggered updates.
Number of routes changes	Number of changed routes in the database.
Number of replies to queries	Number of RIP responses.

display rip database

Syntax

display rip *process-id* **database** [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

process-id: RIP process ID, in the range of 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rip database** to display active routes in the database of the specified RIP process, which are sent in normal RIP routing updates.

Examples

Display the active routes in the database of RIP process 100.

```
<Sysname> display rip 100 database
 10.0.0.0/8, cost 1, ClassfulSumm
 10.0.0.0/24, cost 1, nexthop 10.0.0.1, Rip-interface
 11.0.0.0/8, cost 1, ClassfulSumm
 11.0.0.0/24, cost 1, nexthop 10.0.0.1, Imported
```

Table 8 Command output

Field	Description
X.X.X.X/X	Destination address and subnet mask.

Field	Description
cost	Cost of the route.
classful-summ	Indicates the route is a RIP summary route.
Nexthop	Address of the next hop.
Rip-interface	Routes learned from a RIP-enabled interface.
imported	Routes redistributed from other routing protocols.

display rip interface

Syntax

```
display rip process-id interface [ interface-type interface-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: RIP process ID, in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rip interface** to display the RIP interface information of the RIP process.

If no interface is specified, information about all RIP interfaces of the RIP process is displayed.

Examples

```
# Display all the interface information of RIP process 1.
```

```
<Sysname> display rip 1 interface
```

```
Interface-name: Vlan-interface11
  Address/Mask:1.1.1.1/24          Version:RIPv1
  MetricIn:5                      MetricIn route policy:123
  MetricOut:5                     MetricOut route policy:234
  Split-horizon/Poison-reverse:on/off  Input/Output:on/on
  Default route:off
  Current packets number/Maximum packets number:234/2000
```


Table 9 Command output

Field	Description
Interface-name	The name of an interface running RIP.
Address/Mask	IP address and mask of the interface.
Version	RIP version running on the interface.
MetricIn	Additional routing metric added to the incoming routes.
MetricIn route policy	Name of the routing policy used to add the additional routing metric for the incoming routes. If no routing policy is referenced, the field displays Not designated .
MetricOut	Additional routing metric added to the outgoing routes.
MetricOut route policy	Name of the routing policy used to add the additional routing metric for the outgoing routes. If no routing policy is referenced, the field displays Not designated .
Split-horizon	Indicates whether split-horizon is enabled: <ul style="list-style-type: none"> • on—Enabled. • off—Disabled.
Poison-reverse	Indicates whether poison-reverse is enabled: <ul style="list-style-type: none"> • on—Enabled. • off—Disabled.
Input/Output	Indicates if the interface is allowed to receive (Input) or send (Output) RIP messages: <ul style="list-style-type: none"> • on—Means it is allowed. • off—Means it is not allowed.
Default route	Indicates whether sending the default route to RIP neighbors is allowed: <ul style="list-style-type: none"> • on—Means it is allowed. • off—Means it is not allowed.
Current packets number/Maximum packets number	Packets to be sent/Maximum packets that can be sent on the interface.

display rip route

Syntax

```
display rip process-id route [ ip-address { mask | mask-length } | peer ip-address | statistics ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: RIP process ID, in the range of 1 to 65535.

ip-address { *mask* | *mask-length* }: Displays route information about a specified IP address.

peer *ip-address*: Displays all routing information learned from a specified neighbor.

statistics: Displays the route statistics, including total number of routes and number of routes of each neighbor.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display rip route** to display the routing information of a specified RIP process.

Examples

Display all routing information of RIP process 1.

```
<Sysname> display rip 1 route
Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
-----
Peer 111.1.1.2 on Vlan-interface11
  Destination/Mask    Nexthop    Cost    Tag    Flags    Sec
  122.0.0.0/8        111.1.1.2    1       0     RA       22
```

Table 10 Command output

Field	Description
Route Flags	<ul style="list-style-type: none">• R—RIP route.• T—TRIP route.• P—The route never expires.• A—The route is aging.• S—The route is suppressed.• G—The route is in Garbage-collect state.
Peer 21.0.0.23 on Vlan-interface11	Routing information learned on a RIP interface from the specified neighbor.
Destination/Mask	Destination IP address and subnet mask.
Nexthop	Next hop of the route.
Cost	Cost of the route.
Tag	Route tag.
Flags	Indicates the route state.
Sec	Remaining time of the timer corresponding to the route state.

Display the routing statistics of RIP process 1.

```
<Sysname> display rip 1 route statistics
Peer           Aging      Permanent  Garbage
111.1.1.2      1          0          0
Total          1          0          0
```

Table 11 Command output

Field	Description
Peer	IP address of a neighbor
Aging	Total number of aging routes learned from the specified neighbor
Permanent	Total number of permanent routes learned from the specified neighbor
Garbage	Total number of routes in Garbage-collection state learned from the specified neighbor
Total	Total number of routes learned from all RIP neighbors

dscp (RIP view)

Syntax

dscp *dscp-value*

undo dscp

View

RIP view

Default level

2: System level

Parameters

dscp-value: Sets the Differentiated Services Code Point (DSCP) value for RIP packets, in the range of 0 to 63.

Description

Use **dscp** to set the DSCP value for RIP packets.

Use **undo dscp** to restore the default.

By default, the DSCP value in RIP packets is 48.

Examples

Set the DSCP value for RIP packets of RIP process 1 to 63.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] dscp 63
```

fast-reroute

Syntax

fast-reroute route-policy *route-policy-name*

undo fast-reroute

View

RIP view

Default level

2: System level

Parameters

route-policy *route-policy-name*: References a routing policy to designate a backup next hop. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

Description

Use **fast-reroute** to configure RIP fast reroute (FRR).

Use **undo fast-reroute** to restore the default.

By default, RIP FRR is disabled.



IMPORTANT:

- RIP FRR is only effective for non-recursive RIP routes that are learned from directly connected neighbors.
 - Do not use RIP FRR and BFD for RIP at the same time; otherwise, RIP FRR may fail to take effect.
 - RIP FRR is available only when the state of primary link (with Layer 3 interfaces staying up) changes from bidirectional to unidirectional or down. A unidirectional link refers to the link through which packets are forwarded only from one end to the other.
-

Examples

```
# Enable RIP FRR and reference routing policy frr to specify a backup next hop.
<Sysname> system-view
[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] ip ip-prefix abc index 10 permit 100.1.1.0 24
[Sysname] route-policy frr permit node 10
[Sysname-route-policy] if-match ip-prefix abc
[Sysname-route-policy] apply fast-reroute backup-interface vlan-interface 1
backup-nexthop 193.1.1.8
[Sysname-route-policy] quit
[Sysname] rip 100
[Sysname-rip-100] fast-reroute route-policy frr
```

filter-policy export (RIP view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*] | *interface-type* *interface-number*]

undo filter-policy export [*protocol* [*process-id*] | *interface-type* *interface-number*]

View

RIP view

Default level

2: System level

Parameters

acl-number: Number of an ACL used to filter outbound routes, in the range of 2000 to 3999.

ip-prefix *ip-prefix-name*: Name of an IP prefix list used to filter outbound routes, a string of 1 to 19 characters.

protocol: Filters outbound routes redistributed from a specified routing protocol, which can be **bgp**, **direct**, **isis**, **ospf**, **rip**, and **static**.

process-id: Process ID of the specified routing protocol, in the range of 1 to 65535. You need to specify a process ID when the routing protocol is **rip**, **ospf**, or **isis**.

interface-type interface-number: Specifies an interface by its type and number.

Description

Use **filter-policy export** to configure the filtering of RIP outgoing routes. Only routes not filtered out can be advertised.

Use **undo filter-policy export** to remove the filtering.

By default, RIP does not filter outbound routes.

If a *protocol* is specified, RIP filters only the routes redistributed from the specified routing protocol. Otherwise, RIP filters all routes to be advertised.

If *interface-type interface-number* is specified, RIP filters only the routes advertised by the specified interface. Otherwise, RIP filters routes advertised by all RIP interfaces.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command, the ACL should be configured with the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command to deny/permit a route with the specified destination, or with the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard destination dest-addr dest-wildcard* command to deny/permit a route with the specified destination and mask. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route (the subnet mask must be valid; otherwise, the configuration is ineffective).

Related commands: **import-route** and **ip ip-prefix; acl** (*ACL and QoS Command Reference*).

Examples

Reference ACL 2000 to filter outbound routes.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 export
```

Reference IP prefix list **abc** to filter outbound routes on Vlan-interface11.

```
[Sysname-rip-1] filter-policy ip-prefix abc export Vlan-interface 11
```

Configure ACL 3000 to permit only route 113.0.0.0/16 to pass, and reference ACL 3000 to filter outbound routes.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0
[Sysname-acl-adv-3000] rule 100 deny ip
[Sysname-acl-adv-3000] quit
```

```
[Sysname] rip 1
[Sysname-rip 1] filter-policy 3000 export
```

filter-policy import (RIP view)

Syntax

```
filter-policy { acl-number | gateway ip-prefix-name | ip-prefix ip-prefix-name [ gateway ip-prefix-name ] }
import [ interface-type interface-number ]

undo filter-policy import [ interface-type interface-number ]
```

View

RIP view

Default level

2: System level

Parameters

acl-number: Number of the ACL used for filtering incoming routes, in the range of 2000 to 3999.

ip-prefix *ip-prefix-name*: References an IP prefix list to filter incoming routes. The *ip-prefix-name* is a string of 1 to 19 characters.

gateway *ip-prefix-name*: References an IP prefix list to filter routes from the gateway. *ip-prefix-name* is a string of 1 to 19 characters.

interface-type interface-number: Specifies an interface by its type and number.

Description

Use **filter-policy import** to configure RIP to filter the incoming routes.

Use **undo filter-policy import** to restore the default.

By default, RIP does not filter incoming routes.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command, the ACL should be configured with the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command to deny/permit a route with the specified destination, or with the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard destination dest-addr dest-wildcard* command to deny/permit a route with the specified destination and mask. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route (the subnet mask must be valid; otherwise, the configuration is ineffective).

Related commands: **ip ip-prefix**; **acl** (*ACL and QoS Command Reference*).

Examples

```
# Reference ACL 2000 to filter incoming routes.
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 import

# Reference IP prefix list abc on Vlan-interface 11 to filter all received RIP routes.
[Sysname-rip-1] filter-policy ip-prefix abc import Vlan-interface 11
```

Configure ACL 3000 to permit only route 113.0.0.0/16 to pass, and reference ACL 3000 to filter incoming routes.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0
[Sysname-acl-adv-3000] rule 100 deny ip
[Sysname-acl-adv-3000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 3000 import
```

host-route

Syntax

host-route

undo host-route

View

RIP view

Default level

2: System level

Parameters

None

Description

Use **host-route** to enable host route reception.

Use **undo host-route** to disable host route reception.

By default, receiving host routes is enabled.

In some cases, a router may receive many host routes from the same network segment. These routes are not helpful for routing and occupy a large amount of network resources. Use **undo host-route** to disable receiving of host routes.

RIPv2 can be disabled from receiving host routes, but RIPv1 cannot.

Examples

```
# Disable RIP from receiving host routes.
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] undo host-route
```

import-route (RIP view)

Syntax

import-route *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**cost** *cost* | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route *protocol* [*process-id* | **all-processes**]

View

RIP view

Default level

2: System level

Parameters

protocol: Specifies a routing protocol from which to redistribute routes. It can be **bgp**, **direct**, **isis**, **ospf**, **rip**, or **static**.

process-id: Process ID, in the range of 1 to 65535. The default is 1. It is available only when the protocol is **isis**, **rip**, or **ospf**.

all-processes: Enables route redistribution from all the processes of a protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

allow-ibgp: When the *protocol* argument is set to **bgp**, **allow-ibgp** is an optional keyword.

cost: Cost for redistributed routes, in the range of 0 to 16. If *cost* is not specified, the default cost specified by the **default cost** command applies.

tag: Tag marking redistributed routes, in the range of 0 to 65,535. The default is 0.

route-policy *route-policy-name*: Specifies a routing policy with 1 to 63 case-sensitive characters.

Description

Use **import-route** to enable route redistribution from another routing protocol.

Use **undo import-route** to disable route redistribution.

By default, RIP does not redistribute routes from other routing protocols.

The **import-route bgp** command only redistributes eBGP routes. The **import-route bgp allow-ibgp** command additionally redistributes IBGP routes, which may cause routing loops.

Only active routes can be redistributed. Use the **display ip routing-table protocol** command to display route state information.

The **undo import-route protocol all-processes** command cancels the configuration made by the **import-route protocol all-processes** command, rather than the **import-route protocol process-id** command.

Related commands: **default cost**.

Examples

```
# Redistribute static routes, and set the cost to 4.
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] import-route static cost 4

# Configure the default cost for redistributed routes as 3.
[Sysname-rip-1] default cost 3

# Redistribute OSPF routes with the cost being the default cost.
[Sysname-rip-1] import-route ospf
```


maximum load-balancing (RIP view)

Syntax

```
maximum load-balancing number  
undo maximum load-balancing
```

View

RIP view

Default level

2: System level

Parameters

number: Maximum number of ECMP routes , in the range of 1 to 8.

Description

Use **maximum load-balancing** to specify the maximum number of ECMP routes.

Use **undo maximum load-balancing** to restore the default.

By default, the maximum number of ECMP routes is 8.

Examples

```
# Specify the maximum number of ECMP routes as 2.  
<Sysname> system-view  
[Sysname] rip  
[Sysname-rip-1] maximum load-balancing 2
```

network

Syntax

```
network network-address  
undo network network-address
```

View

RIP view

Default level

2: System level

Parameters

network-address: IP address of a network segment, which can be the IP network address of any interface.

Description

Use **network** to enable RIP on the interface attached to the specified network.

Use **undo network** to disable RIP on the interface attached to the specified network.

RIP is disabled on an interface by default.

RIP runs only on the interfaces attached to the specified network. For an interface not on the specified network, RIP neither receives/sends routes on it nor forwards interface route through it. You need to specify the network after enabling RIP to validate RIP on a specific interface.

For a single process, the **network** 0.0.0.0 command can enable RIP on all interfaces, but the command is not applicable in case of multi-process.

If a physical interface is attached to multiple networks, you cannot advertise these networks in different RIP processes.

Examples

```
# Enable RIP on the interface attached to the network 129.102.0.0.
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] network 129.102.0.0
```

output-delay

Syntax

```
output-delay time count count
undo output-delay
```

View

RIP view

Default level

2: System level

Parameters

time: RIP packet sending interval, in milliseconds. It is in the range of 10 to 100.

count: Maximum number of RIP packets sent at each interval. It is in the range of 1 to 20.

Description

Use **output-delay** to configure the maximum RIP packets that can be sent at the specified interval for all interfaces under the RIP process.

Use **undo output-delay** to restore the default.

By default, an interface sends up to three RIP packets every 20 milliseconds.

Examples

```
# Configure all the interfaces under RIP process 1 to send up to 10 RIP packets every 30 milliseconds.
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] output-delay 30 count 10
```

peer

Syntax

```
peer ip-address
undo peer ip-address
```

View

RIP view

Default level

2: System level

Parameters

ip-address: IP address of a RIP neighbor, in dotted decimal format.

Description

Use **peer** to specify the IP address of a neighbor in the non-broadcast multi-access (NBMA) network, where routing updates destined for the peer are unicast, rather than multicast or broadcast.

Use **undo peer** to remove the IP address of a neighbor.

By default, no neighbor is specified.

You need not use the **peer ip-address** command when the neighbor is directly connected; otherwise the neighbor may receive both the unicast and multicast (or broadcast) of the same routing information.

Examples

```
# Specify to send unicast updates to peer 202.38.165.1
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] peer 202.38.165.1
```

preference

Syntax

```
preference [ route-policy route-policy-name ] value
undo preference [ route-policy ]
```

View

RIP view

Default level

2: System level

Parameters

route-policy-name: Routing policy name with 1 to 63 case-sensitive characters.

value: Preference for RIP routes, in the range of 1 to 255. The smaller the value, the higher the preference.

Description

Use **preference** to specify the preference for RIP routes.

Use **undo preference** to restore the default.

By default, the preference of RIP routes is 100.

You can specify a routing policy by using the keyword **route-policy** to set a preference for the matching RIP routes.

- The preference set by the routing policy applies to all matching RIP routes. The preference of other routes is set by the **preference** command.
- If no preference is set by the routing policy, the preference of all RIP routes is set by the **preference** command.

Examples

```
# Set the RIP route preference to 120.
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] preference 120
```

reset rip process

Syntax

```
reset rip process-id process
```

View

User view

Default level

1: Monitor level

Parameters

process-id: RIP process ID, in the range of 1 to 65535.

Description

Use **reset rip process** to reset the specified RIP process.

After executing the command, you are prompted whether you want to reset the RIP process.

Examples

```
# Reset RIP process 100.
<Sysname> reset rip 100 process
Warning : Reset RIP process? [Y/N]:Y
```

reset rip statistics

Syntax

```
reset rip process-id statistics
```

View

User view

Default level

2: System level

Parameters

process-id: RIP process ID, in the range of 1 to 65535.

Description

Use **reset rip statistics** to clear the statistics of the specified RIP process. This command can clear the statistics of debugging.

Examples

```
# Clear statistics in RIP process 100.
<Sysname> reset rip 100 statistics
```

rip

Syntax

```
rip [ process-id ] [ vpn-instance vpn-instance-name ]  
undo rip [ process-id ] [ vpn-instance vpn-instance-name ]
```

View

System view

Default level

2: System level

Parameters

process-id: RIP process ID, in the range of 1 to 65535. The default is 1.

vpn-instance vpn-instance-name: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the RIP process will run under the public network.

Description

Use **rip** to create a RIP process and enter RIP view.

Use **undo rip** to disable a RIP process.

By default, no RIP process runs.

You must create a VPN instance before you apply a RIP process to it. For related configuration, see the **ip vpn-instance** command in the *MCE Command Reference*.

You must enable the RIP process before configuring the global parameters. This limitation is not for configuration of interface parameters.

The configured interface parameters become invalid after you disable the RIP process.

Examples

```
# Create a RIP process and enter RIP process view.  
<Sysname> system-view  
[Sysname] rip  
[Sysname-rip-1]
```

rip authentication-mode

Syntax

```
rip authentication-mode { md5 { rfc2082 [ cipher ] key-string key-id | rfc2453 [ cipher ] key-string } |  
simple [ cipher ] password }  
undo rip authentication-mode
```

View

Interface view

Default level

2: System level

Parameters

md5: Specifies the MD5 authentication mode.

rfc2082: Uses the message format defined in RFC 2082.

cipher: Sets a ciphertext authentication key or password. If this keyword is not specified, you set a plaintext authentication key or password.

key-string: Specifies the MD5 key string. This argument is case sensitive. It must be a plaintext string of 1 to 16 characters, or a ciphertext string of 33 to 53 characters.

key-id: Specifies the MD5 key number, in the range of 1 to 255.

rfc2453: Uses the message format defined in RFC 2453 (IETF standard).

simple: Specifies the simple authentication mode.

password: Sets the password in simple authentication mode. This argument is case sensitive. It must be a plaintext string of 1 to 16 characters, or a ciphertext string of 33 to 53 characters.

Description

Use **rip authentication-mode** to configure RIPv2 authentication mode and parameters.

Use **undo rip authentication-mode** to cancel authentication.

The key string you configured can overwrite the old one, if any.

The authentication key or password, set in either plain text or cipher text, is saved to the configuration file in cipher text.

This feature does not apply to RIPv1 because RIPv1 does not support authentication. Although you can specify an authentication mode for RIPv1 in interface view, the configuration does not take effect.

Related commands: **rip version**.

Examples

Configure MD5 authentication on VLAN-interface 10 with the plaintext key string being **rose** in the format defined in RFC 2453.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip version 2
[Sysname-Vlan-interface10] rip authentication-mode md5 rfc2453 rose
```

rip bfd enable

Syntax

rip bfd enable

undo rip bfd enable

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **rip bfd enable** to enable BFD on the RIP interface.

Use **undo rip bfd enable** to restore the default and delete the relevant BFD session.

By default, a RIP interface is not enabled with BFD.

BFD echo-mode detection only works for a RIP neighbor one hop away.

Using the **undo peer** command does not delete the neighbor relationship at once and cannot bring down the BFD session at once.

Examples

```
# Enable BFD on RIP interface VLAN-interface 11.
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] rip bfd enable
```

rip default-route

Syntax

```
rip default-route { { only | originate } [ cost cost ] | no-originate }
undo rip default-route
```

View

Interface view

Default level

2: System level

Parameters

only: Advertises only a default route.

originate: Advertises a default route and other routes.

cost: Cost of the default route, in the range of 1 to 15. The default is 1.

no-originate: Advertises routes other than a default route.

Description

Use **rip default-route** to configure the RIP interface to advertise a default route with the specified metric.

Use **undo rip default-route** to disable the RIP interface from sending a default route.

By default, a RIP interface can advertise a default route if the RIP process is configured with default route advertisement.

A RIP router configured to advertise a default route will not receive any default routes from RIP neighbors.

Related commands: **default-route**.

Examples

```
# Configure VLAN-interface 10 to advertise only a default route with a metric of 2.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip default-route only cost 2
```

rip input

Syntax

```
rip input
undo rip input
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **rip input** to enable the interface to receive RIP messages.

Use **undo rip input** to disable the interface from receiving RIP messages.

By default, an interface is enabled to receive RIP messages.

Examples

```
# Disable VLAN-interface 10 from receiving RIP messages.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] undo rip input
```

rip metricin

Syntax

```
rip metricin [ route-policy route-policy-name ] value
undo rip metricin
```

View

Interface view

Default level

2: System level

Parameters

route-policy route-policy-name: Specifies the name of a routing policy used to add an additional metric for the routes matching it. The name is a string of 1 to 63 case-sensitive characters.

value: Additional metric added to received routes, in the range of 0 to 16.

Description

Use **rip metricin** to configure the interface to add a metric to the routes it receives.

Use **undo rip metricin** to restore the default.

By default, the additional metric of a received route is 0.

When a valid RIP route is received, the system adds a metric to it and then installs it into the routing table. The metric of the route received on the configured interface is then increased. If the sum of the additional metric and the original metric is greater than 16, the metric of the route will be 16.

If a routing policy is referenced with the **route-policy** keyword, the following operations can be performed:

- Routes matching the policy is added with the metric specified in the **apply cost** command configured in the policy. Routes not matching it is added with the metric specified in the **rip metricout** command. The **rip metricout** command does not support the + or – keyword—used to add or reduce a metric—specified in the **apply cost** command. For more information about the **apply cost** command, see "[Routing policy configuration commands.](#)"
- If the **apply cost** command is not configured in the policy, all the advertised routes is added with the metric specified in the **rip metricout** command.

Examples

```
# Configure VLAN-interface 10 to add a metric of 6 for incoming route 1.0.0.0/8 and to add a metric of 2 for other incoming routes.
```

```
<Sysname> system-view
[Sysname] ip ip-prefix 123 permit 1.0.0.0 8
[Sysname] route-policy abc permit node 0
[Sysname-route-policy] if-match ip-prefix 123
[Sysname-route-policy] apply cost 6
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip metricin route-policy abc 2
```

rip metricout

Syntax

```
rip metricout [ route-policy route-policy-name ] value
undo rip metricout
```

View

Interface view

Parameters

route-policy *route-policy-name*: Specifies the name of a routing policy used to add an additional metric for the routes matching it. The name is a string of 1 to 63 case-sensitive characters.

value: Additional metric of sent routes, in the range of 1 to 16.

Description

Use **rip metricout** to add a metric to sent routes.

Use **undo rip metricout** to restore the default.

By default, the additional metric for sent routes is 1.

With the command configured on an interface, the metric of RIP routes sent on the interface will be increased.

If a routing policy is referenced with the **route-policy** keyword, the following operations can be performed:

- Routes matching the policy is added with the metric specified in the **apply cost** command configured in the policy. Routes not matching it is added with the metric specified in the **rip metricout** command. The **rip metricout** command does not support the + or – keyword—used to add or reduce a metric—specified in the **apply cost** command. For more information about the **apply cost** command, see "[Routing policy configuration commands.](#)"
- If the **apply cost** command is not configured in the policy, all the advertised routes is added with the metric specified in the **rip metricout** command.

Examples

Configure VLAN-interface 10 to add a metric of 6 for the outgoing route 1.0.0.0/8 and to add a metric of 2 for other outgoing routes.

```
<Sysname> system-view
[Sysname] ip ip-prefix 123 permit 1.0.0.0 8
[Sysname] route-policy abc permit node 0
[Sysname-route-policy] if-match ip-prefix 123
[Sysname-route-policy] apply cost 6
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip metricout route-policy abc 2
```

rip mib-binding

Syntax

```
rip mib-binding process-id
undo rip mib-binding
```

View

System view

Default level

2: System level

Parameters

process-id: RIP process ID, in the range of 1 to 65535.

Description

Use **rip mib-binding** to bind MIB operations with a specified RIP process, so that the RIP process can receive SNMP requests.

Use **undo rip mib-binding** to restore the default.

By default, MIB operations are bound to RIP process 1. RIP process 1 is enabled to receive SNMP requests.

Examples

Enable RIP process 100 to receive SNMP requests.

```
<Sysname> system-view
[Sysname] rip mib-binding 100
```

Restore the default.

```
[Sysname] undo rip mib-binding
```

rip output

Syntax

```
rip output
undo rip output
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **rip output** to enable the interface to send RIP messages.

Use **undo rip output** to disable the interface from sending RIP messages.

Sending RIP messages is enabled on an interface by default.

Examples

```
# Disable VLAN-interface 10 from receiving RIP messages.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] undo rip output
```

rip poison-reverse

Syntax

```
rip poison-reverse
undo rip poison-reverse
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **rip poison-reverse** to enable the poison reverse function.

Use **undo rip poison-reverse** to disable the poison reverse function.

By default, the poison reverse function is disabled.

Examples

```
# Enable the poison reverse function for RIP routing updates on VLAN-interface 10.
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip poison-reverse
```

rip split-horizon

Syntax

```
rip split-horizon
undo rip split-horizon
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **rip split-horizon** to enable the split horizon function.

Use **undo rip split-horizon** to disable the split horizon function.

The split horizon function is enabled by default.

The split horizon function is necessary for preventing routing loops. To disable it in special cases, make sure it is necessary.

Only the poison reverse function takes effect if both the split horizon and poison reverse functions are enabled.

Examples

```
# Enable the split horizon function on VLAN-interface 10.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip split-horizon
```

rip summary-address

Syntax

```
rip summary-address ip-address { mask | mask-length }
undo rip summary-address ip-address { mask | mask-length }
```

View

Interface view

Default level

2: System level

Parameters

ip-address: Destination IP address of summary route.

mask: Subnet mask of summary route, in dotted decimal format.

mask-length: Subnet mask length of summary route, in the range of 0 to 32.

Description

Use **rip summary-address** to configure RIPv2 to advertise a summary route through the interface.

Use **undo rip summary-address** to remove the configuration.

The summary address is valid only when the automatic summarization is disabled.

Related commands: **summary**.

Examples

```
# Advertise a local summary address on VLAN-interface 10.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip summary-address 10.0.0.0 255.255.255.0
```

rip version

Syntax

```
rip version { 1 | 2 [ broadcast | multicast ] }
undo rip version
```

View

Interface view

Default level

2: System level

Parameters

1: RIP version 1.

2: RIP version 2.

broadcast: Sends RIPv2 messages in broadcast mode.

multicast: Sends RIPv2 messages in multicast mode.

Description

Use **rip version** to specify a RIP version for the interface.

Use **undo rip version** to remove the specified RIP version.

By default, no RIP version is configured for an interface, which uses the global RIP version. If the global RIP version is not configured, the interface can only send RIPv1 broadcasts and can receive RIPv1 broadcasts and unicasts, and RIPv2 broadcasts, multicasts, and unicasts.

If RIPv2 is specified with no sending mode configured, RIPv2 messages will be sent in multicast mode.

When RIPv1 runs on an interface, the interface can perform the following operations:

- Sends RIPv1 broadcast messages
- Receives RIPv1 broadcast and unicast messages

When RIPv2 runs on the interface in broadcast mode, the interface can perform the following operations:

- Sends RIPv2 broadcast messages

- Receives RIPv1 broadcast and unicast messages, and RIPv2 broadcast, multicast, and unicast messages

When RIPv2 runs on the interface in multicast mode, the interface can perform the following operations:

- Sends RIPv2 multicast messages
- Receives RIPv2 broadcast, multicast, and unicast messages

Examples

```
# Configure VLAN-interface 10 to broadcast RIPv2 messages.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip version 2 broadcast
```

silent-interface (RIP view)

Syntax

```
silent-interface { interface-type interface-number | all }
undo silent-interface { interface-type interface-number | all }
```

View

RIP view

Default level

2: System level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

all: Disables all interfaces from sending routing updates.

Description

Use **silent-interface** to disable an interface or all interfaces from sending routing updates. The interface only receives but does not send RIP messages.

Use **undo silent-interface** to restore the default.

By default, all interfaces are allowed to send routing updates.

Examples

```
# Configure all VLAN interfaces to work in silent state, and activate VLAN-interface 10.
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] silent-interface all
[Sysname-rip-100] undo silent-interface vlan-interface 10
[Sysname-rip-100] network 131.108.0.0
```

summary

Syntax

summary

undo summary

View

RIP view

Default level

2: System level

Parameters

None

Description

Use **summary** to enable automatic RIPv2 summarization. Natural masks are used to advertise summary routes so as to reduce the size of routing tables.

Use **undo summary** to disable automatic RIPv2 summarization so that all subnet routes can be broadcast.

By default, automatic RIPv2 summarization is enabled.

Enabling automatic RIPv2 summarization can reduce the size of the routing table to enhance the scalability and efficiency of large networks.

Related commands: **rip version**.

Examples

```
# Disable RIPv2 automatic summarization.
```

```
<Sysname> system-view
```

```
[Sysname] rip
```

```
[Sysname-rip-1] undo summary
```

timers

Syntax

```
timers { garbage-collect garbage-collect-value | suppress suppress-value | timeout timeout-value | update update-value }*
```

```
undo timers { garbage-collect | suppress | timeout | update } *
```

View

RIP view

Default level

2: System level

Parameters

garbage-collect-value: Garbage-collect timer time in seconds, in the range of 1 to 3600.

suppress-value: Suppress timer time in seconds, in the range of 0 to 3600.

timeout-value: Timeout timer time in seconds, in the range of 1 to 3600.

update-value: Update timer time in seconds, in the range of 1 to 3600.

Description

Use **timers** to configure RIP timers. By adjusting RIP timers, you can improve network performance.

Use **undo timers** to restore the default.

By default, the garbage-collect timer is 120 seconds, the suppress timer is 120 seconds, the timeout timer is 180 seconds, and the update timer is 30 seconds.

RIP is controlled by the following timers:

- **Update timer**—Defines the interval between routing updates.
- **Timeout timer**—Defines the route aging time. If no routing update related to a route is received after the aging time, the metric of the route is set to 16 in the routing table.
- **Suppress timer**—Defines how long a RIP route stays in suppressed state. When the metric of a route is 16, the route enters the suppressed state. In suppressed state, only routes which come from the same neighbor and whose metric is less than 16 will be received by the router to replace unreachable routes.
- **Garbage-collect timer**—Defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the Garbage-Collect timer length, RIP advertises the route with the routing metric set to 16. If no routing update is announced for that route after the Garbage-Collect timer expires, the route will be deleted from the routing table.

! **IMPORTANT:**

- HP does not recommend changing the default values of these timers.
 - The time lengths of these timers must be kept consistent on all routers in the network.
-

Examples

Specifies the update, timeout, suppress, and garbage-collect timers as 5, 15, 15 and 30.

```
<Sysname> system-view
```

```
[Sysname] rip 100
```

```
[Sysname-rip-100] timers update 5 timeout 15 suppress 15 garbage-collect 30
```

validate-source-address

Syntax

validate-source-address

undo validate-source-address

View

RIP view

Default level

2: System level

Parameters

None

Description

Use **validate-source-address** to enable the source IP address validation on incoming RIP routing updates.

Use **undo validate-source-address** to disable the source IP address validation.

The source IP address validation is enabled by default.

Typically HP does not recommend disabling the validation.

Examples

```
# Disable the source IP address validation on incoming RIP routing updates.
<Sysname> system-view
[Sysname-rip] rip 100
[Sysname-rip-100] undo validate-source-address
```

version

Syntax

```
version { 1 | 2 }
undo version
```

View

RIP view

Default level

2: System level

Parameters

- 1: Specifies the RIP version as RIPv1.
- 2: Specifies the RIP version as RIPv2. RIPv2 messages are multicast.

Description

Use **version** to specify a global RIP version.

Use **undo version** to remove the configured global RIP version.

By default, if an interface has a RIP version specified, the RIP version takes effect; if it has no RIP version specified, it can send RIPv1 broadcasts, and receive RIPv1 broadcasts and unicasts, and RIPv2 broadcasts, multicasts, and unicasts.

If an interface has an RIP version specified, the RIP version takes precedence over the global RIP version.

If no RIP version is specified for the interface and the global version is RIPv1, the interface inherits RIPv1, and it can send RIPv1 broadcasts, and receive RIPv1 broadcasts and unicasts.

If no RIP version is specified for the interface and the global version is RIPv2, the interface operates in the RIPv2 multicast mode, and it can send RIPv2 multicasts, and receive RIPv2 broadcasts, multicasts, and unicasts.

Examples

```
# Specify RIPv2 as the global RIP version.
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] version 2
```

OSPF configuration commands

For OSPF TE related commands and OSPF VPN related commands, see *MPLS Command Reference*.

The term "router" in this chapter refers to both routers and Layer 3 switches.

The A5500 SI Switch Series does not support OSPF.

abr-summary (OSPF area view)

Syntax

```
abr-summary ip-address { mask | mask-length } [ advertise | not-advertise ] [ cost cost ]  
undo abr-summary ip-address { mask | mask-length }
```

View

OSPF area view

Default level

2: System level

Parameters

ip-address: Destination IP address of the summary route, in dotted decimal format.

mask: Mask of the IP address in dotted decimal format.

mask-length: Mask length, in the range of 0 to 32 bits.

advertise | **not-advertise**: Advertises the summary route or not. If none of the **advertise** and **not-advertise** keywords is set, the summary route is advertised.

cost *cost*: Specifies the cost of the summary route, in the range of 1 to 16777215. The default cost is the largest cost value among routes that are summarized.

Description

Use **abr-summary** to configure a summary route on an area border router (ABR).

Use **undo abr-summary** to remove a summary route.

By default, no route summarization is configured on an ABR.

You can enable advertising the summary route or not, and specify a route cost.

This command is available only on an ABR to summarize multiple contiguous networks into one network.

With the **undo abr-summary** command used, summarized routes will be advertised.

Examples

```
# Summarize networks 36.42.10.0/24 and 36.42.110.0/24 in Area 1 into 36.42.0.0/16.
```

```
<Sysname> system-view
```

```
[Sysname] ospf 100
```

```
[Sysname-ospf-100] area 1
```

```
[Sysname-ospf-100-area-0.0.0.1] network 36.42.10.0 0.0.0.255
```

```
[Sysname-ospf-100-area-0.0.0.1] network 36.42.110.0 0.0.0.255
```

```
[Sysname-ospf-100-area-0.0.0.1] abr-summary 36.42.0.0 255.255.0.0
```

area (OSPF view)

Syntax

```
area area-id
```

```
undo area area-id
```

View

OSPF view

Default level

2: System level

Parameters

area-id: ID of an area, which is an IP address, or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format by the system.

Description

Use **area** to create an area and enter area view.

Use **undo area** to remove an area.

No OSPF area is created by default.

Examples

```
# Create area 0 and enter area 0 view
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0]
```

asbr-summary

Syntax

```
asbr-summary ip-address { mask | mask-length } [ cost cost | not-advertise | tag tag ] *
```

```
undo asbr-summary ip-address { mask | mask-length }
```

View

OSPF view

Default level

2: System level

Parameters

ip-address: IP address of the summary route in dotted decimal notation.

mask: Summary route mask, in dotted decimal notation.

mask-length: Length of summary route mask, in the range of 0 to 32 bits.

cost cost: Specifies the cost of the summary route, in the range of 1 to 16777214. For Type-1 external routes, the cost defaults to the largest cost among routes that are summarized. For Type-2 external routes, the cost defaults to the largest cost among routes that are summarized plus 1.

not-advertise: Disables advertising the summary route. If the keyword is not specified, the route is advertised.

tag tag: Specifies a tag value for the summary route, used by a routing policy to control summary route advertisement, in the range of 0 to 4294967295. The default is 1.

Description

Use **asbr-summary** to configure a summary route.

Use **undo asbr-summary** to remove a summary route.

No ASBR route summarization is configured by default.

With the **asbr-summary** command configured, an ASBR summarizes redistributed routes that fall into the specified address range into a single route. If the ASBR resides in an NSSA area, it advertises the summary route in a Type-7 LSA into the area.

With the **asbr-summary** command configured, an NSSA ABR summarizes routes described by Type-5 LSAs translated from Type-7 LSAs into a single route and advertises the summary route to other areas. This command does not take effect on non NSSA ABRs.

If the **undo asbr-summary** command is used, summarized routes will be advertised.

Related command: **display ospf asbr-summary**.

Examples

Summarize redistributed static routes into a single route, and specify a tag value of 2 and a cost of 100 for the summary route.

```
<Sysname> system-view
[Sysname] ip route-static 10.2.1.0 24 null 0
[Sysname] ip route-static 10.2.2.0 24 null 0
[Sysname] ospf 100
[Sysname-ospf-100] import-route static
[Sysname-ospf-100] asbr-summary 10.2.0.0 255.255.0.0 tag 2 cost 100
```

authentication-mode

Syntax

authentication-mode { md5 | simple }

undo authentication-mode

View

OSPF area view

Default level

2: System level

Parameters

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

Description

Use **authentication-mode** to specify an authentication mode for the OSPF area.

Use **undo authentication-mode** to remove the authentication mode.

By default, no authentication mode is configured for an OSPF area.

Routers that reside in the same area must have the same authentication mode: non-authentication, simple, or MD5.

Related commands: **ospf authentication-mode**.

Examples

```
# Configure OSPF area 0 to use the MD5 authentication mode.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] authentication-mode md5
```

bandwidth-reference (OSPF view)

Syntax

bandwidth-reference *value*

undo bandwidth-reference

View

OSPF view

Default level

2: System level

Parameters

value: Bandwidth reference value for link cost calculation, in the range of 1 to 2147483648 Mbps.

Description

Use **bandwidth-reference** to specify a reference bandwidth value for link cost calculation.

Use **undo bandwidth-reference** to restore the default value.

The default value is 100 Mbps.

When links have no cost values configured, OSPF calculates their cost values using formula: $\text{Cost} = \text{Reference bandwidth value} / \text{Link bandwidth}$. If the calculated cost is greater than 65535, the value of 65535 is used.

Examples

```
# Specify the reference bandwidth value as 1000 Mbps.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] bandwidth-reference 1000
```

default

Syntax

```
default { cost cost | limit limit | tag tag | type type } *  
undo default { cost | limit | tag | type } *
```

View

OSPF view

Default level

2: System level

Parameters

cost: Specifies the default cost for redistributed routes, in the range of 0 to 16777214.

limit: Specifies the default upper limit of routes redistributed per time, in the range of 1 to 2147483647.

tag: Specifies the default tag for redistributed routes, in the range of 0 to 4294967295.

type: Specifies the default type for redistributed routes: 1 or 2.

Description

Use **default** to configure default parameters for redistributed routes.

Use **undo default** to restore default values.

The cost, route type, tag, and the upper limit are 1, 2, 1 and 1000 by default.

Related commands: **import-route**.

Examples

```
# Configure the default cost, upper limit, tag and type as 10, 20000, 100 and 2 for redistributed external routes.
```

```
<Sysname> system-view
```

```
[Sysname] ospf 100
```

```
[Sysname-ospf-100] default cost 10 limit 20000 tag 100 type 2
```

default-cost (OSPF area view)

Syntax

```
default-cost cost  
undo default-cost
```

View

OSPF area view

Default level

2: System level

Parameters

cost: Specifies a cost for the default route advertised to the Stub or NSSA area, in the range of 0 to 16777214.

Description

Use **default-cost** to configure a cost for the default route advertised to the stub or NSSA area.

Use **undo default-cost** to restore the default value.

The cost defaults to 1.

This command is only applicable to the ABR of a stub area or the ABR/ASBR of an NSSA area.

Related commands: **stub** and **nssa**.

Examples

Configure Area 1 as a stub area, and specify the cost of the default route advertised to the stub area as 20.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
[Sysname-ospf-100-area-0.0.0.1] default-cost 20
```

default-route-advertise (OSPF view)

Syntax

default-route-advertise [[[**always** | **permit-calculate-other**] | **cost** *cost* | **route-policy** *route-policy-name* | **type** *type*] * | **summary** *cost* *cost*]

undo default-route-advertise

View

OSPF view

Default level

2: System level

Parameters

always: Generates a default route in a Type-5 LSA into the OSPF routing domain regardless of whether there is a default route in the routing table. If this keyword is not specified, the router generates a default route in a Type-5 LSA into the OSPF routing domain only when an active default route that does not belong to the current OSPF process exists in the IP routing table.

permit-calculate-other: Calculates default routes from other routers with this keyword specified or does not calculate default routes from other routers without this keyword specified when the router generates a default route in a Type-5 LSA into the OSPF routing domain. If the router generates no default route in a Type-5 LSA into the OSPF routing domain, the router calculates default routes from other routers regardless of whether this keyword is specified.

cost *cost*: Specifies a cost for the default route, in the range of 0 to 16777214. If no *cost* is specified, the default cost specified by the **default cost** command applies.

route-policy *route-policy-name*: Specifies a routing policy name, a string of 1 to 63 case-sensitive characters. When a default route exists in the routing table and the specified routing policy is matched, the command distributes a default route in a Type-5 LSA into the OSPF routing domain, and the routing policy modifies some values in the Type-5 LSA. If the **always** keyword is specified at the same time, the command can distribute a default route in a Type-5 LSA into the OSPF routing domain when the specified

routing policy is matched, regardless of whether a default route exists in the routing table, and the routing policy modifies some values in the Type-5 LSA.

type *type*: Specifies a type for the Type-5 LSA: 1 or 2. If *type* is not specified, the default type for the Type-5 LSA specified by the **default type** command applies.

summary: Advertises the Type-3 summary LSA of the specified default route.

Description

Use **default-route-advertise** to generate a default route into the OSPF routing domain.

Use **undo default-route-advertise** to disable OSPF from distributing a default external route.

By default, no default route is distributed.

The **default-route-advertise summary cost** command is applicable only to VPNs, and the default route is redistributed in a Type-3 LSA. The PE router advertises the redistributed default route to the CE router.

Using the **import-route** command cannot redistribute a default route. To redistribute a default route, use the **default-route-advertise** command.

If neither the **always** nor **permit-calculate-other** keyword is specified, the router generates a default route in a Type-5 LSA into the OSPF routing domain only when an active default route that does not belong to the current OSPF process exists in the IP routing table. The router then does not calculate default routes from other routers.

Related commands: **import-route** and **default**.

Examples

Generate a default route in an ASE LSA into the OSPF routing domain, regardless of whether the default route is available in the routing table.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default-route-advertise always
```

description (OSPF/OSPF area view)

Syntax

description *description*

undo description

View

OSPF view/OSPF area view

Default level

2: System level

Parameters

description: Configures a description for the OSPF process in OSPF view, or for the OSPF area in OSPF area view. *description* is a string of up to 80 characters.

Description

Use **description** to configure a description for an OSPF process or area.

Use **undo description** to remove the description.

No description is configured by default.

Use of this command is only for the identification of an OSPF process or area. The description has no special meaning.

Examples

```
# Describe OSPF process 100 as abc.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] description abc

# Describe OSPF area 0 as bone area.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] description bone area
```

display ospf abr-asbr

Syntax

```
display ospf [ process-id ] abr-asbr [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535. Use this argument to display information about the routes to the ABR/ASBR under the specified OSPF process.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf abr-asbr** to display information about the routes to OSPF ABR/ASBR.

If you use this command on routers in a stub area, no ASBR information is displayed.

Examples

```
# Display information about the routes to the OSPF ABR and ASBR.
<Sysname> display ospf abr-asbr
```

```
OSPF Process 1 with Router ID 192.168.1.2
  Routing Table to ABR and ASBR
```

Type	Destination	Area	Cost	NextHop	RtType
Inter	3.3.3.3	0.0.0.0	3124	10.1.1.2	ASBR

Intra 2.2.2.2 0.0.0.0 1562 10.1.1.2 ABR

Table 12 Command output

Field	Description
Type	Type of the route to the ABR or ASBR: <ul style="list-style-type: none">• Intra— intra-area route• Inter—Inter-area route
Destination	Router ID of an ABR/ASBR
Area	ID of the area of the next hop
Cost	Cost from the router to the ABR/ASBR
Nexthop	Next hop address
RtType	Router type: ABR, ASBR

display ospf asbr-summary

Syntax

```
display ospf [ process-id ] asbr-summary [ ip-address { mask | mask-length } ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

ip-address: IP address, in dotted decimal format.

mask: IP address mask, in dotted decimal format.

mask-length: Mask length, in the range of 0 to 32 bits.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf asbr-summary** to display information about the redistributed routes that are summarized.

If no OSPF process is specified, related information of all OSPF processes is displayed.

If no IP address is specified, information about all summarized redistributed routes will be displayed.

Related commands: **asbr-summary**.

Examples

```
# Display information about all summarized redistributed routes.
```

```
<Sysname> display ospf asbr-summary
```

```
OSPF Process 1 with Router ID 2.2.2.2
Summary Addresses
```

```
Total Summary Address Count: 1
```

```
Summary Address
```

```
Net       : 30.1.0.0
Mask      : 255.255.0.0
Tag       : 20
Status    : Advertise
Cost      : 10 (Configured)
The Count of Route is : 2
```

Destination	Net Mask	Proto	Process	Type	Metric
30.1.2.0	255.255.255.0	OSPF	2	2	1
30.1.1.0	255.255.255.0	OSPF	2	2	1

Table 13 Command output

Field	Description
Total Summary Address Count	Total number of summary routes
Net	Address of the summary route
Mask	Mask of the summary route address
Tag	Tag of the summary route
Status	Advertisement status of the summary route
Cost	Cost to the summary net
The Count of Route	Number of routes that are summarized
Destination	Destination address of a summarized route
Net Mask	Network mask of a summarized route
Proto	Routing protocol
Process	Process ID of the routing protocol
Type	Type of a summarized route
Metric	Metric of a summarized route

display ospf brief

Syntax

```
display ospf [ process-id ] brief [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf brief** to display OSPF brief information. If no OSPF process is specified, brief information about all OSPF processes is displayed.

Examples

Display OSPF brief information.

```
<Sysname> display ospf brief
```

```
                OSPF Process 1 with Router ID 192.168.1.2
                OSPF Protocol Information

RouterID: 192.168.1.2      Router Type:  NSSA
Route Tag: 0
Multi-VPN-Instance is not enabled
SPF-schedule-interval: 5 0 5000
LSA generation interval: 5 0 5000
LSA arrival interval: 1000
Transmit pacing: Interval: 20 Count: 3
Default ASE parameters: Metric: 1 Tag: 1 Type: 2
Route Preference: 10
ASE Route Preference: 150
SPF Computation Count: 22
RFC 1583 Compatible
Area Count: 1   Nssa Area Count: 1
7/5 translator state: Disabled
7/5 translate stability timer interval: 0

ExChange/Loading Neighbors: 0

Area: 0.0.0.1           (MPLS TE not enabled)
Authtype: None Area flag: NSSA
```

SPF Scheduled Count: 5
 ExChange/Loading Neighbors: 0

Interface: 192.168.1.2 (Vlan-interface11)
 Cost: 1 State: DR Type: Broadcast MTU: 1500
 Priority: 1
 Designated Router: 192.168.1.2
 Backup Designated Router: 192.168.1.1
 Timers: Hello 10 , Dead 40 , Poll 40 , Retransmit 5 , Transmit Delay 1

Table 14 Command output

Field	Description
OSPF Process 1 with Router ID 192.168.1.2	OSPF process ID and OSPF router ID.
RouterID	Router ID.
Router Type	Router type: <ul style="list-style-type: none"> • ABR • ASBR • NSSA • Null
Route Tag	The tag of redistributed routes.
Multi-VPN-Instance is not enabled	The OSPF process does not support multi-VPN-instance.
SPF-schedule-interval	Interval for SPF calculations.
LSA generation interval	LSA generation interval.
LSA arrival interval	LSA arrival interval.
Transmit pacing	LSU packet transmit rate of the interface: <ul style="list-style-type: none"> • Interval—Indicates the LSU transmit interval of the interface. • Count—Indicates the maximum number of LSU packets sent at each interval.
Default ASE Parameter	Default ASE Parameters: metric, tag, route type.
Route Preference	Internal route priority.
ASE Route Preference	External route priority.
SPF Computation count	SPF computation count of the OSPF process.
RFC1583 Compatible	Compatible with routing rules defined in RFC 1583.
Area Count	Area number of the current process.
Nssa Area Count	NSSA area number of the current process.
7/5 translator state	State of the translator that translates Type-7 LSAs to Type-5 LSAs. The value can be one of the following: <ul style="list-style-type: none"> • Enabled—Indicates the translator is specified through commands. • Elected—Indicates the translator is designated through election. • Disabled—Indicates the device is not a translator that translates Type-7 LSAs to Type-5 LSAs.

Field	Description
7/5 translate stability timer interval	Stability interval for Type-7 LSA-to-Type-5 LSA translation.
ExChange/Loading Neighbors	Neighbors in ExChange/Loading state.
Area	Area ID in the IP address format .
Authtype	Authentication type of the area: <ul style="list-style-type: none"> • None—No authentication. • Simple—Simple authentication. • MD5—MD5 authentication.
Area flag	The type of the area.
SPF scheduled Count	SPF calculation count in the OSPF area.
Interface	Interface in the area.
Cost	Interface cost.
State	Interface state.
Type	Interface network type.
MTU	Interface MTU.
Priority	Router priority.
Designated Router	The Designated Router.
Backup Designated Router	The Backup Designated Router.
Timers	Intervals of timers: hello, dead, poll, retransmit, and transmit delay.

display ospf cumulative

Syntax

```
display ospf [ process-id ] cumulative [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf cumulative** to display OSPF statistics.

Use of this command is helpful for troubleshooting.

Examples

Display OSPF statistics.

```
<Sysname> display ospf cumulative
      OSPF Process 1 with Router ID 2.2.2.2
      Cumulations

IO Statistics
      Type           Input      Output
      Hello          61         122
      DB Description    2          3
      Link-State Req    1          1
Link-State Update    3          3
      Link-State Ack    3          2

LSAs originated by this router
Router: 4
Network: 0
Sum-Net: 0
Sum-Asbr: 0
External: 0
NSSA: 0
Opq-Link: 0
Opq-Area: 0
Opq-As: 0

LSAs Originated: 4  LSAs Received: 7

Routing Table:
      Intra Area: 2  Inter Area: 3  ASE/NSSA: 0
```

Table 15 Command output

Field	Description
IO statistics	Statistics about input/output packets and LSAs
Type	OSPF packet type
Input	Packets received
Output	Packets sent
Hello	Hell packet
DB Description	Database Description packet
Link-State Req	Link-State Request packet
Link-State Update	Link-State Update packet
Link-State Ack	Link-State Acknowledge packet

Field	Description
LSAs originated by this router	LSAs originated by this router
Router	Number of Type-1 LSAs originated
Network	Number of Type-2 LSAs originated
Sum-Net	Number of Type-3 LSAs originated
Sum-Asbr	Number of Type-4 LSAs originated
External	Number of Type-5 LSAs originated
NSSA	Number of Type-7 LSAs originated
Opq-Link	Number of Type-9 LSAs originated
Opq-Area	Number of Type-10 LSAs originated
Opq-As	Number of Type-11 LSAs originated
LSA originated	Number of LSAs originated
LSA Received	Number of LSAs received
Routing Table	Routing table information
Intra Area	Intra-area route number
Inter Area	Inter-area route number
ASE	ASE route number

display ospf error

Syntax

```
display ospf [ process-id ] error [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf error** to display OSPF error information.

If no process is specified, the OSPF error information of all OSPF processes is displayed.

Examples

Display OSPF error information.

```
<Sysname> display ospf error
```

```

                OSPF Process 1 with Router ID 192.168.80.100
                OSPF Packet Error Statistics

0   : OSPF Router ID confusion      0   : OSPF bad packet
0   : OSPF bad version              0   : OSPF bad checksum
0   : OSPF bad area ID              0   : OSPF drop on unnumber interface
0   : OSPF bad virtual link         0   : OSPF bad authentication type
0   : OSPF bad authentication key   0   : OSPF packet too small
0   : OSPF Neighbor state low       0   : OSPF transmit error
0   : OSPF interface down           0   : OSPF unknown neighbor
0   : HELLO: Netmask mismatch       0   : HELLO: Hello timer mismatch
0   : HELLO: Dead timer mismatch    0   : HELLO: Extern option mismatch
0   : HELLO: Neighbor unknown       0   : DD: MTU option mismatch
0   : DD: Unknown LSA type          0   : DD: Extern option mismatch
0   : LS ACK: Bad ack               0   : LS ACK: Unknown LSA type
0   : LS REQ: Empty request         0   : LS REQ: Bad request
0   : LS UPD: LSA checksum bad      0   : LS UPD: Received less recent LSA
0   : LS UPD: Unknown LSA type

```

Table 16 Command output

Field	Description
OSPF Router ID confusion	Packets with duplicate route ID
OSPF bad packet	Packets illegal
OSPF bad version	Packets with wrong version
OSPF bad checksum	Packets with wrong checksum
OSPF bad area ID	Packets with invalid area ID
OSPF drop on unnumber interface	Packets dropped on the unnumbered interface
OSPF bad virtual link	Packets on wrong virtual links
OSPF bad authentication type	Packets with invalid authentication type
OSPF bad authentication key	Packets with invalid authentication key
OSPF packet too small	Packets too small in length
OSPF Neighbor state low	Packets received in low neighbor state
OSPF transmit error	Packets with error when being transmitted
OSPF interface down	Shutdown times of the interface
OSPF unknown neighbor	Packets received from unknown neighbors
HELLO: Netmask mismatch	Hello packets with mismatched mask
HELLO: Hello timer mismatch	Hello packets with mismatched hello timer
HELLO: Dead timer mismatch	Hello packets with mismatched dead timer

Field	Description
HELLO: Extern option mismatch	Hello packets with mismatched option field
HELLO: Neighbor unknown	Hello packets received from unknown neighbors
DD: MTU option mismatch	DD packets with mismatched MTU
DD: Unknown LSA type	DD packets with unknown LSA type
DD: Extern option mismatch	DD packets with mismatched option field
LS ACK: Bad ack	Bad LSACK packets for LSU packets
LS ACK: Unknown LSA type	LSACK packets with unknown LSA type
LS REQ: Empty request	LSR packets with no request information
LS REQ: Bad request	Bad LSR packets
LS UPD: LSA checksum bad	LSU packets with wrong LSA checksum
LS UPD: Received less recent LSA	LSU packets without latest LSA
LS UPD: Unknown LSA type	LSU packets with unknown LSA type

display ospf interface

Syntax

```
display ospf [ process-id ] interface [ interface-type interface-number | all ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number.

all: Displays the OSPF information of all interfaces.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf interface** to display OSPF interface information.

If no OSPF process is specified, the OSPF interface information of all OSPF processes is displayed.

Examples

```
# Display OSPF interface information.
<Sysname> display ospf interface
```

```

                OSPF Process 1 with Router ID 192.168.1.1
                  Interfaces

Area: 0.0.0.0
IP Address      Type      State      Cost  Pri  DR          BDR
192.168.1.1    PTP        P-2-P     1562  1   0.0.0.0    0.0.0.0

Area: 0.0.0.1
IP Address      Type      State      Cost  Pri  DR          BDR
172.16.0.1     Broadcast  DR         1     1   172.16.0.1 0.0.0.0

```

Table 17 Command output

Field	Description
Area	Area ID of the interface.
IP address	Interface IP address (regardless of whether TE is enabled or not).
Type	Interface network type: <ul style="list-style-type: none"> • PTP • PTMP • Broadcast • NBMA
State	Interface state defined by interface state machine: <ul style="list-style-type: none"> • Down—In this state, no protocol traffic will be sent or received on the interface. • Waiting—Means the interface starts sending and receiving Hello packets and the router is trying to determine the identity of the (Backup) designated router for the network. • p-2-p—Means the interface will send Hello packets at the interval of HelloInterval, and try to establish an adjacency with the neighbor. • DR—Means the router itself is the designated router on the attached network. • BDR—Means the router itself is the backup designated router on the attached network. • DROther—Means the router is a DROther router on the attached network.
Cost	Interface cost.
Pri	Router priority.
DR	The DR on the interface's network segment.
BDR	The BDR on the interface's network segment.

display ospf lsdb

Syntax

```
display ospf [ process-id ] lsdb [ brief | [ { asbr | ase | network | nssa | opaque-area | opaque-as | opaque-link | router | summary } [ link-state-id ] ] [ originate-router advertising-router-id | self-originate ] ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

brief: Displays brief LSDB information.

asbr: Displays Type-4 LSA (ASBR Summary LSA) information in the LSDB.

ase: Displays Type-5 LSA (AS External LSA) information in the LSDB.

network: Displays Type-2 LSA (Network LSA) information in the LSDB.

nssa: Displays Type-7 LSA (NSSA External LSA) information in the LSDB.

opaque-area: Displays Type-10 LSA (Opaque-area LSA) information in the LSDB.

opaque-as: Displays Type-11 LSA (Opaque-AS LSA) information in the LSDB.

opaque-link: Displays Type-9 LSA (Opaque-link LSA) information in the LSDB.

router: Displays Type-1 LSA (Router LSA) information in the LSDB.

summary: Displays Type-3 LSA (Network Summary LSA) information in the LSDB.

link-state-id: Link state ID, in the IP address format.

originate-router advertising-router-id: Displays information about LSAs originated by the specified router.

self-originate: Displays information about self-originated LSAs.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf lsdb** to display LSDB information.

If no OSPF process is specified, LSDB information of all OSPF processes is displayed.

Examples

```
# Display OSPF LSDB information.
```

```
<Sysname> display ospf lsdb
```

```
OSPF Process 1 with Router ID 192.168.0.1
```

Link State Database

```

Area: 0.0.0.0
Type      LinkState ID  AdvRouter      Age  Len  Sequence  Metric
Router    192.168.0.2   192.168.0.2   474  36   80000004   0
Router    192.168.0.1   192.168.0.1   21   36   80000009   0
Network   192.168.0.1   192.168.0.1   321  32   80000003   0
Sum-Net   192.168.1.0   192.168.0.1   321  28   80000002   1
Sum-Net   192.168.2.0   192.168.0.2   474  28   80000002   1

Area: 0.0.0.1
Type      LinkState ID  AdvRouter      Age  Len  Sequence  Metric
Router    192.168.0.1   192.168.0.1   21   36   80000005   0
Sum-Net   192.168.2.0   192.168.0.1   321  28   80000002   2
Sum-Net   192.168.0.0   192.168.0.1   321  28   80000002   1

```

Table 18 Command output

Field	Description
Area	LSDB information of the area
Type	LSA type
LinkState ID	Link state ID
AdvRouter	Advertising router
Age	Age of the LSA
Len	Length of the LSA
Sequence	Sequence number of the LSA
Metric	Cost of the LSA

Display Type2 LSA (Network LSA) information in the LSDB.

```
<Sysname> display ospf 1 lsdb network
```

```

OSPF Process 1 with Router ID 192.168.1.1
      Area: 0.0.0.0
      Link State Database

Type      : Network
LS ID     : 192.168.0.2
Adv Rtr   : 192.168.2.1
LS Age    : 922
Len       : 32
Options   : E
Seq#      : 80000003
Checksum  : 0x8d1b
Net Mask  : 255.255.255.0
  Attached Router 192.168.1.1
  Attached Router 192.168.2.1
      Area: 0.0.0.1
      Link State Database

```

```

Type       : Network
LS ID      : 192.168.1.2
Adv Rtr    : 192.168.1.2
LS Age     : 782
Len        : 32
Options    : NP
Seq#       : 80000003
Checksum   : 0x2a77
Net Mask   : 255.255.255.0
  Attached Router 192.168.1.1
  Attached Router 192.168.1.2

```

Table 19 Command output

Field	Description
Type	LSA type
LS ID	DR IP address
Adv Rtr	Router that advertised the LSA
LS Age	LSA age time
Len	LSA length
Options	LSA options: <ul style="list-style-type: none"> • O—Opaque LSA advertisement capability • E—AS External LSA reception capability • EA—External extended LSA reception capability • DC—On-demand link support • N—NSSA external LSA support • P—Capability of an NSSA ABR to translate Type-7 LSAs into Type-5 LSAs
Seq#	LSA sequence number
Checksum	LSA checksum
Net Mask	Network mask
Attached Router	ID of the router that established adjacency with the DR, and ID of the DR itself

display ospf nexthop

Syntax

```
display ospf [ process-id ] nexthop [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf nexthop** to display OSPF next hop information.

If no OSPF process is specified, the next hop information of all OSPF processes is displayed.

Examples

```
# Display OSPF next hop information.
```

```
<Sysname> display ospf nexthop
      OSPF Process 1 with Router ID 192.168.0.1
      Routing Nexthop Information

      Next Hops:
      Address          Refcount  IntfAddr      Intf Name
      -----
      192.168.0.1      1         192.168.0.1  Vlan-interface1
      192.168.0.2      1         192.168.0.1  Vlan-interface1
      192.168.1.1      1         192.168.1.1  Vlan-interface12
```

Table 20 Command output

Field	Description
Next Hops	Information about Next hops
Address	Next hop address
Refcount	Reference count (routes that reference the next hop)
IntfAddr	Outbound interface address
Intf Name	Outbound interface name

display ospf peer

Syntax

```
display ospf [ process-id ] peer [ verbose ] [ interface-type interface-number ] [ neighbor-id ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

verbose: Displays detailed neighbor information.

interface-type interface-number: Specifies an interface by its type and number.

neighbor-id: Neighbor router ID.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf peer** to display information about OSPF neighbors.

If no OSPF process is specified, OSPF neighbor information of all OSPF processes is displayed.

If an interface is specified, the neighbor on the interface is displayed.

If a neighbor ID is specified, detailed information about the neighbor is displayed,

If neither interface nor neighbor ID is specified, brief information about neighbors of the specified OSPF process or all OSPF processes is displayed.

Examples

Display detailed OSPF neighbor information.

```
<Sysname> display ospf peer verbose
```

```
OSPF Process 1 with Router ID 1.1.1.1
Neighbors
```

```
Area 0.0.0.0 interface 1.1.1.1(Vlan-interface11)'s neighbors
Router ID: 1.1.1.2          Address: 1.1.1.2          GR State: Normal
State: Full  Mode: Nbr is Master  Priority: 1
DR: 1.1.1.2  BDR: 1.1.1.1  MTU: 0
Dead timer due in 33 sec
Neighbor is up for 02:03:35
Authentication Sequence: [ 0 ]
Neighbor state change count: 6
```


Table 21 Command output

Field	Description
Area <i>areaID</i> interface <i>IPAddress(InterfaceName)</i> 's neighbors	Neighbor information of the interface in the specified area: <ul style="list-style-type: none"> • areaID—Area to which the neighbor belongs. • IPAddress—Interface IP address. • InterfaceName—Interface name.
interface	Interface attached with the neighbor.
Router ID	Neighbor router ID.
Address	Neighbor router address.
GR State	GR state.
State	Neighbor state: <ul style="list-style-type: none"> • Down—This is the initial state of a neighbor conversation. • Init—In this state, the router has seen a Hello packet from the neighbor. However, the router has not established bidirectional communication with the neighbor (the router itself did not appear in the neighbor's hello packet). • Attempt—Available only in an NBMA network, Under this state, the OSPF router has not received any information from a neighbor for a period but can send Hello packets at a longer interval to keep neighbor relationship. • 2-Way—In this state, communication between the two routers is bidirectional. The router itself appears in the neighbor's Hello packet. • Exstart—The goal of this state is to decide which router is the master, and to decide upon the initial Database Description (DD) sequence number. • Exchange—In this state, the router is sending DD packets to the neighbor, describing its entire link-state database. • Loading—In this state, the router sends Link State Request packets to the neighbor, requesting more recent LSAs. • Full—In this state, the neighboring routers are fully adjacent.
Mode	Neighbor mode for LSDB synchronization.
Priority	Neighboring router priority.
DR	The DR on the interface's network segment.
BDR	The BDR on the interface's network segment.
MTU	Interface MTU.
Dead timer due in 33 sec	Dead timer times out in 33 seconds.
Neighbor is up for 02:03:35	The neighbor has been up for 02:03:35.
Authentication Sequence	Authentication sequence number.
Neighbor state change count	Count of neighbor state changes.

Display brief OSPF neighbor information.

```
<Sysname> display ospf peer
```

```
                OSPF Process 1 with Router ID 1.1.1.1
                Neighbor Brief Information

Area: 0.0.0.0
Router ID      Address          Pri Dead-Time Interface      State
1.1.1.2       1.1.1.2          1  40          Vlan11         Full/DR
```

Table 22 Command output

Field	Description
Area	Neighbor area
Router ID	Neighbor router ID
Address	Neighbor interface address
Pri	Neighboring router priority
Dead-Time	Dead interval remained
Interface	Interface connected to the neighbor
State	Neighbor state: Down, Init, Attempt, 2-Way, Exstart, Exchange, Loading or Full

display ospf peer statistics

Syntax

```
display ospf [ process-id ] peer statistics [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf peer statistics** to display OSPF neighbor statistics.

If no OSPF process is specified, OSPF neighbor statistics of all OSPF processes is displayed.

Examples

Display OSPF neighbor statistics.

```
<Sysname> display ospf peer statistics
      OSPF Process 1 with Router ID 10.3.1.1
          Neighbor Statistics
Area ID      Down Attempt  Init  2-Way ExStart Exchange Loading Full Total
0.0.0.0      0    0         0    0    0    0    0    1    1
0.0.0.2      0    0         0    0    0    0    0    1    1
Total        0    0         0    0    0    0    0    2    2
```

Table 23 Command output

Field	Description
Area ID	Area ID. The state statistics of all the routers in the area to which the router belongs is displayed.
Down	Number of neighboring routers in Down state in the same area.
Attempt	Number of neighboring routers in Attempt state in the same area.
Init	Number of neighboring routers in Init state in the same area.
2-Way	Number of neighboring routers in 2-Way state in the same area.
ExStart	Number of neighboring routers in ExStart state in the same area.
Exchange	Number of neighboring routers in Exchange state in the same area.
Loading	Number of neighboring routers in Loading state in the same area.
Full	Number of neighboring routers in Full state in the same area.
Total	Total number of neighbors under the same state: Down, Attempt, Init, 2-Way, ExStart, Exchange, Loading, or Full.

display ospf request-queue

Syntax

```
display ospf [ process-id ] request-queue [ interface-type interface-number ] [ neighbor-id ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number.

neighbor-id: Neighbor's router ID.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf request-queue** to display OSPF request queue information.

If no OSPF process is specified, the OSPF request queue information of all OSPF processes is displayed.

Examples

Display OSPF request queue information.

```
<Sysname> display ospf request-queue
```

```
The Router's Neighbor is Router ID 2.2.2.2           Address 10.1.1.2
Interface 10.1.1.1           Area 0.0.0.0
Request list:
  Type      LinkState ID   AdvRouter      Sequence   Age
  Router    2.2.2.2        1.1.1.1        80000004   1
  Network   192.168.0.1    1.1.1.1        80000003   1
  Sum-Net   192.168.1.0    1.1.1.1        80000002   2
```

Table 24 Command output

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID
Address	Neighbor interface IP address
Interface	Local interface IP address
Area	Area ID
Request list	Request list information
Type	LSA type
LinkState ID	Link state ID
AdvRouter	Advertising router
Sequence	LSA sequence number
Age	LSA age

display ospf retrans-queue

Syntax

```
display ospf [ process-id ] retrans-queue [ interface-type interface-number ] [ neighbor-id ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number.

neighbor-id: Neighbor's router ID.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf retrans-queue** to display retransmission queue information.

If no OSPF process is specified, the retransmission queue information of all OSPF processes is displayed.

Examples

```
# Display OSPF retransmission queue information.
```

```
<Sysname> display ospf retrans-queue
```

```
The Router's Neighbor is Router ID 2.2.2.2           Address 10.1.1.2
Interface 10.1.1.1           Area 0.0.0.0
Retransmit list:
  Type      LinkState ID   AdvRouter      Sequence      Age
  Router    2.2.2.2        2.2.2.2        80000004     1
  Network   12.18.0.1      2.2.2.2        80000003     1
  Sum-Net   12.18.1.0      2.2.2.2        80000002     2
```

Table 25 Command output

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID
Address	Neighbor interface IP address
Interface	Interface address of the router
Area	Area ID
Retrans List	Retransmission list
Type	LSA type
LinkState ID	Link state ID
AdvRouter	Advertising router
Sequence	LSA sequence number
Age	LSA age

display ospf routing

Syntax

```
display ospf [ process-id ] routing [ interface interface-type interface-number ] [ nexthop  
nexthop-address ] [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

interface *interface-type interface-number*: Displays OSPF routing information advertised via the specified interface.

nexthop *nexthop-address*: Displays OSPF routing information with the specified next hop.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf routing** to display OSPF routing information.

If no OSPF process is specified, the routing information of all OSPF processes is displayed.

Examples

```
# Display OSPF routing information.
```

```
<Sysname> display ospf routing
```

```
OSPF Process 1 with Router ID 192.168.1.2
Routing Tables

Routing for Network
Destination          Cost  Type      NextHop      AdvRouter     Area
192.168.1.0/24       1562  Stub      192.168.1.2  192.168.1.2   0.0.0.0
172.16.0.0/16        1563  Inter     192.168.1.1  192.168.1.1   0.0.0.0

Total Nets: 2
Intra Area: 1  Inter Area: 1  ASE: 0  NSSA: 0
```

Table 26 Command output

Field	Description
Destination	Destination network

Field	Description
Cost	Cost to destination
Type	Route type: intra-area, transit, stub, inter-area, type1 external, type2 external.
NextHop	Next hop address
AdvRouter	Advertising router
Area	Area ID
Total Nets	Total networks
Intra Area	Total intra-area routes
Inter Area	Total inter-area routes
ASE	Total ASE routes
NSSA	Total NSSA routes

display ospf vlink

Syntax

```
display ospf [ process-id ] vlink [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospf vlink** to display OSPF virtual link information.

If no OSPF process is specified, the OSPF virtual link information of all OSPF processes is displayed.

Examples

```
# Display OSPF virtual link information.
```

```
<Sysname> display ospf vlink
      OSPF Process 1 with Router ID 3.3.3.3
      Virtual Links

Virtual-link Neighbor-ID -> 2.2.2.2, Neighbor-State: Full
Interface: 10.1.2.1 (Vlan-interface20)
```

```
Cost: 1562 State: P-2-P Type: Virtual
Transit Area: 0.0.0.1
Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
```

Table 27 Command output

Field	Description
Virtual-link Neighbor-ID	ID of the neighbor on the virtual link
Neighbor-State	Neighbor State: Down, Init, 2-Way, ExStart, Exchange, Loading, Full.
Interface	IP address and name of the local interface on the virtual link
Cost	Interface route cost
State	Interface state
Type	Type: virtual link
Transit Area	Transit area ID
Timers	Values of timers: hello, dead, retransmit, and interface transmission delay

displayrouter id

Syntax

```
display router id [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display router id** to display the global router ID.

Examples

```
# Display the global router ID.
<Sysname> display router id
        Configured router ID is 1.1.1.1
```


dscp (OSPF view)

Syntax

```
dscp dscp-value  
undo dscp
```

View

OSPF view

Default level

2: System level

Parameters

dscp-value: Sets the Differentiated Services Code Point (DSCP) value for OSPF packets, in the range of 0 to 63.

Description

Use **dscp** to set the DSCP value for OSPF packets.

Use **undo dscp** to restore the default.

By default, the DSCP value in OSPF packets is 48.

Examples

```
# Set the DSCP value for OSPF packets of OSPF process 1 to 63.  
<Sysname> system-view  
[Sysname] ospf  
[Sysname-ospf-1] dscp 63
```

enable link-local-signaling

Syntax

```
enable link-local-signaling  
undo enable link-local-signaling
```

View

OSPF view

Default level

2: System level

Parameters

None

Description

Use **enable link-local-signaling** to enable the OSPF link-local signaling (LLC) capability.

Use **undo enable link-local-signaling** to disable the OSPF link-local signaling capability.

By default, this capability is disabled.

