

HP 5500 EI & 5500 SI Switch Series

IP Multicast

Command Reference

Part number: 5998-1711

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

IGMP snooping configuration commands	1
display igmp-snooping group	1
display igmp-snooping host	2
display igmp-snooping statistics	4
display mac-address multicast	5
dot1p-priority (IGMP-snooping view)	6
dscp (IGMP-snooping view)	7
fast-leave (IGMP-snooping view)	7
group-policy (IGMP-snooping view)	8
host-aging-time (IGMP-snooping view)	9
host-tracking (IGMP-snooping view)	10
igmp-snooping	10
igmp-snooping access-policy	11
igmp-snooping dot1p-priority	12
igmp-snooping drop-unknown	12
igmp-snooping enable	13
igmp-snooping fast-leave	14
igmp-snooping general-query source-ip	14
igmp-snooping group-limit	15
igmp-snooping group-policy	16
igmp-snooping host-aging-time	17
igmp-snooping host-join	18
igmp-snooping host-tracking	19
igmp-snooping last-member-query-interval	20
igmp-snooping leave source-ip	20
igmp-snooping max-response-time	21
igmp-snooping overflow-replace	22
igmp-snooping proxying enable	23
igmp-snooping querier	23
igmp-snooping query-interval	24
igmp-snooping report source-ip	25
igmp-snooping router-aging-time	26
igmp-snooping router-port-deny	26
igmp-snooping source-deny	27
igmp-snooping special-query source-ip	28
igmp-snooping static-group	29
igmp-snooping static-router-port	30
igmp-snooping version	30
last-member-query-interval (IGMP-snooping view)	31
mac-address multicast	32
max-response-time (IGMP-snooping view)	33
overflow-replace (IGMP-snooping view)	33
report-aggregation (IGMP-snooping view)	34
reset igmp-snooping group	35
reset igmp-snooping statistics	35
router-aging-time (IGMP-snooping view)	36
source-deny (IGMP-snooping view)	36

PIM snooping configuration commands	38
display pim-snooping neighbor	38
display pim-snooping routing-table	39
display pim-snooping statistics	40
pim-snooping enable	41
reset pim-snooping statistics	42
Multicast VLAN configuration commands	43
display multicast-vlan	43
multicast-vlan	44
port (multicast VLAN view)	45
port multicast-vlan	45
subvlan (multicast VLAN view)	46
Multicast routing and forwarding configuration commands (available only on the HP 5500 EI)	47
delete ip rpf-route-static	47
display multicast boundary	47
display multicast forwarding-table	49
display multicast forwarding-table df-info	51
display multicast routing-table	53
display multicast routing-table static	55
display multicast rpf-info	56
ip rpf-route-static	57
mtracert	59
multicast boundary	60
multicast forwarding-table downstream-limit	61
multicast forwarding-table route-limit	62
multicast load-splitting	62
multicast longest-match	63
multicast routing-enable	64
reset multicast forwarding-table	64
reset multicast routing-table	65
IGMP configuration commands (available only on the HP 5500 EI)	67
display igmp group	67
display igmp group port-info	69
display igmp host interface	71
display igmp host port-info	72
display igmp interface	73
display igmp proxying group	75
display igmp routing-table	77
display igmp ssm-mapping	79
display igmp ssm-mapping group	80
display igmp ssm-mapping host interface	82
dscp (IGMP view)	83
fast-leave (IGMP view)	83
host-tracking (IGMP view)	84
igmp	85
igmp enable	86
igmp fast-leave	86
igmp group-limit	87
igmp group-policy	88
igmp host-tracking	89
igmp last-member-query-interval	89
igmp max-response-time	90
igmp proxying enable	90

igmp proxying forwarding	91
igmp require-router-alert	92
igmp robust-count	92
igmp send-router-alert	93
igmp ssm-mapping enable	94
igmp startup-query-count	94
igmp startup-query-interval	95
igmp static-group	95
igmp timer other-querier-present	96
igmp timer query	97
igmp version	98
last-member-query-interval (IGMP view)	98
max-response-time (IGMP view)	99
require-router-alert (IGMP view)	99
reset igmp group	100
reset igmp group port-info	101
reset igmp ssm-mapping group	102
robust-count (IGMP view)	103
send-router-alert (IGMP view)	104
ssm-mapping (IGMP view)	104
startup-query-count (IGMP view)	105
startup-query-interval (IGMP view)	106
timer other-querier-present (IGMP view)	106
timer query (IGMP view)	107
version (IGMP view)	108
PIM configuration commands (available only on the HP 5500 EI)	109
auto-rp enable	109
bidir-pim enable (PIM view)	109
bsm-fragment enable (PIM view)	110
bsr-policy (PIM view)	111
c-bsr (PIM view)	112
c-bsr admin-scope (PIM view)	113
c-bsr global	113
c-bsr group	114
c-bsr hash-length (PIM view)	115
c-bsr holdtime (PIM view)	116
c-bsr interval (PIM view)	116
c-bsr priority (PIM view)	117
c-rp (PIM view)	118
c-rp advertisement-interval (PIM view)	119
c-rp holdtime (PIM view)	120
crp-policy (PIM view)	120
display pim bsr-info	121
display pim claimed-route	123
display pim control-message counters	125
display pim df-info	127
display pim grafts	128
display pim interface	129
display pim join-prune	131
display pim neighbor	133
display pim routing-table	135
display pim rp-info	139
dscp (PIM view)	140
hello-option dr-priority (PIM view)	141

hello-option holdtime (PIM view).....	141
hello-option lan-delay (PIM view).....	142
hello-option neighbor-tracking (PIM view).....	143
hello-option override-interval (PIM view).....	144
holdtime assert (PIM view).....	144
holdtime join-prune (PIM view).....	145
jp-pkt-size (PIM view).....	146
jp-queue-size (PIM view).....	146
pim.....	147
pim bfd enable.....	148
pim bsr-boundary.....	149
pim dm.....	149
pim hello-option dr-priority.....	150
pim hello-option holdtime.....	150
pim hello-option lan-delay.....	151
pim hello-option neighbor-tracking.....	152
pim hello-option override-interval.....	152
pim holdtime assert.....	153
pim holdtime join-prune.....	153
pim neighbor-policy.....	154
pim require-genid.....	155
pim sm.....	155
pim state-refresh-capable.....	156
pim timer graft-retry.....	156
pim timer hello.....	157
pim timer join-prune.....	157
pim triggered-hello-delay.....	158
probe-interval (PIM view).....	159
prune delay (PIM view).....	159
register-policy (PIM view).....	160
register-suppression-timeout (PIM view).....	161
register-whole-checksum (PIM view).....	161
reset pim control-message counters.....	162
source-lifetime (PIM view).....	163
source-policy (PIM view).....	163
spt-switch-threshold infinity (PIM view).....	164
ssm-policy (PIM view).....	165
state-refresh-interval (PIM view).....	166
state-refresh-rate-limit (PIM view).....	167
state-refresh-ttl.....	167
static-rp (PIM view).....	168
timer hello (PIM view).....	169
timer join-prune (PIM view).....	170

MSDP configuration commands (available only on the HP 5500 EI).....	172
cache-sa-enable.....	172
display msdp brief.....	173
display msdp peer-status.....	174
display msdp sa-cache.....	177
display msdp sa-count.....	178
encap-data-enable.....	180
import-source.....	180
msdp.....	182
originating-rp.....	182
peer connect-interface.....	183

peer description	184
peer mesh-group	185
peer minimum-ttl	185
peer password	186
peer request-sa-enable	187
peer sa-cache-maximum	188
peer sa-policy	189
peer sa-request-policy	190
reset msdp peer	191
reset msdp sa-cache	191
reset msdp statistics	192
shutdown (MSDP view)	192
static-rpf-peer	193
timer retry	194

MBGP configuration commands (available only on the HP 5500 EI) 196

aggregate (MBGP address family view)	196
balance (MBGP address family view)	197
bestroute as-path-neglect (MBGP address family view)	198
bestroute compare-med (MBGP address family view)	198
bestroute med-confederation (MBGP address family view)	199
compare-different-as-med (MBGP address family view)	200
dampening (MBGP address family view)	200
default local-preference (MBGP address family view)	201
default med (MBGP address family view)	202
default-route imported (MBGP address family view)	202
display ip multicast routing-table	203
display ip multicast routing-table <i>ip-address</i>	205
display bgp multicast group	207
display bgp multicast network	209
display bgp multicast paths	210
display bgp multicast peer	211
display bgp multicast peer received ip-prefix	214
display bgp multicast routing-table	215
display bgp multicast routing-table as-path-acl	216
display bgp multicast routing-table cidr	217
display bgp multicast routing-table community	218
display bgp multicast routing-table community-list	219
display bgp multicast routing-table dampened	220
display bgp multicast routing-table dampening parameter	221
display bgp multicast routing-table different-origin-as	222
display bgp multicast routing-table flap-info	223
display bgp multicast routing-table peer	224
display bgp multicast routing-table regular-expression	225
display bgp multicast routing-table statistic	226
filter-policy export (MBGP address family view)	226
filter-policy import (MBGP address family view)	227
import-route (MBGP address family view)	228
ipv4-family multicast	229
network (MBGP address family view)	229
peer advertise-community (MBGP address family view)	230
peer advertise-ext-community (MBGP address family view)	231
peer allow-as-loop (MBGP address family view)	232
peer as-path-acl (MBGP address family view)	232
peer capability-advertise orf (MBGP address family view)	233

peer default-route-advertise (MBGP address family view)	234
peer enable (MBGP address family view)	235
peer filter-policy (MBGP address family view)	236
peer group (MBGP address family view)	236
peer ip-prefix (MBGP address family view)	237
peer keep-all-routes (MBGP address family view)	238
peer next-hop-local (MBGP address family view)	238
peer preferred-value (MBGP address family view)	239
peer public-as-only (MBGP address family view)	240
peer reflect-client (MBGP address family view)	241
peer route-limit (MBGP address family view)	241
peer route-policy (MBGP address family view)	242
preference (MBGP address family view)	243
reflect between-clients (MBGP address family view)	244
reflector cluster-id (MBGP address family view)	244
refresh bgp ipv4 multicast	245
reset bgp ipv4 multicast	246
reset bgp ipv4 multicast dampening	246
reset bgp ipv4 multicast flap-info	247
summary automatic (MBGP address family view)	247

MLD snooping configuration commands..... 249

display mld-snooping group	249
display mld-snooping host	250
display mld-snooping statistics	252
dot1p-priority (MLD-snooping view)	253
dscp (MLD-snooping view)	253
fast-leave (MLD-snooping view)	254
group-policy (MLD-snooping view)	255
host-aging-time (MLD-snooping view)	256
host-tracking (MLD-snooping view)	256
last-listener-query-interval (MLD-snooping view)	257
max-response-time (MLD-snooping view)	257
mld-snooping	258
mld-snooping access-policy	259
mld-snooping done source-ip	259
mld-snooping dot1p-priority	260
mld-snooping drop-unknown	261
mld-snooping enable	262
mld-snooping fast-leave	262
mld-snooping general-query source-ip	263
mld-snooping group-limit	264
mld-snooping group-policy	265
mld-snooping host-aging-time	266
mld-snooping host-join	267
mld-snooping host-tracking	268
mld-snooping last-listener-query-interval	268
mld-snooping max-response-time	269
mld-snooping overflow-replace	270
mld-snooping proxying enable	271
mld-snooping querier	271
mld-snooping query-interval	272
mld-snooping report source-ip	273
mld-snooping router-aging-time	274
mld-snooping router-port-deny	274

mld-snooping source-deny	275
mld-snooping special-query source-ip	276
mld-snooping static-group	277
mld-snooping static-router-port	278
mld-snooping version	278
overflow-replace (MLD-snooping view)	279
report-aggregation (MLD-snooping view)	280
reset mld-snooping group	280
reset mld-snooping statistics	281
router-aging-time (MLD-snooping view)	281
source-deny (MLD-snooping view)	282
IPv6 PIM snooping configuration commands	284
display pim-snooping ipv6 neighbor	284
display pim-snooping ipv6 routing-table	285
display pim-snooping ipv6 statistics	286
pim-snooping ipv6 enable	287
reset pim-snooping ipv6 statistics	288
IPv6 multicast VLAN configuration commands	289
display multicast-vlan ipv6	289
multicast-vlan ipv6	290
port (IPv6 multicast VLAN view)	291
port multicast-vlan ipv6	291
subvlan (IPv6 multicast VLAN view)	292
IPv6 multicast routing and forwarding configuration commands (available only on the HP 5500 EI)	293
display multicast ipv6 boundary	293
display multicast ipv6 forwarding-table	294
display multicast ipv6 forwarding-table df-info	297
display multicast ipv6 routing-table	298
display multicast ipv6 rpf-info	299
multicast ipv6 boundary	301
multicast ipv6 forwarding-table downstream-limit	302
multicast ipv6 forwarding-table route-limit	302
multicast ipv6 load-splitting	303
multicast ipv6 longest-match	304
multicast ipv6 routing-enable	304
reset multicast ipv6 forwarding-table	305
reset multicast ipv6 routing-table	305
MLD configuration commands (available only on the HP 5500 EI)	307
display mld group	307
display mld group port-info	308
display mld host interface	310
display mld host port-info	311
display mld interface	313
display mld proxying group	315
display mld routing-table	316
display mld ssm-mapping	318
display mld ssm-mapping group	319
display mld ssm-mapping host interface	320
dscp (MLD view)	321
fast-leave (MLD view)	322
host-tracking (MLD view)	322
last-listener-query-interval (MLD view)	323

max-response-time (MLD view).....	324
mld	324
mld enable	325
mld fast-leave	325
mld group-limit.....	326
mld group-policy.....	327
mld host-tracking.....	328
mld last-listener-query-interval.....	328
mld max-response-time.....	329
mld proxying enable.....	330
mld proxying forwarding.....	330
mld require-router-alert.....	331
mld robust-count.....	332
mld send-router-alert.....	332
mld ssm-mapping enable.....	333
mld startup-query-count	334
mld startup-query-interval.....	334
mld static-group	335
mld timer other-querier-present.....	336
mld timer query.....	336
mld version.....	337
require-router-alert (MLD view).....	337
reset mld group.....	338
reset mld group port-info	339
reset mld ssm-mapping group.....	340
robust-count (MLD view).....	340
send-router-alert (MLD view).....	341
ssm-mapping (MLD view).....	342
startup-query-count (MLD view).....	342
startup-query-interval (MLD view).....	343
timer other-querier-present (MLD view).....	344
timer query (MLD view).....	344
version (MLD view).....	345