Examples

```
# Enable link-local signaling for OSPF process 1.
```

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
```

enable log

Syntax

```
enable log [ config | error | state ]
undo enable log [ config | error | state ]
```

View

OSPF view

Default level

2: System level

Parameters

config: Enables configuration logging.

error: Enables error logging.

state: Enables state logging.

Description

Use **enable log** to enable specified OSPF logging.

Use **undo enable log** to disable specified OSPF logging.

OSPF logging is disabled by default.

If no keyword is specified, all logging is enabled.

Examples

```
# Enable OSPF logging.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] enable log
```

enable out-of-band-resynchronization

Syntax

```
enable out-of-band-resynchronization
undo enable out-of-band-resynchronization
```

View

OSPF view

Default level

2: System level

Parameters

None

Description

Use **enable out-of-band-resynchronization** to enable the OSPF out-of-band resynchronization (OOB-Resynch) capability.

Use **undo enable out-of-band-resynchronization** to disable the OSPF out-of-band resynchronization capability.

By default, the capability is disabled.

Before configuring this command, you must enable the link-local signaling capability.

Related commands: **enable link-local-signaling**.

Examples

```
# Enable the out-of-band resynchronization capability for OSPF process 1.
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
```

fast-reroute

Syntax

fast-reroute { **auto** [**abr-only**] | **route-policy** *route-policy-name* }

undo fast-reroute

View

OSPF view

Default level

2: System level

Parameters

auto: Calculates a backup next hop automatically for all routes.

abr-only: Selects only the route to the ABR as the backup path.

route-policy *route-policy-name*: References a routing policy to designate a backup next hop. The *route-policy-name* argument is a string of 1 to 63 case-sensitive characters.

Description

Use **fast-reroute** to configure OSPF fast reroute (FRR).

Use **undo fast-reroute** to restore the default.

By default, OSPF FRR is not configured.



IMPORTANT:

- Do not use OSPF FRR and BFD (for OSPF) at the same time; otherwise, OSPF FRR may fail to take effect.
 - Do not use the **fast-reroute auto** command together with the command **vlink-peer**.
-

Examples

```
# Enable FRR to automatically calculate a backup next hop for all routes in OSPF process 100.
<Sysname> system-view
```

```

[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] ospf 100
[Sysname-ospf-100] fast-reroute auto

# Enable FRR to designate a backup next hop by using routing policy frr for OSPF process 100.
<Sysname> system-view
[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] ip ip-prefix abc index 10 permit 100.1.1.0 24
[Sysname] route-policy frr permit node 10
[Sysname-route-policy] if-match ip-prefix abc
[Sysname-route-policy] apply fast-reroute backup-interface vlan-interface 1
backup-nexthop 193.1.1.8
[Sysname-route-policy] quit
[Sysname] ospf 100
[Sysname-ospf-100] fast-reroute route-policy frr

```

filter

Syntax

```

filter { acl-number | ip-prefix ip-prefix-name } { export | import }
undo filter { export | import }

```

View

OSPF area view

Default level

2: System level

Parameters

acl-number: ACL number, in the range of 2000 to 3999.

ip-prefix-name: IP prefix list name, a string of up to 19 characters. For more information about IP prefix lists, see *Layer 3 – IP Routing Configuration Guide*.

export: Filters Type-3 LSAs advertised to other areas.

import: Filters Type-3 LSAs advertised into the area.

Description

Use **filter** to configure incoming/outgoing Type-3 LSAs filtering on an ABR.

Use **undo filter** to disable Type-3 LSA filtering.

By default, Type-3 LSAs filtering is disabled.

NOTE:

This command is only available on an ABR.

Examples

```

# Apply IP prefix list my-prefix-list to filter inbound Type-3 LSAs, and apply ACL 2000 to filter outbound Type-3 LSAs in OSPF Area 1.

```

```

<Sysname> system-view
[Sysname] ospf 100

```

```
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] filter ip-prefix my-prefix-list import
[Sysname-ospf-100-area-0.0.0.1] filter 2000 export
```

filter-policy export (OSPF view)

Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name } export [ protocol [ process-id ] ]
undo filter-policy export [ protocol [ process-id ] ]
```

View

OSPF view

Default level

2: System level

Parameters

acl-number: Number of an ACL used to filter redistributed routes, in the range of 2000 to 3999.

ip-prefix-name: Name of an IP prefix list used to filter redistributed routes, a string of up to 19 characters.

protocol: Specifies a protocol from which to filter redistributed routes. The protocol can be **direct**, **static**, **rip**, **ospf**, **isis** or **bgp**. If no protocol is specified, all redistributed routes are filtered.

process-id: Process ID, which is required when the *protocol* is **rip**, **ospf** or **isis**, in the range of 1 to 65535.

Description

Use **filter-policy export** to configure the filtering of redistributed routes.

Use **undo filter-policy export** to disable the filtering.

By default, the filtering of redistributed routes is not configured.

You can use this command to filter redistributed routes as needed.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command, the ACL should be configured with the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr* *sour-wildcard* command to deny/permit a route with the specified destination, or with the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr* *sour-wildcard* **destination** *dest-addr* *dest-wildcard* command to deny/permit a route with the specified destination and mask. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route (the subnet mask must be valid; otherwise, the configuration is ineffective).

Related commands: **import-route**.

Examples

```
# Filter redistributed routes using ACL 2000.
```

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 export
```

```
# Configure ACL 3000 to permit only route 113.0.0.0/16 to pass, and reference ACL 3000 to filter redistributed routes.
```

```

<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0
[Sysname-acl-adv-3000] rule 100 deny ip
[Sysname-acl-adv-3000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 3000 export

```

filter-policy import (OSPF view)

Syntax

filter-policy { *acl-number* [**gateway** *ip-prefix-name*] | **gateway** *ip-prefix-name* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] | **route-policy** *route-policy-name* } **import**

undo filter-policy import

View

OSPF view

Default level

2: System level

Parameters

acl-number: Number of an ACL used to filter incoming routes, in the range of 2000 to 3999.

gateway *ip-prefix-name*: Name of an IP address prefix list used to filter routes received from specific neighbors. It is a string of up to 19 characters. For more information about IP prefix lists, see *Layer 3—IP Routing Configuration Guide*.

ip-prefix *ip-prefix-name*: Name of an IP address prefix list used to filter incoming routes based on destination IP address. It is a string of up to 19 characters. For more information about IP prefix lists, see *Layer 3—IP Routing Configuration Guide*.

route-policy *route-policy-name*: Name of a routing policy used to filter incoming routes based on routing policy, a string of up to 63 case-sensitive characters. For more information about routing policy, see *Layer 3—IP Routing Configuration Guide*.

Description

Use **filter-policy import** to configure the filtering of routes calculated from received LSAs.

Use **undo filter-policy import** to disable the filtering.

By default, the filtering is not configured.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command or in the routing policy, the ACL should be configured with the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr* *sour-wildcard* command to deny/permit a route with the specified destination, or with the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr* *sour-wildcard* **destination** *dest-addr* *dest-wildcard* command to deny/permit a route with the specified destination and mask. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route (the subnet mask must be valid; otherwise, the configuration is ineffective).

Examples

Filter incoming routes using ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 import
```

Configure ACL 3000 to permit only route 113.0.0.0/16 to pass, and reference ACL 3000 to filter incoming routes.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0
[Sysname-acl-adv-3000] rule 100 deny ip
[Sysname-acl-adv-3000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 3000 import
```

graceful-restart (OSPF view)

Syntax

```
graceful-restart [ ietf | nonstandard ]
undo graceful-restart
```

View

OSPF view

Default level

2: System level

Parameters

ietf: Enables the IETF GR capability.

nonstandard: Enables the non-IETF GR capability.

Description

Use **graceful-restart** to enable OSPF Graceful Restart capability.

Use **undo graceful-restart** to disable OSPF Graceful Restart capability.

By default, OSPF Graceful Restart capability is disabled.

Enable Opaque LSA advertisement and reception with the **opaque-capability enable** command before enabling the IETF GR capability for OSPF.

Before enabling non-IETF GR capability for OSPF, enable OSPF LLS (link local signaling) with the **enable link-local-signaling** command and OOB (out of band resynchronization) with the **enable out-of-band-resynchronization** command.

If the keywords **nonstandard** and **ietf** are not specified when OSPF GR is enabled, **nonstandard** is the default.

Related commands: **enable link-local-signaling**, **enable out-of-band-resynchronization**, and **opaque-capability enable**.

Examples

```
# Enable IETF Graceful Restart for OSPF process 1.
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] opaque-capability enable
[Sysname-ospf-1] graceful-restart ietf

# Enable non-IETF Graceful Restart for OSPF process 1.
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
[Sysname-ospf-1] graceful-restart nonstandard
```

graceful-restart help

Syntax

```
graceful-restart help { acl-number | prefix prefix-list }
undo graceful-restart help
```

View

OSPF view

Default level

2: System level

Parameters

acl-number: Basic or advanced ACL number, in the range of 2000 to 3999.

prefix-list: Name of the specified IP prefix list, a string of 1 to 19 characters.

Description

Use **graceful-restart help** to configure for which OSPF neighbors the current router can serve as a GR Helper. (The neighbors are specified by the ACL or the IP prefix list.)

Use **undo graceful-restart help** to restore the default.

By default, the router can serve as a GR Helper for any OSPF neighbor.

Examples

```
# Enable IETF standard GR for OSPF process 1 and configure the router as a GR Helper for OSPF
neighbors defined in the ACL 2001.
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] opaque-capability enable
[Sysname-ospf-1] graceful-restart help 2001

# Enable non IETF standard GR for OSPF process 1 and configure the router as a GR Helper for OSPF
neighbors defined in the ACL 2001.
<Sysname> system-view
```



```
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
[Sysname-ospf-1] graceful-restart help 2001
```

graceful-restart interval (OSPF view)

Syntax

```
graceful-restart interval interval-value
undo graceful-restart interval
```

View

OSPF view

Default level

2: System level

Parameters

interval-value: Specifies the Graceful Restart interval, in the range of 40 to 1,800 seconds.

Description

Use **graceful-restart interval** to configure the Graceful Restart interval.

Use **undo graceful-restart interval** to restore the default Graceful Restart interval.

By default, the Graceful Restart interval is 120 seconds.

The Graceful Restart interval of OSPF cannot be less than the maximum value of dead intervals on all OSPF interfaces; otherwise, the Graceful Restart of OSPF may fail.

Related commands: **ospf timer dead**.

Examples

```
# Configure the Graceful Restart interval for OSPF process 1 as 100 seconds.
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] graceful-restart interval 100
```

host-advertise

Syntax

```
host-advertise ip-address cost
undo host-advertise ip-address
```

View

OSPF area view

Default level

2: System level

Parameters

ip-address: IP address of a host

cost: Cost of the route, in the range of 1 to 65535.

Description

Use **host-advertise** to advertise a host route.

Use **undo host-advertise** to remove a host route.

No host route is advertised by default.

Examples

```
# Advertise route 1.1.1.1 with a cost of 100.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] host-advertise 1.1.1.1 100
```

import-route (OSPF view)

Syntax

import-route *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id* | **all-processes**]

View

OSPF view

Default level

2: System level

Parameters

protocol: Redistributes routes from the specified protocol, which can be **bgp**, **direct**, **isis**, **ospf**, **rip**, or **static**.

process-id: Process ID, in the range of 1 to 65535. The default is 1. It is available only when the *protocol* is **rip**, **ospf**, or **isis**.

all-processes: Redistributes routes from all the processes of the specified routing protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

allow-ibgp: Allows IBGP routes redistribution. It is optional only when the *protocol* is **bgp**.

cost *cost*: Specifies a route cost, in the range of 0 to 16777214. The default is 1.

type *type*: Specifies a cost type, 1 or 2. The default is 2.

tag *tag* : Specifies a tag for external LSAs. The default is 1.

route-policy *route-policy-name*: Specifies a routing policy to redistribute qualified routes only. A routing policy name is a string of up to 63 case-sensitive characters.

Description

Use **import-route** to redistribute routes from another protocol.

Use **undo import-route** to disable route redistribution from a protocol.

Route redistribution from another protocol is not configured by default.

OSPF prioritize routes into the following levels:

- Intra-area route
- Inter-area route
- Type1 External route
- Type2 External route

An intra-area route is a route in an OSPF area. An inter-area route is between any two OSPF areas. Both of them are internal routes.

An external route is a route to a destination outside the OSPF AS.

A Type-1 external route has high reliability. Its cost is comparable with the cost of OSPF internal routes. The cost from an OSPF router to a Type-1 external route's destination equals the cost from the router to the ASBR plus the cost from the ASBR to the external route's destination.

A Type-2 external route has low credibility, so OSPF considers the cost from the ASBR to a Type-2 external route is much bigger than the cost from the ASBR to an OSPF internal router. The cost from an internal router to a Type-2 external route's destination equals the cost from the ASBR to the Type-2 external route's destination.

The **import-route** command cannot redistribute default routes.

Use the **import-route bgp allow-ibgp** command with care, because it redistributes both EBGP and IBGP routes that may cause routing loops.

Only active routes can be redistributed. Use the **display ip routing-table protocol** command to display route state information.

The **undo import-route protocol all-processes** command cancels the configuration made by the **import-route protocol all-processes** command, rather than the **import-route protocol process-id** command.

Related commands: **default-route-advertise**.

Examples

Redistribute routes from RIP process 40 and specify the type, tag, and cost as 2, 33 and 50 for redistributed routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] import-route rip 40 type 2 tag 33 cost 50
```

ispf enable

Syntax

ispf enable

undo ispf enable

View

OSPF view

Default level

2: System level

Parameters

None

Description

Use **ispf enable** to enable OSPF ISPF.

Use **undo ispf enable** to disable OSPF ISPF.

By default, OSPF ISPF is disabled.

When a network topology is changed, ISPF allows the system to recompute only the affected part of the shortest path tree (SPT), instead of the entire SPT.

Examples

```
# Enable OSPF ISPF.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] ispf enable
```

log-peer-change

Syntax

log-peer-change

undo log-peer-change

View

OSPF view

Default level

2: System level

Parameters

None

Description

Use **log-peer-change** to enable the logging of OSPF neighbor state changes.

Use **undo log-peer-change** to disable the logging.

The logging is enabled by default.

With this feature enabled, information about neighbor state changes is displayed on the terminal until the feature is disabled.

Examples

```
# Disable the logging of neighbor state changes for OSPF process 100.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo log-peer-change
```

lsa-arrival-interval

Syntax

lsa-arrival-interval *interval*

undo lsa-arrival-interval

View

OSPF view

Default level

2: System level

Parameters

interval: Specifies the LSA arrival interval in milliseconds, in the range of 0 to 60000.

Description

Use **lsa-arrival-interval** to specify the LSA arrival interval.

Use **undo lsa-arrival-interval** to restore the default.

The interval defaults to 1000 milliseconds.

If an LSA that has the same LSA type, LS ID, originating router ID with the previous LSA is received within the interval, the LSA will be discarded. This feature helps protect routers and bandwidth from being over-consumed due to frequent network changes.

HP recommends that the interval set with the **lsa-arrival-interval** command is smaller or equal to the initial interval set with the **lsa-generation-interval** command.

Related commands: **lsa-generation-interval**.

Examples

```
# Set the LSA arrival interval to 200 milliseconds.  
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] lsa-arrival-interval 200
```

lsa-generation-interval

Syntax

```
lsa-generation-interval maximum-interval [ initial-interval [ incremental-interval ] ]  
undo lsa-generation-interval
```

View

OSPF view

Default level

2: System level

Parameters

maximum-interval: Maximum LSA generation interval in seconds, in the range of 1 to 60. The default is 5 seconds.

initial-interval: Minimum LSA generation interval in milliseconds, in the range of 10 to 60000. The default is 0.

incremental-interval: LSA generation incremental interval in milliseconds, in the range of 10 to 60000. The default is 5000 milliseconds.

Description

Use **lsa-generation-interval** to configure the OSPF LSA generation interval.

Use **undo lsa-generation-interval** to restore the default.

By default, the maximum interval is 5 seconds, the minimum interval is 0 milliseconds, and the incremental interval is 5000 milliseconds..

With this command configured, when network changes are not frequent, LSAs are generated at the *initial-interval*. If network changes become frequent, LSA generation interval is incremented by a specified value each time a generation happens, up to the *maximum-interval*.

Related commands: **lsa-arrival-interval**.

Examples

```
# Configure the maximum LSA generation interval as 2 seconds, minimum interval as 100 milliseconds
and incremental interval as 100 milliseconds.
```

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-generation-interval 2 100 100
```

lsdb-overflow-limit

Syntax

lsdb-overflow-limit *number*

undo lsdb-overflow-limit

View

OSPF view

Default level

2: System level

Parameters

number: Specifies the upper limit of external LSAs in the LSDB, in the range of 1 to 1000000.

Description

Use **lsdb-overflow-limit** to specify the upper limit of external LSAs in the LSDB.

Use **undo lsdb-overflow-limit** to restore the default.

External LSAs in the LSDB are not limited by default.

Examples

```
# Specify the upper limit of external LSAs as 400000.
```

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsdb-overflow-limit 400000
```

maximum load-balancing (OSPF view)

Syntax

maximum load-balancing *maximum*

undo maximum load-balancing

View

OSPF view

Default level

2: System level

Parameters

maximum: Maximum number of ECMP routes, in the range of 1 to 8. No load balancing is available when the number is set to 1.

Description

Use **maximum load-balancing** to specify the maximum number of ECMP routes.

Use **undo maximum load-balancing** to restore the default.

By default, the maximum number of ECMP routes is 8.

Examples

```
# Specify the maximum number of ECMP routes as 2.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] maximum load-balancing 2
```

maximum-routes

Syntax

```
maximum-routes { external | inter | intra } number
undo maximum-routes { external | inter | intra }
```

View

OSPF view

Default level

2: System level

Parameters

external: Specifies the maximum number of external routes.

inter: Specifies the maximum number of inter-area routes.

intra: Specifies the maximum number of intra-area routes.

number: Maximum route number. The maximum and default route numbers vary with devices.

Description

Use **maximum-routes** to specify the maximum route number of a specified type, inter-area, intra-area or external.

Use **undo maximum-routes** to restore the default route maximum value of a specified type.

Examples

```
# Specify the maximum number of intra-area routes as 500.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] maximum-routes intra 500
```

network (OSPF area view)

Syntax

```
network ip-address wildcard-mask  
undo network ip-address wildcard-mask
```

View

OSPF area view

Default level

2: System level

Parameters

ip-address: IP address of a network.

wildcard-mask: Wildcard mask of the IP address. For example, the wildcard mask of mask 255.0.0.0 is 0.255.255.255.

Description

Use **network** to enable OSPF on the interface attached to the specified network in the area.

Use **undo network** to disable OSPF for the interface attached to the specified network in the area.

By default, an interface neither belongs to any area nor runs OSPF.

You can configure one or multiple interfaces in an area to run OSPF. The interface's primary IP address must fall into the specified network segment to make the interface run OSPF. If only the interface's secondary IP address falls into the network segment, the interface cannot run OSPF.

Related commands: **ospf**.

Examples

```
# Specify the interface whose primary IP address falls into 131.108.20.0/24 to run OSPF in Area 2.
```

```
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] area 2  
[Sysname-ospf-100-area-0.0.0.2] network 131.108.20.0 0.0.0.255
```

nssa

Syntax

```
nssa [ default-route-advertise | no-import-route | no-summary | translate-always |  
translator-stability-interval value ] *
```

```
undo nssa
```

View

OSPF area view

Default level

2: System level

Parameters

default-route-advertise: Usable on an NSSA ABR or an ASBR only. If it is configured on an NSSA ABR, the ABR generates a default route in a Type-7 LSA into the NSSA area regardless of whether a default route is configured. If it is configured on an ASBR, only a default route is configured on the ASBR can it generates the default route in a Type-7 LSA into the attached area.

no-import-route: Usable only on an NSSA ABR that is also the ASBR of the OSPF routing domain to disable redistributing routes in Type-7 LSAs into the NSSA area, making sure that correct external routes are redistributed.

no-summary: Usable only on an NSSA ABR to advertise a default route in a Type-3 summary LSA into the NSSA area and to not advertise other summary LSAs into the area. Such an area is a totally NSSA area.

translate-always: Specifies the NSSA ABR as a translator to translate Type-7 LSAs to Type-5 LSAs.

translator-stability-interval *value*: Specifies the stability interval of the translator, during which the translator can maintain its translating capability after a device with a higher priority becomes a new translator. The *value* argument is the stability interval in seconds, which is in the range of 0 to 900 and defaults to 0 (which means the translator does not maintain its translating capability if a new translator arises).

Description

Use **nssa** to configure the current area as an NSSA area.

Use **undo nssa** to restore the default.

By default, no NSSA area is configured.

All routers attached to an NSSA area must be configured with the **nssa** command in area view.

Related commands: **default-cost**.

Examples

```
# Configure Area 1 as an NSSA area.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] nssa
```

opaque-capability enable

Syntax

opaque-capability enable

undo opaque-capability

View

OSPF view

Default level

2: System level

Parameters

None

Description

Use **opaque-capability enable** to enable opaque LSA advertisement and reception. With the command configured, the OSPF device can receive and advertise the Type-9, Type-10 and Type-11 opaque LSAs.

Use the **undo opaque-capability** command to restore the default.

The feature is disabled by default.

Examples

```
# Enable advertising and receiving opaque LSAs.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] opaque-capability enable
```

ospf

Syntax

```
ospf [ process-id | router-id router-id | vpn-instance vpn-instance-name ] *
undo ospf [ process-id ]
```

View

System view

Default level

2: System level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

router-id *router-id*: OSPF Router ID, in dotted decimal format.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN that the OSPF process belongs to. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the OSPF process belongs to the public network.

Description

Use **ospf** to enable an OSPF process.

Use **undo ospf** to disable an OSPF process.

No OSPF process is enabled by default.

You can enable multiple OSPF processes on a router and specify different Router IDs for these processes.

Enabling OSPF first is required before performing other tasks.

Examples

```
# Enable OSPF process 100 and specify Router ID 10.10.10.1.
<Sysname> system-view
[Sysname] ospf 100 router-id 10.10.10.1
[Sysname-ospf-100]
```

ospf authentication-mode

Syntax

For MD5/HMAC-MD5 authentication:

```
ospf authentication-mode { hmac-md5 | md5 } key-id [ cipher | plain ] password
```

```
undo ospf authentication-mode { hmac-md5 | md5 } key-id
```

For simple authentication:

```
ospf authentication-mode simple [ cipher | plain ] password
```

```
undo ospf authentication-mode simple
```

View

Interface view

Default level

2: System level

Parameters

hmac-md5: HMAC-MD5 authentication.

md5: MD5 authentication.

simple: Simple authentication.

key-id: Authentication key ID, in the range of 1 to 255.

cipher: Sets a ciphertext password.

plain: Sets a plaintext password.

password: Sets the authentication password. This argument is case sensitive. For simple authentication mode, it is plaintext string of 1 to 8 characters, or a ciphertext string of 1 to 41 characters. For MD5/HMAC-MD5 authentication mode, it is a plaintext string of 1 to 16 characters, or a ciphertext string of 1 to 53 characters.

Description

Use **ospf authentication-mode** to set the authentication mode and authentication parameters on an interface.

Use **undo ospf authentication-mode** to remove specified configuration.

By default, no authentication is available on an interface.

Interfaces attached to the same network segment must have the same authentication password and mode.

The authentication password, set in either plain text or cipher text, is saved to the configuration file in cipher text.

If neither **cipher** nor **plain** is specified, **cipher** applies to the MD5/HMAC-MD5 authentication mode and **plain** applies to the simple authentication mode, by default.

Related commands: **authentication-mode**.

Examples

```
# Configure the network 131.119.0.0/16 in Area 1 to support MD5 authentication, and set the interface key ID to 15 and plaintext authentication password to abc.
```

```

<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[Sysname-ospf-100-area-0.0.0.1] authentication-mode md5
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf authentication-mode md5 15 plain abc

```

Configure the network 131.119.0.0/16 in Area 1 to support simple authentication, and set for the interface the plaintext authentication password to **abc**.

```

<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[Sysname-ospf-100-area-0.0.0.1] authentication-mode simple
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf authentication-mode simple plain abc

```

ospf bfd enable

Syntax

```

ospf bfd enable [ echo ]
undo ospf bfd enable

```

View

Interface view

Default level

2: System level

Parameters

echo: Configures BFD echo packet single-hop detection. If this keyword is not specified, BFD control packet bidirectional detection is enabled.

Description

Use **ospf bfd enable** to enable BFD for link failure detection on an OSPF interface.

Use **undo ospf bfd enable** to disable BFD on an OSPF interface.

By default, an OSPF interface is not enabled with BFD.

Examples

Enable OSPF and BFD on VLAN-interface 11.

```

<Sysname> system-view
[Sysname] ospf
[Sysname-ospf-1] area 0
[Sysname-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
[Sysname] interface vlan-interface 11

```

```
[Sysname-Vlan-interface11] ospf bfd enable
```

ospf cost

Syntax

ospf cost *value*

undo ospf cost

View

Interface view

Default level

2: System level

Parameters

value: OSPF cost, in the range of 0 to 65535 for a loopback interface and 1 to 65535 for other interfaces.

Description

Use **ospf cost** to set an OSPF cost for the interface.

Use **undo ospf cost** to restore the default.

The default cost depends on the interface type: 1 for a VLAN interface; 0 for a loopback interface; computed according to the bandwidth for other interfaces with the formula: Interface OSPF cost = Bandwidth reference value (100 Mbps) ÷ Interface bandwidth (Mbps).

If the calculated cost is greater than 65535, the value of 65535 is used; if the calculated cost is smaller than 1, the value of 1 is used.

Examples

```
# Set the OSPF cost for the interface to 65.  
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] ospf cost 65
```

ospf dr-priority

Syntax

ospf dr-priority *priority*

undo ospf dr-priority

View

Interface view

Default level

2: System level

Parameters

priority: DR Priority of the interface, in the range of 0 to 255.

Description

Use **ospf dr-priority** to set the priority for DR/BDR election on an interface.

Use **undo ospf dr-priority** to restore the default value.

By default, the priority is 1.

The bigger the value, the higher the priority. If a device has a priority of 0, it will not be elected as a DR or BDR.

Examples

```
# Set the DR priority on the current interface to 8.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf dr-priority 8
```

ospf mib-binding

Syntax

ospf mib-binding *process-id*

undo ospf mib-binding

View

System view

Default level

2: System level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

Description

Use **ospf mib-binding** to bind an OSPF process to MIB operation for responding to SNMP requests.

Use **undo ospf mib-binding** to restore the default.

By default, MIB operation is bound to the OSPF process with the smallest process ID.

Examples

```
# Bind OSPF process 100 to MIB operation.
<Sysname> system-view
[Sysname] ospf mib-binding 100

# Restore the default, which means binding the OSPF process with the smallest process ID to MIB operation.
<Sysname> system-view
[Sysname] undo ospf mib-binding
```

ospf mtu-enable

Syntax

ospf mtu-enable

undo ospf mtu-enable

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **ospf mtu-enable** to enable an interface to add the real MTU into DD packets.

Use **undo ospf mtu-enable** to restore the default.

By default, an interface adds a MTU of 0 into DD packets, which means no real MTU is added.

- After a virtual link is established via a Tunnel, two devices on the link from different vendors may have different MTU values. To make them consistent, set the attached interfaces' default MTU to 0.
- After this command is configured, upon receiving a DD packet, the interface checks whether the MTU in the packet is greater than its own MTU; if yes, the interface discards the packet.

Examples

Enable the interface to add the real MTU value into DD packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf mtu-enable
```

ospf network-type

Syntax

```
ospf network-type { broadcast | nbma | p2mp [ unicast ] | p2p }
undo ospf network-type
```

View

Interface view

Default level

2: System level

Parameters

broadcast: Specifies the network type as Broadcast.

nbma: Specifies the network type as NBMA.

p2mp: Specifies the network type as P2MP.

unicast: Specifies the P2MP interface to unicast OSPF packets. By default, a P2MP interface multicasts OSPF packets.

p2p: Specifies the network type as P2P.

Description

Use **ospf network-type** to set the network type for an interface.

Use **undo ospf network-type** to restore the default network type for an interface.

By default, the network type of an interface depends on its link layer protocol.

- For Ethernet, and FDDI, the default network type is broadcast.

- For ATM, FR, and X.25, the default network type is NBMA.
- For PPP, LAPB, HDLC, and POS, the default network type is P2P.

If a router on a broadcast network does not support multicast, you can configure the interface's network type as NBMA.

If any two routers on an NBMA network are directly connected via a virtual link—the network is fully meshed, you can configure the network type as NBMA; otherwise, you need to configure it as P2MP for two routers having no direct link to exchange routing information via another router.

When the network type of an interface is NBMA or P2MP unicast, you need to use the **peer** command to specify a neighbor.

If only two routers run OSPF on a network segment, you can configure associated interfaces' network type as P2P.

When the network type of an interface is P2MP unicast, all OSPF packets are sent out the interface through unicast.

Related commands: **ospf dr-priority**.

Examples

```
# Configure an interface's OSPF network type as NBMA.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf network-type nbma
```

ospf packet-process prioritized-treatment

Syntax

```
ospf packet-process prioritized-treatment
undo ospf packet-process prioritized-treatment
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **ospf packet-process prioritized-treatment** to enable OSPF to give priority to receiving and processing Hello packets.

Use **undo ospf packet-process prioritized-treatment** to restore the default.

By default, this function is not enabled.

Examples

```
# Enable OSPF to give priority to receiving and processing Hello packets.
<Sysname> system-view
[Sysname] ospf packet-process prioritized-treatment
```


ospf timer dead

Syntax

ospf timer dead *seconds*

undo ospf timer dead

View

Interface view

Default level

2: System level

Parameters

seconds: Dead interval in seconds, in the range of 1 to 2147483647.

Description

Use **ospf timer dead** to set the dead interval.

Use **undo ospf timer dead** to restore the default.

The dead interval defaults to 40s for Broadcast, P2P interfaces and defaults to 120s for P2MP and NBMA interfaces.

If an interface receives no hello packet from a neighbor within the dead interval, the interface considers the neighbor down. The dead interval on an interface is at least four times the hello interval. Any two routers attached to the same segment must have the same dead interval.

Related commands: **ospf timer hello**.

Examples

Configure the dead interval on the current interface as 60 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer dead 60
```

ospf timer hello

Syntax

ospf timer hello *seconds*

undo ospf timer hello

View

Interface view

Default level

2: System level

Parameters

seconds: Hello interval in seconds, in the range of 1 to 65535.

Description

Use **ospf timer hello** to set the hello interval on an interface.

Use **undo ospf timer hello** to restore the default hello interval on an interface.

The hello interval defaults to 10s for P2P and Broadcast interfaces, and defaults to 30s for P2MP and NBMA interfaces.

The shorter the hello interval is, the faster the topology converges and the more resources are consumed. Make sure the hello interval on two neighboring interfaces is the same.

Related commands: **ospf timer dead**.

Examples

```
# Configure the hello interval on the current interface as 20 seconds.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer hello 20
```

ospf timer poll

Syntax

ospf timer poll *seconds*

undo ospf timer poll

View

Interface view

Default level

2: System level

Parameters

seconds: Poll interval in seconds, in the range of 1 to 2147483647.

Description

Use **ospf timer poll** to set the poll interval on an NBMA interface.

Use **undo ospf timer poll** to restore the default value.

By default, the poll interval is 120s.

When an NBMA interface finds its neighbor is down, it will send hello packets at the poll interval.



IMPORTANT:

The poll interval must be at least four times the hello interval.

Related commands: **ospf timer hello**.

Examples

```
# Set the poll timer interval on the current interface to 130 seconds.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer poll 130
```

ospf timer retransmit

Syntax

```
ospf timer retransmit interval  
undo ospf timer retransmit
```

View

Interface view

Default level

2: System level

Parameters

interval: LSA retransmission interval in seconds, in the range of 1 to 3600.

Description

Use **ospf timer retransmit** to set the LSA retransmission interval on an interface.

Use **undo ospf timer retransmit** to restore the default.

The interval defaults to 5s.

After sending an LSA, an interface waits for an acknowledgement packet. If the interface receives no acknowledgement within the retransmission interval, it will retransmit the LSA.

The retransmission interval should not be so small to avoid unnecessary retransmissions.

Examples

```
# Set the LSA retransmission interval to 8 seconds.  
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] ospf timer retransmit 8
```

ospf trans-delay

Syntax

```
ospf trans-delay seconds  
undo ospf trans-delay
```

View

Interface view

Default level

2: System level

Parameters

seconds: LSA transmission delay in seconds, in the range of 1 to 3600.

Description

Use **ospf trans-delay** to set the LSA transmission delay on an interface.

Use **undo ospf trans-delay** to restore the default.

The LSA transmission delay defaults to 1 second.

Each LSA in the LSDB has an age that is incremented by 1 every second, but the age does not change during transmission. It is necessary to add a transmission delay into its age time, which is important for low speed networks.

Examples

```
# Set the LSA transmission delay to 3 seconds on the current interface.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf trans-delay 3
```

peer

Syntax

```
peer ip-address [ cost value | dr-priority dr-priority ]
undo peer ip-address
```

View

OSPF view

Default level

2: System level

Parameters

ip-address: Neighbor IP address.

cost *value*: Specifies the cost to reach the neighbor, in the range of 1 to 65535.

dr-priority *dr-priority*: Specifies the neighbor DR priority, in the range of 0 to 255. The default neighbor DR priority is 1.

Description

Use **peer** to specify a neighbor, and the DR priority of the neighbor.

Use **undo peer** to remove the configuration.

On an X.25 or Frame Relay network, you can configure mappings to make the network fully meshed (any two routers have a direct link in between), so OSPF can handle DR/BDR election as it does on a broadcast network. However, since routers on the network cannot find neighbors via broadcasting hello packets, you need to specify neighbors and neighbor DR priorities on the routers.

After startup, a router sends a hello packet to neighbors with DR priorities higher than 0. When the DR and BDR are elected, the DR will send hello packets to all neighbors for adjacency establishment.

The cost set with the **peer** command is the cost to the specified neighbor on the P2MP link. If no cost is specified, the cost to the neighbor equals the local interface's cost.

A router uses the priority set with the **peer** command to determine whether to send a hello packet to the neighbor rather than for DR election. The DR priority set with the **ospf dr-priority** command is used for DR election.

Related commands: **ospf dr-priority**.

Examples

```
# Specify the neighbor 1.1.1.1.
```

```
<Sysname> system-view
[Sysname] ospf 100
```

```
[Sysname-ospf-100] peer 1.1.1.1
```

preference

Syntax

```
preference [ ase ] [ route-policy route-policy-name ] value
```

```
undo preference [ ase ]
```

View

OSPF view

Default level

2: System level

Parameters

ase: Sets a preference for ASE routes. If the keyword is not specified, using the command sets a preference for OSPF internal routes.

route-policy *route-policy-name*: References a routing policy to set priorities for specified routes. A *route-policy-name* is a string of 1 to 63 case-sensitive characters.

value: Preference value, in the range of 1 to 255. A smaller value represents a higher preference.

Description

Use **preference** to set the preference of OSPF routes.

Use **undo preference** to restore the default.

The preference of OSPF internal routes defaults to 10, and the preference of OSPF external routes defaults to 150.

If a routing policy is specified, priorities defined by the routing policy will apply to matching routes, and the priorities set with the **preference** command apply to OSPF routes not matching the routing policy.

A router may run multiple routing protocols. When several routing protocols find routes to the same destination, the router uses the route found by the protocol with the highest preference.

Examples

```
# Set a preference of 200 for OSPF external routes.
```

```
<Sysname> system-view
```

```
[Sysname] ospf 100
```

```
[Sysname-ospf-100] preference ase 200
```

reset ospf counters

Syntax

```
reset ospf [ process-id ] counters [ neighbor [ interface-type interface-number ] [ router-id ] ]
```

View

User view

Default level

1: Monitor level

Parameters

process-id: Clears the statistics of the specified OSPF process, in the range of 1 to 65535.

neighbor: Clears neighbor statistics.

interface-type interface-number: Clears the statistics of the neighbor connected to the specified interface.

router-id: Clears the statistics of the specified neighbor.

Description

Use **reset ospf counters** to clear OSPF statistics.

Examples

```
# Reset OSPF counters.
<Sysname> reset ospf counters
```

reset ospf process

Syntax

```
reset ospf [ process-id ] process [ graceful-restart ]
```

View

User view

Default level

2: System level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

graceful-restart: Reset the OSPF process using GR.

Description

Use **reset ospf process** to reset all OSPF processes or a specified process.

Using the **reset ospf process** command will:

- Clear all invalid LSAs without waiting for their timeouts;
- Make a newly configured Router ID take effect;
- Start a new round of DR/BDR election;
- Not remove any previous OSPF configurations.

The system prompts you to select whether to reset OSPF process upon execution of this command.

Examples

```
# Reset all OSPF processes.
<Sysname> reset ospf process
Warning : Reset OSPF process? [Y/N]:Y

# Reset all OSPF processes using GR.
<Sysname> reset ospf process graceful-restart
Warning : Reset OSPF process? [Y/N]:Y
```

reset ospf redistribution

Syntax

```
reset ospf [ process-id ] redistribution
```

View

User view

Default level

2: System level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

Description

Use **reset ospf redistribution** to restart route redistribution. If no process ID is specified, using the command restarts route redistribution for all OSPF processes.

Examples

```
# Restart route redistribution.  
<Sysname> reset ospf redistribution
```

rfc1583 compatible

Syntax

```
rfc1583 compatible  
undo rfc1583 compatible
```

View

OSPF view

Default level

2: System level

Parameters

None

Description

Use **rfc1583 compatible** to make routing rules defined in RFC 1583 compatible.

Use **undo rfc1583 compatible** to disable the function.

By default, RFC 1583 routing rules are compatible.

RFC 1583 and RFC 2328 have different routing rules on selecting the best route when multiple AS external LSAs describe routes to the same destination. Using this command can make them compatible. If RFC 1583 is made compatible with RFC 2328, the routes in the backbone area are preferred, if not, the routes in the non-backbone area are preferred to reduce the burden of the backbone area.

Examples

```
# Disable making RFC 1583 routing rules compatible.  
<Sysname> system-view  
[Sysname] ospf 100
```

```
[Sysname-ospf-100] undo rfc1583 compatible
```

router id

Syntax

```
router id router-id
```

```
undo router id
```

View

System view

Default level

2: System level

Parameters

router-id: Router ID, in the form of a dotted decimal IPv4 address.

Description

Use **router id** to configure a global router ID.

Use **undo router id** to remove the global router ID.

By default, no global router ID is configured.

Some routing protocols use a router ID to identify a device. You can configure a global router ID, which is used by routing protocols that have no router ID configured.

If no global router ID is configured, the highest loopback interface IP address, if any, is used as the router ID. If no loopback interface IP address is available, the highest physical interface IP address is used, regardless of the interface status.

If the interface whose IP address is the router ID is removed or modified, a new router ID is selected. Other events, (the interface goes down; after a physical interface address is selected as the router ID, an IP address is configured for a loopback interface; a higher interface IP address is configured) will not trigger a router ID re-selection.

After a router ID is changed, you need to use the **reset ospf process** command to make it effective.

Examples

```
# Configure a global router ID.  
<Sysname> system-view  
[Sysname] router id 1.1.1.1
```

silent-interface (OSPF view)

Syntax

```
silent-interface { interface-type interface-number | all }
```

```
undo silent-interface { interface-type interface-number | all }
```

View

OSPF view

Default level

2: System level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

all: Specifies all interfaces.

Description

Use **silent-interface** to disable an interface or all interfaces from receiving and sending OSPF packets.

Use **undo silent-interface** to restore the default.

By default, an interface can receive send OSPF packets.

A disabled interface is a passive interface, which cannot receive and send any hello packet.

To make no routing information obtained by other routers on a network segment, you can use this command to disable the interface from receiving and sending OSPF packets.

Examples

```
# Disable an interface from receiving and sending OSPF packets.
```

```
<Sysname> system-view
```

```
[Sysname] ospf 100
```

```
[Sysname-ospf-100] silent-interface vlan-interface 10
```

snmp-agent trap enable ospf

Syntax

```
snmp-agent trap enable ospf [ process-id ] [ ifauthfail | ifcfgerror | ifrxbadpkt | ifstatechange | iftxretransmit | lsdbapproachoverflow | lsdboverflow | maxagelsa | nbrstatechange | originatelsa | vifcfgerror | virifauthfail | virifrxbadpkt | virifstatechange | viriftxretransmit | virnbrstatechange ] *
```

```
undo snmp-agent trap enable ospf [ process-id ] [ ifauthfail | ifcfgerror | ifrxbadpkt | ifstatechange | iftxretransmit | lsdbapproachoverflow | lsdboverflow | maxagelsa | nbrstatechange | originatelsa | vifcfgerror | virifauthfail | virifrxbadpkt | virifstatechange | viriftxretransmit | virnbrstatechange ] *
```

View

System view

Default level

3: Manage level

Parameters

process-id: OSPF process ID, in the range of 1 to 65535.

ifauthfail: Interface authentication failure information.

ifcfgerror: Interface configuration error information.

ifrxbadpkt: Information about error packets received.

ifstatechange: Interface state change information.

iftxretransmit: Packet receiving and forwarding information.

lsdbapproachoverflow: Information about cases approaching LSDB overflow.

lsdboverflow: LSDB overflow information.

maxagelsa: LSA max age information.

nbrstatechange: Neighbor state change information.
originatelsa: Information about LSAs originated locally.
vifauthfail: Virtual interface authentication failure information.
vifcfgerror: Virtual interface configuration error information.
virifauthfail: Virtual interface authentication failure information.
virifrxbadpkt: Information about error packets received by virtual interfaces.
virifstatechange: Virtual interface state change information.
virifxretransmit: Virtual interface packet retransmission information.
virnbrstatechange: Virtual interface neighbor state change information.

Description

Use **snmp-agent trap enable ospf** to enable the sending of SNMP traps for a specified OSPF process. If no process is specified, the feature is enabled for all processes.

Use **undo snmp-agent trap enable ospf** to disable the feature.

By default, this feature is enabled.

See *Network Management and Monitoring Command Reference* for related information.

Examples

```
# Enable the sending of SNMP traps for OSPF process 1.  
<Sysname> system-view  
[Sysname] snmp-agent trap enable ospf 1
```

spf-schedule-interval

Syntax

spf-schedule-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo spf-schedule-interval

View

OSPF view

Default level

2: System level

Parameters

maximum-interval: Maximum OSPF route calculation interval in seconds, in the range of 1 to 60.

minimum-interval: Minimum OSPF route calculation interval in milliseconds, in the range of 10 to 60000, which defaults to 0.

incremental-interval: Incremental value in milliseconds, in the range of 10 to 60000, which defaults to 5000.

Description

Use **spf-schedule-interval** to set the OSPF SPF calculation interval.

Use **undo spf-schedule-interval** to restore the default.

The interval defaults to 5 seconds.

Based on its LSDB, an OSPF router calculates the shortest path tree with itself being the root, and uses it to determine the next hop to a destination. Through adjusting the SPF calculation interval, you can protect bandwidth and router resources from being over-consumed due to frequent network changes.

With this command configured, when network changes are not frequent, SPF calculation applies at the *minimum-interval*. If network changes become frequent, the SPF calculation interval is incremented by the *incremental-interval* each time a calculation happens, up to the *maximum-interval*.

Examples

```
# Configure the SPF calculation maximum interval as 10 seconds, minimum interval as 500 milliseconds and incremental interval as 200 milliseconds.
```

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] spf-schedule-interval 10 500 200
```

stub (OSPF area view)

Syntax

```
stub [ default-route-advertise-always | no-summary ] *
undo stub
```

View

OSPF area view

Default level

2: System level

Parameters

default-route-advertise-always: Usable only on a stub ABR. With this keyword configured, the ABR advertises a default route in a Type-3 LSA into the stub area regardless of whether **FULL**-state neighbors exist in the backbone area. Without this keyword, the ABR advertises a default route in a Type-3 LSA into the stub area only when at least one **FULL**-state neighbor exists in the backbone area.

no-summary: Usable only on a stub ABR. With this keyword configured, the ABR advertises only a default route in a Summary LSA into the stub area (such a stub area is a totally stub area).

Description

Use **stub** to configure an area as a stub area.

Use **undo stub** to remove the configuration.

No area is stub area by default.

To cancel the **default-route-advertise-always** or the **no-summary** configuration on the ABR, execute the **stub** command again to overwrite it.

To configure an area as a stub area, all routers attached to it must be configured with this command.

Related commands: **default-cost**.

Examples

```
# Configure Area 1 as a stub area.
```

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
```

```
[Sysname-ospf-100-area-0.0.0.1] stub
```

stub-router

Syntax

```
stub-router  
undo stub-router
```

View

OSPF view

Default level

2: System level

Parameters

None

Description

Use **stub-router** to configure the router as a stub router.

Use **undo stub-router** to restore the default.

By default, no router is configured as a stub router.

The router LSAs from the stub router may contain different link type values. A value of 3 means a link to the stub network, so the cost of the link remains unchanged. A value of 1, 2 or 4 means a point-to-point link, a link to a transit network or a virtual link; in such cases, a maximum cost value of 65535 is used. If other neighbors find the links to the stub router have such big costs, they will not send packets to the stub router as long as a route with a smaller cost exists.

Examples

```
# Configure the router as a stub router.  
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] stub-router
```

transmit-pacing

Syntax

```
transmit-pacing interval interval count count  
undo transmit-pacing
```

View

OSPF view

Default level

2: System level

Parameters

interval: Interval at which an interface sends LSU packets, in milliseconds. Its value is in the range of 10 to 1000. If the router has a number of OSPF interfaces, HP recommends increasing this interval to reduce the total numbers of LSU packets sent by the router every second.

count: Maximum number of LSU packets sent by an interface at each interval. It is in the range of 1 to 200. If the router has a number of OSPF interfaces, HP recommends decreasing this interval to reduce the total numbers of LSU packets sent by the router every second.

Description

Use **transmit-pacing** to configure the maximum number of LSU packets that can be sent every the specified interval.

Use **undo transmit-pacing** to restore the default.

By default, an OSPF interface sends up to three LSU packets every 20 milliseconds.

Examples

Configure all the interfaces under OSPF process 1 to send up to 10 LSU packets every 30 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] transmit-pacing interval 30 count 10
```

vlink-peer (OSPF area view)

Syntax

vlink-peer *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **simple** [**cipher** | **plain**] *password* | { **md5** | **hmac-md5** } *key-id* [**cipher** | **plain**] *password*] *

undo vlink-peer *router-id* [**hello** | **retransmit** | **trans-delay** | **dead** | [**simple** | { **md5** | **hmac-md5** } *key-id*]] *

View

OSPF area view

Default level

2: System level

Parameters

router-id: Router ID of the neighbor on the virtual link.

hello *seconds*: Hello interval in seconds, in the range of 1 to 8192. The default is 10. It must be identical to the hello interval on the virtual link neighbor.

retransmit *seconds*: Retransmission interval in seconds, in the range of 1 to 3600. The default is 5.

trans-delay *seconds*: Transmission delay interval in seconds, in the range of 1 to 3600. The default is 1.

dead *seconds*: Dead interval in seconds, in the range of 1 to 32768. The default is 40. It must be identical to that on the virtual link neighbor. The dead interval is at least four times the hello interval.

md5: MD5 authentication.

hmac-md5: HMAC-MD5 authentication.

simple: Simple authentication.

key-id: Key ID for MD5 or HMAC-MD5 authentication, in the range of 1 to 255.

cipher: Sets a ciphertext password.

plain: Sets a plaintext password.

password: Sets the authentication password. This argument is case sensitive. For simple authentication mode, it is a plaintext string of 1 to 8 characters, or a ciphertext string of 1 to 41 characters. For MD5/HMAC-MD5 authentication mode, it is a plaintext string of 1 to 16 characters, or a ciphertext string of 1 to 53 characters.

Description

Use **vlink-peer** to configure a virtual link.

Use **undo vlink-peer** to remove a virtual link.

As defined in RFC 2328, all non-backbone areas must maintain connectivity to the backbone. You can use the **vlink-peer** command to configure a virtual link to connect an area to the backbone.

Considerations on parameters:

- The smaller the hello interval is, the faster the network converges and the more network resources are consumed.
- A so small retransmission interval will lead to unnecessary retransmissions. A big value is appropriate for a low speed link.
- You need to specify an appropriate transmission delay with the **trans-delay** keyword.

The authentication mode at the non-backbone virtual link end follows the one at the backbone virtual link end. The two authentication modes (MD5 or Simple) are independent, and you can specify neither of them.

The authentication password, set in either text or cipher text, is saved to the configuration file in cipher text.

If neither **cipher** nor **plain** is specified, **cipher** applies to the MD5/HMAC-MD5 authentication mode and **plain** applies to the simple authentication mode, by default.

Related commands: **authentication-mode** and **display ospf**.

Examples

```
# Configure a virtual link to the neighbor with router ID 1.1.1.1.  
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] area 2  
[Sysname-ospf-100-area-0.0.0.2] vlink-peer 1.1.1.1
```

IS-IS configuration commands

The term "router" in this chapter refers to both routers and Layer 3 switches.

The A5500 SI Switch Series does not support IS-IS.

area-authentication-mode

Syntax

```
area-authentication-mode { md5 | simple } [ cipher ] password [ ip | osi ]  
undo area-authentication-mode
```

View

IS-IS view

Default level

2: System level

Parameters

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Sets a ciphertext password. If this keyword is not specified, you set a plaintext password.

password: Sets the password. This argument is case sensitive. It must be a plaintext string of 1 to 16 characters, or a ciphertext string of 33 to 53 characters.

ip: Checks IP related fields in LSPs.

osi: Checks OSI related fields in LSPs.

NOTE:

Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Description

Use **area-authentication-mode** to specify the area authentication mode and a password.

Use **undo area-authentication-mode** to restore the default.

No area authentication is configured by default.

The password in the specified mode is inserted into all outgoing Level-1 packets (LSP, CSNP, and PSNP) and is used for authenticating the incoming Level-1 packets.

With area authentication configured, IS-IS discards incoming routes from untrusted routers.

Routers in a common area must have the same authentication mode and password.

If neither **ip** nor **osi** is specified, OSI related fields are checked.

The authentication password, set in either plain text or cipher text, is saved to the configuration file in cipher text.

Related commands: **reset isis all**, **domain-authentication-mode**, **isis authentication-mode**

Examples

```
# Configure the area authentication mode as simple, and set the plaintext password to ivg.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] area-authentication-mode simple ivg
```

auto-cost enable

Syntax

auto-cost enable

undo auto-cost enable

View

IS-IS view

Default level

2: System level

Parameters

None

Description

Use **auto-cost enable** to enable automatic link cost calculation.

Use **undo auto-cost enable** to disable the function.

This function is disabled by default.

After automatic link cost calculation is enabled, the link cost is automatically calculated based on the bandwidth reference value of an interface. When the cost-style is wide or wide-compatible, the cost value of an interface is calculated by using the formula: Cost = (reference bandwidth value/link bandwidth) × 10, which is in the range of 1 to 16777214. For other cost styles, [Table 28](#) applies.

Table 28 Automatic cost calculation scheme for cost styles other than wide and wide-compatible

Interface bandwidth	Cost
≤10 Mbps	60
≤100 Mbps	50
≤155 Mbps	40
≤622 Mbps	30
≤2500 Mbps	20
>2500 Mbps	10

Related commands: **bandwidth-reference** and **cost-style**.

Examples

```
# Enable automatic link cost calculation.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] auto-cost enable
```


bandwidth-reference (IS-IS view)

Syntax

```
bandwidth-reference value  
undo bandwidth-reference
```

View

IS-IS view

Default level

2: System level

Parameters

value: Bandwidth reference value in Mbps, ranging from 1 to 2147483648.

Description

Use **bandwidth-reference** to set the bandwidth reference value for automatic link cost calculation.

Use **undo bandwidth-reference** to restore the default.

By default, the bandwidth reference value is 100 Mbps.

Related commands: **auto-cost enable**.

Examples

```
# Configure the bandwidth reference of IS-IS process 1 as 200 Mbps.
```

```
<Sysname> system-view  
[Sysname] isis 1  
[Sysname-isis-1] bandwidth-reference 200
```

circuit-cost

Syntax

```
circuit-cost value [ level-1 | level-2 ]  
undo circuit-cost [ level-1 | level-2 ]
```

View

IS-IS view

Default level

2: System level

Parameters

value: Link cost value. The value range varies with cost styles.

- For styles **narrow**, **narrow-compatible** and **compatible**, the cost value ranges from 0 to 63.
- For styles **wide** and **wide-compatible**, the cost value ranges from 0 to 16777215. When the cost value is 16777215, the neighbor TLV generated on the link is used only to carry relevant information about TE.

level-1: Applies the link cost to Level-1.

level-2: Applies the link cost to Level-2.

Description

Use **circuit-cost** to set a global IS-IS link cost.

Use **undo circuit-cost** to restore the default.

By default, no global link cost is configured.

If no level is specified, the specified cost applies to both Level-1 and Level-2.

Related commands: **isis cost** and **cost-style**.

Examples

```
# Set the global Level-1 link cost of IS-IS process 1 to 11.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] circuit-cost 11 level-1
```

cost-style

Syntax

```
cost-style { narrow | wide | wide-compatible | { compatible | narrow-compatible } [ relax-spf-limit ] }  
undo cost-style
```

View

IS-IS view

Default level

2: System level

Parameters

narrow: Receives and sends only narrow cost style packets (The narrow cost ranges from 0 to 63).

wide: Receives and sends only wide cost style packets (The wide cost ranges from 0 to 16777215).

compatible: Receives and sends both wide and narrow cost style packets.

narrow-compatible: Receives both narrow and wide cost style packets, but sends only narrow cost style packets.

wide-compatible: Receives both narrow and wide cost style packets, but sends only wide cost style packets.

relax-spf-limit: Allows receiving routes with a cost greater than 1023. If this keyword is not specified, any route with a cost bigger than 1023 will be discarded. This keyword is only available when **compatible** or **narrow-compatible** is included.

Description

Use **cost-style** to set a cost style.

Use **undo cost-style** to restore the default.

Only narrow cost style packets can be received and sent by default.

Related commands: **isis cost** and **circuit-cost**.

Examples

Configure the router to send only narrow cost style packets, but receive both narrow and wide cost style packets.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] cost-style narrow-compatible
```

default-route-advertise (IS-IS view)

Syntax

```
default-route-advertise [ route-policy route-policy-name | [ level-1 | level-1-2 | level-2 ] ] *
undo default-route-advertise [ route-policy route-policy-name ]
```

View

IS-IS view

Default level

2: System level

Parameters

route-policy-name: Specifies the name of a routing policy, a case-sensitive string of 1 to 63 characters.

level-1: Advertises a Level-1 default route.

level-1-2: Advertises both Level-1 and Level-2 default routes.

level-2: Advertises a Level-2 default route.

Description

Use **default-route-advertise** to advertise a default route of 0.0.0.0/0.

Use **undo default-route-advertise** to disable default route advertisement.

Default route advertisement is disabled by default.

If no level is specified, a Level-2 default route is advertised.

The Level-1 default route is advertised to other routers in the same area, and the Level-2 default route is advertised to all the Level-2 and Level-1-2 routers.

Using the **apply isis level-1** command in routing policy view will generate a default route in a Level-1 LSP.

Using the **apply isis level-2** command in routing policy view will generate a default route in a Level-2 LSP.

Using the **apply isis level-1-2** command in routing policy view will generate a default route in a Level-1 LSP and Level-2 LSP respectively.

Examples

Advertise a Level-2 default route.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] default-route-advertise
```

display isis brief

Syntax

```
display isis brief [ process-id | vpn-instance vpn-instance-name ] [ | { begin | exclude | include }  
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: Displays IS-IS brief configuration information for the IS-IS process. The process ID is in the range of 1 to 65535.

vpn-instance vpn-instance-name: Displays IS-IS brief configuration information for the MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the IS-IS brief configuration information of the public network is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display isis brief** to view IS-IS brief configuration information.

Examples

```
# Display IS-IS brief configuration information.
```

```
<Sysname> display isis brief
```

```
ISIS (1) Protocol Brief Information :  
  
network-entity:  
  10.0000.0000.0001.00  
is-level :level-1-2  
cost-style: narrow  
preference : 15  
Lsp-length receive : 1497  
Lsp-length originate : level-1 1497  
                      level-2 1497  
maximum imported routes number : 10000  
Timers:  
  lsp-max-age: 1200  
  lsp-refresh: 900  
Interval between SPF: 10
```

Table 29 Command output

Field	Description
network-entity	Network entity name
is-level	IS-IS Routing level
cost-style	Cost style
preference	Preference
Lsp-length receive	Maximum LSP that can be received
Lsp-length originate	Maximum LSP that can be generated
maximum imported routes number	Maximum number of redistributed Level-1/Level-2 IPv4 routes
Timers	<ul style="list-style-type: none"> • lsp-max-age—Maximum life period of LSP • lsp-refresh—Refresh interval of LSP • Interval between SPFs—Interval between SPF calculations

display isis debug-switches

Syntax

```
display isis debug-switches { process-id | vpn-instance vpn-instance-name } [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: Displays the IS-IS debugging switch state for the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Displays the IS-IS debugging switch state for the MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the IS-IS debugging switch state for the public network is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display isis debug-switches** to display IS-IS debugging switch state.

Examples

```
# Display the debugging switch state of IS-IS process 1.
<Sysname> display isis debug-switches 1
IS-IS - Debug settings.
        IS-IS SPF Triggering Events debugging is on
```

display isis graceful-restart status

Syntax

```
display isis graceful-restart status [ level-1 | level-2 ] [ process-id | vpn-instance vpn-instance-name ] [ |
{ begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

level-1: Displays the IS-IS Level-1 Graceful Restart state.

level-2: Displays the IS-IS Level-2 Graceful Restart state.

process-id: IS-IS Process ID, in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the IS-IS Graceful Restart status for the public network is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display isis graceful-restart status** to display IS-IS Graceful Restart status.

Examples

```
# Display IS-IS Graceful Restart status.
<Sysname> display isis graceful-restart status
        Restart information for IS-IS(1)
-----
IS-IS(1) Level-1 Restart Status
Restart Interval: 150
SA Bit Supported
  Total Number of Interfaces = 1
  Restart Status: RESTARTING
  Number of LSPs Awaited: 3
  T3 Timer Status:
```

```

    Remaining Time: 140
T2 Timer Status:
    Remaining Time: 59

IS-IS(1) Level-2 Restart Status
Restart Interval: 150
SA Bit Supported
    Total Number of Interfaces = 1
    Restart Status: RESTARTING
    Number of LSPs Awaited: 3
    T3 Timer Status:
        Remaining Time: 140
    T2 Timer Status:
        Remaining Time: 59

```

Table 30 Command output

Field	Description
Restart Interval	Graceful Restart interval.
SA Bit Supported	The SA bit is set.
Total Number of Interfaces = 1	The current IS-IS interface number.
Restart Status	Graceful Restart status.
Number of LSPs Awaited	Number of LSPs not obtained by the GR restarter from GR helpers during LSDB synchronization.
T3 Timer Status	Remaining time of T3 timer.
T2 Timer Status	Remaining time of T2 Timer.

display isis interface

Syntax

```

display isis interface [ statistics ] [ interface-type interface-number ] [ verbose ] ] [ process-id |
vpn-instance vpn-instance-name ] [ | { begin | exclude | include } regular-expression ]

```

View

Any view

Default level

1: Monitor level

Parameters

statistics: Displays IS-IS interface statistics.

interface-type interface-number: Specifies an interface by its type and number.

verbose: Displays detailed IS-IS interface information.

process-id: Displays the IS-IS interface information of the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Displays the IS-IS interface information of the MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the IS-IS interface information of the public network is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display isis interface** to display IS-IS interface information.

Examples

Display brief IS-IS interface information.

```
<Sysname> display isis interface
                        Interface information for ISIS(1)
                        -----
Interface: Vlan-interface11
Id      IPV4.State      IPV6.State      MTU      Type      DIS
001     Up                Down            1497     L1/L2     No/No
```

Display detailed IS-IS interface information.

```
<Sysname> display isis interface verbose
                        Interface information for ISIS(1)
                        -----
Interface: Vlan-interface999
Id      IPV4.State      IPV6.State      MTU      Type      DIS
001     Up                Down            1497     L1/L2     No/No
SNPA Address      : 000f-e237-c6e0
IP Address        : 192.168.1.48
Secondary IP Address(es) :
IPV6 Link Local Address :
IPV6 Global Address(es) :
Csnp Timer Value : L1 10 L2 10
Hello Timer Value : L1 10 L2 10
Hello Multiplier Value : L1 3 L2 3
Lsp Timer Value   : L12 33
Lsp Transmit-Throttle Count : L12 5
Cost              : L1 10 L2 10
Priority          : L1 64 L2 64
BFD              : Disabled
MPLS TE Status   : ON
INTF L1 TE Status : OFF
INTF L2 TE Status : ON
TE Cost          : 0
```



```

TE Admin Group          : 0
TE Max Bandwidth        : 0
TE Max Res Bandwidth    : 0

```

Displays detailed information of the specified IS-IS interface.

```
<Sysname> display isis interface tunnel 1 verbose
```

```

                                Interface information for ISIS(1)
                                -----

Interface: Tunnell
Id      IPv4.State      IPv6.State      MTU  Type  DIS
005     Up              Down            16384 L1/L2 --
SNPA Address      : 0000-0000-0000
IP Address        : 10.1.1.4
Secondary IP Address(es) :
IPv6 Link Local Address :
IPv6 Global Address(es) :
Csnp Timer Value  : L1   10  L2   10
Hello Timer Value :      10
Hello Multiplier Value :      3
Lsp Timer Value   : L12  33
Lsp Transmit-Throttle Count : L12  5
Cost              : L1   10  L2   10
Priority           : L1   64  L2   64
Retransmit Timer Value : L12  5
BFD               : Disabled
Tunnel L1 State   : OFF
Tunnel L2 State   : ON
Tunnel Type       : AA
Tunnel Metric     : 0
Destination Router ID : 5.5.5.5

```

Table 31 Command output

Field	Description
Interface	Interface type and number
Id	Circuit ID
IPV4.State	IPv4 state
IPV6.State	IPv6 state
MTU	Interface MTU
Type	Interface link adjacency type
DIS	Whether the interface is elected as the DIS or not
SNPA Address	Subnet access point address
IP Address	Primary IP address
Secondary IP Address(es)	Secondary IP addresses

Field	Description
IPv6 Link Local Address	IPv6 link local address
IPv6 Global Address(es)	IPv6 global address
Csnp Timer Value	Interval for sending CSNP packets
Hello Timer Value	Interval for sending Hello packets
Hello Multiplier Value	Number of invalid Hello packets
Lsp Timer Value	Minimum interval for sending LSP packets
Lsp Transmit-Throttle Count	Number of LSP packets sent each time
Cost	Cost of the interface
Priority	DIS priority
Retransmit Timer Value	LSP retransmission interval over the point-to-point link
BFD	Whether BFD is enabled on the interface
MPLS TE Status	Whether MPLS TE is enabled on the interface
INTF L1 TE Status	Whether level-1 MPLS TE is enabled on the interface
INTF L2 TE Status	Whether level-2 MPLS TE is enabled on the interface
TE Cost	MPLS TE cost configured on the interface
TE Admin Group	TE link administration group
TE Max Bandwidth	TE link maximum bandwidth
TE Max Res Bandwidth	TE link maximum reserved bandwidth
Tunnel L1 State	IS-IS TE tunnel level-1 state
Tunnel L2 State	IS-IS TE tunnel level-2 state
Tunnel Type	Tunnel type
Tunnel Metric	IGP metric of the TE tunnel
Destination Router ID	Destination address of TE tunnel interface

Display IS-IS interface statistics.

```
<sysname> display isis interface statistics
          Interface Statistics information for ISIS(1)
          -----
          Type          IPv4 Up/Down          IPv6 Up/Down
          LAN            0/1                    -/-
          P2P            4/0                    -/-
```

Table 32 Command output

Field	Description
Type	Network type of the interface: <ul style="list-style-type: none"> • LAN for broadcast network. • P2P for point-to-point network.
IPv4 UP	Number of IS-IS interfaces in up state.
IPv4 DOWN	Number of IS-IS interfaces in down state.

Field	Description
IPv6 UP	Number of IS-ISv6 interfaces in up state. If IPv6 is not enabled, this field displays a hyphen (-).
IPv6 DOWN	Number of IS-ISv6 interfaces in down state. If IPv6 is not enabled, this field displays a hyphen (-).

display isis lsdb

Syntax

```
display isis lsdb [ [ I1 | I2 | level-1 | level-2 ] | [ lsp-id lspid | lsp-name lspname ] | local | verbose ]
* [ process-id | vpn-instance vpn-instance-name ] [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

I1, level-1: Displays the level-1 LSDB.

I2, level-2: Displays the level-2 LSDB.

lspid: LSP ID, in the form of *sysID.Pseudo ID-fragment num*, where *sysID* represents the originating node or pseudo node, and *Pseudo ID* is separated by a dot from *sysID* and by a hyphen from *fragment num*.

lspname: LSP name, in the form of *Symbolic name.Pseudo ID-fragment num*, where the *Pseudo ID* is separated by a dot from *Symbolic name* and by a hyphen from *fragment num*. If the *Pseudo ID* is 0, specify the LSP name in the form *Symbolic name-fragment num*.

local: Displays LSP information generated locally.

verbose: Displays LSDB detailed information.

process-id: Displays the LSDB of the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Displays the LSDB of the MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the LSDB of the public network is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display isis lsdb** to display IS-IS link state database.

If no level is specified, both Level-1 and Level-2 link state databases are displayed.

Examples

Display brief Level-1 LSDB information.

```
<Sysname> display isis lsdb level-1
```

```
                        Level-1 Link State Database
LSPID                Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-----
1000.0000.0001.00-00* 0x00000016  0x314e        557           112    0/0/0
1000.0000.0001.00-01* 0x0000000b  0xbd7         0 (616)       27     0/0/0
1000.0000.0001.00-02* 0x0000000f  0x68aa        557           67     0/0/0
1000.0000.0002.00-00  0x00000009  0x20ba        945           110    0/0/0
1000.0000.0002.00-01  0x00000006  0x9f1c        945           67     0/0/0
1000.0000.0002.01-00  0x00000004  0x1b9c        945           55     0/0/0
    *-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
```

Display detailed Level-1 LSDB information.

```
<Sysname> display isis lsdb level-1 verbose
```

```
                        Database information for ISIS(1)
                        -----
                        Level-1 Link State Database
LSPID                Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-----
1000.0000.0001.00-00* 0x00000016  0x314e        1130          112    0/0/0
SOURCE              1000.0000.0001.00
NLPID               IPV4
NLPID               IPV6
AREA ADDR           10
INTF ADDR           3.1.1.20
INTF ADDR V6        3::20
+NBR ID
    1000.0000.0002.01          COST: 63
1000.0000.0001.00-01* 0x0000000b  0xbd7         0 (1188)     27     0/0/0
1000.0000.0001.00-02* 0x0000000f  0x68aa        1129         67     0/0/0
SOURCE              1000.0000.0001.00
IP-Internal
    3.1.1.0          255.255.255.0  COST: 63
IPV6
    3::/64          COST: 63
1000.0000.0002.00-00  0x00000008  0x22b9        884          110    0/0/0
SOURCE              1000.0000.0002.00
NLPID               IPV4
NLPID               IPV6
AREA ADDR           10
INTF ADDR           3.1.1.21
INTF ADDR V6        3::21
+NBR ID
    1000.0000.0002.01          COST: 10
1000.0000.0002.00-01  0x00000005  0xa11b        878          67     0/0/0
SOURCE              1000.0000.0002.00
IP-Internal
```

```

3.1.1.0          255.255.255.0   COST: 10
IPV6
3::/64          COST: 10
1000.0000.0002.01-00  0x00000003  0x1d9b      878      55      0/0/0
SOURCE          1000.0000.0002.01
NLPID          IPV4
NLPID          IPV6
+NBR ID
1000.0000.0002.00          COST: 0
+NBR ID
1000.0000.0001.00          COST: 0
*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

```

Table 33 Command output

Field	Description
LSPID	Link state packet ID.
Seq Num	LSP sequence number.
Checksum	LSP checksum.
Holdtime	LSP lifetime which decreases as time elapses.
Length	LSP length.
ATT/P/OL	<ul style="list-style-type: none"> • ATT—Attach bit. • P—Partition bit. • OL—Overload bit. <p>1 means the bit is set and 0 means the bit is not set.</p>
SOURCE	System ID of the originating router.
NLPID	Network layer protocol the originating router runs.
AREA ADDR	Area address of the originating router.
INTF ADDR	IP address of the originating router's IS-IS interface.
INTF ADDR V6	IPv6 address of the originating router's IS-ISv6 interface .
NBR ID	Neighbor ID of the originating router.
IP-Internal	Internal IP address and mask of the originating router.
IP-External	External IP address and mask of the originating router.
IP-Extended	Extended IP address and mask of the originating router.
COST	Cost.
HOST NAME	Dynamic host name of the originating router.
ORG ID	Original system ID of the virtual system ID of the originating router.
Auth	Authentication information of the originating router.
IPV6	Internal IPv6 address and prefix of the originating router.
IPV6-Ext	External IPv6 address and prefix of the originating router.

display isis name-table

Syntax

```
display isis name-table [ process-id | vpn-instance vpn-instance-name ] [ | { begin | exclude | include }  
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: Displays the host name-to-system ID mapping table for the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance vpn-instance-name: Displays the host name-to-system ID mapping table for the MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the host name-to-system ID mapping table for the public network is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display isis name-table** to display the host name-to-system ID mapping table.

Examples

```
# Configure a name for the local IS system.  
<Sysname> system-view  
[Sysname] isis 1  
[Sysname-isis-1] is-name RUTA  
  
# Configure a static mapping for the remote IS system (system ID 0000.0000.0041, host name RUTB).  
[Sysname-isis-1] is-name map 0000.0000.0041 RUTB  
  
# Display the IS-IS host name-to-system ID mapping table.  
[Sysname-isis-1] display isis name-table  
Name table information for ISIS(1)  
-----  
System ID           Hostname           Type  
6789.0000.0001      RUTA               DYNAMIC  
0000.0000.0041      RUTB               STATIC
```

Table 34 Command output

Field	Description
System ID	System ID

Field	Description
Hostname	Host name
Type	Mapping type (static or dynamic)

display isis peer

Syntax

```
display isis peer [ statistics | verbose ] [ process-id | vpn-instance vpn-instance-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

statistics: Displays IS-IS neighbor statistics.

verbose: Displays detailed IS-IS neighbor information. Without the keyword, the command displays brief IS-IS neighbor information.

process-id: Displays the IS-IS neighbor information of the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Displays the IS-IS neighbor information of the MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the IS-IS neighbor information of the public network is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display isis peer** to display IS-IS neighbor information.

Examples

```
# Display brief IS-IS neighbor information.
```

```
<Sysname> display isis peer
```

```

Peer information for ISIS(1)
-----

System Id: 1111.1111.1111
Interface: Vlan-interface11          Circuit Id: 1111.1111.1112.01
State: Up      HoldTime: 23s      Type: L1(L1L2)      PRI: 64
```

```

System Id: 1111.1111.1111
Interface: Vlan-interface11          Circuit Id: 1111.1111.1112.01
State: Up      HoldTime: 23s        Type: L2(L1L2)      PRI: 64

```

Display detailed IS-IS neighbor information.

```
<Sysname> display isis peer verbose
```

```

Peer information for ISIS(1)
-----

System Id: 1111.1111.1111
Interface: Vlan-interface11          Circuit Id: 1111.1111.1112.01
State: Up      HoldTime: 27s        Type: L1(L1L2)      PRI: 64
Area Address(es):10
Peer IP Address(es): 3.1.1.2
Uptime: 00:38:15
Adj Protocol:  IPV4

System Id: 1111.1111.1111
Interface: Vlan-interface11          Circuit Id: 1111.1111.1112.01
State: Up      HoldTime: 28s        Type: L2(L1L2)      PRI: 64
Area Address(es):10
Peer IP Address(es): 3.1.1.2
Uptime: 00:38:15
Adj Protocol:  IPV4

```

Table 35 Command output

Field	Description
System Id	System ID of the neighbor.
Interface	Interface connecting to the neighbor.
Circuit Id	Circuit ID.
State	Circuit state.
HoldTime	Holdtime. Within the holdtime if no hellos are received from the neighbor, the neighbor is considered down. If a hello is received, the holdtime is reset to the initial value.
Type	Circuit type: <ul style="list-style-type: none"> • L1—Means the circuit type is Level-1 and the neighbor is a Level-1 router. • L2—Means the circuit type is Level-2 and the neighbor is a Level-2 router. • L1(L1L2)—Means the circuit type is Level-1 and the neighbor is a Level-1-2 router. • L2(L1L2)—Means the circuit type is Level-2 and the neighbor is a Level-1-2 router.
PRI	DIS priority of the neighbor.
Area Address(es)	The neighbor's area address.
Peer IP Address(es)	IP address of the neighbor.

Field	Description
Uptime	Time that elapsed since the neighbor relationship was formed.
Adj Protocol	Adjacency protocol.

Display IS-IS neighbor statistics.

```
<Sysname> display isis peer statistics
```

```

Peer Statistics information for ISIS(1)
-----
Type                IPv4 Up/Init          IPv6 Up/Init
LAN Level-1         0/0                   0/0
LAN Level-2         0/0                   0/0
P2P                 3/0                   0/0

```

Table 36 Command output

Field	Description
Type	Neighbor type: <ul style="list-style-type: none"> • LAN Level-1—Number of Level-1 neighbors whose network type is broadcast • LAN Level-2—Number of Level-2 neighbors whose network type is broadcast • P2P—Number of neighbors whose network type is P2P
IPv4 Up	Number of IPv4 neighbors in up state
IPv4 Init	Number of IPv4 neighbors in init state
IPv6 Up	Number of IPv6 neighbors in up state
IPv6 Init	Number of IPv6 neighbors in init state

display isis route

Syntax

```
display isis route [ ipv4 ] [ [ level-1 | level-2 ] | verbose ] * [ process-id | vpn-instance vpn-instance-name ] [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv4: Displays IS-IS IPv4 routing information (the default).

verbose: Displays detailed IS-IS IPv4 routing information.

process-id: Displays the IS-IS IPv4 routing information of the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Displays the IS-IS IPv4 routing information of the MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the IS-IS IPv4 routing information of the public network is displayed.

level-1: Displays Level-1 IS-IS routes.

level-2: Displays Level-2 IS-IS routes.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display isis route** to display IS-IS IPv4 routing information.

If no level is specified, both Level-1 and Level-2 routing information will be displayed.

Examples

Display IS-IS IPv4 routing information.

```
<Sysname> display isis route 1
```

```
Route information for ISIS(1)
-----

ISIS(1) IPv4 Level-1 Forwarding Table
-----

IPv4 Destination      IntCost    ExtCost  ExitInterface  NextHop      Flags
-----
1.1.0.0/16            20         NULL     Vlan11         1.2.1.1      R/L/-
1.2.0.0/16            10         NULL     Vlan11         Direct       D/L/-
```

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

```
ISIS(1) IPv4 Level-2 Forwarding Table
-----

IPv4 Destination      IntCost    ExtCost  ExitInterface  NextHop      Flags
-----
1.1.0.0/16            20         NULL
1.2.0.0/16            10         NULL     Vlan11         Direct       D/L/-
```

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

Table 37 Command output

Field	Description
Route information for ISIS(1)	Route information for IS-IS process 1.
ISIS(1) IPv4 Level-1 Forwarding Table	IS-IS IPv4 routing information for Level-1.

Field	Description
ISIS(1) IPv4 Level-2 Forwarding Table	IS-IS IPv4 routing information for Level-2.
IPv4 Destination	IPv4 destination address.
IntCost	Interior routing cost.
ExtCost	Exterior routing cost.
ExitInterface	Exit interface.
NextHop	Next hop.
Flags	Routing state flag: <ul style="list-style-type: none"> • D—Direct route. • R—The route has been added into the routing table. • L—The route has been advertised in an LSP. • U—A route's penetration flag. Setting it to UP can prevent an LSP sent from L2 to L1 from being sent back to L2.

Display detailed IS-IS IPv4 routing information.