IPv6 PIM configuration commands (available only on the HP 5500 EI)..... 346

bidir-pim enable (IPv6 PIM view).....	346
bsm-fragment enable (IPv6 PIM view)	346
bsr-policy (IPv6 PIM view).....	347
c-bsr (IPv6 PIM view).....	348
c-bsr admin-scope (IPv6 PIM view)	348
c-bsr hash-length (IPv6 PIM view)	349
c-bsr holdtime (IPv6 PIM view)	350
c-bsr interval (IPv6 PIM view)	350
c-bsr priority (IPv6 PIM view).....	351
c-bsr scope	351
c-rp (IPv6 PIM view).....	352
c-rp advertisement-interval (IPv6 PIM view)	353
c-rp holdtime (IPv6 PIM view).....	354
crp-policy (IPv6 PIM view)	355
display pim ipv6 bsr-info	355
display pim ipv6 claimed-route.....	357
display pim ipv6 control-message counters.....	358
display pim ipv6 df-info.....	360
display pim ipv6 grafts.....	361
display pim ipv6 interface.....	362

display pim ipv6 join-prune	364
display pim ipv6 neighbor	365
display pim ipv6 routing-table	367
display pim ipv6 rp-info	370
dscp (IPv6 PIM view)	371
embedded-rp	372
hello-option dr-priority (IPv6 PIM view)	373
hello-option holdtime (IPv6 PIM view)	373
hello-option lan-delay (IPv6 PIM view)	374
hello-option neighbor-tracking (IPv6 PIM view)	375
hello-option override-interval (IPv6 PIM view)	375
holdtime assert (IPv6 PIM view)	376
holdtime join-prune (IPv6 PIM view)	376
jp-pkt-size (IPv6 PIM view)	377
jp-queue-size (IPv6 PIM view)	378
pim ipv6	378
pim ipv6 bfd enable	379
pim ipv6 bsr-boundary	380
pim ipv6 dm	380
pim ipv6 hello-option dr-priority	381
pim ipv6 hello-option holdtime	381
pim ipv6 hello-option lan-delay	382
pim ipv6 hello-option neighbor-tracking	383
pim ipv6 hello-option override-interval	383
pim ipv6 holdtime assert	384
pim ipv6 holdtime join-prune	384
pim ipv6 neighbor-policy	385
pim ipv6 require-genid	386
pim ipv6 sm	386
pim ipv6 state-refresh-capable	387
pim ipv6 timer graft-retry	387
pim ipv6 timer hello	388
pim ipv6 timer join-prune	388
pim ipv6 triggered-hello-delay	389
probe-interval (IPv6 PIM view)	390
prune delay (IPv6 PIM view)	390
register-policy (IPv6 PIM view)	391
register-suppression-timeout (IPv6 PIM view)	391
register-whole-checksum (IPv6 PIM view)	392
reset pim ipv6 control-message counters	393
source-lifetime (IPv6 PIM view)	393
source-policy (IPv6 PIM view)	394
spt-switch-threshold infinity (IPv6 PIM view)	394
ssm-policy (IPv6 PIM view)	395
state-refresh-hoplimit	396
state-refresh-interval (IPv6 PIM view)	397
state-refresh-rate-limit (IPv6 PIM view)	397
static-rp (IPv6 PIM view)	398
timer hello (IPv6 PIM view)	399
timer join-prune (IPv6 PIM view)	399

IPv6 MBGP configuration commands (available only on the HP 5500 EI)	401
aggregate (IPv6 MBGP address family view)	401
balance (IPv6 MBGP address family view)	402
bestroute as-path-neglect (IPv6 MBGP address family view)	403

bestroute compare-med (IPv6 MBGP address family view)	403
bestroute med-confederation (IPv6 MBGP address family view)	404
compare-different-as-med (IPv6 MBGP address family view)	404
dampening (IPv6 MBGP address family view)	405
default local-preference (IPv6 MBGP address family view)	406
default med (IPv6 MBGP address family view)	407
default-route imported (IPv6 MBGP address family view)	407
display bgp ipv6 multicast group	408
display bgp ipv6 multicast network	410
display bgp ipv6 multicast paths	411
display bgp ipv6 multicast peer	412
display bgp ipv6 multicast peer received ipv6-prefix	413
display bgp ipv6 multicast routing-table	414
display bgp ipv6 multicast routing-table as-path-acl	416
display bgp ipv6 multicast routing-table community	417
display bgp ipv6 multicast routing-table community-list	418
display bgp ipv6 multicast routing-table dampened	419
display bgp ipv6 multicast routing-table dampening parameter	420
display bgp ipv6 multicast routing-table different-origin-as	421
display bgp ipv6 multicast routing-table flap-info	422
display bgp ipv6 multicast routing-table peer	423
display bgp ipv6 multicast routing-table regular-expression	424
display bgp ipv6 multicast routing-table statistic	425
display ipv6 multicast routing-table	425
display ipv6 multicast routing-table <i>ipv6-address</i>	427
filter-policy export (IPv6 MBGP address family view)	428
filter-policy import (IPv6 MBGP address family view)	429
import-route (IPv6 MBGP address family view)	430
ipv6-family multicast	430
network (IPv6 MBGP address family view)	431
peer advertise-community (IPv6 MBGP address family view)	432
peer advertise-ext-community (IPv6 MBGP address family view)	433
peer allow-as-loop (IPv6 MBGP address family view)	433
peer as-path-acl (IPv6 MBGP address family view)	434
peer capability-advertise orf (IPv6 MBGP address family view)	435
peer default-route-advertise (IPv6 MBGP address family view)	436
peer enable (IPv6 MBGP address family view)	437
peer filter-policy (IPv6 MBGP address family view)	438
peer group (IPv6 MBGP address family view)	438
peer ipv6-prefix (IPv6 MBGP address family view)	439
peer keep-all-routes (IPv6 MBGP address family view)	440
peer next-hop-local (IPv6 MBGP address family view)	441
peer preferred-value (IPv6 MBGP address family view)	441
peer public-as-only (IPv6 MBGP address family view)	442
peer reflect-client (IPv6 MBGP address family view)	443
peer route-limit (IPv6 MBGP address family view)	444
peer route-policy (IPv6 MBGP address family view)	445
preference (IPv6 MBGP address family view)	446
reflect between-clients (IPv6 MBGP address family view)	446
reflector cluster-id (IPv6 MBGP address family view)	447
refresh bgp ipv6 multicast	448
reset bgp ipv6 multicast	448
reset bgp ipv6 multicast dampening	449
reset bgp ipv6 multicast flap-info	449

Support and other resources	451
Contacting HP	451
Subscription service	451
Related information	451
Documents	451
Websites	451
Conventions	452
Index	454

IGMP snooping configuration commands

display igmp-snooping group

Syntax

```
display igmp-snooping group [ vlan vlan-id ] [ slot slot-number ] [ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the IGMP snooping group information in the specified VLAN, where the *vlan-id* argument is in the range of 1 to 4094. If you do not specify a VLAN, this command displays the IGMP snooping group information in all VLANs.

slot *slot-number*: Displays the IGMP snooping group information on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

verbose: Displays the detailed IGMP snooping group 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 igmp-snooping group** to display IGMP snooping group information, including both dynamic entries and static entries.

Examples

```
# Display detailed IGMP snooping group information in VLAN 2.
```

```
<Sysname> display igmp-snooping group vlan 2 verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):2.
Total 1 IP Group(s).
```

```

Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port(s).
    GE1/0/1                (D) ( 00:01:30 )
IP group(s):the following ip group(s) match to one mac group.
  IP group address:224.1.1.1
    (0.0.0.0, 224.1.1.1):
      Attribute:   Host Port
      Host port(s):total 1 port(s).
        GE1/0/2                (D) ( 00:03:23 )
MAC group(s):
  MAC group address:0100-5e01-0101
  Host port(s):total 1 port(s).
    GE1/0/2

```

Table 1 Command output

Field	Description
Total 1 IP Group(s).	Total number of IP multicast groups.
Total 1 IP Source(s).	Total number of multicast sources.
Total 1 MAC Group(s).	Total number of MAC multicast groups.
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port	Port flags: D —Dynamic port. S —Static port. C —Port copied from a (*, G) entry to an (S, G) entry. P —Port added by PIM snooping.
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R —Real egress sub-VLAN under the current entry. C —Sub-VLAN copied from a (*, G) entry to an (S, G) entry.
Router port(s)	Number of router ports.
(00:01:30)	Remaining time of the aging timer for the dynamic member port or router port.
IP group address	Address of IP multicast group.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where 0.0.0.0 implies any multicast source.
MAC group address	Address of MAC multicast group.
Attribute	Attribute of IP multicast group.
Host port(s)	Number of member ports.

display igmp-snooping host

Syntax

```

display igmp-snooping host vlan vlan-id group group-address [ source source-address ] [ slot slot-number ] [ { begin | exclude | include } regular-expression ]

```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays information about the hosts tracked by IGMP snooping in the specified VLAN, where *vlan-id* is in the range of 1 to 4094.

group *group-address*: Displays information about the hosts tracked by IGMP snooping that are in the specified IGMP snooping group. The value of *group-address* ranges from 224.0.1.0 to 239.255.255.255.

source *source-address*: Displays information about the hosts tracked by IGMP snooping that are in the specified multicast source, where *source-address* is a valid unicast address or 0.0.0.0. A source IP address of 0.0.0.0 specifies all multicast sources.

slot *slot-number*: Displays information about the hosts tracked by IGMP snooping on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device 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 igmp-snooping host** to display information about the hosts tracked by IGMP snooping.

Examples

```
# Display information about the hosts tracked by IGMP snooping in VLAN 2 that are in multicast group 224.1.1.1.
```

```
<Sysname> display igmp-snooping host vlan 2 group 224.1.1.1
VLAN(ID) : 2
(0.0.0.0, 224.1.1.1)
  Port : GigabitEthernet1/0/1
    Host                Uptime                Expires
    1.1.1.1              00:02:20              00:00:40
    2.2.2.2              00:02:21              00:00:39
  Port : GigabitEthernet1/0/2
    Host                Uptime                Expires
    3.3.3.3              00:02:20              00:00:40
```

Table 2 Command output

Field	Description
(0.0.0.0, 224.1.1.1)	(S, G) entry, where 0.0.0.0 indicates all multicast sources

Field	Description
Port	Member port
Host	Host IP address
Uptime	Host running duration
Expires	Host expiration time, where <i>timeout</i> means that the host has expired

display igmp-snooping statistics

Syntax

display igmp-snooping 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 igmp-snooping statistics** to display statistics for IGMP messages learned through IGMP snooping.

Examples

Display statistics for IGMP messages learned through IGMP snooping.

```
<Sysname> display igmp-snooping statistics
  Received IGMP general queries:0.
  Received IGMPv1 reports:0.
  Received IGMPv2 reports:19.
  Received IGMP leaves:0.
  Received IGMPv2 specific queries:0.
  Sent    IGMPv2 specific queries:0.
  Received IGMPv3 reports:1.
  Received IGMPv3 reports with right and wrong records:0.
  Received IGMPv3 specific queries:0.
  Received IGMPv3 specific sg queries:0.
  Sent    IGMPv3 specific queries:0.
  Sent    IGMPv3 specific sg queries:0.
  Received error IGMP messages:19.
```

Table 3 Command output

Field	Description
general queries	General query messages
specific queries	Group-specific query messages
reports	Report messages
leaves	Leave messages
reports with right and wrong records	Report messages with correct and incorrect records
specific sg query packet(s)	Group-and-source-specific query message or messages
error IGMP messages	IGMP messages with errors

display mac-address multicast

Syntax

```
display mac-address [ mac-address [ vlan vlan-id ] | [ multicast ] [ vlan vlan-id ] [ count ] ] [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

mac-address: Displays the multicast MAC address entry for the specified MAC address. The MAC address can be any multicast MAC address except 0100-5Exx-xxxx and 3333-xxxx-xxxx, where x represents an arbitrary hexadecimal number from 0 to F. A multicast MAC address is a MAC address whose the least significant bit of the most significant octet is 1.

vlan *vlan-id*: Displays multicast MAC address entries for the specified VLAN, where *vlan-id* is in the range of 1 to 4094. If you do not specify a VLAN, this command displays the static multicast MAC address entries for all VLANs.

multicast: Displays static multicast MAC address entries.

count: Displays the number of matched static multicast MAC address entries. With this argument specified, the number of matched static multicast MAC address entries is displayed, without displaying any content of the matched entries.

|: 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 mac-address multicast** to display the static multicast MAC address entries.

With no parameters specified or with only **vlan**, **count**, or both of them specified, this command displays all MAC address table entries, including static multicast MAC address entries and unicast MAC address entries.

Related commands: **mac-address multicast**; **display mac-address** (*Layer 2—LAN Switching Command Reference*).

Examples

Display the static multicast MAC address entries for VLAN 2.

```
<Sysname> display mac-address multicast vlan 2
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
0100-0001-0001    2        Multicast      GigabitEthernet1/0/1 NOAGED
                  GigabitEthernet1/0/2
                  GigabitEthernet1/0/3
                  GigabitEthernet1/0/4

--- 1 mac address(es) found ---
```

Table 4 Command output

Field	Description
MAC ADDR	MAC address.
VLAN ID	ID of the VLAN to which the network device identified by the MAC address belongs.
STATE	Status of the MAC address; multicast indicates a static multicast MAC address entry.
PORT INDEX	Outgoing ports of the multicast MAC address entry.
AGING TIME(s)	State of the aging timer. The aging timer for static multicast MAC addresses has only one state NOAGED , which indicates that this entry never expires.
1 mac address(es) found	One static multicast MAC address entry is found.

dot1p-priority (IGMP-snooping view)

Syntax

dot1p-priority *priority-number*

undo dot1p-priority

View

IGMP-snooping view

Default level

2: System level

Parameters

priority-number: Specifies an 802.1p precedence for IGMP messages, in the range of 0 to 7. A higher number indicates a higher precedence.

Description

Use **dot1p-priority** to set the 802.1p precedence for IGMP messages globally.

Use **undo dot1p-priority** to restore the default.