```
<Sysname> display isis route verbose
```

```
Route information for ISIS(1)
```

```
-----
ISIS(1) IPv4 Level-1 Forwarding Table
-----
```

```

IPv4 Dest  : 1.1.0.0/16      Int. Cost : 20              Ext. Cost : NULL
Admin Tag  : -              Src Count : 2              Flag      : R/L/-
NextHop    :                Interface  :                ExitIndex :
    1.2.1.1                  Vlan11      0x00000008

IPv4 Dest  : 1.2.0.0/16      Int. Cost : 10              Ext. Cost : NULL
Admin Tag  : -              Src Count : 2              Flag      : D/L/-
NextHop    :                Interface  :                ExitIndex :
    Direct                   Vlan11      0x00000000
```

```
Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

```
-----
ISIS(1) IPv4 Level-2 Forwarding Table
-----
```

```

IPv4 Dest  : 1.1.0.0/16      Int. Cost : 20              Ext. Cost : NULL
Admin Tag  : -              Src Count : 2              Flag      : -/-/-
NextHop    :                Interface  :                ExitIndex :

IPv4 Dest  : 1.2.0.0/16      Int. Cost : 10              Ext. Cost : NULL
Admin Tag  : -              Src Count : 3              Flag      : D/L/-
NextHop    :                Interface  :                ExitIndex :
```

Direct

Vlan11

0x00000000

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

Table 38 Command output

Field	Description
Route information for ISIS(1)	Route information for IS-IS process 1.
ISIS(1) IPv4 Level-1 Forwarding Table	IS-IS IPv4 routing information for Level-1.
ISIS(1) IPv4 Level-2 Forwarding Table	IS-IS IPv4 routing information for Level-2.
IPv4 Dest	IPv4 destination.
Int. Cost	Internal route cost.
Ext. Cost	External route cost.
Admin Tag	Tag.
Src Count	Count of advertising sources
Flag	Route state flag: <ul style="list-style-type: none"> • R—Indicates the route have been installed into the routing table. • L—The route has been flooded in an LSP. • U—Route leaking flag. If it is UP, routes from L2 to L1 cannot be advertised back to L2.
Next Hop	Next hop.
Interface	Outgoing interface.
ExitIndex	Index of the outgoing interface.

display isis spf-log

Syntax

display isis spf-log [*process-id* | **vpn-instance** *vpn-instance-name*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

process-id: Displays IS-IS SPF log information for the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Displays IS-IS SPF log information for the MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the IS-IS SPF log information for the public network is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display isis spf-log** to display IS-IS SPF log information.

Examples

Display IS-IS SPF log information.

```
<Sysname> display isis spf-log
          SPF Log information for ISIS(1)
          -----
          Level      Trig.Event                No.Nodes  Duration  StartTime
          L2         IS_SPFTRIG_PERIODIC      2         0         13:3:24
          L1         IS_SPFTRIG_PERIODIC      2         0         13:18:8
          L2         IS_SPFTRIG_PERIODIC      2         0         13:18:8
          L1         IS_SPFTRIG_PERIODIC      2         0         13:32:28
          L2         IS_SPFTRIG_PERIODIC      2         0         13:32:28
          L1         IS_SPFTRIG_PERIODIC      2         0         13:44:0
          L2         IS_SPFTRIG_PERIODIC      2         0         13:44:0
          L1         IS_SPFTRIG_PERIODIC      2         0         13:55:43
          -->L2      IS_SPFTRIG_PERIODIC      2         0         13:55:43
          L1         IS_SPFTRIG_PERIODIC      2         0         11:54:12
          L2         IS_SPFTRIG_PERIODIC      2         0         11:54:12
          L1         IS_SPFTRIG_PERIODIC      2         0         12:7:24
          L2         IS_SPFTRIG_PERIODIC      2         0         12:7:24
          L1         IS_SPFTRIG_PERIODIC      2         0         12:21:24
          L2         IS_SPFTRIG_PERIODIC      2         0         12:21:24
          L1         IS_SPFTRIG_PERIODIC      2         0         12:35:24
          L2         IS_SPFTRIG_PERIODIC      2         0         12:35:24
          L1         IS_SPFTRIG_PERIODIC      2         0         12:49:24
          L2         IS_SPFTRIG_PERIODIC      2         0         12:49:24
          L1         IS_SPFTRIG_PERIODIC      2         0         13:3:24
```

Table 39 Command output

Field	Description
SPF Log information for ISIS(1)	SPF log information for IS-IS process 1
Level	SPF calculation level
Trig.Event	SPF triggered event
No.Nodes	Number of SPF calculation nodes
Duration	SPF calculation duration
StartTime	SPF calculation start time

display isis statistics

Syntax

```
display isis statistics [ level-1 | level-1-2 | level-2 ] [ process-id | vpn-instance vpn-instance-name ] [ |  
{ begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

level-1: Displays IS-IS Level-1 statistics.

level-1-2: Displays IS-IS Level-1-2 statistics.

level-2: Displays IS-IS Level-2 statistics.

process-id: Displays IS-IS statistics for the IS-IS process. The ID is in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Displays IS-IS statistics for the MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the IS-IS statistics for the public network is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display isis statistics** to display IS-IS statistics.

Examples

```
# Display IS-IS statistics.
```

```
<Sysname> display isis statistics  
Statistics information for ISIS(1)  
-----  
Level-1 Statistics  
-----  
  
MTR(Basic-V4):  
-----  
Learnt routes information:  
Total IPv4 Learnt Routes in IPv4 Routing Table: 0  
Total IPv6 Learnt Routes in IPv6 Routing Table: 0  
  
Imported routes information:  
IPv4 Imported Routes:
```

```

                Static: 0      Direct: 0
                ISIS:   0      BGP:   0
                RIP:    0      OSPF:  0
                Total Number: 0
IPv6 Imported Routes:
                Static: 0      Direct: 0
                ISISv6: 0      BGP4+: 0
                RIPng:  0      OSPFv3: 0
                Total Number: 0

Lsp information:
                LSP Source ID:      No. of used LSPs
                0000.0000.0001      002

```

Level-2 Statistics

MTR(Basic-V4):

Learnt routes information:

Total IPv4 Learnt Routes in IPv4 Routing Table: 0

Total IPv6 Learnt Routes in IPv6 Routing Table: 0

Imported routes information:

IPv4 Imported Routes:

Static: 0 Direct: 0

ISIS: 0 BGP: 0

RIP: 0 OSPF: 0

Total Number: 0

IPv6 Imported Routes:

Static: 0 Direct: 0

ISISv6: 0 BGP4+: 0

RIPng: 0 OSPFv3: 0

Total Number: 0

Lsp information:

LSP Source ID: No. of used LSPs

0000.0000.0001 002

Table 40 Command output

Field	Description
Statistics information for ISIS(<i>processid</i>)	Statistics for the IS-IS process
Level-1 Statistics	Level-1 Statistics
Level-2 Statistics	Level-2 Statistics

Field	Description
Learnt routes information	Number of learned IPv4 routes Number of learned IPv6 routes
MTR(Basic-V4) IPv4 Imported Routes	Redistributed IPv4 routes: <ul style="list-style-type: none"> • Static • Direct • IS-IS • BGP • RIP • OSPF
Imported routes information	Redistributed IPv6 routes: <ul style="list-style-type: none"> • Static • Direct • IS-ISv6 • BGP4+ • RIPng • OSPFv3
IPv6 Imported Routes	
Lsp information	LSP information: <ul style="list-style-type: none"> • LSP Source ID—ID of the source system • No. of used LSPs—Number of used LSPs

domain-authentication-mode

Syntax

```
domain-authentication-mode { md5 | simple } [ cipher ] password [ ip | osi ]
undo domain-authentication-mode
```

View

IS-IS view

Default level

2: System level

Parameters

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Sets a ciphertext password. If this keyword is not specified, you set a plaintext password.

password: Sets the password. This argument is case sensitive. It must be a plaintext string of 1 to 16 characters, or a ciphertext string of 33 to 53 characters.

ip: Checks IP related fields in LSPs.

osi: Checks OSI related fields in LSPs.

NOTE:

Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Description

Use **domain-authentication-mode** to specify the routing domain authentication mode and a password.

Use **undo domain-authentication-mode** to restore the default.

No routing domain authentication is configured by default

The configured password in the specified mode is inserted into all outgoing Level-2 packets (LSP, CSNP and PSNP) and is used for authenticating the incoming Level-2 packets.

All the backbone routers must have the same authentication mode and password.

If neither **ip** nor **osi** is specified, the OSI related fields in LSPs are checked.

Related commands: **area-authentication-mode** and **isis authentication-mode**.

Examples

```
# Specify the routing domain authentication mode as simple, and set the plaintext password to 123456.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] domain-authentication-mode simple 123456
```

fast-reroute

Syntax

```
fast-reroute { auto | route-policy route-policy-name }
undo fast-reroute
```

View

IS-IS view

Default level

2: System level

Parameters

auto: Calculates a backup next hop automatically for all routes.

route-policy *route-policy-name*: References a routing policy to designate a next hop. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters. You can specify the backup next hop in the routing policy.

Description

Use **fast-reroute** to configure IS-IS fast reroute (FRR).

Use **undo fast-reroute** to restore the default.

By default, IS-IS FRR is disabled.

! IMPORTANT:

- Do not use FRR and BFD at the same time. Otherwise, FRR may fail to take effect.
 - The automatic backup next hop calculation of FRR and that of TE are mutually exclusive.
-

Example

```
# Enable IS-IS FRR to automatically calculate a backup next hop for all routes.
<Sysname> system-view
```

```

[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] isis
[Sysname-isis-1] fast-reroute auto
# Enable IS-IS FRR to designate a backup next hop by using a referenced routing policy named frr.
<Sysname> system-view
[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] ip ip-prefix abc index 10 permit 100.1.1.0 24
[Sysname] route-policy frr permit node 10
[Sysname-route-policy] if-match ip-prefix abc
[Sysname-route-policy] apply fast-reroute backup-interface vlan-interface 1
backup-nexthop 193.1.1.8
[Sysname-route-policy] quit
[Sysname] isis 100
[Sysname-isis-100] fast-reroute route-policy frr

```

filter-policy export (IS-IS view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

View

IS-IS view

Default level

2: System level

Parameters

acl-number: Specifies the number of an ACL that is used to filter redistributed routes, ranging from 2000 to 3999. For ACL configuration information, see *ACL and QoS Command Reference*.

ip-prefix *ip-prefix-name*: Specifies the name of an IP prefix list that is used to filter redistributed routes, a case-sensitive string of 1 to 19 characters. For IP prefix list configuration information, see "[Routing policy configuration commands](#)."

route-policy *route-policy-name*: Specifies the name of a routing policy that is used to filter redistributed routes, a case-sensitive string of 1 to 63 characters. For routing policy configuration information, see "[Routing policy configuration commands](#)."

protocol: Filters routes redistributed from the routing protocol, which can be BGP, direct, IS-IS, OSPF, RIP or static.

process-id: Process ID, in the range of 1 to 65535. It is optional only when the protocol is IS-IS, OSPF or RIP.

Description

Use **filter-policy export** to configure IS-IS to filter redistributed routes.

Use **undo filter-policy export** to disable IS-IS from filtering redistributed routes.

IS-IS does not filter redistributed routes by default.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command or in the routing policy, the ACL should be configured with the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command to deny/permit a route with the specified destination, or with the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard destination dest-addr dest-wildcard* command to deny/permit a route with the specified destination and mask. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route (the subnet mask must be valid; otherwise, the configuration is ineffective).

Related commands: **filter-policy import**.

Examples

Reference ACL 2000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] isis 1
[Sysname-isis-1] filter-policy 2000 export
```

Configure ACL 3000 to permit only route 113.0.0.0/16 to pass, and reference ACL 3000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0
[Sysname-acl-adv-3000] rule 100 deny ip
[Sysname-acl-adv-3000] quit
[Sysname] isis 1
[Sysname-isis 1] filter-policy 3000 export
```

filter-policy import (IS-IS view)

Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name | route-policy route-policy-name } import  
undo filter-policy import
```

View

IS-IS view

Default level

2: System level

Parameters

acl-number: Specifies the number of an ACL that is used to filter routes calculated from received LSPs, ranging from 2000 to 3999. For ACL configuration information, see *ACL and QoS Command Reference*.

ip-prefix ip-prefix-name: Specifies the name of an IP prefix list that is used to filter routes calculated from received LSPs, a case-sensitive string of 1 to 19 characters. For IP prefix list configuration information, see "[Routing policy configuration commands](#)."

route-policy route-policy-name: Specifies the name of a routing policy that is used to filter routes calculated from received LSPs, a case-sensitive string of 1 to 63 characters. For routing policy configuration information, see "[Routing policy configuration commands](#)."

Description

Use **filter-policy import** to configure IS-IS to filter routes calculated from received LSPs.

Use **undo filter-policy import** to disable IS-IS from filtering routes calculated from received LSPs.

IS-IS does not filter routes calculated from received LSPs by default.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command or in the routing policy, the ACL should be configured with the **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard** command to deny/permit a route with the specified destination, or with the **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard destination dest-addr dest-wildcard** command to deny/permit a route with the specified destination and mask. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route (the subnet mask must be valid; otherwise, the configuration is ineffective).

Related commands: **filter-policy export**.

Examples

Reference ACL 2000 to filter routes calculated from received LSPs.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] isis 1
[Sysname-isis-1] filter-policy 2000 import
```

Configure ACL 3000 to permit only route 113.0.0.0/16 to pass, and reference ACL 3000 to filter routes calculated from received LSPs.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0
[Sysname-acl-adv-3000] rule 100 deny ip
[Sysname-acl-adv-3000] quit
[Sysname] isis 1
[Sysname-isis 1] filter-policy 3000 import
```

flash-flood

Syntax

```
flash-flood [ flood-count flooding-count | max-timer-interval flooding-interval | [ level-1 | level-2 ] ] *
undo flash-flood [ level-1 | level-2 ]
```

View

IS-IS view

Default level

2: System level

Parameters

flood-count *flooding-count*: Specifies the maximum number of LSPs to be flooded before the next SPF calculation, ranging from 1 to 15. The default is 5.

max-timer-interval *flooding-interval*: Specifies the delay (in milliseconds) of the flash flooding, ranging from 10 to 50000. The default is 10.

level-1: Enables flash flooding for **level-1**.

level-2: Enables flash flooding for **level-2**.

Description

Use **flash-flood** to enable IS-IS LSP flash flooding.

Use **undo flash-flood** to disable IS-IS LSP flash flooding.

IS-IS LSP flash flooding is disabled by default.

If no level is specified, the command enables IS-IS LSP flash flooding for both Level-1 and Level-2.

Examples

```
# Enable fast flooding and specify the maximum LSPs to be sent as 10 and the delay time as 100 milliseconds.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] flash-flood flood-count 10 max-timer-interval 100
```

graceful-restart (IS-IS view)

Syntax

graceful-restart

undo graceful-restart

View

IS-IS view

Default level

2: System level

Parameters

None

Description

Use **graceful-restart** to enable IS-IS Graceful Restart capability.

Use **undo graceful-restart** to disable IS-IS Graceful Restart capability.

By default, IS-IS Graceful Restart capability is disabled.



IMPORTANT:

The IS-IS GR and IS-IS non-stop routing (NSR) features are mutually exclusive. Do not configure the **graceful-restart** and **non-stop-routing** commands at the same time.

Examples

```
# Enable the Graceful Restart capability for IS-IS process 1.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] graceful-restart
```

graceful-restart interval (IS-IS view)

Syntax

```
graceful-restart interval interval-value  
undo graceful-restart interval
```

View

IS-IS view

Default level

2: System level

Parameters

interval-value: Graceful Restart interval, in the range of 30 to 1800 seconds.

Description

Use **graceful-restart interval** to configure the Graceful Restart interval.

Use **undo graceful-restart interval** to restore the default Graceful Restart interval.

By default, the Graceful Restart interval is 300 seconds.

Examples

```
# Configure the Graceful Restart interval for IS-IS process 1 as 120 seconds.  
<Sysname> system-view  
[Sysname] isis 1  
[Sysname-isis-1] graceful-restart interval 120
```

graceful-restart suppress-sa

Syntax

```
graceful-restart suppress-sa  
undo graceful-restart suppress-sa
```

View

IS-IS view

Default level

2: System level

Parameters

None

Description

Use **graceful-restart suppress-sa** to suppress the SA (Suppress-Advertisement) bit during restart.

Use **undo graceful-restart suppress-sa** to set the SA bit.

By default, the SA bit is set during restart.

Suppressing the SA bit is mainly for avoiding black hole route. If a router starts or reboots without keeping the local forwarding table, sending packets to the router may result in a severe packet loss. To

avoid this, you can set the SA bit of the hello packet sent by the GR Restarter to 1. Upon receiving such hello packets, the GR Helpers will not advertise the GR Restarter through LSP.

Examples

```
# Suppress the SA bit during Graceful Restart.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart suppress-sa
```

import-route (IS-IS view)

Syntax

```
import-route protocol [ process-id | all-processes | allow-ibgp ] [ cost cost | cost-type { external | internal } ] [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
undo import-route protocol [ process-id | all-processes ]
```

View

IS-IS view

Default level

2: System level

Parameters

protocol: Redistributes routes from a routing protocol, which can be BGP, direct, IS-IS, OSPF, RIP or static.

process-id: Process ID, in the range of 1 to 65535. It is available only when the protocol is IS-IS, OSPF or RIP.

all-processes: Redistributes routes from all the processes of the specified routing protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

allow-ibgp: Allows redistribution of IBGP routes. It is available when the protocol is BGP.

cost: Specifies a cost for redistributed routes.

The range of the cost depends on its style:

- For the styles of narrow, narrow-compatible and compatible, the cost ranges from 0 to 63.
- For the styles of wide, wide-compatible, the cost ranges from 0 to 16777215.

cost-type { **external** | **internal** }: Specifies the cost type. The **internal** type indicates internal routes, and the **external** type indicates external routes. If **external** is specified, the cost of a redistributed route to be advertised is added by 64 to make internal routes take priority over external routes. The type is **external** by default. The keywords are available only when the cost type is **narrow**, **narrow-compatible** or **compatible**.

level-1: Redistributes routes into the Level-1 routing table.

level-1-2: Redistributes routes into both Level-1 and Level-2 routing tables.

level-2: Redistributes routes into the Level-2 routing table. If no level is specified, the routes are redistributed into the Level-2 routing table by default.

route-policy *route-policy-name*: Redistributes only routes satisfying the matching criteria of a routing policy. A routing policy name is a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag value for redistributed routes from 1 to 4294967295.

Description

Use **import-route** to redistribute routes from another routing protocol or another IS-IS process.

Use **undo import-route** to disable route redistribution from another routing protocol or another IS-IS process.

No route redistribution is configured by default.

IS-IS takes all the redistributed routes as external routes to destinations outside the IS-IS routing domain.

Related commands: **import-route isis level-2 into level-1**.

Using the **import-route bgp** command redistributes only EBGp routes. Using the **import-route bgp allow-ibgp** command redistributes both EBGp and IBGP routes, but this may cause routing loops; be cautious with this command.

Only active routes can be redistributed. Use the **display ip routing-table protocol** command to display route state information.

The **undo import-route protocol all-processes** command cancels the configuration made by the **import-route protocol all-processes** command, rather than the **import-route protocol process-id** command.

Examples

```
# Redistribute static routes and set the cost to 15.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] import-route static cost 15
```

import-route isis level-2 into level-1

Syntax

```
import-route isis level-2 into level-1 [ filter-policy { acl-number | ip-prefix ip-prefix-name | route-policy route-policy-name } | tag tag ] *
```

```
undo import-route isis level-2 into level-1
```

View

IS-IS view

Default level

2: System level

Parameters

acl-number: Specifies the number of an ACL that is used to filter routes from Level-2 to Level-1, ranging from 2000 to 3999. For ACL configuration information, see *ACL and QoS Command Reference*.

ip-prefix ip-prefix-name: Specifies the name of an IP prefix list that is used to filter routes from Level-2 to Level-1, a case-sensitive string of 1 to 19 characters. For IP prefix list configuration information, see "[Routing policy configuration commands](#)."

route-policy route-policy-name: Specifies the name of a routing policy that is used to filter routes from Level-2 to Level-1, a case-sensitive string of 1 to 63 characters. For routing policy configuration information, see "[Routing policy configuration commands](#)."

tag tag: Specifies a tag value from 1 to 4294967295 for redistributed routes.

Description

Use **import-route isis level-2 into level-1** to enable route leaking from Level-2 to Level-1.

Use **undo import-route isis level-2 into level-1** to disable routing leaking.

No route leaking is configured by default.

You can specify a routing policy in the **import-route isis level-2 into level-1** command to filter routes from Level-2 to Level-1. Other routing policies specified for route reception and redistribution does not affect the route leaking.

If a filter policy is configured, only routes passing it can be advertised into the Level-1 area.

Related commands: **import-route**.

Examples

```
# Enable route leaking from Level-2 to Level-1.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] import-route isis level-2 into level-1
```

import-route limit (IS-IS view)

Syntax

```
import-route limit number
```

```
undo import-route limit
```

View

IS-IS view

Default level

2: System level

Parameters

number: Maximum number of redistributed Level 1/Level 2 IPv4 routes. The default varies with devices.

Description

Use **import-route limit** to configure the maximum number of redistributed Level 1/Level 2 IPv4 routes.

Use **undo import-route limit** to restore the default.

By default, the maximum number of redistributed Level 1/Level 2 IPv4 routes varies with devices.

Examples

```
# Configure IS-IS process 1 to redistribute up to 1000 Level 1/Level 2 IPv4 routes.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] import-route limit 1000
```

isis

Syntax

```
isis [ process-id ] [ vpn-instance vpn-instance-name ]
```

```
undo isis [ process-id ]
```

View

System view

Default level

2: System level

Parameters

process-id: Process ID, ranging from 1 to 65535. The default is 1.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the IS-IS process belongs to the public network.

Description

Use **isis** to enable an IS-IS process and specify an associated VPN instance, enter IS-IS view, or both.

Use **undo isis** to disable an IS-IS process.

Related commands: **isis enable**, **network-entity**.

Examples

```
# Enable IS-IS routing process 1, with the system ID being 0000.0000.0002, and area ID being 01.0001.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] network-entity 01.0001.0000.0000.0002.00
```

isis authentication-mode

Syntax

```
isis authentication-mode { md5 | simple } [ cipher ] password [ level-1 | level-2 ] [ ip | osi ]
```

```
undo isis authentication-mode [ { md5 | simple } [ cipher ] password ] [ level-1 | level-2 ]
```

View

Interface view

Default level

2: System level

Parameters

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Sets a ciphertext password. If this keyword is not specified, you set a plaintext password.

password: Sets the password. This argument is case sensitive. It must be a plaintext string of 1 to 16 characters, or a ciphertext string of 33 to 53 characters.

level-1: Configures the password for Level-1.

level-2: Configures the password for Level-2.

ip: Checks IP related fields in LSPs and SNPs.

osi: Checks OSI related fields in LSPs and SNPs.

NOTE:

- This command is not available in loopback interface view.
 - Whether a password should use **ip** or **osi** is not affected by the actual network environment.
-

Description

Use **isis authentication-mode** to set the IS-IS authentication mode and password for an interface.

Use **undo isis authentication-mode** to restore the default.

No neighbor relationship authentication is configured by default.

The password in the specified mode is inserted into all outgoing hello packets and is used for authenticating the incoming hello packets. Only the authentication succeeds can the neighbor relationship be formed.

For two routers to become neighbors, the same authentication mode and password must be specified at both ends.

The authentication password, set in either plain text or cipher text, is saved to the configuration file in cipher text.

If you configure a password without specifying a level, the password applies to both Level-1 and Level-2.

If neither **ip** nor **osi** is specified, the OSI related fields in LSPs are checked.

The **level-1** and **level-2** keywords are configurable on an interface that has had IS-IS enabled with the **isis enable** command.

Related commands: **area-authentication-mode**, **domain authentication-mode**.

Examples

On VLAN-interface 10, configure the Level-1 adjacency authentication mode as **simple**, and set the plaintext password to **123456**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis authentication-mode simple 123456 level-1
```

isis bfd enable

Syntax

isis bfd enable

undo isis bfd enable

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **isis bfd enable** to enable BFD on an IS-IS interface for link failure detection.

Use **undo isis bfd enable** to disable BFD on an IS-IS interface.

By default, an IS-IS interface is not enabled with BFD.

Examples

```
# Enable BFD for IS-IS on VLAN-interface 11.
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] isis enable
[Sysname-Vlan-interface11] isis bfd enable
```

isis circuit-level

Syntax

isis circuit-level [**level-1** | **level-1-2** | **level-2**]

undo isis circuit-level

View

Interface view

Default level

2: System level

Parameters

level-1: Sets the circuit level to Level-1.

level-1-2: Sets the circuit level to Level-1-2.

level-2: Sets the circuit level to Level-2.

Description

Use **isis circuit-level** to set the circuit level for the interface.

Use **undo isis circuit-level** to restore the default.

An interface can establish either the Level-1 or Level-2 adjacency by default.

For a Level-1 (Level-2) router, the circuit level can only be Level-1 (Level-2). For a Level-1-2 router, you need to specify a circuit level for a specific interface to form only the specified level neighbor relationship.

Related commands: **is-level**.

Examples

VLAN-interface 10 is connected to a non backbone router in the same area. Configure the circuit level of VLAN-interface 10 as Level-1 to prevent sending and receiving Level-2 Hello packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable
[Sysname-Vlan-interface10] isis circuit-level level-1
```

isis circuit-type p2p

Syntax

isis circuit-type p2p

undo isis circuit-type

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **isis circuit-type p2p** to configure the network type for an interface as P2P.

Use **undo isis circuit-type** to cancel the configuration.

By default, the network type of an interface depends on the physical media. (The network type of a VLAN interface is broadcast.)

Interfaces with different network types operate differently. For example, broadcast interfaces on a network need to elect a DIS and flood CSNP packets to synchronize the LSDBs, and P2P interfaces on a network need not elect a DIS and have a different LSDB synchronization mechanism.

If only two routers exist on a broadcast network, configure the network type of attached interfaces as P2P to avoid DIS election and CSNP flooding, saving network bandwidth and speeding up network convergence.

You can perform this configuration only for a broadcast network with only two attached routers.

NOTE:

This command is not supported in loopback interface view.

Examples

```
# Configure the network type of VLAN-interface 10 as P2P.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] isis enable  
[Sysname-Vlan-interface10] isis circuit-type p2p
```

isis cost

Syntax

```
isis cost value [ level-1 | level-2 ]
```

```
undo isis cost [ value ] [ level-1 | level-2 ]
```

View

Interface view

Default level

2: System level

Parameters

value: Specifies an IS-IS cost for the interface. The cost range differs with cost styles.

- For cost styles **narrow**, **narrow-compatible** and **compatible**, the cost ranges from 1 to 63.
- For cost styles **wide** and **wide-compatible**, the cost ranges from 1 to 16777215.

level-1: Applies the cost to Level-1.

level-2: Applies the cost to Level-2.

Description

Use **isis cost** to set the IS-IS cost of an interface.

Use **undo isis cost** to restore the default.

No cost is configured by default.

If neither **level-1** nor **level-2** is included, the cost applies to both **level-1** and **level-2**.

HP recommends to configure a proper IS-IS cost for each interface to guarantee correct route calculation.

Relate command: **circuit-cost**.

Examples

```
# Configure the Level-2 IS-IS cost as 5 for VLAN-interface10.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis cost 5 level-2
```

isis dis-name

Syntax

isis dis-name *symbolic-name*

undo isis dis-name

View

Interface view

Default level

2: System level

Parameters

symbolic-name: Specifies a DIS name, a string of 1 to 64 characters.

Description

Use **isis dis-name** to configure a name for a DIS to represent the pseudo node on a broadcast network.

Use **undo isis dis-name** to remove the configuration.

No name is configured for the DIS by default.

This command takes effect only on a router that must have dynamic system ID to host name mapping enabled. This command is not supported on a Point-to-Point interface.

NOTE:

This command is not available in loopback interface view.

Examples

```
# Configure the DIS name as LOCALAREA.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis dis-name LOCALAREA
```

isis dis-priority

Syntax

```
isis dis-priority value [ level-1 | level-2 ]
undo isis dis-priority [ value ] [ level-1 | level-2 ]
```

View

Interface view

Default level

2: System level

Parameters

value: Specifies a DIS priority for the interface, ranging from 0 to 127.

level-1: Applies the DIS priority to Level-1.

level-2: Applies the DIS priority to Level-2.

Description

Use **isis dis-priority** to specify a DIS priority at a specified level for an interface.

Use **undo isis dis-priority** to restore the default priority of 64 for Level-1 and Level-2.

If neither **level-1** nor **level-2** is specified in this command, the DIS priority applies to both Level-1 and Level-2.

On an IS-IS broadcast network, a router should be elected as the DIS at each routing level. You can specify a DIS priority at a level for an interface. The greater the interface's priority is, the more likelihood it becomes the DIS. If multiple routers in the broadcast network have the same highest DIS priority, the router with the highest SNPA (Subnetwork Point of Attachment) address (SNPA addresses are MAC addresses on a broadcast network) becomes the DIS.

IS-IS has no backup DIS and the router with a priority of 0 can also participate in DIS election.

NOTE:

This command is not available in loopback interface view.

Examples

```
# Configure the Level-2 DIS priority as 127 for VLAN-interface 10.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis dis-priority 127 level-2
```

isis enable

Syntax

```
isis enable [ process-id ]
undo isis enable
```

View

Interface view

Default level

2: System level

Parameters

process-id: Specifies a IS-IS process ID, ranging from 1 to 65535. The default is 1.

Description

Use **isis enable** to enable an IS-IS process on the interface.

Use **undo isis enable** to disable IS-IS.

No IS-IS routing process is enabled on an interface by default.

Related commands: **isis**, **network-entity**.

Examples

Create IS-IS routing process 1, and enable the IS-IS routing process on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable 1
```

isis mib-binding

Syntax

isis mib-binding *process-id*

undo isis mib-binding

View

System view

Default level

2: System level

Parameters

process-id: IS-IS process ID, in the range of 1 to 65535.

Description

Use **isis mib-binding** to bind MIBs with an IS-IS process.

Use **undo isis mib-binding** to restore the default.

By default, MIBs are bound with IS-IS process 1.

Examples

Bind MIBs with IS-IS process 100.

```
<Sysname> system-view
[Sysname] isis mib-binding 100
```


isis silent

Syntax

isis silent
undo isis silent

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **isis silent** to disable the interface from sending and receiving IS-IS packets.

Use **undo isis silent** to restore the default.

By default, an interface is not disabled from sending and receiving IS-IS packets.

NOTE:

The feature is not supported on the loopback interface.

Examples

```
# Disable VLAN-interface 10 from sending and receiving IS-IS packets.  
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] isis silent
```

isis small-hello

Syntax

isis small-hello
undo isis small-hello

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **isis small-hello** to configure the interface to send small hello packets without CLVs.

Use **undo isis small-hello** to restore the default.

An interface sends standard hello packets by default.

NOTE:

This command is not available in loopback interface view.

Examples

```
# Configure VLAN-interface 10 to send small Hello packets.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis small-hello
```

isis timer csnp

Syntax

```
isis timer csnp seconds [ level-1 | level-2 ]
undo isis timer csnp [ seconds ] [ level-1 | level-2 ]
```

View

Interface view

Default level

2: System level

Parameters

seconds: Specifies on the DIS of a broadcast network the interval in seconds for sending CSNP packets, ranging from 1 to 600.

level-1: Applies the interval to Level-1.

level-2: Applies the interval to Level-2.

Description

Use **isis timer csnp** to specify on the DIS of a broadcast network the interval for sending CSNP packets.

Use **undo isis timer csnp** to restore the default.

The default CSNP interval is 10 seconds.

If no level is specified, the CSNP interval applies to both Level-1 and Level-2.

This command only applies to the DIS of a broadcast network, which sends CSNP packets periodically for LSDB synchronization.

NOTE:

This command is not supported in loopback interface view.

Examples

```
# Configure Level-2 CSNP packets to be sent every 15 seconds over VLAN-interface 10.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer csnp 15 level-2
```

isis timer hello

Syntax

```
isis timer hello seconds [ level-1 | level-2 ]  
undo isis timer hello [ seconds ] [ level-1 | level-2 ]
```

View

Interface view

Default level

2: System level

Parameters

seconds: Specifies the interval in seconds for sending hello packets, ranging from 3 to 255.

level-1: Specifies the interval for sending Level-1 hello packets.

level-2: Specifies the interval for sending Level-2 hello packets.

Description

Use **isis timer hello** to specify the interval for sending hello packets.

Use **undo isis timer hello** to restore the default.

The default hello interval is 10 seconds.

Level-1 and Level-2 hello packets are sent independently on a broadcast network, so you need to specify an interval for the two levels respectively. On a P2P link, Level-1 and Level-2 packets are both sent in P2P hello packets, and you need not specify an interval for two levels respectively.

You can configure keywords **level-1** and **level-2** only on broadcast interfaces. Before doing that, you need to enable IS-IS on the interface.

As the shorter the interval is, the more system resources will be occupied, you should configure a proper interval as needed.

If no level is specified, the hello interval applies to both Level-1 and Level-2.

NOTE:

This command is not supported in loopback interface view.

Related commands: **isis timer holding-multiplier**.

Examples

```
# Configure Level-2 hello packets to be sent every 20 seconds over VLAN-interface 10.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] isis timer hello 20 level-2
```

isis timer holding-multiplier

Syntax

```
isis timer holding-multiplier value [ level-1 | level-2 ]  
undo isis timer holding-multiplier [ value ] [ level-1 | level-2 ]
```

View

Interface view

Default level

2: System level

Parameters

value: Number of hello intervals, in the range of 3 to 1000.

level-1: Applies the number to the Level-1 IS-IS neighbor.

level-2: Applies the number to the Level-2 IS-IS neighbor.

NOTE:

This command is not available in loopback interface view.

Description

Use **isis timer holding-multiplier** to specify the IS-IS hello multiplier.

Use **undo isis timer holding-multiplier** to restore the default.

The default IS-IS hello multiplier is 3.

With the IS-IS hello multiplier configured, a router can use hello packets to notify its neighbor router of the adjacency hold time (hello multiplier times hello interval). If the neighbor router receives no hello packets from this router within the hold time, it declares the adjacency down. You can adjust the adjacency hold time by changing the hello multiplier or the hello interval on an interface.

Level-1 and Level-2 hello packets are sent independently on a broadcast network, so you need to specify a hello multiplier for the two levels respectively. On a P2P link, Level-1 and Level-2 packets are both sent in P2P hello packets, and you need not specify Level-1 or Level-2.

You can configure keywords **level-1** and **level-2** only on broadcast interfaces. Before doing that, you need to enable IS-IS on the interface.

If no level is specified, the hello multiplier applies to the current level.

Related commands: **isis timer hello**.

Examples

```
# Configure the hello multiplier as 6 for VLAN-interface 10.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer holding-multiplier 6
```

isis timer lsp

Syntax

isis timer lsp *time* [**count** *count*]

undo isis timer lsp

View

Interface view

Default level

2: System level

Parameters

time: Specifies the minimum interval in milliseconds for sending link-state packets, ranging from 1 to 1000.

count: Specifies the maximum number of link-state packets to be sent at one time, in the range of 1 to 1000. The default is 5.

Description

Use **isis timer lsp** to configure the minimum interval for sending LSPs on the interface and specify the maximum LSPs that can be sent per time.

Use **undo isis timer lsp** to restore the default of 33 ms.

Related commands: **isis timer retransmit**.

NOTE:

This command is not available in loopback interface view.

Examples

Configure the interval as 500 milliseconds for sending LSPs on interface VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer lsp 500
```

isis timer retransmit

Syntax

isis timer retransmit *seconds*

undo isis timer retransmit

View

Interface view

Default level

2: System level

Parameters

seconds: Specifies the interval in seconds for retransmitting LSP packets, ranging from 1 to 300.

Description

Use **isis timer retransmit** to configure the interval for retransmitting LSP packets over a point-to-point link.

Use **undo isis timer retransmit** to restore the default.

By default, the retransmission interval is 5 seconds.

A P2P link requires a response to a sent LSP. If no response is received within the retransmission interval, the LSP is retransmitted.

You need not use this command over a broadcast link where CSNPs are broadcast periodically.

Configure a proper retransmission interval to avoid unnecessary retransmissions.

Perform this configuration only when the link layer protocol is PPP.

NOTE:

This command is not available in loopback interface view.

Related commands: **isis timer lsp**.

Examples

Configure the LSP retransmission interval as 10 seconds for Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] isis timer retransmit 10
```

is-level

Syntax

is-level { **level-1** | **level-1-2** | **level-2** }

undo is-level

View

IS-IS view

Default level

2: System level

Parameters

level-1: Configures the router to work on Level-1, which means it only calculates routes within the area, and maintains the L1 LSDB.

level-1-2: Configures the router to work on Level-1-2, which means it calculates routes and maintains the LSDBs for both L1 and L2.

level-2: Configures the router to work on Level-2, which means it calculates routes and maintains the LSDB for L2 only.

Description

Use **is-level** to specify the IS level.

Use **undo is-level** to restore the default.

The default IS level is **level-1-2**.

Configure all the routers as either Level-1 or Level-2 if only one area is present, because the routers do not need to maintain two identical databases at the same time. If the only area is an IP network, configure all the routers as Level-2 for scalability.

Related commands: **isis circuit-level**.

Examples

Configure the router to work in Level-1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] is-level level-1
```

is-name

Syntax

is-name *sys-name*

undo is-name

View

IS-IS view

Default level

2: System level

Parameters

symbolic-name: Specifies a host name for the local IS, a string of 1 to 64 characters.

Description

Use **is-name** to specify a host name for the IS to enable dynamic system ID to hostname mapping.

Use **undo is-name** to disable dynamic system ID to hostname mapping.

Dynamic system ID to hostname mapping is not enabled by default.

Examples

```
# Configure a host name for the local IS.
```

```
<Sysname> system-view  
[Sysname] isis 1  
[Sysname-isis-1] is-name RUTA
```

is-name map

Syntax

is-name map *sys-id map-sys-name*

undo is-name map *sys-id*

View

IS-IS view

Default level

2: System level

Parameters

sys-id: System ID or pseudonode ID of a remote IS.

map-sys-name: Specifies a host name for the remote IS, a string of 1 to 64 characters.

Description

Use **is-name map** to configure a system ID to host name mapping for a remote IS.

Use **undo is-name map** to remove the mapping.

Each remote IS system ID corresponds to only one name.

Examples

```
# Map the host name RUTB to the system ID 0000.0000.0041 of the remote IS.
```

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] is-name map 0000.0000.0041 RUTB
```

is-snmp-traps enable

Syntax

```
is-snmp-traps enable
undo is-snmp-traps
```

View

IS-IS view

Default level

2: System level

Parameters

None

Description

Use **is-snmp-traps enable** to enable the SNMP Trap function of IS-IS.

Use the **undo is-snmp-traps** command to disable this function.

SNMP Trap is enabled by default.

Examples

```
# Enable SNMP Trap.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] is-snmp-traps enable
```

log-peer-change (IS-IS view)

Syntax

```
log-peer-change
undo log-peer-change
```

View

IS-IS view

Default level

2: System level

Parameters

None

Description

Use **log-peer-change** to enable the logging of IS-IS neighbor state changes.

Use **undo log-peer-change** to disable the logging.

The logging is enabled by default.

After the logging is enabled, information about IS-IS adjacency state changes is sent to the configuration terminal.

Examples

```
# Enable logging on the IS-IS adjacency state changes.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] log-peer-change
```

lsp-fragments-extend

Syntax

```
lsp-fragments-extend [ [ level-1 | level-1-2 | level-2 ] | [ mode-1 | mode-2 ] ] *
undo lsp-fragments-extend
```

View

IS-IS view

Default level

2: System level

Parameters

level-1: Applies the fragment extension mode to Level-1 LSPs.

level-1-2: Applies the fragment extension mode to both Level-1 and Level-2 LSPs.

level-2: Applies the fragment extension mode to Level-2 LSPs.

mode-1: Fragment extension mode 1, used on a network where some routers do not support LSP fragment extension.

mode-2: Fragment extension mode 2, used on a network where all routers support LSP fragment extension.

Description

Use **lsp-fragments-extend** to enable an LSP fragment extension mode for a level.

Use **undo lsp-fragments-extend** to disable LSP fragment extension for a level.

LSP fragment extension is disabled by default.

If no mode is specified, LSP fragment extension mode 1 is enabled.

If no level is specified, the LSP fragment extension mode is enabled for both Level-1 and Level-2.

Examples

```
# Enable LSP fragment extension mode 1 for Level-2.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] lsp-fragments-extend mode-1 level-2
```

lsp-length originate

Syntax

```
lsp-length originate size [ level-1 | level-2 ]
```

undo lsp-length originate [**level-1** | **level-2**]

View

IS-IS view

Default level

2: System level

Parameters

size: Specifies the maximum size in bytes of LSP packets, ranging from 512 to 16384.

level-1: Applies the size to Level-1 LSP packets.

level-2: Applies the size to Level-2 LSP packets.

Description

Use **lsp-length originate** to configure the maximum size of generated Level-1 or Level-2 LSPs.

Use **undo lsp-length originate** to restore the default.

By default, the maximum size of generated Level-1 and Level-2 LSPs is 1497 bytes.

If neither Level-1 nor Level-2 is specified in the command, the configured maximum size applies to the current IS-IS level.

Examples

```
# Configure the maximum size of the generated Level-2 LSPs as 1024 bytes.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] lsp-length originate 1024 level-2
```

lsp-length receive

Syntax

lsp-length receive *size*

undo lsp-length receive

View

IS-IS view

Default level

2: System level

Parameters

size: Maximum size of received LSPs, in the range of 512 to 16384 bytes.

Description

Use **lsp-length receive** to configure the maximum size of received LSPs.

Use **undo lsp-length receive** to restore the default.

By default, the maximum size of received LSPs is 1497 bytes.

Examples

```
# Configure the maximum size of received LSPs.
<Sysname> system-view
```

```
[Sysname] isis 1
[Sysname-isis-1] lsp-length receive 1024
```

maximum load-balancing (IS-IS view)

Syntax

```
maximum load-balancing number
undo maximum load-balancing
```

View

IS-IS view

Default level

2: System level

Parameters

number: Maximum number of equal-cost routes, in the range of 1 to 8.

Description

Use **maximum load-balancing** to configure the maximum number of ECMP routes.

Use **undo maximum load-balancing** to restore the default.

By default, the maximum number of ECMP routes is 8.

Examples

```
# Configure the maximum number of ECMP routes as 2.
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] maximum load-balancing 2
```

network-entity

Syntax

```
network-entity net
undo network-entity net
```

View

IS-IS view

Default level

2: System level

Parameters

net: Network Entity Title (NET) in the format of X...X.XXXX...XXXX.00 in hexadecimal notation, with the first part X...X being the area address, the middle part XXXX...XXXX (a total of 12 "X") being the router's system ID, and the last part 00 being SEL.

Description

Use **network-entity** to configure the Network Entity Title for an IS-IS routing process.

Use **undo network-entity** to delete a NET.

No NET is configured by default.

A NET is a special NSAP address with the SEL being 0. The length of the NET is in the range of 8 bytes to 20 bytes.

A NET comprises the following parts:

- Area ID. Its length is in the range of 1 to 13 bytes.
- System ID. A system ID uniquely identifies a host or router in the area and has a fixed 6-byte length.
- SEL. It has a value of 0 and a fixed 1-byte length.

For example, a NET is ab.cdef.1234.5678.9abc.00, where area ID is ab.cdef, system ID is 1234.5678.9abc, and SEL is 00.

Related commands: **isis**, **isis enable**.

Examples

```
# Specify the NET as 10.0001.1010.1020.1030.00, of which 10.0001 is the area ID and 1010.1020.1030 is the system ID.
```

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
```

non-stop-routing

Syntax

non-stop-routing

undo non-stop-routing

View

IS-IS view

Default level

2: System level

Parameters

None

Description

Use **non-stop-routing** to enable IS-IS NSR.

Use **undo non-stop-routing** to disable IS-IS NSR.

By default, IS-IS NSR is disabled.



IMPORTANT:

The IS-IS GR and IS-IS NSR features are mutually exclusive. Do not configure the **non-stop-routing** and **graceful-restart** commands at the same time.

Examples

```
# Enable NSR for IS-IS process 1.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] non-stop-routing
```

non-stop-routing interval

Syntax

```
non-stop-routing interval interval-value  
undo non-stop-routing interval
```

View

IS-IS view

Default level

2: System view

Parameters

interval-value: NSR interval, in the range of 30 to 1800 seconds. The NSR interval refers to the expected interval of a master/slave switchover on an IRF fabric.

Description

Use **non-stop-routing interval** to set the NSR interval.

Use **undo non-stop-routing interval** to restore the default.

By default, the NSR interval is 0 seconds—no NSR interval is set.

If an NSR interval is set on a device, a neighbor of the device uses the larger value of the NSR interval and hold time of the device as the hold time to ensure the neighbor relationship does not time out during a master/slave switchover on the device.

If no NSR interval is configured on the device, the hold time configured on a specific interface is used by the relevant neighbor.

Examples

```
# Set the NSR interval to 40 seconds for IS-IS process 1.  
<Sysname> system-view  
[Sysname] isis 1  
[Sysname-isis-1] non-stop-routing  
[Sysname-isis-1] non-stop-routing interval 40
```

preference (IS-IS view)

Syntax

```
preference { preference | route-policy route-policy-name } *  
undo preference
```

View

IS-IS view

Default level

2: System level

Parameters

preference: Specifies the preference for IS-IS protocol, ranging from 1 to 255.

route-policy *route-policy-name*: Routing policy name, a case-sensitive string of 1 to 63 characters. The preference applies to routes passing the routing policy.

Description

Use **preference** to configure the preference for IS-IS.

Use **undo preference** to restore the default.

By default, IS-IS preference is 15.

If a routing policy is specified in this command, the preference (if any) set by the routing policy applies to those matched routes. Other routes use the preference set by the **preference** command.

When a router runs multiple routing protocols at the same time, the system will configure a preference to each routing protocol. If several protocols find routes to the same destination, the route of the routing protocol with the highest preference is selected.

Examples

```
# Configure the preference of IS-IS protocol as 25.
```

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] preference 25
```

priority high

Syntax

```
priority high { ip-prefix prefix-name | tag tag-value }
```

```
undo priority high [ ip-prefix | tag ]
```

View

IS-IS view

Default level

2: System level

Parameters

ip-prefix *ip-prefix-name*: Specifies the name of an IP prefix list, a case-sensitive string of 1 to 19 characters.

tag *tag-value*: Specifies a tag value, in the range of 1 to 4294967295.

Description

Use **priority high** to assign a high priority to specific routes for faster network convergence.

Use **undo priority high** to restore the default.

By default, no IS-IS route is assigned a high priority.

If no IS-IS route is assigned a high priority, IS-IS host routes are processed first in network convergence because they have higher priority than other types of IS-IS routes.

Examples

```
# Assign a high priority to the IS-IS routes matching IP prefix list standtest.
```

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] priority high ip-prefix standtest
```

reset isis all

Syntax

```
reset isis all [ process-id | vpn-instance vpn-instance-name ]
```

View

User view

Default level

2: System level

Parameters

process-id: Clears the data structure information of an IS-IS process numbered from 1 to 65535.

vpn-instance *vpn-instance-name*: Clears the data structure information of the MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the data structure information of the public network is cleared.

Description

Use **reset isis all** to clear all IS-IS data structure information.

No data structure information is cleared by default.

This command is used when the LSP needs to be updated immediately. For example, after performing the **area-authentication-mode** and **domain-authentication-mode** commands, you can use this command to clear old LSPs.

Related commands: **area-authentication-mode**, **domain authentication-mode**.

Examples

```
# Clear all IS-IS data structure information.  
<Sysname> reset isis all
```

reset isis peer

Syntax

```
reset isis peer system-id [ process-id | vpn-instance vpn-instance-name ]
```

View

User view

Default level

2: System level

Parameters

system-id: Specifies the system ID of an IS-IS neighbor.

process-id: Clears the data structure information of an IS-IS process with an ID from 1 to 65535.

vpn-instance *vpn-instance-name*: Clears the data structure information of the MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the data structure information of the public network is cleared.

Description

Use **reset isis peer** to clear the data structure information of a specified IS-IS neighbor.

This command is used when you need to re-establish an IS-IS neighbor relationship.

Examples

```
# Clear the data structure information of the neighbor with the system ID 0000.0c11.1111.  
<Sysname> reset isis peer 0000.0c11.1111
```

set-overload

Syntax

```
set-overload [ on-startup [ [ start-from-nbr system-id [ timeout1 [ nbr-timeout ] ] ] | timeout2 ] [ allow  
{ external | interlevel } * ]
```

```
undo set-overload
```

View

IS-IS view

Default level

2: System level

Parameters

on-startup: Sets the overload bit upon system startup.

start-from-nbr *system-id* [*timeout1* [*nbr-timeout*]]: Starts the *nbr-timeout* timer when the router begins to establish the neighbor relationship with the neighbor after system startup. If the neighbor relationship is formed within the *nbr-timeout* interval, IS-IS keeps the overload bit set; if not, the bit is cleared. IS-IS keeps the overload bit set within the *timeout1* interval after the neighbor relationship is formed within the *nbr-timeout* interval.

- *system-id*: Specifies the neighbor.
- *timeout1*: The *timeout1* interval is in the range of 5 to 86400 seconds and defaults to 600 seconds.
- *nbr-timeout*: The timer has an interval from 5 to 86400 seconds. The default is 1200 seconds.

timeout2: Sets the overload bit within the *timeout2* interval after system startup. The interval is in the range of 5 to 86400 seconds and defaults to 600 seconds.

allow: Allows advertising address prefixes. By default, no address prefixes are allowed to be advertised when the overload bit is set.

external: Allows advertising IP address prefixes redistributed from other routing protocols with the **allow** keyword specified.

interlevel: Allows advertising IP address prefixes learned from different IS-IS levels with the **allow** keyword specified.

Description

Use **set-overload** to set the overload bit.

Use **undo set-overload** to clear the overload bit.

The overload bit is not set by default.

If the **on-startup** keyword is not specified, the command sets the overload bit immediately until the **undo set-overload** command is executed.

If the **on-startup** keyword is specified, IS-IS sets the overload bit upon system startup and keeps it set within the *timeout2* interval.

Examples

```
# Set overload flag on the current router.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] set-overload
```

summary (IS-IS view)

Syntax

```
summary ip-address { mask | mask-length } [ avoid-feedback | generate_null0_route | [ level-1 | level-1-2 | level-2 ] | tag tag ] *
```

```
undo summary ip-address { mask | mask-length } [ level-1 | level-1-2 | level-2 ]
```

View

IS-IS view

Default level

2: System level

Parameters

ip-address: Destination IP address of the summary route.

mask: Mask of the destination IP address, in dotted decimal format.

mask-length: Mask length, in the range of 0 to 32.

avoid-feedback: Avoids learning summary routes by route calculation.

generate_null0_route: Generate the Null 0 route to avoid routing loops.

level-1: Summarize only the routes redistributed to Level-1.

level-1-2: Summarizes the routes redistributed to both Level-1 and Level-2.

level-2: Summarizes only the routes redistributed to Level-2.

tag *tag*: Specifies a management tag, in the range of 1 to 4294967295.

Description

Use **summary** to configure a summary route.

Use **undo summary** to remove a summary route.

No summarization is configured by default.

If no level is specified, only the **level-2** routes will be summarized by default.

You can summarize multiple contiguous networks into a single network to reduce the size of the routing table, as well as that of LSP and LSDB generated by the router. It is allowed to summarize native IS-IS routes and redistributed routes. After summarization, the cost of the summary route is the smallest cost of those summarized routes.

The router summarizes only routes in local LSPs.

Examples

```
# Configure a summary route of 202.0.0.0/8.
<Sysname> system-view
[Sysname] isis 1
```

timer lsp-generation

Syntax

```
timer lsp-generation maximum-interval [ initial-interval [ second-wait-interval ] ] [ level-1 | level-2 ]  
undo timer lsp-generation [ level-1 | level-2 ]
```

View

IS-IS view

Default level

2: System level

Parameters

maximum-interval: Maximum wait interval in seconds for generating IS-IS LSPs, in the range of 1 to 120.

initial-interval: Initial wait interval in milliseconds before generating the first IS-IS LSP, in the range of 10 to 60000. The default is 0.

second-wait-interval: Wait interval in milliseconds before generating the second LSP, in the range of 10 to 60000. The default is 0.

level-1: Applies the intervals to Level-1.

level-2: Applies the intervals to Level-2. If no level is specified, the specified intervals apply to both Level-1 and Level-2.

Description

Use **timer lsp-generation** to specify the wait interval before generating IS-IS LSPs.

Use **undo timer lsp-generation** to restore the default.

By default, the wait interval before LSP generation is 2 seconds.

1. If only the maximum interval is specified, IS-IS waits the maximum interval before generating an LSP.
2. If both the maximum and initial intervals are specified:
 - IS-IS waits the initial interval before generating the first LSP.
 - If the network topology is unstable—triggers occur at intervals shorter than the maximum interval, IS-IS waits the maximum interval before generating the first LSP until the network topology is stable.
3. If the maximum, initial, and second wait intervals are specified:
 - IS-IS waits the initial interval before generating the first LSP.
 - If the network topology is unstable—triggers occur at intervals shorter than the maximum interval, IS-IS waits the *second-wait-interval* before generating the second LSP and penalty is applied on the wait interval before generating the next LSP. For each subsequent trigger, the wait interval before generating the LSP will be two times the previous wait interval until the maximum interval is reached.
 - After the network topology is stable—triggers occur at intervals greater than the maximum interval, the wait interval before generating LSPs is restored to the initial interval.

Examples

```
# Set the maximum, initial, and second wait intervals to 10 seconds, 100 milliseconds and 200
milliseconds respectively.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1]timer lsp-generation 10 100 200
```

timer lsp-max-age

Syntax

```
timer lsp-max-age seconds
undo timer lsp-max-age
```

View

IS-IS view

Default level

2: System level

Parameters

seconds: Specifies the LSP maximum aging time in seconds, ranging from 1 to 65535.

Description

Use **timer lsp-max-age** to set the LSP maximum age in the LSDB.

Use **undo timer lsp-max-age** to restore the default.

The default LSP maximum age is 1200 seconds.

Related commands: **timer lsp-refresh**.

Examples

```
# Set the maximum LSP age to 1500 seconds.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] timer lsp-max-age 1500
```

timer lsp-refresh

Syntax

```
timer lsp-refresh seconds
undo timer lsp-refresh
```

View

IS-IS view

Default level

2: System level

Parameters

seconds: LSP refresh interval in seconds, ranging from 1 to 65534.

Description

Use **timer lsp-refresh** to configure the LSP refresh interval.

Use **undo timer lsp-refresh** to restore the default.

The default LSP refresh interval is 900 seconds.

To refresh LSPs before they are aged out, the interval configured by the **timer lsp-refresh** command must be smaller than that configured by the **timer lsp-max-age** command.

Related commands: **timer lsp-max-age**.

Examples

Configure the LSP refresh interval as 1500 seconds.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] timer lsp-refresh 1500
```

timer spf

Syntax

timer spf *maximum-interval* [*initial-interval* [*second-wait-interval*]]

undo timer spf

View

IS-IS view

Default level

2: System level

Parameters

maximum-interval: Maximum SPF calculation interval in seconds, ranging from 1 to 120.

initial-interval: Wait interval before the first SPF calculation, in milliseconds, ranging from 10 to 60000.

second-wait-interval: Wait interval before the second SPF calculation, in milliseconds, ranging from 10 to 60000.

Description

Use **timer spf** to set the SPF calculation interval.

Use **undo timer spf** to restore the default.

The default IS-IS SPF calculation interval is 10 seconds.

- If only the maximum interval is specified, IS-IS waits the maximum interval before performing the SPF calculation.
- If both the maximum and initial intervals are specified:
 - IS-IS waits the initial interval before performing the first SPF calculation.
 - When SPF calculation triggers occur at intervals shorter than the maximum interval, the topology is considered unstable and IS-IS waits the maximum interval before performing the SPF calculation until the topology is stable.
- If maximum-interval, initial-interval, and second-wait-interval are specified:
 - IS-IS waits the initial interval before performing the first SPF calculation.

- When SPF calculation triggers occur at intervals shorter than the maximum interval, the topology is considered unstable, IS-IS will wait the *second-interval* before performing the second SPF calculation and penalty is applied on the wait interval for the next SPF calculation. For each subsequent trigger, the wait interval before SPF calculation will be two times the previous wait interval until the maximum interval is reached.
- After the network topology becomes stable—triggers occur at intervals greater than the maximum interval, the wait interval before SPF calculation is restored to the initial interval.

Examples

Configure the maximum SPF calculation interval as 10 seconds, the wait interval before the first SPF calculation as 100 milliseconds, and the wait interval before the second SPF calculation as 200 milliseconds.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] timer spf 10 100 200
```

virtual-system

Syntax

```
virtual-system virtual-system-id
undo virtual-system virtual-system-id
```

View

IS-IS view

Default level

2: System level

Parameters

virtual-system-id: Virtual system ID of the IS-IS process.

Description

Use **virtual-system** to configure a virtual system ID for the IS-IS process. Use **undo virtual-system** to remove a virtual system ID.

Up to 50 virtual system IDs can be configured for the IS-IS process.

Examples

```
# Set a virtual system ID of 2222.2222.2222 for IS-IS process 1.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] virtual-system 2222.2222.2222
```

BGP configuration commands

The term "router" in this chapter refers to both routers and Layer 3 switches.

For more information about routing policy configuration commands in this document, see "[Routing policy configuration commands](#)."

The A5500 SI Switch Series does not support BGP.

aggregate

Syntax

```
aggregate ip-address { mask | mask-length } [ as-set | attribute-policy route-policy-name | detail-suppressed | origin-policy route-policy-name | suppress-policy route-policy-name ] *
```

```
undo aggregate ip-address { mask | mask-length }
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

ip-address: Summary address.

mask: Summary route mask, in dotted decimal notation.

mask-length: Length of summary route mask, in the range of 0 to 32.

as-set: Creates a summary with AS set.

attribute-policy *route-policy-name*: Sets the attributes of the summary route according to the routing policy. The routing policy name is a case-sensitive string of 1 to 63 characters.

detail-suppressed: Only advertises the summary route.

suppress-policy *route-policy-name*: Suppresses specific routes defined in the routing policy. The routing policy name is a case-sensitive string of 1 to 63 characters.

origin-policy *route-policy-name*: References the routing policy to specify routes for summarization. The routing policy name is a case-sensitive string of 1 to 63 characters.

Table 41 Functions of the keywords

Keywords	Function
as-set	Used to create a summary route, whose AS path contains the AS path information of summarized routes. Use this keyword carefully when many AS paths need to be summarized, because the frequent changes of these specific routes may lead to route oscillation.
detail-suppressed	This keyword does not suppress the summary route, but it suppresses the advertisement of all the more specific routes. To summarize only some specific routes, use the peer filter-policy command.

Keywords	Function
suppress-policy	Used to create a summary route and suppress the advertisement of some summarized routes. If you want to suppress some routes selectively and leave other routes still advertised, use the if-match clause of the route-policy command.
origin-policy	Selects only routes satisfying the routing policy for route summarization.
attribute-policy	Sets attributes except the AS_PATH attribute for the summary route. The same work can be done by using the peer route-policy command.

Description

Use **aggregate** to create a summary route in the BGP routing table.

Use **undo aggregate** to remove a summary route.

By default, no summary route is configured.

The output interface of a BGP summary route is Null 0. With route summarization, BGP advertises fewer routes to its peers. A summary route must not be optimal; otherwise, BGP will fail to forward the packets matching the route. If a summarized specific route has the same mask as the summary route but has a lower priority, the summary route becomes the optimal route. In this case, you must change the priority of the summary or the specific route to make the specific route optimal.

Examples

In BGP view, create a summary of 192.213.0.0/16 in the BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] aggregate 192.213.0.0 255.255.0.0
```

In BGP-VPN instance view, create a summary of 192.213.0.0/16 in BGP routing table. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] aggregate 192.213.0.0 255.255.0.0
```

balance (BGP/BGP-VPN instance view)

Syntax

balance *number*

undo balance

View

BGP view, VPN instance view

Default level

2: System level

Parameters

number: Number of BGP routes for load balancing, in the range of 1 to 8. When it is set to 1, load balancing is disabled.

Description

Use **balance** to configure the number of BGP routes for load balancing.

Use **undo balance** to disable load balancing.

By default, no load balancing is configured.

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing using route selection rules.

Related commands: **display bgp routing-table**.

Examples

In BGP view, set the number of routes participating in BGP load balancing to 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] balance 2
```

In BGP-VPN instance view, set the number of routes participating in BGP load balancing to 2. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] balance 2
```

bestroute as-path-neglect (BGP/BGP-VPN instance view)

Syntax

bestroute as-path-neglect

undo bestroute as-path-neglect

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

None

Description

Use **bestroute as-path-neglect** to configure BGP not to consider the AS_PATH during best route selection.

Use **undo bestroute as-path-neglect** to configure BGP to consider the AS_PATH during best route selection.

By default, BGP considers the AS_PATH during best route selection.

Examples

In BGP view, ignore AS_PATH in route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute as-path-neglect
```

In BGP-VPN instance view, ignore AS_PATH in route selection. (The VPN has been created.)


```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] bestroute as-path-neglect
```

bestroute compare-med (BGP/BGP-VPN instance view)

Syntax

```
bestroute compare-med
undo bestroute compare-med
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

None

Description

Use **bestroute compare-med** to enable the comparison of the MED for routes on a per-AS basis.

Use **undo bestroute compare-med** to disable this comparison.

This comparison is not enabled by default.

Examples

In BGP view, enable the comparison of MEDs for routes on a per-AS basis when selecting the best route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute compare-med
```

In BGP-VPN instance view, enable the comparison of MED for routes on a per-AS basis when selecting the best route. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] bestroute compare-med
```

bestroute med-confederation (BGP/BGP-VPN instance view)

Syntax

```
bestroute med-confederation
undo bestroute med-confederation
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

None

Description

Use **bestroute med-confederation** to enable the comparison of the MED for paths from confederation peers during best route selection.

Use **undo bestroute med-confederation** to disable the comparison.

The comparison is not enabled by default.

The system only compares MED values for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

Examples

In BGP view, enable the comparison of the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute med-confederation
```

In BGP-VPN instance view, enable the comparison of the MED for paths from peers within the confederation. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] bestroute med-confederation
```

bgp

Syntax

bgp *as-number*

undo bgp [*as-number*]

View

System view

Default level

2: System level

Parameters

as-number: Specifies the local AS number from 1 to 4294967295.

Description

Use **bgp** to enable BGP and enter the BGP view.

Use **undo bgp** to disable BGP.

By default, BGP is not enabled.

Examples

Enable BGP and set local AS number to 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp]
```

compare-different-as-med (BGP/BGP-VPN instance view)

Syntax

compare-different-as-med

undo compare-different-as-med

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

None

Description

Use **compare-different-as-med** to enable the comparison of the MED for paths from peers in different ASs.

Use **undo compare-different-as-med** to disable the comparison.

The comparison is disabled by default.

If several paths to one destination are available, the path with the smallest MED is selected.

Do not use this command unless associated ASs adopt the same IGP protocol and routing selection method.

Examples

In BGP view, enable the comparison of the MED for paths from peers in different ASs.

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] compare-different-as-med
```

In BGP-VPN instance view, enable the comparison of the MED for paths from peers in different Ass. (The VPN has been created.)

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv4-family vpn-instance vpn1
```

```
[Sysname-bgp-ipv4-vpn1] compare-different-as-med
```

confederation id

Syntax

confederation id *as-number*

undo confederation id

View

BGP view

Default level

2: System level

Parameters

as-number: Number of the AS that contains multiple sub-ASs, in the range of 1 to 4294967295.

Description

Use **confederation id** to configure a confederation ID.

Use **undo confederation id** to remove a specified confederation.

By default, no confederation ID is configured.

Configuring a confederation can reduce IBGP connections in a large AS. You can split the AS into several sub-ASs, and each sub-AS remains fully meshed. These sub-ASs form a confederation. Key IGP attributes of a route, such as the next hop, MED, local preference, are not discarded when crossing each sub-AS. The sub-ASs still look like a whole from the perspective of other ASs. This can ensure the integrity of the former AS, and solve the problem of too many IBGP connections in the AS.

Related commands: **confederation nonstandard** and **confederation peer-as**.

Examples

Confederation 9 consists of four sub-ASs numbered 38, 39, 40 and 41. The peer 10.1.1.1 is a member of the confederation and the peer 200.1.1.1 is outside of the confederation. Take sub AS 41 as an example.

```
<Sysname> system-view
[Sysname] bgp 41
[Sysname-bgp] confederation id 9
[Sysname-bgp] confederation peer-as 38 39 40
[Sysname-bgp] group Confed38 external
[Sysname-bgp] peer Confed38 as-number 38
[Sysname-bgp] peer 10.1.1.1 group Confed38
[Sysname-bgp] group Remote98 external
[Sysname-bgp] peer Remote98 as-number 98
[Sysname-bgp] peer 200.1.1.1 group Remote98
```

confederation nonstandard

Syntax

confederation nonstandard

undo confederation nonstandard

View

BGP view

Default level

2: System level

Parameters

None

Description

Use **confederation nonstandard** to make the router compatible with routers not compliant with RFC 3065 in the confederation.

Use **undo confederation nonstandard** to restore the default.

By default, all routers in the confederation comply with RFC 3065.

All devices should be configured with this command to interact with those nonstandard devices in the confederation.

Related commands: **confederation id** and **confederation peer-as**.

Examples

```
# AS 100 contains routers not compliant with RFC 3065 and comprises two sub-ASs, 64000 and 65000.
```

```
<Sysname> system-view
[Sysname] bgp 64000
[Sysname-bgp] confederation id 100
[Sysname-bgp] confederation peer-as 65000
[Sysname-bgp] confederation nonstandard
```

confederation peer-as

Syntax

```
confederation peer-as as-number-list
undo confederation peer-as [ as-number-list ]
```

View

BGP view

Default level

2: System level

Parameters

as-number-list: Sub-AS number list. Up to 32 sub-ASs can be configured in one command line. The expression is *as-number-list* = *as-number* &<1-32>, in which *as-number* specifies a sub-AS number, and &<1-32> indicates up to 32 numbers can be specified.

Description

Use **confederation peer-as** to specify confederation peer sub-ASs.

Use **undo confederation peer-as** to remove specified confederation peer sub-ASs.

By default, no confederation peer sub-ASs are configured.

Before this configuration, you must use the **confederation id** command to specify the confederation for the sub-ASs.

If the **undo confederation peer-as** command without the *as-number-list* argument is used, all confederation peer sub-ASs are removed.

Related commands: **confederation nonstandard** and **confederation id**.

Examples

```
# Specify confederation peer sub ASs 2000 and 2001.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] confederation id 10
[Sysname-bgp] confederation peer-as 2000 2001
```

dampening (BGP/BGP-VPN instance view)

Syntax

dampening [*half-life-reachable* *half-life-unreachable* *reuse* *suppress* *ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

half-life-reachable: Specifies a half-life for active routes from 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Specifies a half-life for suppressed routes from 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Specifies a reuse threshold value for suppressed routes from 1 to 20000. A suppressed route whose penalty value decreases under the value is reused. By default, the reuse value is 750.

suppress: Specifies a suppression threshold from 1 to 20000. The route with a penalty value higher than the threshold is suppressed. The default value is 2000.

ceiling: Specifies a ceiling penalty value from 1001 to 20000. The value must be bigger than the *suppress* value. By default, the value is 16000.

route-policy-name: Routing policy name, a case-sensitive string of 1 to 63 characters.

half-life-reachable, *half-life-unreachable*, *reuse*, *suppress* and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified.

Description

Use **dampening** to enable BGP route dampening, configure dampening parameters, or both.

Use **undo dampening** to disable route dampening.

By default, no route dampening is configured.

The command dampens only EBGp routes rather than IBGP routes.

Related commands: **reset bgp dampening**, **reset bgp flap-info**, **display bgp routing-table dampened**, **display bgp routing-table dampening parameter**, and **display bgp routing-table flap-info**.

Examples

In BGP view, configure BGP route dampening.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] dampening 15 15 1000 2000 10000
```

In BGP-VPN instance view, configure BGP route dampening. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] dampening 15 15 1000 2000 10000
```

default ipv4-unicast

Syntax

```
default ipv4-unicast
undo default ipv4-unicast
```

View

BGP view

Default level

2: System level

Parameters

None

Description

Use **default ipv4-unicast** to enable the default use of IPv4 unicast address family for the peers that are established using the **peer as-number** command.

Use **undo default ipv4-unicast** to disable the default use of IPv4 unicast address family for the peers that are established using the **peer as-number** command.

The use of IPv4 unicast address family is enabled by default.

The **default ipv4-unicast** or **undo default ipv4-unicast** command applies to only BGP peers that are established after it is executed.

The **default ipv4-unicast** or **undo default ipv4-unicast** command applies to only BGP peers that are established using the **peer as-number** command.

After executing the **undo default ipv4-unicast** command, you can use the **peer enable** command to enable the use of IPv4 address family for a peer.

Examples

```
# Enable the default use of IPv4 unicast address family for the peers that are established using the peer
as-number command.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default ipv4-unicast
```

default local-preference (BGP/BGP-VPN instance view)

Syntax

```
default local-preference value
undo default local-preference
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

value: Default local preference, in the range of 0 to 4294967295. The larger the value is, the higher the preference is.

Description

Use **default local-preference** to configure the default local preference.

Use **undo default local-preference** to restore the default value.

By default, the default local preference is 100.

Using this command can affect BGP route selection.

Examples

```
# In BGP view, set the default local preference to 180.
```

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] default local-preference 180
```

```
# In BGP-VPN instance view, set the default local preference to 180. (The VPN has been created.)
```

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv4-family vpn-instance vpn1
```

```
[Sysname-bgp-ipv4-vpn1] default local-preference 180
```

default med (BGP/BGP-VPN instance view)

Syntax

```
default med med-value
```

```
undo default med
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

med-value: Default MED value, in the range of 0 to 4294967295.

Description

Use **default med** to specify a default MED value.

Use **undo default med** to restore the default.

By default, the default *med-value* is 0.

Multi-exit discriminator (MED) is an external metric for routes. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a router running BGP obtains several routes with an identical destination but different next-hops from various external peers, it will select the best route depending on the MED value. In the case that all other conditions are the same, the system first selects the route with the smallest MED as the best external route.

Examples

```
# In BGP view, configure the default MED as 25.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default med 25

# In BGP-VPN instance view, configure the default MED as 25. (The VPN has been created.)
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] default med 25
```

default-route imported (BGP/BGP-VPN instance view)

Syntax

```
default-route imported
undo default-route imported
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

None

Description

Use **default-route imported** to allow default route redistribution into the BGP routing table.

Use **undo default-route imported** to disallow the redistribution.

By default, default route redistribution is not allowed.

You must use the **default-route imported** command together with the **import-route** command to redistribute default routes from other protocols.

Related commands: **import-route**.

Examples

```
# In BGP view, allow default route redistribution from OSPF into BGP.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default-route imported
[Sysname-bgp] import-route ospf 1

# In BGP-VPN instance view, enable redistributing default route from OSPF into BGP. (The VPN has been created.)
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] default-route imported
[Sysname-bgp-ipv4-vpn1] import-route ospf 1
```

display bgp group

Syntax

```
display bgp group [ group-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

group-name: Peer group name, a string of 1 to 47 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp group** to display peer group information.

Examples

```
# Display the information of the peer group aaa.
```

```
<Sysname> display bgp group aaa
```

```
BGP peer-group is aaa
Remote AS 200
Type : external
Maximum allowed prefix number: 4294967295
Threshold: 75%
Configured hold timer value: 180
Keepalive timer value: 60
Minimum time between advertisement runs is 30 seconds
Peer Preferred Value: 0
No routing policy is configured
Members:
Peer          AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
-----
2.2.2.1      200      0        0        0      0  00:00:35  Active
```

Table 42 Command output

Field	Description
BGP peer-group	Name of the BGP peer group
Remote AS	AS number of peer group

Field	Description
type	Type of the BGP peer group: IBGP or EBGP
Maximum allowed prefix number	Maximum prefixes allowed to receive from the peer group
Threshold	Percentage of received prefixes from the peer group to maximum prefixes allowed to receive from the peer group; If the percentage is reached, the system generates alarm messages.
Configured hold timer value	Holdtime interval
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum interval for route advertisements
Peer Preferred Value	Preferred value specified for the routes from the peer
No routing policy is configured	No routing policy is configured.
Members	Detailed information of the members in the peer group
Peer	IPv4 address of the peer
V	BGP version running on the peer
AS	AS number of the peer
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	Lasting time of the session/Lasting time of the current state (when no session is established)
State	State machine state of the peer

display bgp network

Syntax

```
display bgp network [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp network** to display routing information advertised with the **network** command.

Examples

Display routing information advertised with the **network** command.

```
<Sysname> display bgp network
```

```
BGP Local Router ID is 10.1.4.2.
Local AS Number is 400.
Network          Mask          Route-policy    Short-cut
100.1.2.0        255.255.255.0
100.1.1.0        255.255.255.0          Short-cut
```

Table 43 Command output

Field	Description
BGP Local Router ID	BGP Local Router ID
Local AS Number	Local AS Number
Network	Network address
Mask	Mask
Route-policy	Routing policy
Short-cut	Short-cut route

display bgp paths

Syntax

```
display bgp paths [ as-regular-expression | | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

as-regular-expression: AS path regular expression, a string of 1 to 80 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp paths** to display information about BGP AS paths.

Examples

```
# Display information about BGP AS paths with AS number starting from 200.
```

```
<Sysname> display bgp paths ^200
```

Address	Hash	Refcount	MED	Path/Origin
0x5917100	11	1	0	200 300i

Table 44 Command output

Field	Description
Address	Route address in the local database, in dotted hexadecimal notation.
Hash	Hash index.
Refcount	Count of routes that reference the path.
MED	MED of the path.
Path	AS_PATH attribute of the path, recording the ASs it has passed to avoid routing loops.
Origin	ORIGIN attribute of the path: <ul style="list-style-type: none">• i—Indicates the route is interior to the AS.• Summary routes and routes defined using the network command are considered IGP routes.• e—Indicates that a route is learned from the exterior gateway protocol (EGP).• ?—Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means.

display bgp peer

Syntax

```
display bgp peer [ ip-address { log-info | verbose } ] [ group-name log-info | verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ip-address: IP address of an peer to be displayed, in dotted decimal notation.

group-name: Name of a peer group to be displayed, a string of 1 to 47 characters.

log-info: Displays the log information of the specified peer.

verbose: Displays the detailed information of the peer/peer group.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp peer** to display peer/peer group information.

Examples

```
# Display the detailed information of the peer 10.110.25.20.
```

```
<Sysname> display bgp peer 10.110.25.20 verbose
```

```
Peer: 10.110.25.20 Local: 2.2.2.2
Type: EBGp link
BGP version 4, remote router ID 1.1.1.1
BGP current state: Established, Up for 00h01m51s
BGP current event: RecvKeepalive
BGP last state: OpenConfirm
Port: Local - 1029 Remote - 179
Configured: Active Hold Time: 180 sec Keepalive Time: 60 sec
Received : Active Hold Time: 180 sec
Negotiated: Active Hold Time: 180 sec Keepalive Time: 60 sec
Peer optional capabilities:
Peer support bgp multi-protocol extended
Peer support bgp route refresh capability
Address family IPv4 Unicast: advertised and received
```

```
Received: Total 5 messages, Update messages 1
Sent: Total 4 messages, Update messages 0
Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisement runs is 30 seconds
Optional capabilities:
Route refresh capability has been enabled
ORF advertise capability based on prefix (type 64):
Local: both
Negotiated: send
Peer Preferred Value: 0
BFD: Enabled
```

```
Routing policy configured:
No routing policy is configured
```

Table 45 Command output

Field	Description
Peer	IP address of the peer.
Local	Local router ID.

Field	Description
Type	Peer type.
BGP version	BGP version.
remote router ID	Router ID of the peer.
BGP current state	Current state of the peer.
BGP current event	Current event of the peer.
BGP last state	Previous state of the peer.
Port	TCP port numbers of the local router and its peer.
Configured: Active Hold Time	Local holdtime interval.
Keepalive Time	Local keepalive interval.
Received: Active Hold Time	Remote holdtime interval.
Negotiated: Active Hold Time	Negotiated holdtime interval.
Peer optional capabilities	Optional capabilities supported by the peer, including BGP multiprotocol extensions and route refresh.
Address family IPv4 Unicast	Routes are advertised and received in IPv4 unicasts.
Received	Total numbers of received packets and updates.
Sent	Total numbers of sent packets and updates.
Maximum allowed prefix number	Maximum allowed prefix number.
Threshold	Percentage of received prefixes from the peer group to maximum prefixes allowed to receive from the peer group; If the percentage is reached, the system generates alarm messages.
Minimum time between advertisement runs	Minimum route advertisement interval.
Optional capabilities	Optional capabilities enabled by the peer.
Route refresh capability has been enabled	The route-refresh capability has been enabled.
ORF advertise capability based on prefix (type 64):	The BGP peer supports the ORF capability based on IP prefix. The capability value is 64.
Local: both	The local BGP router supports both the ORF sending and receiving capabilities.
Negotiated: send	Negotiation result: The local BGP router can send Router-refresh messages carrying the ORF information, and the peer can receive Router-refresh messages carrying the ORF information. (This field is not displayed if neither the send nor the receive capability is supported.)
Peer Preferred Value	Preferred value specified for the routes from the peer.
BFD	BFD state: enabled or disabled.
Routing policy configured	Local routing policy.

```
# Display the log information of the peer 10.110.25.20.
<sysname> display bgp peer 10.110.25.20 log-info
```

Peer : 10.110.25.20

Date	Time	State	Notification Error/SubError
10-Jul-2008	15:46:17	Down	Send Notification with Error 1/1 Message Header Error/Connection Not Synchronized
10-Jul-2008	09:23:00	Up	
10-Jul-2008	07:46:17	Down	Receive Notification with Error 3/2 UPDATE Message Error/Unsupported optional Parameter
10-Jul-2008	06:23:00	Up	
10-Jul-2008	05:46:17	Down	Send Notification with Error 6/4 Cease/Administrative Reset

Table 46 Command output

Field	Description
Peer	IP address of the peer.
Date	Date on which the Notification was sent or received.
Time	Time at which the Notification was sent or received.
State	BGP session state, which can be: <ul style="list-style-type: none">• Up—Indicates the BGP session is up.• Down—Indicates the BGP session is down.
Notification	Notification message.
Error/SubError	<ul style="list-style-type: none">• Error—Refers to the error code, which identifies the type of the Notification.• SubError—Refers to the error subcode of the Notification, which identifies the specific information about the reported error.

display bgp peer received ip-prefix

Syntax

```
display bgp peer ip-address received ip-prefix [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ip-address: IP address of a BGP peer.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp peer received ip-prefix** to display the prefix information in the ORF packet from the specified BGP peer.

Examples

```
# Display the prefix information in the ORF packet from the BGP peer 10.110.25.20.
```

```
<Sysname> display bgp peer 10.110.25.20 received ip-prefix
```

```
ORF ip-prefix entries: 2
```

```
ge: greater-equal  le: less-equal
```

index	rule	prefix	ge	le
10	permit	111.111.111.0/24	26	32
20	deny	2.1.1.0/24	26	32

Table 47 Command output

Field	Description
ORF ip-prefix entries	Number of ORF prefix entries
index	Index of a prefix entry
rule	Matching rule of the prefix
prefix	Prefix information
ge	greater-equal, indicating the mask length must be greater than or equal to the specific value.
le	less-equal, indicating the mask length must be less than or equal to the specific value.

display bgp routing-table

Syntax

```
display bgp routing-table [ ip-address [ { mask | mask-length } [ longer-prefixes ] ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ip-address: Destination IP address.

mask: Network mask, in dotted decimal notation.

mask-length: Mask length, in the range of 0 to 32.

longer-prefixes: Displays the routing entries selected through the following steps:

1. AND the specified destination IP address with the specified mask.
2. AND the destination IP address of each route with the specified mask.
3. Find the calculation results of 2) that match the result of 1) and display the route with the longest mask among the matching routes that have a mask shorter than or equal to the specified mask.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp routing-table** to display specified BGP routing information in the BGP routing table.

Examples

```
# Display BGP routing table information.
```

```
<Sysname> display bgp routing-table
```

```
Total Number of Routes: 1
```

```
BGP Local router ID is 10.10.10.1
```

```
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 40.40.40.0/24	20.20.20.1	0		0	200 300i

Table 48 Command output

Field	Description
Total Number of Routes	Total Number of Routes
BGP Local router ID	BGP local router ID
Status codes	Status codes: <ul style="list-style-type: none"> • * - valid—Valid route. • ^ - VPNv4 best—Best VPNv4 route. • > - best—Best route. • d - damped—Dampened route. • h - history—History route. • i - internal—Internal route. • s - suppressed—Suppressed route. • S - Stale—Stale route.

Field	Description
Origin	<p>ORIGIN attributes, including:</p> <ul style="list-style-type: none"> • i – IGP—Originated in the AS. • e – EGP—Learned through EGP. • ? – incomplete—Learned by some other means.
Network	Destination network address
Next Hop	Next hop IP address
MED	Multi-Exit Discriminator
LocPrf	Local preference value
PrefVal	Preferred value of the route
Path	AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops
PrefVal	Preferred value
Ogn	<p>ORIGIN attribute of the route, which can be one of the following values:</p> <ul style="list-style-type: none"> • i—Indicates that the route is interior to the AS. • Summary routes and the routes injected with the network command are considered IGP routes. • e—Indicates that the route is learned from the Exterior Gateway Protocol (EGP). • ?—Short for INCOMPLETE. It indicates that the origin of the route is unknown and the route is learned by other means.

display bgp routing-table as-path-acl

Syntax

```
display bgp routing-table as-path-acl as-path-acl-number [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

as-path-acl-number: Displays routing information permitted by the AS path list, which is specified with a number from 1 to 256.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp routing-table as-path-acl** to display BGP routes permitted by an AS path list.

Examples

```
# Display BGP routes permitted by AS path list 1.
```

```
<Sysname> display bgp routing-table as-path-acl 1
```

```
BGP Local router ID is 20.20.20.1
```

```
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 40.40.40.0/24	30.30.30.1	0		0	300i

For description of the fields, see [Table 49](#).

display bgp routing-table cidr

Syntax

```
display bgp routing-table cidr [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp routing-table cidr** to display BGP CIDR (Classless Inter-Domain Routing) routing information.

Examples

```
# Display BGP CIDR routing information.
```

```
<Sysname> display bgp routing-table cidr
```

```
Total Number of Routes: 1
```

```
BGP Local router ID is 20.20.20.1
```

```
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
```

h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 40.40.40.0/24	30.30.30.1	0		0	300i

For description of the fields, see [Table 49](#).

display bgp routing-table community

Syntax

```
display bgp routing-table community [ aa:nn&<1-13> ] [ no-advertise | no-export | no-export-subconfed ] * [ whole-match ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

aa:nn: Community number. Both aa and nn are in the range of 0 to 65535.

&<1-13>: Argument before it can be entered up to 13 times.

no-advertise: Displays BGP routes that cannot be advertised to any peer.

no-export: Displays BGP routes that cannot be advertised out the AS. If a confederation is configured, it displays routes that cannot be advertised out the confederation, but can be advertised to other sub ASs in the confederation.

no-export-subconfed: Displays BGP routes that cannot be advertised out the AS or to other sub ASs in the configured confederation.

whole-match: Displays the BGP routes exactly matching the specified COMMUNITY attribute.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp routing-table community** to display BGP routing information with the specified BGP COMMUNITY attribute.

Examples

```
# Display BGP routing information with the specified BGP community.
```

```
<Sysname> display bgp routing-table community 11:22
```

```
BGP Local router ID is 10.10.10.1
```

```
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 10.10.10.0/24	0.0.0.0	0		0	i
*> 40.40.40.0/24	20.20.20.1	0		0	200 300i

For description of the fields, [Table 49](#).

display bgp routing-table community-list

Syntax

```
display bgp routing-table community-list { { basic-community-list-number | comm-list-name }
[ whole-match ] | adv-community-list-number } [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

basic-community-list-number: Specifies a basic community-list number from 1 to 99.

adv-community-list-number: Specifies an advanced community-list number from 100 to 199.

comm-list-name: Community list name, a string of 1 to 31 characters (not all are numbers).

whole-match: Displays routes exactly matching the specified *basic-community-list*.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp routing-table community-list** to display BGP routing information matching the specified BGP community list.

Examples

```
# Display BGP routing information matching BGP community list 100.
```

```
<Sysname> display bgp routing-table community-list 100
```

```
BGP Local router ID is 1.2.3.4
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
              h - history, i - internal, s - suppressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
```

	Network	NextHop	Metric	LocPrf	PrefVal	Path
*>	3.3.3.0/30	1.2.3.4			0	?
*>	4.4.0.0/20	1.2.3.4			0	?
*>	4.5.6.0/26	1.2.3.4			0	?

For description of the fields, see [Table 49](#).

display bgp routing-table dampened

Syntax

```
display bgp routing-table dampened [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp routing-table dampened** to display dampened BGP routes.

Examples

```
# Display dampened BGP routes.
```

```
<Sysname> display bgp routing-table dampened
```

```
BGP Local router ID is 2.2.2.2
Status codes: * - valid, ^- VPNv4 best, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete
```

Network	From	Reuse	Path/Origin
*d 77.0.0.0	12.1.1.1	00:29:20	100?

Table 49 Command output

Field	Description
From	IP address from which the route was received
Reuse	Reuse time of the route

For description of the other fields, see [Table 49](#).

display bgp routing-table dampening parameter

Syntax

```
display bgp routing-table dampening parameter [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp routing-table dampening parameter** to display BGP route dampening parameters.

Related commands: **dampening**.

Examples

```
# Display BGP route dampening parameters.
```

```
<Sysname> display bgp routing-table dampening parameter
Maximum Suppress Time(in second) : 3069
Ceiling Value                    : 16000
Reuse Value                      : 750
Reach HalfLife Time(in second)  : 900
Unreach HalfLife Time(in second): 900
Suppress-Limit                  : 2000
```

Table 50 Command output

Field	Description
Maximum Suppress Time	Maximum Suppress Time
Ceiling Value	Ceiling penalty value
Reuse Value	Reuse value
Reach HalfLife Time(in second)	Half-life time of active routes
Unreach HalfLife Time(in second)	Half-life time of inactive routes
Suppress-Limit	Limit for a route to be suppressed

display bgp routing-table different-origin-as

Syntax

```
display bgp routing-table different-origin-as [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp routing-table different-origin-as** to display BGP routes originating from different autonomous systems.

Examples

```
# Display BGP routes originating from different ASs.
```

```
<Sysname> display bgp routing-table different-origin-as
```

```
BGP Local router ID is 2.2.2.2
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete
```

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	55.0.0.0	12.1.1.1	0		0	100?
*		14.1.1.2	0		0	300?

For description of the fields, see [Table 49](#).

display bgp routing-table flap-info

Syntax

```
display bgp routing-table flap-info [ regular-expression as-regular-expression | [ as-path-acl as-path-acl-number | ip-address [ { mask | mask-length } [ longer-match ] ] ] [ | { begin | exclude | include } regular-expression ] ]
```

View

Any view

Default level

1: Monitor level

Parameters

as-regular-expression: Displays route flap information that matches the AS path regular expression, which is a string of 1 to 80 characters.

as-path-acl-number: Displays route flap information matching the AS path list. The number is in the range of 1 to 256.

ip-address: Destination IP address.

mask: Mask, in dotted decimal notation.

mask-length: Mask length, in the range of 0 to 32.

longer-match: Matches the longest prefix.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp routing-table flap-info** to display BGP route flap statistics.

Examples

```
# Display BGP route flap statistics.
```

```
<Sysname> display bgp routing-table flap-info
```

```
BGP Local router ID is 2.2.2.2
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

      Network          From          Flaps  Duration          Reuse  Path/Origin
* >  55.0.0.0          12.1.1.1      2      00:00:16          100?
*d   77.0.0.0          12.1.1.1      5      00:34:02  00:27:08  100?
```

Table 51 Command output

Field	Description
From	Source IP address of the route
Flaps	Number of routing flaps
Duration	Duration time of the flap route
Reuse	Reuse time of the route

For description of the other fields, see [Table 49](#).

display bgp routing-table label

Syntax

```
display bgp routing-table label [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp routing-table label** to display labeled BGP routing information.

Examples

Display labeled BGP routing information.

```
<Sysname> display bgp routing-table label
```

```
BGP Local router ID is 6.6.6.7
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 2
```

	Network	NextHop	In/Out Label
*>	4.4.4.4/32	127.0.0.1	3/NULL
*>	5.5.5.5/32	1.1.1.1	NULL/1024

The In/Out Label field refers to the inbound/outbound label. For the description of other fields, see [Table 49](#).

display bgp routing-table peer

Syntax

```
display bgp routing-table peer ip-address { advertised-routes | received-routes } [ network-address [ mask | mask-length ] | statistic ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ip-address: IP address of a peer.

advertised-routes: Displays routing information advertised to the specified peer.

received-routes: Displays routing information received from the specified peer.

network-address: IP address of the destination network.

mask: Mask of the destination network, in dotted decimal notation.

mask-length: Mask length, in the range of 0 to 32.

statistic: Displays route statistics.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp routing-table peer** to display BGP routing information advertised to or received from the specified BGP peer.

Related commands: **display bgp peer**.

Examples

```
# Display BGP routing information advertised to BGP peer 20.20.20.1.
```

```
<Sysname> display bgp routing-table peer 20.20.20.1 advertised-routes
```

```
Total Number of Routes: 2
```

```
BGP Local router ID is 30.30.30.1
```

```
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	30.30.30.0/24	0.0.0.0	0		0	i
*>	40.40.40.0/24	0.0.0.0	0		0	i

For description of the fields, see [Table 49](#).

display bgp routing-table regular-expression

Syntax

```
display bgp routing-table regular-expression as-regular-expression
```

View

Any view

Default level

1: Monitor level

Parameters

as-regular-expression: AS path regular expression, a string of 1 to 80 characters.

Description

Use **display bgp routing-table regular-expression** to display BGP routing information matching the specified AS path regular expression.

Examples

Display BGP routing information with AS number ended with 300.

```
<Sysname> display bgp routing-table regular-expression 300$
```

```
BGP Local router ID is 20.20.20.1
```

```
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 40.40.40.0/24	30.30.30.1	0		0	300i

For description of the fields, see [Table 49](#).

display bgp routing-table statistic

Syntax

```
display bgp routing-table statistic [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp routing-table statistic** to display BGP routing statistics.

Examples

```
# Display BGP routing statistics.
<Sysname> display bgp routing-table statistic

Total Number of Routes: 4
```

display router id

Syntax

```
display router id [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display router id** to display the global router ID.

Examples

```
# Display the global router ID.
<Sysname> display router id
    Configured router ID is 1.1.1.1
```

ebgp-interface-sensitive

Syntax

```
ebgp-interface-sensitive
undo ebgp-interface-sensitive
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

None

Description

Use **ebgp-interface-sensitive** to enable the clearing of EBGP session on any interface that becomes down.

Use **undo ebgp-interface-sensitive** to disable the function.

This function is enabled by default.

Examples

In BGP view, enable the clearing of EBGP session on any interface that becomes down.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ebgp-interface-sensitive
```

In BGP-VPN instance view, enable the clearing of EBGP session on any interface that becomes down. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] ebgp-interface-sensitive
```

filter-policy export (BGP/BGP-VPN instance view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

undo filter-policy export [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

acl-number: Number of an ACL used to filter outgoing routing information, ranging from 2000 to 3999.

ip-prefix-name: Name of an IP prefix list used to filter outgoing routing information, a string of 1 to 19 characters.

direct: Filters direct routes.

isis process-id: Filters outgoing routes redistributed from an ISIS process. The ID is in the range of 1 to 65535.

ospf process-id: Filters outgoing routes redistributed from the OSPF process with an ID from 1 to 65535.

rip process-id: Filters outgoing routes redistributed from a RIP process. The ID is in the range of 1 to 65535.

static: Filters static routes.

Description

Use **filter-policy export** to configure the filtering of outgoing routes.

Use **undo filter-policy export** to remove the filtering.

If no routing protocol is specified, all outgoing routes are filtered.

By default, no route filtering is configured.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command, the ACL should be configured with the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command to deny/permit a route with the specified destination, or with the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard destination dest-addr dest-wildcard* command to deny/permit a route with the specified destination and mask. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route (the subnet mask must be valid; otherwise, the configuration is ineffective).

Examples

In BGP view, reference ACL 2000 to filter all outgoing routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] filter-policy 2000 export
```

In BGP-VPN instance view, reference ACL 2000 to filter all outgoing routes. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] filter-policy 2000 export
```

Configure ACL 3000 to permit only route 113.0.0.0/16 to pass, and reference ACL 3000 to filter outgoing routes.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0
[Sysname-acl-adv-3000] rule 100 deny ip
[Sysname-acl-adv-3000] quit
[Sysname] bgp 100
[Sysname-bgp] filter-policy 3000 export
```

filter-policy import (BGP/BGP-VPN instance view)

Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name } import
undo filter-policy import
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

acl-number: Number of an ACL used to filter incoming routing information, ranging from 2000 to 3999.

ip-prefix-name: Name of an IP prefix list used to filter incoming routing information, a string of 1 to 19 characters.

Description

Use **filter-policy import** to configure the filtering of incoming routing information.

Use **undo filter-policy import** to disable the filtering.

By default, incoming routing information is not filtered.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command, the ACL should be configured with the **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard** command to deny/permit a route with the specified destination, or with the **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard destination dest-addr dest-wildcard** command to deny/permit a route with the specified destination and mask. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route (the subnet mask must be valid; otherwise, the configuration is ineffective).

Examples

In BGP view, reference ACL 2000 to filter incoming routing information.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] filter-policy 2000 import
```

In BGP-VPN instance view, reference ACL 2000 to filter incoming routing information. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] filter-policy 2000 import
```

Configure ACL 3000 to permit only route 113.0.0.0/16 to pass, and reference ACL 3000 to filter incoming route information.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0
[Sysname-acl-adv-3000] rule 100 deny ip
[Sysname-acl-adv-3000] quit
[Sysname] bgp 100
[Sysname-bgp] filter-policy 3000 import
```

graceful-restart (BGP view)

Syntax

graceful-restart

undo graceful-restart

View

BGP view

Default level

2: System level

Parameters

None

Description

Use **graceful-restart** to enable BGP Graceful Restart capability.

Use **undo graceful-restart** to disable BGP Graceful Restart capability.

By default, BGP Graceful Restart capability is disabled.

During main and backup boards switchover, a GR-capable BGP speaker can maintain the packet forwarding table. During restart, it may not maintain the forwarding table.

Examples

```
# Enable the Graceful Restart capability for BGP process 100.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] graceful-restart
```

graceful-restart timer restart

Syntax

graceful-restart timer restart *timer*

undo graceful-restart timer restart

View

BGP view

Default level

2: System level

Parameters

timer: Maximum time for a peer to reestablish a BGP session, in the range of 3 to 600 seconds.

Description

Use **graceful-restart timer restart** to configure the maximum time for a peer to reestablish a BGP session.

Use **undo graceful-restart timer restart** to restore the default.

By default, the maximum time for a peer to reestablish a BGP session is 150 seconds.

Before configuring this command, you must enable the BGP Graceful Restart capability.

Related commands: **graceful-restart**.

Examples

```
# Configure the maximum time for a peer to reestablish a BGP session as 300 seconds.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] graceful-restart timer restart 300
```

graceful-restart timer wait-for-rib

Syntax

```
graceful-restart timer wait-for-rib timer  
undo graceful-restart timer wait-for-rib
```

View

BGP view

Default level

2: System level

Parameters

timer: Time to wait for the End-of-RIB marker, in the range of 3 to 300 seconds.

Description

Use **graceful-restart timer wait-for-rib** to configure the time to wait for the End-of-RIB marker.

Use **undo graceful-restart timer wait-for-rib** to restore the default.

By default, the time to wait for the End-of-RIB marker is 180 seconds.

After a BGP session has been successfully (re)established, the End-of-RIB marker must be received within the time specified with this command.

Using this command can speed up route convergence.

Before configuring this command, you must enable the BGP Graceful Restart capability.

Related commands: **graceful-restart**.

Examples

```
# Set the time to wait for the End-of-RIB marker to 100 seconds.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] graceful-restart timer wait-for-rib 100
```

group (BGP/BGP-VPN instance view)

Syntax

```
group group-name [ external | internal ]  
undo group group-name
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

external: Creates an EBGP peer group, which can be the group of another sub AS in a confederation.

internal: Creates an IBGP peer group.

Description

Use **group** to create a peer group.

Use **undo group** to delete a peer group.

An IBGP peer group is created if neither **internal** nor **external** is specified.

Examples

In BGP view, create an EBGP peer group **test** with AS number 200, and add EBGP peers 10.1.1.1 and 10.1.2.1 into the group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] peer 10.1.1.1 group test
[Sysname-bgp] peer 10.1.2.1 group test
```

In BGP-VPN instance view, create an EBGP peer group **test** with AS number 200, and add EBGP peers 10.1.1.1 and 10.1.2.1 into the group. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] group test external
[Sysname-bgp-ipv4-vpn1] peer test as-number 200
[Sysname-bgp-ipv4-vpn1] peer 10.1.1.1 group test
[Sysname-bgp-ipv4-vpn1] peer 10.1.2.1 group test
```

ignore-first-as

Syntax

ignore-first-as

undo ignore-first-as

View

BGP view

Parameters

None

Description

Use **ignore-first-as** to configure BGP to ignore the first AS number of EBGP route updates.

Use **undo ignore-first-as** to configure BGP to check the first AS number of EBGP route updates.

By default, BGP checks the first AS number of a received EBGP route update. If the first AS number is not that of the BGP peer, the BGP router discards the route update.

Examples

Configure BGP to ignore the first AS number of EBGP route updates.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ignore-first-as
```

import-route (BGP/BGP-VPN instance view)

Syntax

```
import-route protocol [ { process-id | all-processes } [ allow-direct | med med-value | route-policy route-policy-name ] * ]  
undo import-route protocol [ process-id | all-processes ]
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

protocol: Redistributes routes from the specified routing protocol, which can be **direct**, **isis**, **ospf**, **rip** or **static**.

process-id: Process ID, in the range of 1 to 65535. The default is 1. It is available only when the protocol is **isis**, **ospf**, or **rip**.

all-processes: Redistributes routes from all the processes of the specified protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

allow-direct: Redistributes direct routes from the specified protocol. This keyword is available only when the specified protocol is OSPF. Without this keyword, BGP does not redistribute direct routes from OSPF. If you specify the **route-policy** *route-policy-name* keyword together with the **allow-direct** keyword, make sure that no rule in the routing policy conflicts with any direct route. For example, do not configure the **if-match route-type** command for the routing policy to filter OSPF routes. Otherwise, the **allow-direct** keyword does not take effect.

med-value: Specifies a MED value for redistributed routes, ranging from 0 to 4294967295. If the argument is not specified, the cost of the redistributed route is used as its MED in the BGP routing domain.

route-policy-name: Name of a routing policy used to filter redistributed routes, a case-sensitive string of 1 to 63 characters.

Description

Use **import-route** to configure BGP to redistribute routes from a specified routing protocol and advertise redistributed routes.

Use **undo import-route** to disable route redistribution from a routing protocol.

By default, BGP does not redistribute routes from other protocols.

Only active routes can be redistributed. You can use the **display ip routing-table protocol** command to display route state information.

The ORIGIN attribute of routes redistributed with the **import-route** command is INCOMPLETE.

The **undo import-route protocol all-processes** command cancels the configuration made by the **import-route protocol all-processes** command, rather than the **import-route protocol process-id** command.

Examples

```
# In BGP view, redistribute routes from RIP.
```

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] import-route rip
# In BGP-VPN instance view, redistribute routes from RIP. (The VPN has been created.)
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] import-route rip
```

log-peer-change

Syntax

```
log-peer-change
undo log-peer-change
```

View

BGP view

Default level

2: System level

Parameters

None

Description

Use **log-peer-change** to enable the global BGP logging on peers going up and down.

Use **undo log-peer-change** to disable the function.

By default, the function is enabled.

Examples

```
# Enable BGP logging on peers going up and down.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] log-peer-change
```

network (BGP/BGP-VPN instance view)

Syntax

```
network ip-address [ mask | mask-length ] route-policy route-policy-name
undo network ip-address [ mask | mask-length ]
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

ip-address: Destination IP address.

mask: Mask of the network address, in dotted decimal notation.

mask-length: Mask length, in the range of 0 to 32.

route-policy-name: Routing policy applied to the route. The name is a case-sensitive string of 1 to 63 characters.

Description

Use **network** to inject a network to the local BGP routing table.

Use **undo network** to remove a network from the BGP routing table.

By default, no network route is injected.

The network route to be injected must exist in the local IP routing table, and using a routing policy makes route management more flexible.

The ORIGIN attribute of the network route injected with the **network** command is IGP.

Examples

```
# In BGP view, inject the network segment 10.0.0.0/16.
```

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] network 10.0.0.0 255.255.0.0
```

```
# In BGP-VPN instance view, advertise the network segment 10.0.0.0/16. (The VPN has been created.)
```

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv4-family vpn-instance vpn1
```

```
[Sysname-bgp-ipv4-vpn1] network 10.0.0.0 255.255.0.0
```

network short-cut (BGP/BGP-VPN instance view)

Syntax

```
network ip-address [ mask | mask-length ] short-cut
```

```
undo network ip-address [ mask | mask-length ] short-cut
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

ip-address: Destination IP address.

mask: Mask of the network address, in dotted decimal notation.

mask-length: Mask length, in the range of 0 to 32.

Description

Use **network short-cut** to configure an EBGP route as a shortcut route.

Use **undo network short-cut** to restore the default.

By default, a received EBGP route has a priority of 255.

The **network short-cut** command allows you configure an EBGP route as a shortcut route that has the same priority as a local route and is more likely to become the optimal route.

Examples

In BGP view, configure route 10.0.0.0/16 as a shortcut route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] network 10.0.0.0 255.255.0.0 short-cut
```

In BGP-VPN instance view, configure route 10.0.0.0/16 as a shortcut route. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] network 10.0.0.0 255.255.0.0 short-cut
```

peer advertise-community (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } advertise-community
undo peer { group-name | ip-address } advertise-community
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use **peer advertise-community** to advertise the COMMUNITY attribute to a peer/peer group.

Use **undo peer advertise-community** to disable the COMMUNITY attribute advertisement to a peer/peer group.

By default, no COMMUNITY attribute is advertised to any peer group/peer.

Related commands: **ip community-list**, **if-match community**, and **apply community**.

Examples

In BGP view, advertise the COMMUNITY attribute to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test advertise-community
```

In BGP-VPN instance view, advertise the COMMUNITY attribute to peer group **test**. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test advertise-community
```


peer advertise-ext-community (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } advertise-ext-community
undo peer { group-name | ip-address } advertise-ext-community
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use **peer advertise-ext-community** to advertise the extended community attribute to a peer/peer group.

Use **undo peer advertise-ext-community** to disable the extended community attribute advertisement to a peer/peer group.

By default, no extended community attribute is advertised to a peer/peer group.

Related commands: **ip extcommunity-list**, **if-match extcommunity**, and **apply extcommunity**.

Examples

In BGP view, advertise the extended community attribute to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test advertise-ext-community
```

In BGP-VPN view, advertise the extended community attribute to the peer group **test**. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test advertise-ext-community
```

peer allow-as-loop (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } allow-as-loop [ number ]
undo peer { group-name | ip-address } allow-as-loop
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

number: Specifies the number of times for which the local AS number can appear in routes from the peer/peer group, in the range of 1 to 10. The default number is 1.

Description

Use **peer allow-as-loop** to allow the local AS number to exist in the AS_PATH attribute of routes from a peer/peer group, and to configure the number of times the local AS number can appear.

Use **undo peer allow-as-loop** to remove the configuration.

By default, the local AS number is not allowed in routes from a peer/peer group.

Related commands: **display bgp routing-table peer**.

Examples

In BGP view, configure the number of times the local AS number can appear in AS_PATH attribute of routes from peer 1.1.1.1 as 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 allow-as-loop 2
```

In BGP-VPN instance view, configure the number of times for which the local AS number can appear in AS_PATH attribute of routes from peer 1.1.1.1 as 2. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer 1.1.1.1 allow-as-loop 2
```

peer as-number (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **as-number** *as-number*

undo peer *group-name* **as-number**

undo peer *ip-address*

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-number: AS number of the peer or peer group, in the range of 1 to 4294967295.

Description

Use **peer** { *group-name* | *ip-address* } **as-number** *as-number* to specify a peer/peer group with an AS number.

Use **undo peer** *group-name* **as-number** to delete a peer group.

Use **undo peer** *ip-address* to delete a peer.

By default, no peer or peer group is specified.

You can specify the AS number of a peer in either of the following ways:

- Use the **peer** *ip-address* **as-number** *as-number* command. After that, the system creates the specified peer by default.
- Specify the AS number of the peer when adding it to the specified peer group by using the **peer** *ip-address* **group** *group-name* **as-number** *as-number* command; or use the **peer** **as-number** command to specify the AS number of a peer group, and then a newly added peer will belong to the AS.

The AS number of a peer/peer group cannot be modified directly. To do so, you have to delete the peer/peer group and configure it again.

Examples

```
# In BGP view, specify peer group test in AS 100.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-number 100
```

```
# In BGP-VPN instance view, specify peer group test2 in AS 200. (The VPN has been created.)
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test2 as-number 200
```

peer as-path-acl (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } as-path-acl as-path-acl-number { export | import }
undo peer { group-name | ip-address } as-path-acl as-path-acl-number { export | import }
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-path-acl-number: AS path list number, in the range of 1 to 256.

export: Filters outgoing routes.

import: Filters incoming routes.

Description

Use **peer as-path-acl** to configure the filtering of routes incoming from or outgoing to a peer/peer group based on a specified AS path list.

Use **undo peer as-path-acl** to remove the configuration.

By default, no AS path list filtering is configured.

Related commands: **ip as-path**, **if-match as-path**, and **apply as-path**.

Examples

In BGP view, reference the AS path list 1 to filter routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-path-acl 1 export
```

In BGP-VPN instance view, reference the AS path list 1 to filter routes outgoing to the peer group **test**.
(The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test as-path-acl 1 export
```

peer bfd

Syntax

peer ip-address bfd

undo peer ip-address bfd

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

ip-address: IP address of a peer.

Description

Use **peer bfd** to enable BFD for a BGP peer.

Use **undo peer bfd** to disable BFD for a BGP peer.

By default, BFD is disabled.

After the link to the BGP peer fails, BFD may detect the failure before the system performs GR. As a result, GR will fail. If GR capability is enabled for BGP, use BFD with caution. If GR and BFD are both enabled, do not disable BFD during a GR process; otherwise, GR may fail.

Examples

Enable BFD for BGP peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 bfd
```

peer capability-advertise conventional

Syntax

```
peer { group-name | ip-address } capability-advertise conventional
undo peer { group-name | ip-address } capability-advertise conventional
```

View

BGP view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use **peer capability-advertise conventional** to disable BGP multi-protocol extension and route refresh for a peer/peer group.

Use **undo peer capability-advertise conventional** to enable BGP multi-protocol extension and route refresh for a peer/peer group.

By default, BGP multi-protocol extension and route refresh are enabled.

Examples

In BGP view, disable multi-protocol extension and route refresh for peer 160.89.2.33.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 160.89.2.33 as-number 100
[Sysname-bgp] peer 160.89.2.33 capability-advertise conventional
```

peer capability-advertise orf

Syntax

```
peer { group-name | ip-address } capability-advertise orf ip-prefix { both | receive | send }
undo peer { group-name | ip-address } capability-advertise orf ip-prefix { both | receive | send }
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

both: Supports sending and receiving route-refresh messages carrying the ORF information.

receive: Supports receiving route-refresh messages carrying the ORF information.

send: Supports sending route-refresh messages carrying the ORF information.

Description

Use **peer capability-advertise orf** to enable the ORF capability for a BGP peer or peer group.

Use **undo peer capability-advertise orf** to disable the ORF capability for the BGP peer or peer group.

By default, the ORF capability is not enabled for a BGP peer or peer group.

- After you enable the ORF capability, the local BGP router negotiates the ORF capability with the BGP peer through Open messages. After that, the BGP router can exchange ORF information in route-refresh messages with the peer. For non-standard ORF capability negotiation, you need also to configure the **peer capability-advertise orf non-standard** command.
- After you disable the ORF capability, the local BGP router does not negotiate the ORF capability with the specified peer or peer group.

Table 52 Description of the both, send, and receive parameters and the negotiation result

Local parameter	Peer parameter	Negotiation result
send	<ul style="list-style-type: none">• receive• both	The ORF sending capability is enabled locally and the ORF receiving capability is enabled on the peer.
receive	<ul style="list-style-type: none">• send• both	The ORF receiving capability is enabled locally and the ORF sending capability is enabled on the peer.
both	both	Both the ORF sending and receiving capabilities are enabled locally and on the peer.

Examples

Enable the ORF capability for the BGP peer 18.10.0.9. Then, after negotiation, the local router can exchange ORF information with the peer 18.10.0.9.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 18.10.0.9 as-number 100
[Sysname-bgp] peer 18.10.0.9 capability-advertise orf ip-prefix both
```

The related configuration needs to be made on the peer.

In BGP-VPN instance view, enable the ORF capability for the BGP peer 18.10.0.9. Then, after negotiation, the local router can exchange ORF information with the peer 18.10.0.9. (**vpn1** must have been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer 18.10.0.9 as-number 200
[Sysname-bgp-ipv4-vpn1] peer 18.10.0.9 capability-advertise orf ip-prefix both
```

The related configuration needs to be made on the peer.

peer capability-advertise orf non-standard

Syntax

peer { *group-name* | *ip-address* } **capability-advertise orf non-standard**

undo peer { *group-name* | *ip-address* } capability-advertise orf non-standard

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Parameters

Use **peer capability-advertise orf non-standard** to enable the non-standard ORF capability (the early implementation of ORF is different from that defined in RFC) for a BGP peer or peer group.

Use **undo peer capability-advertise orf non-standard** to disable the non-standard ORF capability for the BGP peer or peer group.

By default, the non-standard ORF capability is not enabled for a BGP peer or peer group.

This command needs to be configured when the peer supports only non-standard ORF.

Related commands: **peer capability-advertise orf**.

Examples

Enable the non-standard ORF capability for the BGP peer 18.10.0.9 (suppose the BGP peer 18.10.0.9 can only send non-standard ORF packets).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 18.10.0.9 as-number 100
[Sysname-bgp] peer 18.10.0.9 capability-advertise orf non-standard
[Sysname-bgp] peer 18.10.0.9 capability-advertise orf ip-prefix both
```

In BGP-VPN instance view, enable the non-standard ORF capability for the BGP peer 18.10.0.9 (suppose the BGP peer 18.10.0.9 can only send non-standard ORF packets). (**vpn1** must have been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer 18.10.0.9 as-number 200
[Sysname-bgp-ipv4-vpn1] peer 18.10.0.9 capability-advertise orf non-standard
[Sysname-bgp-ipv4-vpn1] peer 18.10.0.9 capability-advertise orf ip-prefix both
```

peer capability-advertise route-refresh

Syntax

peer { *group-name* | *ip-address* } capability-advertise route-refresh

undo peer { *group-name* | *ip-address* } capability-advertise route-refresh

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use **peer capability-advertise route-refresh** to enable the BGP route refresh capability.

Use **undo peer capability-advertise route-refresh** to disable the capability.

The capability is enabled by default.

Examples

In BGP view, enable BGP route refresh for peer 160.89.2.33.

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] peer 160.89.2.33 as-number 100
```

```
[Sysname-bgp] peer 160.89.2.33 capability-advertise route-refresh
```

In BGP-VPN instance view, enable BGP route refresh for peer 160.89.2.33. (The VPN has been created.)

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv4-family vpn-instance vpn1
```

```
[Sysname-bgp-ipv4-vpn1] peer 160.89.2.33 as-number 200
```

```
[Sysname-bgp-ipv4-vpn1] peer 160.89.2.33 capability-advertise route-refresh
```

peer capability-advertise suppress-4-byte-as

Syntax

peer { *group-name* | *ip-address* } capability-advertise suppress-4-byte-as

undo peer { *group-name* | *ip-address* } capability-advertise suppress-4-byte-as

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use **peer capability-advertise suppress-4-byte-as** to enable 4-byte AS number suppression.

Use **undo peer capability-advertise suppress-4-byte-as** to disable the function.

By default, the 4-byte AS number suppression function is disabled.

The device supports 4-byte AS numbers and uses 4-byte AS numbers by default. If the peer devices support only 2-byte AS numbers, you must enable the 4-byte AS number suppression function on the device.

If the peer device supports 4-byte AS numbers, do not enable the suppression function; otherwise, the BGP peer relationship cannot be established.

Examples

```
# In BGP view, enable 4-byte AS number suppression for peer 160.89.2.33.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 160.89.2.33 as-number 100
[Sysname-bgp] peer 160.89.2.33 capability-advertise suppress-4-byte-as
```

```
# In BGP-VPN instance view, enable 4-byte AS number suppression for peer 160.89.2.33. (The VPN must have been created.)
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer 160.89.2.33 as-number 200
[Sysname-bgp-ipv4-vpn1] peer 160.89.2.33 capability-advertise suppress-4-byte-as
```

peer connect-interface (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } connect-interface interface-type interface-number
undo peer { group-name | ip-address } connect-interface
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string 1 to 47 characters.

ip-address: IP address of a peer.

interface-type interface-number: Specifies an interface by its type and number.

Description

Use **peer connect-interface** to specify the source interface for establishing TCP connections to a peer/peer group.

Use **undo peer connect-interface** to restore the default.

By default, BGP uses the outbound interface of the best route to the BGP peer/peer group as the source interface for establishing a TCP connection to the peer/peer group.

Suppose interface A on the local device is connected to interface B on the peer device. When using the **peer x.x.x.x as-number as-number** command on the local device but x.x.x.x is not the IP address of interface B, you need to execute the **peer connect-interface** command on the peer to specify the source interface (the owner of IP address x.x.x.x) for establishing TCP connections.

To establish multiple BGP connections to another BGP router, you need to specify on the local router the respective source interfaces for establishing TCP connections to the peers on the peering BGP router; otherwise, the local BGP router may fail to establish TCP connections to the peers when using the outbound interfaces of the best routes as the source interfaces.

Examples

```
# In BGP view, specify loopback 0 as the source interface for routing updates to the peer group test.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test connect-interface loopback 0

# In BGP-VPN instance view, specify loopback 0 as the source interface for routing updates to the peer
group test. (The VPN has been created.)
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test connect-interface loopback 0
```

peer default-route-advertise (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } default-route-advertise [ route-policy route-policy-name ]
undo peer { group-name | ip-address } default-route-advertise
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

route-policy-name: Routing policy name, a case-sensitive string of 1 to 63 characters.

Description

Use **peer default-route-advertise** to advertise a default route to a peer/peer group.

Use **undo peer default-route-advertise** to disable default route advertisement to a peer/peer group.

By default, no default route is advertised to a peer/peer group.

With this command used, the router unconditionally sends a default route with the next hop being itself to the peer/peer group regardless of whether the default route is available in the routing table.

Examples

```
# In BGP view, advertise a default route to peer group test.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test default-route-advertise

# In BGP-VPN instance view, advertise a default route to peer group test. (The VPN has been created.)
<Sysname> system-view
```

```
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test default-route-advertise
```

peer description (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } description description-text
undo peer { group-name | ip-address } description
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

description-text: Description information for the peer/peer group, a string of 1 to 79 characters.

Description

Use **peer description** to configure the description information for a peer/peer group.

Use **undo peer description** to remove the description information of a peer/peer group.

By default, no description information is configured for a peer/peer group.

Create a peer/peer group before configuring a description for it.

Related commands: **display bgp peer**.

Examples

In BGP view, configure the description information of the peer group test as ISP1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test description ISP1
```

In BGP-VPN instance view, configure the description information of the peer group test as ISP1. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test description ISP1
```

peer dscp (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } dscp dscp-value
undo peer { group-name | ip-address } dscp
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Specifies the name of a peer group, a string of 1 to 47 characters.

ip-address: Specifies the IP address of a peer.

dscp-value: Sets the DSCP value for BGP packets.

Description

Use **peer dscp** to set the DSCP value for the BGP packets sent to the specified peer or peer group.

Use **undo peer dscp** to remove the configuration.

By default, the DSCP value in BGP packets is 48.

The peer or peer group you specified must have been created.

Examples

In BGP view, set the DSCP value for the BGP packets sent to peer group **test** to 63.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test dscp 63
```

In BGP-VPN instance view, set the DSCP value for the BGP packets sent to peer group **test** to 63. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test dscp 63
```

peer ebgp-max-hop (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } ebgp-max-hop [ hop-count ]
```

```
undo peer { group-name | ip-address } ebgp-max-hop
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

hop-count: Maximum hop count, in the range of 1 to 255. The default is 64.

Description

Use **peer ebgp-max-hop** to allow establishing an EBGP connection with a peer/peer group that is on an indirectly connected network.

Use **undo peer ebgp-max-hop** to restore the default.

By default, this feature is disabled.

You can use the argument *hop-count* to specify the maximum route hop count of the EBGP connection.

Examples

In BGP view, allow establishing the EBGP connection with the peer group **test** that is on an indirectly connected network.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test ebgp-max-hop
```

In BGP-VPN instance view, allow establishing the EBGP connection with the peer group **test** that is on an indirectly connected network. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test ebgp-max-hop
```

peer enable (BGP/BGP-VPN instance view)

Syntax

peer ip-address enable

undo peer ip-address enable

View

BGP view, BGP VPN instance view

Default level

2: System level

Parameters

ip-address: IP address of a peer.

Description

Use **peer enable** to enable the specified peer.

Use **undo peer enable** to disable the specified peer.

By default, the BGP peer is enabled.

If a peer is disabled, the router will not exchange routing information with the peer.

Examples

```
# Disable peer 18.10.0.9.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 18.10.0.9 group group1
[Sysname-bgp] undo peer 18.10.0.9 enable
```

peer fake-as (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } fake-as as-number  
undo peer { group-name | ip-address } fake-as
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-number: Local autonomous system number, in the range of 1 to 4294967295.

Description

Use **peer fake-as** to configure a fake local AS number for a peer or peer group.

Use **undo peer fake-as** to remove the configuration.

By default, no fake local AS number is configured for a peer or peer group.

NOTE:

The **peer fake-as** command is only applicable to an EBGp peer or peer group.

Examples

```
# In BGP view, configure a fake AS number of 200 for the peer group test.
```

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] peer test fake-as 200
```

```
# In BGP-VPN instance view, configure a fake AS number of 200 for the peer group test. (The VPN has been created.)
```

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv4-family vpn-instance vpn1  
[Sysname-bgp-ipv4-vpn1] peer test fake-as 200
```

peer filter-policy (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } filter-policy acl-number { export | import }  
undo peer { group-name | ip-address } filter-policy [ acl-number ] { export | import }
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

acl-number: ACL number, in the range of 2000 to 3999.

export: Applies the filter-policy to routes advertised to the peer/peer group.

import: Applies the filter-policy to routes received from the peer/peer group.

Description

Use **peer filter-policy** to configure an ACL-based filter policy for a peer or peer group.

Use **undo peer filter-policy** to remove the configuration.

By default, no ACL-based filter policy is configured for a peer or peer group.

Related commands: **peer as-path-acl**.

Examples

In BGP view, apply the ACL 2000 to filter routes advertised to the peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test filter-policy 2000 export
```

In BGP-VPN instance view, apply the ACL 2000 to filter routes advertised to the peer group test. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test filter-policy 2000 export
```

peer group (BGP/BGP-VPN instance view)

Syntax

```
peer ip-address group group-name [ as-number as-number ]
```

```
undo peer ip-address group group-name
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-number: AS number of the peer, in the range of 1 to 4294967295.

Description

Use **peer group** to add a peer to a peer group.

Use **undo peer group** to delete a specified peer from a peer group.

By default, no peer is added into a peer group.

If you have specified an AS number for the peer to be added, make sure that the *as-number* argument is consistent with the specified peer AS number.

If you have not created the peer to be added, the system automatically creates the peer when you execute the command.

Examples

In BGP view, add the peer 10.1.1.1 to the EBGP peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 2004
[Sysname-bgp] peer 10.1.1.1 group test
```

In BGP-VPN view, add the peer 10.1.1.1 to the EBGP peer group test. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] group test external
[Sysname-bgp-ipv4-vpn1] peer test as-number 2004
[Sysname-bgp-ipv4-vpn1] peer 10.1.1.1 group test
```

peer ignore (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } ignore
undo peer { group-name | ip-address } ignore
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use **peer ignore** to disable session establishment with a peer or peer group.

Use **undo peer ignore** to remove the configuration.

By default, session establishment with a peer or peer group is allowed.

After the **peer ignore** command is executed, the system disables the session with the specified peer or peer group and clears all the related routing information. For a peer group, all sessions with the peer group will be torn down.

Examples

```
# In BGP view, disable session establishment with peer 10.10.10.10.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.10.10.10 ignore
```

```
# In BGP-VPN instance view, disable session establishment with peer 10.10.10.10. (The VPN has been created.)
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer 10.10.10.10 ignore
```

peer ip-prefix

Syntax

```
peer { group-name | ip-address } ip-prefix ip-prefix-name { export | import }
undo peer { group-name | ip-address } ip-prefix { export | import }
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

ip-prefix-name: IP prefix list name, a string of 1 to 19 characters.

export: Applies the filter to routes advertised to the specified peer/peer group.

import: Applies the filter to routes received from the specified peer/peer group.

Description

Use **peer ip-prefix** to reference an IP prefix list to filter routes received from or advertised to a peer or peer group.

Use **undo peer ip-prefix** to remove the configuration.

By default, no IP prefix list based filtering is configured.

Examples

```
# In BGP view, use the IP prefix list list 1 to filter routes advertised to the peer group test.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test ip-prefix list1 export
```

In BGP-VPN view, use the IP prefix list **list 1** to filter routes advertised to the peer group **test**. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test ip-prefix list1 export
```

peer keep-all-routes (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } keep-all-routes
undo peer { group-name | ip-address } keep-all-routes
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use **peer keep-all-routes** to save original routing information from a peer or peer group, including routes that fail to pass the inbound policy (if configured).

Use **undo peer keep-all-routes** to disable this function.

By default, the function is not enabled.

Examples

In BGP view, save routing information from peer 131.100.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.100.1.1 as-number 200
[Sysname-bgp] peer 131.100.1.1 keep-all-routes
```

In BGP-VPN instance view, save routing information from peer 131.100.1.1. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer 131.100.1.1 as-number 200
[Sysname-bgp-ipv4-vpn1] peer 131.100.1.1 keep-all-routes
```

peer log-change (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } log-change
undo peer { group-name | ip-address } log-change
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use **peer log-change** to enable the logging of session state and event information for a specified peer or peer group.

Use **undo peer log-change** to remove the configuration.

The logging is enabled by default.

Examples

In BGP view, enable the logging of session state and event information for peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test log-change
```

In BGP-VPN instance view, enable the logging of session state and event information for peer group **test**. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test log-change
```

peer next-hop-local (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } next-hop-local
undo peer { group-name | ip-address } next-hop-local
```

View

BGP view /BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use **peer next-hop-local** to specify the router as the next hop for routes sent to a peer/peer group.

Use **undo peer next-hop-local** to remove the configuration.

By default, routes advertised to an EBGp peer/peer group take the local router as the next hop, and routes sent to an IBGP peer/peer group do not take the local router as the next hop.

Examples

In BGP view, set the next hop of routes advertised to peer group **test** to the router itself.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test next-hop-local
```

In BGP-VPN instance view, set the next hop of routes advertised to peer group **test** to the router itself. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test next-hop-local
```

peer password

Syntax

```
peer { group-name | ip-address } password { cipher | simple } password
undo peer { group-name | ip-address } password
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Sets the password. This argument is case sensitive. It must be a ciphertext string of 1 to 137 characters, or a plaintext string of 1 to 80 characters.

Description

Use **peer password** to configure BGP to perform MD5 authentication when a TCP connection is being established with a peer/peer group.

Use **undo peer password** to disable the function.

By default, no MD5 authentication is performed for TCP connection establishment.

Once MD5 authentication is enabled, both parties must be configured with the same authentication mode and password. Otherwise, the TCP connection will not be set up.

The authentication password, set in plain text or cipher text, is saved to the configuration file in cipher text.

Examples

In BGP view, perform MD5 authentication on the TCP connection set up between the local router 10.1.100.1 and the peer router 10.1.100.2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.1.100.2 password simple aabbcc
```

Perform the similar configuration on the peer.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.1.100.1 password simple aabbcc
```

In BGP-VPN instance view, perform MD5 authentication on the TCP connection set up between the local router 10.1.100.1 and the peer router 10.1.100.2. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer 10.1.100.2 password simple aabbcc
```

Perform the similar configuration on the peer.

```
<Sysname> system-view
[Sysname] bgp 200
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer 10.1.100.1 password simple aabbcc
```

peer preferred-value (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } preferred-value value
undo peer { group-name | ip-address } preferred-value
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

value: Preferred value, in the range of 0 to 65535.

Description

Use **peer preferred-value** to assign a preferred value to routes received from a peer or peer group.

Use **undo peer preferred-value** to restore the default value.

The default preferred value is 0.

Routes learned from a peer have an initial preferred value. Among multiple routes that have the same destination/mask and are learned from different peers, the one with the greatest preferred value is selected as the route to the destination.

If you both reference a routing policy and use the **peer** { *group-name* | *ip-address* } **preferred-value** *value* command to set a preferred value for routes from a peer, the routing policy sets the specified preferred value for routes matching it. Other routes not matching the routing policy uses the value set with the command. If the preferred value specified in the routing policy is zero, the routes matching it will also use the value set with the **peer** { *group-name* | *ip-address* } **preferred-value** *value* command. For information about using a routing policy to set a preferred value, see the command **peer** { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** } in this document, and the command **apply preferred-value** *preferred-value* in "Routing policy configuration commands."

Examples

```
# In BGP view, configure the preferred value as 50 for routes from peer 131.108.1.1.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.108.1.1 preferred-value 50
```

```
# In BGP-VPN instance view, configure the preferred value as 50 for routes from peer 131.108.1.1. (The VPN has been created.)
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer 131.108.1.1 preferred-value 50
```

peer public-as-only (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } public-as-only
undo peer { group-name | ip-address } public-as-only
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use **peer public-as-only** to not keep private AS numbers in BGP updates sent to a peer/peer group.

Use **undo peer public-as-only** to keep private AS numbers in BGP updates sent to a peer/peer group.

By default, BGP updates carry private AS numbers.

The command does not take effect if the BGP update has both public and private AS numbers. The range of private AS number is from 64512 to 65535.

Examples

```
# In BGP view, carry no private AS number in BGP updates sent to the peer group test.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test public-as-only
```

In BGP-VPN instance view, carry no private AS number in BGP updates sent to the peer group **test**. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test public-as-only
```

peer reflect-client (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } reflect-client
undo peer { group-name | ip-address } reflect-client
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description

Use **peer reflect-client** to configure the router as a route reflector and specify a peer/peer group as a client.

Use **undo peer reflect-client** to remove the configuration.

By default, neither the route reflector nor the client is configured.

Related commands: **reflect between-clients** and **reflect cluster-id**.

Examples

In BGP view, configure the local device as a route reflector and specify the IBGP peer group **test** as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test reflect-client
```

In BGP-VPN instance view, configure the local device as a route reflector and specify the IBGP peer group **test** as a client. (**vpn1** must have been created.)

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test reflect-client
```

peer route-limit (BGP/BGP-VPN instance view)

Syntax

```
peer { group-name | ip-address } route-limit prefix-number [ { alert-only | reconnect reconnect-time } | percentage-value ] *
```

undo peer { *group-name* | *ip-address* } **route-limit**

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

prefix-number: Number of prefixes that can be received from the peer or peer group. Its range varies with devices. If the number of prefixes received from the peer/peer group reaches the *prefix-number*, the router will tear down the connection to the peer/peer group.

alert-only: If the number of prefixes received from the peer/peer group reaches the *prefix-number*, the router will not tear down the connection to the peer/peer group but display an alarm message.

reconnect *reconnect-time*: Specifies a reconnect time, after which, the router will re-establish a connection to the peer/peer group. It has no default value and is in the range of 1 to 65535 seconds.

percentage-value: Threshold value for the router to display an alarm message (the router displays an alarm message when the ratio of the number of received prefixes to the *prefix-number* exceeds the *percentage*). It is in the range of 1 to 100 and defaults to 75.

Description

Use **peer route-limit** to set the number of route prefixes that can be received from a peer/peer group.

Use **undo peer route-limit** to restore the default.

The number is not limited by default.

Examples

In BGP view, set the number of route prefixes that can be received from peer 129.140.6.6 to 10000.

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp] peer 129.140.6.6 as-number 110
[Sysname-bgp] peer 129.140.6.6 route-limit 10000
```

In BGP-VPN instance view, set the number of route prefixes that can be received from peer 129.140.6.6 to 10000. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer 129.140.6.6 as-number 110
[Sysname-bgp-ipv4-vpn1] peer 129.140.6.6 route-limit 10000
```

peer route-policy (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

route-policy-name: Routing policy name, a case-sensitive string of 1 to 63 characters.

export: Applies the routing policy to routes outgoing to the peer (or peer group).

import: Applies the routing policy to routes incoming from the peer (or peer group).

Description

Use **peer route-policy** to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use **undo peer route-policy** to remove the configuration.

By default, no routing policy is applied to routes from/to the peer/peer group.

The **peer route-policy** command does not apply the **if-match interface** clause in the referenced routing policy. See "Routing policy configuration commands" for related commands.

Examples

In BGP view, apply routing policy **test-policy** to routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test route-policy test-policy export
```

In BGP-VPN instance view, apply the routing policy **test-policy** to routes outgoing to the peer group **test**.
(The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test route-policy test-policy export
```

peer route-update-interval (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **route-update-interval** *interval*

undo peer { *group-name* | *ip-address* } **route-update-interval**

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a sting of 1 to 47 characters.

ip-address: IP address of a peer.

interval: Minimum interval for sending the same update message. The range is 0 to 600 seconds. A value of 0 means to send the update message immediately.

Description

Use **peer route-update-interval** to specify the interval for sending the same update to a peer or peer group.

Use **undo peer route-update-interval** to restore the default value.

By default, the interval is 5 seconds for IBGP peers, and 30 seconds for EBGP peers.

Examples

In BGP view, specify the interval for sending the same update to peer group **test** as 10 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-number 100
[Sysname-bgp] peer test route-update-interval 10
```

In BGP-VPN instance view, specify the interval for sending the same update to peer group **test** as 10 seconds. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test as-number 100
[Sysname-bgp-ipv4-vpn1] peer test route-update-interval 10
```

peer timer (BGP/BGP-VPN instance view)

Syntax

peer { *group-name* | *ip-address* } **timer** **keepalive** *keepalive* **hold** *holdtime*

undo peer { *group-name* | *ip-address* } **timer**

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

keepalive: Keepalive interval in seconds, ranging from 0 to 21845.

holdtime: Holdtime interval in seconds, whose value is 0 or in the range of 3 to 65535.

Description

Use **peer timer** to configure the keepalive interval and holdtime interval for a peer or peer group.

Use **undo peer timer** to restore the default.

By default, the *keepalive* and *holdtime* are 60s and 180s.

The timers configured with this command are preferred to the timers configured with the **timer** command.

If the holdtime interval is configured as 0, no keepalive message will be sent to the peer, and the peer connection will never time out. If the keepalive interval is configured as 0 and the negotiated hold time is not 0, one third of the hold time is taken as the interval for sending keepalive messages.

If neither the holdtime interval nor the keepalive interval is configured as 0, the holdtime interval must be at least three times the keepalive interval.

After this command is executed, the peer connection is closed at once, and a new connection to the peer is negotiated using the configured hold time.

Related commands: **timer**.

Examples

In BGP view, configure the keepalive interval and holdtime interval for peer group **test** as 60s and 180s.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test timer keepalive 60 hold 180
```

In BGP-VPN instance view, configure the keepalive interval and holdtime interval for peer group **test** as 60s and 180s. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test timer keepalive 60 hold 180
```

In BGP view, configure both the keepalive interval and holdtime interval for peer group **test** as 0 seconds, indicating the peer group will never time out.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test timer keepalive 0 hold 0
```

In BGP-VPN instance view, configure both the keepalive interval and holdtime interval for peer group **test** as 0 seconds, indicating the peer group will never time out. (**vpn1** must have been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] peer test timer keepalive 0 hold 0
```

preference (BGP/BGP-VPN instance view)

Syntax

preference { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }

undo preference

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

external-preference: Preference of EBGp routes, in the range of 1 to 255.

internal-preference: Preference of IBGP routes, in the range of 1 to 255.

local-preference: Preference of local routes, in the range of 1 to 255.

route-policy-name: Routing policy name, a case-sensitive string of 1 to 63 characters. Using the routing policy can set a preference for routes matching it. The default value applies to routes not matching the routing policy.

Description

Use **preference** to configure preferences for external, internal, and local routes.

Use **undo preference** to restore the default.

For *external-preference*, *internal-preference*, and *local-preference*, the greater the preference value is, the lower the preference is, and the default values are 255, 255, and 130.

Examples

In BGP view, configure preferences for EBGp, IBGP and local routes as 20, 20, and 200.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] preference 20 20 200
```

In BGP-VPN instance view, configure preferences for EBGp, IBGP and local routes as 20, 20, and 200. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] preference 20 20 200
```

reflect between-clients (BGP view/BGP-VPN instance view)

Syntax

reflect between-clients

undo reflect between-clients

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

None

Description

Use **reflect between-clients** to enable route reflection between clients.

Use **undo reflect between-clients** to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects the routes of a client to other clients. If the clients of a route reflector are fully meshed, you need disable route reflection between clients to reduce routing costs.

Related commands: **reflector cluster-id** and **peer reflect-client**.

Examples

```
# Disable route reflection between clients.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] undo reflect between-clients

# In BGP-VPN instance view, disable route reflection between clients. (vpn1 must have been created.)
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] undo reflect between-clients
```

reflector cluster-id (BGP view/BGP-VPN instance view)

Syntax

```
reflector cluster-id { cluster-id | ip-address }
undo reflector cluster-id
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

cluster-id: Cluster ID in the format of an integer from 1 to 4294967295.

ip-address: Cluster ID in the format of an IPv4 address in dotted decimal notation.

Description

Use **reflector cluster-id** to configure the cluster ID of the route reflector.

Use **undo reflector cluster-id** to remove the configured cluster ID.

By default, each route reflector uses its router ID as the cluster ID.

Typically, a cluster has only one route reflector. The router ID of the route reflector is the ID of the cluster. You can configure multiple route reflectors to improve network stability. Using this command can configure the identical cluster ID for all the route reflectors to avoid routing loops.

Related commands: **reflect between-clients** and **peer reflect-client**.

Examples

```
# Set the cluster ID to 80.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] reflector cluster-id 80

# In BGP-VPN instance view, set the cluster ID to 80. (vpn1 must have been created.)
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
```

```
[Sysname-bgp-ipv4-vpn1] reflector cluster-id 80
```

refresh bgp

Syntax

```
refresh bgp { ip-address | all | group group-name | external | internal } { export | import }
```

View

User view

Default level

1: Monitor level

Parameters

ip-address: Soft-resets the BGP connection to a peer.

all: Soft-resets all BGP connections.

group-name: Soft-resets connections to a peer group, name of which is a string of 1 to 47 characters.

external: EBGP connection.

internal: IBGP connection.

export: Outbound soft reset.

import: Inbound soft reset.

Description

Use **refresh bgp** to perform soft reset on specified BGP connections. Using this function can refresh the BGP routing table without tearing down BGP connections and apply a newly configured routing policy.

To perform BGP soft reset, all routers in the network must support route-refresh. If a router not supporting route-refresh exists in the network, you need to configure the **peer keep-all-routes** command to save all routing updates before performing soft reset.

Examples

```
# Perform inbound BGP soft reset.  
<Sysname> refresh bgp all import
```

reset bgp

Syntax

```
reset bgp { as-number | ip-address [ flap-info ] | all | external | group group-name | internal }
```

View

User view

Default level

1: Monitor level

Parameters

as-number: Resets BGP connections to peers in the AS.

ip-address: Specifies the IP address of a peer with which to reset the connection.

flap-info: Clears route flap information.

all: Resets all BGP connections.

external: Resets all the EBGP connections.

group *group-name*: Resets connections with the specified BGP peer group.

internal: Resets all the IBGP connections.

Description

Use **reset bgp** to reset specified BGP connections.

Examples

```
# Reset all the BGP connections.  
<Sysname> reset bgp all
```

reset bgp dampening

Syntax

```
reset bgp dampening [ ip-address [ mask | mask-length ] ]
```

View

User view

Default level

1: Monitor level

Parameters

ip-address: Destination IP address of a route.

mask: Mask, in dotted decimal notation.

mask-length: Mask length, in the range of 0 to 32.

Description

Use **reset bgp dampening** to clear route dampening information and release suppressed routes.

Related commands: **dampening** and **display bgp routing-table dampened**.

Examples

```
# Clear damping information of route 20.1.0.0/16 and release the suppressed route.  
<Sysname> reset bgp dampening 20.1.0.0 255.255.0.0
```

reset bgp flap-info

Syntax

```
reset bgp flap-info [ ip-address [ mask-length | mask ] | as-path-acl as-path-acl-number | regex as-path-regular-expression ]
```

```
reset bgp peer-ip-address flap-info
```

View

User view

Default level

1: Monitor level

Parameters

ip-address: Clears the flap statistics of a route.

mask-length: Mask length, in the range of 0 to 32.

mask: Network mask, in dotted decimal notation.

as-path-acl-number: Clears the flap statistics of routes matching an AS path list. The AS path list number is in the range of 1 to 256.

as-path-regular-expression: Clears the flap statistics of routes matching the AS path regular expression, a string of 1 to 80 characters.

peer-ip-address: Clears the flap statistics of routes received from the specified peer.

Description

Use **reset bgp flap-info** to clear the flap statistics of routes matching the specified filter.

Examples

```
# Clear the flap statistics of all routes matching AS path list 10.
```

```
<Sysname> reset bgp flap-info as-path-acl 10
```

reset bgp ipv4 all

Syntax

```
reset bgp ipv4 all
```

View

User view

Default level

2: System level

Parameters

None

Description

Use **reset bgp ipv4 all** to reset all the BGP connections of IPv4 unicast address family.

Examples

```
# Reset all the BGP connections of IPv4 unicast address family.
```

```
<Sysname> reset bgp ipv4 all
```

router id

Syntax

```
router id router-id
```

```
undo router id
```

View

System view

Default level

2: System level

Parameters

router-id: Router ID, in the form of a dotted decimal IPv4 address.

Description

Use **router id** to configure a global router ID.

Use **undo router id** to remove the global router ID.

By default, no global router ID is configured.

Some routing protocols use a router ID to identify a device. You can configure a global router ID, which is used by routing protocols that have no router ID configured.

If no global router ID is configured, the highest loopback interface IP address, if any, is used as the router ID. If no loopback interface IP address is available, the highest physical interface IP address is used, regardless of the interface status.

If the interface whose IP address is the router ID is removed or modified, a new router ID is selected. Other events, (the interface goes down; after a physical interface address is selected as the router ID, an IP address is configured for a loopback interface; a higher interface IP address is configured) will not trigger a router ID re-selection.

Examples

```
# Configure a global router ID.  
<Sysname> system-view  
[Sysname] router id 1.1.1.1
```

router-id

Syntax

router-id *router-id*

undo router-id

View

BGP view

Default level

2: System level

Parameters

router-id: Router ID in IP address format.

Description

Use **router-id** to specify a router ID.

Use **undo router-id** to remove the router ID.

To run BGP protocol, a router must have a router ID (an unsigned 32-bit integer), the unique ID of the router in the AS.

You can specify a router ID manually. Otherwise, the system selects the highest IP address among loopback interface addresses as the router ID. If no loopback interface addresses are available, the system selects the highest IP address among physical interface IP addresses as the router ID. Specify a loopback interface address as the router ID to enhance network reliability.

If the interface whose IP address is selected as the router ID or the manual router ID is deleted, the system selects a new router ID for the router.

Examples

```
# Specifies the Router ID as 10.18.4.221.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] router-id 10.18.4.221
```

summary automatic

Syntax

```
summary automatic
undo summary automatic
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

None

Description

Use **summary automatic** to enable automatic summarization for redistributed subnets.

Use **undo summary automatic** to disable automatic summarization.

By default, automatic summarization is disabled.

Neither the default route nor the routes imported using the **network** command can be summarized automatically.

The **summary automatic** command helps BGP limit the number of routes redistributed from IGP to reduce the size of the routing table.

Examples

```
# In BGP view, enable automatic route summarization.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] summary automatic

# In BGP-VPN instance view, enable automatic summarization. (The VPN has been created.)
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] summary automatic
```

synchronization (BGP view)

Syntax

```
synchronization
```

undo synchronization

View

BGP view

Default level

2: System level

Parameters

None

Description

Use **synchronization** to enable the synchronization between the BGP and IGP routes.

Use **undo synchronization** to disable the synchronization.

The feature is disabled by default.

With this feature enabled and when a non-BGP router is responsible for forwarding packets in an AS, BGP speakers in the AS cannot advertise routing information to other ASs unless all routers in the AS know the latest routing information.

When a BGP router receives an IBGP route, it checks only whether the next hop is reachable by default. If the synchronization is enabled, the IBGP route is synchronized and advertised to EBGP peers only when the route is also advertised by IGP. Otherwise, the IBGP route cannot be advertised to EBGP peers.

Examples

```
# Enable the synchronization between BGP and IGP routes.
```

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] synchronization
```

timer (BGP/BGP-VPN instance view)

Syntax

```
timer keepalive keepalive hold holdtime
```

```
undo timer
```

View

BGP view, BGP-VPN instance view

Default level

2: System level

Parameters

keepalive: Keepalive interval in seconds, ranging from 0 to 21845.

holdtime: Holdtime interval in seconds, whose value is 0 or in the range of 3 to 65535.

Description

Use **timer** to configure the BGP keepalive interval and holdtime interval.

Use **undo timer** to restore the default.

By default, the BGP keepalive interval and the holdtime interval are 60 seconds and 180 seconds.

The timers configured with the **peer timer** command are preferred to the timers configured with this command.

If the holdtime interval is configured as 0, no keepalive message will be sent to the peer, and the peer connection will never time out. If the keepalive interval is configured as 0 and the negotiated hold time is not 0, one third of the hold time is taken as the interval for sending keepalive messages.

If neither the holdtime interval nor the keepalive interval is configured as 0, the holdtime interval must be at least three times the keepalive interval.

The configured timers apply to all BGP peers, but they become valid for a BGP peer only after the relevant BGP connection is reset.

After this command is executed, no peer connection is closed at once. The configured hold time is used for negotiation when a peer relationship is reestablished.

Related commands: **peer timer**.

Examples

Configure keepalive interval and holdtime interval as 60s and 180s.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] timer keepalive 60 hold 180
```

In BGP-VPN instance view, configure keepalive interval and holdtime interval as 60s and 180s. (The VPN has been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] timer keepalive 60 hold 180
```

In BGP view, configure both the BGP keepalive interval and holdtime interval as 0 seconds, indicating no peer connection will time out.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] timer keepalive 0 hold 0
```

In BGP-VPN instance view, configure both the keepalive interval and holdtime interval for **vpn1** as 0 seconds, indicating no peer connection will time out. (**vpn1** must have been created.)

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-ipv4-vpn1] timer keepalive 0 hold 0
```

IPv6 static routing configuration commands

The term "router" in this chapter refers to both routers and Layer 3 switches.

The A5500 SI Switch Series does not support VPN-related parameters.

delete ipv6 static-routes all

Syntax

```
delete ipv6 [ vpn-instance vpn-instance-name ] static-routes all
```

View

System view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, all static routes of the public network are deleted.

Description

Use **delete ipv6 static-routes all** to delete all static routes including the default route.

When using this command, you will be prompted whether to continue the deletion and only after you confirm the deletion will the static routes be deleted.

Related commands: **ipv6 route-static** and **display ipv6 routing-table**.

Examples

```
# Delete all IPv6 static routes.
```

```
<Sysname> system-view
```

```
[Sysname] delete ipv6 static-routes all
```

```
This will erase all ipv6 static routes and their configurations, you must reconfigure all static routes
```

```
Are you sure?[Y/N]Y
```

ipv6 route-static

Syntax

```
ipv6 route-static ipv6-address prefix-length { interface-type interface-number [ next-hop-address ] | next-hop-address | vpn-instance d-vpn-instance-name nexthop-address } [ preference preference-value ]
```

```
undo ipv6 route-static ipv6-address prefix-length [ interface-type interface-number [ next-hop-address ] | next-hop-address | vpn-instance d-vpn-instance-name nexthop-address ] [ preference preference-value ]
```

```
ipv6 route-static vpn-instance s-vpn-instance-name&<1-6> ipv6-address prefix-length { interface-type interface-number [ next-hop-address ] | nexthop-address [ public ] | vpn-instance d-vpn-instance-name nexthop-address } [ preference preference-value ]
```

```
undo ipv6 route-static vpn-instance s-vpn-instance-name&<1-6> ipv6-address prefix-length  
[ interface-type interface-number [ next-hop-address ] | nexthop-address [ public ] | vpn-instance  
d-vpn-instance-name nexthop-address ] [ preference preference-value ]
```

View

System view

Default level

2: System level

Parameters

ipv6-address prefix-length: Specifies the IPv6 address and prefix length.

interface-type interface-number: Specifies an output interface by its type and number. If the output interface is a non-P2P interface, such as an NBMA interface or broadcast interface (for example, an Ethernet interface, or a VLAN interface), the next hop address must be specified.

nexthop-address: Specifies the next hop IPv6 address.

vpn-instance *d-vpn-instance-name*: Specifies the name of the destination VPN, a case-sensitive string. If it is specified, packets will search for the outgoing interface based on the specified next hop (IPv6 address) for the static route.

preference *preference-value*: Specifies the route preference value, in the range of 1 to 255. The default is 60.

vpn-instance *s-vpn-instance-name*&<1-6>: Specifies the name of the source VPN, a case-sensitive string of 1 to 31 characters. &<1-6> means the parameter can be input up to six times. If a VPN is specified, the configured static route is added to the routing table of the VPN.

public: Specifies a next hop in the public network.

Description

Use **ipv6 route-static** to configure an IPv6 static route.

Use **undo ipv6 route-static** to remove an IPv6 static route.

An IPv6 static route that has the destination address configured as **::/0** (a prefix length of 0) is the default IPv6 route. If the destination address of an IPv6 packet does not match any entry in the routing table, this default route will be used to forward the packet.

If you specify a broadcast interface, such as an Ethernet interface or a VLAN interface, as the output interface for a static route, you must specify the next hop address.

Related commands: **delete ipv6 static-routes all** and **display ipv6 routing-table**.

Examples

```
# Configure a static IPv6 route, with the destination address being 1:1:2::/24 and next hop being 1:1:3::1.  
<Sysname> system-view  
[Sysname] ipv6 route-static 1:1:2:: 24 1:1:3::1
```

RIPng configuration commands

The term "router" in this chapter refers to both routers and Layer 3 switches.

checkzero

Syntax

checkzero
undo checkzero

View

RIPng view

Default level

2: System level

Parameters

None

Description

Use **checkzero** to enable the zero field check on RIPng packets.