The default 802.1p precedence for IGMP messages is 0.

Examples

```
# Set the 802.1p precedence for IGMP messages to 3 globally.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dot1p-priority 3
```

dscp (IGMP-snooping view)

Syntax

```
dscp dscp-value
undo dscp
```

View

IGMP-snooping view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value for IGMP messages, in the range of 0 to 63.

Description

Use **dscp** to set the DSCP value for IGMP messages.

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

The default DSCP value in IGMP messages is 48.

This command applies to only the IGMP messages that the local switch generates when the switch or its port acts as a member host, rather than those forwarded ones.

Examples

```
# Set the DSCP value to 63 for IGMP messages.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dscp 63
```

fast-leave (IGMP-snooping view)

Syntax

```
fast-leave [ vlan vlan-list ]
undo fast-leave [ vlan vlan-list ]
```

View

IGMP-snooping view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command takes effect for all VLANs. If you specify one or more VLANs, the command takes effect for the specified VLANs only.

Description

Use **fast-leave** to enable fast-leave processing globally. With this function enabled, when the switch receives an IGMP leave message on a port, it directly removes that port from the multicast forwarding entry of the specific group.

Use **undo fast-leave** to disable fast-leave processing globally.

By default, fast-leave processing is disabled.

For the HP 5500 EI switches, this command takes effect in both IGMP snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in IGMP snooping-enabled VLANs.

Related commands: **igmp-snooping fast-leave**.

Examples

```
# Enable fast-leave processing in VLAN 2 globally.  
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] fast-leave vlan 2
```

group-policy (IGMP-snooping view)

Syntax

group-policy *acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

View

IGMP-snooping view

Default level

2: System level

Parameters

acl-number: Specifies a basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule matches the multicast source addresses specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX or TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command takes effect for all VLANs. If you specify one or more VLANs, the command takes effect for the specified VLANs only.

Description

Use **group-policy** to configure a global multicast group filter, namely, to control the multicast groups that a host can join.

Use **undo group-policy** to remove the configured global multicast group filter.

By default, no global multicast group filter is configured. Namely, a host can join any valid multicast group.

If the specified ACL does not exist or the ACL rule is null, all multicast groups are filtered out.

You can configure different ACL rules for a port in different VLANs. For a given VLAN, a newly configured ACL rule overrides the existing one.

Related commands: **igmp-snooping group-policy**.

Examples

Apply ACL 2000 as a multicast group filter in VLAN 2 so that hosts in this VLAN can join 225.1.1.1 only.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] igmp-snooping
[Sysname-igmp-snooping] group-policy 2000 vlan 2
```

host-aging-time (IGMP-snooping view)

Syntax

host-aging-time *interval*

undo host-aging-time

View

IGMP-snooping view

Default level

2: System level

Parameters

interval: Specifies an aging timer in seconds for dynamic member ports. The value ranges from 200 to 1000.

Description

Use **host-aging-time** to configure the aging timer for dynamic member ports globally.

Use **undo host-aging-time** to restore the default.

By default, the aging timer of a dynamic member port is 260 seconds.

This command takes effect only in IGMP snooping-enabled VLANs.

Related commands: **igmp-snooping host-aging-time**.

Examples

Set the aging timer for dynamic member ports to 300 seconds globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
```

```
[Sysname-igmp-snooping] host-aging-time 300
```

host-tracking (IGMP-snooping view)

Syntax

host-tracking

undo host-tracking

View

IGMP-snooping view

Default level

2: System level

Parameters

None

Description

Use **host-tracking** to enable the IGMP snooping host tracking function globally.

Use **undo host-tracking** to disable the IGMP snooping host tracking function globally.

By default, this function is disabled.

This command takes effect only in IGMP snooping-enabled VLANs.

Related commands: **display igmp-snooping host** and **igmp-snooping host-tracking**.

Examples

```
# Enable the IGMP snooping host tracking function globally.
```

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

```
[Sysname] igmp-snooping
```

```
[Sysname-igmp-snooping] host-tracking
```

igmp-snooping

Syntax

igmp-snooping

undo igmp-snooping

View

System view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping** to enable IGMP snooping globally and enter IGMP-snooping view.

Use **undo igmp-snooping** to disable IGMP snooping globally.

By default, IGMP snooping is disabled.

Related commands: **igmp-snooping enable**.

Examples

```
# Enable IGMP snooping globally and enter IGMP-snooping view.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping]
```

igmp-snooping access-policy

Syntax

```
igmp-snooping access-policy acl-number
undo igmp-snooping access-policy { acl-number | all }
```

View

User profile view

Default level

2: System level

Parameters

acl-number: Specifies a basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL matches the multicast source address or addresses specified in IGMPv3 reports, rather than the source addresses of the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX and TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

all: Specifies all ACLs.

Description

Use **igmp-snooping access-policy** to configure a multicast user control policy.

Use **undo igmp-snooping access-policy** to remove the configuration.

By default, no user control policy is configured. Namely, a user can join any valid multicast group.

You can use this command repeatedly to configure multiple multicast user control policies.

Examples

```
# Create and enable a user profile named abc to allow users to join 225.1.1.1 only.
```

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2001] quit
[Sysname] user-profile abc
[Sysname-user-profile-abc] igmp-snooping access-policy 2001
[Sysname-user-profile-abc] quit
[Sysname] user-profile abc enable
```


igmp-snooping dot1p-priority

Syntax

```
igmp-snooping dot1p-priority priority-number  
undo igmp-snooping dot1p-priority
```

View

VLAN view

Default level

2: System level

Parameters

priority-number: Specifies an 802.1p precedence for IGMP messages, in the range of 0 to 7. A higher number indicates a higher precedence.

Description

Use **igmp-snooping dot1p-priority** to set the 802.1p precedence for the IGMP messages in a VLAN.

Use **undo igmp-snooping dot1p-priority** to restore the default.

The default 802.1p precedence for the IGMP messages in a VLAN is 0.

Before you configure this command in a VLAN, enable IGMP snooping in the VLAN.

Related commands: **igmp-snooping enable**.

Examples

```
# Enable IGMP snooping in VLAN 2 and set the 802.1p precedence for the IGMP messages in the VLAN to 3.
```

```
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] quit  
[Sysname] vlan 2  
[Sysname-vlan2] igmp-snooping enable  
[Sysname-vlan2] igmp-snooping dot1p-priority 3
```

igmp-snooping drop-unknown

Syntax

```
igmp-snooping drop-unknown  
undo igmp-snooping drop-unknown
```

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping drop-unknown** to enable dropping unknown multicast data for a VLAN.

Use **undo igmp-snooping drop-unknown** to disable dropping unknown multicast data for a VLAN.

By default, this function is disabled. That is, unknown multicast data is flooded.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**.

Examples

In VLAN 2, enable IGMP snooping and the function of dropping unknown multicast data.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping drop-unknown
```

igmp-snooping enable

Syntax

igmp-snooping enable

undo igmp-snooping enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping enable** to enable IGMP snooping for a VLAN.

Use **undo igmp-snooping enable** to disable IGMP snooping for a VLAN.

By default, IGMP snooping is disabled in a VLAN.

IGMP snooping must be enabled globally before it can be enabled in a VLAN.

Related commands: **igmp-snooping**.

Examples

Enable IGMP snooping in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
```

igmp-snooping fast-leave

Syntax

```
igmp-snooping fast-leave [ vlan vlan-list ]  
undo igmp-snooping fast-leave [ vlan vlan-list ]
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **igmp-snooping fast-leave** to enable fast-leave processing on the current port or group of ports. With this function enabled, when the switch receives an IGMP leave message on a port, it directly removes that port from the multicast forwarding entry of the specific group.

Use **undo igmp-snooping fast-leave** to disable fast-leave processing on the current port or group of ports. By default, fast-leave processing is disabled.

For the HP 5500 EI switches, this command takes effect in both IGMP snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in IGMP snooping-enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **fast-leave**.

Examples

```
# Enable fast-leave processing on GigabitEthernet 1/0/1 in VLAN 2.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] igmp-snooping fast-leave vlan 2
```

igmp-snooping general-query source-ip

Syntax

```
igmp-snooping general-query source-ip { ip-address | current-interface }  
undo igmp-snooping general-query source-ip
```

View

VLAN view

Default level

2: System level

Parameters

ip-address: Specifies the source address of IGMP general queries, which can be any legal IP address.

current-interface: Sets the source address of IGMP general queries to the address of the current VLAN interface. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 is used as the source IP address of IGMP general queries.

Description

Use **igmp-snooping general-query source-ip** to configure the source address of IGMP general queries.

Use **undo igmp-snooping general-query source-ip** to restore the default.

By default, the source IP address of IGMP general queries is 0.0.0.0.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**.

Examples

In VLAN 2, enable IGMP snooping and specify 10.1.1.1 as the source IP address of IGMP general queries.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping general-query source-ip 10.1.1.1
```

igmp-snooping group-limit

Syntax

igmp-snooping group-limit *limit* [**vlan** *vlan-list*]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

limit: Specifies the maximum number of multicast groups that a port can join. For the HP 5500 EI switches, the value ranges from 0 to 2000. For the HP 5500 SI switches, the value ranges from 0 to 1000.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **igmp-snooping group-limit** to set the maximum number of multicast groups that a port can join.

Use **undo igmp-snooping group-limit** to restore the default.

By default, the upper limit is 2000 for the HP 5500 EI switches, and 1000 for the HP 5500 SI switches.

For the HP 5500 EI switches, you can also use the **igmp group-limit** command to limit the number of multicast groups that an interface can join. However, if you configure the limit both in a VLAN and on a VLAN interface of this VLAN by using these two commands, inconsistencies might exist between Layer 2 and Layer 3 table entries. Therefore, HP recommends you to configure the limit only on the VLAN interface.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **igmp group-limit**.

Examples

```
# Specify to allow GigabitEthernet 1/0/1 in VLAN 2 to join up to 10 multicast groups.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-limit 10 vlan 2
```

igmp-snooping group-policy

Syntax

```
igmp-snooping group-policy acl-number [ vlan vlan-list ]
```

```
undo igmp-snooping group-policy [ vlan vlan-list ]
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

acl-number: Specifies a basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule matches the multicast source address or addresses specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX and TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **igmp-snooping group-policy** to configure a multicast group filter on the current port, namely, to control the multicast groups that the hosts on the port can join.

Use **undo igmp-snooping group-policy** to remove a multicast group filter.

By default, no multicast group filter is configured on an interface. Namely, a host can join any valid multicast group.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

If the specified ACL does not exist or the ACL rule is null, all multicast groups are filtered out.

You can configure different ACL rules for a port in different VLANs. For a given VLAN, a newly configured ACL rule overrides the existing one.

Related commands: **group-policy**.

Examples

```
# Apply ACL 2000 as a multicast group filter so that hosts on GigabitEthernet 1/0/1 in VLAN 2 can join 225.1.1.1 only.
```

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
```

igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *interval*

undo igmp-snooping host-aging-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an aging timer in seconds for dynamic member ports. The value ranges from 200 to 1000.

Description

Use **igmp-snooping host-aging-time** to set the aging timer for dynamic member ports for a VLAN.

Use **undo igmp-snooping host-aging-time** to restore the default.

By default, the aging time of a dynamic member port is 260 seconds.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **host-aging-time** and **igmp-snooping enable**.

Examples

```
# Enable IGMP snooping and set the aging timer for dynamic member ports in VLAN 2 to 300 seconds.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping host-aging-time 300
```

igmp-snooping host-join

Syntax

igmp-snooping host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

group-address: Specifies the address of the multicast group that the simulated host will join, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Specifies the address of the multicast source that the simulated host will join. The value of this argument should be a valid unicast address or 0.0.0.0. A source IP address of 0.0.0.0 specifies all multicast sources.

vlan *vlan-id*: Specifies the VLAN that comprises the ports, where *vlan-id* is in the range of 1 to 4094.

Description

Use **igmp-snooping host-join** to enable simulated joining on a port. That is, you configure the port as a simulated member host for the specified multicast group or source and group.

Use **undo igmp-snooping host-join** to remove the simulated member hosts from the specified multicast group or source and group.

By default, this function is disabled.

For the HP 5500 EI switches, this command takes effect in both IGMP snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces. The version of IGMP on the simulated host is consistent with the version of IGMP snooping that is running in the VLAN or the version of IGMP that is running on the VLAN interface.

For the HP 5500 SI switches, this command takes effect in IGMP snooping-enabled VLANs. The IGMP version on the simulated member host is consistent with the version of IGMP snooping that is running in the VLAN.

The **source-ip source-address** option in the command is meaningful only for IGMPv3 snooping. If IGMPv2 snooping is running, the **source-ip source-address** option does not take effect although you can include **source-ip source-address** in the command.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN.

In port group view, this command takes effect only on the ports in this port group that belong to the specified VLAN.

Examples

```
# Configure GigabitEthernet 1/0/1 as a simulated member host in VLAN 2 for multicast source 1.1.1.1 and multicast group 232.1.1.1.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping host-join 232.1.1.1 source-ip 1.1.1.1 vlan 2
```

igmp-snooping host-tracking

Syntax

```
igmp-snooping host-tracking
undo igmp-snooping host-tracking
```

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping host-tracking** to enable the IGMP snooping host tracking function in a VLAN.

Use **undo igmp-snooping host-tracking** to disable the IGMP snooping host tracking function in a VLAN.

By default, this function is disabled.

Before you configure this command, enable IGMP snooping in the VLAN first.

Related commands: **display igmp-snooping host**, **host-tracking**, and **igmp-snooping enable**.

Examples

```
# Enable IGMP snooping and IGMP snooping host tracking in VLAN 2.
<Sysname> system-view
[Sysname] igmp-snooping
```



```
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping host-tracking
```

igmp-snooping last-member-query-interval

Syntax

```
igmp-snooping last-member-query-interval interval
undo igmp-snooping last-member-query-interval
```

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies the IGMP last-member query interval in seconds. The value ranges from 1 to 5.

Description

Use **igmp-snooping last-member-query-interval** to set the IGMP last-member query interval in the VLAN.

Use **undo igmp-snooping last-member-query-interval** to restore the default.

By default, the IGMP last-member query interval is 1 second.

The IGMP last-member query interval determines the interval for sending IGMP group-specific queries and the maximum response delay for IGMP group-specific queries in a VLAN.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable** and **last-member-query-interval**.

Examples

```
# Enable IGMP snooping and set the IGMP last-member query interval to 3 seconds in VLAN 2.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping last-member-query-interval 3
```

igmp-snooping leave source-ip

Syntax

```
igmp-snooping leave source-ip { ip-address | current-interface }
undo igmp-snooping leave source-ip
```

View

VLAN view

Default level

2: System level

Parameters

ip-address: Specifies a source address for the IGMP leave messages that the IGMP snooping proxy sends, which can be any legal IP address.

current-interface: Specifies the IP address of the current VLAN interface as the source address of IGMP leave messages that the IGMP snooping proxy sends. If no IP address has been assigned to the current VLAN interface, the default IP address 0.0.0.0 is used.

Description

Use **igmp-snooping leave source-ip** to configure the source IP address of the IGMP leave messages that the IGMP snooping proxy sends.

Use **undo igmp-snooping leave source-ip** to restore the default.

By default, the source IP address of the IGMP leave messages that the IGMP snooping proxy sends is 0.0.0.0.

Before you configure this command in a VLAN, enable IGMP snooping in the VLAN.

The source IP address configured in the **igmp-snooping leave source-ip** command also applies when the simulated host sends IGMP leave messages.

Related commands: **igmp-snooping enable**.

Examples

Enable IGMP snooping in VLAN 2 and configure the source IP address of IGMP leave messages that the IGMP snooping proxy sends in VLAN 2 to 10.1.1.1.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping leave source-ip 10.1.1.1
```

igmp-snooping max-response-time

Syntax

igmp-snooping max-response-time *interval*

undo igmp-snooping max-response-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for IGMP general queries in seconds. The value ranges from 1 to 25.

Description

Use **igmp-snooping max-response-time** to configure the maximum response delay for IGMP general queries in the VLAN.

Use **undo igmp-snooping max-response-time** to restore the default.

By default, the maximum response delay for IGMP general queries is 10 seconds.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**, **igmp-snooping query-interval**, and **max-response-time**.

Examples

Enable IGMP snooping and set the maximum response delay for IGMP general queries to 5 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping max-response-time 5
```

igmp-snooping overflow-replace

Syntax

igmp-snooping overflow-replace [**vlan** *vlan-list*]

undo igmp-snooping overflow-replace [**vlan** *vlan-list*]

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **igmp-snooping overflow-replace** to enable the multicast group replacement function on the current port.

Use **undo igmp-snooping overflow-replace** to disable the multicast group replacement function.

By default, the multicast group replacement function is disabled.

For the HP 5500 EI switches, this command takes effect in both IGMP snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in IGMP snooping-enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you

specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **overflow-replace**.

Examples

```
# Enable the multicast group replacement function on GigabitEthernet 1/0/1 in VLAN 2.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping overflow-replace vlan 2
```

igmp-snooping proxying enable

Syntax

```
igmp-snooping proxying enable
undo igmp-snooping proxying enable
```

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping proxying enable** to enable the IGMP snooping proxying function in a VLAN.

Use **undo igmp-snooping proxying enable** to disable the IGMP snooping proxying function in a VLAN.

By default, IGMP snooping proxying is disabled in all VLANs.

Before you configure this command in a VLAN, enable IGMP snooping in the VLAN.

Related commands: **igmp-snooping enable**.

Examples

```
# Enable IGMP snooping and then IGMP snooping proxying in VLAN 2.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping proxying enable
```

igmp-snooping querier

Syntax

```
igmp-snooping querier
```

undo igmp-snooping querier

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping querier** to enable the IGMP snooping querier function.

Use **undo igmp-snooping querier** to disable the IGMP snooping querier function.

By default, the IGMP snooping querier function is disabled.

This command takes effect only if IGMP snooping is enabled in the VLAN.

This command does not take effect in a sub-VLAN of a multicast VLAN.

Related commands: **igmp-snooping enable** and **subvlan**.

Examples

```
# Enable IGMP snooping and the IGMP snooping querier function in VLAN 2.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping querier
```

igmp-snooping query-interval

Syntax

```
igmp-snooping query-interval interval
```

```
undo igmp-snooping query-interval
```

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an interval in seconds for sending IGMP general queries. The value ranges from 2 to 300.

Description

Use **igmp-snooping query-interval** to configure the interval for sending IGMP general queries.

Use **undo igmp-snooping query-interval** to restore the default.

By default, the IGMP general query interval is 60 seconds.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**, **igmp-snooping max-response-time**, **igmp-snooping querier**, and **max-response-time**.

Examples

```
# Enable IGMP snooping and set the interval for sending IGMP general queries to 20 seconds in VLAN 2.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping query-interval 20
```

igmp-snooping report source-ip

Syntax

```
igmp-snooping report source-ip { ip-address | current-interface }
undo igmp-snooping report source-ip
```

View

VLAN view

Default level

2: System level

Parameters

ip-address: Specifies a source address for the IGMP reports that the IGMP snooping proxy sends. The address can be any legal IP address.

current-interface: Specifies the IP address of the current VLAN interface as the source address of IGMP reports that the IGMP snooping proxy sends. If no IP address has been assigned to the current VLAN interface, the default IP address 0.0.0.0 is used.

Description

Use **igmp-snooping report source-ip** to configure the source IP address of the IGMP reports that the IGMP snooping proxy sends.

Use **undo igmp-snooping report source-ip** to restore the default.

By default, the source IP address of the IGMP reports that the IGMP snooping proxy sends is 0.0.0.0.

Before you configure this command in a VLAN, enable IGMP snooping in the VLAN.

The source IP address configured in the **igmp-snooping report source-ip** command also applies when the simulated host sends IGMP reports.

Related commands: **igmp-snooping enable**.

Examples

```
# Enable IGMP snooping in VLAN 2 and configure the source IP address of IGMP reports that the IGMP snooping proxy sends in VLAN 2 to 10.1.1.1.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
```

```
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping report source-ip 10.1.1.1
```

igmp-snooping router-aging-time

Syntax

```
igmp-snooping router-aging-time interval
undo igmp-snooping router-aging-time
```

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an aging timer for dynamic router ports in seconds. The value ranges from 1 to 1000.

Description

Use **igmp-snooping router-aging-time** to configure the aging timer for dynamic router ports for a VLAN.

Use **undo igmp-snooping router-aging-time** to restore the default.

By default, the aging timer of a dynamic router port is 105 seconds.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable** and **router-aging-time**.

Examples

Enable IGMP snooping and set the aging timer for dynamic router ports to 100 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping router-aging-time 100
```

igmp-snooping router-port-deny

Syntax

```
igmp-snooping router-port-deny [ vlan vlan-list ]
undo igmp-snooping router-port-deny [ vlan vlan-list ]
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **igmp-snooping router-port-deny** to disable a port from becoming a dynamic router port.

Use **undo igmp-snooping router-port-deny** to restore the default.

By default, a port can become a dynamic router port.

For the HP 5500 EI switches, this command takes effect in both IGMP snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in IGMP snooping-enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Examples

```
# Disable GigabitEthernet 1/0/1 from becoming a dynamic router port in VLAN 2.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping router-port-deny vlan 2
```

igmp-snooping source-deny

Syntax

igmp-snooping source-deny

undo igmp-snooping source-deny

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping source-deny** to enable multicast source port filtering.

Use **undo igmp-snooping source-deny** to disable multicast source port filtering.

By default, multicast source port filtering is disabled.

For the HP 5500 EI switches, this command takes effect in both IGMP snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in IGMP snooping-enabled VLANs.

Examples

```
# Enable source port filtering for multicast data on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping source-deny
```

igmp-snooping special-query source-ip

Syntax

```
igmp-snooping special-query source-ip { ip-address | current-interface }
undo igmp-snooping special-query source-ip
```

View

VLAN view

Default level

2: System level

Parameters

ip-address: Specifies a source address for IGMP group-specific queries.

current-interface: Specifies the address of the current VLAN interface as the source address of IGMP group-specific queries. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 is used as the source IP address of IGMP group-specific queries.

Description

Use **igmp-snooping special-query source-ip** to configure the source IP address for IGMP group-specific queries.

Use **undo igmp-snooping special-query source-ip** to restore the default.

By default, the source IP address of IGMP group-specific queries is 0.0.0.0.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**.

Examples

```
# In VLAN 2, enable IGMP snooping and specify 10.1.1.1 as the source IP address of IGMP
group-specific queries.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping special-query source-ip 10.1.1.1
```

igmp-snooping static-group

Syntax

```
igmp-snooping static-group group-address [ source-ip source-address ] vlan vlan-id  
undo igmp-snooping static-group group-address [ source-ip source-address ] vlan vlan-id
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

group-address: Specifies the address of the multicast group that the port joins as a static member port, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Specifies the address of the multicast source that the port joins as a static member port. The value of this argument should be a valid unicast address or 0.0.0.0. A source IP address of 0.0.0.0 means no restriction on the multicast source.

vlan *vlan-id*: Specifies the VLAN that comprises the ports, where *vlan-id* is in the range of 1 to 4094.

Description

Use **igmp-snooping static-group** to configure the static (*, G) or (S, G) entry for the port, namely, to configure the port as a static member port of the specified multicast group or source-group.

Use **undo igmp-snooping static-group** to restore the default.

By default, no ports are static member ports.

The **source-ip source-address** option in the command is meaningful only for IGMPv3 snooping. If IGMPv2 snooping is running, the **source-ip source-address** option does not take effect although you can include **source-ip source-address** in the command.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN.

In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Examples

```
# Configure GigabitEthernet 1/0/1 in VLAN 2 to be a static member port for (1.1.1.1, 232.1.1.1).  
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] quit  
[Sysname] vlan 2  
[Sysname-vlan2] igmp-snooping enable  
[Sysname-vlan2] igmp-snooping version 3  
[Sysname-vlan2] quit  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-group 232.1.1.1 source-ip 1.1.1.1  
vlan 2
```

igmp-snooping static-router-port

Syntax

```
igmp-snooping static-router-port vlan vlan-id  
undo igmp-snooping static-router-port vlan vlan-id
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-id*: Specifies a VLAN, where *vlan-id* is in the range of 1 to 4094.

Description

Use **igmp-snooping static-router-port** to configure the current port as a static router port.

Use **undo igmp-snooping static-router-port** to restore the default.

By default, no ports are static router ports.

For the HP 5500 EI switches, this command takes effect in both IGMP snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in IGMP snooping-enabled VLANs.

This command does not take effect in a sub-VLAN of a multicast VLAN.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN.

In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Related commands: **subvlan**.

Examples

```
# Configure GigabitEthernet 1/0/1 in VLAN 2 as a static router port.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-router-port vlan 2
```

igmp-snooping version

Syntax

```
igmp-snooping version version-number  
undo igmp-snooping version
```

View

VLAN view

Default level

2: System level

Parameters

version-number: Specifies an IGMP snooping version, in the range of 2 to 3.

Description

Use **igmp-snooping version** to configure the IGMP snooping version.

Use **undo igmp-snooping version** to restore the default.

By default, the IGMPv2 snooping is used.

This command can take effect only if IGMP snooping is enabled in the VLAN.

This command does not take effect in a sub-VLAN of a multicast VLAN.

Related commands: **igmp-snooping enable** and **subvlan**.

Examples

```
# Enable IGMP snooping in VLAN 2, and specify IGMPv3 snooping.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
```

last-member-query-interval (IGMP-snooping view)

Syntax

```
last-member-query-interval interval
undo last-member-query-interval
```

View

IGMP-snooping view

Default level

2: System level

Parameters

interval: Specifies the IGMP last-member query interval in seconds. The value ranges from 1 to 5.

Description

Use **last-member-query-interval** to set the IGMP last-member query interval globally.

Use **undo last-member-query-interval** to restore the default.

By default, the IGMP last-member query interval is 1 second.

The IGMP last-member query interval determines the interval for sending IGMP group-specific queries and the maximum response delay for IGMP group-specific queries.

This command takes effect only in IGMP snooping-enabled VLANs.

Related commands: **igmp-snooping last-member-query-interval**.

Examples

```
# Set the IGMP last-member query interval to 3 seconds globally.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] last-member-query-interval 3
```

mac-address multicast

Syntax

In system view:

```
mac-address multicast mac-address interface interface-list vlan vlan-id
```

```
undo mac-address [ multicast ] [ [ mac-address [ interface interface-list ] ] ] vlan vlan-id ]
```

In Ethernet interface view or Layer 2 aggregate interface view:

```
mac-address multicast mac-address vlan vlan-id
```

```
undo mac-address [ multicast ] mac-address vlan vlan-id
```

In port group view:

```
mac-address multicast mac-address vlan vlan-id
```

```
undo mac-address multicast mac-address vlan vlan-id
```

View

System view, Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

mac-address: Specifies a static multicast MAC address, which can be any multicast MAC address except 0100-5Exx-xxxx and 3333-xxxx-xxxx, where x represents an arbitrary hexadecimal number from 0 to F. A multicast MAC address is a MAC address whose the least significant bit of the most significant octet is 1. The system gives a prompt if the configured static multicast MAC address conflicts with the MAC address of other protocols.

interface-list: Specifies a list of interfaces. You can specify up to **n** single interfaces, interface ranges, or combinations of both for the list. A single interface takes the form of *interface-type interface-number*. An interface range takes the form of *interface-type interface-number to interface-type interface-number*, where the end interface number must be greater than the start interface number.

vlan *vlan-id*: Specifies the VLAN to which the interface belongs. *vlan-id* is in the range of 1 to 4094. The specified VLAN must exist and the system gives a prompt if the specified interface does not belong to the VLAN.

Description

Use **mac-address multicast** to configure a static multicast MAC address entry.

Use **undo mac-address multicast** to delete a static multicast MAC address entry.

By default, no static multicast MAC address entry is configured.

If **multicast** is not specified when using the **undo mac-address multicast** command, all MAC address entries (including static multicast MAC address entries and unicast MAC address entries) are deleted.

Related commands: **display mac-address multicast**; **mac-address** (*Layer 2—LAN Switching Command Reference*).

Examples

Configure a static multicast MAC address entry with the MAC address of 0100-0001-0001 and outgoing interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 in VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address multicast 0100-0001-0001 interface gigabitethernet 1/0/1 to
gigabitethernet 1/0/5 vlan 2
```

Configure a static multicast MAC address entry with the MAC address of 0100-0001-0001 in interface view of GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address multicast 0100-0001-0001 vlan 2
```

max-response-time (IGMP-snooping view)

Syntax

max-response-time *interval*

undo max-response-time

View

IGMP-snooping view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for IGMP general queries in seconds. The value ranges from 1 to 25.

Description

Use **max-response-time** to set the maximum response delay for IGMP general queries globally.

Use **undo max-response-time** to restore the default.

This command takes effect only in IGMP snooping-enabled VLANs.

Related commands: **igmp-snooping max-response-time** and **igmp-snooping query-interval**.

Examples

Set the maximum response delay for IGMP general queries globally to 5 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] max-response-time 5
```

overflow-replace (IGMP-snooping view)

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

View

IGMP-snooping view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command takes effect for all VLANs. If you specify one or more VLANs, the command takes effect for the specified VLANs only.