Use **undo checkzero** to disable the zero field check.

The zero field check is enabled by default.

Some fields in RIPng packet headers must be zero. These fields are called "zero fields". You can enable the zero field check on RIPng packet headers. If any such field contains a non-zero value, the RIPng packet will be discarded.

Examples

```
# Disable the zero field check on RIPng packet headers of RIPng 100.  
<Sysname> system-view  
[Sysname] ripng 100  
[Sysname-ripng-100] undo checkzero
```

default cost (RIPng view)

Syntax

default cost *cost*
undo default cost

View

RIPng view

Default level

2: System level

Parameters

cost: Default metric of redistributed routes, in the range of 0 to 16.

Description

Use **default cost** to specify the default metric of redistributed routes.

Use **undo default cost** to restore the default.

The default metric of redistributed routes is 0.

The specified default metric applies to the routes redistributed by the **import-route** command with no metric specified.

Related commands: **import-route**.

Examples

```
# Set the default metric of redistributed routes to 2.
```

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] default cost 2
```

display ripng

Syntax

```
display ripng [ process-id | vpn-instance vpn-instance-name ] [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

process-id: RIPng process ID, in the range of 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ripng** to display the running status and configuration information of a RIPng process. If no *process-id* is specified, information about all RIPng processes is displayed. If a VPN is specified, information about all the RIPng processes of the VPN is displayed.

Examples

```
# Display the running status and configuration information of all configured RIPng processes.
```



```

<Sysname> display ripng
Public VPN-instance name :
  RIPng process : 1
    Preference : 100
    Checkzero : Enabled
    Default Cost : 0
    Maximum number of balanced paths : 8
    Update time : 30 sec(s) Timeout time : 180 sec(s)
    Suppress time : 120 sec(s) Garbage-Collect time : 120 sec(s)
    Number of periodic updates sent : 0
    Number of trigger updates sent : 0
    IPsec policy name: policy001, SPI: 300

```

Table 53 Command output

Field	Description
Public VPN-instance name	Public VPN instance name.
RIPng process	RIPng process ID.
Preference	RIPng preference.
Checkzero	Indicates whether zero field check for RIPng packet headers is enabled.
Default Cost	Default metric of redistributed routes.
Maximum number of balanced paths	Maximum number of load balanced routes.
Update time	RIPng update interval, in seconds.
Timeout time	RIPng timeout interval, in seconds.
Suppress time	RIPng suppress interval, in seconds.
Garbage-Collect time	RIPng garbage collection interval, in seconds.
Number of periodic updates sent	Number of periodic updates sent.
Number of trigger updates sent	Number of triggered updates sent.
IPsec policy name	IPsec policy applied in the process.
SPI	SPI defined in the IPsec policy.

display ripng database

Syntax

```
display ripng process-id database [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: RIPng process ID, in the range of 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ripng database** to display all active routes in the advertising database of the specified RIPng process, which are sent in normal RIPng update messages.

Examples

Display the active routes in the database of RIPng process 100.

```
<Sysname> display ripng 100 database
 2001:7B::2:2A1:5DE/64,
     cost 4, Imported
 1:13::/120,
     cost 4, Imported
 1:32::/120,
     cost 4, Imported
 1:33::/120,
     cost 4, Imported
 100::/32,
     via FE80::200:5EFF:FE04:3302, cost 2
 3FFE:C00:C18:1::/64,
     via FE80::200:5EFF:FE04:B602, cost 2
 3FFE:C00:C18:1::/64,
     via FE80::200:5EFF:FE04:B601, cost 2
 3FFE:C00:C18:2::/64,
     via FE80::200:5EFF:FE04:B602, cost 2
 3FFE:C00:C18:3::/64,
     via FE80::200:5EFF:FE04:B601, cost 2
 4000:1::/64,
     via FE80::200:5EFF:FE04:3302, cost 2
 4000:2::/64,
     via FE80::200:5EFF:FE04:3302, cost 2
 1111::/64,
     cost 0, RIPng-interface
```

Table 54 Command output

Field	Description
2001:7B::2:2A1:5DE/64	IPv6 destination address/prefix length
via	Next hop IPv6 address
cost	Route metric value
Imported	Route redistributed from another routing protocol
RIPng-interface	Route learned from the interface

display ripng interface

Syntax

```
display ripng process-id interface [ interface-type interface-number ] [ | { begin | exclude | include }  
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: RIPng process ID, in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ripng interface** to display the interface information of the RIPng process.

If no interface is specified, information about all interfaces of the RIPng process will be displayed.

Examples

```
# Display the interface information of RIPng process 1.
```

```
<Sysname> display ripng 1 interface  
Interface-name: Vlan-interfacell  
Link Local Address: FE80::20F:E2FF:FE30:C16C  
Split-horizon: on Poisson-reverse: off  
MetricIn: 0 MetricOut: 1  
Default route: off  
Summary address:  
3:: 64  
3:: 16  
IPsec policy name: policy001, SPI: 300
```

Table 55 Command output

Field	Description
Interface-name	Name of an interface running RIPng.
Link Local Address	Link-local address of an interface running RIPng.

Field	Description
Split-horizon	Indicates whether the split horizon function is enabled: <ul style="list-style-type: none"> • on—Enabled. • off—Disabled.
Poison-reverse	Indicates whether the poison reverse function is enabled: <ul style="list-style-type: none"> • on—Enabled. • off—Disabled.
MetricIn/MetricOut	Additional metric to incoming and outgoing routes
Default route	<ul style="list-style-type: none"> • Only/Originate—Only means that the interface advertises only the default route. Originate means that the default route and other RIPng routes are advertised. • Off—Indicates that no default route is advertised or the garbage-collect time expires after the default route advertisement was disabled. • In garbage-collect status—With default route advertisement disabled, the interface advertises the default route with metric 16 during the garbage-collect time.
Summary address	The summarized IPv6 prefix and the summary IPv6 prefix on the interface.
IPsec policy name	IPsec policy applied on the interface.
SPI	SPI defined in the IPsec policy.

display ripng route

Syntax

```
display ripng process-id route [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: RIPng process ID, in the range of 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ripng route** to display all RIPng routes and timers associated with each route of a RIPng process.

Examples

Display the routing information of RIPng process 100.

```
<Sysname> display ripng 100 route
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
  -----

Peer FE80::200:5EFF:FE04:B602 on Vlan-interface11
Dest 3FFE:C00:C18:1::/64,
  via FE80::200:5EFF:FE04:B602, cost 2, tag 0, A, 34 Sec

Dest 3FFE:C00:C18:2::/64,
  via FE80::200:5EFF:FE04:B602, cost 2, tag 0, A, 34 Sec

Peer FE80::200:5EFF:FE04:B601 on Vlan-interface12
Dest 3FFE:C00:C18:1::/64,
  via FE80::200:5EFF:FE04:B601, cost 2, tag 0, A, 13 Sec
Dest 3FFE:C00:C18:3::/64,
  via FE80::200:5EFF:FE04:B601, cost 2, tag 0, A, 13 Sec

Peer FE80::200:5EFF:FE04:3302 on Vlan-interface13
Dest 100::/32,
  via FE80::200:5EFF:FE04:3302, cost 2, tag 0, A, 6 Sec
Dest 4000:1::/64,
  via FE80::200:5EFF:FE04:3302, cost 2, tag 0, A, 6 Sec
Dest 4000:2::/64,
  via FE80::200:5EFF:FE04:3302, cost 2, tag 0, A, 6 Sec
Dest 4000:3::/64,
  via FE80::200:5EFF:FE04:3302, cost 2, tag 0, A, 6 Sec
Dest 4000:4::/64,
```

Table 56 Command output

Field	Description
Peer	Neighbor connected to the interface.
Dest	IPv6 destination address.
via	Next hop IPv6 address.
cost	Routing metric value.
tag	Route tag.
Sec	Time that a route entry stays in a particular state.
"A"	The route is in aging state.
"S"	The route is in suppressed state.
"G"	The route is in Garbage-collect state.

enable ipsec-policy (RIPng view)

Syntax

```
enable ipsec-policy policy-name  
undo enable ipsec-policy
```

View

RIPng view

Default level

2: System level

Parameters

policy-name: IPsec policy name, a string of 1 to 15 characters.

Description

Use **enable ipsec-policy** to apply an IPsec policy in a RIPng process.

Use **undo enable ipsec-policy** to remove the IPsec policy from the RIPng process.

By default, no IPsec policy is configured for the RIPng process.

The IPsec policy to be applied must have been configured.

Examples

```
# Apply IPsec policy policy001 to RIPng process 1.  
<Sysname> system-view  
[Sysname] ripng 1  
[Sysname-ripng-1] enable ipsec-policy policy001
```

filter-policy export (RIPng view)

Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } export [ protocol [ process-id ] ]  
undo filter-policy export [ protocol [ process-id ] ]
```

View

RIPng view

Default level

2: System level

Parameters

acl6-number: Specifies the number of an ACL to filter advertised routing information, in the range of 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list used to filter routing information, a string of 1 to 19 characters.

protocol: Filters routes redistributed from a routing protocol, including **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, and **static**.

process-id: Process number of the specified routing protocol, in the range of 1 to 65535. This argument is available only when the routing protocol is **rip**, **ospf**, or **isis**.

Description

Use **filter-policy export** to define an outbound route filtering policy. Only routes passing the filter can be advertised in the update messages.

Use **undo filter-policy export** to disable the outbound route filtering.

By default, RIPng does not filter any outbound routing information.

With the *protocol* argument specified, only routing information redistributed from the specified routing protocol will be filtered. Otherwise, all outgoing routing information will be filtered.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command, the ACL should be configured with the **rule [rule-id] { deny | permit } ipv6 source sour sour-prefix** command to deny/permit a route with the specified destination, or with the **rule [rule-id] { deny | permit } ipv6 source sour sour-prefix destination dest dest-prefix** command to deny/permit a route with the specified destination and prefix. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route (the prefix must be valid; otherwise, the configuration is ineffective).

Examples

Use IPv6 prefix list **Filter 2** to filter advertised RIPng updates.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy ipv6-prefix Filter2 export
```

Configure ACL6 3000 to permit only route 2001::1/128 to pass, and reference ACL6 3000 to filter advertised RIPng updates.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl6-adv-3000] rule 100 deny ipv6
[Sysname-acl6-adv-3000] quit
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy 3000 export
```

filter-policy import (RIPng view)

Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } import  
undo filter-policy import
```

View

RIPng view

Default level

2: System level

Parameters

acl6-number: Specifies the number of an ACL to filter incoming routing information, in the range of 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list to filter incoming routes, in the range of 1 to 19 characters.

Description

Use **filter-policy import** to define an inbound route filtering policy. Only routes which match the filtering policy can be received.

Use **undo filter-policy import** to disable inbound route filtering.

By default, RIPng does not filter incoming routing information.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command, the ACL should be configured with the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* command to deny/permit a route with the specified destination, or with the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix destination dest dest-prefix* command to deny/permit a route with the specified destination and prefix. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route (the prefix must be valid; otherwise, the configuration is ineffective).

Examples

Reference IPv6 prefix list **Filter1** to filter incoming RIPng updates.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy ipv6-prefix Filter1 import
```

Configure ACL6 3000 to permit only route 2001::1/128 to pass, and reference ACL6 3000 to filter incoming RIPng updates.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl6-adv-3000] rule 100 deny ipv6
[Sysname-acl6-adv-3000] quit
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy 3000 import
```

import-route

Syntax

import-route *protocol* [*process-id*] [**allow-ibgp**] [**cost** *cost* | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id*]

View

RIPng view

Default level

2: System level

Parameters

protocol: Specifies a routing protocol from which to redistribute routes. It can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

process-id: Process ID, in the range of 1 to 65535. The default is 1. This argument is available only when the protocol is **isisv6**, **ospfv3**, or **ripng**.

cost: Routing metric of redistributed routes, in the range of 0 to 16. If *cost value* is not specified, the metric is the default metric specified by the **default cost** command.

route-policy *route-policy-name*: Specifies a routing policy by its name with 1 to 63 case-sensitive characters.

allow-ibgp: Optional keyword when the specified *protocol* is **bgp4+**.

Description

Use **import-route** to redistribute routes from another routing protocol.

Use **undo import-route** to disable redistributing routes from another routing protocol.

By default, RIPng does not redistribute routes from other routing protocols.

The **import-route bgp4+** command redistributes only EBGP routes. The **import-route bgp4+ allow-ibgp** command redistributes additionally IBGP routes.

Related commands: **default cost**.

Examples

```
# Redistribute IPv6-IS-IS routes (process 7) and specify the metric as 7.
```

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] import-route isisv6 7 cost 7
```

maximum load-balancing (RIPng view)

Syntax

maximum load-balancing *number*

undo maximum load-balancing

View

RIPng view

Default level

2: System level

Parameters

number: Maximum number of ECMP routes, in the range of 1 to 8.

Description

Use **maximum load-balancing** to specify the maximum number of ECMP routes.

Use **undo maximum load-balancing** to restore the default.

By default, the maximum number of ECMP routes is 8.

Configure the maximum number according to the memory size.

Examples

```
# Set the maximum number of ECMP routes to 2.
```

```
<Sysname> system-view
[Sysname] ripng 100
```

preference

Syntax

```
preference [ route-policy route-policy-name ] preference  
undo preference [ route-policy ]
```

View

RIPng view

Default level

2: System level

Parameters

route-policy-name: Routing policy name with 1 to 63 case-sensitive characters.

value: Preference for RIPng routes, in the range of 1 to 255.

Description

Use **preference** to specify the preference for RIPng routes.

Use **undo preference** to restore the default.

By default, the preference of RIPng routes is 100.

You can specify a routing policy by using the keyword **route-policy** to set a preference for the matching RIPng routes.

- The preference set by the routing policy applies to all matching RIPng routes. The preference of other routes is set by the **preference** command.
- If no preference is set by the routing policy, the preference of all RIPng routes is set by the **preference** command.

Examples

```
# Set the RIPng route preference to 120.  
<Sysname> system-view  
[Sysname] ripng 100  
[Sysname-ripng-100] preference 120  
  
# Restore the default RIPng route preference.  
[Sysname-ripng-100] undo preference
```

reset ripng process

Syntax

```
reset ripng process-id process
```

View

User view

Default level

2: System level

Parameters

process-id: RIPng process ID, in the range of 1 to 65535.

Description

Use **reset ripng process** to reset the specified RIPng process.

After executing the command, you are prompted whether you want to reset the RIPng process.

Examples

```
# Reset RIPng process 100.
<Sysname> reset ripng 100 process
Warning : Reset RIPng process? [Y/N]:Y
```

reset ripng statistics

Syntax

```
reset ripng process-id statistics
```

View

User view

Default level

1: Monitor level

Parameters

process-id: RIPng process ID, in the range of 1 to 65535.

Description

Use **reset ripng statistics** to clear the statistics of the specified RIPng process.

Examples

```
# Clear the statistics of RIPng process 100.
<Sysname> reset ripng 100 statistics
```

ripng

Syntax

```
ripng [ process-id ] [ vpn-instance vpn-instance-name ]
undo ripng [ process-id ] [ vpn-instance vpn-instance-name ]
```

View

System view

Default level

2: System level

Parameters

process-id: RIPng process ID, in the range of 1 to 65535. The default value is 1.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

Description

Use **ripng** to create a RIPng process and enter RIPng view.

Use **undo ripng** to disable a RIPng process.

By default, no RIPng process is enabled.

- If no VPN is specified, the RIPng process is enabled for the public network.
- The specified VPN instance must have been created with the **ip vpn-instance** command.
- Before configuring global RIPng parameters, you must create a RIPng process. This requirement does not apply to interface RIPng parameter configuration.
- After you disable a RIPng process, the RIPng parameters on interface running the process also become ineffective.

Examples

```
# Create RIPng process 100 and enter its view.
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100]

# Disable RIPng process 100.
[Sysname] undo ripng 100

# Create RIPng process 101 and bind it to VPN instance vpn101.
<Sysname> system-view
[Sysname] ripng 101 vpn-instance vpn101
```

ripng default-route

Syntax

```
ripng default-route { only | originate } [ cost cost ]
```

```
undo ripng default-route
```

View

Interface view

Default level

2: System level

Parameters

only: Indicates that only the IPv6 default route (::/0) is advertised through the interface.

originate: Indicates that the IPv6 default route (::/0) is advertised without suppressing other routes.

cost: Metric of the advertised default route, in the range of 1 to 15, with a default value of 1.

Description

Use **ripng default-route** to advertise a default route with the specified routing metric to a RIPng neighbor.

Use **undo ripng default-route** to stop advertising or forwarding the default route.

By default, a RIP process does not advertise any default route.

After you execute this command, the generated RIPng default route is advertised in a route update over the specified interface. This IPv6 default route is advertised without considering whether it already exists in the local IPv6 routing table.

Examples

```
# Advertise only the default route through VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng default-route only

# Advertise the default route together with other routes through VLAN-interface 101.
<Sysname> system-view
[Sysname] interface vlan-interface 101
[Sysname-Vlan-interface101] ripng default-route originate
```

ripng enable

Syntax

```
ripng process-id enable
undo ripng [ process-id ] enable
```

View

Interface view

Default level

2: System level

Parameters

process-id: RIPng process ID, in the range of 1 to 65535.

Description

Use **ripng enable** to enable RIPng on the specified interface.

Use **undo ripng enable** to disable RIPng on the specified interface.

By default, RIPng is disabled on an interface.

Examples

```
# Enable RIPng 100 on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng 100 enable
```

ripng ipsec-policy

Syntax

```
ripng ipsec-policy policy-name
undo ripng ipsec-policy
```

View

Interface view

Default level

2: System level

Parameters

policy-name: IPsec policy name, a string of 1 to 15 characters.

Description

Use **ripng ipsec-policy** to apply an IPsec policy on a RIPng interface.

Use **undo ripng ipsec-policy** to remove the IPsec policy from the RIPng interface.

By default, no IPsec policy is configured for the RIPng interface.

The IPsec policy to be applied must have been configured.

Examples

```
# Apply IPsec policy policy001 to VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] ripng ipsec-policy policy001
```

ripng metricin

Syntax

ripng metricin *value*

undo ripng metricin

View

Interface view

Default level

2: System level

Parameters

value: Additional metric for received routes, in the range of 0 to 16.

Description

Use **ripng metricin** to specify an additional metric for received RIPng routes.

Use **undo ripng metricin** to restore the default.

By default, the additional metric to received routes is 0.

Related commands: **ripng metricout**.

Examples

```
# Specify the additional routing metric as 12 for RIPng routes received by VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] ripng metricin 12
```

ripng metricout

Syntax

```
ripng metricout value  
undo ripng metricout
```

View

Interface view

Default level

2: System level

Parameters

value: Additional metric to advertised routes, in the range of 1 to 16.

Description

Use **ripng metricout** to configure an additional metric for RIPng routes advertised by an interface.

Use **undo rip metricout** to restore the default.

The default additional routing metric is 1.

Related commands: **ripng metricin**.

Examples

```
# Set the additional metric to 12 for routes advertised by VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] ripng metricout 12
```

ripng poison-reverse

Syntax

```
ripng poison-reverse  
undo ripng poison-reverse
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **ripng poison-reverse** to enable the poison reverse function.

Use **undo ripng poison-reverse** to disable the poison reverse function.

By default, the poison reverse function is disabled.

Examples

Enable the poison reverse function for RIPng update messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng poison-reverse
```

ripng split-horizon

Syntax

```
ripng split-horizon
undo ripng split-horizon
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **ripng split-horizon** to enable the split horizon function.

Use **undo ripng split-horizon** to disable the split horizon function.

By default, the split horizon function is enabled.

The split horizon function is necessary for preventing routing loops. Do not disable it unless you make sure that it is necessary.

If both the poison reverse and split horizon functions are enabled, only the poison reverse function takes effect.

Examples

```
# Enable the split horizon function on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng split-horizon
```

ripng summary-address

Syntax

```
ripng summary-address ipv6-address prefix-length
undo ripng summary-address ipv6-address prefix-length
```

View

Interface view

Default level

2: System level

Parameters

ipv6-address: Destination IPv6 address of the summary route.

prefix-length: Prefix length of the destination IPv6 address of the summary route, in the range of 0 to 128. It indicates the number of consecutive 1s of the prefix, which defines the network ID.

Description

Use **ripng summary-address** to configure a summary network to be advertised through the interface.

Use **undo ripng summary-address** to remove the summary.

Networks falling into the summary network will not be advertised. The cost of the summary route is the lowest cost among summarized routes.

Examples

Assign an IPv6 address with the 64-bit prefix to VLAN-interface 100 and configure a summary with the 35-bit prefix length.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001:200::3EFF:FE11:6770/64
[Sysname-Vlan-interface100] ripng summary-address 2001:200:: 35
```

timers

Syntax

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

View

RIPng view

Default level

2: System level

Parameters

garbage-collect-value: Interval of the garbage-collect timer in seconds, in the range of 1 to 86400.

suppress-value: Interval of the suppress timer in seconds, in the range of 0 to 86400.

timeout-value: Interval of the timeout timer in seconds, in the range of 1 to 86400.

update-value: Interval of the update timer in seconds, in the range of 1 to 86400.

Description

Use **timers** to configure RIPng timers.

Use **undo timers** to restore the default.

By default, the garbage-collect timer is 120 seconds, the suppress timer 120 seconds, the timeout timer 180 seconds, and the update timer 30 seconds.

RIPng is controlled by the following timers:

- **Update timer**—Defines the interval between update messages.
- **Timeout timer**—Defines the route aging time. If no update message related to a route is received within the aging time, the metric of the route is set to 16 in the routing table.
- **Suppress timer**—Defines for how long a RIPng route stays in suppressed state. When the metric of a route is 16, the route enters the suppressed state. In suppressed state, only routes which come from

the same neighbor and whose metric is less than 16 will be received by the router to replace unreachable routes.

- **Garbage-collect timer**—Defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIPv2 advertises the route with the routing metric set to 16. If no update message is announced for that route before the garbage-collect timer expires, the route will be completely deleted from the routing table.

ⓘ **IMPORTANT:**

- HP does not recommend changing the default values of these timers under normal circumstances.
 - The lengths of these timers must be kept consistent on all routers in the network.
-

Examples

Configure the update, timeout, suppress, and garbage-collect timers as 5s, 15s, 15s, and 30s.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] timers update 5
[Sysname-ripng-100] timers timeout 15
[Sysname-ripng-100] timers suppress 15
[Sysname-ripng-100] timers garbage-collect 30
```

OSPFv3 configuration commands

The term "router" in the chapter refers to both routers and Layer 3 switches.

The A5500 SI Switch Series does not support OSPFv3.

abr-summary (OSPFv3 area view)

Syntax

abr-summary *ipv6-address prefix-length* [**not-advertise**]

undo abr-summary *ipv6-address prefix-length*

View

OSPFv3 area view

Default level

2: System level

Parameters

ipv6-address: Destination IPv6 address of the summary route.

prefix-length: Prefix length of the destination IPv6 address, in the range of 0 to 128. This argument specifies the number of consecutive 1s of the prefix, which defines the network ID.

not-advertise: Specifies not to advertise the summary IPv6 route.

Description

Use **abr-summary** to configure an IPv6 summary route on an area border router.

Use **undo abr-summary** to remove an IPv6 summary route. Then the summarized routes are advertised.

By default, no route summarization is available on an ABR.

You can use this command only on an ABR to configure a summary route for the area. The ABR advertises only the summary route to other areas. Multiple contiguous networks may be available in an area, where you can summarize them with one route for advertisement.

Examples

```
# Summarize networks 2000:1:1:1::/64 and 2000:1:1:2::/64 in Area 1 with 2000:1:1::/48.
```

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] abr-summary 2000:1:1:: 48
```

area (OSPFv3 view)

Syntax

area *area-id*

View

OSPFv3 view

Default level

2: System level

Parameters

area-id: ID of an area, a decimal integer (in the range of 0 to 4294967295 and changed to IPv4 address format by the system) or an IPv4 address.

Description

Use **area** to enter OSPFv3 area view.

The undo form of the command is not available. An area is removed automatically if no configuration is made and no interface is up in the area.

Examples

```
# Enter OSPFv3 Area 0 view.
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 0
[Sysname-ospfv3-1-area-0.0.0.0]
```

bandwidth-reference

Syntax

```
bandwidth-reference value
undo bandwidth-reference
```

View

OSPFv3 view

Default level

2: System level

Parameters

value: Bandwidth reference value for link cost calculation, in the range of 1 to 2147483648 Mbps.

Description

Use **bandwidth-reference** to specify a reference bandwidth value for link cost calculation.

Use **undo bandwidth-reference** to restore the default value.

The default value is 100 Mbps.

You can configure an OSPFv3 cost for an interface with one of the following methods:

- Configure the cost value in interface view
- Configure a bandwidth reference value, and OSPFv3 computes the cost automatically based on the bandwidth reference value: Interface OSPFv3 cost = Bandwidth reference value/Interface bandwidth. If the calculated cost is greater than 65535, the value of 65535 is used.

If no cost value is configured for an interface, OSPFv3 computes the interface cost value automatically:

Examples

```
# Specify the reference bandwidth value as 1000 Mbps.
<Sysname> system-view
```

```
[Sysname] ospfv3 1
[Sysname-ospfv3-1] bandwidth-reference 1000
```

default cost

Syntax

```
default cost value
undo default cost
```

View

OSPFv3 view

Default level

2: System level

Parameters

value: Specifies a default cost for redistributed routes, in the range of 1 to 16777214.

Description

Use **default cost** to configure a default cost for redistributed routes.

Use **undo default cost** to restore the default.

By default, the default cost is 1.

You need to configure the default cost value for redistributed routes to advertise them throughout the whole AS.

If multiple OSPFv3 processes are available, use of this command takes effect for the current process only.

Examples

```
# Specify the default cost for redistributed routes as 10.
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default cost 10
```

default-cost (OSPFv3 area view)

Syntax

```
default-cost value
undo default-cost
```

View

OSPFv3 area view

Default level

2: System level

Parameters

value: Specifies a cost for the default route advertised to the stub area, in the range of 0 to 65535. The default is 1.

Description

Use **default-cost** to specify the cost of the default route to be advertised to the stub area.

Use **undo default-cost** to restore the default value.

Use of this command is only available on the ABR that is connected to a stub area.

You have two commands to configure a stub area: **stub**, **defaulted-cost**. You need to use the **stub** command on routers connected to a stub area to configure the area as stub.

If multiple OSPFv3 processes are running, use of this command takes effect only for the current process.

Related commands: **stub**.

Examples

Configure Area 1 as a stub area, and specify the cost of the default route advertised to the stub area as 60.

```
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
[Sysname-ospfv3-1-area-0.0.0.1] default-cost 60
```

default-route-advertise

Syntax

```
default-route-advertise [ always | cost value | route-policy route-policy-name | type type ] *
undo default-route-advertise
```

View

OSPFv3 view

Default level

2: System level

Parameters

always: Generates a default route in an ASE LSA into the OSPF routing domain regardless of whether the default route exists in the routing table. Without this keyword, the command can distribute a default route in a Type-5 LSA into the OSPF routing domain only when the default route exists in the routing table.

cost *value*: Specifies a cost for the default route, in the range of 1 to 16777214. The default is 1.

route-policy *route-policy-name*: Specifies a routing policy, a case-sensitive string of 1 to 63 characters.

type *type*: Specifies a type for the ASE LSA: 1 or 2. The default is 2.

Description

Use **default-route-advertise** to generate a default route into the OSPF routing domain.

Use **undo default-route-advertise** to disable OSPF from redistributing a default route.

By default, no default route is redistributed.

Using the **import-route** command cannot redistribute a default route. To do so, you need to use the **default-route-advertise** command. If no default route exists in the router's routing table, use the **default-route-advertise always** command to generate a default route in a Type-5 LSA.

You can reference a routing policy to set the cost and type of the default route:

- The router advertises the default route only when it passes the routing policy.
- The default route passing the routing policy uses the cost set by the **apply cost** clause, and the type set by the **apply cost-type** clause in the routing policy.
- The default route cost's priority from high to low is: the cost set by the **apply cost** clause in the routing policy, the one set by the **default-route-advertise** command and the one set by the **default cost** command.
- The default route type's priority from high to low is: the type set by the **apply cost-type** clause in the routing policy, and the one set by the **default-route-advertise** command.
- If the **always** keyword is included, the default route is advertised regardless of whether it passes the routing policy and uses the cost and type specified by the **apply cost**, **apply cost-type** clauses in the first node of the routing policy.

Related commands: **import-route**.

Examples

```
# Generate a default route into the OSPFv3 routing domain.
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default-route-advertise always
```

display ospfv3

Syntax

```
display ospfv3 [ process-id ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3** to display the brief information of an OSPFv3 process.

If no process ID is specified, OSPFv3 brief information about all processes will be displayed.

Examples

```
# Display brief information about all OSPFv3 processes.
<Sysname> display ospfv3
```

```

Routing Process "OSPFv3 (1)" with ID 1.1.1.1
Graceful restart restarter enabled
Graceful restart helper enabled
Graceful restart helper strict-lsa-checking enabled
Graceful restart interval 150 secs
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
Number of external LSA 0. These external LSAs' checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 3
Number of LSA received 0
Number of areas in this router is 1
  Area 0.0.0.1
    Number of interfaces in this area is 1
    SPF algorithm executed 1 times
    Number of LSA 2. These LSAs' checksum Sum 0x20C8
    Number of Unknown LSA 0
    IPsec policy name: policy001, SPI: 300

```

Table 57 Command output

Field	Description
Routing Process "OSPFv3 (1)" with ID 1.1.1.1	OSPFv3 process is 1, and router ID is 1.1.1.1.
Graceful restart restarter enabled	The current process supports GR.
Graceful restart helper enabled	The current process supports the GR Helper capability.
Graceful restart helper strict-lsa-checking enabled	The current process supports GR Helper strict LSA checking.
Graceful restart interval 150 secs	GR restart interval.
SPF schedule delay	Delay interval of SPF calculation.
Hold time between SPFs	Hold time between SPF calculations.
Minimum LSA interval	Minimum interval for generating LSAs.
Minimum LSA arrival	Minimum LSA repeat arrival interval.
Number of external LSA	Number of ASE LSAs.
These external LSAs' checksum Sum	Sum of all the ASE LSAs' checksum.
Number of AS-Scoped Unknown LSA	Number of LSAs with unknown flooding scope.
Number of LSA originated	Number of LSAs originated.
Number of LSA received	Number of LSAs received.
Number of areas in this router	Number of areas this router is attached to.
Area	Area ID.
Number of interfaces in this area	Number of interfaces attached to this area.
SPF algorithm executed 1 times	SPF algorithm is executed 1 time.
Number of LSA	Number of LSAs.
These LSAs' checksum Sum	Sum of all LSAs' checksum.

Field	Description
Number of Unknown LSA	Number of unknown LSAs.
IPsec policy name	IPsec policy used.
SPI	SPI defined in the IPsec policy.

display ospfv3 graceful-restart status

Syntax

```
display ospfv3 [ process-id ] graceful-restart status [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: ID of an OSPFv3 process, ranging from 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3 graceful-restart status** to display GR status of the specified OSPFv3 process.

If no process ID is specified, GR status of all processes will be displayed.

Examples

Display GR status of all OSPFv3 processes (GR Restarter).

```
<Sysname> display ospfv3 graceful-restart status
      OSPFv3 Router with ID (1.1.1.1) (Process 1)
      graceful restart information
```

```
GR status          : GR in progress
```

```
GR remaining time: 100
```

Display GR status of all OSPFv3 processes (GR Helper).

```
<Sysname> display ospfv3 graceful-restart status
      OSPFv3 Router with ID (1.1.1.1) (Process 1)
      graceful restart information
```

```
GR status: Helper
```

```
Neighbor ID      Interface  Instance ID  Remaining time
1.1.1.1          Vlan11    1            100
2.2.2.2          Vlan20    2            200
```

Table 58 Command output

Field	Description
OSPFv3 Router with ID (1.1.1.1) (Process 1) graceful restart information	The GR status of OSPFv3 process 1 with router ID 1.1.1.1 is displayed.
GR status	GR status, which can be: <ul style="list-style-type: none">• GR in progress—Indicates GR is in process.• Calculating routes—Indicates route calculation is in process.• Flushing LSAs—Indicates the device is flushing stale LSA.• Normal—Indicates the device is not in GR or Helper status.• Helper—Indicates the Helper status.
GR remaining time	Remaining time before the GR timer expires.
Neighbor ID	Router ID of the neighbor router.
Interface	Outbound interface.
Instance ID	Instance ID.

display ospfv3 interface

Syntax

```
display ospfv3 interface [ interface-type interface-number | statistic ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

statistic: Displays the interface statistics.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3 interface** to display OSPFv3 interface information.

Examples

```
# Display OSPFv3 interface information.
```

```

<Sysname> display ospfv3 interface vlan-interface 10
Vlan-interface 10 is up, line protocol is up
  Interface ID 518
  IPv6 Prefixes
    FE80::1441:0:E213:1 (Link-Local Address)
    2000:1::1
  OSPFv3 Process (1), Area 0.0.0.1, Instance ID 0
    Router ID 2.2.2.2, Network Type POINTOPOINT, Cost: 1562
    Transmit Delay is 1 sec, State Point-To-Point, Priority 1
    No designated router on this link
    No backup designated router on this link
    Timer interval configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
      Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
  IPsec policy name: policy001, SPI: 300
  BFD: Enabled

```

Table 59 Command output

Field	Description
Interface ID	Interface ID.
IPv6 Prefixes	IPv6 Prefix.
OSPFv3 Process	OSPFv3 Process.
Area	Area ID.
Instance ID	Instance ID.
Router ID	Router ID.
Network Type	Network type of the interface.
Cost	Cost value of the interface.
Transmit Delay	Transmission delay of the interface.
State	Interface state.
Priority	DR priority of the interface.
No designated router on this link	No designated router on this link.
No backup designated router on this link	No backup designated router on this link.
Timer interval configured	Time intervals in seconds configured on the interface: <ul style="list-style-type: none"> • Hello—Hello interval. • Dead—Dead interval. • Wait—After this timer expires, the interface quits from the waiting state. • Retransmit—LSA retransmission interval.
Hello due in 00:00:02	Hello packet will be sent in 2 seconds.
Neighbor Count	Number of Neighbors on the interface
Adjacent neighbor count	Number of Adjacencies on the interface
IPsec policy name	IPsec policy used on the interface

Field	Description
SPI	SPI defined in the IPsec policy
BFD	BFD status on the interface (enabled or disabled).

display ospfv3 lsdb

Syntax

```
display ospfv3 [ process-id ] lsdb [ [ external | inter-prefix | inter-router | intra-prefix | link | network
| router | grace ] [ link-state-id ] [ originate-router router-id ] | total ] [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: Specifies ID of an OSPFv3 process, ranging from 1 to 65535.

external: Displays information about AS-external LSAs.

inter-prefix: Displays information about Inter-area-prefix LSAs.

inter-router: Displays information about Inter-area-router LSAs.

intra-prefix: Displays information about Intra-area-prefix LSAs.

link: Displays information about Link-LSAs.

network: Displays information about Network-LSAs.

router: Displays information about Router-LSAs.

grace: Displays information about Grace-LSAs

link-state-id: Link state ID, an IPv4 address.

originate-router *router-id*: ID of the advertising router .

total: Displays the LSA statistics in the LSDB.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3 lsdb** to display OSPFv3 LSDB information.

Examples

```
# Display OSPFv3 LSDB information.
```

```
<Sysname> display ospfv3 lsdb
```

OSPFv3 Router with ID (2.2.2.2) (Process 1)

Link-LSA (Interface Vlan-interface10)

Link State ID	Origin Router	Age	Seq#	CkSum	Prefix
0.0.2.6	1.1.1.1	0055	0x80000001	0x4642	0
0.0.2.6	2.2.2.2	0053	0x80000001	0xf267	0

Grace-LSA (Interface Vlan-interface10)

Link State ID	Origin Router	Age	SeqNum	CkSum
0.0.2.6	1.1.1.1	100	0x8000004	0xb1af

Router-LSA (Area 0.0.0.1)

Link State ID	Origin Router	Age	Seq#	CkSum	Link
0.0.0.0	1.1.1.1	0050	0x80000002	0x12d1	1
0.0.0.0	2.2.2.2	0048	0x80000002	0xa142	1

Table 60 Command output

Field	Description
Link-LSA	Type 8 LSA
Link State ID	Link State ID
Origin Router	Originating Router
Age	Age of LSAs
Seq#	LSA sequence number
CkSum	LSA Checksum
Prefix	Number of Prefixes
Router-LSA	Router-LSA
Link	Number of links
Network-LSA	Network-LSA
Intra-Area-Prefix-LSA	Type 9 LSA
Grace-LSA	Type 11 LSA
Reference	Type of referenced LSA

Display Link-local LSA information in the LSDB.

```
<Sysname> display ospfv3 lsdb link
      OSPFv3 Router with ID (2.2.2.2) (Process 1)

      Link-LSA (Interface Vlan-interface20)

      LS age: 11
      LS Type: Link-LSA
      Link State ID: 0.0.2.6
```

```

Originating Router: 2.2.2.2
LS Seq Number: 0x80000002
Checksum: 0xEFFA
Length: 56
Priority: 1
Options: 0x000013 (-|R|-|-|E|V6)
Link-Local Address: FE80::1441:0:E213:1
Number of Prefixes: 1
  Prefix: 2000:1::/64
  Prefix Options: 0 (-|-|-|-)

```

Table 61 Command output

Field	Description
LS age	Age of LSA
LS Type	Type of LSA
Originating Router	Originating Router
LS Seq Number	LSA Sequence Number
Checksum	LSA Checksum
Length	LSA Length
Priority	Router Priority
Options	Options
Link-Local Address	Link-Local Address
Number of Prefixes	Number of Prefixes
Prefix	Address prefix
Prefix Options	Prefix options

Display Grace-LSA information in the LSDB.

```

<Sysname> display ospfv3 lsdb grace
      OSPFv3 Router with ID (1.1.1.1) (Process 1)

      Grace-LSA (Interface Vlan-interface20)

LS age           : 15
LS Type          : Grace-LSA
Link State ID    : 0.0.2.6
Originating Router : 1.1.1.1
LS Seq Number    : 0x80000014
Checksum         : 0XB1F
Length          : 44
Graceful Restart Period: 120
Restart Reason   : 3 - switch-over

```

Table 62 Command output

Field	Description
LS age	Age of LSA
LS Type	Type of LSA
Originating Router	Originating Router
LS Seq Number	LSA Sequence Number
Checksum	LSA Checksum
Length	LSA Length
Graceful Restart Period	GR restart interval
Restart Reason	Cause of the GR restart

Display LSA statistics in the LSDB.

```
<Sysname> display ospfv3 lsdb total
                OSPFv3 (Process 1) Database Total

Type Of LSA           Number
Router-LSA            :      1
Network-LSA           :      0
Inter-Area-Prefix-LSA :      0
Inter-Area-Router-LSA :      0
AS-external-LSA       :      0
Link-LSA              :      1
Intra-Area-Prefix-LSA :      0
Grace-LSA             :      0
Unknown-LSA           :      0

Total Number Of LSAs :      2
```

Table 63 Command output

Field	Description
Type Of LSA	Type of LSA
Number	Number of LSAs
Router-LSA	Type 1 LSA
Network-LSA	Type 2 LSA
Inter-Area-Prefix-LSA	Type 3 LSA
Inter-Area-Router-LSA	Type 4 LSA
AS-external-LSA	Type 5 LSA
Link-LSA	Type 8 LSA
Intra-Area-Prefix-LSA	Type 9 LSA
Grace-LSA	Type 11 LSA
Unknown-LSA	Unknown LSA

Field	Description
Total Number Of LSAs	Total number of LSAs

display ospfv3 lsdb statistic

Syntax

```
display ospfv3 lsdb statistic [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3 lsdb statistic** to display LSA statistics in the OSPFv3 LSDB.

Examples

```
# Display OSPFv3 LSDB statistics.
```

```
<System> display ospfv3 lsdb statistic
```

```

                OSPFv3 Router with ID (1.1.1.1) (Process 1)
                    LSA Statistics
-----
Area ID          Router  Network  InterPre  InterRou  IntraPre  Link  Grace  ASE
0.0.0.0          2       1        1         0         1
0.0.0.1          1       0        1         0         1
Total            3       1        2         0         2         3    0      0

```

Table 64 Command output

Field	Description
Area ID	Area ID
Router	Router-LSA number
Network	Network-LSA number
InterPre	Inter-Area-Prefix-LSA number
InterRou	Inter-Area-Router-LSA number
IntraPre	Intra-Area-Prefix-LSA number

Field	Description
Link	Link-LSA number
Grace	Grace-LSA number
ASE	AS-external-LSA number
Total	Total LSA number

display ospfv3 next-hop

Syntax

```
display ospfv3 [ process-id ] next-hop [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: Specifies ID of an OSPFv3 process, ranging from 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3 next-hop** to display OSPFv3 next hop information.

If no process is specified, next hop information of all OSPFv3 processes is displayed.

Examples

```
# Display OSPFv3 next hop information.
```

```
<Sysname> display ospfv3 next-hop
```

```

                OSPFv3 Router with ID (2.2.2.2) (Process 1)
Neighbor-Id      Next-Hop                Interface  RefCount
1.1.1.1          FE80::20F:E2FF:FE00:1  Vlan11    1

```

Table 65 Command output

Field	Description
Neighbor-Id	Neighboring router ID
Next-hop	Next-hop address
Interface	Outbound interface
RefCount	Reference count

display ospfv3 peer

Syntax

```
display ospfv3 [ process-id ] [ area area-id ] peer [ [ interface-type interface-number ] [ verbose ] | peer-router-id ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

area: Specifies to display neighbor information of the specified area.

area-id: The ID of an area, a decimal integer that is translated into IPv4 address format by the system (in the range of 0 to 4294967295) or an IPv4 address.

interface-type interface-number: Specifies an interface by its type and number.

verbose: Display detailed neighbor information.

peer-router-id: Router-ID of the specified neighbor.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3 peer** to display OSPFv3 neighbor information.

- If no *area-id* is specified, the neighbor information of all areas is displayed.
- If no *process-id* is specified, the information of all processes is displayed.
- If no interface or neighbor Router-ID is specified, the neighbor information of all interfaces is displayed.

Examples

```
# Display the neighbor information of OSPFv3 process 1 on an interface.
```

```
<Sysname> display ospfv3 1 peer vlan-interface 10
                OSPFv3 Process (1)
Neighbor ID    Pri   State           Dead Time   Interface   Instance ID
1.1.1.1        1     Full/ -         00:00:30   vlan10      0
```

Table 66 Command output

Field	Description
Neighbor ID	Router ID of a neighbor

Field	Description
Pri	Priority of neighbor router
State	Neighbor state
Dead Time	Dead time remained
Interface	Interface connected to the neighbor
Instance ID	Instance ID

Display detailed neighbor information of OSPFv3 process 100 of an interface.

```
<Sysname> display ospfv3 1 peer vlan-interface 33 verbose
```

```

                OSPFv3 Process (1)
Neighbor 1.1.1.1 is Full, interface address FE80::20F:E2FF:FE49:8050
  In the area 0.0.0.1 via interface Vlan-interface33
  DR is 1.1.1.1 BDR is 2.2.2.2
  Options is 0x000013 (-|R|-|-|E|V6)
  Dead timer due in 00:00:39
  Neighbor is up for 00:25:31
  Database Summary List 0
  Link State Request List 0
  Link State Retransmission List 0
  Graceful restart state: Normal

```

Table 67 Command output

Field	Description
Neighbor	Neighbor ID.
interface address	Interface address.
In the area 0.0.0.1 via interface Vlan-interface33	Interface Vlan-interface33 belongs to area 1.
DR is 0.0.0.0 BDR is 0.0.0.0	Neither DR nor BDR is elected.
Options is 0x000013 (- R - - E V6)	The option is 0x000013 (- R - - E V6).
Dead timer due in 00:00:29	Dead timer due in 00:00:29
Neighbor is up for 00:06:28	Neighbor is up for 00:06:28.
Database Summary List	Number of LSAs sent in DD packet.
Link State Request List	Number of LSAs in the link state request list.
Link State Retransmission List	Number of LSAs in the link state retransmission list.
Graceful restart state	GR status, which can be: <ul style="list-style-type: none"> • Doing GR—Indicates GR is in process. • Complete GR—Indicates the neighbor has completed GR. • Normal—Indicates normal status. • Helper—Indicates the device is a GR Helper of the neighbor.

display ospfv3 peer statistics

Syntax

```
display ospfv3 peer statistics [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3 peer statistics** to display information about all OSPFv3 neighbors on the router—numbers of neighbors in different states.

Examples

```
# Display information about all OSPFv3 neighbors.
```

```
<Sysname> display ospfv3 peer statistics
```

```
                OSPFv3 Router with ID (1.1.1.1) (Process 1)
                Neighbor Statistics
-----
Area ID          Down      Init      2-way     ExStar    Exchange  Loading  Full
0.0.0.0          0         0         0         0         0         0        1
Total            0         0         0         0         0         0        1
```

Table 68 Command output

Field	Description
Area ID	Area ID.
Down	In this state, neighbor initial state, the router has not received any information from a neighboring router for a period of time.
Init	In this state, the device received a Hello packet from the neighbor but the packet contains no Router ID of the neighbor. Mutual communication is not setup.
2-Way	Indicates mutual communication between the router and its neighbor is available. DR/BDR election is finished under this state (or higher).
ExStart	In this state, the router decides on the initial DD sequence number and master/slave relationship of the two parties.
Exchange	In this state, the router exchanges DD packets with the neighbor.

Field	Description
Loading	In this state, the router sends LSRs to request the neighbor for needed LSAs.
Full	Indicates LSDB synchronization has been accomplished between neighbors.
Total	Total number of neighbors under the same state.

display ospfv3 request-list

Syntax

```
display ospfv3 [ process-id ] request-list [ { external | inter-prefix | inter-router | intra-prefix | link |
network | router | grace } [ link-state-id ] [ originate-router ip-address ] | statistics ] [ | { begin | exclude
| include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPFv3 process ID, in the range of 1 to 65535.

external: Displays the AS-external LSA information of the OSPFv3 link state request list.

inter-prefix: Displays the Inter-area-prefix LSA information of the OSPFv3 link state request list.

inter-router: Displays the Inter-area-router LSA information of the OSPFv3 link state request list.

intra-prefix: Displays the Intra-area-prefix LSA information of the OSPFv3 link state request list.

link: Displays the Link LSA information of the OSPFv3 link state request list.

network: Displays the Network-LSA information of the OSPFv3 link state request list.

router: Displays the Router-LSA information of the OSPFv3 link state request list.

grace: Displays the Grace-LSA information of the OSPFv3 link state request list.

link-state-id: Link state ID, in the format of an IPv4 address.

originate-router ip-address: Specifies the router ID of an advertising router.

statistics: Displays the LSA statistics of the OSPFv3 link state request list.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3 request-list** to display OSPFv3 link state request list information.

If no process is specified, the link state request list information of all OSPFv3 processes is displayed.

Examples

Display the information of OSPFv3 link state request list.

```
<Sysname> display ospfv3 request-list
      OSPFv3 Router with ID (11.1.1.1) (Process 1)
      Interface Vlan11      Area-ID 0.0.0.0
-----
      Nbr-ID      12.1.1.1
LS-Type          LS-ID          AdvRouter      SeqNum        Age  CkSum
Router-LSA      0.0.0.0          12.1.1.1      0x80000014   774  0xe5b0
```

Table 69 Command output

Field	Description
Interface	Interface name
Area-ID	Area ID
Nbr-ID	Neighbor router ID
LS-Type	Type of LSA
LS-ID	Link state ID
AdvRouter	Advertising router
SeqNum	LSA sequence number
Age	Age of LSA
CkSum	Checksum

Display the statistics of OSPFv3 link state request list.

```
<Sysname> display ospfv3 request-list statistics
      OSPFv3 Router with ID (11.1.1.1) (Process 1)
Interface Neighbor      LSA-Count
Vlan11   10.1.1.1      0
```

Table 70 Command output

Field	Description
Interface	Interface name
Neighbor	Neighbor router ID
LSA-Count	Number of LSAs in the request list

display ospfv3 retrans-list

Syntax

```
display ospfv3 [ process-id ] retrans-list [ { external | inter-prefix | inter-router | intra-prefix | link | network | router | grace } [ link-state-id ] [ originate-router ip-address ] | statistics [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: OSPFv3 process ID, in the range of 1 to 65535.

external: Displays the AS-external LSA information of the OSPFv3 link state retransmission list.

inter-prefix: Displays the Inter-area-prefix LSA information of the OSPFv3 link state retransmission list.

inter-router: Displays the Inter-area-router LSA information of the OSPFv3 link state retransmission list.

intra-prefix: Displays the Intra-area-prefix LSA information of the OSPFv3 link state retransmission list.

link: Displays the Link LSA information of the OSPFv3 link state retransmission list.

network: Displays the Network-LSA information of the OSPFv3 link state retransmission list.

router: Displays the Router-LSA information of the OSPFv3 link state retransmission list.

grace: Displays the Grace-LSA information of the OSPFv3 link state retransmission list.

link-state-id: Link state ID, in the format of an IPv4 address.

originate-router ip-address: Specifies the router ID of an advertising router.

statistics: Displays the LSA statistics of the OSPFv3 link state retransmission list.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3 retrans-list** to display the OSPFv3 link state retransmission list.

If no process is specified, the link state retransmission list information of all OSPFv3 processes is displayed.

Examples

```
# Display the information of the OSPFv3 link state retransmission list.
```

```
<Sysname> display ospfv3 retrans-list
      OSPFv3 Router with ID (11.1.1.1) (Process 1)
      Interface Vlan11   Area-ID 0.0.0.0
-----
Nbr-ID   12.1.1.1
LS-Type   LS-ID           AdvRouter        SeqNum           Age   CkSum
Link-LSA  0.15.0.24       12.1.1.1         0x80000003      519   0x7823
Router-LSA 0.0.0.0         12.1.1.1         0x80000014      774   0xe5b0
```

Table 71 Command output

Field	Description
Interface	Interface name

Field	Description
Area-ID	Area ID
Nbr-ID	Neighbor router ID
LS-Type	Type of LSA
LS-ID	Link state ID
AdvRouter	Advertising Router
SeqNum	LSA sequence Number
Age	Age of LSA
CkSum	Checksum

Display the statistics of OSPFv3 link state retransmission list.

```
<Sysname>display ospfv3 retrans-list statistics
                OSPFv3 Router with ID (11.1.1.1) (Process 1)
Interface  Neighbor      LSA-Count
Vlan11    12.1.1.1      2
```

Table 72 Command output

Field	Description
Interface	Interface name
Neighbor	Neighbor ID
LSA-Count	Number of LSAs in the retransmission request list

display ospfv3 routing

Syntax

```
display ospfv3 [ process-id ] routing [ ipv6-address prefix-length | ipv6-address/prefix-length |
abr-routes | asbr-routes | all | statistics ] [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

ipv6-address: IPv6 address prefix.

prefix-length: Prefix length, in the range of 0 to 128.

abr-routes: Displays routes to ABR.

asbr-routes: Displays routes to ASBR.

all: Displays all routes.

statistics: Displays the OSPFv3 routing table statistics .

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3 routing** to display OSPFv3 routing table information.

If no process is specified, routing table information of all OSPFv3 processes is displayed.

Examples

Display OSPFv3 routing table information.

```
<Sysname> display ospfv3 routing
```

```
E1 - Type 1 external route,    IA - Inter area route,    I - Intra area route
E2 - Type 2 external route,    * - Selected route
```

```
OSPFv3 Router with ID (1.1.1.1) (Process 1)
```

```
-----
*Destination: 2001::/64
Type          : I                      Cost          : 1
NextHop       : directly-connected      Interface: Vlan11
```

Table 73 Command output

Field	Description
Destination	Destination network segment
Type	Route type
Cost	Route cost value
Next-hop	Next hop address
Interface	Outbound interface

Display the statistics of OSPFv3 routing table.

```
<Sysname> display ospfv3 routing statistics
```

```
OSPFv3 Router with ID (1.1.1.1) (Process 1)
```

```
OSPFv3 Routing Statistics
```

```
Intra-area-routes : 1
Inter-area-routes : 0
External-routes   : 0
```

Table 74 Command output

Field	Description
Intra-area-routes	Number of Intra-area-routes
Inter-area-routes	Number of inter-area routes

Field	Description
External-routes	Number of external routes

display ospfv3 statistics

Syntax

```
display ospfv3 statistics [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3 statistics** to display outbound/inbound OSPFv3 packet statistics on associated interface(s).

Examples

```
# Display outbound/inbound OSPFv3 packet statistics on associated interfaces.
```

```
<Sysname> display ospfv3 statistics
```

```

                                OSPFv3 Statistics
Interface Vlan-interface11 Instance 0
Type           Input      Output
Hello          189          63
DB Description  10           8
Ls Req         2            1
Ls Upd         16           6
Ls Ack         10           6
Discarded      0            0

```

Table 75 Command output

Field	Description
Interface	Interface name
Instance	Instance number
Type	Type of packet
Input	Number of packets received by the interface

Field	Description
Output	Number of packets sent by the interface
Hello	Hello packet
DB Description	Database description packet
Ls Req	Link state request packet
Ls Upd	Link state update packet
Ls Ack	Link state acknowledgement packet
Discarded	Number of discarded packets

display ospfv3 topology

Syntax

```
display ospfv3 [ process-id ] topology [ area area-id ] [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: Displays the topology information of an OSPFv3 process; The process ID ranges from 1 to 65535.

area: Displays the topology information of the specified area.

area-id: ID of an area, a decimal integer (in the range of 0 to 4294967295) that is translated into IPv4 address format by the system or an IPv4 address.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3 topology** to display OSPFv3 topology information.

If no process is specified, topology information of all OSPFv3 processes is displayed.

Examples

```
# Display OSPFv3 area 1 topology information.
```

```
<Sysname> display ospfv3 topology area 1
```

```
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.1) topology
```

Type	ID(If-Index)	Bits	Metric	Next-Hop	Interface
Rtr	1.1.1.1		--		
Rtr	2.2.2.2		1	2.2.2.2	Vlan11
Rtr	3.3.3.3		1	3.3.3.3	Vlan11
Rtr	4.4.4.4		1	4.4.4.4	Vlan11
Net	4.4.4.4(983049)		1	0.0.0.0	Vlan11

Table 76 Command output

Field	Description
Type	Type of node
ID(If-Index)	Router ID
Bits	Flag bit
Metric	Cost value
Next-Hop	Next hop
Interface	Outbound interface

display ospfv3 vlink

Syntax

```
display ospfv3 [ process-id ] vlink [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

process-id: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ospfv3 vlink** to display OSPFv3 virtual link information.

If no process is specified, virtual link information of all OSPFv3 processes is displayed.

Examples

```
# Display OSPFv3 virtual link information.
```

```
<Sysname> display ospfv3 vlink
Virtual Link VLINK1 to router 1.1.1.1 is up
Transit area :0.0.0.1 via interface Vlan-interface20, instance ID: 0
```

```

Local address: 2000:1::1
Remote address: 2001:1:1::1
Transmit Delay is 1 sec, State: P-To-P,
Timer intervals configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
  Hello due in 00:00:02
  Adjacency state :Full
IPsec policy name: policy001, SPI: 300

```

Table 77 Command output

Field	Description
Virtual Link VLINK1 to router 1.1.1.1 is up	The virtual link VLINK1 to router 1.1.1.1 is up.
Transit area 0.0.0.1 via interface Vlan-interface20	Interface Vlan-interface20 in transit area 0.0.0.1.
instance ID	Instance ID.
Local address	Local IPv6 address.
Remote address	Remote IPv6 address.
Transmit Delay	Transmit delay of sending LSAs.
State	Interface state.
Timer intervals configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5	Timer intervals in seconds: <ul style="list-style-type: none"> • Hello—10 • Dead—40 • Wait—40 • Retransmit—5
Hello due in 00:00:02	Send hello packets in 2 seconds.
Adjacency state	Adjacency state.
IPsec policy name	IPsec policy used on the virtual link.
SPI	SPI defined in the IPsec policy.

enable ipsec-policy (OSPFv3 area view)

Syntax

enable ipsec-policy *policy-name*

undo enable ipsec-policy

View

OSPFv3 area view

Default level

2: System level

Parameters

policy-name: IPsec policy name, a string of 1 to 15 characters.

Description

Use **enable ipsec-policy** to apply an IPsec policy in the OSPFv3 area.

Use **undo enable ipsec-policy** to remove the IPsec policy from the OSPFv3 area.

By default, no IPsec policy is applied in an area.

The IPsec policy to be applied must have been configured.

Examples

```
# Apply IPsec policy policy001 to OSPFv3 area 0.
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 0
[Sysname-ospfv3-1-area-0.0.0.0] enable ipsec-policy policy001
```

filter-policy export (OSPFv3 view)

Syntax

filter-policy { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **export** [**bgp4+** | **direct** | **isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **static**]

undo filter-policy export [**bgp4+** | **direct** | **isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **static**]

View

OSPFv3 view

Default level

2: System level

Parameters

acl6-number: Specifies the ACL6 number, ranging from 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list, a string of up to 19 characters.

bgp4+: Filters IPv6 BGP routes.

direct: Filters direct routes.

isisv6 *process-id*: Specifies to filter the routes of an IPv6 IS-IS process, which is in the range of 1 to 65535.

ospfv3 *process-id*: Specifies to filter the routes of an OSPFv3 process, which is in the range of 1 to 65535.

ripng *process-id*: Specifies to filter the routes of a RIPng process, which is in the range of 1 to 65535.

static: Specifies to filter static routes.

Description

Use **filter-policy export** to filter redistributed routes.

Use **undo filter-policy export** to remove the configuration.

By default, IPv6 OSPFv3 does not filter redistributed routes.

If no protocol is specified, all redistributed routes will be filtered.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command, the ACL should be configured with the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* command to deny/permit a route with the specified destination, or with the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix destination dest dest-prefix* command to deny/permit a route with the specified

destination and prefix. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route (the prefix must be valid; otherwise, the configuration is ineffective).

Using the **filter-policy export** command filters only routes redistributed by the **import-route** command. If the **import-route** command is not configured to redistribute routes from other protocols and other OSPFv3 processes, use of the **filter-policy export** command does not take effect.

Examples

```
# Filter all redistributed routes using IPv6 ACL 2001.
```

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2002:1:: 64
[Sysname-acl6-basic-2001] quit
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 2001 export
```

```
# Configure ACL6 3000 to permit only route 2001::1/128 to pass, and reference ACL6 3000 to filter redistributed routes.
```

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl6-adv-3000] rule 100 deny ipv6
[Sysname-acl6-adv-3000] quit
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 3000 export
```

filter-policy import (OSPFv3 view)

Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } import  
undo filter-policy import
```

View

OSPFv3 view

Default level

2: System level

Parameters

acl6-number: Specifies an ACL number, ranging from 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list, a string of up to 19 characters.

Description

Use **filter-policy import** to configure OSPFv3 to filter routes computed from received LSAs.

Use **undo filter-policy import** to remove the configuration.

By default, OSPFv3 does not filter routes computed from received LSAs.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command, the ACL should be configured with the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* command to

deny/permit a route with the specified destination, or with the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix destination dest dest-prefix* command to deny/permit a route with the specified destination and prefix. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route (the prefix must be valid; otherwise, the configuration is ineffective).

Using the **filter-policy import** command only filters routes computed by OSPFv3. The routes that fail to pass are not added to the routing table.

Examples

```
# Filter received routes using the IPv6 prefix list abc.
<Sysname> system-view
[Sysname] ip ipv6-prefix abc permit 2002:1:: 64
[Sysname] ospfv3 1
[Sysname-ospfv3-1] filter-policy ipv6-prefix abc import

# Configure ACL6 3000 to permit only route 2001::1/128 to pass, and reference ACL6 3000 to filter
received routes.
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl6-adv-3000] rule 100 deny ipv6
[Sysname-acl6-adv-3000] quit
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 3000 import
```

graceful-restart enable

Syntax

```
graceful-restart enable
undo graceful-restart enable
```

View

OSPFv3 view

Default level

2: System level

Parameters

None

Description

Use **graceful-restart enable** to enable the GR capability for OSPFv3.

Use **undo graceful-restart enable** to disable the GR capability for OSPFv3.

By default, the GR capability for OSPFv3 is disabled.

You cannot enable the GR capability for an area of the current process already configured with the **vlink-peer** command.

Examples

```
# Enable the GR capability for OSPFv3 process 1.
```



```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart enable
```

graceful-restart helper enable

Syntax

```
graceful-restart helper enable
undo graceful-restart helper enable
```

View

OSPFv3 view

Default level

2: System level

Parameters

None

Description

Use **graceful-restart helper enable** to enable the GR Helper capability for OSPFv3.

Use **undo graceful-restart helper enable** to disable the GR Helper capability for OSPFv3.

By default, the GR Helper capability for OSPFv3 is enabled.

Examples

```
# Enable the GR Helper capability for OSPFv3 process 1.
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart helper enable
```

graceful-restart helper strict-lsa-checking

Syntax

```
graceful-restart helper strict-lsa-checking
undo graceful-restart helper strict-lsa-checking
```

View

OSPFv3 view

Default level

2: System level

Parameters

None

Description

Use **graceful-restart helper strict-lsa-checking** to enable strict LSA checking for the GR Helper. When an LSA change on the GR Helper is detected, the GR Helper device exits the GR Helper mode.

Use **undo graceful-restart helper strict-lsa-checking** to disable strict LSA checking for the GR Helper.

By default, strict LSA checking for the GR Helper is disabled.

Examples

```
# Enable strict LSA checking for the GR Helper in OSPFv3 process 1.
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart helper strict-lsa-checking
```

graceful-restart interval

Syntax

graceful-restart interval *interval-value*

undo graceful-restart interval

View

OSPFv3 view

Default level

2: System level

Parameters

interval-value: GR restart interval, in the range of 40 to 1800 seconds.

Description

Use **graceful-restart interval** to configure the GR restart interval.

Use **undo graceful-restart interval** to restore the default.

By default, the GR restart interval is 120 seconds.

The value of the GR restart interval cannot be smaller than the maximum OSPFv3 neighbor dead time of all the OSPFv3 interfaces; otherwise, GR restart may fail.

Related commands: **ospfv3 timer dead**.

Examples

```
# Configure the GR restart interval for OSPFv3 process 1 as 100 seconds.
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart interval 100
```

import-route (OSPFv3 view)

Syntax

import-route *protocol* [*process-id* | **allow-ibgp**] [**cost** *value* | **route-policy** *route-policy-name* | **type** *type*] *

undo import-route *protocol* [*process-id*]

View

OSPFv3 view

Default level

2: System level

Parameters

protocol: Redistributes routes from a specified routing protocol, which can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

process-id: Process ID of the routing protocol, in the range of 1 to 65536. It defaults to 1. This argument takes effect only when the protocol is **isisv6**, **ospfv3**, or **ripng**.

allow-ibgp: Allows redistributing IBGP routes. This keyword takes effect only the protocol is **bgp4+**.

cost value: Specifies a cost for redistributed routes, ranging from 1 to 16777214. The default is 1.

route-policy route-policy-name: Redistributes only the routes that match the specified routing policy. *route-policy-name* is a case-sensitive string of 1 to 63 characters.

type type: Specifies the type for redistributed routes, 1 or 2. It defaults to 2.

NOTE:

Using the **import-route bgp4+** command redistributes only eBGP routes, and using the **import-route bgp4+ allow-ibgp** command redistributes both eBGP and IBGP routes.

Description

Use **import-route** to redistribute routes.

Use **undo import-route** to disable routes redistribution.

IPv6 OSPFv3 does not redistribute routes from other protocols by default.

Examples

```
# Configure to redistribute routes from RIPng and specify the type as type 2 and cost as 50.
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] import-route ripng 10 type 2 cost 50

# Configure OSPFv3 process 100 to redistribute the routes found by OSPFv3 process 160.
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] import-route ospfv3 160
```

log-peer-change

Syntax

log-peer-change

undo log-peer-change

View

OSPFv3 view

Default level

2: System level

Parameters

None

Description

Use **log-peer-change** to enable the logging on neighbor state changes.

Use **undo log-peer-change** to disable the logging.

With this feature enabled, information about neighbor state changes of the current OSPFv3 process will display on the configuration terminal.

Examples

```
# Disable the logging on neighbor state changes of OSPFv3 process 100.
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] undo log-peer-change
```

maximum load-balancing (OSPFv3 view)

Syntax

maximum load-balancing *maximum*

undo maximum load-balancing

View

OSPFv3 view

Default level

2: System level

Parameters

maximum: Maximum number of ECMP routes , in the range of 1 to 8.

Description

Use **maximum load-balancing** to configure the maximum number of ECMP routes.

Use **undo maximum load-balancing** to restore the default.

By default, the maximum number of ECMP routes is 8.

Examples

```
# Configure the maximum number of ECMP routes as 6.
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] maximum load-balancing 6
```

ospfv3

Syntax

ospfv3 [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo ospfv3 [*process-id*]

View

System view

Default level

2: System level

Parameters

process-id: OSPFv3 process ID, ranging from 1 to 65535. The process ID defaults to 1.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the OSPFv3 process belongs to the public network.

Description

Use **ospfv3** to enable an OSPFv3 process and enter OSPFv3 view.

Use **undo ospfv3** to disable an OSPFv3 process.

The system runs no OSPFv3 process by default.

An OSPFv3 process can run properly only when router ID is configured in OSPFv3 view. Otherwise, you can find the process, but which cannot generate any LSA.

Related commands: **router-id**.

Examples

Enable the OSPFv3 process with process ID as 120 and configure the Router ID as 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospfv3 120
[Sysname-ospfv3-120] router-id 1.1.1.1
```

ospfv3 area

Syntax

ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

undo ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

View

Interface view

Default level

2: System level

Parameters

process-id: OSPFv3 process ID, in the range of 1 to 65535.

area-id: Area ID, a decimal integer (in the range of 0 to 4294967295) that is translated into IPv4 address format by the system or an IPv4 address.

instance-id: Instance ID of an interface, in the range of 0 to 255. The default is 0.

Description

Use **ospfv3 area** to enable an OSPFv3 process on the interface and specify the area for the interface.

Use **undo ospfv3 area** to disable an OSPFv3 process.

OSPFv3 is not enabled on an interface by default.

Examples

Enable OSPFv3 process 1 on an interface that belongs to instance 1 and specify area 1 for the interface.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 1 area 1 instance 1
```

ospfv3 bfd enable

Syntax

```
ospfv3 bfd enable [ instance instance-id ]
undo ospfv3 bfd enable [ instance instance-id ]
```

View

Interface view

Default level

2: System level

Parameters

instance-id: Instance ID of the interface. It ranges from 0 to 255 and defaults to 0.

Description

Use **ospfv3 bfd enable** to enable BFD for link failure detection on an OSPFv3 interface.

Use **undo ospfv3 bfd enable** to disable BFD on the OSPFv3 interface.

By default, the OSPFv3 interface is not enabled with BFD.

Examples

```
# Enable BFD on VLAN-interface 11 in instance 1.
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] ospfv3 bfd enable instance 1
```

ospfv3 cost

Syntax

```
ospfv3 cost value [ instance instance-id ]
undo ospfv3 cost [ value ] [ instance instance-id ]
```

View

Interface view

Default level

2: System level

Parameters

value: OSPFv3 cost, in the range of 0 to 65535 for a loopback interface and 1 to 65535 for other interfaces.

instance-id: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description

Use **ospfv3 cost** to configure the OSPFv3 cost of the interface in an instance.

Use **undo ospfv3 cost** to restore the default OSPFv3 cost of the interface in an instance.

The default cost depends on the interface type: 1 for a VLAN interface; 0 for a loopback interface; computed according to the bandwidth for other interfaces with the formula: Interface OSPF cost = Bandwidth reference value (100 Mbps) ÷ Interface bandwidth (Mbps).

If the calculated cost is greater than 65535, the value of 65535 is used; if the calculated cost is smaller than 1, the value of 1 is used.

Examples

```
# Specifies the OSPFv3 cost of the interface in instance 1 as 33.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 cost 33 instance 1
```

ospfv3 dr-priority

Syntax

```
ospfv3 dr-priority priority [ instance instance-id ]
undo ospfv3 dr-priority [ priority ] [ instance instance-id ]
```

View

Interface view

Default level

2: System level

Parameters

priority: DR priority, in the range of 0 to 255.

instance-id: ID of the instance an interface belongs to, in the range of 0 to 255, which defaults to 0.

Description

Use **ospfv3 dr-priority** to set the DR priority for an interface in an instance.

Use **undo ospfv3 dr-priority** to restore the default value.

The DR priority on an interface defaults to 1.

An interface's DR priority determines its privilege in DR/BDR selection, and the interface with the highest priority is preferred.

Examples

```
# Set the DR priority for an interface in instance 1 to 8.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 dr-priority 8 instance 1
```

ospfv3 ipsec-policy

Syntax

```
ospfv3 ipsec-policy policy-name [ instance instance-id ]  
undo ospfv3 ipsec-policy policy-name [ instance instance-id ]
```

View

Interface view

Default level

2: System level

Parameters

policy-name: IPsec policy name, a string of 1 to 15 characters.

instance-id: ID of the instance of the interface, in the range of 0 to 255. It defaults to 0.

Description

Use **ospfv3 ipsec-policy** to apply an IPsec policy on an OSPFv3 interface.

Use **undo ospfv3 ipsec-policy** to remove the IPsec policy from the OSPFv3 interface.

By default, no IPsec policy is applied on an OSPFv3 interface.

The IPsec policy to be applied must have been configured.

Examples

```
# Apply IPsec policy policy001 to OSPFv3 interface VLAN-interface 10.  
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] ospfv3 ipsec-policy policy001 instance 1
```

ospfv3 mtu-ignore

Syntax

```
ospfv3 mtu-ignore [ instance instance-id ]  
undo ospfv3 mtu-ignore [ instance instance-id ]
```

View

Interface view

Default level

2: System level

Parameters

instance-id: Instance ID, in the range of 0 to 255, which defaults to 0.

Description

Use **ospfv3 mtu-ignore** to configure an interface to ignore MTU check during DD packet exchange.

Use **undo ospfv3 mtu-ignore** to restore the default.

By default, an interface performs MTU check during DD packet exchange. A neighbor relationship can be established only if the interface's MTU is the same as that of the peer.

Examples

```
# Configure an interface that belongs to instance 1 to ignore MTU check during DD packet exchange.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 mtu-ignore instance 1
```

ospfv3 network-type

Syntax

```
ospfv3 network-type { broadcast | nbma | p2mp [ non-broadcast ] | p2p } [ instance instance-id ]
undo ospfv3 network-type [ broadcast | nbma | p2mp [ non-broadcast ] | p2p ] [ instance instance-id ]
```

View

Interface view

Default level

2: System level

Parameters

broadcast: Specifies the network type as Broadcast.

nbma: Specifies the network type as NBMA.

p2mp: Specifies the network type as P2MP.

p2p: Specifies the network type as P2P.

non-broadcast: Specifies the interface to send packets in unicast mode. By default, an OSPFv3 interface whose network type is P2MP sends packets in multicast mode.

instance-id: The instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description

Use **ospfv3 network-type** to set the network type for an OSPFv3 interface.

Use **undo ospfv3 network-type** to restore the default.

By default, the network type of an interface depends on its link layer protocol. For example:

- For PPP, the default network type is P2P.
- For Ethernet, the default network type is broadcast.

Examples

```
# Configure the interface's network type as NBMA.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 network-type nbma
```

ospfv3 peer

Syntax

```
ospfv3 peer ipv6-address [ dr-priority dr-priority ] [ instance instance-id ]
undo ospfv3 peer ipv6-address [ dr-priority dr-priority ] [ instance instance-id ]
```

View

Interface view

Default level

2: System level

Parameters

ipv6-address: Neighbor link-local IP address.

dr-priority: Neighbor DR priority, in the range of 0 to 255. The default is 1.

instance-id: Interface instance ID, in the range of 0 to 255. The default is 0.

Description

Use **ospfv3 peer** to specify a neighbor and the DR priority of the neighbor.

Use **undo ospfv3 peer** to remove the configuration.

A router uses the priority set with the **ospfv3 peer** command to determine whether to send a hello packet to the neighbor rather than use it for DR election.

Examples

```
# Specify the neighbor fe80::1111.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 peer fe80::1111
```

ospfv3 timer dead

Syntax

```
ospfv3 timer dead seconds [ instance instance-id ]
undo ospfv3 timer dead [ seconds ] [ instance instance-id ]
```

View

Interface view

Default level

2: System level

Parameters

seconds: Dead time in seconds, ranging from 1 to 65535.

instance-id: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description

Use **ospfv3 timer dead** to configure the OSPFv3 neighbor dead time for an interface that belongs to a specified instance.

Use **undo ospfv3 timer dead** to restore the default.

By default, the OSPFv3 neighbor dead time is 40 seconds for P2P and Broadcast interfaces, and is not supported on P2MP and NBMA interfaces.

OSPFv3 neighbor dead time: if an interface receives no hello packet from a neighbor after dead time elapses, the interface will consider the neighbor dead.

The **dead seconds** value is at least four times the **Hello seconds** value and must be identical on interfaces attached to the same network segment.

Related commands: **ospfv3 timer hello**.

Examples

```
# Configure the OSPFv3 neighbor dead time as 80 seconds for the interface in instance 1.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer dead 80 instance 1
```

ospfv3 timer hello

Syntax

```
ospfv3 timer hello seconds [ instance instance-id ]
undo ospfv3 timer hello [ seconds ] [ instance instance-id ]
```

View

Interface view

Default level

2: System level

Parameters

seconds: Interval between hello packets, ranging from 1 to 65535.

instance-id: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description

Use **ospfv3 timer hello** to configure the hello interval for an interface that belongs to an instance.

Use **undo ospfv3 timer hello** to restore the default .

By default, the hello interval is 10 seconds for P2P and Broadcast interfaces, and is not supported on the P2MP or NBMA interfaces.

Related commands: **ospfv3 timer dead**.

Examples

```
# Configure the hello interval as 20 seconds for an interface in instance 1.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer hello 20 instance 1
```

ospfv3 timer retransmit

Syntax

```
ospfv3 timer retransmit interval [ instance instance-id ]
undo ospfv3 timer retransmit [ interval ] [ instance instance-id ]
```

View

Interface view

Default level

2: System level

Parameters

interval: LSA retransmission interval in seconds, ranging from 1 to 65535.

instance-id: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description

Use **ospfv3 timer retransmit** to configure the LSA retransmission interval for an interface in an instance.

Use **undo ospfv3 timer retransmit** to restore the default.

The interval defaults to 5 seconds.

After sending a LSA to its neighbor, the device waits for an acknowledgement. If receiving no acknowledgement after the LSA retransmission interval elapses, it will retransmit the LSA.

The LSA retransmission interval should not be too small for avoidance of unnecessary retransmissions.

Examples

Configure the LSA retransmission interval on an interface in instance 1 as 12 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer retransmit 12 instance 1
```

ospfv3 timer poll

Syntax

ospfv3 timer poll *seconds* [**instance** *instance-id*]

undo ospfv3 timer poll [*seconds*] [**instance** *instance-id*]

View

Interface view

Default level

2: System level

Parameters

seconds: Poll interval in seconds, in the range of 1 to 65535.

instance-id: Interface instance ID, in the range of 0 to 255. The default is 0.