Description

Use **overflow-replace** to enable the multicast group replacement function globally.

Use **undo overflow-replace** to disable the multicast group replacement function globally.

By default, the multicast group replacement function is disabled.

For the HP 5500 EI switches, this command takes effect in both IGMP snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in IGMP snooping-enabled VLANs.

Related commands: **igmp-snooping overflow-replace**.

Examples

```
# Enable the multicast group replacement function globally in VLAN 2.
```

```
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] overflow-replace vlan 2
```

report-aggregation (IGMP-snooping view)

Syntax

report-aggregation

undo report-aggregation

View

IGMP-snooping view

Default level

2: System level

Parameters

None

Description

Use **report-aggregation** to enable IGMP report suppression.

Use **undo report-aggregation** to disable IGMP report suppression.

By default, IGMP report suppression is enabled.

For the HP 5500 EI switches, this command takes effect in both IGMP snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in IGMP snooping-enabled VLANs.

Examples

```
# Disable IGMP report suppression.  
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] undo report-aggregation
```

reset igmp-snooping group

Syntax

```
reset igmp-snooping group { group-address | all } [ vlan vlan-id ]
```

View

User view

Default level

2: System level

Parameters

group-address: Specifies an IGMP snooping group. The value range of *group-address* is 224.0.1.0 to 239.255.255.255.

all: Specifies all IGMP snooping groups.

vlan *vlan-id*: Specifies a VLAN. The value range of *vlan-id* is 1 to 4094.

Description

Use **reset igmp-snooping group** to remove the dynamic group entries of the specified IGMP snooping groups.

This command takes effect only in IGMP snooping-enabled VLANs.

This command cannot remove the static group entries of IGMP snooping groups.

Examples

```
# Remove the dynamic group entries of all IGMP snooping groups.  
<Sysname> reset igmp-snooping group all
```

reset igmp-snooping statistics

Syntax

```
reset igmp-snooping statistics
```

View

User view

Default level

2: System level

Parameters

None

Description

Use **reset igmp-snooping statistics** to clear statistics for the IGMP messages learned by IGMP snooping.

Examples

```
# Clear statistics for the IGMP messages learned by IGMP snooping.  
<Sysname> reset igmp-snooping statistics
```

router-aging-time (IGMP-snooping view)

Syntax

```
router-aging-time interval  
undo router-aging-time
```

View

IGMP-snooping view

Default level

2: System level

Parameters

interval: Specifies an aging timer in seconds for dynamic router ports. The value ranges from 1 to 1000.

Description

Use **router-aging-time** to set the aging timer for dynamic router ports globally.

Use **undo router-aging-time** to restore the default.

By default, the aging timer of a dynamic router port is 105 seconds.

This command takes effect only in IGMP snooping-enabled VLANs.

Related commands: **igmp-snooping router-aging-time**.

Examples

```
# Set the aging timer for dynamic router ports to 100 seconds globally.  
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] router-aging-time 100
```

source-deny (IGMP-snooping view)

Syntax

```
source-deny port interface-list  
undo source-deny port interface-list
```

View

IGMP-snooping view

Default level

2: System level

Parameters

interface-list: Specifies one or multiple ports. You can provide up to 10 port lists. For each list, you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of

interface-type start-interface-number to interface-type end-interface-number, where the end interface number must be greater than the start interface number.

Description

Use **source-deny** to enable multicast source port filtering so that all multicast data packets are blocked.

Use **undo source-deny** to disable multicast source port filtering.

By default, multicast source port filtering is not enabled.

For the HP 5500 EI switches, this command takes effect in both IGMP snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in IGMP snooping-enabled VLANs.

Examples

Enable source port filtering for multicast data on interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

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

```
[Sysname] igmp-snooping
```

```
[Sysname-igmp-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

PIM snooping configuration commands

display pim-snooping neighbor

Syntax

```
display pim-snooping neighbor [ vlan vlan-id ] [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the PIM snooping neighbor information of the specified VLAN. The *vlan-id* argument is in the range of 1 to 4094. If no VLAN is specified, this command displays the PIM snooping neighbor information of all VLANs.

slot *slot-number*: Displays the PIM snooping neighbor information of the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device 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 pim-snooping neighbor** to display PIM snooping neighbor information.

Examples

```
# Display information about PIM snooping neighbors in VLAN 2.
```

```
<Sysname> display pim-snooping neighbor vlan 2
```

```
Total number of neighbors: 2
```

```
VLAN ID: 2
```

```
Total number of neighbors: 2
```

Neighbor	Port	Expires	Option	Flags
10.1.1.2	GE1/0/1	02:02:23	LAN Prune	Delay(T)
20.1.1.2	GE1/0/2	03:00:05	LAN Prune	Delay

Table 5 Command output

Field	Description
Total number of neighbors	Total number of PIM snooping neighbors.
Neighbor	IP address of the PIM snooping neighbor.
Port	Name of the port that connects to the PIM snooping neighbor.
Expires	Remaining time before the PIM snooping neighbor expires. <i>Never</i> means the PIM snooping neighbor never expires.
Option Flags	<p>Possible values includes the following items:</p> <ul style="list-style-type: none"> • LAN Prune Delay—Indicates that the PIM hello messages received from the neighbor carry the LAN_Prune_Delay option. • LAN Prune Delay(T)—Indicates that the PIM hello messages received from the neighbor carry the LAN_Prune_Delay option, and the join suppression function has been disabled

display pim-snooping routing-table

Syntax

```
display pim-snooping routing-table [ vlan vlan-id ] [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the PIM snooping routing entries of the specified VLAN. The *vlan-id* argument is in the range of 1 to 4094. If no VLAN is specified, this command displays the PIM snooping routing entries in all VLANs.

slot *slot-number*: Displays the PIM snooping routing entries on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device 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 pim-snooping routing-table** to display PIM snooping routing entries.

Examples

```
# Display the PIM snooping routing entries of VLAN 2.
```

```

<Sysname> display pim-snooping routing-table vlan 2 slot 1
Total 1 entry(ies)
FSM Flag: NI-no info, J-join, PP-prune pending

VLAN ID: 2
Total 2 entry(ies)
(172.10.10.1, 225.1.1.1)
Upstream neighbor: 20.1.1.1
Upstream port: GE1/0/1
Total number of downstream ports: 1
1: GE1/0/3
Expires: 00:03:01, FSM: J
Upstream neighbor: 10.1.1.1
Upstream port: GE1/0/2
Total number of downstream ports: 1
1: GE1/0/4
Expires: 00:01:05, FSM: J

```

Table 6 Command output

Field	Description
Total 1 entry(ies)	Total number of (S, G) entries and (*, G) entries in the PIM snooping routing table
FSM Flag: NI-no info, J-join, PP-prune pending	State machine flag of the downstream port. Possible values include: <ul style="list-style-type: none"> • NI—Initial state • J—Join • PP—Prune pending
(172.10.10.1, 225.1.1.1)	(S, G) entry
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry
Upstream port	Upstream port of the (S, G) entry or (*, G) entry
Expires	Expiration time of the downstream port
FSM	State machine flag of the downstream port

display pim-snooping statistics

Syntax

```
display pim-snooping 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 pim-snooping statistics** to display statistics for the PIM messages learned by PIM snooping.

Examples

Display statistics for the PIM messages learned by PIM snooping.

```
<Sysname> display pim-snooping statistics
Received PIMv2 hello: 100
Received PIMv2 join/prune: 100
Received PIMv2 error: 0
Received PIMv2 messages in total: 200
Received PIMv1 messages in total: 0
```

Table 7 Command output

Field	Description
Received PIMv2 hello	Number of received PIMv2 hello messages
Received PIMv2 join/prune	Number of received PIMv2 join/prune messages
Received PIMv2 error	Number of received PIMv2 messages with errors
Received PIMv2 messages in total	Total number of received PIMv2 messages
Received PIMv1 messages in total	Total number of received PIMv1 messages

pim-snooping enable

Syntax

pim-snooping enable

undo pim-snooping enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **pim-snooping enable** to enable PIM snooping in a VLAN.

Use **undo pim-snooping enable** to disable PIM snooping in a VLAN.

By default, PIM snooping is disabled.

Before you enable PIM snooping in a VLAN, be sure to enable IGMP snooping globally and specifically in the VLAN.

PIM snooping does not work in a sub-VLAN of a multicast VLAN.

Related commands: **igmp-snooping enable**.

Examples

```
# Enable IGMP snooping globally, and enable IGMP snooping and PIM snooping in VLAN 2.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] pim-snooping enable
```

reset pim-snooping statistics

Syntax

```
reset pim-snooping statistics
```

View

User view

Default level

2: System level

Parameters

None

Description

Use **reset pim-snooping statistics** to clear statistics for the PIM messages learned by PIM snooping.

Examples

```
# Clear statistics for the PIM messages learned by PIM snooping.
```

```
<Sysname> reset pim-snooping statistics
```

Multicast VLAN configuration commands

display multicast-vlan

Syntax

```
display multicast-vlan [ vlan-id ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan-id: Specifies a multicast VLAN, in the range of 1 to 4094. If this argument is not specified, this command displays information about all multicast VLANs.

|: 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 multicast-vlan** to display information about the specified multicast VLAN.

Examples

```
# Display information about all multicast VLANs.
```

```
<Sysname> display multicast-vlan
Total 2 multicast-vlan(s)
```

```
Multicast vlan 100
  subvlan list:
    vlan 2 4-6
  port list:
    no port
```

```
Multicast vlan 200
  subvlan list:
    no subvlan
  port list:
    GE1/0/1                GE1/0/2
```


Table 8 Command output

Field	Description
subvlan list	List of sub-VLANs of the multicast VLAN
port list	Port list of the multicast VLAN

multicast-vlan

Syntax

multicast-vlan *vlan-id*

undo multicast-vlan { **all** | *vlan-id* }

View

System view

Default level

2: System level

Parameters

vlan-id: Specifies a VLAN by its ID, in the range of 1 to 4094.

all: Specifies all multicast VLANs.

Description

Use **multicast-vlan** to configure the specified VLAN as a multicast VLAN and enter multicast VLAN view.

Use **undo multicast-vlan** to remove the specified VLAN as a multicast VLAN.

The VLAN to be configured is not a multicast VLAN by default.

The specified VLAN to be configured as a multicast VLAN must exist.

For the HP 5500 EI switches, the multicast VLAN feature cannot be enabled on a device with IP multicast routing enabled.

For a sub-VLAN-based multicast VLAN, you must enable IGMP snooping only in the multicast VLAN. For a port-based multicast VLAN, you must enable IGMP snooping in both the multicast VLAN and all the user VLANs.

Related commands: **igmp-snooping enable** and **multicast routing-enable**.

Examples

Enable IGMP snooping in VLAN 100. Configure it as a multicast VLAN and enter multicast VLAN view.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 100
[Sysname-vlan100] igmp-snooping enable
[Sysname-vlan100] quit
[Sysname] multicast-vlan 100
[Sysname-mvlan-100]
```

port (multicast VLAN view)

Syntax

```
port interface-list  
undo port { all | interface-list }
```

View

Multicast VLAN view

Default level

2: System level

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number* to *interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

all: Specifies all the ports in the current multicast VLAN.

Description

Use **port** to assign the specified ports to the current multicast VLAN.

Use **undo port** to delete the specified ports or all ports from the current multicast VLAN.

By default, a multicast VLAN has no ports.

A port can belong to only one multicast VLAN.

You can assign only Ethernet ports, and Layer 2 aggregate interfaces as multicast VLAN ports.

Examples

```
# Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to multicast VLAN 100.  
<Sysname> system-view  
[Sysname] multicast-vlan 100  
[Sysname-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

port multicast-vlan

Syntax

```
port multicast-vlan vlan-id  
undo port multicast-vlan
```

View

Ethernet interface view, Layer 2 aggregate interface view, port group view.

Default level

2: System level

Parameters

vlan-id: Specifies a multicast VLAN by its ID, in the range of 1 to 4094.

Description

Use **port multicast-vlan** to assign the current port to the specified multicast VLAN.

Use **undo port multicast-vlan** to restore the default.

By default, a port does not belong to any multicast VLAN.

A port can belong to only one multicast VLAN.

Examples

```
# Assign GigabitEthernet 1/0/1 to multicast VLAN 100.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port multicast-vlan 100
```

subvlan (multicast VLAN view)

Syntax

```
subvlan vlan-list
undo subvlan { all | vlan-list }
```

View

Multicast VLAN view

Default level

2: System level

Parameters

vlan-list: Specifies a VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

all: Specifies all the sub-VLANs of the current multicast VLAN.

Description

Use **subvlan** to configure sub-VLANs for the current multicast VLAN.

Use **undo subvlan** to remove the specified sub-VLANs or all sub-VLANs from the current multicast VLAN.

A multicast VLAN has no sub-VLANs by default.

The VLANs to be configured as sub-VLANs of the multicast VLAN must have existed and must not be multicast VLANs or sub-VLANs of another multicast VLAN.

The number of sub-VLANs of the multicast VLAN must not exceed the system-defined limit.

Examples

```
# Configure VLAN 10 through VLAN 15 as sub-VLANs of multicast VLAN 100.
<Sysname> system-view
[Sysname] multicast-vlan 100
[Sysname-mvlan-100] subvlan 10 to 15
```

Multicast routing and forwarding configuration commands (available only on the HP 5500 EI)

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

The term "interface" in the multicast routing and forwarding 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*).

delete ip rpf-route-static

Syntax

```
delete ip rpf-route-static [ vpn-instance vpn-instance-name ]
```

View

System view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters. If this option is not specified, the command deletes all multicast static routes on the public network.

Description

Use **delete ip rpf-route-static** to delete all multicast static routes.

Related commands: **ip rpf-route-static**.

Examples

```
# Delete all multicast static routes on the public network.
```

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

```
[Sysname] delete ip rpf-route-static
```

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

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

display multicast boundary

Syntax

```
display multicast [ all-instance | vpn-instance vpn-instance-name ] boundary [ group-address [ mask | mask-length ] ] [ interface interface-type interface-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

group-address: Specifies a multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Specifies the mask of the multicast group address, 255.255.255.255 by default.

mask-length: Specifies the mask length of the multicast group address, in the range of 4 to 32. The default is 32.