Description

Use **ospfv3 timer poll** to set the poll interval on an NBMA interface.

Use **undo ospfv3 timer poll** to restore the default value.

By default, the poll interval is 120 seconds.

Examples

Set the poll timer interval on the current interface to 130 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer poll 130
```

ospfv3 trans-delay

Syntax

```
ospfv3 trans-delay seconds [ instance instance-id ]  
undo ospfv3 trans-delay [ seconds ] [ instance instance-id ]
```

View

Interface view

Default level

2: System level

Parameters

seconds: Transmission delay in seconds, ranging from 1 to 3600.

instance-id: Instance ID of an interface, in the range of 0 to 255, with the default as 0.

Description

Use **ospfv3 trans-delay** to configure the transmission delay for an interface with an instance ID.

Use **undo ospfv3 trans-delay** to restore the default.

The transmission delay defaults to 1s.

As LSAs are aged in the LSDB (incremented by 1 every second) but not aged on transmission, it is necessary to add a delay time to the age time before sending a LSA. This configuration is important for low-speed networks.

Examples

```
# Configure the transmission delay as 3 seconds for an interface in instance 1.  
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] ospfv3 trans-delay 3 instance 1
```

preference

Syntax

```
preference [ ase ] [ route-policy route-policy-name ] preference  
undo preference [ ase ]
```

View

OSPFv3 view

Default level

2: System level

Parameters

ase: Applies the preference to OSPFv3 external routes. If the keyword is not specified, the preference applies to OSPFv3 internal routes.

route-policy *route-policy-name*: References a routing policy to set preference for specific routes. The name is a case-sensitive string of 1 to 63 characters.

Preference: Preference of OSPFv3, in the range of 1 to 255.

Description

Use **preference** to specify a preference for OSPFv3 routes.

Use **undo preference** to restore the default.

By default, the preference for OSPFv3 internal routes is 10, and that for OSPFv3 external routes is 150.

The smaller the value is, the higher the preference is.

A router may run multiple routing protocols. Each protocol has a preference. When several routing protocols find multiple routes to the same destination, the route found by the protocol with the highest preference is selected.

Examples

```
# Set a preference of 150 for OSPFv3 routes.
```

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] preference 150
```

router-id

Syntax

router-id *router-id*

undo router-id

View

OSPFv3 view

Default level

2: System level

Parameters

router-id: 32-bit router ID, in IPv4 address format.

Description

Use **router-id** to configure the OSPFv3 router ID.

Use **undo router-id** to remove a configured router ID.

Router ID is the unique identifier of a device running an OSPFv3 process in the AS. The OSPFv3 process cannot run without a Router ID.

Make sure that different processes have different Router IDs.

By configuring different router IDs for different processes, you can run multiple OSPFv3 processes on a router.

Related commands: **ospfv3**.

Examples

```
# Configure the Router ID as 10.1.1.3 for OSPFv3 process 1.
```

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] router-id 10.1.1.3
```

silent-interface(OSPFv3 view)

Syntax

```
silent-interface { interface-type interface-number | all }  
undo silent-interface { interface-type interface-number | all }
```

View

OSPFv3 view

Default level

2: System level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

all: Specifies all interfaces.

Description

Use **silent-interface** to disable the specified interface from receiving and sending OSPFv3 packets.

Use **undo silent-interface** to restore the default.

An interface is able to receive and send OSPFv3 packets by default.

Multiple processes can disable the same interface from receiving and sending OSPFv3 packets, but use of the **silent-interface** command takes effect only on interfaces enabled with the current process.

Examples

```
# Disable an interface from receiving and sending OSPFv3 packets in OSPFv3 processes 100 and 200.  
<Sysname> system-view  
[Sysname] ospfv3 100  
[Sysname-ospfv3-100] router-id 10.110.1.9  
[Sysname-ospfv3-100] silent-interface vlan-interface 10  
[Sysname-ospfv3-100] quit  
[Sysname] ospfv3 200  
[Sysname-ospfv3-200] router-id 20.18.0.7  
[Sysname-ospfv3-200] silent-interface vlan-interface 10
```

spf timers

Syntax

```
spf timers delay-interval hold-interval  
undo spf timers
```

View

OSPFv3 view

Default level

2: System level

Parameters

delay-interval: Interval in seconds between when OSPFv3 receives a topology change and when it starts SPF calculation. in the range of 0 to 65535.

hold-interval: Hold interval in seconds between two consecutive SPF calculations, in the range of 0 to 65535.

Description

Use **spf timers** to configure the delay interval and hold interval for OSPFv3 SPF calculation.

Use **undo spf timers** to restore the default.

The delay interval and hold interval default to 5s and 10s.

An OSPFv3 router works out a shortest path tree with itself as root based on the LSDB, and decides on the next hop to a destination network according the tree. Adjusting the SPF calculation interval can restrain bandwidth and router resource from over consumption due to frequent network changes.

Setting both the *delay-interval* and *hold-interval* to 0 triggers an SPF calculation at once, improving the network convergence speed.

Examples

```
# Configure the delay interval and hold interval as 6 seconds for SPF calculation.
```

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] spf timers 6 6
```

stub (OSPFv3 area view)

Syntax

```
stub [ no-summary ]
```

```
undo stub
```

View

OSPFv3 area view

Default level

2: System level

Parameters

no-summary: This argument is only applicable to the ABR of a stub area. With it configured, the ABR advertises only a default route in a Summary-LSA to the stub area (such an area is called a totally stub area).

Description

Use **stub** to configure an area as a stub area.

Use **undo stub** to remove the configuration.

By default, an area is not configured as a stub area.

When an area is configured as a stub area, all the routers attached to the area must be configured with the **stub** command.

Related commands: **default-cost**.

Examples

```
# Configure OSPFv3 area 1 as a stub area.
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
```

vlink-peer (OSPFv3 area view)

Syntax

vlink-peer *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **instance** *instance-id* | **ipsec-policy** *policy-name*] *

undo vlink-peer *router-id* [**hello** | **retransmit** | **trans-delay** | **dead** | **ipsec-policy**] *

View

OSPFv3 area view

Default level

2: System level

Parameters

router-id: Router ID for a virtual link neighbor.

hello *seconds*: Specifies the interval in seconds for sending Hello packets, ranging from 1 to 8192, with the default as 10. This value must be equal to the **hello** *seconds* configured on the virtual link peer.

retransmit *seconds*: Specifies the interval in seconds for retransmitting LSA packets, ranging from 1 to 3600, with the default as 5.

trans-delay *seconds*: Specifies the delay interval in seconds for sending LSA packets, ranging from 1 to 3600, with the default as 1.

dead *seconds*: Specifies the neighbor dead time in seconds, ranging from 1 to 32768, with the default as 40. This value must be equal to the **dead** *seconds* configured on the virtual link peer, and at least four times the value of **hello** *seconds*.

instance *Instance-id*: Instance ID of an virtual link, in the range of 0 to 255, with the default as 0.

ipsec-policy *policy-name*: Applies an IPsec policy, a string of 1 to 15 characters.

Description

Use **vlink-peer** to create and configure a virtual link.

Use **undo vlink-peer** to remove a virtual link.

For a non-backbone area without a direct connection to the backbone area or for a backbone area that cannot maintain connectivity, you can use the **vlink-peer** command to create logical links. A virtual link can be considered as an interface with OSPFv3 enabled, because parameters such as **hello**, **dead**, **retransmit** and **trans-delay** are configured in the similar way.

Both ends of a virtual link are ABRs that are configured with the **vlink-peer** command.

If you have enabled the GR capability for the current process, you cannot execute the **vlink-peer** command for the process.

Examples

Create a virtual link to 10.110.0.3.

```
<Sysname> system-view
```

```
[Sysname] ospfv3 1
```

```
[Sysname-ospfv3-1] area 10.0.0.0
```

```
[Sysname-ospfv3-1-area-10.0.0.0] vlink-peer 10.110.0.3
```

IPv6 IS-IS configuration commands

IPv6 IS-IS supports all the features of IPv4 IS-IS except that it advertises IPv6 routing information instead. This document describes only IPv6 IS-IS exclusive commands. See ["IS-IS configuration commands"](#) for other IS-IS configuration commands.

The term "router" in this chapter refers to both routers and Layer 3 switches.

The A5500 SI Switch Series does not support IPv6 IS-IS.

display isis route ipv6

Syntax

```
display isis route ipv6 [ [ level-1 | level-2 ] | verbose ] * [ process-id | vpn-instance vpn-instance-name ]  
[ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

level-1: Display Level-1 IPv6 IS-IS routes only.

level-2: Displays Level-2 IPv6 IS-IS routes only.

verbose: Displays detailed IPv6 IS-IS routing information.

process-id: IS-IS process ID, in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN. *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

NOTE:

If no level is specified, both Level-1 and Level-2 (Level-1-2) routing information will be displayed.

Description

Use **display isis route ipv6** to display IPv6 IS-IS routing information.

Examples

```
# Display IPv6 IS-IS routing information.
```

<Sysname> display isis route ipv6

```
Route information for ISIS(1)
-----

ISIS(1) IPv6 Level-1 Forwarding Table
-----
Destination: 2001:1::                               PrefixLen: 64
Flag       : R/L/-                                   Cost      : 20
Next Hop   : FE80::200:5EFF:FE64:8905               Interface: Vlan11

Destination: 2001:2::                               PrefixLen: 64
Flag       : D/L/-                                   Cost      : 10
Next Hop   : Direct                                  Interface: Vlan11

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

```
ISIS(1) IPv6 Level-2 Forwarding Table
-----
Destination: 2001:1::                               PrefixLen: 64
Flag       : -/-/-                                   Cost      : 20

Destination: 2001:2::                               PrefixLen: 64
Flag       : D/L/-                                   Cost      : 10
Next Hop   : Direct                                  Interface: Vlan11

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

Table 78 Command output

Field	Description
Destination	IPv6 destination address prefix.
PrefixLen	Length of the prefix.
Flag/Flags	Flag of routing information status: <ul style="list-style-type: none">• D—This is a direct route.• R—The route has been added into the routing table.• L—The route has been advertised in an LSP.• U—Route leaking flag, indicating the Level-1 route is from Level-2. U means the route will not be returned to Level-2.
Cost	Value of cost.
Next Hop	Next hop.
Interface	Outbound interface.

Display detailed IPv6 IS-IS routing information of VPN instance 1.

<Sysname> display isis route ipv6 verbose vpn-instance vpn1

Route information for ISIS(vpn1-1)

ISIS(1) IPv6 Level-1 Forwarding Table

```

IPV6 Dest   : 2001:1::/64                Cost : 20                Flag : R/L/-
Admin Tag   : -                          Src Count : 1
NextHop     :                             Interface :                 ExitIndex :
    FE80::200:5EFF:FE64:8905             Vlan11                   0x00000003

IPV6 Dest   : 2001:2::/64                Cost : 10                Flag : D/L/-
Admin Tag   : -                          Src Count : 2
NextHop     :                             Interface :                 ExitIndex :
    Direct                                 Vlan11                   0x00000000
    
```

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

-----ISIS(1) IPv6 Level-2 Forwarding Table-----

```

IPV6 Dest   : 2001:1::/64                Cost : 20                Flag : -/-/-
Admin Tag   : -                          Src Count : 1

IPV6 Dest   : 2001:2::/64                Cost : 10                Flag : D/L/-
Admin Tag   : -                          Src Count : 2
NextHop     :                             Interface :                 ExitIndex :
    Direct                                 Vlan11                   0x00000000
    
```

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

Table 79 Command output

Field	Description
IPV6 Dest	IPv6 destination.
Cost	Value of cost.
Flag/Flags	Flag of routing information status: <ul style="list-style-type: none"> • D—This is a direct route. • R—The route has been added into the routing table. • L—The route has been advertised in an LSP. • U—Route leaking flag, indicating the Level-1 route is from Level-2. U means the route will not be returned to Level-2.
Admin Tag	Administrative tag.
Src Count	Number of advertisement sources.
Next Hop	Next hop.
Interface	Outbound interface.
ExitIndex	Outbound interface index.

ipv6 default-route-advertise

Syntax

```
ipv6 default-route-advertise [ [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name ] *
```

```
undo ipv6 default-route-advertise [ route-policy route-policy-name ]
```

View

IS-IS view

Default level

2: System level

Parameters

level-1: Specifies the default route as Level-1.

level-1-2: Specifies the default route as Level-1-2.

level-2: Specifies the default route as Level-2.

route-policy-name: Specifies the name of a routing policy with a case-sensitive string of 1 to 63 characters.

NOTE:

If no level is specified, the default route belongs to Level-2.

Description

Use **ipv6 default-route-advertise** to generate a Level-1 or Level-2 IPv6 IS-IS default route.

Use **undo ipv6 default-route-advertise** to disable generating a default route.

No IPv6 IS-IS default route is generated by default.

With a routing policy, you can configure IPv6 IS-IS to generate the default route that must match the routing policy. You can use the **apply isis level-1** command in routing policy view to generate a default route in L1 LSPs, or use the **apply isis level-2** command in routing policy view to generate a default route in L2 LSPs, and use the **apply isis level-1-2** in routing policy view to generate a default route in L1 and L2 LSPs.

Related commands: **apply isis**.

Examples

```
# Configure the router to generate a default route in Level-2 LSPs.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] ipv6 default-route-advertise
```

ipv6 enable

Syntax

```
ipv6 enable
```

```
undo ipv6 enable
```

View

IS-IS view

Default level

2: System level

Parameters

None

Description

Use **ipv6 enable** to enable IPv6 for the IPv6 IS-IS process.

Use **undo ipv6 enable** to disable IPv6.

IPv6 is disabled by default.

Examples

```
# Create IS-IS routing process 1, and enable IPv6 for the process.
<Sysname> system-view
[Sysname] ipv6
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] ipv6 enable
```

ipv6 filter-policy export

Syntax

```
ipv6 filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name | route-policy route-policy-name } export
[ protocol [ process-id ] ]
```

```
undo ipv6 filter-policy export [ protocol [ process-id ] ]
```

View

IS-IS view

Default level

2: System level

Parameters

acl6-number: Number of a basic or advanced IPv6 ACL used to filter redistributed routes before advertisement, ranging from 2000 to 3999. See *ACL and QoS Configuration Guide* for ACL information.

ipv6-prefix-name: Name of an IPv6 prefix list used to filter the redistributed routes before advertisement, a case-sensitive string of 1 to 19 characters. See *Layer 3—IP Routing Configuration Guide* for IPv6 prefix list information.

route-policy-name: Name of a routing policy used to filter the redistributed routes before advertisement, a case-sensitive string of 1 to 63 characters. See *Layer 3—IP Routing Configuration Guide* for routing policy information.

protocol: Routing protocol from which the redistributed routes are to be filtered. The routing protocol can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**. If no protocol is specified, routes redistributed from all protocols are filtered.

process-id: Process ID of the routing protocol, ranging from 1 to 65535. This argument is available when the protocol is **isisv6**, **ospfv3**, or **ripng**.

Description

Use **ipv6 filter-policy export** to configure IPv6 IS-IS to filter redistributed routes before advertisement.

Use **undo ipv6 filter-policy export** to disable the filtering.

The filtering is disabled by default.

In some cases, only routes satisfying certain conditions will be advertised. You can configure the filtering conditions using the **ipv6 filter-policy** command.

You can use the **ipv6 filter-policy export** command, which filters redistributed routes only when they are advertised to other routers, in combination with the **ipv6 import-route** command.

- If no protocol is specified, routes redistributed from all protocols are filtered before advertisement.
- If a protocol is specified, only routes redistributed from the protocol are filtered before advertisement.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command or in the routing policy, the ACL should be configured with the **rule [rule-id] { deny | permit } ipv6 source sour sour-prefix** command to deny/permit a route with the specified destination, or with the **rule [rule-id] { deny | permit } ipv6 source sour sour-prefix destination dest dest-prefix** command to deny/permit a route with the specified destination and prefix. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route (the prefix must be valid; otherwise, the configuration is ineffective).

Related commands: **ipv6 filter-policy import**.

Examples

```
# Reference the ACL6 2006 to filter all the redistributed routes.
```

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] ipv6 filter-policy 2006 export
```

```
# Configure ACL6 3000 to permit only route 2001::1/128 to pass, and reference ACL6 3000 to filter redistributed routes.
```

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
fff:fff:fff:fff:fff:fff:fff:fff 128
[Sysname-acl6-adv-3000] rule 100 deny ipv6
[Sysname-acl6-adv-3000] quit
[Sysname] isis 1
[Sysname-isis-1] ipv6 filter-policy 3000 export
```

ipv6 filter-policy import

Syntax

```
ipv6 filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name | route-policy route-policy-name } import  
undo ipv6 filter-policy import
```

View

IS-IS view

Default level

2: System level

Parameters

acl6-number: Number of a basic or advanced IPv6 ACL used to filter incoming routes, ranging from 2000 to 3999.

ipv6-prefix-name: Name of an IPv6 prefix list used to filter incoming routes, a case-sensitive string of 1 to 19 characters.

route-policy-name: Name of a routing policy used to filter incoming routes, a case-sensitive string of 1 to 63 characters.

Description

Use **ipv6 filter-policy import** to configure IPv6 IS-IS to filter the received routes.

Use **undo ipv6 filter-policy import** to disable the filtering.

The filtering is disabled by default.

In some cases, only the routing information satisfying certain conditions will be received. You can configure the filtering conditions using the **ipv6 filter-policy** command.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command or in the routing policy, the ACL should be configured with the **rule [rule-id] { deny | permit } ipv6 source sour sour-prefix** command to deny/permit a route with the specified destination, or with the **rule [rule-id] { deny | permit } ipv6 source sour sour-prefix destination dest dest-prefix** command to deny/permit a route with the specified destination and prefix. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route (the prefix must be valid; otherwise, the configuration is ineffective).

Related commands: **ipv6 filter-policy export**.

Examples

Reference the IPv6 ACL 2003 to filter the received routes.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] ipv6 filter-policy 2003 import
```

Configure ACL6 3000 to permit only route 2001::1/128 to pass, and reference ACL6 3000 to filter the received routes.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl6-adv-3000] rule 100 deny ipv6
[Sysname-acl6-adv-3000] quit
[Sysname] isis 1
[Sysname-isis-1] ipv6 filter-policy 3000 import
```

ipv6 import-route

Syntax

ipv6 import-route protocol [process-id] [allow-ibgp] [cost cost | [level-1 | level-1-2 | level-2] | route-policy route-policy-name | tag tag] *

undo ipv6 import-route *protocol* [*process-id*]

View

IS-IS view

Default level

2: System level

Parameters

protocol: Redistributes routes from a specified routing protocol, which can be **direct**, **static**, **ripng**, **isisv6**, **bgp4+**, or **ospfv3**.

process-id: Process ID of the routing protocol of **ripng**, **isisv6**, or **ospfv3**, in the range of 1 to 65535. The default is 1.

cost: Cost for redistributed routes, ranging from 0 to 4261412864.

level-1: Redistributes routes into Level-1 routing table.

level-1-2: Redistributes routes into Level-1 and Level-2 routing tables.

level-2: Redistributes routes into Level-2 routing table.

route-policy-name: Name of a routing policy used to filter routes when they are being redistributed, a case-sensitive string of 1 to 63 characters.

tag: Specifies a administrative tag number for the redistributed routes, in the range of 1 to 4294967295.

allow-ibgp: Allows to redistribute IBGP routes. This keyword is optional when the *protocol* is **bgp4+**.

Description

Use **ipv6 import-route** to enable IPv6 IS-IS to redistribute routes from another routing protocol.

Use **undo ipv6 import-route** to disable route redistribution.

Route redistribution is disabled by default.

If no level is specified, the routes are imported to Level-2 routing table by default.

IPv6 IS-IS considers redistributed routes as routes to destinations outside the local routing domain.

You can specify a cost and a level for redistributed routes.



IMPORTANT:

Use the **import-route bgp4+ allow-ibgp** command with caution because it redistributes both EBGP and IBGP routes, and the redistributed IBGP routes can cause routing loops.

Examples

```
# Configure IPv6-IS-IS to redistribute static routes and set the cost 15 for them.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] ipv6 import-route static cost 15
```

ipv6 import-route isisv6 level-2 into level-1

Syntax

```
ipv6 import-route isisv6 level-2 into level-1 [ filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name | route-policy route-policy-name } | tag tag ] *
```

undo ipv6 import-route isisv6 level-2 into level-1

View

IS-IS view

Default level

2: System level

Parameters

acl6-number: Number of a basic or advanced ACL6 used to filter routes when they are leaking from Level-2 to Level-1, ranging from 2000 to 3999.

ipv6-prefix-name: Name of an IPv6 prefix list used to filter routes when they are leaking from Level-2 to Level-1, a case-sensitive string of 1 to 19 characters.

route-policy-name: Name of a routing policy used to filter routes when they are leaking from Level-2 to Level-1, a case-sensitive string of 1 to 63 characters.

tag: Specifies a administrative tag number for the leaked routes, in the range of 1 to 4294967295.

Description

Use **ipv6 import-route isisv6 level-2 into level-1** to enable IPv6 IS-IS route leaking from Level-2 to Level-1.

Use **undo ipv6 import-route isisv6 level-2 into level-1** to disable the leaking.

The leaking is disabled by default.

The route leaking feature enables a Level-1-2 router to advertise routes destined to other Level-2 areas to the Level-1 and Level-1-2 routers in the local area.

Examples

```
# Enable IPv6 IS-IS route leaking from Level-2 to Level-1.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] ipv6 import-route isisv6 level-2 into level-1
```

ipv6 import-route limit

Syntax

ipv6 import-route limit *number*

undo ipv6 import-route limit

View

IS-IS view

Default level

2: System level

Parameters

number: Maximum number of redistributed Level 1/Level 2 IPv6 routes. The default varies with devices.

Description

Use **ipv6 import-route limit** to configure the maximum number of redistributed Level 1/Level 2 IPv6 routes.

Use **undo ipv6 import-route limit** to restore the default.

The default varies with devices.

Examples

```
# Configure IS-IS process 1 to redistribute up to 1000 Level 1/Level 2 IPv6 routes.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] ipv6 import-route limit 1000
```

ipv6 maximum load-balancing

Syntax

```
ipv6 maximum load-balancing number
undo ipv6 maximum load-balancing
```

View

IS-IS view

Default level

2: System level

Parameters

number: Maximum number of ECMP routes , in the range of 1 to 8.

Description

Use **ipv6 maximum load-balancing** to configure the maximum number of ECMP routes.

Use **undo ipv6 maximum load-balancing** to restore the default.

By default, the maximum number of ECMP routes is 8.

Configure the maximum number of equal-cost routes according to the memory capacity.

Examples

```
# Configure the maximum number of ECMP routes as 2.
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] ipv6 maximum load-balancing 2
```

ipv6 preference

Syntax

```
ipv6 preference { preference | route-policy route-policy-name } *
undo ipv6 preference
```

View

IS-IS view

Default level

2: System level

Parameters

preference: Preference for IPv6 IS-IS, ranging from 1 to 255.

route-policy-name: Name of a routing policy, a case-sensitive string of 1 to 63 characters.

Description

Use **ipv6 preference** to configure the preference for IPv6 IS-IS protocol.

Use **undo ipv6 preference** to restore the default.

The default preference for IPv6 IS-IS protocol is 15.

When a router runs multiple dynamic routing protocols at the same time, the system will assign a preference to each routing protocol. If several protocols find routes to the same destination, the route found by the protocol with the highest preference is selected.

Examples

```
# Configure the preference of IPv6 IS-IS protocol as 20.
```

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] ipv6 preference 20
```

ipv6 summary

Syntax

```
ipv6 summary ipv6-prefix prefix-length [ avoid-feedback | generate_null0_route | [ level-1 | level-1-2 | level-2 ] ] [ tag tag ] *
```

```
undo ipv6 summary ipv6-prefix prefix-length [ level-1 | level-1-2 | level-2 ]
```

View

IS-IS view

Default level

2: System level

Parameters

ipv6-prefix: IPv6 prefix of the summary route.

prefix-length: Length of the IPv6 prefix, in the range of 0 to 128.

avoid-feedback: Specifies to avoid learning summary routes via routing calculation.

generate_null0_route: Generates the NULL 0 route to avoid routing loops.

level-1: Specifies to summarize only the routes redistributed to Level-1 area.

level-1-2: Specifies to summarize all the routes redistributed to Level-1 and Level-2 areas.

level-2: Specifies to summarize only the routes redistributed to Level-2 area.

tag: Value of a administrative tag, in the range of 1 to 4294967295.

NOTE:

If no level is specified in the command, the default is **level-2**.

Description

Use **ipv6 summary** to configure an IPv6 IS-IS summary route.

Use **undo ipv6 summary** to remove the summary route.

Route summarization is disabled by default.

Configuring summary routes can reduce the size of the route table, LSPs and LSDB. Routes to be summarized can be IS-IS routes or redistributed routes. The cost of a summary route is the smallest cost among all summarized routes.

Examples

```
# Configure a summary route of 2002::/32.  
<Sysname> system-view  
[Sysname] isis  
[Sysname-isis-1] ipv6 summary 2002:: 32
```

isis ipv6 bfd enable

Syntax

```
isis ipv6 bfd enable  
undo isis ipv6 bfd enable
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **isis ipv6 bfd enable** to enable BFD on an IPv6 IS-IS interface for link failure detection.

Use **undo isis ipv6 bfd enable** to disable BFD on an IPv6 IS-IS interface.

By default, an IPv6 IS-IS interface is not enabled with BFD.

Examples

```
# Enable BFD for IPv6 IS-IS on VLAN-interface 11.  
<Sysname> system-view  
[Sysname] interface vlan-interface 11  
[Sysname-Vlan-interfacel1] isis ipv6 bfd enable
```

isis ipv6 enable

Syntax

```
isis ipv6 enable [ process-id ]  
undo isis ipv6 enable
```

View

Interface view

Default level

2: System level

Parameters

process-id: IS-IS process ID, ranging from 1 to 65535. The default is 1.

Description

Use **isis ipv6 enable** to enable IPv6 for the specified IS-IS process on the interface.

Use **undo isis ipv6 enable** to disable the configuration.

IPv6 is disabled on the interface by default.

Examples

Enable global IPv6, create IS-IS routing process 1, enable IPv6 for the process, and enable IPv6 for the process on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] ipv6
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] ipv6 enable
[Sysname-isis-1] quit
[Sysname] interface vlan-interface 100
[Sysname--Vlan-interface100] ipv6 address 2002::1/64
[Sysname--Vlan-interface100] isis ipv6 enable 1
```

multiple-topology ipv6-unicast

Syntax

multiple-topology ipv6-unicast

undo multiple-topology ipv6-unicast

View

IS-IS view

Default level

2: System level

Parameters

None

Description

Use **multiple-topology ipv6-unicast** to enable IPv6 IS-IS MTR. This command enables separate route calculation in IPv4 and IPv6 topologies.

Use **undo multiple-topology ipv6-unicast** to disable IPv6 IS-IS MTR.

By default, IPv6 IS-IS MTR is disabled.

Before configuring this command, you must enable IPv6 for the IS-IS process and set the cost style to **wide**, **wide-compatible**, or **compatible** for the system.

Examples

```
# Enable IPv6 IS-IS MTR.
<Sysname> system-view
[Sysname] isis 1
```

```
[Sysname-isis-1] multiple-topology ipv6-unicast
```


IPv6 BGP configuration commands

The term "router" in this chapter refers to both routers and Layer 3 switches.

For more information about routing policy configuration commands in this document, see "[Routing policy configuration commands](#)."

The A5500 SI Switch Series does not support IPv6 BGP.

aggregate (IPv6 address family view)

Syntax

```
aggregate ipv6-address prefix-length [ as-set | attribute-policy route-policy-name | detail-suppressed | origin-policy route-policy-name | suppress-policy route-policy-name ] *
```

```
undo aggregate ipv6-address prefix-length
```

View

IPv6 address family view

Default level

2 System level

Parameters

ipv6-address: Summary address.

prefix-length: Length of summary route mask, in the range of 0 to 128.

as-set: Creates a summary with AS set.

attribute-policy *route-policy-name*: Sets the attributes of the summary route according to the routing policy. The routing policy name is a string of 1 to 63 characters.

detail-suppressed: Only advertises the summary route.

suppress-policy *route-policy-name*: Suppresses specific routes defined in the routing policy. The routing policy name is a string of 1 to 63 characters.

origin-policy *route-policy-name*: References the routing policy to specify routes for summarization. The routing policy name is a string of 1 to 63 characters.

Table 80 Functions of the keywords

Keywords	Function
as-set	Used to create a summary route, whose AS path contains the AS path information of summarized routes. Use this keyword carefully when many AS paths need to be summarized, because the frequent changes of these specific routes may lead to route oscillation.
detail-suppressed	This keyword does not suppress the summary route, but it suppresses the advertisement of all the more specific routes. To summarize only some specific routes, use the peer filter-policy command.

Keywords	Function
suppress-policy	Used to create a summary route and suppress the advertisement of some summarized routes. If you want to suppress some routes selectively and leave other routes still advertised, use the if-match clause of the route-policy command.
origin-policy	Selects only routes satisfying the routing policy for route summarization.
attribute-policy	Sets attributes except the AS_PATH attribute for the summary route. The same work can be done by using the peer route-policy command.

Description

Use **aggregate** to create an IPv6 summary route in the IPv6 BGP routing table.

Use **undo aggregate** to remove an IPv6 summary route.

By default, no summary route is configured.

Examples

```
# In IPv6 address family view, create a summary of 12::/64 in the IPv6 routing table.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] aggregate 12:: 64
```

balance (IPv6 address family view/IPv6 BGP-VPN instance view)

Syntax

balance *number*

undo balance

View

IPv6 address family view, IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

number: Number of BGP routes participating in load balancing , in the range of 1 to 8. When it is set to 1, load balancing is disabled.

Description

Use **balance** to configure the number of routes participating in IPv6 BGP load balancing.

Use **undo balance** to restore the default.

The feature is not available by default.

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing by defining its routing rule.

Related commands: **display bgp ipv6 routing-table**.

Examples

```
# Set the number of routes participating in IPv6 BGP load balancing to 2.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] balance 2
```

bestroute as-path-neglect (IPv6 address family view)

Syntax

```
bestroute as-path-neglect
undo bestroute as-path-neglect
```

View

IPv6 address family view

Default level

2: System level

Parameters

None

Description

Use **bestroute as-path-neglect** to configure the IPv6 BGP router to not evaluate the AS_PATH during best route selection.

Use **undo bestroute as-path-neglect** to configure the IPv6 BGP router to use the AS_PATH during best route selection.

By default, the router takes AS_PATH as a factor when selecting the best route.

Examples

```
# Ignore AS_PATH in route selection.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute as-path-neglect
```

bestroute compare-med (IPv6 address family view)

Syntax

```
bestroute compare-med
undo bestroute compare-med
```

View

IPv6 address family view

Default level

2: System level

Parameters

None

Description

Use **bestroute compare-med** to enable the comparison of the MED for paths from each AS.

Use **undo bestroute compare-med** to disable this comparison.

This comparison is not enabled by default.

After the **bestroute compare-med** command is executed, the **balance** command does not take effect.

Examples

```
# Compare the MED for paths from an AS for selecting the best route.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute compare-med
```

bestroute med-confederation (IPv6 address family view)

Syntax

bestroute med-confederation

undo bestroute med-confederation

View

IPv6 address family view

Default level

2: System level

Parameters

None

Description

Use **bestroute med-confederation** to enable the comparison of the MED for paths from confederation peers for best route selection.

Use **undo bestroute med-confederation** to disable the configuration.

By default, this comparison is not enabled.

With this feature enabled, the system can only compare the MED for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

Examples

```
# Compare the MED for paths from peers within the confederation.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute med-confederation
```

compare-different-as-med (IPv6 address family view)

Syntax

compare-different-as-med

undo compare-different-as-med

View

IPv6 address family view

Default level

2: System level

Parameters

None

Description

Use **compare-different-as-med** to enable the comparison of the MED for paths from peers in different ASs.

Use **undo compare-different-as-med** to disable the comparison.

The comparison is disabled by default.

If several paths are available for one destination, the path with the smallest MED value is selected.

Do not use this command unless associated ASs adopt the same IGP protocol and routing selection method.

Examples

```
# Enable to compare the MED for paths from peers in different ASs.
```

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv6-family
```

```
[Sysname-bgp-af-ipv6] compare-different-as-med
```

dampening (IPv6 address family view)

Syntax

dampening [*half-life-reachable* *half-life-unreachable* *reuse* *suppress* *ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View

IPv6 address family view

Default level

2: System level

Parameters

half-life-reachable: Half-life for reachable routes, in the range of 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Half-life for unreachable routes, in the range of 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Reuse threshold value for suppressed routes, in the range of 1 to 20000. Penalty value of a suppressed route decreasing under the value is reused. By default, its value is 750.

suppress: Suppression threshold from 1 to 20000, which should be bigger than the *reuse* value. Routes with a penalty value bigger than the threshold are suppressed. By default, it is 2000.

ceiling: Ceiling penalty value from 1001 to 20000. The value must be bigger than the *suppress* value. By default, the value is 16000.

route-policy-name: Routing policy name, a string of 1 to 63 characters.

half-life-reachable, *half-life-unreachable*, *reuse*, *suppress* and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified.

Description

Use **dampening** to enable IPv6 BGP route dampening, configure dampening parameters, or both.

Use **undo dampening** to disable route dampening.

By default, no route dampening is configured.

Related commands: **reset bgp ipv6 dampening**, **reset bgp ipv6 flap-info**, **display bgp ipv6 routing-table dampened**, **display bgp ipv6 routing-table dampening parameter**, and **display bgp ipv6 routing-table flap-info**.

Examples

```
# Enable IPv6 BGP route dampening and configure route dampening parameters.
```

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv6-family
```

```
[Sysname-bgp-af-ipv6] dampening 10 10 1000 2000 3000
```

default local-preference (IPv6 address family view/IPv6 BGP-VPN instance view)

Syntax

```
default local-preference value
```

```
undo default local-preference
```

View

IPv6 address family view, IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

value: Default local preference, in the range of 0 to 4294967295. The larger the value is, the higher the preference is.

Description

Use **default local-preference** to configure the default local preference.

Use **undo default local-preference** to restore the default value.

By default, the default local preference is 100.

Use this command to affect IPv6 BGP route selection.

Examples

Two devices A and B in the same AS are connected to another AS. Change the local preference of B from default value 100 to 180, making the route passing B preferred.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default local-preference 180
```

default med (IPv6 address family view/IPv6 BGP-VPN instance view)

Syntax

default med *med-value*

undo default med

View

IPv6 address family view, IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

med-value: MED value, in the range of 0 to 4294967295.

Description

Use **default med** to specify the default MED value.

Use **undo default med** to restore the default.

By default, the default *med-value* is 0.

The multi-exit discriminator (MED) is an external metric of a route. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a router running BGP obtains several routes with the identical destination and different next-hops from various external peers, it will select the best route depending on the MED value. In the case that all other conditions are the same, the system first selects the route with the smaller MED value as the best route for the autonomous system.

Examples

Devices A and B belong to AS100 and device C belongs to AS200. C is the peer of A and B. Configure the MED of A as 25 to make C select the path from B.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default med 25
```

default-route imported (IPv6 address family view/IPv6 BGP-VPN instance view)

Syntax

```
default-route imported
undo default-route imported
```

View

IPv6 address family view, IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

None

Description

Use **default-route imported** to enable the redistribution of default route into the IPv6 BGP routing table.

Use **undo default-route imported** to disable the redistribution.

By default, the redistribution is not enabled.

Examples

```
# Enable the redistribution of default route from OSPFv3 into IPv6 BGP.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default-route imported
[Sysname-bgp-af-ipv6] import-route ospfv3 1
```

display bgp ipv6 group

Syntax

```
display bgp ipv6 group [ ipv6-group-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-group-name: Peer group name, a string of 1 to 47 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 group** to display IPv6 peer group information.

If no *ipv6-group-name* is specified, information about all peer groups is displayed.

Examples

Display the information of the IPv6 peer group **aaa**.

```
<Sysname> display bgp ipv6 group aaa
```

```
BGP peer-group is aaa
Remote AS 100
Type: internal
Maximum allowed prefix number: 4294967295
Threshold: 75%
Configured hold timer value: 180
Keepalive timer value: 60
Minimum time between advertisement runs is 15 seconds
Peer Preferred Value: 0
No routing policy is configured
Members:
Peer                AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
-----
2001::1            100      0         0       0       0  00:00:07  Idle
```

Table 81 Command output

Field	Description
BGP peer-group	Name of the peer group.
Remote AS	AS number of the peer group If the peer group AS number has been specified with the peer ipv6-address as-number as-number command, the specified AS number is displayed in this field. Otherwise, a "Remote AS number not specified" prompt is displayed.
Type	Type of the peer group: <ul style="list-style-type: none">• internal—IBGP peer group.• external—EBGP peer group.
Maximum allowed prefix number	Maximum allowed prefix number.
Threshold	Threshold value.
Configured hold timer value	Holdtime.
Keepalive timer value	Keepalive interval.
Minimum time between advertisement runs	Minimum interval between advertisements.
Route refresh capability has been enabled	The route-refresh capability has been enabled.
ORF advertise capability based on prefix (type 64):	The BGP peer supports the ORF capability based on IP prefix. The capability value is 64.
Local: both	The local BGP router supports both the ORF sending and receiving capabilities.

Field	Description
Negotiated: send	Negotiation result: The local BGP router can send Router-refresh messages carrying the ORF information, and the peer can receive Router-refresh messages carrying the ORF information. If receive is displayed, the local BGP router can receive Router-refresh messages carrying the ORF information, and the peer can send Router-refresh messages carrying the ORF information. This field is not displayed if neither the send nor the receive capability is supported.)
Peer Preferred Value	Preferred value of the routes from the peer.
IPsec policy name	IPsec policy applied to the peer group.
SPI	SPI of the IPsec policy.
Routing policy configured	A routing policy is configured.
No routing policy is configured	No routing policy is configured.
Members	Group members.
Peer	IPv6 address of the peer.
AS	AS number.
MsgRcvd	Number of messages received.
MsgSent	Number of messages sent.
OutQ	Number of messages to be sent.
PrefRcv	Number of prefixes received.
Up/Down	The lasting time of a session/the lasting time of present state (when no session is established).
State	State machine state of peer.

display bgp ipv6 network

Syntax

```
display bgp ipv6 network [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 network** to display IPv6 routes advertised with the **network** command.

Examples

```
# Display IPv6 routes advertised with the network command.
```

```
<Sysname> display bgp ipv6 network
```

```
BGP Local Router ID is 1.1.1.2.
Local AS Number is 200.
Network          Prefix          Route-policy      Short-cut

2002::          64
2001::          64                Short-cut
```

Table 82 Command output

Field	Description
BGP Local Router ID	BGP Local Router ID
Local AS Number	Local AS Number
Network	Network address
Prefix	Prefix length
Route-policy	Routing policy (A null value indicates no routing policy is configured.)
Short-cut	Shortcut route (A null value indicates the route is not a shortcut route.)

display bgp ipv6 paths

Syntax

```
display bgp ipv6 paths [ as-regular-expression | | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

as-regular-expression: AS path regular expression, a string of 1 to 80 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 paths** to display IPv6 BGP path information.

If no parameter is specified, all path information will be displayed.

Examples

```
# Display IPv6 BGP path information.
```

```
<Sysname> display bgp ipv6 paths
```

Address	Hash	Refcount	MED	Path/Origin
0x5917098	1	1	0	i
0x59171D0	9	2	0	100i

Table 83 Command output

Field	Description
Address	Route destination address in local database, in dotted hexadecimal notation.
Hash	Hash index.
Refcount	Count of routes that used the path.
MED	MED of the path.
Path	AS_PATH attribute of the path, recording the ASs it has passed, for avoiding routing loops

ORIGIN attribute of the route, which can take on one of the following values:

- **i**—Indicates the route is interior to the AS. Summary routes and routes defined using the **network** command are considered IGP routes.
- **e**—Indicates that a route is learned from the exterior gateway protocol (EGP).
- **?**—Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means. BGP sets ORIGIN attribute of routes learned from other IGP protocols to INCOMPLETE.

display bgp ipv6 peer

Syntax

```
display bgp ipv6 peer [ group-name log-info | ipv4-address verbose | ipv6-address { log-info | verbose } | verbose ] [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: Specifies the IPv6 address of a peer to be displayed.

log-info: Displays log information of the specified peer.

verbose: Displays the detailed information of the peer.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 peer** to display peer/peer group information.

If no parameter specified, information about all peers and peer groups is displayed.

Examples

```
# Display all IPv6 peer information.
```

```
<Sysname> display bgp ipv6 peer
```

```
BGP local router ID : 192.168.1.40
Local AS number : 100
Total number of peers : 1                Peers in established state : 0

Peer                AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
-----
2001::1             100      0        0      0      0  00:02:02  Active
```

Table 84 Command output

Field	Description
BGP local router ID	Local router ID
Local AS number	Local AS number
Total number of peers	Total number of BGP peers
Peers in established state	Number of established BGP peers
Peer	IPv6 address of the peer
AS	AS number
MsgRcvd	Messages received
MsgSent	Messages sent
OutQ	Messages to be sent
PrefRcv	Number of prefixes received
Up/Down	Lasting time of a session/Lasting time of present state (when no session is established)
State	Peer state

```
# Display the detailed information of IPv6 peer 1::1.
```

```
<Sysname> display bgp ipv6 peer 1::1 verbose
```

```
BGP Peer is 1::1, remote AS 100,
```

```
Type: EBGp link
BGP version 4, remote router ID 45.1.1.1
BGP current state: Established, Up for 00h01m34s
BGP current event: KATimerExpired
BGP last state: OpenConfirm
Port: Local - 1031 Remote - 179
Configured: Active Hold Time: 180 sec Keepalive Time: 60 sec
Received : Active Hold Time: 180 sec
Negotiated: Active Hold Time: 180 sec Keepalive Time:60 sec
Peer optional capabilities:
Peer support bgp multi-protocol extended
Peer support bgp route refresh capability
Peer support bgp route AS4 capability
Graceful Restart Capability: advertised and received
Restart Timer Value of Peer: 150 seconds
Forwarding State preserved by Peer for following Address families:
Address family IPv6 Unicast: advertised and received
```

```
Received: Total 4 messages, Update messages 1
Sent: Total 6 messages, Update messages 3
Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisement runs is 30 seconds
Optional capabilities:
Route refresh capability has been enabled
Peer Preferred Value: 0
```

```
Routing policy configured:
No routing policy is configured
BFD: Enabled
```

Display the detailed information of IPv6 BGP peers.

```
<Sysname> display bgp ipv6 peer verbose
```

```
BGP Peer is 2::4, remote AS 1,
Type: IBGP link
BGP version 4, remote router ID 1.1.1.1
BGP current state: Established, Up for 00h01m51s
BGP current event: RecvKeepalive
BGP last state: OpenConfirm
```

```
Received: Total 5 messages, Update messages 1
Sent: Total 4 messages, Update messages 0
Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisement runs is 30 seconds
Optional capabilities:
Route refresh capability has been enabled
ORF advertise capability based on prefix (type 64):
```

Local: both
 Negotiated: send
 Peer Preferred Value: 0
 IPsec policy name: policy001, SPI: 300

Routing policy configured:
 No routing policy is configured

Table 85 Command output

Field	Description
Type	BGP connection type: EBGP or IBGP.
Up for	Lasting time of a BGP connection.
Peer optional capabilities:	
Peer support bgp multi-protocol extended	Optional capabilities supported by the BGP peer: <ul style="list-style-type: none"> Multi-protocol extension for BGP.
Peer support bgp route refresh capability	<ul style="list-style-type: none"> Route-refresh feature.
Peer support bgp route AS4 capability	<ul style="list-style-type: none"> 4-byte AS number
Graceful Restart Capability: advertised and received Restart Timer Value of Peer: 150 seconds Forwarding State preserved by Peer for following Address families:	GR capability: the advertising and receiving capabilities have been successfully negotiated. <ul style="list-style-type: none"> GR restart timer of the peer is 150 seconds Address family information for which the peer preserves the forwarding state
Address family IPv6 Unicast: advertised and received	BGP IPv6 unicast capability: the advertising and receiving capabilities have been successfully negotiated.
Threshold	Threshold of the routes received from the peer (ratio of the number of received routes to the configured upper limit in percentage) when an alarm is generated.
Minimum time between advertisement runs is 30 seconds	Minimum interval between advertisements.
Optional capabilities Route refresh capability has been enabled ORF advertise capability based on prefix (type 64): Local: both Negotiated: send	Optional capabilities enabled on the peer: <ul style="list-style-type: none"> Route-refresh is enabled. The IPv6 BGP peer supports the ORF capability based on IP prefix. The capability value is 64. The local IPv6 BGP router supports both the ORF sending and receiving capabilities. Negotiation result: The local IPv6 BGP router can send Router-refresh messages carrying the ORF information, and the peer can receive Router-refresh messages carrying the ORF information. (If receive is displayed, the local BGP router can receive Router-refresh messages carrying the ORF information, and the peer can send Router-refresh messages carrying the ORF information. This field is not displayed if neither the send nor the receive capability is supported.
Peer Preferred Value	Preferred value assigned to routes received from the peer.
IPsec policy name: policy001, SPI: 300	IPsec policy applied to the peer and SPI of the IPsec policy.

Field	Description
BFD	Indicates whether BFD is enabled over the link to the IPv6 BGP peer.

Display the log information of the IPv6 peer 20::21.

```
<Sysname> display bgp ipv6 peer 20::21 log-info
```

```
Peer : 20::21
```

Date	Time	State	Notification Error/SubError
10-Jul-2008	15:46:17	Down	Send Notification with Error 1/1 Message Header Error/Connection Not Synchronized
10-Jul-2008	09:23:00	Up	
10-Jul-2008	07:46:17	Down	Receive Notification with Error 3/2 UPDATE Message Error/Unsupported optional Parameter
10-Jul-2008	06:23:00	Up	
10-Jul-2008	05:46:17	Down	Send Notification with Error 6/4 Administrative Reset

Table 86 Command output

Field	Description
Peer	IPv6 address of the peer.
Date	Date on which the Notification was sent or received.
Time	Time at which the Notification was sent or received.
State	BGP session state, which can be: <ul style="list-style-type: none"> • Up—Indicates the BGP session is up. • Down—Indicates the BGP session is down.
Notification	Notification message.
Error/SubError	<ul style="list-style-type: none"> • Error—Refers to the error code, which identifies the type of the Notification. • SubError—Refers to the error subcode of the Notification, which identifies the specific information about the reported error.

display bgp ipv6 peer received ipv6-prefix

Syntax

```
display bgp ipv6 peer { ip-address | ipv6-address } received ipv6-prefix [ | { begin | exclude | include }  
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ip-address: IP address of a BGP peer.

ipv6-address: IPv6 address of a BGP peer.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 peer received ipv6-prefix** to display the prefix entries in the ORF information of the specified BGP peer.

Examples

```
# Display the prefix information in the ORF packet from the BGP peer 4::4.
```

```
<Sysname> display bgp ipv6 peer 4::4 received ipv6-prefix
ORF ipv6-prefix entries: 2
ge: greater-equal   le: less-equal
  index rule  prefix                ge    le
  ---  ---  ---                ---  ---
  10   permit 1::/64                80   128
  20   deny  100::/64              80   128
```

Table 87 Command output

Field	Description
ORF ipv6-prefix entries	Number of ORF prefix entries.
index	Index of a prefix entry.
rule	Matching rule of the prefix.
prefix	Prefix information.
ge	greater-equal, indicating the mask length must be greater than or equal to the specific value.
le	less-equal, indicating the mask length must be less than or equal to the specific value.

display bgp ipv6 routing-table

Syntax

```
display bgp ipv6 routing-table [ ipv6-address prefix-length ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Destination IPv6 address.

prefix-length: Prefix length of the IPv6 address, in the range of 0 to 128.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 routing-table** to display IPv6 BGP routing table information.

Examples

```
# Display the IPv6 BGP routing table.
```

```
<Sysname> display bgp ipv6 routing-table
```

```
Total Number of Routes: 2
```

```
BGP Local router ID is 30.30.30.1
```

```
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,  
              h - history, i - internal, s - suppressed, S - Stale  
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*> Network : 30:30::                               PrefixLen : 64  
    NextHop : 30:30::30:1                           LocPrf    :  
    PrefVal : 0                                       Label     : NULL  
    MED     : 0  
    Path/Ogn: i
```

```
*> Network : 40:40::                               PrefixLen : 64  
    NextHop : 40:40::40:1                           LocPrf    :  
    PrefVal : 0                                       Label     : NULL  
    MED     : 0  
    Path/Ogn: i
```

Table 88 Command output

Field	Description
Local router ID	Local router ID

Field	Description
Status codes	<p>Status codes:</p> <p>Status codes:</p> <ul style="list-style-type: none"> • * – valid—Valid route. • ^ - VPNv4 best—Best VPNv4 route. • > – best—Best route. • d – damped—Dampened route. • h – history—History route. • i – internal—Internal route. • s – suppressed—Suppressed route. • S – Stale—Stale route.
Origin	<p>ORIGIN attributes:</p> <ul style="list-style-type: none"> • i – IGP—Originated in the AS. • e – EGP—Learned through EGP. • ? – incomplete—Learned by other means.
Network	Destination network address.
PrefixLen	Prefix length.
NextHop	Next Hop.
MED	Multi-Exit Discriminator.
LocPrf	Local preference value.
Path	AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops.
PrefVal	Preferred value.
Label	Label
Ogn	<p>ORIGIN attribute of the route, which can take on one of the following values:</p> <ul style="list-style-type: none"> • i—Indicates that a route is interior to the AS. • Summary routes and the routes configured using the network command are considered IGP routes. • e—Indicates that a route is learned from the exterior gateway protocol (EGP). • ?—Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means. BGP sets ORIGIN attribute of routes learned from other IGP protocols to INCOMPLETE.

display bgp ipv6 routing-table as-path-acl

Syntax

```
display bgp ipv6 routing-table as-path-acl as-path-acl-number [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

as-path-acl-number: Number of an AS path ACL permitted by which to display routing information, ranging from 1 to 256.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 routing-table as-path-acl** to display routes filtered through the specified AS path ACL.

Examples

Display routes filtered through the AS path ACL 20.

```
<Sysname> display bgp ipv6 routing-table as-path-acl 20
BGP Local router ID is 30.30.30.1
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 30:30::                               PrefixLen : 64
    NextHop : 30:30::30:1                           LocPrf    :
    PrefVal : 0                                       Label     : NULL
    MED     : 0
    Path/Ogn: i
```

For description of the fields, see [Table 88](#).

display bgp ipv6 routing-table community

Syntax

```
display bgp ipv6 routing-table community [ aa:nn&<1-13> ] [ no-advertise | no-export | no-export-subconfed ] * [ whole-match ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

aa:nn: Community number; both *aa* and *nn* are in the range of 0 to 65535.

&<1-13>: Indicates the argument before it can be entered up to 13 times.

no-advertise: Displays IPv6 BGP routes that cannot be advertised to any peer.

no-export: Displays IPv6 BGP routes that cannot be advertised out the AS; if a confederation exists, it displays IPv6 BGP routes that cannot be advertised out the confederation, but can be advertised to other sub ASs in the confederation.

no-export-subconfed: Displays IPv6 BGP routes that cannot be advertised out the AS or to other sub ASs if a confederation is configured.

whole-match: Displays the IPv6 BGP routes exactly matching the specified COMMUNITY attribute.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 routing-table community** to display the routing information with the specified COMMUNITY attribute.

Examples

```
# Display the routing information with community attribute NO_EXPORT.
```

```
<Sysname> display bgp ipv6 routing-table community no-export
BGP Local router ID is 30.30.30.1
  Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
                h - history, i - internal, s - suppressed, S - Stale
  Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 30:30::                               PrefixLen : 64
    NextHop : 30:30::30:1                           LocPrf    :
    PrefVal  : 0                                     Label     : NULL
    MED      : 0
    Path/Ogn: i
```

For description of the fields, see [Table 88](#).

display bgp ipv6 routing-table community-list

Syntax

```
display bgp ipv6 routing-table community-list { { basic-community-list-number | comm-list-name }
[ whole-match ] | adv-community-list-number } [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

basic-community-list-number: Specifies a basic community-list number, in the range of 1 to 99.

adv-community-list-number: Specifies an advanced community-list number, in the range of 100 to 199.

comm-list-name: Specifies a community list name, a string of 1 to 31 characters (not all are numbers).

whole-match: Displays routes exactly matching the specified *basic-community-list-number*.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 routing-table community-list** to view the routing information matching the specified IPv6 BGP community list.

Examples

```
# Display the routing information matching the specified IPv6 BGP community list.
```

```
<Sysname> display bgp ipv6 routing-table community-list 99
```

```
BGP Local router ID is 30.30.30.1
```

```
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
```

```
*> Network : 30:30::                               PrefixLen : 64
     NextHop : 30:30::30:1                           LocPrf    :
     PrefVal : 0                                       Label     : NULL
     MED     : 0
     Path/Ogn: i
```

For description of the fields, see [Table 88](#).

display bgp ipv6 routing-table dampened

Syntax

```
display bgp ipv6 routing-table dampened [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 routing-table dampened** to display the IPv6 BGP dampened routes.

Examples

```
# Display IPv6 BGP dampened routes.
```

```
<Sysname> display bgp ipv6 routing-table dampened
```

```
BGP Local router ID is 1.1.1.1
```

```
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,  
              h - history, i - internal, s - suppressed, S - Stale  
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*d Network : 111::                               PrefixLen : 64  
    From   : 122::1                               Reuse      : 00:29:34  
    Path/Ogn: 200?
```

Table 89 Command output

Field	Description
From	Source IP address of a route
Reuse	Time for reuse

For description of the fields, see [Table 88](#).

display bgp ipv6 routing-table dampening parameter

Syntax

```
display bgp ipv6 routing-table dampening parameter [ | { begin | exclude | include }  
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 routing-table dampening parameter** to display IPv6 BGP routing dampening parameters.

Related commands: **dampening**.

Examples

```
# Display IPv6 BGP routing dampening parameters.
```

```
<Sysname> display bgp ipv6 routing-table dampening parameter
```

```
Maximum Suppress Time(in second) : 950
Ceiling Value                      : 3000
Reuse Value                        : 1000
Reach HalfLife Time(in second)    : 600
Unreach HalfLife Time(in second)  : 600
Suppress-Limit                    : 2000
```

Table 90 Command output

Field	Description
Maximum Suppress Time	Maximum Suppress Time
Ceiling Value	Upper limit of penalty value
Reuse Value	Reuse Value
Reach HalfLife Time(in second)	Half-life time of active routes
Unreach HalfLife Time(in second)	Half-life time of inactive routes
Suppress-Limit	Suppress value

display bgp ipv6 routing-table different-origin-as

Syntax

```
display bgp ipv6 routing-table different-origin-as [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 routing-table different-origin-as** to display IPv6 BGP routes originating from different autonomous systems.

Examples

```
# Display routes from different ASs.
<Sysname> display bgp ipv6 routing-table different-origin-as

BGP Local router ID is 2.2.2.2
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 222::                                PrefixLen : 64
   NextHop : 122::2                                LocPrf    :
   PrefVal  : 0                                    Label     : NULL
   MED      : 0
   Path/Ogn: 100 ?
```

For description of the fields, see [Table 88](#).

display bgp ipv6 routing-table flap-info

Syntax

```
display bgp ipv6 routing-table flap-info [ regular-expression as-regular-expression | [ as-path-acl as-path-acl-number | ipv6-address prefix-length [ longer-match ] ] [ | { begin | exclude | include } regular-expression ] ]
```

View

Any view

Default level

1: Monitor level

Parameters

as-regular-expression: AS path regular expression to be matched, a string of 1 to 80 characters.

as-path-acl-number: Number of the specified AS path ACL to be matched, ranging from 1 to 256.

ipv6-address: IPv6 address of a route to be displayed.

prefix-length: Prefix length of the IPv6 address, in the range of 0 to 128.

longer-match: Matches the longest prefix.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 routing-table flap-info** to display IPv6 BGP route flap statistics.

Examples

```
# Display IPv6 BGP route flap statistics.
<Sysname> display bgp ipv6 routing-table flap-info

BGP Local router ID is 1.1.1.1
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*d Network   : 111:::                               PrefixLen : 64
  From       : 122::1                               Flaps      : 3
  Duration   : 00:13:47                             Reuse      : 00:16:36
  Path/Ogn   : 200?
```

Table 91 Command output

Field	Description
Flaps	Number of flaps
Duration	Flap duration
Reuse	Reuse time of the route

For description of the fields, see [Table 88](#).

display bgp ipv6 routing-table peer

Syntax

```
display bgp ipv6 routing-table peer { ipv4-address | ipv6-address } { advertised-routes | received-routes } [ network-address prefix-length | statistic ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv4-address: Specifies the IPv4 peer to be displayed.

ipv6-address: Specifies the IPv6 peer to be displayed.

advertised-routes: Routing information advertised to the specified peer.

received-routes: Routing information received from the specified peer.

network-address prefix-length: IPv6 address and prefix length. The prefix length ranges from 0 to 128.

statistic: Displays route statistics.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 routing-table peer** to display the routing information advertised to or received from the specified IPv4 or IPv6 BGP peer.

Examples

```
# Display the routing information advertised to the specified BGP peer.
<Sysname> display bgp ipv6 routing-table peer 10:10::10:1 advertised-routes
Total Number of Routes: 2

BGP Local router ID is 20.20.20.1
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 20:20::                                PrefixLen : 64
    NextHop : 20:20::20:1                            LocPrf    :
    PrefVal  : 0                                     Label     : NULL
    MED      : 0
    Path/Ogn: i

*> Network : 40:40::                                PrefixLen : 64
    NextHop : 30:30::30:1                            LocPrf    :
    PrefVal  : 0                                     Label     : NULL
    MED      : 0
    Path/Ogn: 300 i
```

For description of the fields, see [Table 88](#).

display bgp ipv6 routing-table regular-expression

Syntax

```
display bgp ipv6 routing-table regular-expression as-regular-expression
```

View

Any view

Default level

1: Monitor level

Parameters

as-regular-expression: AS regular expression, a string of 1 to 80 characters.

Description

Use **display bgp ipv6 routing-table regular-expression** to display the routes permitted by the specified AS regular expression.

Examples

```
# Display routing information matching the specified AS regular expression.
```

```
<Sysname> display bgp ipv6 routing-table regular-expression ^100
```

```
BGP Local router ID is 20.20.20.1
```

```
Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*> Network : 50:50::                               PrefixLen : 64
NextHop   : 10:10::10:1                             LocPrf    :
PrefVal   : 0                                         Label     : NULL
MED       : 0
Path/Ogn  : 100 i
```

For description of the fields, see [Table 88](#).

display bgp ipv6 routing-table statistic

Syntax

```
display bgp ipv6 routing-table statistic [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp ipv6 routing-table statistic** to display IPv6 BGP routing statistics.

Examples

```
# Display IPv6 BGP routing statistics.
```

```
<Sysname> display bgp ipv6 routing-table statistic
```

```
Total Number of Routes: 1
```

filter-policy export (IPv6 address family view/IPv6 BGP-VPN instance view)

Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } export [ protocol process-id ]  
undo filter-policy export [ protocol process-id ]
```

View

IPv6 address family view, IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

acl6-number: Specifies the number of an ACL6 used to match against the destination of routing information. The number is in the range of 2000 to 3999.

ipv6-prefix-name: Specifies the name of an IPv6 prefix list used to match against the destination of routing information. The name is a string of 1 to 19 characters.

protocol: Filters routes redistributed from the routing protocol. It can be **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**. If no protocol is specified, all routes will be filtered when advertised.

process-id: Process ID of the routing protocol, in the range of 1 to 65535. It is available only when the protocol is **isisv6**, **ospfv3** or **ripng**.

Description

Use **filter-policy export** to filter outbound routes using a specified filter.

Use **undo filter-policy export** to cancel filtering outbound routes.

By default, no outbound routing information is filtered.

If a protocol is specified, only routes redistributed from the specified protocol are filtered. If no protocol is specified, all redistributed routes will be filtered.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command, the ACL should be configured with the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* command to deny/permit a route with the specified destination, or with the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix destination dest dest-prefix* command to deny/permit a route with the specified destination and prefix. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route (the prefix must be valid; otherwise, the configuration is ineffective).

Examples

```
# Reference ACL6 2001 to filter all outbound IPv6 BGP routes.
```

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] filter-policy 2001 export
```

```
# Configure ACL6 3000 to permit only route 2001::1/128 to pass, and reference ACL6 3000 to filter outbound routes.
```

```
<Sysname> system-view
```

```

[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl6-adv-3000] rule 100 deny ipv6
[Sysname-acl6-adv-3000] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] filter-policy 3000 export

```

filter-policy import (IPv6 address family view/IPv6 BGP-VPN instance view)

Syntax

```

filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } import
undo filter-policy import

```

View

IPv6 address family view, IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

acl6-number: Number of an IPv6 ACL used to match against the destination address field of routing information, ranging from 2000 to 3999.

ipv6-prefix-name: Name of an IPv6 prefix list used to match against the destination address field of routing information, a string of 1 to 19 characters.

Description

Use **filter-policy import** to filter inbound routing information using a specified filter.

Use **undo filter-policy import** to cancel filtering inbound routing information.

By default, no inbound routing information is filtered.

If you want to reference an advanced ACL (with a number from 3000 to 3999) in the command, the ACL should be configured with the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* command to deny/permit a route with the specified destination, or with the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix destination dest dest-prefix* command to deny/permit a route with the specified destination and prefix. The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route (the prefix must be valid; otherwise, the configuration is ineffective).

Examples

Reference ACL6 2001 to filter all inbound routes.

```

<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] filter-policy 2001 import

```

Configure ACL6 3000 to permit only route 2001::1/128 to pass, and reference ACL6 3000 to filter inbound routes.

```

<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl6-adv-3000] rule 100 deny ipv6
[Sysname-acl6-adv-3000] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] filter-policy 3000 import

```

group (IPv6 address family view)

Syntax

```

group ipv6-group-name [ internal | external ]
undo group ipv6-group-name

```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of an IPv6 peer group, a string of 1 to 47 characters.

internal: Creates an IBGP peer group.

external: Creates an EBGP peer group, which can be a group of another sub AS in the confederation.

Description

Use **group** to create a peer group.

Use **undo group** to delete a peer group.

An IBGP peer group will be created if neither **internal** nor **external** is selected.

Examples

Create an IBGP peer group named **test**.

```

<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv6-family
[Sysname-bgp-af-ipv6] group test

```

import-route (IPv6 address family view/IPv6 BGP-VPN instance view)

Syntax

```

import-route protocol [ process-id [ med med-value | route-policy route-policy-name ] * ]
undo import-route protocol [ process-id ]

```

View

IPv6 address family view, IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

protocol: Redistributes routes from the specified protocol, which can be **direct**, **isisv6**, **ospfv3**, **ripng** and **static**.

process-id: Process ID, in the range of 1 to 65535. The default is 1. It is available only when the protocol is **isisv6**, **ospfv3** or **ripng**.

med-value: Applies the MED value to redistributed routes. The value is in the range of 0 to 4294967295. If not specified, the cost of the redistributed route is used as its MED in the IPv6 BGP routing domain.

route-policy-name: Name of a routing policy used to filter redistributed routes, a string of 1 to 63 characters.

Description

Use **import-route** to redistribute routes from another routing protocol.

Use **undo import-route** to remove the configuration.

By default, IPv6 BGP does not redistribute routes from any routing protocol.

The routes redistributed using the **import-route** command has the INCOMPLETE origin attribute.

Examples

```
# Redistribute routes from RIPng 1.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] import-route ripng 1
```

ipv6-family

Syntax

ipv6-family [**vpn-instance** *vpn-instance-name*]

undo ipv6-family [**vpn-instance** *vpn-instance-name*]

View

BGP view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Enters IPv6 BGP-VPN instance view. *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

Description

Use **ipv6-family** to enter IPv6 address family view.

Use **undo ipv6-family** to remove all configurations from the view.

Use the **ipv6-family vpn-instance** *vpn-instance-name* command to enter IPv6 BGP-VPN instance view.

Use the **undo ipv6-family vpn-instance** *vpn-instance-name* command to remove all configurations from the view.

IPv4 BGP unicast view is the default.

Before entering IPv6 BGP-VPN instance view, you must create the VPN instance.

Examples

Enter IPv6 address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6]
```

Enter IPv6 BGP-VPN instance view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family vpn-instance vpn1
[Sysname-bgp-ipv6-vpn1]
```

network (IPv6 address family view/IPv6 BGP-VPN instance view)

Syntax

network *ipv6-address prefix-length* [**route-policy** *route-policy-name* | **short-cut**]

undo network *ipv6-address prefix-length* [**short-cut**]

View

IPv6 address family view, IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

ipv6-address: IPv6 address.

prefix-length: Prefix length of the address, in the range of 0 to 128.

route-policy-name: Name of a routing policy, a string of 1 to 63 characters.

short-cut: If the keyword is specified for an EBGP route, the route will use the local routing management value rather than that of EBGP routes, so the preference of the route is reduced.

Description

Use **network** to advertise a network to the IPv6 BGP routing table.

Use **undo network** to remove an entry from the IPv6 BGP routing table.

By default, no route is advertised.

The route to be advertised must exist in the local IP routing table, and using a routing policy makes route management more flexible.

The route advertised to the BGP routing table using the **network** command has the IGP origin attribute.

Examples

```
# Advertise the network 2002::/16 into the IPv6 BGP routing table.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] network 2002:: 16
```

peer advertise-community (IPv6 address family view)

Syntax

```
peer { group-name | ipv4-address | ipv6-address } advertise-community
undo peer { group-name | ipv4-address | ipv6-address } advertise-community
```

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description

Use **peer advertise-community** to advertise the COMMUNITY attribute to a peer/peer group.

Use **undo peer advertise-community** to remove the configuration.

By default, no COMMUNITY attribute is advertised to any peer group/peer.

Examples

```
# Advertise the COMMUNITY attribute to the peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 advertise-community
```

peer advertise-ext-community (IPv6 address family view)

Syntax

```
peer { group-name | ipv4-address | ipv6-address } advertise-ext-community
undo peer { group-name | ipv4-address | ipv6-address } advertise-ext-community
```

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description

Use **peer advertise-ext-community** to advertise the extended community attribute to a peer/peer group.

Use **undo peer advertise-ext-community** to remove the configuration.

By default, no extended community attribute is advertised to a peer/peer group.

Examples

```
# Advertise the extended community attribute to the peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 advertise-ext-community
```

peer allow-as-loop (IPv6 address family view)

Syntax

```
peer { group-name | ipv4-address | ipv6-address } allow-as-loop [ number ]
undo peer { group-name | ipv4-address | ipv6-address } allow-as-loop
```

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

number: Specifies the number of times for which the local AS number can appear in routes from the peer/peer group, in the range of 1 to 10. The default number is 1.

Description

Use **peer allow-as-loop** to configure IPv6 BGP to allow the local AS number to exist in the AS_PATH attribute of routes from a peer/peer group, and to configure the times for which it can appear.

Use **undo peer allow-as-loop** to disable the function.

The local AS number is not allowed to exist in the AS_PATH attribute of routes by default.

Examples

```
# Configure the number of times for which the local AS number can appear in the AS_PATH of routes from
peer 1::1 as 2.
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1::1 allow-as-loop 2
```

peer as-number (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } as-number as-number
undo peer ipv6-group-name as-number
undo peer ipv6-address
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

as-number: AS number of the peer/peer group, in the range of 1 to 4294967295.

Description

Use **peer as-number** to configure an IPv6 peer/peer group.

Use **undo peer *ipv6-group-name* as-number** to delete an IPv6 peer group.

Use **undo peer *ipv6-address*** to delete a peer.

Examples

```
# Configure peer group test in AS 200.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test as-number 200
```

peer as-number (IPv6 BGP-VPN instance view)

Syntax

```
peer ipv6-address as-number as-number
undo peer ipv6-address
```

View

IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

ipv6-address: IPv6 address of a peer.

as-number: AS number of the peer/peer group, in the range of 1 to 4294967295.

Description

Use **peer as-number** to configure an IPv6 peer/peer group.

Use **undo peer** *ipv6-address* to delete a peer.

Examples

```
# Configure peer 2001::1 in AS 200.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family vpn-instance vpn1
[Sysname-bgp-ipv6-vpn1] peer 2001::1 as-number 200
```

peer as-path-acl (IPv6 address family view)

Syntax

```
peer { group-name | ipv4-address | ipv6-address } as-path-acl as-path-acl-number { import | export }
undo peer { group-name | ipv4-address | ipv6-address } as-path-acl as-path-acl-number { import | export }
```

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

as-path-acl-number: Number of an AS path ACL, in the range of 1 to 256.

import: Filters incoming routes.

export: Filters outgoing routes.

Description

Use **peer as-path-acl** to specify an AS path ACL to filter routes incoming from or outgoing to a peer/peer group.

Use **undo peer as-path-acl** to remove the configuration.

By default, no AS path list is specified for filtering.

Examples

```
# Specify the AS path ACL 3 to filter routes outgoing to the peer 1:2::3:4.
<Sysname> system-view
[Sysname] ip as-path 3 permit ^200
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-path-acl 3 export
```

peer bfd (IPv6 address family view/IPv6 BGP-VPN instance view)

Syntax

```
peer ipv6-address bfd
undo peer ipv6-address bfd
```

View

IPv6 address family view, IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

ipv6-address: IPv6 address of a peer.

Description

Use **peer bfd** to enable BFD over the link to a BGP peer.

Use **undo peer bfd** to restore the default.

By default, BFD is not enabled for any BGP peer.

After a link failure occurs, BFD may detect the failure before the system performs GR, and as a result, GR will fail. Therefore, if GR capability is enabled for IPv6 BGP, use BFD with caution.

Examples

```
# Enable BFD over the link to BGP peer 100::1.
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv6-family
[Sysname-bgp-af-ipv6] peer 100::1 bfd
```

peer capability-advertise orf

Syntax

```
peer { group-name | ip-address | ipv6-address } capability-advertise orf ipv6-prefix { both | receive | send }
undo peer { group-name | ip-address | ipv6-address } capability-advertise orf ipv6-prefix { both | receive | send }
```

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

ipv6-address: IPv6 address of a peer.

both: Supports sending and receiving route-refresh messages carrying the ORF information.

receive: Supports receiving route-refresh messages carrying the ORF information.

send: Supports sending route-refresh messages carrying the ORF information.

Description

Use **peer capability-advertise orf** to enable the ORF capability for a BGP peer or peer group.

Use **undo peer capability-advertise orf** to disable the ORF capability for the BGP peer or peer group.

By default, the ORF capability is not enabled for a BGP peer or peer group.

- After you enable the ORF capability, the local BGP router negotiates the ORF capability with the BGP peer through Open messages. After that, the BGP router can process route-refresh messages carrying the standard ORF information from the peer or send route-refresh messages carrying the standard ORF information to the peer. For non-standard ORF capability negotiation, you need also to configure the **peer capability-advertise orf non-standard** command.
- After you disable the ORF capability, the local BGP router does not negotiate the ORF capability with the specified peer or peer group.

Table 92 Description of the both, send, and receive parameters and the negotiation result

Local parameter	Peer parameter	Negotiation result
send	<ul style="list-style-type: none">• receive• both	The ORF sending capability is enabled locally and the ORF receiving capability is enabled on the peer.
receive	<ul style="list-style-type: none">• send• both	The ORF receiving capability is enabled locally and the ORF sending capability is enabled on the peer.
both	both	Both the ORF sending and receiving capabilities are enabled locally and on the peer.

Examples

Enable the ORF capability for the BGP peer 1:2::3:4. Then, after negotiation, the local router can exchange ORF information with the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] peer 1:2::3:4 capability-advertise orf ipv6-prefix both
```

peer capability-advertise orf non-standard (IPv6 address family view)

Syntax

peer { *group-name* | *ipv6-address* } **capability-advertise orf non-standard**

undo peer { *group-name* | *ipv6-address* } **capability-advertise orf non-standard**

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Parameters

Use **peer capability-advertise orf non-standard** to enable the non-standard ORF capability (the early implementation of ORF is different from that defined in RFC) for a BGP peer or peer group.

Use **undo peer capability-advertise orf non-standard** to disable the non-standard ORF capability for the BGP peer or peer group.

By default, the non-standard ORF capability is not enabled for a BGP peer or peer group.

This command needs to be configured when the peer supports only non-standard ORF.

Related commands: **peer capability-advertise orf**.

Examples

Enable the non-standard ORF capability for the BGP peer 1:2::3:4 (suppose the BGP peer 1:2::3:4 can only send non-standard ORF packets).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] peer 1:2::3:4 capability-advertise orf non-standard
[Sysname-bgp-af-ipv6] peer 1:2::3:4 capability-advertise orf ip-prefix both
```

peer capability-advertise route-refresh

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **capability-advertise route-refresh**

undo peer { *ipv6-group-name* | *ipv6-address* } **capability-advertise route-refresh**

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description

Use **peer capability-advertise route-refresh** to enable IPv6 BGP route-refresh.