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 multicast boundary** to display multicast boundary information on the specified interface or all interfaces.

If neither **all-instance** nor **vpn-instance** is specified, this command displays multicast boundary information on the public network.

Related commands: **multicast boundary**.

Examples

```
# Display multicast boundary information on all interfaces on the public network.
```

```
<Sysname> display multicast boundary
Multicast boundary information of VPN-Instance: public net
Boundary           Interface
224.1.1.0/24       Vlan1
239.2.2.0/24       Vlan2
```

Table 9 Command output

Field	Description
Multicast boundary information of VPN-Instance: public net	Multicast boundary for the public network
Boundary	Multicast group that corresponds to the multicast boundary
Interface:	Boundary interface that corresponds to the multicast boundary

display multicast forwarding-table

Syntax

```
display multicast [ all-instance | vpn-instance vpn-instance-name ] forwarding-table [ source-address  
[ mask { mask | mask-length } ] | group-address [ mask { mask | mask-length } ] | incoming-interface  
{ interface-type interface-number | register } | outgoing-interface { exclude | include | match }  
{ interface-type interface-number | register } | statistics | slot slot-number ] * [ port-info ] [ | { begin |  
exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Specifies the mask of the multicast group address or multicast source address, 255.255.255.255 by default.

mask-length: Specifies the mask length of the multicast group address or multicast source address. For a multicast group address, the value ranges from 4 to 32. For a multicast source address, the value ranges from 0 to 32. The default is 32 in both cases.

incoming-interface: Displays multicast forwarding entries, where the incoming interface is the specified one.

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

register: Displays multicast forwarding entries, where the incoming interface is the register interface of PIM-SM.

outgoing-interface: Displays multicast forwarding entries, where the outgoing interface is the specified one.

exclude: Displays the multicast forwarding entries, where the outgoing interface list excludes the specified interface.

include: Displays the multicast forwarding entries, where the outgoing interface list includes the specified interface.

match: Displays the forwarding entries, where the outgoing interface list includes and includes only the specified interface.

statistics: Displays statistics for the multicast forwarding table.

slot *slot-number*: Displays the multicast forwarding entries of the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

port-info: Displays Layer 2 port 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 multicast forwarding-table** to display multicast forwarding table information.

If neither **all-instance** nor **vpn-instance** is specified, this command displays information about multicast forwarding tables on the public network.

Multicast forwarding tables guide multicast forwarding. You can determine the forwarding state of multicast traffic by viewing the multicast forwarding tables.

Related commands: **display multicast routing-table**, **multicast forwarding-table downstream-limit**, and **multicast forwarding-table route-limit**.

Examples

Display multicast forwarding table information on the public network.

```
<Sysname> display multicast forwarding-table
Multicast Forwarding Table of VPN-Instance: public net
Total 1 entry

Total 1 entry matched

00001. (172.168.0.2, 227.0.0.1)
  MID: 0, Flags: 0x100000:0
  Uptime: 00:08:32, Timeout in: 00:03:26
  Incoming interface: Vlan-interface1
  List of 1 outgoing interfaces:
    1: Vlan-interface2
  Matched 19648 packets(20512512 bytes), Wrong If 0 packets
  Forwarded 19648 packets(20512512 bytes)
```

Table 10 Command output

Field	Description
Total 1 entry	Total number of (S, G) entries in the multicast forwarding table.
Total 1 entry matched	Total number of matched (S, G) entries in the multicast forwarding table.
00001	Sequence number of the (S, G) entry.
(172.168.0.2,227.0.0.1)	An (S, G) entry of the multicast forwarding table.
MID	(S, G) entry ID. Each (S, G) entry has a unique MID.

Field	Description
Flags	Current state of the (S, G) entry. Different bits indicate different states of (S, G) entries. The flags field comprises two hexadecimal numbers separated by a colon (:). Major values of the flags field before the colon are described in Table 11 . The value of the flags field after the colon is 0.
Uptime	Length of time for which the (S, G) entry has been up, in hours:minutes:seconds.
Timeout in	Length of time in which the (S, G) entry will expire, in hours:minutes:seconds.
Incoming interface	Incoming interface of the (S, G) entry. If the incoming interface is an interface in another VPN, the VPN name is displayed.
List of 1 outgoing interface: 1: Vlan-interface2	Outgoing interface list Interface number: outgoing interface and number. If the outgoing interface is an interface in another VPN, the VPN name is displayed.
Matched 19648 packets(20512512 bytes), Wrong If 0 packets	(S, G)-matched packets (bytes), packets with incoming interface errors.
Forwarded 19648 packets(20512512 bytes)	(S, G)-forwarded packets (bytes).

Table 11 Major values of the flags field (before the colon)

Value	Meaning
0x1	A register-stop message must be sent.
0x2	Whether the multicast source that corresponds to the (S, G) is active.
0x4	Null forwarding entry.
0x8	Whether the RP is a PIM domain border router.
0x10	A register outgoing interface is available.
0x400	(S, G) entry to be deleted.
0x8000	The (S, G) entry is in the smoothening process after active/standby switchover.
0x10000	The (S, G) has been updated during the smoothening process.
0x80000	The (S, G) entry has been repeatedly updated and must be deleted before a new entry is added.
0x100000	An entry is successfully added.
0x1000000	Multicast forwarding entry for BIDIR-PIM.
0x2000000	RP for BIDIR-PIM.

display multicast forwarding-table df-info

Syntax

```
display multicast [ all-instance | vpn-instance vpn-instance-name ] forwarding-table df-info
[ rp-address ] [ slot slot-number ] [ { begin | exclude | include } regular-expression ]
```


View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

rp-address: Specifies an RP address of BIDIR-PIM.

slot *slot-number*: Displays the DF information of the multicast forwarding table of the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device 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 the 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 multicast forwarding-table df-info** to display the DF information of the multicast forwarding table.

If neither **all-instance** nor **vpn-instance** is specified, this command displays the DF information for the public network.

Examples

Display the DF information of the multicast forwarding table for the public network.

```
<Sysname> display multicast forwarding-table df-info
Multicast DF information of VPN-Instance: public net
Total 1 RP
```

```
Total 1 RP matched
```

```
00001. RP Address: 1.1.1.1
    MID: 0, Flags: 0x2100000:0
    Uptime: 00:08:32
    RPF interface: Vlan-interface1
    List of 1 DF interfaces:
        1: Vlan-interface2
```

Table 12 Command output

Field	Description
Total 1 RP	Total number of RPs.

Field	Description
Total 1 RP matched	Total number of matched RPs.
00001	Sequence number of the RP.
MID	ID of the RP. Each RP has a unique MID.
Flags	Current state of the RP. Different bits indicate different states of an RP. Major values of the flags field before the colon are described in Table 11 . The value of the flags field after the colon is 0.
Uptime	Length of time for which the RP has been up, in the format hours:minutes:seconds.
RPF interface	RPF interface to the RP.
List of 1 DF interfaces	DF interface list.

display multicast routing-table

Syntax

```
display multicast [ all-instance | vpn-instance vpn-instance-name ] routing-table [ source-address [ mask { mask | mask-length } ] | group-address [ mask { mask | mask-length } ] | incoming-interface { interface-type interface-number | register } | outgoing-interface { exclude | include | match } { interface-type interface-number | register } ] * [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Specifies the mask of the multicast group address or multicast source address. The default is 255.255.255.255.

mask-length: Specifies the mask length of the multicast group address or multicast source address. For a multicast group address, the value ranges from 4 to 32. For a multicast source address, the value ranges from 0 to 32. The default is 32 in both cases.

incoming-interface: Displays the multicast routing entries, where the incoming interface is the specified one.

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

register: Displays the multicast routing entries, where the incoming interface is the specified register interface of PIM-SM.

outgoing-interface: Displays the multicast routing entries, where the outgoing interface is the specified one.

exclude: Displays the multicast routing entries, where the outgoing interface list excludes the specified interface.

include: Displays the multicast routing entries, where the outgoing interface list includes the specified interface.

match: Displays the multicast routing entries, where the outgoing interface list includes only the specified interface.

|: 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 multicast routing-table** to display multicast routing table information.

If neither **all-instance** nor **vpn-instance** is specified, this command displays multicast routing information on the public network.

Multicast routing tables are the basis of multicast forwarding. You can view the establishment state of an (S, G) entry by checking the multicast routing table.

Related commands: **display multicast forwarding-table**.

Examples

Display the routing information in the multicast routing table on the public network.

```
<Sysname> display multicast routing-table
Multicast routing table of VPN-Instance: public net
Total 1 entry
00001. (172.168.0.2, 227.0.0.1)
    Uptime: 00:00:28
    Upstream Interface: Vlan-interface1
    List of 2 downstream interfaces
        1: Vlan-interface2
        2: Vlan-interface3
```

Table 13 Command output

Field	Description
Total 1 entry	Total number of (S, G) entries in the multicast routing table.
00001	Sequence number of the (S, G) entry.
(172.168.0.2, 227.0.0.1)	(S, G) entry of the multicast forwarding table.
Uptime	Length of time for which the (S, G) entry has been up, in hours:minutes:seconds.
Upstream interface	Upstream interface of the (S, G) entry. Multicast packets should arrive at this interface. If the upstream interface is an interface in another VPN, the VPN name is displayed.

Field	Description
List of 2 downstream interfaces	Downstream interface list. These interfaces must forward multicast packets. If the downstream interface is an interface in another VPN, the VPN name is displayed.

display multicast routing-table static

Syntax

```
display multicast routing-table [ all-instance | vpn-instance vpn-instance-name ] static [ source-address { mask-length | mask } ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

source-address: Specifies a multicast source address.

mask: Specifies the mask of the multicast source address.

mask-length: Specifies the mask length of the multicast source address, 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 multicast routing-table static** to display information about multicast static routes.

If neither **all-instance** nor **vpn-instance** is specified, this command displays information about multicast static routes on the public network.

Examples

```
# Display all multicast static routes on the public network.
```

```
<Sysname> display multicast routing-table static
Multicast Routing Table of VPN-Instance: public net
Routes : 1
```

```
Mroute 10.10.0.0/16
    Interface = Vlan-interface1          RPF Neighbor = 2.2.2.2
    Matched routing protocol = <none>, Route-policy = <none>
```

```
Preference = 1, Order = 1
Running Configuration = ip rpf-route-static 10.10.0.0 16 2.2.2.2 order 1
```

Table 14 Command output

Field	Description
Mroute	Multicast route source address and its mask length.
Interface	Outgoing interface to the multicast source.
RPF Neighbor	IP address of the RPF neighbor through which the multicast source is reachable.
Route-policy	Routing policy. The multicast source address of the route should match the routing policy.
Preference	Route preference.
Order	Sequence number of the route.
Running Configuration	Command line that configures the multicast static route.

display multicast rpf-info

Syntax

```
display multicast [ all-instance | vpn-instance vpn-instance-name ] rpf-info source-address
[ group-address ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

|: 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 multicast rpf-info** to display the RPF information of a multicast source.

If neither **all-instance** nor **vpn-instance** is specified, this command displays the information on the public network.

Related commands: **display multicast forwarding-table** and **display multicast routing-table**.

Examples

Display the RPF information of multicast source 192.168.1.55 on the public network.

```
<Sysname> display multicast rpf-info 192.168.1.55
RPF information about source 192.168.1.55:
  VPN instance: public net
  RPF interface: Vlan-interface1, RPF neighbor: 10.1.1.1
  Referenced route/mask: 192.168.1.0/24
  Referenced route type: igp
  Route selection rule: preference-preferred
  Load splitting rule: disable
```

Table 15 Command output

Field	Description
RPF interface	RPF interface. If the RPF interface is an interface in another VPN, the VPN name is displayed.
RPF neighbor	IP address of the RPF neighbor.
Referenced route/mask	Referenced route and its mask length.
Referenced route type	Type of the referenced route, which can be any of the following: <ul style="list-style-type: none">• igp—Unicast route (IGP).• egp—Unicast route (EGP).• unicast (direct)—Unicast route (directly connected).• unicast—Other unicast route (such as unicast static route).• mbgp—MBGP route.• multicast static—Multicast static route.
Route selection rule	Rule for RPF route selection, which can be based on the preference of the routing protocol or based on the longest match on the destination address.
Load splitting rule	Status of the load splitting rule (enabled/disabled).

ip rpf-route-static

Syntax

```
ip rpf-route-static [ vpn-instance vpn-instance-name ] source-address { mask | mask-length } [ protocol [ process-id ] ] [ route-policy policy-name ] { rpf-nbr-address | interface-type interface-number } [ preference preference ] [ order order-number ]
```

```
undo ip rpf-route-static [ vpn-instance vpn-instance-name ] source-address { mask | mask-length } [ protocol [ process-id ] ] [ route-policy policy-name ]
```

View

System view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters. If this option is not specified, this command configures a multicast static route on the public network.

source-address: Specifies a multicast source address.

mask: Specifies the mask of the multicast source address.

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

protocol: Specifies a routing protocol, which can be any of the following values:

- **bgp**: Specifies the BGP protocol.
- **isis**: Specifies the IS-IS protocol.
- **ospf**: Specifies the OSPF protocol.
- **rip**: Specifies the RIP protocol.
- **static**: Specifies a static route.

process-id: Specifies the process number of the unicast routing protocol, in the range of 1 to 65535. This argument must be provided if IS-IS, OSPF or RIP is the specified unicast routing protocol.

policy-name: Specifies the name of the routing policy used for matching multicast static routes, a case-sensitive string of 1 to 63 characters.

rpf-nbr-address: Specifies an RPF neighbor by the IP address.

interface-type interface-number: Specifies an interface by its type and number. The interface connects the RPF neighbor.

preference: Specifies a route preference, in the range of 1 to 255 and defaulting to 1.

order-number: Specifies the match order for routes on the same segment, in the range of 1 to 100.

Description

Use **ip rpf-route-static** to configure a multicast static route.

Use **undo ip rpf-route-static** to delete a multicast static route from the multicast static routing table.

By default, no multicast static route is configured.

The arguments *source-address { mask | mask-length }*, *protocol* and *policy-name* are critical elements in multicast static route configuration. The variation of any of these arguments results in a different configuration.

When you configure a multicast static route, the system first checks whether any of these argument exists. If the system finds a match, you must modify the corresponding fields without changing the configuration sequence. Otherwise, the system adds a multicast static route.

When you configure a multicast static route, specify an RPF neighbor only by providing its IP address (*rpf-nbr-address*) rather than providing the type and number (*interface-type interface-number*) of the interface that connects the RPF if the interface of the RPF neighbor is a Layer 3 Ethernet port, Layer 3 aggregate interface, Loopback interface, or VLAN interface.

Because outgoing interface iteration might fail or the specified interface might be in the down state, the multicast static route configured with this command might fail to take effect. Therefore, use the **display multicast routing-table static** command after you configure a multicast static route to check whether the route has been successfully configured or whether the route has taken effect.

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

Examples

```
# Configure a multicast static route to the multicast source 10.1.1.1/24. Specify a router with the IP address of 192.168.1.23 as its RPF neighbor.
```

```
<Sysname> system-view
[Sysname] ip rpf-route-static 10.1.1.1 24 192.168.1.23
```

mtracert

Syntax

```
mtracert source-address [ [ last-hop-router-address ] group-address ]
```

View

Any view

Default level

1: Monitor level

Parameters

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

last-hop-router-address: Specifies a last-hop router address, which is the IP address of the local router by default.

Description

Use **mtracert** to trace the path down which the multicast traffic flows to the last-hop router.

If the command to trace the path for a specific (S, G) multicast stream includes the *last-hop-router-address* argument, the interface that corresponds to the last-hop router address must be the outgoing interface for the (S, G) entry. Otherwise, the multicast traceroute might fail.

Examples

```
# Trace the path down which the (6.6.6.6, 225.2.1.1) multicast traffic flows to the last-hop router with an IP address of 5.5.5.8.
```

```
<Sysname> mtracert 6.6.6.6 5.5.5.8 225.2.1.1
Type Ctrl+C to quit mtrace facility
Tracing reverse path of (6.6.6.6, 225.2.1.1) from last-hop router (5.5.5.8) to source via multicast routing-table
```

```
-1 5.5.5.8
  Incoming interface address: 4.4.4.8
  Previous-hop router address: 4.4.4.7
  Input packet count on incoming interface: 17837
  Output packet count on outgoing interface: 0
  Total number of packets for this source-group pair: 8000
  Protocol: PIM
  Forwarding TTL: 0
  Forwarding code: No error

-2 4.4.4.7
  Incoming interface address: 6.6.6.7
```



```

Previous-hop router address: 0.0.0.0
Input packet count on incoming interface: 2
Output packet count on outgoing interface: 259
Total number of packets for this source-group pair: 8100
Protocol: PIM
Forwarding TTL: 0
Forwarding code: No error

```

Table 16 Command output

Field	Description
(6.6.6.6, 225.2.1.1)	(S, G) multicast stream for which the forwarding path is being traced
-1 5.5.5.8	(S, G) outgoing interface address of each hop, starting from the last-hop router
Incoming interface address	IP address of the interface that received the (S, G) packets
Previous-hop router address	IP address of the previous router that forwards the packets to the current router
Input packet count on incoming interface	Total number of multicast packets that the incoming interface received
Output packet count on outgoing interface	Total number of multicast packets that the outgoing interface transmitted
Total number of packets for this source-group pair	Total number of packets from the specified source that this router forwards to the specified group
Protocol	Multicast routing protocol in use
Forwarding TTL	Minimum TTL that a packet must have before it can be forwarded over the outgoing interface

multicast boundary

Syntax

```

multicast boundary group-address { mask | mask-length }
undo multicast boundary { group-address { mask | mask-length } | all }

```

View

Interface view

Default level

2: System level

Parameters

group-address: Specifies a multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Specifies the mask of the multicast group address.

mask-length: Specifies the mask length of the multicast group address, in the range of 4 to 32.

all: Specifies all forwarding boundaries configured on the interface.

Description

Use **multicast boundary** to configure a multicast forwarding boundary.

Use **undo multicast boundary** to remove a multicast forwarding boundary.

By default, no multicast forwarding boundary is configured.

A multicast forwarding boundary sets the boundary condition for the multicast groups in the specified address range. If the destination address of a multicast packet matches the set boundary condition, the packet is not forwarded.

An interface can act as a forwarding boundary for multiple multicast groups in different address ranges. To achieve this, use this command on the interface for each multicast address range.

Assume that Set A and Set B are multicast forwarding boundary sets with different address ranges, and B is a subset of A. If B is configured after A, A still takes effect. If A is configured after B, B is removed.

Related commands: **display multicast boundary**.

Examples

```
# Configure VLAN-interface 100 as the forwarding boundary of multicast groups in the range of 239.2.0.0/16.
```

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

```
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] multicast boundary 239.2.0.0 16
```

multicast forwarding-table downstream-limit

Syntax

multicast forwarding-table downstream-limit *limit*

undo multicast forwarding-table downstream-limit

View

System view, VPN instance view

Default level

2: System level

Parameters

limit: Specifies the maximum number of downstream nodes (the maximum number of outgoing interfaces) for a single multicast forwarding entry. The value ranges from 0 to 128.

Description

Use **multicast forwarding-table downstream-limit** to configure the maximum number of downstream nodes for a single entry in the multicast forwarding table.

Use **undo multicast forwarding-table downstream-limit** to restore the default.

By default, the maximum number of downstream nodes for a single multicast forwarding entry is 128.

Related commands: **display multicast forwarding-table**.

Examples

```
# Set the maximum number of downstream nodes for a single multicast forwarding entry on the public network to 120.
```

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

```
[Sysname] multicast forwarding-table downstream-limit 120
```

```
# Set the maximum number of downstream nodes for a single multicast forwarding entry of VPN instance
mvpn to 60.
```

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast forwarding-table downstream-limit 60
```

multicast forwarding-table route-limit

Syntax

```
multicast forwarding-table route-limit limit
undo multicast forwarding-table route-limit
```

View

System view, VPN instance view

Default level

2: System level

Parameters

limit: Specifies the maximum number of entries in the multicast forwarding table. The value ranges from 0 to 2000.

Description

Use **multicast forwarding-table route-limit** to configure the maximum number of entries in the multicast forwarding table.

Use **undo multicast forwarding-table route-limit** to restore the maximum number of entries in the multicast forwarding table to the default.

By default, the upper limit is 2000.

Related commands: **display multicast forwarding-table**.

Examples

```
# Set the maximum number of entries in the multicast forwarding table on the public network to 200.
<Sysname> system-view
[Sysname] multicast forwarding-table route-limit 200

# Set the maximum number of entries in the multicast forwarding table of VPN instance mvpn to 200.
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast forwarding-table route-limit 200
```

multicast load-splitting

Syntax

```
multicast load-splitting { source | source-group }
undo multicast load-splitting
```

View

System view, VPN instance view

Default level

2: System level

Parameters

source: Specifies load splitting on a per-source basis.

source-group: Specifies load splitting both on a per-source basis and a per-group basis.

Description

Use **multicast load-splitting** to enable load splitting of multicast traffic.

Use **undo multicast load-splitting** to disable load splitting of multicast traffic.

By default, load splitting of multicast traffic is disabled.

This command does not take effect in BIDIR-PIM.

Examples

```
# Enable per-source load splitting of multicast traffic on the public network.
```

```
<Sysname> system-view  
[Sysname] multicast load-splitting source
```

```
# Enable per-source load splitting of multicast traffic in VPN instance mvpn.
```

```
<Sysname> system-view  
[Sysname] ip vpn-instance mvpn  
[Sysname-vpn-instance-mvpn] multicast load-splitting source
```

multicast longest-match

Syntax

multicast longest-match

undo multicast longest-match

View

System view, VPN instance view

Default level

2: System level

Parameters

None

Description

Use **multicast longest-match** to configure the device to select the RPF route using longest match.

Use **undo multicast longest-match** to restore the default.

By default, the device selects the route with the highest priority as the RPF route.

Examples

```
# Configure the device to select the RPF route based on the longest match principle on the public network.
```

```
<Sysname> system-view  
[Sysname] multicast longest-match
```

```
# Configure route selection based on the longest match in VPN instance mvpn.
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast longest-match
```

multicast routing-enable

Syntax

```
multicast routing-enable
undo multicast routing-enable
```

View

System view, VPN instance view

Default level

2: System level

Parameters

None

Description

Use **multicast routing-enable** to enable IP multicast routing.

Use **undo multicast routing-enable** to disable IP multicast routing.

By default, IP multicast routing is disabled.

You must enable IP multicast routing on the public network or VPN instance before you can use other Layer 3 multicast commands in the corresponding instance.

The device does not forward any multicast packets before IP multicast routing is enabled.

Examples

```
# Enable IP multicast routing on the public network.
<Sysname> system-view
[Sysname] multicast routing-enable

# Enable IP multicast routing in VPN instance mvpn.
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] route-distinguisher 100:1
[Sysname-vpn-instance-mvpn] multicast routing-enable
```

reset multicast forwarding-table

Syntax

```
reset multicast [ all-instance | vpn-instance vpn-instance-name ] forwarding-table { { source-address [ mask { mask | mask-length } ] | group-address [ mask { mask | mask-length } ] | incoming-interface { interface-type interface-number | register } } * | all }
```

View

User view

Default level

2: System level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Specifies the mask of the multicast group address or multicast source address, 255.255.255.255 by default.

mask-length: Specifies the mask length of the multicast group address or multicast source address. For a multicast group address, the value ranges from 4 to 32. For a multicast source address, the value range from 0 to 32. The default is 32 in both cases.

incoming-interface: Specifies the multicast forwarding entries where the incoming interface is the specified one.

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

register: Specifies the multicast forwarding entries where the incoming interface is the specified register interface of PIM-SM.

all: Specifies all forwarding entries in the multicast forwarding table.

Description

Use **reset multicast forwarding-table** to remove multicast forwarding table entries.

If neither **all-instance** nor **vpn-instance** is specified, this command removes the forwarding table entries on the public network.

When a multicast forwarding entry is removed, the associated multicast routing entry is also removed.

Related commands: **display multicast forwarding-table**, **display multicast routing-table**, and **reset multicast routing-table**.

Examples

```
# Remove the multicast forwarding entry for the multicast group 225.5.4.3 on the public network.
```

```
<Sysname> reset multicast forwarding-table 225.5.4.3
```

```
# Remove the multicast forwarding entry for the multicast group 226.1.2.3 in VPN instance mvpn.
```

```
<Sysname> reset multicast vpn-instance mvpn forwarding-table 226.1.2.3
```

reset multicast routing-table

Syntax

```
reset multicast [ all-instance | vpn-instance vpn-instance-name ] routing-table { { source-address [ mask { mask | mask-length } ] | group-address [ mask { mask | mask-length } ] | incoming-interface { interface-type interface-number | register } } * | all }
```

View

User view

Default level

2: System level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Specifies the mask of the multicast group address or multicast source address, 255.255.255.255 by default.

mask-length: Specifies the mask length of the multicast group address or multicast source address. For a multicast group address, the value ranges from 4 to 32. For a multicast source address, the value ranges from 0 to 32. The default is 32 in both cases.

incoming-interface: Specifies the routing entries where the incoming interface is the specified one.

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

register: Specifies the routing entries where the incoming interface is the specified register interface of PIM-SM.

all: Specifies all the routing entries in the multicast routing table.

Description

Use **reset multicast routing-table** to remove multicast routing table entries.

If neither **all-instance** nor **vpn-instance** is specified, this command removes the multicast routing table entries on the public network.

When a multicast routing entry is removed, the associated multicast forwarding entry is also removed.

Related commands: **display multicast forwarding-table**, **display multicast routing-table**, and **reset multicast forwarding-table**.

Examples

```
# Remove the multicast routing entry for the multicast group 225.5.4.3 on the public network.
```

```
<Sysname> reset multicast routing-table 225.5.4.3
```

```
# Remove the multicast routing entry for the multicast group 226.1.2.3 in VPN instance mvpn.
```

```
<Sysname> reset multicast vpn-instance mvpn routing-table 226.1.2.3
```

IGMP configuration commands (available only on the HP 5500 EI)

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

The term "interface" in this chapter 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*).

display igmp group

Syntax

```
display igmp [ all-instance | vpn-instance vpn-instance-name ] group [ group-address | interface interface-type interface-number ] [ static | verbose ] [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255. If you do not specify this argument, the command displays the IGMP group information of all multicast groups.

interface *interface-type interface-number*: Displays the IGMP group information about a particular interface. If you do not specify *interface-type interface-number*, this command displays the IGMP group information on all interfaces.

static: Displays the information of statically joined IGMP groups. If you do not specify this keyword, the command displays only dynamic group entries of IGMP groups.

verbose: Displays detailed information about IGMP groups.

|: 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 igmp group** to display IGMP group information.

If neither **all-instance** nor **vpn-instance** is specified, this command displays the IGMP group information on the public network.