Use **undo peer capability-advertise route-refresh** to disable the function.

By default, route-refresh is enabled.

Examples

```
# Disable route-refresh of peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] undo peer 1:2::3:4 capability-advertise route-refresh
```

peer capability-advertise suppress-4-byte-as (IPv6 address family view)

Syntax

```
peer { group-name | ipv6-address } capability-advertise suppress-4-byte-as
undo peer { group-name | ipv6-address } capability-advertise suppress-4-byte-as
```

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description

Use **peer capability-advertise suppress-4-byte-as** to enable 4-byte AS number suppression.

Use **undo peer capability-advertise suppress-4-byte-as** to disable the function.

By default, the 4-byte AS number suppression function is disabled.

The device supports 4-byte AS numbers and uses 4-byte AS numbers by default. If the peer devices support only 2-byte AS numbers, you must enable the 4-byte AS number suppression function on the device.

If the peer device supports 4-byte AS numbers, do not enable the suppression function; otherwise, the BGP peer relationship cannot be established.

Examples

```
# In IPv6 address family view, enable 4-byte AS number suppression for peer 2001::1.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 2001::1 as-number 200
[Sysname-bgp-af-ipv6] peer 2001::1 capability-advertise suppress-4-byte-as
```

peer capability-advertise suppress-4-byte-as (IPv6 BGP-VPN instance view)

Syntax

```
peer ipv6-address capability-advertise suppress-4-byte-as  
undo peer ipv6-address capability-advertise suppress-4-byte-as
```

View

IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

ipv6-address: IPv6 address of a peer.

Description

Use **peer capability-advertise suppress-4-byte-as** to enable 4-byte AS number suppression.

Use **undo peer capability-advertise suppress-4-byte-as** to disable the function.

By default, the 4-byte AS number suppression function is disabled.

The device supports 4-byte AS numbers and uses 4-byte AS numbers by default. If the peer devices support only 2-byte AS numbers, you must enable the 4-byte AS number suppression function on the device.

If the peer device supports 4-byte AS numbers, do not enable the suppression function; otherwise, the BGP peer relationship cannot be established.

Examples

```
# In IPv6 BGP-VPN instance view, enable 4-byte AS number suppression for peer 2001::1.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family vpn-instance 11  
[Sysname-bgp-ipv6-11] peer 2001::1 as-number 200  
[Sysname-bgp-ipv6-11] peer 2001::1 capability-advertise suppress-4-byte-as
```

peer connect-interface (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } connect-interface interface-type interface-number  
undo peer { ipv6-group-name | ipv6-address } connect-interface
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

interface-type interface-number: Specifies an interface by its type and number.

Description

Use **peer connect-interface** to specify the source interface for establishing TCP connections to an IPv6 BGP peer or peer group.

Use **undo peer connect-interface** to restore the default.

By default, BGP uses the outbound interface of the best route to the IPv6 BGP peer/peer group as the source interface for establishing a TCP connection.

To enhance stability of IPv6 BGP connections, HP recommends using a loopback interface as the source interface for establishing a TCP connection.

To establish multiple BGP connections to a BGP router, you need to specify on the local router the respective source interfaces for establishing TCP connections to the peers on the peering BGP router; otherwise, the local BGP router may fail to establish TCP connections to the peers when using the outbound interfaces of the best routes as the source interfaces.

Examples

```
# Specify loopback 0 as the source interface for routing updates to peer 1:2::3:4.
```

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv6-family
```

```
[Sysname-bgp-af-ipv6] peer 1:2::3:4 connect-interface loopback 0
```

peer default-route-advertise

Syntax

```
peer { group-name | ipv4-address | ipv6-address } default-route-advertise [ route-policy route-policy-name ]
```

```
undo peer { group-name | ipv4-address | ipv6-address } default-route-advertise
```

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

route-policy-name: Name of a routing policy, a string of 1 to 63 characters.

Description

Use **peer default-route-advertise** to advertise a default route to a peer/peer group.

Use **undo peer default-route-advertise** to disable advertising a default route.

By default, no default route is advertised to a peer/peer group.

Using this command does not require the default route available in the routing table. With this command used, the router sends the default route unconditionally to the peer/peer group with the next hop being itself.

Examples

```
# Advertise a default route to peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 default-route-advertise
```

peer description (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } description description-text
undo peer { ipv6-group-name | ipv6-address } description
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

description-text: Description information for the peer/peer group, a string of 1 to 79 characters.

Description

Use **peer description** to configure the description information for a peer/peer group.

Use **undo peer description** to remove the description information of a peer/peer group.

By default, no description information is configured for a peer (group).

You need create a peer/peer group before configuring a description for it.

Examples

```
# Configure the description for the peer group test as ISP1.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test description ISP1
```

peer dscp (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } dscp dscp-value
undo peer { ipv6-group-name | ipv6-address } dscp
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies the name of a peer group, a string of 1 to 47 characters.

ipv6-address: Specifies the IPv6 address of a peer.

dscp-value: Specifies the DSCP value for IPv6 BGP packets, in the range of 0 to 63.

Description

Use **peer dscp** to set the DSCP value for IPv6 BGP packets sent to the specified IPv6 BGP peer or peer group.

Use **undo peer dscp** to remove the configuration.

By default, the DSCP value in BGP packets is 48.

The IPv6 BGP peer or peer group you specified must have been created.

Examples

In BGP view, set the DSCP value for IPv6 BGP packets sent to peer group **test** to 63.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test dscp 63
```

peer ebgp-max-hop (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } ebgp-max-hop [ hop-count ]
undo peer { ipv6-group-name | ipv6-address } ebgp-max-hop
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

hop-count: Maximum hop count, in the range of 1 to 255. By default, the value is 64.

Description

Use **peer ebgp-max-hop** to allow establishing the EBGp connection to a peer/peer group indirectly connected.

Use **undo peer ebgp-max-hop** to remove the configuration.

By default, this feature is disabled.

You can use the argument *hop-count* to specify the maximum router hops of the EBGP connection.

Examples

Allow establishing the EBGP connection with the peer group **test** on an indirectly connected network.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test ebgp-max-hop
```

peer enable (IPv6 address family view)

Syntax

```
peer { ipv4-group-name | ipv4-address | ipv6-address } enable
undo peer { ipv4-group-name | ipv4-address | ipv6-address } enable
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv4-group-name: Name of an IPv4 peer group, a string of 1 to 47 characters. The IPv4 peer group should be created beforehand.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description

Use **peer enable** to enable an IPv4 peer or peer group.

Use **undo peer enable** to disable an IPv4 peer or peer group.

By default, no IPv4 peer or peer group is enabled.

If an IPv4 peer or peer group is disabled, the router will not exchange routing information with it.

Examples

```
# Enable peer 1.1.1.1.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1.1.1.1 enable

# Enable peer 1::1.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1::1 group group1
[Sysname-bgp-af-ipv6] peer 1::1 enable
```

peer fake-as (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } fake-as as-number
undo peer { ipv6-group-name | ipv6-address } fake-as
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

as-number: Local AS number, in the range of 1 to 4294967295.

Description

Use **peer fake-as** to configure a fake local AS number for a peer or peer group.

Use **undo peer fake-as** to remove the configuration.

By default, no fake local AS number is configured for a peer or peer group.

Examples

```
# Configure a fake AS number of 200 for the peer group test.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test fake-as 200
```

peer filter-policy (IPv6 address family view)

Syntax

```
peer { group-name | ipv4-address | ipv6-address } filter-policy acl6-number { import | export }
undo peer { group-name | ipv4-address | ipv6-address } filter-policy [ acl6-number ] { import | export }
```

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

acl6-number: IPv6 ACL number, in the range of 2000 to 3999.

import: Applies the filter-policy to routes received from the peer/peer group.

export: Applies the filter-policy to routes advertised to the peer/peer group.

Description

Use **peer filter-policy** to configure an ACL-based filter policy for a peer or peer group.

Use **undo peer filter-policy** to remove the configuration.

By default, no ACL-based filter policy is configured for a peer or peer group.

Examples

```
# Apply the ACL6 2000 to filter routes advertised to the peer 1:2::3:4.
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2001:1:: 64
[Sysname-acl6-basic-2000] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 filter-policy 2000 export
```

peer group (IPv6 address family view)

Syntax

peer { *ipv4-address* | *ipv6-address* } **group** *group-name* [**as-number** *as-number*]

undo peer *ipv6-address* **group** *group-name*

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

as-number: Specifies the AS number of the peer/peer group, in the range of 1 to 4294967295.

Description

Use **peer group** to add a peer to a configured peer group.

Use **undo peer group** to delete a specified peer from a peer group.

By default, the peer does not belong to any peer group.

Examples

```
# Create a peer group named test and add the peer 1:2::3:4 to the peer group.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
```



```
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 200
[Sysname-bgp-af-ipv6] peer 1:2::3:4 group test
```

peer ignore (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } ignore
undo peer { ipv6-group-name | ipv6-address } ignore
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description

Use **peer ignore** to terminate the session to a peer or peer group.

Use **undo peer ignore** to remove the configuration.

By default, a router can establish sessions with a peer or peer group.

After the **peer ignore** command is executed, the system terminates the active session(s) with the specified peer or peer group and clears all the related routing information. For a peer group, all the sessions with the peer group will be torn down.

Examples

```
# Terminate the session with peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 ignore
```

peer ipv6-prefix

Syntax

```
peer { group-name | ipv4-address | ipv6-address } ipv6-prefix ipv6-prefix-name { import | export }
undo peer { group-name | ipv4-address | ipv6-address } ipv6-prefix { import | export }
```

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

ipv6-prefix-name: IPv6 prefix list name, a string of 1 to 19 characters.

import: Applies the filtering policy to routes received from the specified peer/peer group.

export: Applies the filtering policy to routes advertised to the specified peer/peer group.

Description

Use **peer ipv6-prefix** to specify an IPv6 prefix list to filter routes incoming from or outgoing to a peer or peer group.

Use **undo peer ipv6-prefix** to remove the configuration.

By default, no IPv6 prefix list is specified for filtering.

Examples

Reference the IPv6 prefix list **list 1** to filter routes outgoing to peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix list1 permit 2002:: 64
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 ipv6-prefix list1 export
```

peer ipsec-policy (IPv6 address family view)

Syntax

peer { *group-name* | *ipv6-address* } **ipsec-policy** *policy-name*

undo peer { *group-name* | *ipv6-address* } **ipsec-policy**

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of an IPv6 peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

policy-name: IPsec policy name, a string of 1 to 15 characters.

Description

Use **peer ipsec-policy** to apply an IPsec policy to an IPv6 BGP peer or peer group.

Use **undo peer ipsec-policy** to remove the applied IPsec policy.

By default, no IPsec policy is applied to any peer or peer group.

The IPsec policy to be applied must have been configured. Otherwise, the configuration fails.

You also need to make IPsec policy configuration on the peer or peer group. Otherwise, the local device will not receive IPv6 BGP packets from the peer or peer group.

Examples

```
# Apply IPsec policy policy001 to IPv6 BGP peer 1212::1111.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1212::1111 ipsec-policy policy001
```

peer keep-all-routes (IPv6 address family view)

Syntax

```
peer { group-name | ipv4-address | ipv6-address } keep-all-routes
undo peer { group-name | ipv4-address | ipv6-address } keep-all-routes
```

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description

Use **peer keep-all-routes** to save the original routing information from a peer or peer group, including even routes that failed to pass the inbound policy.

Use **undo peer keep-all-routes** to disable this function.

By default, the function is not enabled.

Examples

```
# Save routing information from peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 keep-all-routes
```

peer log-change (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } log-change
undo peer { ipv6-group-name | ipv6-address } log-change
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description

Use **peer log-change** to enable the logging of session state and event information of a specified peer or peer group.

Use **undo peer log-change** to remove the configuration.

The logging is enabled by default.

Examples

```
# Enable the logging of session state and event information of peer 1:2::3:4.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 log-change
```

peer next-hop-local (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } next-hop-local
undo peer { ipv6-group-name | ipv6-address } next-hop-local
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description

Use **peer next-hop-local** to configure the next hop of routes advertised to a peer/peer group as the local router.

Use **undo peer next-hop-local** to restore the default.

By default, the system sets the next hop of routes advertised to an EBGp peer/peer group to the local router, but does not change the next hop for routes outgoing to an IBGP peer/peer group.

Examples

```
# Set the next hop of routes advertised to IBGP peer group test to the router itself.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test internal
[Sysname-bgp-af-ipv6] peer test next-hop-local
```

peer password

Syntax

```
peer { group-name | ipv6-address } password { cipher | simple } password
undo peer { group-name | ipv6-address } password
```

View

IPv6 address family view

Default level

2: System view

Parameters

group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Sets the password. This argument is case sensitive. It must be a ciphertext string of 1 to 137 characters, or a plaintext string of 1 to 80 characters.

Description

Use **peer password** to configure BGP to perform MD5 authentication when a TCP connection is being established with a peer/peer group.

Use **undo peer password** to restore the default.

By default, no MD5 authentication is performed for TCP connection establishment.

The MD5 authentication requires that the two parties have the same authentication mode and password to establish TCP connection; otherwise, the TCP connection cannot be established due to authentication failure.

The authentication password, set in either plain text or cipher text, is saved to the configuration file in cipher text.

Examples

```
# Enable MD5 authentication for establishing TCP connection between the local device (1:2::3:3) and peer device (1:2::3:4), and configure the authentication password as aabbcc.
```

- On the local device:

```
<Sysname> system-view
[Sysname] bgp 3
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 password cipher aabbcc
```

- On the peer device:

```
<Sysname> system-view
[Sysname] bgp 4
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:3 password cipher aabbcc
```

peer preferred-value (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } preferred-value value  
undo peer { ipv6-group-name | ipv6-address } preferred-value
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

value: Preferred value, in the range of 0 to 65535.

Description

Use **peer preferred-value** to assign a preferred value to routes received from a peer or peer group.

Use **undo peer preferred-value** to restore the default.

By default, routes received from a peer or peer group have a preferred value of 0.

Routes learned from peers each have an initial preferred value. Among multiple routes to the same destination, the route with the biggest value is selected.

If you both reference a routing policy and use the command **peer { ipv6-group-name | ipv6-address } preferred-value value** to set a preferred value for routes from a peer, the routing policy sets the specific preferred value for routes matching it. If the preferred value in the routing policy is zero, the routes use the value set with the **peer { ipv6-group-name | ipv6-address } preferred-value value** command. For how to use a routing policy to set a preferred value, see the command **peer { group-name | ipv4-address | ipv6-address } route-policy route-policy-name { import | export }** in this document, and the command **apply preferred-value preferred-value** in "Routing policy configuration commands."

Examples

```
# Configure the preferred value as 50 for routes from peer 1:2::3:4.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] peer 1:2::3:4 preferred-value 50
```

peer preferred-value (IPv6 BGP-VPN instance view)

Syntax

```
peer ipv6-address preferred-value value  
undo peer ipv6-address [ preferred-value ]
```

View

IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

ipv6-address: IPv6 address of a peer.

value: Preferred value, in the range of 0 to 65535.

Description

Use **peer preferred-value** to assign a preferred value to routes received from a peer or peer group.

Use **undo peer preferred-value** to restore the default.

By default, routes received from a peer or peer group have a preferred value of 0.

Routes learned from peers each have an initial preferred value. Among multiple routes to the same destination, the route with the biggest value is selected.

If you both reference a routing policy and use the command **peer ipv6-address preferred-value value** to set a preferred value for routes from a peer, the routing policy sets the specific preferred value for routes matching it. If the preferred value in the routing policy is zero, the routes use the value set with the **peer ipv6-address preferred-value value** command. For how to use a routing policy to set a preferred value, see the command **peer ipv6-address route-policy route-policy-name { import | export }** in this document, and the command **apply preferred-value preferred-value** in "Routing policy configuration commands."

Examples

```
# Configure the preferred value as 50 for routes from peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family vpn-instance 11
[Sysname-bgp-ipv6-11] peer 1:2::3:4 preferred-value 50
```

peer public-as-only (IPv6 address family view)

Syntax

peer { ipv6-group-name | ipv6-address } public-as-only

undo peer { ipv6-group-name | ipv6-address } public-as-only

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description

Use **peer public-as-only** to configure IPv6 BGP updates to a peer/peer group to not carry private AS numbers.

Use **undo peer public-as-only** to allow IPv6 BGP updates to a peer/peer group to carry private AS numbers.

By default, BGP updates carry the private AS number.

The command does not take effect if the BGP update has both the public AS number and private AS number. The range of private AS number is from 64512 to 65535.

Examples

```
# Configure BGP updates sent to the peer 1:2::3:4 to not carry private AS numbers.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 public-as-only
```

peer reflect-client (IPv6 address family view)

Syntax

```
peer { group-name | ipv4-address | ipv6-address } reflect-client
undo peer { group-name | ipv4-address | ipv6-address } reflect-client
```

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description

Use **peer reflect-client** to configure the router as a route reflector and specify a peer/peer group as a client.

Use **undo peer reflect-client** to remove the configuration.

By default, neither route reflector nor client is configured.

Related commands: **reflect between-clients** and **reflector cluster-id**.

Examples

```
# Configure the local device as a route reflector and specify the peer group test as a client.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test
[Sysname-bgp-af-ipv6] peer test reflect-client
```

peer route-limit (IPv6 address family view)

Syntax

```
peer { group-name | ipv4-address | ipv6-address } route-limit prefix-number [ { alert-only | reconnect
reconnect-time } | percentage ] *
```


undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-limit**

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

prefix number: Specifies the upper limit of prefixes that can be received from the peer or peer group. The limit range varies depending on the switch model. When the received prefixes from the peer/peer group reach the specified upper limit, the router will disconnect from the peer/peer group.

alert-only: When the received prefixes from the peer/peer group reach the specified upper limit, the router will display alarm messages rather than disconnect from the peer/peer group.

reconnect-time: Interval for the router to reconnect to the peer/peer group. The argument has no default. It ranges from 1 to 65535 seconds.

percentage: Specifies a percentage value. If the percentage of received routes to the upper limit reaches the value, the router will generate alarm messages. The default is 75. The value is in the range of 1 to 100.

Description

Use **peer route-limit** to set the maximum number of prefixes that can be received from a peer/peer group.

Use **undo peer route-limit** to restore the default.

By default, the router has no limit on prefixes from a peer/peer group.

The router will end the peer relation when the number of address prefixes received for the peer exceeds the limit.

Examples

```
# Set the number of prefixes allowed to receive from the peer 1:2::3:4 to 100.
```

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv6-family
```

```
[Sysname-bgp-af-ipv6] peer 1:2::3:4 route-limit 100
```

peer route-policy (IPv6 address family view)

Syntax

peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

route-policy-name: Name of a routing policy, a string of 1 to 63 characters.

import: Applies the routing policy to routes from the peer (group).

export: Applies the routing policy to routes sent to the peer (group).

Description

Use **peer route-policy** to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use **undo peer route-policy** to remove the configuration.

By default, no routing policy is specified for the peer (group).

The **peer route-policy** command does not use the **if-match interface** clause defined in the routing policy. See "Routing policy configuration commands" for related information.

Examples

Apply the routing policy test-policy to routes received from the peer group test.

```
<Sysname> system-view
[Sysname] route-policy test-policy permit node 10
[Sysname-route-policy] if-match cost 10
[Sysname-route-policy] apply cost 65535
[Sysname-route-policy] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test route-policy test-policy import
```

peer route-policy (IPv6 BGP-VPN instance view)

Syntax

peer *ipv6-address* **route-policy** *route-policy-name* { **export** | **import** }

undo peer *ipv6-address* [**route-policy** *route-policy-name* { **export** | **import** }]

View

IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

ipv6-address: IPv6 address of a peer.

route-policy-name: Name of a routing policy, a string of 1 to 63 characters.

import: Applies the routing policy to routes from the peer (group).

export: Applies the routing policy to routes sent to the peer (group).

Description

Use **peer route-policy** to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use **undo peer route-policy** to remove the configuration.

By default, no routing policy is specified for the peer (group).

The **peer route-policy** command does not use the **if-match interface** clause defined in the routing policy. See "Routing policy configuration commands" for related information.

Examples

```
# Apply the routing policy test-policy to routes received from the peer 2001::1.
<Sysname> system-view
[Sysname] route-policy test-policy permit node 10
[Sysname-route-policy] if-match cost 10
[Sysname-route-policy] apply cost 65535
[Sysname-route-policy] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family vpn-instance vpn1
[Sysname-bgp-ipv6-vpn1] peer 2001::1 route-policy test-policy import
```

peer route-update-interval (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } route-update-interval interval
undo peer { ipv6-group-name | ipv6-address } route-update-interval
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

interval: Specifies the minimum interval for sending the same update to a peer (group) from 0 to 600 seconds.

Description

Use **peer route-update-interval** to specify the interval for sending the same update to a peer/peer group.

Use **undo peer route-update-interval** to restore the default.

By default, the interval is 15 seconds for the IBGP peer, and 30 seconds for the EBGP peer.

Examples

```
# Specify the interval for sending the same update to the peer 1:2::3:4 as 10 seconds.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] peer 1:2::3:4 route-update-interval 10
```

peer substitute-as (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } substitute-as
undo peer { ipv6-group-name | ipv6-address } substitute-as
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description

Use **peer substitute-as** to substitute the local AS number for the AS number of a peer/peer group in the AS_PATH attribute.

Use **undo peer substitute-as** to remove the configuration.

The substitution is not configured by default.

Examples

```
# Substitute the local AS number for the AS number of peer 1:2::3:4.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 substitute-as
```

peer timer (IPv6 address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } timer keepalive keepalive hold holdtime
undo peer { ipv6-group-name | ipv6-address } timer
```

View

IPv6 address family view

Default level

2: System level

Parameters

ipv6-group-name: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

keepalive: Specifies the keepalive interval in seconds, ranging from 0 to 21845.

holdtime: Specifies the holdtime in seconds, whose value is 0 or in the range of 3 to 65535.

Description

Use **peer timer** to configure keepalive interval and holdtime interval for a peer or peer group.

Use **undo peer timer** to restore the default.

keepalive interval defaults to 60 seconds, and *holdtime* interval defaults to 180 seconds.

The timers configured with this command are preferred to the timers configured with the **timer** command.

If the holdtime interval is configured as 0, no keepalive message will be sent to the peer, and the peer connection will never time out. If the keepalive interval is configured as 0 and the negotiated hold time is not 0, one third of the hold time is taken as the interval for sending keepalive messages.

If neither the holdtime interval nor the keepalive interval is configured as 0, the holdtime interval must be at least three times the keepalive interval.

After this command is executed, the peer connection is closed at once, and a new connection to the peer is negotiated using the configured hold time.

Related commands: **timer**.

Examples

Configure the keepalive interval and holdtime interval for the peer group test as 60 seconds and 180 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test timer keepalive 60 hold 180
```

Configure both the keepalive interval and holdtime interval for peer group **test** as 0 seconds, indicating the peer group will never time out.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test timer keepalive 0 hold 0
```

preference (IPv6 address family view/IPv6 BGP-VPN instance view)

Syntax

preference { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }

undo preference

View

IPv6 address family view, IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

external-preference: Preference of EBGP route learned from an EBGP peer, in the range of 1 to 255.

internal-preference: Preference of IBGP route learned from an IBGP peer, in the range of 1 to 255.

local-preference: Preference of IPv6 BGP local route, in the range of 1 to 255.

route-policy-name: Routing policy name, a string of 1 to 63 characters. The routing policy can set a preference for routes passing it. The default value applies to the routes filtered out.

Description

Use **preference** to configure preferences for EBGP, IBGP, and local routes.

Use **undo preference** to restore the default.

The bigger the preference value is, the lower the preference is. The default values of *external-preference*, *internal-preference* and *local-preference* are 255, 255 and 130.

Examples

```
# Configure preferences for EBGP, IBGP, and local routes as 20, 20 and 200.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] preference 20 20 200
```

reflect between-clients (IPv6 address family view)

Syntax

reflect between-clients

undo reflect between-clients

View

IPv6 address family view

Default level

2: System level

Parameters

None

Description

Use **reflect between-clients** to enable route reflection between clients.

Use **undo reflect between-clients** to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects routes between clients. If the clients are fully meshed, HP recommends disabling route reflection on the route reflector to reduce costs.

Related commands: **reflector cluster-id** and **peer reflect-client**.

Examples

```
# Enable route reflection between clients.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] reflect between-clients
```

reflector cluster-id (IPv6 address family view)

Syntax

reflector cluster-id *cluster-id*

undo reflector cluster-id

View

IPv6 address family view

Default level

2: System level

Parameters

cluster-id: Specifies the cluster ID of the route reflector, an integer from 1 to 4294967295 (the system translates it into an IPv4 address) or an IPv4 address.

Description

Use **reflector cluster-id** to configure the cluster ID of the route reflector.

Use **undo reflector cluster-id** to remove the configured cluster ID.

By default, a route reflector uses its router ID as the cluster ID.

Typically, a cluster has only one route reflector, so the router ID of the route reflector identifies the cluster. If multiple route reflectors are configured to improve the stability of the network, you should use this command to configure the identical cluster ID for all the reflectors to avoid routing loops.

Related commands: **reflect between-clients** and **peer reflect-client**.

Examples

```
# Set 50 as the cluster ID for the route reflector, which is one of multiple route reflectors in the cluster.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] reflector cluster-id 50
```

refresh bgp ipv6

Syntax

refresh bgp ipv6 { *ipv4-address* | *ipv6-address* | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** }

View

User view

Default level

1: Monitor level

Parameters

ipv4-address: Soft-resets the connection with an IPv4 BGP peer.

ipv6-address: Soft-resets the connection with an IPv6 BGP peer.

all: Soft-resets all IPv6 BGP connections.

external: Soft-resets EBGP connections.

group *ipv6-group-name*: Soft-resets connections with a peer group. The name of the peer group is a string of 1 to 47 characters.

internal: Soft-resets IBGP connections.

export: Performs soft reset in outbound direction.

import: Performs soft reset in inbound direction.

Description

Use **refresh bgp ipv6** to soft reset specified IPv4/IPv6 BGP connections. With this feature, you can refresh the IPv4/IPv6 BGP routing table and apply a new available policy without tearing down BGP connections.

To perform IPv4/IPv6 BGP soft reset, all routers in the network should support route-refresh. If a router not supporting route refresh exists in the network, you need to use the **peer keep-all-routes** command on the local router to save all route updates before performing soft reset.

Examples

```
# Soft reset inbound IPv6 BGP connections.  
<Sysname> refresh bgp ipv6 all import
```

reset bgp ipv6

Syntax

```
reset bgp ipv6 { as-number | ipv4-address | ipv6-address | all | external | group group-name | internal }
```

View

User view

Default level

2: System level

Parameters

as-number: Resets the IPv6 BGP connections to peers in the specified AS. The AS number is in the range of 1 to 4294967295.

ipv4-address: Resets the connection to the specified IPv4 BGP peer.

ipv6-address: Resets the connection to the specified IPv6 BGP peer.

all: Resets all IPv6 BGP connections.

external: Resets all the EBGP connections.

group *group-name*: Resets the connections to the specified IPv6 BGP peer group.

internal: Resets all the IBGP connections.

Description

Use **reset bgp ipv6** to reset specified IPv4/IPv6 BGP connections.

Examples

```
# Reset all the IPv6 BGP connections.  
<Sysname> reset bgp ipv6 all
```

reset bgp ipv6 dampening

Syntax

```
reset bgp ipv6 dampening [ ipv6-address prefix-length ]
```

View

User view

Default level

1: Monitor level

Parameters

ipv6-address: IPv6 address

prefix-length: Prefix length of the address, in the range of 0 to 128.

Description

Use **reset bgp ipv6 dampening** to clear dampened IPv6 BGP route information and release suppressed routes.

If no *ipv6-address prefix-length* is specified, all dampened IPv6 BGP route information will be cleared.

Examples

```
# Clear the dampened information of routes to 2345::/64 and release suppressed routes.  
<Sysname> reset bgp ipv6 dampening 2345:: 64
```

reset bgp ipv6 flap-info

Syntax

```
reset bgp ipv6 flap-info [ ipv6-address/prefix-length | as-path-acl as-path-acl-number | regex as-path-regexp ]
```

```
reset bgp ipv6 peer-ipv6-address flap-info
```

View

User view

Default level

1: Monitor level

Parameters

ipv6-address: Clears the flap statistics for the specified IPv6 address.

prefix-length: Prefix length of the address, in the range of 1 to 128.

as-path-acl-number: Clears the flap statistics for routes matching the AS path list. The number is in the range of 1 to 256.

as-path-regexp: Clears the flap statistics for routes matching the AS path regular expression.

peer-ipv6-address: Clears the flap statistics for inbound routes from the peer. *peer-ipv6-address* is the address of the peer.

Description

Use **reset bgp ipv6 flap-info** to clear IPv6 routing flap statistics.

If no parameters are specified, the flap statistics of all the routes will be cleared

Examples

```
# Clear the flap statistics of the routes matching AS path ACL 10.
```

```
<Sysname> system-view
[Sysname] ip as-path 10 permit ^100.*200$
[Sysname] quit
<Sysname> reset bgp ipv6 flap-info as-path-acl 10
```

router-id

Syntax

router-id *router-id*

undo router-id

View

BGP view

Default level

2: System level

Parameters

router-id: Router ID in IP address format.

Description

Use **router-id** to specify a router ID for the router.

Use **undo router-id** to remove a router ID.

To run IPv6 BGP protocol, a router must have a router ID, an unsigned 32-bit integer and the unique ID of the router in the AS.

You can specify a router ID manually. Otherwise, the system selects the highest IPv4 address among loopback interface addresses as the router ID. If no loopback interface addresses are available, the system selects the highest IPv4 address among physical interface IPv4 addresses as the router ID. Specify a loopback interface address as the router ID to enhance network reliability.

If the interface whose IPv4 address is selected as the router ID or the manual router ID is deleted, the system selects a new router ID for the router.

Examples

```
# Specify the router ID of the router as 10.18.4.221.
```

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] router-id 10.18.4.221
```

synchronization (IPv6 address family view)

Syntax

```
synchronization  
undo synchronization
```

View

IPv6 address family view

Default level

2: System level

Parameters

None

Description

Use **synchronization** to enable the synchronization between IPv6 BGP and IGP.

Use **undo synchronization** to disable the synchronization.

The feature is disabled by default.

With this feature enabled and when a non-BGP router is responsible for forwarding packets in an AS, IPv6 BGP speakers in the AS cannot advertise routing information to other ASs unless all routers in the AS know the latest routing information.

By default, upon receiving an IPv6 IBGP route, the BGP router only checks whether the next hop is reachable before advertisement. If synchronization is enabled, the IBGP route can be advertised to EBGp peers only when the route is also advertised by the IGP.

Examples

```
# Enable the route synchronization between IPv6 BGP and IGP.
```

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] synchronization
```

timer (IPv6 address family view)

Syntax

```
timer keepalive keepalive hold holdtime  
undo timer
```

View

IPv6 address family view

Default level

2: System level

Parameters

keepalive: Keepalive interval in seconds, ranging from 0 to 21845.

holdtime: Holdtime interval in seconds, whose value is 0 or in the range of 3 to 65535.

Description

Use **timer** to specify the IPv6 BGP keepalive interval and holdtime interval.

Use **undo timer** to restore the default.

By default, the keepalive and holdtime intervals are 60s and 180s.

The timers configured with the **peer timer** command are preferred to the timers configured with the **timer** command.

If the holdtime interval is configured as 0, no keepalive message will be sent to the peer, and the peer connection will never time out. If the keepalive interval is configured as 0 and the negotiated hold time is not 0, one third of the hold time is taken as the interval for sending keepalive messages.

If neither the holdtime interval nor the keepalive interval is configured as 0, the holdtime interval must be at least three times the keepalive interval.

The configured timers apply to all IPv6 BGP peers, but they become valid for an IPv6 BGP peer only after the relevant IPv6 BGP connection is reset.

After this command is executed, no peer connection is closed at once. The configured hold time is used for negotiation when a peer relationship is reestablished.

Related commands: **peer timer**.

Examples

Configure keepalive interval and holdtime interval as 60 and 180 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] timer keepalive 60 hold 180
```

Routing policy configuration commands

The common routing policy configuration commands are applicable to both IPv4 and IPv6.

The A5500 SI Switch Series does not support OSPF, BGP, IS-IS, OSPFv3, IPv6 BGP, or IPv6 IS-IS.

Common routing policy configuration commands

apply as-path

Syntax

```
apply as-path as-number&<1-10> [ replace ]
```

```
undo apply as-path
```

View

Routing policy view

Default level

2: System level

Parameters

as-number&<1-10>: AS number, in the range of 1 to 4294967295. &<1-10>: Indicates you can enter up to 10 AS numbers.

replace: Replaces the original AS numbers.

Description

Use **apply as-path** to apply the specified AS numbers to BGP routes.

Use **undo apply as-path** to remove the clause configuration.

No AS_PATH attribute is set by default.

With the **replace** keyword included, the **apply as-path** command replaces the original AS_PATH attribute with the specified AS numbers. Without the **replace** keyword, this command adds the specified AS numbers before the original AS_PATH attribute.

Examples

```
# Configure node 10 in permit mode of routing policy policy1: add AS number 200 before the original AS_PATH attribute of BGP routing information matching AS path list 1.
```

```
<Sysname> system-view  
[Sysname] route-policy policy1 permit node 10  
[Sysname-route-policy] if-match as-path 1  
[Sysname-route-policy] apply as-path 200
```

apply comm-list delete

Syntax

```
apply comm-list { comm-list-number | comm-list-name } delete
```

undo apply comm-list

View

Routing policy view

Default level

2: System level

Parameters

comm-list-number: Community list number. A basic community list number ranges from 1 to 99. An advanced community list number ranges from 100 to 199.

comm-list-name: Community list name, a string of 1 to 31 characters, which can contain letters, numbers, and signs.

Description

Use **apply comm-list delete** to remove the COMMUNITY attributes specified by the community list from BGP routing information.

Use **undo apply comm-list** to remove the clause configuration.

No COMMUNITY attributes are removed from BGP routing information by default.

Examples

Configure node 10 in **permit** mode of routing policy **policy1**: remove the COMMUNITY attributes specified in community list 1 from the BGP routing information matching AS path list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply comm-list 1 delete
```

apply community

Syntax

apply community { **none** | **additive** | { *community-number*&<1-16> | *aa:nn*&<1-16> | **internet** | **no-advertise** | **no-export** | **no-export-subconfed** } * [**additive**] }

undo apply community

View

Routing policy view

Default level

2: System level

Parameters

none: Removes the COMMUNITY attributes of BGP routes.

community-number: Community sequence number, in the range of 1 to 4294967295.

aa:nn: Community number; both *aa* and *nn* are in the range of 0 to 65535.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

internet: Sets the INTERNET community attribute for BGP routes. Routes with this attribute can be advertised to all BGP peers.

no-advertise: Sets the NO_ADVERTISE community attribute for BGP routes. Routes with this attribute cannot be advertised to any peers.

no-export: Sets the NO_EXPORT community attribute for BGP routes. Routes with this attribute cannot be advertised out of the autonomous system or confederation, but can be advertised to other sub ASs in the confederation.

no-export-subconfed: Sets the NO_EXPORT_SUBCONFED community attribute for BGP routes. Routes with this attribute cannot be advertised out of the sub autonomous system.

additive: Adds the specified COMMUNITY attribute to the original COMMUNITY attribute of BGP routes.

Description

Use **apply community** to set the specified COMMUNITY attribute for BGP routes.

Use **undo apply community** to remove the apply clause.

No COMMUNITY attribute is set for BGP routes by default.

Related commands: **ip community-list** and **if-match community**.

Examples

Configure node 16 in **permit** mode of routing policy **setcommunity** to set the NO_EXPORT community attribute for BGP routes matching AS path list 8.

```
<Sysname> system-view
[Sysname] route-policy setcommunity permit node 16
[Sysname-route-policy] if-match as-path 8
[Sysname-route-policy] apply community no-export
```

apply cost

Syntax

apply cost [+ | -] *value*

undo apply cost

View

Routing policy view

Default level

2: System level

Parameters

+: Increases a cost value.

-: Decreases a cost value.

value: Cost in the range of 0 to 4294967295.

Description

Use **apply cost** to set a cost for routing information.

Use **undo apply cost** to remove the clause configuration.

No cost is set for routing information by default.

Examples

Configure node 10 in **permit** mode of routing policy **policy1**: set a cost of 120 for routing information whose outbound interface is Vlan-interface 20.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match interface Vlan-interface 20
[Sysname-route-policy] apply cost 120
```

apply cost-type

Syntax

apply cost-type { **external** | **internal** | **type-1** | **type-2** }

undo apply cost-type

View

Routing policy view

Default level

2: System level

Parameters

external: Sets the cost type to IS-IS external route.

internal: Sets the cost type to IS-IS internal route, or sets the MED value for a matching BGP route as the IGP metric to the route's next hop.

type-1: Sets the cost type to Type-1 external route of OSPF.

type-2: Sets the cost type to Type-2 external route of OSPF.

Description

Use **apply cost-type** to set a cost type for routing information.

Use **undo apply cost-type** to remove the clause configuration.

No cost type is set for routing information by default.

- Used for IS-IS, the **apply cost-type internal** command sets the cost type of a matching IS-IS route as IS-IS internal route.
- Use for BGP, the **apply cost-type internal** command sets the MED of a matching BGP route learned from an IBGP peer as the IGP metric to the route's next hop before BGP advertises the route to an eBGP peer.

Examples

Create node 10 in **permit** mode of routing policy **policy1**: If a route has a tag of 8, set the cost type for the route to IS-IS internal route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
[Sysname-route-policy] apply cost-type internal
```


apply extcommunity

Syntax

```
apply extcommunity { rt route-target }&<1-16> [ additive ]  
undo apply extcommunity
```

View

Routing policy view

Default level

2: System level

Parameters

rt route-target: Sets the route target (RT) extended community attribute, a string of 3 to 21 characters.

A *route-target* has one of the following forms:

- **16-bit AS number**—32-bit self-defined number, for example, 101:3
- **32-bit IP address**—16-bit self-defined number, for example, 192.168.122.15:1
- **32-bit AS number**—16-bit self-defined number, for example, 70000:3. The AS number should be no less than 65536.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

additive: Adds the specified attribute to the original RT community attribute.

Description

Use **apply extcommunity** to apply the specified RT extended community attribute to BGP routes.

Use **undo apply extcommunity** to remove the clause configuration.

No RT extended community attribute is set for BGP routing information by default.

Examples

Configure node 10 in **permit** mode of routing policy **policy1**: If a BGP route matches AS path list 1, add the RT extended community attribute 100:2 to the route.

```
<Sysname> system-view  
[Sysname] route-policy policy1 permit node 10  
[Sysname-route-policy] if-match as-path 1  
[Sysname-route-policy] apply extcommunity rt 100:2 additive
```

apply isis

Syntax

```
apply isis { level-1 | level-1-2 | level-2 }  
undo apply isis
```

View

Routing policy view

Default level

2: System level

Parameters

level-1: Redistributes routes into IS-IS level-1.

level-1-2: Redistributes routes into both IS-IS level-1 and level-2.

level-2: Redistributes routes into IS-IS level-2.

Description

Use **apply isis** to redistribute routes into a specified ISIS level.

Use **undo apply isis** to remove the clause configuration.

No IS-IS level is set by default.

Examples

Configure node 10 in **permit** mode of routing policy **policy1**: If a route has a tag of 8, redistribute the route to IS-IS level-2.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
[Sysname-route-policy] apply isis level-2
```

apply local-preference

Syntax

apply local-preference *preference*

undo apply local-preference

View

Routing policy view

Default level

2: System level

Parameters

preference: Local preference for BGP routes, in the range of 0 to 4294967295.

Description

Use **apply local-preference** to configure the specified local preference for BGP routes.

Use **undo apply local-preference** to remove the clause configuration.

No local preference is configured for BGP routing information by default.

Examples

Configure node 10 in **permit** mode of routing policy **policy1**: If a route matches AS path list 1, configure a local preference of 130 for the route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply local-preference 130
```

apply origin

Syntax

```
apply origin { egp as-number | igp | incomplete }  
undo apply origin
```

View

Routing policy view

Default level

2: System level

Parameters

egp: Sets the ORIGIN attribute of BGP routing information to EGP.

as-number: AS number for EGP routes, in the range of 1 to 4294967295.

igp: Sets the ORIGIN attribute of BGP routing information to IGP.

incomplete: Sets the ORIGIN attribute of BGP routing information to unknown.

Description

Use **apply origin** to set the specified origin attribute for BGP routes.

Use **undo apply origin** to remove the clause configuration.

No ORIGIN attribute is set for BGP routing information by default.

Examples

Configure node 10 in **permit** mode of routing policy **policy1**: If BGP routing information matches AS path list 1, set the ORIGIN attribute of the routing information to IGP.

```
<Sysname> system-view  
[Sysname] route-policy policy1 permit node 10  
[Sysname-route-policy] if-match as-path 1  
[Sysname-route-policy] apply origin igp
```

apply preference

Syntax

```
apply preference preference  
undo apply preference
```

View

Routing policy view

Default level

2: System level

Parameters

preference: Routing protocol preference, in the range of 1 to 255.

Description

Use **apply preference** to set a preference for a routing protocol.

Use **undo apply preference** to remove the clause configuration.

No preference is set for a routing protocol by default.

If you have set preferences for routing protocols with the **preference** command, using the **apply preference** command will set a new preference for the matching routing protocol. Non-matching routing protocols still use the preferences set by the **preference** command.

Examples

```
# Configure node 10 in permit mode of routing policy policy1: Set the preference for OSPF external routes to 90.
```

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type external-type1or2
[Sysname-route-policy] apply preference 90
```

apply preferred-value

Syntax

apply preferred-value *preferred-value*

undo apply preferred-value

View

Routing policy view

Default level

2: System level

Parameters

preferred-value: Preferred value, in the range of 0 to 65535.

Description

Use **apply preferred-value** to set a preferred value for BGP routes.

Use **undo apply preferred-value** to remove the clause configuration.

No preferred value is set for BGP routes by default.

Examples

```
# Configure node 10 in permit mode of routing policy policy1: Set a preferred value of 66 for BGP routing information matching AS path list 1.
```

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply preferred-value 66
```

apply tag

Syntax

apply tag *value*

undo apply tag

View

Routing policy view

Default level

2: System level

Parameters

value: Tag value, in the range of 0 to 4294967295.

Description

Use **apply tag** to set a specified tag value for RIP, OSPF or IS-IS routing information.

Use **undo apply tag** to remove the clause configuration.

No routing tag is set for RIP, OSPF or IS-IS routing information by default.

Examples

Configure node 10 in **permit** mode of routing policy **policy1**: set a tag of 100 for OSPF external routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type external-type1
[Sysname-route-policy] apply tag 100
```

continue

Syntax

continue [*node-number*]

undo continue

View

Routing policy view

Default level

2: System level

Parameters

node-number: Routing policy node number, in the range of 0 to 65535.

Description

Use **continue** to specify the next node of the routing policy to be matched.

Use **undo continue** to remove the configuration.

By default, no next routing policy node is specified.

The node number specified must be larger than the current node number.

Example

Create routing policy **policy1** with node 10, and specify the match mode as **permit**. Specify the number of the next routing policy node to be matched as 20.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] continue 20
```

display ip as-path

Syntax

```
display ip as-path [ as-path-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

as-path-number: AS path list number, in the range of 1 to 256.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip as-path** to display BGP AS path list information.

Information about all BGP AS path lists will be displayed if no *as-path-number* is specified.

Related commands: **ip as-path**, **if-match as-path**, and **apply as-path**.

Examples

```
# Display the information of BGP AS path list 1.
```

```
<Sysname> display ip as-path 1
```

```
ListID   Mode      Expression
1        permit    2
```

Table 93 Command output

Field	Description
ListID	AS path list ID
Mode	Match mode: permit or deny
Expression	Regular expression for matching

display ip community-list

Syntax

```
display ip community-list [ basic-community-list-number | adv-community-list-number | comm-list-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

basic-community-list-number: Basic community list number, in the range of 1 to 99.

adv-community-list-number: Advanced community list number, in the range of 100 to 199.

comm-list-name: Community list name, a string of 1 to 31 characters, which can contain letters, numbers, and signs.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip community-list** to display BGP community list information.

All BGP community list information will be displayed if no *basic-community-list-number* or *adv-community-list-number* is specified.

Related commands: **ip community-list**, **if-match community**, and **apply community**.

Examples

```
# Display the information of the BGP community list 1.
<Sysname> display ip community-list 1
Community List Number 1
    permit 1:1 1:2 2:2
```

display ip extcommunity-list

Syntax

```
display ip extcommunity-list [ ext-comm-list-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ext-comm-list-number: Extended community list number, in the range of 1 to 199.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip extcommunity-list** to display BGP extended community list information.

All BGP extended community list information will be displayed if no *ext-comm-list-number* is specified.

Related commands: **ip extcommunity-list**, **if-match extcommunity**, and **apply extcommunity**.

Examples

Display the information of BGP extended community list 1.

```
<Sysname> display ip extcommunity-list 1
Extended Community List Number 1
    permit rt : 9:6
```

display route-policy

Syntax

```
display route-policy [ route-policy-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

route-policy-name: Routing policy name, a case-sensitive string of 1 to 63 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display route-policy** to display routing policy information.

All routing policy information will be displayed if no *route-policy-name* is specified.

Related commands: **route-policy**.

Examples

Display the information of routing policy 1.

```
<Sysname> display route-policy policy1
Route-policy : policy1
    permit : 10
        if-match ip-prefix abc
        apply cost 120
```


Table 94 Command output.

Field	Description
Route-policy	Routing policy name.
Permit	Match mode of routing policy node 10.
if-match ip-prefix abc	Match criterion.
apply cost 120	If the match criterion is satisfied, set a cost of 120 for routing information.

if-match as-path

Syntax

```
if-match as-path as-path-number&<1-16>  
undo if-match as-path [ as-path-number&<1-16> ]
```

View

Routing policy view

Default level

2: System level

Parameters

as-path-number: AS path list number, in the range of 1 to 256.
&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description

Use **if-match as-path** to specify AS path lists for matching against the AS_PATH attribute of BGP routing information.

Use **undo if-match as-path** to remove the match criterion.

The match criterion is not configured by default.

Related commands: **ip as-path-acl**.

Examples

```
# Define AS path list 2, allowing BGP routing information containing AS number 200 or 300 to pass.  
Configure node 10 in permit mode of routing policy test to match AS path list.  
<Sysname> system-view  
[Sysname] ip as-path 2 permit _*200.*300  
[Sysname] route-policy test permit node 10  
[Sysname-route-policy] if-match as-path 2
```

if-match community

Syntax

```
if-match community { { basic-community-list-number | comm-list-name } [ whole-match ] |  
adv-community-list-number }&<1-16>  
undo if-match community [ { basic-community-list-number | comm-list-name } [ whole-match ] |  
adv-community-list-number ]&<1-16>
```

View

Routing policy view

Default level

2: System level

Parameters

basic-community-list-number: Basic community list number, in the range of 1 to 99.

adv-community-list-number: Advanced community list number, in the range of 100 to 199.

comm-list-name: Community list name, a string of 1 to 31 characters, which can contain letters, numbers, and signs.

whole-match: Exactly matches the specified community lists.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description

Use **if-match community** to specify community lists for matching against the COMMUNITY attribute of BGP routing information.

Use **undo if-match community** to remove the match criterion.

The match criterion is not configured by default.

Related commands: **ip community-list**.

Examples

Define community list 1, allowing BGP routing information with community number 100 or 200 to pass. Then configure node 10 in **permit** mode of routing policy **test**: specify community-list 1 for matching.

```
<Sysname> system-view
[Sysname] ip community-list 1 permit 100 200
[Sysname] route-policy test permit node 10
[Sysname-route-policy] if-match community 1
```

if-match cost

Syntax

if-match cost *value*

undo if-match cost

View

Routing policy view

Default level

2: System level

Parameters

value: Cost in the range of 0 to 4294967295.

Description

Use **if-match cost** to match routing information having the specified cost.

Use **undo if-match cost** to remove the match criterion.

The match criterion is not configured by default.

Examples

Configure node 10 in **permit** mode of routing policy **policy1**: define an if-match clause to permit routing information with a cost of 8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match cost 8
```

if-match extcommunity

Syntax

```
if-match extcommunity ext-comm-list-number&<1-16>
undo if-match extcommunity [ ext-comm-list-number&<1-16> ]
```

View

Routing policy view

Default level

2: System level

Parameters

ext-comm-list-number: Extended community list number, in the range of 1 to 199.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description

Use **if-match extcommunity** to specify extended community lists for matching against the extended community attribute of BGP routing information.

Use **undo if-match extcommunity** to remove the match criterion.

The match criterion is not configured by default.

Examples

Configure node 10 in **permit** mode of routing policy **policy1** to match BGP routing information to extended community lists 100 and 150.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match extcommunity 100 150
```

if-match interface

Syntax

```
if-match interface { interface-type interface-number }&<1-16>
undo if-match interface [ interface-type interface-number ]&<1-16>
```

View

Routing policy view

Default level

2: System level

Parameters

interface-type interface-number: Specifies an interface by its type and number

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description

Use **if-match interface** to specify interfaces for matching against the outbound interface of routing information.

Use **undo if-match interface** to remove the match criterion.

The match criterion is not configured by default.

BGP does not support criteria for matching against the outbound interface of routing information.

Examples

Configure node 10 in **permit** mode of routing policy **policy1** to permit routing information with the outbound interface as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match interface vlan-interface 1
```

if-match route-type

Syntax

if-match route-type { **external-type1** | **external-type1or2** | **external-type2** | **internal** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2** } *

undo if-match route-type [**external-type1** | **external-type1or2** | **external-type2** | **internal** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2**] *

View

Routing policy view

Default level

2: System level

Parameters

external-type1: OSPF Type 1 external routes.

external-type1or2: OSPF Type 1 or 2 external routes.

external-type2: OSPF Type 2 external routes.

internal: Internal routes (OSPF intra-area and inter-area routes).

is-is-level-1: IS-IS Level-1 routes.

is-is-level-2: IS-IS Level-2 routes.

nssa-external-type1: OSPF NSSA Type 1 external routes.

nssa-external-type1or2: OSPF NSSA Type 1 or 2 external routes.

nssa-external-type2: OSPF NSSA Type 2 external routes.

Description

Use **if-match route-type** to configure a route type match criterion.

Use **undo if-match route-type** to remove the match criterion.

The match criterion is not configured by default.

Examples

Configure node 10 in **permit** mode of routing policy **policy1** to match OSPF internal routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type internal
```

if-match tag

Syntax

if-match tag *value*

undo if-match tag

View

Routing policy view

Default level

2: System level

Parameters

value: Specifies a tag from 0 to 4294967295.

Description

Use **if-match tag** to match routing information having the specified tag.

Use **undo if-match tag** to remove the match criterion.

The match criterion is not configured by default.

Examples

Configure node 10 in **permit** mode of routing policy **policy1** to permit RIP, OSPF and IS-IS routing information with a tag of 8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
```

ip as-path

Syntax

ip as-path *as-path-number* { **deny** | **permit** } *regular-expression*

undo ip as-path *as-path-number*

View

System view

Default level

2: System level

Parameters

as-path-number: AS path list number, in the range of 1 to 256.

deny: Specifies the match mode for the AS path list as **deny**.

permit: Specifies the match mode for the AS path list as **permit**.

regular-expression: AS_PATH regular expression, a string of 1 to 50 characters.

BGP routing updates contain the AS_PATH attribute field that identifies the autonomous systems through which the routing information has passed. An AS-PATH regular expression, for example, `^200.*100$`, matches the AS path attribute that starts with AS 200 and ends with AS 100. For the meanings of special characters used in regular expressions, see *Fundamentals Configuration Guide*.

Description

Use **ip as-path** to create an AS path list.

Use **undo ip as-path** to remove an AS path list.

No AS path list is created by default.

Examples

```
# Create AS path list 1, permitting routing information whose AS_PATH attribute starts with 10.
<Sysname> system-view
[Sysname] ip as-path 1 permit ^10
```

ip community-list

Syntax

```
ip community-list { basic-comm-list-num | basic comm-list-name } { deny | permit }
[ community-number-list ] [ internet | no-advertise | no-export | no-export-subconfed ] *
```

```
undo ip community-list { basic-comm-list-num | basic comm-list-name } [ deny | permit ]
[ community-number-list ] [ internet | no-advertise | no-export | no-export-subconfed ] *
```

```
ip community-list { adv-comm-list-num | advanced comm-list-name } { deny | permit } regular-expression
```

```
undo ip community-list { adv-comm-list-num | advanced comm-list-name } [ deny | permit ]
[ regular-expression ]
```

View

System view

Default level

2: System level

Parameters

basic-comm-list-num: Basic community list number, in the range of 1 to 99.

basic: Specifies a basic communist list name.

advanced: Specifies an advanced communist list name.

comm-list-name: Community list name, a string of 1 to 31 characters, which can contain letters, numbers, and signs.

adv-comm-list-num: Advanced community list number, in the range of 100 to 199.

regular-expression: Regular expression of advanced community attribute, a string of 1 to 50 characters. For more information about regular expressions, see *Fundamentals Configuration Guide*.

deny: Specifies the match mode for the community list as **deny**.

permit: Specifies the match mode for the community list as **permit**.

community-number-list: Community number list, which is in the *community number* or *aa:nn* format; a *community number* is in the range of 1 to 4294967295; *aa* and *nn* are in the range of 0 to 65535. Up to 16 community numbers can be entered.

internet: Routes with this attribute can be advertised to all BGP peers. By default, all routes have this attribute.

no-advertise: Routes with this attribute cannot be advertised to other BGP peers.

no-export: Routes with this attribute cannot be advertised out of the local AS, or the confederation but can be advertised to other ASs in the confederation.

no-export-subconfed: Routes with this attribute cannot be advertised out of the local AS, or to other sub ASs in the confederation.

Description

Use **ip community-list** to define a community list entry.

Use **undo ip community-list** to remove a community list or entry.

No community list is defined by default.

Examples

```
# Define basic community list 1 to permit routing information with the INTERNET community attribute.
```

```
<Sysname> system-view
[Sysname] ip community-list 1 permit internet
```

```
# Define advanced community list 100 to permit routing information with the COMMUNITY attribute starting with 10.
```

```
<Sysname> system-view
[Sysname] ip community-list 100 permit ^10
```

ip extcommunity-list

Syntax

```
ip extcommunity-list ext-comm-list-number { deny | permit } { rt route-target }&<1-16>
```

```
undo ip extcommunity-list ext-comm-list-number
```

View

System view

Default level

2: System level

Parameters

ext-comm-list-number: Extended community list number, in the range of 1 to 199.

deny: Specifies the match mode for the extended community list as **deny**.

permit: Specifies the match mode for the extended community list as **permit**.

soo *site-of-origin*: Sets the SOO extended community attribute, a string of 3 to 21 characters.

A *route-target* has three forms:

- A 16-bit AS number: a 32-bit self-defined number, for example, 101:3;
- A 32-bit IP address: a 16-bit self-defined number, for example, 192.168.122.15:1.
- A 32-bit AS number: 16-bit self-defined number, for example, 70000:3. The AS number should be no less than 65536.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description

Use **ip extcommunity-list** to define an extended community list entry.

Use **undo ip extcommunity-list** to remove an extended community list.

No extended community list is defined by default.

Examples

```
# Define extended community list 1 to permit routing information with RT 200:200.
<Sysname> system-view
[Sysname] ip extcommunity-list 1 permit rt 200:200

# Define extended community list 2 to permit routing information with SOO 100:100.
<Sysname> system-view
[Sysname] ip extcommunity-list 2 permit soo 100:100
```

route-policy

Syntax

route-policy *route-policy-name* { **deny** | **permit** } **node** *node-number*

undo route-policy *route-policy-name* [**deny** | **permit**] [**node** *node-number*]

View

System view

Default level

2: System level

Parameters

route-policy-name: Routing policy name, a case-sensitive string of 1 to 63 characters.

deny: Specifies the match mode of the routing policy node as **deny**. If a route satisfies all the if-match clauses of the node, it cannot pass the node and will not go to the next node.

permit: Specifies the match mode of the routing policy node as **permit**. If a route satisfies all the if-match clauses of the node, it passes the node and then is executed with the apply clauses of the node. If not, it goes to the next node of the routing policy.

node *node-number*: Node number, in the range of 0 to 65535. A node with a smaller number is matched first.

Description

Use **route-policy** to create a routing policy and a node of it and enter routing policy view.

Use **undo route-policy** to remove a routing policy or a node of it.

No routing policy is created by default.

A routing policy is used for filtering routing information. It contains several nodes and each node comprises a set of if-match and apply clauses. The if-match clauses define the matching criteria of the node and the apply clauses define the actions to be taken on packets passing the node. The relation between the if-match clauses of a node is logic AND; all the if-match clauses must be satisfied. The relation between different routing policy nodes is logic OR; a packet passing a node passes the routing policy.

Examples

```
# Configure node 10 in permit mode of routing policy policy1 and enter routing policy view.  
<Sysname> system-view  
[Sysname] route-policy policy1 permit node 10  
[Sysname-route-policy]
```

IPv4 routing policy configuration commands

apply fast-reroute

Syntax

```
apply fast-reroute { backup-interface interface-type interface-number [ backup-nexthop ip-address ] }  
undo apply fast-reroute
```

View

Routing policy view

Default level

2: System level

Parameters

backup-interface *interface-type interface-number*: Specifies a backup outbound interface by its type and number. If the specified backup outbound interface is a non-P2P interface (including NBMA and broadcast interfaces, such as an Ethernet interface, or VLAN interface), you need to specify a backup next hop at the same time.

backup-nexthop *ip-address*: Backup next hop address.

Description

Use **apply fast-reroute** to configure FRR.

Use **undo apply fast-reroute** to remove the configuration.

By default, FRR is not configured.

When a link or a router in the network fails, the packets on the path may be discarded, or a routing loop may occur. Then, the traffic will be interrupted until the routing protocol completes routing convergence based on the new network topology.

With FRR, a routing protocol can designate a backup next hop by using the referenced routing policy when a network failure is detected, and packets are directed to the backup next hop to reduce traffic recovery time.

This command allows you to specify a backup next hop in a routing policy for routes matching specified criteria.

Examples

Create a routing policy named **policy1**, and specify backup outbound interface VLAN-interface 1 and backup next hop 193.1.1.8 in the routing policy for packets destined to 100.1.1.0/24.

```
<Sysname> system-view
[Sysname] ip ip-prefix abc index 10 permit 100.1.1.0 24
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match ip-prefix abc
[Sysname-route-policy] apply fast-reroute backup-interface vlan-interface 1
backup-nexthop 193.1.1.8
```

apply ip-address next-hop

Syntax

apply ip-address next-hop *ip-address*

undo apply ip-address next-hop

View

Routing policy view

Default level

2: System level

Parameters

ip-address: IP address of the next hop.

Description

Use **apply ip-address next-hop** to set a next hop for IPv4 routing information.

Use **undo apply ip-address next-hop** to remove the clause configuration.

No next hop is set for IPv4 routing information by default.

This command cannot set a next hop for redistributed routes.

Examples

Configure node 10 in **permit** mode of routing policy **policy1** to set next hop 193.1.1.8 for routes matching AS path list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply ip-address next-hop 193.1.1.8
```

display ip ip-prefix

Syntax

display ip ip-prefix [*ip-prefix-name*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip-prefix-name: IP prefix list name, a string of 1 to 19 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip ip-prefix** to display the statistics of an IPv4 prefix list. If no *ip-prefix-name* is specified, statistics for all IPv4 prefix lists will be displayed.

Related commands: **ip ip-prefix**.

Examples

```
# Display the statistics of IPv4 prefix list abc.
```

```
<Sysname> display ip ip-prefix abc
```

```
Prefix-list abc
```

```
Permitted 0
```

```
Denied 0
```

```
index: 10
```

```
permit 1.0.0.0/11
```

```
ge 22 le 32
```

Table 95 Command output.

Field	Description
Prefix-list	Name of the IPv4 prefix list
Permitted	Number of routes satisfying the match criterion
Denied	Number of routes not satisfying the match criterion
index	Index of the IPv4 prefix list
permit	Match mode: permit or deny
1.0.0.0/11	IP address and mask
ge	greater-equal, the lower limit
le	less-equal, the higher limit

if-match acl

Syntax

```
if-match acl acl-number
```

```
undo if-match acl
```

View

Routing policy view

Default level

2: System level

Parameters

acl-number: ACL number from 2000 to 3999.

Description

Use **if-match acl** to configure an ACL match criterion.

Use **undo if-match acl** to remove the match criterion.

No ACL match criterion is configured by default.

Examples

```
# Configure node 10 of routing policy policy1 to permit routes matching ACL 2000.
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match acl 2000
```

if-match ip

Syntax

```
if-match ip { next-hop | route-source } { acl acl-number | ip-prefix ip-prefix-name }
undo if-match ip { next-hop | route-source } [ acl | ip-prefix ]
```

View

Routing policy view

Default level

2: System level

Parameters

next-hop: Matches the next hop of routing information to the filter.

route-source: Matches the source address of routing information to the filter.

acl *acl-number*: Matches an ACL with a number from 2000 to 2999.

ip-prefix *ip-prefix-name*: Matches an IP prefix list with a name being a string of 1 to 19 characters.

Description

Use **if-match ip** to configure a next hop or source address match criterion for IPv4 routes.

Use **undo if-match ip** to remove the match criterion.

The match criterion is not configured by default.

Examples

```
# Configure node 10 of routing policy policy1 to permit routing information whose next hop address
matches IP prefix list p1.
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match ip next-hop ip-prefix p1
```

if-match ip-prefix

Syntax

if-match ip-prefix *ip-prefix-name*

undo if-match ip-prefix

View

Routing policy view

Default level

2: System level

Parameters

ip-prefix-name: Matches an IP prefix list with a name being a string of 1 to 19 characters.

Description

Use **if-match ip-prefix** to configure an IP prefix list based match criterion.

Use **undo if-match ip-prefix** to remove the match criterion.

No IP prefix list based match criterion is configured by default.

Examples

Configure node 10 of routing policy **policy2** to permit routes whose destination address matches IP prefix list **p1**.

```
<Sysname> system-view
[Sysname] route-policy policy2 permit node 10
[Sysname-route-policy] if-match ip-prefix p1
```

ip ip-prefix

Syntax

ip ip-prefix *ip-prefix-name* [**index** *index-number*] { **deny** | **permit** } *ip-address mask-length*
[**greater-equal** *min-mask-length*] [**less-equal** *max-mask-length*]

undo ip ip-prefix *ip-prefix-name* [**index** *index-number*]

View

System view

Default level

2: System level

Parameters

ip-prefix-name: IPv4 prefix list name, a string of 1 to 19 characters.

index-number: Index number, in the range of 1 to 65535, for uniquely specifying an item of the IPv4 prefix list. An index with a smaller number is matched first.

deny: Specifies the match mode for the IPv4 prefix list as **deny**. If a route matches the IPv4 prefix list, the route neither passes the filter nor matches against the next item; if not, the route matches against the next item (suppose the IPv4 prefix list has multiple items configured).

permit: Specifies the match mode for the IPv4 prefix list as **permit**. If a route matches the IPv4 prefix list, it passes the IPv4 prefix list. If not, it matches against the next item (suppose the IPv4 prefix list has multiple items configured).

ip-address mask-length: Specifies an IPv4 prefix and mask length. The *mask-length* is in the range of 0 to 32.

min-mask-length, max-mask-length: Specifies the prefix range. **greater-equal** means "greater than or equal to" and **less-equal** means "less than or equal to". The range relation is $mask-length \leq min-mask-length \leq max-mask-length \leq 32$. If only the *min-mask-length* is specified, the prefix length range is $[min-mask-length, 32]$. If only the *max-mask-length* is specified, the prefix length range is $[mask-length, max-mask-length]$. If both *min-mask-length* and *max-mask-length* are specified, the prefix length range is $[min-mask-length, max-mask-length]$.

Description

Use **ip ip-prefix** to configure an IPv4 prefix list or an item of it.

Use **undo ip ip-prefix** to remove an IPv4 prefix list or an item of it.

No IPv4 prefix list is configured by default.

An IPv4 prefix list is used to filter IPv4 addresses. It may have multiple items, each of which specifies a range of IPv4 prefixes. The relation between the items is logic OR. If an item is passed, the IPv4 prefix list is passed. If no item is passed, the IP prefix list cannot be passed.

The IP prefix range is determined by *mask-length* and $[min-mask-length, max-mask-length]$. If both *mask-length* and $[min-mask-length, max-mask-length]$ are specified, the IP address must satisfy both of them.

If both *ip-address* and *mask-length* are specified as 0.0.0.0 0, only the default route will be matched.

To match all routes, use 0.0.0.0 0 **less-equal** 32.

Examples

```
# Define IP prefix list p1 to permit routes matching network 10.0.192.0/8 and with mask length 17 or 18.
```

```
<Sysname> system-view
```

```
[Sysname] ip ip-prefix p1 permit 10.0.192.0 8 greater-equal 17 less-equal 18
```

reset ip ip-prefix

Syntax

```
reset ip ip-prefix [ ip-prefix-name ]
```

View

User view

Default level

2: System level

Parameters

ip-prefix-name: IP prefix list name, a string of 1 to 19 characters.

Description

Use **reset ip ip-prefix** to clear the statistics of a specified IPv4 prefix list. If no *ip-prefix-name* is specified, the statistics of all IPv4 prefix lists will be cleared.

Examples

```
# Clear the statistics of IPv4 prefix list abc.
<Sysname> reset ip ip-prefix abc
```

IPv6 routing policy configuration commands

apply ipv6 next-hop

Syntax

```
apply ipv6 next-hop ipv6-address
undo apply ipv6 next-hop
```

View

Routing policy view

Default level

2: System level

Parameters

ipv6-address: Next hop IPv6 address.

Description

Use **apply ipv6 next-hop** to configure a next hop for IPv6 routes.

Use **undo apply ipv6 next-hop** to remove the clause configuration.

No next hop address is configured for IPv6 routing information by default.

This command cannot set a next hop for redistributed routes.

Examples

```
# Configure node 10 of routing policy policy1 to configure next hop 3ffe:506::1 for IPv6 routing
information matching AS path list 1.
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply ipv6 next-hop 3ffe:506::1
```

display ip ipv6-prefix

Syntax

```
display ip ipv6-prefix [ ipv6-prefix-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-prefix-name: IPv6 prefix list name, a string of 1 to 19 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip ipv6-prefix** to display the statistics of the specified IPv6 prefix list. If no IPv6 prefix list is specified, the statistics of all IPv6 prefix lists will be displayed.

Examples

```
# Display the statistics of all IPv6 prefix lists.
```

```
<Sysname> display ip ipv6-prefix
```

```
Prefix-list6 abc
```

```
Permitted 0
```

```
Denied 0
```

```
    index:    10                permit  ::/0
```

```
    index:    20                permit  ::/1                ge 1    le 128
```

Table 96 Command output

Field	Description
Prefix-list6	Name of the IPv6 prefix list
Permitted	Number of routes satisfying the match criterion
Denied	Number of routes not satisfying the match criterion
Index	Index number of the prefix list
Permit	Match mode of the item: permit or deny
::/1	IPv6 address and prefix length for matching
ge	greater-equal, the lower prefix length
le	less-equal, the upper prefix length

if-match ipv6

Syntax

```
if-match ipv6 { address | next-hop | route-source } { acl acl6-number | prefix-list ipv6-prefix-name }
```

```
undo if-match ipv6 { address | next-hop | route-source } [ acl | prefix-list ]
```

View

Routing policy view

Default level

2: System level

Parameters

address: Matches the destination address of IPv6 routing information.

next-hop: Matches the next hop of IPv6 routing information.

route-source: Matches the source address of IPv6 routing information.

acl *acl6-number*: Specifies the number of an IPv6 ACL for filtering, in the range of 2000 to 3999 for **address**, and 2000 to 2999 for **next-hop** and **route-source**.

prefix-list *ipv6-prefix-name*: Specifies the name of a IPv6 prefix list for filtering, a string of 1 to 19 characters.

Description

Use **if-match ipv6** to configure a destination, next hop or source address based match criterion for IPv6 routes.

Use **undo if-match ipv6** to remove the match criterion.

The match criterion is not configured by default.

Examples

```
# Configure node 10 of routing policy policy1 to permit routing information whose next hop address matches IPv6 prefix list p1.
```

```
<Sysname> system-view
```

```
[Sysname] route-policy policy1 permit node 10
```

```
[Sysname-route-policy] if-match ipv6 next-hop prefix-list p1
```

ip ipv6-prefix

Syntax

```
ip ipv6-prefix ipv6-prefix-name [ index index-number ] { deny | permit } ipv6-address prefix-length [ greater-equal min-prefix-length ] [ less-equal max-prefix-length ]
```

```
undo ip ipv6-prefix ipv6-prefix-name [ index index-number ]
```

View

System view

Default level

2: System level

Parameters

ipv6-prefix-name: IPv6 prefix list name, a string of 1 to 19 characters, for uniquely specifying an IPv6 prefix list.

index-number: Index number, in the range of 1 to 65535, for uniquely specifying an IPv6 prefix list item. An item with a smaller *index-number* will be matched first.

deny: Specifies the match mode for the IPv6 prefix list as **deny**. If a route matches the IPv6 prefix list, the route neither passes the filter nor matches against the next item; if not, the route matches against the next item (suppose the IPv6 prefix list has multiple items configured).

permit: Specifies the match mode for the IPv6 prefix list as **permit**. If a route matches the IPv6 prefix list, it passes the IPv6 prefix list. If not, it matches against the next item (suppose the IPv6 prefix list has multiple items configured).

ipv6-address prefix-length: Specifies an IPv6 prefix and prefix length. A *prefix-length* is in the range of 0 to 128. When specified as :: 0, the arguments match the default route.

greater-equal *min-prefix-length*: Greater than or equal to the minimum prefix length.

less-equal *max-prefix-length*: Less than or equal to the maximum prefix length.

The length relation is $mask-length \leq min-mask-length \leq max-mask-length \leq 128$. If only the *min-prefix-length* is specified, the prefix length range is [*min-prefix-length*, 128]. If only the *max-prefix-length* is specified, the prefix length range is [*prefix-length*, *max-prefix-length*]. If both the *min-prefix-length* and *max-prefix-length* are specified, the prefix length range is [*min-prefix-length*, *max-prefix-length*].

Description

Use **ip ipv6-prefix** to configure an IPv6 prefix list or an item of it.

Use **undo ip ipv6-prefix** to remove an IPv6 prefix list or an item.

No IPv6 prefix list is configured by default.

An IPv6 prefix list may have multiple items, and each of them specifies a range of IPv6 prefixes. The relation between items is logic OR. If a route passes an item of it, the route will pass the IPv6 prefix list.

The IPv6 prefix range is determined by *prefix-length* and [*min-prefix-length*, *max-prefix-length*]. If both *mask-length* and [*min-mask-length*, *max-mask-length*] are specified, then the IPv6 addresses must satisfy both of them.

If *ipv6-address prefix-length* is specified as :: 0, only the default route matches.

To match all routes, configure :: 0 **less-equal** 128.

Examples

```
# Permit IPv6 addresses with a mask length between 32 bits and 64 bits.
```

```
<Sysname> system-view
```

```
[Sysname] ip ipv6-prefix abc permit :: 0 greater-equal 32 less-equal 64
```

```
# Deny IPv6 addresses with the prefix being 3FFE:D00::/32, and prefix length being greater than or equal to 32 bits.
```

```
<Sysname> system-view
```

```
[Sysname] ip ipv6-prefix abc deny 3FFE:D00:: 32 less-equal 128
```

reset ip ipv6-prefix

Syntax

```
reset ip ipv6-prefix [ ipv6-prefix-name ]
```

View

User view

Default level

2: System level

Parameters

ipv6-prefix-name: IPv6 prefix list name, a string of 1 to 19 characters.

Description

Use **reset ip ipv6-prefix** to clear the statistics of the specified IPv6 prefix list. If no name is specified, the statistics of all IPv6 prefix lists will be cleared.

Examples

```
# Clear the statistics of IPv6 prefix list abc.
```

```
<Sysname> reset ip ipv6-prefix abc
```

Policy-based routing configuration commands

This chapter describes only PBR commands (using a PBR policy).

For description of PBR commands (using a QoS policy), such as the traffic classification, traffic behavior, and QoS policy configuration commands, see *ACL and QoS Command Reference*.

The A5500 SI Switch Series does not support PBR.

apply ip-address default next-hop

Syntax

```
apply ip-address default next-hop ip-address [ track track-entry-number ] [ ip-address [ track track-entry-number ] ]
```

```
undo apply ip-address default next-hop [ ip-address [ ip-address ] ]
```

View

PBR policy node view

Default level

2: System level

Parameters

ip-address: IP address of the default next hop.

track *track-entry-number*: Specifies a track entry. The *track-entry-number* argument is in the range of 1 to 1024.

Description

Use **apply ip-address default next-hop** to set the default next hop(s).

Use **undo apply ip-address default next-hop** to remove the configuration.

You can specify up to two default next hops in one command line.

Using the **undo apply ip-address default next-hop** command with a next hop specified removes the default next hop. Using this command without any next hop specified removes all default next hops.

The default next hop must belong to the public network instead of a VPN.

Examples

```
# Set the default next hop to 1.1.1.1.  
<Sysname> system-view  
[Sysname] policy-based-route aa permit node 11  
[Sysname-pbr-aa-11] apply ip-address default next-hop 1.1.1.1 track 1
```

apply ip-address next-hop

Syntax

```
apply ip-address next-hop ip-address [ direct ] [ track track-entry-number ] [ ip-address [ direct ] [ track track-entry-number ] ]
```

undo apply ip-address next-hop [*ip-address* [*ip-address*]]

View

PBR policy node view

Default level

2: System level

Parameters

ip-address: IP address of the next hop.

direct: Specifies the current next hop as valid when it is a directly connected next hop.

track *track-entry-number*: Specifies a track entry. The *track-entry-number* argument is in the range of 1 to 1024.

Description

Use **apply ip-address next-hop** to set the next hop(s) for packets.

Use **undo apply ip-address next-hop** to remove the configuration.

You can specify up to two next hops in one command line.

Using the **undo apply ip-address next-hop** command with a next hop specified removes the next hop. Using this command without any next hop specified removes all next hops.

The next hop must belong to the public network instead of a VPN.

Examples

```
# Set the directly connected next hop to 1.1.1.1.  
<Sysname> system-view  
[Sysname] policy-based-route aa permit node 11  
[Sysname-pbr-aa-11] apply ip-address next-hop 1.1.1.1 direct
```

apply ip-precedence

Syntax

apply ip-precedence *value*

undo apply ip-precedence

View

PBR policy node view

Default level

2: System level

Parameters

value: Sets the precedence for IP packets. Eight precedence values (0 to 7) are available. Each precedence value corresponds to a precedence type, as shown in [Table 97](#). You can set either a precedence value or a precedence type for IP packets.

Table 97 IP precedences and the corresponding types

Precedence value	Precedence type
0	routine

Precedence value	Precedence type
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

Description

Use **apply ip-precedence** to set a precedence for packets.

Use **undo apply ip-precedence** to remove the configuration.

Examples

```
# Set the precedence to 5 (critical) for packets.
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply ip-precedence critical
```

display ip policy-based-route

Syntax

```
display ip policy-based-route [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip policy-based-route** to display the PBR routing information.

Examples

```
# Display the PBR routing information.
<Sysname> display ip policy-based-route
Policy Name          interface
pr02                 local
```

```
pr02                Vlan-interface 10
pr01                Vlan-interface 11
```

Table 98 Command output

Field	Description
Policy Name	Policy name
	PBR type.
interface	This field displays local for a local PBR or a specific interface (such as VLAN-interface 10) to which the policy has been applied to implement interface PBR.

display ip policy-based-route setup

Syntax

```
display ip policy-based-route setup { policy-name | interface interface-type interface-number [ slot slot-number ] | local [ slot slot-number ] } [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

policy-name: Displays the PBR routing information of the specified policy. A policy name is a string of 1 to 19 characters.

interface *interface-type interface-number*: Displays the PBR routing information on the specified interface.

local: Displays the local PBR information.

slot *slot-number*: Displays session information for an IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip policy-based-route setup** to display the specified PBR routing information.

Examples

```
# Display the PBR routing information of policy pr01.
<Sysname> display ip policy-based-route setup pr01
  policy Name          interface
pr01                  Vlan-interface11
```

```
# Display the PBR routing information on Vlan-interface11.
<Sysname> display ip policy-based-route setup interface Vlan-interface 11
Interface Vlan-interface11 policy based routing configuration information:
policy-based-route: pr01
  permit node 1
    if-match acl 3101
    apply ip-address next-hop 1.1.1.1

# Display the local PBR routing information.
<Sysname> display ip policy-based-route setup local
Local policy based routing configuration information:
policy-based-route: pr01
  permit node 1:
    if-match acl 3101
    apply ip-address next-hop 1.1.1.1
```

Table 99 Command output

Field	Description
policy Name	Policy name.
interface	Interface where the policy is applied. Local means the policy is applied locally.
Interface Vlan-interface11 policy based routing configuration information	PBR routing information on Vlan-interface 11.
Local policy based routing configuration information	Local PBR information.
policy-based-route	Policy name.
permit node 1	The match mode is permit , and the policy has a node (node 1).
if-match acl 3101	Match packets against ACL 3101.
apply ip-address next-hop 1.1.1.1	The next hop address is 1.1.1.1.

display policy-based-route

Syntax

```
display policy-based-route [ policy-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

policy-name: Displays information about the specified policy. A policy name is a string of 1 to 19 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display policy-based-route** to display PBR policy information.

If no policy name is specified, all PBR policy information is displayed. If a policy name is specified, information about the specified policy is displayed.

Examples

```
# Display the PBR policy information.
<Sysname> display policy-based-route
Policy based routing configuration information:
policy-based-route : aaa
  Node 1 permit :
    apply ip-address next-hop 1.1.1.1
```

Table 100 Command output

Field	Description
policy-based-route : aaa	The policy name is aaa .
Node 1 permit :	The matching mode of node 1 is permit .
apply ip-address next-hop 1.1.1.1	The next hop address is 1.1.1.1.

if-match acl

Syntax

if-match acl *acl-number*

undo if-match acl

View

PBR policy node view

Default level

2: System level

Parameters

acl-number: ACL number, in the range of 2000 to 3999. The number of a basic ACL ranges from 2000 to 2999 and that of an advanced ACL ranges from 3000 to 3999.

Description

Use **if-match acl** to define an ACL match criterion.

Use **undo if-match acl** to remove the ACL match criterion.

Examples

```
# Permit the packets matching ACL 2010.
<Sysname> system-view
```

```
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match acl 2010
```

ip local policy-based-route

Syntax

```
ip local policy-based-route policy-name
undo ip local policy-based-route policy-name
```

View

System view

Default level

2: System level

Parameters

policy-name: Policy name, a string of 1 to 19 characters.

Description

Use **ip local policy-based-route** to configure local PBR based on a specified policy.

Use **undo ip local policy-based-route** to remove the configuration.

No policy is referenced for local PBR by default.

Only one policy can be referenced for local PBR.

Local PBR is used to route packets generated locally. Unless otherwise required, HP does not recommend configuring local PBR.

Examples

```
# Configure local PBR based on policy aaa.
<Sysname> system-view
[Sysname] ip local policy-based-route aaa
```

ip policy-based-route

Syntax

```
ip policy-based-route policy-name
undo ip policy-based-route policy-name
```

View

Interface view

Default level

2: System level

Parameters

policy-name: Policy name, a string of 1 to 19 characters.

Description

Use **ip policy-based-route** to configure PBR on the interface.

Use **undo ip policy-based-route** to remove the configuration.

No policy is referenced for interface PBR by default.

Note that:

- Only one policy can be referenced by an interface for PBR.
- The referenced policy applies to all packets arriving on the interface.

Examples

```
# Configure PBR based on policy aaa on Vlan-interface 11.
<Sysname> system-view
[Sysname] interface Vlan-interface 11
[Sysname-Vlan-interface11] ip policy-based-route aaa
```

policy-based-route

Syntax

```
policy-based-route policy-name [ deny | permit ] node node-number
undo policy-based-route policy-name [ deny | node node-number | permit ]
```

View

System view

Default level

2: System level

Parameters

policy-name: Policy name, a string of 1 to 19 characters.

deny: Specifies the match mode of the policy node as **deny**.

permit: Specifies the match mode of the policy node as **permit**.

node *node-number*: Number of a policy node, in the range of 0 to 65535. A node with a smaller *node-number* has a higher match priority than a node with a greater one.

Description

Use **policy-based-route** to create a policy, policy node, or both, and enter PBR policy node view.

Use **undo policy-based-route** to remove a created policy or policy node.

No policy or policy node is created by default.

The default match mode of a policy node is **permit**.

Examples

```
# Configure the match mode of node 10 of policy 1 as permit, and enter PBR policy node view.
<Sysname> system-view
[Sysname] policy-based-route policy1 permit node 10
[Sysname-pbr-policy1-10]
```

MCE configuration commands

This chapter describes only the commands related to the multi-VPN-instance CE (MCE) feature. For information about the routing protocol configuration commands in the configuration examples, see *Layer 3—IP Routing Command Reference*.

The term "Layer 3 Ethernet interface" refers to route-mode (Layer 3) Ethernet ports. You can set an Ethernet port to operate in route mode by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

The MCE function is available only on the HP 5500 EI Switch Series.

description

Syntax

```
description text  
undo description
```

View

VPN instance view

Default level

2: System level

Parameters

text: Description for the VPN instance, a string of 1 to 80 characters.

Description

Use **description** to configure a description for the current VPN instance.

Use **undo description** to delete the description.

Examples

```
# Configure a description for VPN instance vpn1.  
<Sysname> system-view  
[Sysname] ip vpn-instance vpn1  
[Sysname-vpn-instance-vpn1] description vpn1
```

display bgp vpnv4 vpn-instance group

Syntax

```
display bgp vpnv4 vpn-instance vpn-instance-name group [ group-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance-name: Displays information about the specified VPN. *vpn-instance-name* is the VPN instance name, a case-sensitive string of 1 to 31 characters.

group-name: Name of the BGP peer group, a string of 1 to 47 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp vpnv4 vpn-instance group** to display information about a specific BGP VPNv4 peer group or all BGP VPNv4 peer groups.

Examples

Display information about the BGP VPNv4 peer group **a** for VPN instance **vpn1**.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 group a
BGP peer-group is a
remote AS number not specified
Type : external
Maximum allowed prefix number: 150000
Threshold: 75%
Configured hold timer value: 180
Keepalive timer value: 60
Minimum time between advertisement runs is 30 seconds
Optional capabilities:
  ORF advertise capability based on Prefix(type 64):
    Local : both
Peer Preferred Value: 99
No routing policy is configured
Members:
Peer          AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
10.1.1.1     200   18       21       0     1       00:12:58 Established
```

Table 101 Command output

Field	Description
BGP peer-group	Name of the BGP peer group
remote AS number	Number of the remote AS
Type	Peer group type
Maximum allowed prefix number	Maximum number of routes that the VPN instance supports
Threshold	Threshold value
Configured hold timer value	Setting of the hold timer
Keepalive timer value	Keepalive interval

Field	Description
Minimum time between advertisement runs	Minimum route advertisement interval
Local	Indicates whether the local device supports sending and receiving Route-refresh packets with ORF information. The value can be: <ul style="list-style-type: none"> • both—Supports sending and receiving Route-refresh messages with ORF information. • Send—Supports sending Route-refresh messages with ORF information. • Receive—Supports receiving Route-refresh messages with ORF information.
Peer Preferred Value	Weight for the routes from the peer
No routing policy is configured	Whether the VPN instance is configured with a routing policy
Peer	IP address of the peer
AS	AS number of the peer group
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages waiting to be sent to the peer
PrefRcv	Number of prefixes received
Up/Down	Duration of the BGP session in the current state
State	Status of the peer

display bgp vpnv4 vpn-instance network

Syntax

```
display bgp vpnv4 vpn-instance vpn-instance-name network [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance-name: Displays information about the specified VPN. *vpn-instance-name* is the VPN instance name, a case-sensitive string of 1 to 31 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp vpnv4 vpn-instance network** to display information about the BGP VPNv4 routes injected into a specific VPN instance or all VPN instances.

Examples

Display information about the BGP VPNv4 routes injected into the VPN instance **vpn1**.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 network
  BGP Local Router ID is 1.1.1.1.
  Local AS Number is 100.
  Network           Mask           Route-policy       Short-cut
  10.0.0.0          255.0.0.0
```

Table 102 Command output

Field	Description
BGP Local Router ID	Router ID of the local BGP router
Local AS Number	Local AS number
Network	Advertised network route
Mask	Mask of the advertised network route
Route-policy	Routing policy configured
Short-cut	Whether this route is a short-cut route

display bgp vpnv4 vpn-instance paths

Syntax

```
display bgp vpnv4 vpn-instance vpn-instance-name paths [ as-regular-expression | { | { begin | exclude | include } regular-expression } ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance-name: Displays information about the specified VPN. *vpn-instance-name* is the VPN instance name, a case-sensitive string of 1 to 31 characters.

as-regular-expression: Regular expression for filtering the AS path information to be displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp vpnv4 vpn-instance paths** to display the BGP VPNv4 AS path information.

Examples

Display the BGP VPNv4 AS path information of VPN instance **vpn1**.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 paths
  Address      Hash    Refcount  MED      Path/Origin
  0x6E72D18    0       1         0        200?
  0x6E72E50    0       1         0        i
  0x6E72B78    1       1         0        ?
  0x6E72BE0    1       2         0        ?
```

Table 103 Command output

Field	Description
Address	Routing address in the local database
Hash	Hash bucket for storing routes
Refcount	Number of times that the path is referenced
MED	Metric for routes
Path/Origin	AS_PATH attribute/Route origin code

display bgp vpnv4 vpn-instance peer

Syntax

```
display bgp vpnv4 vpn-instance vpn-instance-name peer [ group-name log-info | ip-address { log-info | verbose } | verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance-name: Displays information about the specified VPN. *vpn-instance-name* is the VPN instance name, a case-sensitive string of 1 to 31 characters.

group-name: Name of a peer group, a string of 1 to 47 characters.

log-info: Displays the log information about the peer group.

ip-address: IP address of the peer.

verbose: Displays detailed information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp vpnv4 vpn-instance peer** to display information about the BGP VPNv4 peers.

Examples

Display information about the BGP VPNv4 peers of the VPN instance **vpn1**.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 peer
BGP local router ID : 2.2.2.2
Local AS number : 100
Total number of peers : 1                Peers in established state : 1

Peer          AS      MsgRcvd  MsgSent  OutQ    PrefRcv  Up/Down    State
10.1.1.1     200    24       29       0       1        00:18:47  Established
```

Table 104 Command output

Field	Description
BGP Local router ID	Router ID of the local BGP router
local AS number	Local AS number
Total number of peers	Total number of peers
Peers in established state	Number of peers in the state of established
Peer	IP address of the peer
AS	AS number of the peer group
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages waiting to be sent to the peer
PrefRcv	Number of received prefixes
Up/Down	Duration of the BGP session in the current state
State	Status of the peer

Display detailed information about BGP VPNv4 peers of VPN instance **vpn1**.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 peer verbose
Peer: 10.1.1.1 Local: 2.2.2.2
Type: EBGP link
BGP version 4, remote router ID 10.1.1.1
BGP current state: Established, Up for 00h19m26s
BGP current event: KATimerExpired
BGP last state: OpenConfirm
Port: Local - 179 Remote - 1025
Configured: Active Hold Time: 180 sec Keepalive Time:60 sec
Received : Active Hold Time: 180 sec
Negotiated: Active Hold Time: 180 sec
Peer optional capabilities:
Peer support bgp multi-protocol extended
Peer support bgp route refresh capability
```

Address family IPv4 Unicast: advertised and received

Received: Total 25 messages, Update messages 1
Sent: Total 30 messages, Update messages 4
Maximum allowed prefix number: 150000
Threshold: 75%
Minimum time between advertisement runs is 30 seconds
Optional capabilities:
 ORF advertise capability based on Prefix(type 64):
 Local: both
 Negotiated: send
Peer Preferred Value: 99
BFD: Enabled

Routing policy configured:
No routing policy is configured

Table 105 Command output

Field	Description
Peer	IP address of the peer
Local	IP address of the local router
Type	BGP type
BGP version	Version of BGP that the peer runs
remote router ID	Router ID of the remote router
BGP current state	Current status of the BGP session
Up for	Duration since the peer is established
BGP current event	Current event of the BGP session
BGP last state	State that the BGP session was in before transitioning to the current status
Port	Local and remote ports of the BGP session
Configured	Settings of the local timers, including the active hold interval and keepalive interval
Received	Received active hold interval
Negotiated	Negotiated active hold interval and keepalive time
Peer optional capabilities	Optional capabilities of the peer
Peer support bgp multi-protocol extended	The peer supports multiprotocol extension.
Peer support bgp route refresh capability	The peer supports route refresh capability.
Address family IPv4 Unicast	IPv4 unicast family capability
Received	Total number of received messages and the number of received update messages

Field	Description
Sent	Total number of sent messages and the number of sent update messages
Maximum allowed prefix number	Maximum number of routes that the VPN instance supports
Threshold	Threshold value
Minimum time between advertisement runs	Minimum route advertisement interval
Optional capabilities	Local optional capabilities
Local	Indicates whether the local device supports sending and receiving Route-refresh packets with the ORF information. The value can be: <ul style="list-style-type: none"> both—Supports sending and receiving Route-refresh messages with the ORF information. send—Supports sending Route-refresh messages with the ORF information. receive—Supports receiving Route-refresh messages with the ORF information.
Negotiated	ORF capability negotiated by the local and remote peers. The value can be: <ul style="list-style-type: none"> send—The local peer can send Route-refresh messages with the ORF information and the remote peer can receive Route-refresh messages with the ORF information. receive—The local peer can receive Route-refresh messages with the ORF information and the remote peer can send Route-refresh messages with the ORF information. <p>If ORF capability negotiation fails, this field will not be displayed.</p>
Peer Preferred Value	Weight for the routes from the peer
Routing policy configured	Routing policy configured

display bgp vpnv4 vpn-instance routing-table

Syntax

```
display bgp vpnv4 vpn-instance vpn-instance-name routing-table [ [ network-address [ { mask | mask-length } [ longer-prefixes ] ] | as-path-acl as-path-acl-number | cidr | community [ aa:nn ]&<1-13> [ no-advertise | no-export | no-export-subconfed ] * [ whole-match ] | community-list { basic-community-list-number [ whole-match ] | adv-community-list-number }&<1-16> | dampened | dampening parameter | different-origin-as | flap-info [ network-address [ { mask | mask-length } [ longer-match ] ] ] | as-path-acl as-path-acl-number ] | peer ip-address { advertised-routes | received-routes } | statistic ] [ | { begin | exclude | include } regular-expression ] | [ flap-info ] regular-expression as-regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance-name: The VPN instance name, a case-sensitive string of 1 to 31 characters.

network-address: IP address of the destination segment.

mask-length: Length of the network mask, in the range of 0 to 32.

mask-address: Network mask, in the format of X.X.X.X.

longer-prefixes: Specifies to match the longest prefix.

as-path-acl *as-path-acl-number*: Filters routing information using the specified AS_PATH list. The *as-path-acl-number* argument ranges from 1 to 256.

cidr: Displays classless interdomain routing (CIDR) information.

community: Displays routing information of the specified BGP community in the routing table.

aa:nn<1-13>: Community number. Both the *aa* and *nn* parameters range from 0 to 65535. <1-13> means that you can enter the parameter combination up to 13 times.

no-export-subconfed: A route with this attribute is neither advertised out of the local AS, nor advertised to the other sub-ASs in the confederation.

no-advertise: A route with this attribute is not advertised to any other BGP peer.

no-export: A route with this attribute is not advertised out of the local AS or, if existing, confederation. However, it is advertised to the other sub-ASs in the confederation.

whole-match: Performs exact match.

community-list: Displays routing information of the specified BGP community list.

basic-community-list-number: Basic community list number, in the range of 1 to 99.

adv-community-list-number: Advanced community list number, in the range of 100 to 199.

<1-16>: Specifies that the argument before it can be entered up to 16 times.

dampened: Displays information about dampened BGP VPNv4 routes.

dampening parameter: Configured BGP VPNv4 route dampening parameters.

different-origin-as: Displays information about routes with different AS origins.

flap-info: Displays BGP VPNv4 route flap statistics.

longer-match: Displays flap statistics for routes with greater mask lengths than that specified by the *network-address { mask | mask-length }* combination.

peer *ip-address*: Specifies a peer by its IP address.

advertised-routes: Displays routing information sent to the specified peer.

received-routes: Displays routing information received from the specified peer.

regular-expression *as-regular-expression*: Displays routing information matching the specified AS regular expression.

statistic: Displays BGP VPNv4 route statistics.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp vpnv4 vpn-instance routing-table** to display the BGP VPNv4 routing information for a specific VPN instance.

Examples

Display the BGP VPNv4 routing information of VPN instance **vpn1**.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 routing-table
```

```
Total Number of Routes: 5

BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

Network          NextHop      MED        LocPrf    PrefVal  Path/Ogn
* > i 10.0.0.0    1.1.1.1     0          100       0        i
* > 10.1.1.0/24  0.0.0.0     0          0         0        ?
* > 20.0.0.0     10.1.1.1    0          0         99       200?
* > i 123.1.1.1/32 1.1.1.1     0          100       0        ?
* > 124.1.1.1/32 0.0.0.0     0          0         0        ?
```

Table 106 Command output

Field	Description
Total Number of Routes	Total number of routes
BGP Local router ID	Router ID of the local BGP router
Status codes	Route status code. For valid values.
Origin	Route origin code. For valid values.
Network	Network address in the BGP routing table
NextHop	Address of the next hop
MED	Metric associated with the destination network
LocPrf	Local preference
PrefVal	Preferred value of the protocol
Path/Ogn	AS_PATH attribute/Route origin code.

display fib vpn-instance

Syntax

```
display fib vpn-instance vpn-instance-name [ acl acl-number | ip-prefix ip-prefix-name ] [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance-name: The VPN instance name, a case-sensitive string of 1 to 31 characters.

acl *acl-number*: Displays the FIB information of the VPN instance permitted by the specified ACL. *acl-number* is the number of the ACL, in the range of 2000 to 2999. If the specified ACL does not exist, the command displays all FIB information of the VPN instance.

ip-prefix *ip-prefix-name*: Displays the FIB information of the VPN instance permitted by the specified IP prefix. *ip-prefix-name* is the name of the IP prefix, a case-sensitive string of 1 to 19 characters. If the specified IP prefix does not exist, the command displays all FIB information of the VPN instance.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display fib vpn-instance** to display FIB information for a VPN.

If no parameter is specified, all FIB information for the VPN will be displayed.

Examples

Display all FIB information for the VPN instance **vpn1**.

```
<Sysname> display fib vpn-instance vpn1
Destination count: 2    FIB entry count: 2
```

Flag:

U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static
R:Relay

Destination/Mask	Nexthop	Flag	OutInterface	InnerLabel	Token
10.2.0.0/16	10.2.1.1	U	Vlan1	Null	Invalid
10.2.1.1/32	127.0.0.1	UH	InLoop0	Null	Invalid
127.0.0.0/8	127.0.0.1	U	InLoop0	Null	Invalid
127.0.0.1/32	127.0.0.1	UH	InLoop0	Null	Invalid

Display the FIB information that begins with the line containing the string 127 for the VPN instance **vpn1**.

```
<Sysname> display fib vpn-instance vpn1 | begin 127
10.2.1.1/32      127.0.0.1  UH      InLoop0      Null         Invalid
127.0.0.0/8     127.0.0.1  U       InLoop0      Null         Invalid
127.0.0.1/32   127.0.0.1  UH      InLoop0      Null         Invalid
```

Display the FIB information permitted by ACL 2000 for the VPN instance **vpn1**.

```

<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] display fib vpn-instance vpn1 acl 2000
FIB entry count: 2

```

Flag:

U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static

Destination/Mask	Nexthop	Flag	OutInterface	InnerLabel	Token
10.2.0.0/16	10.2.1.1	U	Vlan1	Null	Invalid
10.2.1.1/32	127.0.0.1	UH	InLoop0	Null	Invalid

Display the FIB information permitted by the IP prefix **abc0** for the VPN instance **vpn1**.

```

<Sysname> system-view
[Sysname] ip ip-prefix abc0 permit 10.2.0.0 16
[Sysname] display fib vpn-instance vpn1 ip-prefix abc0
FIB entry count: 1

```

Flag:

U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static

Destination/Mask	Nexthop	Flag	OutInterface	InnerLabel	Token
10.2.0.0/16	10.2.1.1	U	Vlan1	Null	Invalid

Table 107 Command output

Field	Description
FIB entry count	Number of entries in the FIB
Destination/Mask	Destination address/mask length
Nexthop	Address of the next hop
Flag	Flag of the route. Possible values are: <ul style="list-style-type: none"> • U—usable route • G—gateway route • H—host route • B—blackhole route • D—dynamic route • S—static route
OutInterface	Forwarding interface
Token	LSP index number

display fib vpn-instance ip-address

Syntax

```

display fib vpn-instance vpn-instance-name ip-address [ mask | mask-length ] [ | { begin | exclude | include } regular-expression ]

```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance-name: The VPN instance name, a case-sensitive string of 1 to 31 characters.

ip-address: Destination IP address, in dotted decimal format.

mask: Mask of the IP address, in dotted decimal format.

mask-length: Length of the IP address mask, in the range of 0 to 32.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display fib vpn-instance** *ip-address* to display the FIB information that matches the specified destination IP address in the specified VPN.

If neither the *mask* nor the *mask-length* argument is specified, the command displays the FIB information that matches the specified destination IP address and has the longest mask in the specified VPN. Otherwise, the command displays the FIB information that exactly matches the specified destination IP address and mask in the specified VPN.

Examples

Display the FIB information that matches the destination IP address 10.2.1.1 in VPN instance **vpn1**.

```
<Sysname> display fib vpn-instance vpn1 10.2.1.1
```

```
FIB entry count: 1
```

```
Flag:
```

```
U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static
```

Destination/Mask	Nexthop	Flag	OutInterface	InnerLabel	Token
10.2.1.1/32	127.0.0.1	UH	InLoop0	Null	Invalid

For more information about the command output, see [Table 107](#).

display ip vpn-instance

Syntax

```
display ip vpn-instance [ instance-name vpn-instance-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

instance-name *vpn-instance-name*: Displays information about the specified VPN. *vpn-instance-name* is the VPN instance name, a case-sensitive string of 1 to 31 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip vpn-instance** to display information about VPN instances.

If you do not specify any parameter, the command displays brief information about all VPN instances.

Examples

Display information about all VPN instances.

```
<Sysname> display ip vpn-instance
Total VPN-Instances configured : 2

VPN-Instance Name      RD          Create Time
vpn1                    22:1       2008/10/13 09:32:45
vpn2                    33:3       2008/10/13 09:42:59
```

Table 108 Command output

Field	Description
VPN-Instance Name	Name of the VPN instance
RD	RD of the VPN instance
Create Time	Time when the VPN instance was created

Display detailed information about a specific VPN instance.

```
<Sysname> display ip vpn-instance instance-name vpn1
VPN-Instance Name and ID : vpn1, 1
Create time : 2000/04/26 12:03:26
Up time : 0 days, 00 hours, 03 minutes and 30 seconds
Route Distinguisher : 100:1
Export VPN Targets : 100:1
Import VPN Targets : 100:1
Import Route Policy : policy2
Export Route Policy : policy3
Tunnel Policy : policy1
Description : vpn1
Maximum Routes Limit : 600
Threshold Value(%): 30
```

```

IPv6 Export VPN Targets : 100:1
IPv6 Import VPN Targets : 100:1
IPv6 Import Route Policy : policy2
IPv6 Export Route Policy : policy3
IPv6 Tunnel Policy : policy1
IPv6 Maximum Routes Limit : 600
IPv6 Threshold Value(%): 30
Interfaces : Vlan-interface10

```

Table 109 Command output

Field	Description
VPN-Instance Name and ID	Name and ID of the VPN instance
CreateTime	Time when the VPN instance was created
Up time	Duration of the VPN instance
Route Distinguisher	RD of the VPN instance
Export VPN Targets	Export target attribute of the IPv4 VPN
Import VPN Targets	Import target attribute of the IPv4 VPN
Import Route Policy	Import routing policy of the IPv4 VPN
Export Route Policy	Export routing policy of the IPv4 VPN
Tunnel Policy	Tunneling policy of the IPv4 VPN
Maximum Routes Limit	Maximum number of routes of the IPv4 VPN
IPv6 Export VPN Targets	Export target attribute of the IPv6 VPN
IPv6 Import VPN Targets	Import target attribute of the IPv6 VPN
IPv6 Import Route Policy	Import routing policy of the IPv6 VPN
IPv6 Export Route Policy	Export routing policy of the IPv6 VPN
IPv6 Tunnel Policy	Tunneling policy of the IPv6 VPN
IPv6 Maximum Routes Limit	Maximum number of routes of the IPv6 VPN
Interfaces	Interface to which the VPN instance is bound

domain-id

Syntax

domain-id *domain-id* [**secondary**]

undo domain-id [*domain-id*]

View

OSPF view

Default level

2: System level

Parameters

domain-id: OSPF domain ID, which can be in one of the following formats:

- Integer, in the range of 0 to 4294967295. For example, 1.
- Dotted decimal notation. For example, 0.0.0.1.
- Dotted decimal notation:16-bit user-defined number, in the range of 0 to 65535. For example, 0.0.0.1:512.

secondary: Uses the domain ID as secondary. With this keyword not specified, the domain ID configured is primary.

Description

Use **domain-id** to configure an OSPF domain ID.

Use **undo domain-id** to restore the default.

By default, the OSPF domain ID is 0.

With no parameter specified, the **undo domain-id** command deletes the primary domain ID.

Usually, routes injected from PEs are advertised as External-LSAs. However, routes to different destinations in the same OSPF domain must be advertised as Type-3 LSAs. Therefore, using the same domain ID is required for an OSPF domain.

Examples

```
# Configure the OSPF domain ID.
<Sysname> system-view
[Sysname] ospf 100 vpn-instance vpn1
[Sysname-ospf-100] domain-id 234
```

export route-policy

Syntax

export route-policy *route-policy*

undo export route-policy

View

VPN instance view, IPv4 VPN view

Default level

2: System level

Parameters

route-policy: Name of the export routing policy for the VPN instance, a string of 1 to 63 characters.

Description

Use **export route-policy** to apply an export routing policy to a VPN instance.

Use **undo export route-policy** to remove the application.

By default, no policy is applied to filter the routes to be advertised.

You can specify an export routing policy when the VPN route advertisement control provided by the extended community attributes is not enough. An export routing policy may deny routes that are permitted by the export target attribute.

An export routing policy specified in VPN instance view applies to both the IPv4 VPN and the IPv6 VPN.

An export routing policy specified in IPv4 VPN view applies to only the IPv4 VPN.

An export routing policy specified in IPv4 VPN view takes precedence over that specified in VPN instance view. If you specify an export routing policy in IPv4 VPN view and VPN instance view, the IPv4 VPN uses the policy specified in IPv4 VPN view.

Examples

```
# Apply export routing policy poly-1 to VPN instance vpn1.
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] export route-policy poly-1
```

ext-community-type

Syntax

```
ext-community-type { domain-id type-code1 | router-id type-code2 | route-type type-code3 }
undo ext-community-type { domain-id | router-id | route-type }
```

View

OSPF view

Default level

2: System level

Parameters

domain-id *type-code1*: Specifies the type code for the OSPF extended community attribute of Domain ID. Valid values are 0x0005, 0x0105, 0x0205, and 0x8005.

router-id *type-code2*: Specifies the type code for the OSPF extended community attribute of Router ID. Valid values are 0x0107 and 0x8001.

route-type *type-code3*: Specifies the type code for the OSPF extended community attribute of Route Type. Valid values are 0x0306 and 0x8000.

Description

Use **ext-community-type** to configure the type code of an OSPF extended community attribute.

Use **undo ext-community-type** to restore the default.

By default, the type codes for the OSPF extended community attributes of Domain ID, Router ID, and Route Type are 0x0005, 0x0107, and 0x0306 respectively.

Examples

```
# Configure the type codes of OSPF extended community attributes Domain ID, Router ID, and Route Type as 0x8005, 0x8001, and 0x8000 respectively for OSPF process 100.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] ext-communityroute-type domain-id 8005
[Sysname-ospf-100] ext-communityroute-type router-id 8001
[Sysname-ospf-100] ext-communityroute-type route-type 8000
```

filter-policy export

Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name } export [ direct | isis process-id | ospf process-id | rip process-id | static ]  
undo filter-policy export [ direct | isis process-id | ospf process-id | rip process-id | static ]
```

View

BGP-VPN instance view

Default level

2: System level

Parameters

acl-number: IP ACL number, in the range of 2000 to 3999.

ip-prefix-name: IP address prefix list name, a string of 1 to 19 characters.

direct: Filters direct routes to be advertised.

isis process-id: Filters ISIS routes to be advertised that are from a specific ISIS process. The *process-id* argument is in the range of 1 to 65535.

ospf process-id: Filters OSPF routes to be advertised that are from a specific OSPF process. The *process-id* argument is in the range of 1 to 65535.

rip process-id: Filters RIP routes to be advertised that are from a specific RIP process. The *process-id* argument is in the range of 1 to 4294967295.

static: Filters static routes to be advertised.

Description

Use **filter-policy export** to configure BGP to filter all or certain types of routes to be advertised.

Use **undo filter-policy export** to remove the configuration.

If you specify no routing protocol parameters for the **filter-policy export** command, all routes to be advertised will be filtered.

By default, BGP does not filter routes to be advertised.

Only routes that survive the filtering are advertised by BGP.

Examples

```
# Configure BGP to filter the routes to be advertised by using ACL 2555.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv4-family vpn-instance vpn1  
[Sysname-bgp-vpn1] filter-policy 2555 export
```

filter-policy import

Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name } import  
undo filter-policy import
```

View

BGP-VPN instance view

Default level

2: System level

Parameters

acl-number: IP ACL number, in the range of 2000 to 3999.

ip-prefix-name: IP address prefix list name, a string of 1 to 19 characters.

Description

Use **filter-policy import** to configure BGP to filter received routes.

Use **undo filter-policy import** to remove the configuration.

By default, BGP does not filter received routes.

Only routes that survive the filtering are added into the BGP routing table.

Examples

```
# Configure BGP to filter received routes using ACL 2255.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] filter-policy 2255 import
```

import route-policy

Syntax

import route-policy *route-policy*

undo import route-policy

View

VPN instance view, IPv4 VPN view

Default level

2: System level

Parameters

route-policy: Name of the import routing policy for the VPN instance, a string of 1 to 63 characters.

Description

Use **import route-policy** to apply an import routing policy to a VPN instance.

Use **undo import route-policy** to remove the application.

By default, all routes permitted by the import target attribute are accepted.

You can specify an import routing policy when the route redistribution control provided by the extended community attributes is not enough. An import routing policy may deny routes that are permitted by the import target attributes.

An import routing policy specified in VPN instance view applies to both the IPv4 VPN and the IPv6 VPN.

An import routing policy specified in IPv4 VPN view applies to only the IPv4 VPN.

An import routing policy specified in IPv4 VPN view takes precedence over that specified in VPN instance view. If you specify an import routing policy in both IPv4 VPN view and VPN instance view, the IPv4 VPN uses the policy specified in IPv4 VPN view.

Examples

```
# Apply import routing policy poly-1 to VPN instance vpn1.
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] import route-policy poly-1
```

ip binding vpn-instance

Syntax

```
ip binding vpn-instance vpn-instance-name
undo ip binding vpn-instance vpn-instance-name
```

View

VLAN interface view, tunnel interface view, Layer 3 Ethernet interface view

Default level

2: System level

Parameters

vpn-instance-name: Name of the VPN instance to be associated, a case-sensitive string of 1 to 31 characters.

Description

Use **ip binding vpn-instance** to associate an interface with a VPN instance.

Use **undo ip binding vpn-instance** to remove the association.

By default, an interface is associated with no VPN instance; it belongs to the public network.

When configured on an interface, the **ip binding vpn-instance** command clears the IP address of the interface. Therefore, you must reconfigure the IP address of the interface after configuring the command.

Examples

```
# Associate VLAN-interface 1 with the VPN instance vpn1.
<Sysname> system-view
[Sysname] interface Vlan-interface1
[Sysname-Vlan-interface1] ip binding vpn-instance vpn1

# Associate tunnel 1 interface with the VPN instance vpn1.
<Sysname> system-view
[Sysname] interface Tunnel 1
[Sysname-Tunnel1] ip binding vpn-instance vpn2
```

ip vpn-instance

Syntax

```
ip vpn-instance vpn-instance-name
undo ip vpn-instance vpn-instance-name
```

View

System view

Default level

2: System level

Parameters

vpn-instance-name: Name of the VPN instance, a case-insensitive string of 1 to 31 characters.

Description

Use **ip vpn-instance** to create a VPN instance and enter VPN instance view.

Use **undo ip vpn-instance** to delete a VPN instance.

A VPN instance takes effect only after you configure an RD for it.

Related command: **route-distinguisher**.

Examples

```
# Create a VPN instance named vpn1.  
<Sysname> system-view  
[Sysname] ip vpn-instance vpn1  
[Sysname-vpn-instance-vpn1]
```

ipv4-family

Syntax

```
ipv4-family  
undo ipv4-family
```

Views

VPN instance view

Default level

2: System level

Parameters

None

Description

Use **ipv4-family** to enter IPv4 VPN view.

Use **undo ipv4-family** to remove all configurations performed in IPv4 VPN view.

Examples

```
# Enter IPv4 VPN view.  
<Sysname> system-view  
[Sysname] ip vpn-instance vpn1  
[Sysname-vpn-instance-vpn1] ipv4-family  
[Sysname-vpn-ipv4-vpn1]
```


ipv4-family vpn-instance

Syntax

```
ipv4-family vpn-instance vpn-instance-name  
undo ipv4-family vpn-instance vpn-instance-name
```

View

BGP view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Associates a VPN instance with an IPv4 address family and enters BGP VPN instance view. The *vpn-instance-name* argument specifies the VPN instance name, a case-sensitive string of 1 to 31 characters.

Description

Use **ipv4-family vpn-instance** to enter BGP-VPN instance view.

Use **undo ipv4-family vpn-instance** to remove all the configurations performed in the view.

Before entering BGP VPN instance view, make sure the corresponding VPN instance is created.

Examples

```
# Enter BGP-VPN instance view.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname] ipv4-family vpn-instance vpn1  
[Sysname-bgp-vpn1]
```

peer allow-as-loop

Syntax

```
peer { group-name | ip-address } allow-as-loop [ number ]  
undo peer { group-name | ip-address } allow-as-loop
```

View

BGP-VPN instance view

Default level

2: System level

Parameters

group-name: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

number: Maximum number that the local AS number can appear repeatedly in the AS-PATH attribute. It ranges from 1 to 10 and defaults to 1.

Description

Use **peer allow-as-loop** to allow the local AS number to appear in the AS-PATH attribute of a received route and to set the allowed maximum number of repetitions.

Use **undo peer allow-as-loop** to remove the configuration.

Examples

```
# Allow the local AS number to appear repeatedly in the AS-PATH attribute of a route received from peer 1.1.1.1 for up to twice.
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 1.1.1.1 allow-as-loop 2
```

refresh bgp vpn-instance

Syntax

```
refresh bgp vpn-instance vpn-instance-name { ip-address | all | external | group group-name } { export | import }
```

View

User view

Default level

1: Monitor level

Parameters

vpn-instance-name: VPN instance name, a case-sensitive string of 1 to 31 characters.

ip-address: IP address of a peer.

all: Soft resets all BGP VPN instance connections.

external: Soft resets EBGp sessions.

group *group-name*: Soft resets the connections with the specified BGP peer group. The *group-name* argument is a string of 1 to 47 characters.

export: Performs a soft reset in the outbound direction.

import: Performs a soft reset in the inbound direction.

Description

Use **refresh bgp vpn-instance** to soft reset BGP connections in a VPN instance.

Examples

```
# Perform a soft reset of all BGP connections in VPN instance vpn1 in the inbound direction to make new configurations take effect.
<Sysname> refresh bgp vpn-instance vpn1 all import
```

reset bgp vpn-instance

Syntax

```
reset bgp vpn-instance vpn-instance-name { as-number | ip-address | all | external | group group-name }
```

View

User view

Default level

1: Monitor level

Parameters

vpn-instance-name: VPN instance name, a case-sensitive string of 1 to 31 characters.

as-number: AS number, in the range of 1 to 4294967295.

ip-address: IP address of a peer.

group *group-name*: Resets the connections with the specified BGP peer group. The *group-name* argument is a string of 1 to 47 characters.

all: Resets all BGP connections.

external: Resets EBGP sessions.

Description

Use **reset bgp vpn-instance** to reset the BGP connections of a specific VPN instance.

Examples

```
# Reset all BGP connections of VPN instance vpn1.  
<Sysname> reset bgp vpn-instance vpn1 all
```

reset bgp vpn-instance dampening

Syntax

```
reset bgp vpn-instance vpn-instance-name dampening [ network-address [ mask | mask-length ] ]
```

View

User view

Default level

1: Monitor level

Parameters

vpn-instance-name: VPN instance name, a case-sensitive string of 1 to 31 characters.

dampening: Specifies route flap dampening information.

network-address: Network address.

mask: Network mask, in the format of x.x.x.x.

mask-length: Length of the network mask, in the range of 0 to 32.

Description

Use **reset bgp vpn-instance dampening** to clear the route flap dampening information of a VPN instance.

Examples

```
# Clear the route flap dampening information of VPN instance vpn1.  
<Sysname> reset bgp vpn-instance vpn1 dampening
```

reset bgp vpn-instance flap-info

Syntax

reset bgp vpn-instance *vpn-instance-name* *ip-address* **flap-info**

reset bgp vpn-instance *vpn-instance-name* **flap-info** [*ip-address* [*mask* | *mask-length*] | **as-path-acl** *as-path-acl-number* | **regexp** *as-path-regexp*]

View

User view

Default level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

ip-address: IP address of the peer.

mask: Network mask, in the format of x.x.x.x.

mask-length: Length of the network mask, in the range of 0 to 32.

as-path-acl *as-path-acl-number*: Specifies the AS_PATH filtering list. The *as-path-acl-number* argument ranges from 1 to 256.

regexp *as-path-regexp*: Specifies the AS_PATH regular expression.

Description

Use **reset bgp vpn-instance flap-info** to clear the route flap history information about BGP peers of a VPN instance.

Examples

```
# Clear route flap history information about BGP peer 2.2.2.2 of VPN instance vpn1.
```

```
<Sysname> reset bgp vpn-instance vpn1 2.2.2.2 flap-info
```

route-distinguisher

Syntax

route-distinguisher *route-distinguisher*

View

VPN instance view

Default level

2: System level

Parameters

route-distinguisher: Route distinguisher (RD) for the VPN instance, a string of 3 to 21 characters in one of the following formats:

- *16-bit AS number:32-bit user-defined number*. For example, 101:3.
- *32-bit IP address:16-bit user-defined number*. For example, 192.168.122.15:1.
- *32-bit AS number:16-bit user-defined number*, where the minimum value of the AS number is 65536. For example, 65536:1.

Description

Use **route-distinguisher** to configure a route distinguisher (RD) for a VPN instance.

An RD is used to create the routing and forwarding table of a VPN. By prefixing an RD to an IPv4 prefix, you make the VPN IPv4 prefix unique globally.

NOTE:

- No RD is configured by default; you must configure an RD for each VPN instance.
 - A VPN instance takes effect only after you configure an RD for it.
 - Once you configure an RD for a VPN, you cannot remove the association.
 - You cannot change an RD directly; you can only delete the VPN instance, re-create the VPN instance, and then reconfigure a new RD.
-

Examples

```
# Configure the RD of VPN instance vpn1.
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 22:1
```

routing-table limit

Syntax

routing-table limit *number* { *warn-threshold* | **simply-alert** }

undo routing-table limit

View

VPN instance view, IPv4 VPN view

Default level

2: System level

Parameters

number: Maximum number of routes for the VPN instance to support. The maximum number ranges from 1 to 6144 in VPN instance view and from 1 to 12288 in IPv4 VPN view.

warn-threshold: Specifies a threshold for warning, in the range of 1 to 100, in percentages. When the percentage of the number of existing routes to the maximum number of routes supported exceeds the specified threshold, the system gives an alarm message but still allows new routes. If the number of routes in the VPN instance reaches the maximum supported, no more routes are added.

simply-alert: Specifies that when the number of routes exceeds the maximum number of routes supported, the system still accepts routes but generates a system log (Syslog) message.

Description

Use **routing-table limit** to limit the maximum number of routes in a VPN instance, preventing too many routes from being accepted by a PE.

Use **undo routing-table limit** to restore the default.

By default, no limit is configured.

A limit configured in VPN instance view applies to both the IPv4 VPN and the IPv6 VPN.

A limit configured in IPv4 VPN view applies to only the IPv4 VPN.

A limit configured in IPv4 VPN view takes precedence over that configured in VPN instance view. If you configure a limit in both IPv4 VPN view and VPN instance view, the IPv4 VPN uses the limit configured in IPv4 VPN view.

Examples

Specify that VPN instance **vpn1** supports up to 1000 routes and can receive new routes after the number of existing routes exceeds the limit.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 100:1
[Sysname-vpn-instance-vpn1] routing-table limit 1000 simply-alert
```

vpn-instance-capability simple

Syntax

```
vpn-instance-capability simple
undo vpn-instance-capability
```

View

OSPF multi-instance view

Default level

2: System level

Parameters

None

Description

Use **vpn-instance-capability simple** to disable routing loop detection for a VPN OSPF process.

Use **undo vpn-instance-capability** to restore the default.

By default, the loop detection function is enabled for a VPN OSPF process.

Examples

Disable routing loop detecton for the VPN OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100 vpn-instance vpna
[Sysname-ospf-100] vpn-instance-capability simple
```

vpn-target

Syntax

```
vpn-target vpn-target<1-8> [ both | export-extcommunity | import-extcommunity ]
undo vpn-target { all | vpn-target<1-8> [ both | export-extcommunity | import-extcommunity ] }
```

View

VPN instance view, IPv4 VPN view

Default level

2: System level

Parameters

`vpn-target`<1-8>: Adds VPN target extended community attributes to the import VPN target extended community attribute list (Import Target) or export VPN target extended community attribute list (Export Target). <1-8> means that you can add up to eight VPN targets.

A VPN target attribute can be a string of 3 to 21 characters in one of the following formats:

- 16-bit AS number:32-bit user-defined number. For example, 101:3.
- 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1.
- 32-bit AS number:16-bit user-defined number, where the AS number must not be less than 65536. For example, 65536:1.

both: Uses the specified VPN targets as both import targets and export targets. The **both** keyword is also used when you do not specify any of **both**, **export-extcommunity**, and **import-extcommunity**.

export-extcommunity: Uses the specified VPN targets as export targets.

import-extcommunity: Uses the specified VPN targets as import targets.

all: Removes all VPN targets.

Description

Use **vpn-target** to configure VPN targets for a VPN instance.

Use **undo vpn-target** to remove the specified or all VPN targets of a VPN instance.

By default, no VPN targets are configured for a VPN instance. You must configure VPN targets when creating a VPN instance.

VPN targets configured in VPN instance view applies to both the IPv4 VPN and the IPv6 VPN.

VPN targets configured in IPv4 VPN view applies to only the IPv4 VPN.

VPN targets configured in IPv4 VPN view takes precedence over that configured in VPN instance view. If you configure VPN targets in both IPv4 VPN view and VPN instance view, those configured in IPv4 VPN view are applied to the IPv4 VPN.

Examples

Configure VPN targets for VPN instance **vpn1**.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
[Sysname-vpn-instance-vpn1] vpn-target 4:4 import-extcommunity
[Sysname-vpn-instance-vpn1] vpn-target 5:5 both
```

IPv6 MCE configuration commands

This chapter describes only the commands related to the IPv6 MCE feature. For information about the routing protocol configuration commands in the configuration examples, see *Layer 3—IP Routing Command Reference*.

The IPv6 MCE function is available only on the HP 5500 EI Switch Series.

display bgp vpnv6 vpn-instance peer

Syntax

```
display bgp vpnv6 vpn-instance vpn-instance-name peer [ ipv6-address verbose | verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor

Parameters

vpn-instance-name: Name of a VPN instance, a case-sensitive string of 1 to 31 characters.

ipv6-address: IPv6 address of a peer.

verbose: Displays the detailed information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp vpnv6 vpn-instance peer** to display information about the IPv6 BGP peers in the specified VPN instance.

If you do not specify any optional parameters, the command displays the brief information of all IPv6 BGP peers.

Examples

```
# Display brief information about the IPv6 BGP peers in the VPN instance vpn1.
```

```
<Sysname> display bgp vpnv6 vpn-instance vpn1 peer
```

```
BGP local router ID : 2.2.2.2
```

```
Local AS number : 100
```

```
Total number of peers : 1
```

```
Peers in established state : 1
```


Peer	AS	MsgRcvd	MsgSent	OutQ	PrefRcv	Up/Down	State
2001::1	200	4	6	0	2	00:00:09	Established

Table 110 Command output

Field	Description
BGP local router ID	Router ID of the local BGP router
Peer	IPv6 address of the peer
AS	AS number of the peer
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent to the peer
PrefRcv	Number of prefixes received
Up/Down	Duration of the BGP session in the current state
State	Current state of the peer

Display detailed information about the IPv6 BGP peers in the VPN instance **vpn1**.

```
<Sysname> display bgp vpnv6 vpn-instance vpn1 peer verbose
```

```

BGP Peer is 2001::1, remote AS 200,
Type: EBGp link
BGP version 4, remote router ID 2.2.2.2
BGP current state: Established, Up for 00h00m54s
BGP current event: RecvUpdate
BGP last state: OpenConfirm
Port: Local - 179 Remote - 1024
Configured: Active Hold Time: 180 sec Keepalive Time: 60 sec
Received : Active Hold Time: 180 sec
Negotiated: Active Hold Time: 180 sec Keepalive Time:60 sec
Peer optional capabilities:
Peer support bgp multi-protocol extended
Peer support bgp route refresh capability
Address family IPv6 Unicast: advertised and received

```

```

Received: Total 4 messages, Update messages 2
Sent: Total 6 messages, Update messages 3
Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisement runs is 30 seconds
Optional capabilities:
Route refresh capability has been enabled
Peer Preferred Value: 0

```

```

Routing policy configured:
No routing policy is configured

```

Table 111 Command output

Field	Description
BGP Peer	IPv6 address of the BGP peer
remote AS	AS number of the peer
Type	BGP type
BGP version	Version of BGP that the peer runs
remote router ID	Router ID of the peer
BGP current state	Current state of the BGP session
Up for	Duration since the peer is established
BGP current event	Current event of the BGP session
BGP last state	State that the BGP session was in before transitioning to the current state
Port	Local and remote ports of the BGP session
Configured	Settings of the local timers, including the active hold interval and keepalive interval
Received	Received active hold interval
Negotiated	Negotiated active hold interval
Peer optional capabilities	Optional capabilities of the peer
Peer support bgp multi-protocol extended	The peer supports multiprotocol extension.
Peer support bgp route refresh capability	The peer supports route refreshing.
Address family IPv6 Unicast	IPv6 unicast family capability
Received	Total number of received messages and the number of received update messages
Sent	Total number of sent messages and the number of sent update messages
Maximum allowed prefix number	Maximum number of routes that the VPN instance supports
Threshold	Threshold for warning. When the percentage of the number of the received route prefixes to the maximum number of routes supported reaches this value, the device generates a prompt.
Minimum time between advertisement runs	Minimum interval between route advertisements
Optional capabilities	Local optional capabilities
Route refresh capability	Whether route refreshing is enabled
Peer Preferred Value	Preference value specified for routes from the peer

display bgp vpnv6 vpn-instance routing-table

Syntax

```
display bgp vpnv6 vpn-instance vpn-instance-name routing-table [ network-address prefix-length  
[ longer-prefixes ] | peer ipv6-address { advertised-routes | received-routes } ] [ | { begin | exclude |  
include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance-name: VPN instance name, a case-sensitive string of 1 to 31 characters.

network-address: IPv6 address of the destination network segment.

prefix-length: Length of the prefix, in the range of 0 to 128.

longer-prefixes: Displays each routing entry that meets the following conditions:

- Its destination IPv6 address ANDed with the specified prefix equals the specified destination IPv6 address ANDed with the specified prefix.
- Its prefix length is shorter than or equal to the specified prefix length.
- Its prefix length is the longest among the entries meeting the above two conditions.

peer ipv6-address: Displays the routing information sent to or received from the specified BGP VPNv6 peer. *ipv6-address* is the IPv6 address of the peer.

advertised-routes: Displays the routing information sent to the specified peer.

received-routes: Displays the routing information received from the specified peer.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display bgp vpnv6 vpn-instance routing-table** to display the BGP VPNv6 routing information of the specified VPN.

Examples

```
# Display the BGP VPNv6 routing information of VPN instance vpn1.  
<Sysname> display bgp vpnv6 vpn-instance vpn1 routing-table  
BGP Local router ID is 1.1.1.1  
Status codes: * - valid, ^ - VPN best, > - best, d - damped,  
h - history, i - internal, s - suppressed, S - Stale  
Origin : i - IGP, e - EGP, ? - incomplete
```

Total routes of vpn-instance vpn1: 1

```
*^> Network : 324::                               PrefixLen : 64
      NextHop : 100::2                             LocPrf    : 100
      PrefVal : 0                                   Label     : NULL
      MED     : 0
      Path/Ogn: ?
```

Table 112 Command output

Field	Description
BGP Local router ID	Router ID of the local BGP router
Status codes	Route status codes.
Origin	Route origin codes.
Network	Destination network address
PrefixLen	Prefix length of the destination network address
NextHop	IPv6 address of the next hop
LocPrf	Local preference value
PrefVal	Preference value of the route
Label	Received label
MED	Metric associated with the destination network
Path/Ogn	AS_PATH attribute/route origin of the route.

display ipv6 fib vpn-instance

Syntax

```
display ipv6 fib vpn-instance vpn-instance-name [ acl6 acl6-number | ipv6-prefix ipv6-prefix-name ] [ |  
{ begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance-name: VPN instance name, a case-sensitive string of 1 to 31 characters.

acl6 *acl6-number*: Displays the IPv6 FIB information of the VPN instance permitted by the specified ACL. *acl6-number* is the number of the ACL, in the range of 2000 to 2999. If the specified ACL does not exist, the command displays all IPv6 FIB information of the VPN instance.

ipv6-prefix *ipv6-prefix-name*: Displays the IPv6 FIB information of the VPN instance permitted by the specified prefix list. *ipv6-prefix-name* is the name of the IPv6 prefix list, a case-sensitive string of 1 to 19 characters. If the specified IPv6 prefix list does not exist, the command displays all IPv6 FIB information of the VPN instance.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 fib vpn-instance** to display the IPv6 FIB information of the specified VPN.

If you do not specify any optional parameters, the command displays all IPv6 FIB information of the VPN.

Examples

```
# Display all IPv6 FIB information of VPN instance vpn1.
```

```
<Sysname> display ipv6 fib vpn-instance vpn1
```

```
FIB Table:
```

```
Total number of Routes : 1
```

```
Flag:
```

```
U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static
```

```
Destination:      ::1                               PrefixLength : 128
```

```
NextHop          :      ::1                               Flag          : UH
```

```
Label            :      Null                               Token         : Invalid
```

```
Interface       :      InLoopBack0
```

Table 113 Command output

Field	Description
Total number of Routes	Total number of matched routes in the FIB
Flag	Flag of the route. Possible values are: <ul style="list-style-type: none">• U—Usable route• G—Gateway route.• H—Host route.• B—Blackhole route.• D—Dynamic route.• S—Static route.
Label	Label value added to a packet
Token	LSP index, used to associate an NHLFE entry
Interface	Outgoing interface of packets

display ipv6 fib vpn-instance *ipv6-address*

Syntax

```
display ipv6 fib vpn-instance vpn-instance-name ipv6-address [ prefix-length ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance-name: VPN instance name, a case-sensitive string of 1 to 31 characters.

ipv6-address: Destination IPv6 address.

prefix-length: Prefix length of the destination IPv6 address, in the range of 0 to 128.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 fib vpn-instance** *ipv6-address* to display a VPN's IPv6 FIB information that matches a destination IPv6 address.

If you do not specify the prefix length, the command displays the matched IPv6 FIB information that has the longest prefix. If you specify the prefix length, the command displays the matched IPv6 FIB information that has the exact prefix length.

Examples

Displays the IPv6 FIB information with the destination address of ::1 in the VPN instance **vpn1**.

```
<Sysname> display ipv6 fib vpn-instance vpn1 ::1
```

```
FIB Table:
```

```
Total number of Routes : 1
```

```
Flag:
```

```
U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static
```

```
Destination:      ::1                PrefixLength : 128
```

```
NextHop          :      ::1                Flag          : UH
```

```
Label            :      Null                Token         : Invalid
```

```
Interface        :      InLoopBack0
```

Table 114 Command output

Field	Description
Total number of Routes	Total number of matched routes in the FIB

Field	Description
Flag	Flag of the route. Possible values are: <ul style="list-style-type: none"> • U—Usable route • G—Gateway route. • H—Host route. • B—Blackhole route. • D—Dynamic route. • S—Static route.
Label	Label value added to a packet
Token	LSP index, used to associate an NHLFE entry
Interface	Outgoing interface of packets

export route-policy

Syntax

```
export route-policy route-policy
undo export route-policy
```

View

VPN instance view, IPv6 VPN view

Default level

2: System level

Parameters

route-policy: Name of an export routing policy, a case-sensitive string of 1 to 63 characters.

Description

Use **export route-policy** to apply an export routing policy to a VPN instance, an IPv4 VPN, or an IPv6 VPN.

Use **undo export route-policy** to remove the application.

By default, no policy is applied to filter the routes to be advertised.

You can specify an export routing policy when the VPN route advertisement control provided by the extended community attributes is not enough.

An export routing policy specified in VPN instance view applies to both the IPv4 VPN and the IPv6 VPN.

An export routing policy specified in IPv6 VPN view applies to only the IPv6 VPN.

An export routing policy specified in IPv6 VPN view takes precedence over that specified in VPN instance view. If you specify an export routing policy in IPv6 VPN view and VPN instance view, the IPv6 VPN uses the policy specified in IPv6 VPN view.

Examples

```
# Apply export routing policy poly-1 to VPN instance vpn1.
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] export route-policy poly-1
```

```
# Apply export routing policy poly-3 to the IPv6 VPN of VPN instance vpn3.
<Sysname> system-view
[Sysname] ip vpn-instance vpn3
[Sysname-vpn-instance-vpn3] ipv6-family
[Sysname-vpn-ipv6-vpn3] export route-policy poly-3
```

filter-policy export

Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } export [ direct | isisv6 process-id | ospfv3 process-id | ripng process-id | static ]

undo filter-policy export [ direct | isisv6 process-id | ospfv3 process-id | ripng process-id | static ]
```

View

IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

acl6-number: Specifies an IPv6 ACL number, in the range of 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies an IPv6 address prefix list by its name, a string of 1 to 19 characters.

direct: Filters direct routes to be advertised.

isisv6 *process-id*: Filters IPv6 ISIS routes to be advertised that are from a specific IPv6 ISIS process. The *process-id* argument is in the range of 1 to 65535.

ospfv3 *process-id*: Filters OSPFv3 routes to be advertised that are from a specific OSPFv3 process. The *process-id* argument is in the range of 1 to 65535.

ripng *process-id*: Filters RIPng routes to be advertised that are from a specific RIPng process. The *process-id* argument is in the range of 1 to 65535.

static: Filters static routes to be advertised.

Description

Use **filter-policy export** to filter all or certain types of routes to be advertised.

Use **undo filter-policy export** to remove the configuration.

By default, BGP does not filter routes to be advertised.

Only routes that survive the filtering are advertised by BGP.

If you specify no routing protocol parameters for the **filter-policy export** command, all routes to be advertised are filtered.

Examples

```
# In IPv6 BGP-VPN instance view, use ACL 2555 to filter routes to be advertised by BGP.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family vpn-instance vpn1
[Sysname-bgp-ipv6-vpn1] filter-policy 2555 export
```


filter-policy import

Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } import  
undo filter-policy import
```

View

IPv6 BGP-VPN instance view

Default level

2: System level

Parameters

acl6-number: Specifies an IPv6 ACL number, in the range of 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies an IPv6 address prefix list by its name, a string of 1 to 19 characters.

Description

Use **filter-policy import** to filter received routes.

Use **undo filter-policy import** to remove the configuration.

By default, received routes are not filtered.

Only routes that survive the filtering are added into the BGP routing table.

Examples

```
# In IPv6 BGP-VPN instance view, use ACL 2255 to filter received routes.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family vpn-instance vpn1  
[Sysname-bgp-ipv6-vpn1] filter-policy 2255 import
```

import route-policy

Syntax

```
import route-policy route-policy  
undo import route-policy
```

View

VPN instance view, IPv6 VPN view

Default level

2: System level

Parameters

route-policy: Name of an import routing policy, a case-sensitive string of 1 to 63 characters.

Description

Use **import route-policy** to apply an import routing policy to a VPN instance, an IPv4 VPN or an IPv6 VPN.

Use **undo import route-policy** to remove the application.

By default, all routes permitted by the import target attribute are accepted.

You can specify an import routing policy when the route redistribution control provided by the extended community attributes is not enough.

An import routing policy specified in VPN instance view applies to both the IPv4 VPN and the IPv6 VPN.

An import routing policy specified in IPv6 VPN view applies to only the IPv6 VPN.

An import routing policy specified in IPv6 VPN view takes precedence over that specified in VPN instance view. If you specify an import routing policy in both IPv6 VPN view and VPN instance view, the IPv6 VPN uses the policy specified in IPv6 VPN view.

Examples

```
# Apply import routing policy poly-1 to VPN instance vpn1.
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] import route-policy poly-1

# Apply import routing policy poly-3 to the IPv6 VPN of VPN instance vpn3.
<Sysname> system-view
[Sysname] ip vpn-instance vpn3
[Sysname-vpn-instance-vpn3] ipv6-family
[Sysname-vpn-ipv6-vpn3] import route-policy poly-3
```

ipv6-family

Syntax

```
ipv6-family
undo ipv6-family
```

Views

VPN instance view

Default level

2: System level

Parameters

None

Description

Use **ipv6-family** to enter IPv6 VPN view.

Use **undo ipv6-family** to remove all configurations performed in IPv6 VPN view.

Examples

```
# Enter IPv6 VPN view.
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] ipv6-family
[Sysname-vpn-ipv6-vpn1]
```

ipv6-family vpn-instance

Syntax

```
ipv6-family vpn-instance vpn-instance-name  
undo ipv6-family vpn-instance vpn-instance-name
```

View

BGP view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Associates a VPN instance with an IPv6 address family and enters IPv6 BGP-VPN instance view. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters.

Description

Use **ipv6-family vpn-instance** in BGP view to enter IPv6 BGP-VPN instance view.

Use **undo ipv6-family vpn-instance** to remove all configurations performed in IPv6 BGP-VPN instance view.

Before entering IPv6 BGP-VPN instance view, you must create the VPN instance.

Examples

```
# Associate VPN instance vpn1 with the IPv6 address family and enter IPv6 BGP-VPN instance view.  
<Sysname> system-view  
[Sysname] ip vpn-instance vpn1  
[Sysname-vpn-instance-vpn1] quit  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family vpn-instance vpn1  
[Sysname-bgp-vpn1]
```

refresh bgp ipv6 vpn-instance

Syntax

```
refresh bgp ipv6 vpn-instance vpn-instance-name { ipv6-address | all | external } { export | import }
```

View

User view

Default level

1: Monitor level

Parameters

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

ipv6-address: Soft resets the BGP connection with the BGP peer identified by this IPv6 address.

all: Soft resets all IPv6 BGP connections in the specified VPN instance.

external: Soft resets EBGP sessions.

export: Performs a soft reset in the outbound direction.

import: Performs a soft reset in the inbound direction.

Description

Use **refresh bgp ipv6 vpn-instance** to soft reset IPv6 BGP connections in a VPN instance.

Examples

```
# Soft reset all IPv6 BGP connections in VPN instance vpn1 in the inbound direction to make new configurations take effect.
```

```
<Sysname> refresh bgp ipv6 vpn-instance vpn1 all import
```

reset bgp ipv6 vpn-instance

Syntax

```
reset bgp ipv6 vpn-instance vpn-instance-name { as-number | ipv6-address | all | external }
```

View

User view

Default level

1: Monitor level

Parameters

vpn-instance-name: Resets IPv6 BGP connections with the peers in a VPN instance. The VPN instance name is a case-sensitive string of 1 to 31 characters.

as-number: Resets IPv6 BGP connections with the peers in an AS. The AS number is in the range of 1 to 4294967295.

ipv6-address: Resets the connection with the BGP peer identified by this IPv6 address.

all: Resets all IPv6 BGP connections in the specified VPN instance.

external: Resets EBGP sessions.

Description

Use **reset bgp ipv6 vpn-instance** to reset IPv6 BGP connections in a VPN instance.

Examples

```
# Reset all IPv6 BGP connections in VPN instance vpn1.
```

```
<Sysname> reset bgp ipv6 vpn-instance vpn1 all
```

routing-table limit

Syntax

```
routing-table limit number { warn-threshold | simply-alert }
```

```
undo routing-table limit
```

View

VPN instance view, IPv6 VPN view

Default level

2: System level

Parameters

number: Specifies the maximum number of routes supported. The value ranges from 1 to 6144.

warn-threshold: Specifies a threshold for warning, in the range of 1 to 100, in percentages. When the percentage of the number of existing routes to the maximum number of routes supported exceeds the specified threshold, the system gives an alarm message but still allows new routes. If the number of routes in the VPN instance reaches the maximum supported, no more routes are added.

simply-alert: Specifies that when the number of routes exceeds the maximum number of routes supported, the system still accepts routes but generates a system log (Syslog) message.

Description

Use **routing-table limit** to limit the maximum number of routes in a VPN instance, an IPv4 VPN, or an IPv6 VPN, preventing too many routes from being accepted by a PE.

Use **undo routing-table limit** to restore the default.

By default, no limit is configured.

A limit configured in VPN instance view applies to both the IPv4 VPN and the IPv6 VPN.

A limit configured in IPv6 VPN view applies to only the IPv6 VPN.

A limit configured in IPv6 VPN view takes precedence over that configured in VPN instance view. If you configure a limit in both IPv6 VPN view and VPN instance view, IPv6 VPN uses the limit configured in IPv6 VPN view.

Examples

Configure VPN instance **vpn1** to support up to 1000 routes, and receive new routes after the number of existing routes exceeds the limit.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 100:1
[Sysname-vpn-instance-vpn1] routing-table limit 1000 simply-alert
```

Specify that the IPv6 VPN of VPN instance **vpn3** supports up to 1000 routes, and can receive new routes after the number of existing routes exceeds the limit.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn3
[Sysname-vpn-instance-vpn3] route-distinguisher 100:3
[Sysname-vpn-instance-vpn3] ipv6-family
[Sysname-vpn-ipv4-vpn3] routing-table limit 1000 simply-alert
```

vpn-target

Syntax

```
vpn-target vpn-target&<1-8> [ both | export-extcommunity | import-extcommunity ]
undo vpn-target { all | vpn-target&<1-8> [ both | export-extcommunity | import-extcommunity ] }
```

View

VPN instance view, IPv6 VPN view

Default level

2: System level

Parameters

`vpn-target<1-8>`: Adds VPN target extended community attributes to the import VPN target extended community attribute list (Import Target) or export VPN target extended community attribute list (Export Target). `<1-8>` means that you can add up to eight VPN targets.

A VPN target attribute can be a string of 3 to 21 characters in one of the following formats:

- 16-bit AS number:32-bit user-defined number. For example, 101:3.
- 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1.
- 32-bit AS number:16-bit user-defined number, where the AS number must not be less than 65536. For example, 65536:1.

both: Uses the specified VPN targets as both import targets and export targets. The **both** keyword is also used when you do not specify any of **both**, **export-extcommunity**, and **import-extcommunity**.

export-extcommunity: Uses the specified VPN targets as export targets.

import-extcommunity: Uses the specified VPN targets as import targets.

all: Removes all VPN targets.

Description

Use **vpn-target** to configure VPN targets for a VPN instance, an IPv4 VPN, or an IPv6 VPN.

Use **undo vpn-target** to remove the specified or all VPN targets of a VPN instance, an IPv4 VPN, or an IPv6 VPN.

By default, no VPN targets are configured and you must configure VPN targets when creating a VPN instance, an IPv4 VPN, or an IPv6 VPN.

VPN targets configured in VPN instance view are applicable to both the IPv4 VPN and the IPv6 VPN.

VPN targets configured in IPv6 VPN view are applicable to only the IPv6 VPN.

VPN targets configured in IPv6 VPN view take precedence over those configured in VPN instance view. If you configure VPN targets in both IPv6 VPN view and VPN instance view, the IPv6 VPN uses the VPN targets configured in IPv6 VPN view.

Examples

Configure VPN targets for VPN instance **vpn1**.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
[Sysname-vpn-instance-vpn1] vpn-target 4:4 import-extcommunity
[Sysname-vpn-instance-vpn1] vpn-target 5:5 both
```

Configure VPN targets for the IPv6 VPN of VPN instance **vpn3**.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn3
[Sysname-vpn-instance-vpn3] ipv6-family
[Sysname-vpn-ipv6-vpn3] vpn-target 3:3 export-extcommunity
[Sysname-vpn-ipv6-vpn3] vpn-target 4:4 import-extcommunity
[Sysname-vpn-ipv6-vpn3] vpn-target 5:5 both
```

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

<http://www.hp.com/support>

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

<http://www.hp.com/go/wwalerts>

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

<http://www.hp.com/support/manuals>

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Websites

- HP.com <http://www.hp.com>
- HP Networking <http://www.hp.com/go/networking>
- HP manuals <http://www.hp.com/support/manuals>
- HP download drivers and software <http://www.hp.com/support/downloads>
- HP software depot <http://www.software.hp.com>
- HP Education <http://www.hp.com/learn>

Conventions

This section describes the conventions used in this documentation set.





Command conventions

Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> text represents arguments that you replace with actual values.
[]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x y ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x y ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x y ... } *	Asterisk-marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x y ...] *	Asterisk-marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.








GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the New User window appears; click OK .
>	Multi-level menus are separated by angle brackets. For example, File > Create > Folder .

Symbols

Convention	Description
 WARNING	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 CAUTION	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
 TIP	An alert that provides helpful information.

Network topology icons

	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the switching engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a security product, such as a firewall, a UTM, or a load-balancing or security card that is installed in a device.
	Represents a security card, such as a firewall card, a load-balancing card, or a NetStream card.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index

A B C D E F G H I L M N O P R S T V

A

abr-summary (OSPF area view), 61
area (OSPF view), 62
area-authentication-mode, 130
asbr-summary, 62
authentication-mode, 63
auto-cost enable, 131

B

bandwidth-reference (IS-IS view), 132
bandwidth-reference (OSPF view), 64

C

checkzero, 30
circuit-cost, 132
cost-style, 133

D

default, 65
default cost (RIP view), 30
default-cost (OSPF area view), 65
default-route, 31
default-route-advertise (IS-IS view), 134
default-route-advertise (OSPF view), 66
delete static-routes all, 25
description (OSPF/OSPF area view), 67
display ip routing-table, 1
display ip routing-table acl, 5
display ip routing-table ip-address, 8
display ip routing-table ip-prefix, 11
display ip routing-table protocol, 12
display ip routing-table statistics, 14
display ipv6 routing-table, 15
display ipv6 routing-table acl, 17
display ipv6 routing-table ipv6-address, 18
display ipv6 routing-table ipv6-prefix, 20
display ipv6 routing-table protocol, 21
display ipv6 routing-table statistics, 22
display isis brief, 135

display isis debug-switches, 136
display isis graceful-restart status, 137
display isis interface, 138
display isis lsdb, 142
display isis name-table, 145
display isis peer, 146
display isis route, 148
display isis spf-log, 151
display isis statistics, 153
display ospf abr-asbr, 68
display ospf asbr-summary, 69
display ospf brief, 70
display ospf cumulative, 73
display ospf error, 75
display ospf interface, 77
display ospf lsdb, 79
display ospf nexthop, 81
display ospf peer, 82
display ospf peer statistics, 85
display ospf request-queue, 86
display ospf retrans-queue, 87
display ospf routing, 89
display ospf vlink, 90
display rip, 32
display rip database, 34
display rip interface, 35
display rip route, 36
display router id, 91
domain-authentication-mode, 155
dscp (OSPF view), 92
dscp (RIP view), 38

E

enable link-local-signaling, 92
enable log, 93
enable out-of-band-resynchronization, 93

F

fast-reroute, 156

- fast-reroute, [94](#)
- fast-reroute, [38](#)
- filter, [95](#)
- filter-policy export (IS-IS view), [157](#)
- filter-policy export (OSPF view), [96](#)
- filter-policy export (RIP view), [39](#)
- filter-policy import (IS-IS view), [158](#)
- filter-policy import (OSPF view), [97](#)
- filter-policy import (RIP view), [41](#)
- flash-flood, [159](#)

G

- graceful-restart (IS-IS view), [160](#)
- graceful-restart (OSPF view), [98](#)
- graceful-restart help, [99](#)
- graceful-restart interval (IS-IS view), [161](#)
- graceful-restart interval (OSPF view), [100](#)

H

- host-advertise, [100](#)
- host-route, [42](#)

I

- import-route (OSPF view), [101](#)
- import-route (RIP view), [42](#)
- ip route-static, [25](#)
- ip route-static default-preference, [28](#)
- ip route-static fast-reroute, [28](#)
- ispf enable, [102](#)

L

- log-peer-change, [103](#)
- lsa-arrival-interval, [103](#)
- lsa-generation-interval, [104](#)
- lsdb-overflow-limit, [105](#)

M

- maximum load-balancing (OSPF view), [105](#)
- maximum load-balancing (RIP view), [44](#)
- maximum-routes, [106](#)

N

- network, [44](#)
- network (OSPF area view), [107](#)
- nssa, [107](#)

O

- opaque-capability enable, [108](#)
- ospf, [109](#)
- ospf authentication-mode, [110](#)
- ospf bfd enable, [111](#)
- ospf cost, [112](#)
- ospf dr-priority, [112](#)
- ospf mib-binding, [113](#)
- ospf mtu-enable, [113](#)
- ospf network-type, [114](#)
- ospf packet-process prioritized-treatment, [115](#)
- ospf timer dead, [116](#)
- ospf timer hello, [116](#)
- ospf timer poll, [117](#)
- ospf timer retransmit, [118](#)
- ospf trans-delay, [118](#)
- output-delay, [45](#)

P

- peer, [119](#)
- peer, [45](#)
- preference, [120](#)
- preference, [46](#)

R

- reset ip routing-table statistics protocol, [23](#)
- reset ipv6 routing-table statistics, [23](#)
- reset ospf counters, [120](#)
- reset ospf process, [121](#)
- reset ospf redistribution, [122](#)
- reset rip process, [47](#)
- reset rip statistics, [47](#)
- rfc 1583 compatible, [122](#)
- rip, [48](#)
- rip authentication-mode, [48](#)
- rip bfd enable, [49](#)
- rip default-route, [50](#)
- rip input, [51](#)
- rip metricin, [51](#)
- rip metricout, [52](#)
- rip mib-binding, [53](#)
- rip output, [54](#)
- rip poison-reverse, [54](#)
- rip split-horizon, [55](#)
- rip summary-address, [55](#)
- rip version, [56](#)
- router id, [123](#)

S

silent-interface (OSPF view), [123](#)
silent-interface (RIP view), [57](#)
snmp-agent trap enable ospf, [124](#)
spf-schedule-interval, [125](#)
stub (OSPF area view), [126](#)
stub-router, [127](#)
summary, [57](#)

T

timers, [58](#)
transmit-pacing, [127](#)

V

validate-source-address, [59](#)
version, [60](#)
vlink-peer (OSPF area view), [128](#)