Examples

Display the dynamic group entries of IGMP groups on all interfaces on the public network.

```
<Sysname> display igmp group
Total 3 IGMP Group(s).
Interface group report information of VPN-Instance: public net
Vlan-interface1(10.10.1.20):
  Total 3 IGMP Groups reported
  Group Address      Last Reporter      Uptime           Expires
  225.1.1.1         10.10.1.10        00:02:04        00:01:15
  225.1.1.3         10.10.1.10        00:02:04        00:01:15
  225.1.1.2         10.10.1.10        00:02:04        00:01:17
```

Display detailed information about the dynamic entries of IGMP group 225.1.1.1 on the public network.

```
<Sysname> display igmp group 225.1.1.1 verbose
Interface group report information of VPN-Instance: public net
Vlan-interface1(10.10.1.20):
  Total 3 IGMP Groups reported
  Group: 225.1.1.1
    Uptime: 00:00:34
    Expires: 00:00:40
    Last reporter: 10.10.1.10
    Last-member-query-counter: 0
    Last-member-query-timer-expiry: off
    Group mode: exclude
    Version1-host-present-timer-expiry: off
    Version2-host-present-timer-expiry: off
```

Table 17 Command output

Field	Description
Interface group report information of VPN-Instance: public net	IGMP group information on a public network interface.
Group	Multicast group address.
Uptime	Length of time since the multicast group was reported.
Expires	Remaining time of the multicast group, where "off" means that the multicast group never times out.
Last reporter	Address of the last host that reported its membership for this multicast group.
Last-member-query-counter	Number of last-member queries sent.
Last-member-query-timer-expiry	Remaining time of the last-member query timer, where "off" means that the timer never expires.
Group mode	Multicast source filtering modes: <ul style="list-style-type: none"> • Include. • Exclude. This field is displayed only when the switch is running IGMPv3.

Field	Description
Version1-host-present-timer-expiry	Remaining time of the IGMPv1 host present timer, where "off" means that the timer never expires.
Version2-host-present-timer-expiry	Remaining time of the IGMPv2 host present timer, where "off" means that the timer never expires. This field is displayed only when the switch is running IGMPv3.

display igmp group port-info

Syntax

```
display igmp group port-info [ vlan vlan-id ] [ slot slot-number ] [ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan-id: VLAN ID, in the range of 1 to 4094. If you do not specify a VLAN, this command displays the Layer 2 port information of IGMP groups in all VLANs.

slot slot-number: Displays the Layer 2 port information of IGMP multicast groups on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

verbose: Displays the detailed information about Layer 2 ports of IGMP groups.

|: 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 igmp group port-info** to display Layer 2 port information of IGMP groups, including both dynamic and static Layer 2 port entries.

Examples

Display detailed Layer 2 port information of IGMP groups.

```
<Sysname> display igmp group port-info verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Port flags: D-Dynamic port, S-Static port, C-Copy port
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```

Vlan(id):2.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port unit board: Mask(0x0000)
  Router port(s):total 1 port(s).
    GE1/0/1                (D) ( 00:01:30 )
  IP group(s):the following ip group(s) match to one mac group.
  IP group address:224.1.1.1
  (1.1.1.1, 224.1.1.1):
  Attribute:      Host Port
  Host port unit board: Mask(0x0000)
  Host port(s):total 1 port(s).
    GE1/0/2                (D) ( 00:03:23 )
  MAC group(s):
  MAC group address:0100-5e01-0101
  Host port unit board: Mask(0x0000)
  Host port(s):total 1 port(s).
    GE1/0/2

```

Table 18 Command output

Field	Description
Total 1 IP Group(s).	Total number of IP multicast groups.
Total 1 IP Source(s).	Total number of IP multicast sources.
Total 1 MAC Group(s).	Total number of MAC multicast groups.
Port flags: D-Dynamic port, S-Static port, C-Copy port	Port flags: D for a dynamic port, S for a static port, and C for a port copied from a (*, G) entry to an (S, G) entry.
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R for a real egress sub-VLAN under the current entry, and C for a sub-VLAN copied from a (*, G) entry to an (S, G) entry.
Router port(s)	Number of router ports.
Router port unit board	Mask indicating an IRF member switch with a router port residing on it. If no IRF fabric exists, Mask (0x0000) is displayed.
(00:01:30)	Remaining time of the aging timer for the dynamic member port or router port. On an IRF member switch, to display the remaining life of a non-aggregation port that does not belong to the Master switch, you must specify the member ID of the IRF member switch by using slot slot-number . This is not required for an aggregation port.
IP group address	Address of the IP multicast group.
MAC group address	Address of the MAC multicast group.
Attribute	Attribute of the IP multicast group.
Host port unit board	Mask indicating an IRF member switch with a member port residing on it. If no IRF fabric exists, Mask(0x0000) is displayed
Host port(s)	Number of member ports.

display igmp host interface

Syntax

```
display igmp host interface interface-type interface-number group group-address [ source source-address ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Displays information about the hosts tracked by IGMP on the specified interface. The specified interface can be a Layer 3 Ethernet port, Layer 3 aggregate interface, or Tunnel interface.

group *group-address*: Displays information about the hosts tracked by IGMP that are in the specified IGMP group. The *group-address* argument is in the range of 224.0.1.0 to 239.255.255.255.

source *source-address*: Displays information about the hosts tracked by IGMP that are in the specified multicast source, where *source-address* is a valid unicast address or 0.0.0.0. A source IP address of 0.0.0.0 specifies all multicast sources.

|: 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 igmp host interface** to display information about the hosts tracked by IGMP on the specified interface.

Examples

```
# Display information about the hosts tracked by IGMP in multicast group 224.1.1.1 on Layer 3 Ethernet port GigabitEthernet 1/0/1.
```

```
<Sysname> display igmp host interface gigabitethernet 1/0/1 group 224.1.1.1
```

```
Host information of VPN-Instance: public net
```

```
GigabitEthernet1/0/1(192.168.1.1):
```

```
(0.0.0.0, 224.1.1.1)
```

Host	Uptime	Expires
1.1.1.1	00:02:20	00:00:40
2.2.2.2	00:02:21	00:00:39

Table 19 Command output

Field	Description
Host information of VPN-Instance: public net	Information about the hosts tracked by IGMP on the public network interface

Field	Description
GigabitEthernet1/0/1(192.168.1.1) (0.0.0.0, 224.1.1.1)	Interface and IP address (S, G) entry, where 0.0.0.0 indicates all multicast sources
Host	Host IP address
Uptime	Host running duration
Expires	Host expiration time, where <i>timeout</i> means that the host has expired

display igmp host port-info

Syntax

```
display igmp host port-info vlan vlan-id group group-address [ source source-address ] [ slot slot-number ]
[ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays information about the hosts tracked by IGMP on the Layer 2 ports in the specified VLAN, where *vlan-id* is in the range of 1 to 4094.

group *group-address*: Displays information about the hosts tracked by IGMP that join in the specified IGMP group on the Layer 2 ports. *group-address* is in the range of 224.0.1.0 to 239.255.255.255.

source *source-address*: Displays information about the hosts tracked by IGMP that join in the specified multicast source on the Layer 2 ports, where *source-address* is a valid unicast address or 0.0.0.0. A source IP address of 0.0.0.0 specifies all multicast sources.

slot *slot-number*: Displays information about the hosts tracked by IGMP on the Layer 2 ports on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device 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 igmp host port-info** to display information about the hosts tracked by IGMP on the Layer 2 ports.

Examples

```
# Display information about the hosts tracked by IGMP that join in IGMP group 224.1.1.1 on the Layer 2 ports in VLAN 2.
```

```

<Sysname> display igmp host port-info vlan 2 group 224.1.1.1
VLAN(ID) : 2
(0.0.0.0, 224.1.1.1)
  Port : GigabitEthernet1/0/1
    Host                Uptime                Expires
    1.1.1.1             00:02:20             00:00:40
    2.2.2.2             00:02:21             00:00:39
  Port : GigabitEthernet1/0/2
    Host                Uptime                Expires
    3.3.3.3             00:02:20             00:00:40

```

Table 20 Command output

Field	Description
(0.0.0.0, 224.1.1.1)	(S, G) entry, where 0.0.0.0 indicates all multicast sources
Port	Member port
Host	Host IP address
Uptime	Host running duration
Expires	Host expiration time, where <i>timeout</i> means that the host has expired

display igmp interface

Syntax

```

display igmp [ all-instance | vpn-instance vpn-instance-name ] interface [ interface-type
interface-number ] [ verbose ] [ | { begin | exclude | include } regular-expression ]

```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

interface-type interface-number: Specifies an interface to display its IGMP configuration and operation information. If no interface is specified, the command displays the related information of all IGMP-enabled interfaces.

verbose: Displays the detailed IGMP configuration and operation 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 igmp interface** to display IGMP configuration and operation information of the specified interface or all IGMP-enabled interfaces.

If neither **all-instance** nor **vpn-instance** is specified, this command displays the information on the public network.

Examples

Display the IGMP configuration and operation information on Vlan-interface1 (downstream interface) on the public network.

```
<Sysname> display igmp interface vlan-interface 1 verbose
Vlan-interface1(10.10.1.20):
  IGMP is enabled
  Current IGMP version is 2
  Value of query interval for IGMP(in seconds): 60
  Value of other querier present interval for IGMP(in seconds): 125
  Value of maximum query response time for IGMP(in seconds): 10
  Value of last member query interval(in seconds): 1
  Value of startup query interval(in seconds): 15
  Value of startup query count: 2
  General query timer expiry (hours:minutes:seconds): 00:00:54
  Querier for IGMP: 10.10.1.20 (this router)
  IGMP activity: 1 joins, 0 leaves
  Multicast routing on this interface: enabled
  Robustness: 2
  Require-router-alert: disabled
  Fast-leave: disabled
  Ssm-mapping: disabled
  Startup-query-timer-expiry: off
  Other-querier-present-timer-expiry: off
  Proxying interface: Vlan-interface2(20.10.1.20)
  Total 1 IGMP Group reported
```

Display the detailed IGMP configuration and operation information on Vlan-interface2 (upstream interface) on the public network.

```
<Sysname> display igmp interface vlan-interface 2 verbose
Vlan-interface2(20.10.1.20):
  IGMP proxy is enabled
  Current IGMP version is 3
  Multicast routing on this interface: enabled
  Require-router-alert: disabled
  Version1-querier-present-timer-expiry: off
  Version2-querier-present-timer-expiry: off
```

Table 21 Command output

Field	Description
Vlan-interface1(10.10.1.20)	Interface and IP address
Current IGMP version	Version of IGMP that runs on the interface

Field	Description
Value of query interval for IGMP(in seconds)	IGMP general query interval, in seconds
Value of other querier present interval for IGMP(in seconds)	Other querier present interval, in seconds
Value of maximum query response time for IGMP(in seconds)	Maximum response time for IGMP general queries, in seconds
Value of last-member query interval(in seconds)	IGMP last-member query interval, in seconds
Value of startup query interval(in seconds)	IGMP startup query interval, in seconds
Value of startup query count	Number of IGMP general queries that the switch sends on startup
General query timer expiry	Remaining time of the IGMP general query timer, where "off" means that the timer never expires
Querier for IGMP	IP address of the IGMP querier
IGMP activity	Statistics of IGMP activities (joins and leaves)
Multicast routing on this interface	Whether the multicast routing and forwarding function is enabled
Robustness	Robustness variable of the IGMP querier
Require-router-alert	Dropping of IGMP messages without Router-Alert (enabled/disabled)
Fast-leave	Fast-leave processing status (enabled/disabled)
Ssm-mapping	IGMP SSM mapping status (enabled/disabled)
Startup-query-timer-expiry	Remaining time of the startup query timer, where "off" means that the timer never expires
Other-querier-present-timer-expiry	Remaining time of the other querier present timer, where "off" means that the timer never expires
Proxying interface	IGMP proxy interface, where "none" means that no proxy interface exists
Total 1 IGMP Group reported	Total number of IGMP groups that the interface has dynamically joined
IGMP proxy is enabled	IGMP proxying is enabled
Version1-querier-present-timer-expiry	Remaining time of the IGMPv1 querier present timer, where "off" means that the timer never expires
Version2-querier-present-timer-expiry	Remaining time of the IGMPv2 querier present timer, where "off" means that the timer never expires

display igmp proxying group

Syntax

```
display igmp [ all-instance | vpn-instance vpn-instance-name ] proxying group [ group-address ]
[ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255. With no multicast group address included, this command displays the information of all the IGMP proxying groups.

verbose: Displays the detailed IGMP proxying group 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 igmp proxying group** to display the IGMP proxying group information.

If neither **all-instance** nor **vpn-instance** is specified, this command displays the information on the public network.

Examples

```
# Display the IGMP proxying group information on the public network.
```

```
<Sysname> display igmp proxying group
Proxying group record(s) information of VPN-Instance: public net
  Total 1 IGMP-Proxying group record(s)
  Group Address      Member state    Expires
  225.1.1.1          Delay           00:01:15
```

```
# Display detailed information about IGMP proxying group 225.1.1.1 on the public network.
```

```
<Sysname> display igmp proxying group 225.1.1.1 verbose
Proxying group record(s) information of VPN-Instance: public net
  Total 1 IGMP-Proxying group record(s)
  Group: 225.1.1.1
  Group mode: include
  Member state: Delay
  Expires: 00:00:02
  Source list (total 1 source(s))
  Source: 1.1.1.1
```

Table 22 Command output

Field	Description
Proxying group record(s) information of VPN-Instance: public net	IGMP proxying group information on the public network.

Field	Description
Total 1 IGMP-Proxying group record(s)	One IGMP proxying group is recorded.
Group Address/Group	Multicast group address.
Member state	Host member states: <ul style="list-style-type: none"> • Delay. • Idle.
Expires	Remaining time of the multicast group, where "off" means that the multicast group never times out.
Group mode	Multicast source filtering modes: <ul style="list-style-type: none"> • Include. • Exclude.
Source list	List of multicast sources (only including the sources from which hosts want to receive multicast data).

display igmp routing-table

Syntax

```
display igmp [ all-instance | vpn-instance vpn-instance-name ] routing-table [ source-address [ mask { mask | mask-length } ] | group-address [ mask { mask | mask-length } ] | flags { act | suc } ] * [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

source-address: Multicast source address.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

mask: Subnet mask of the multicast group address or multicast source address, 255.255.255.255 by default.

mask-length: Subnet mask length of the multicast group address or multicast source address. For a multicast source address, this argument has an effective value range of 0 to 32. For a multicast group address, this argument has an effective value range of 4 to 32. The system default is 32 in both cases.

flags: Specifies the route flag.

act: Displays the IGMP routes with the ACT flag.

suc: Displays the IGMP routes with the SUC flag.

|: 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 igmp routing-table** to display the IGMP routing table information.

If neither **all-instance** nor **vpn-instance** is specified, this command displays the information on the public network.

Examples

Display IGMP routing table information on the public network.

```
<Sysname> display igmp routing-table
Routing table of VPN-Instance: public net
Total 3 entries

00001. (*, 225.1.1.1)
    List of 1 downstream interface
        Vlan-interface1 (20.1.1.1),
            Protocol: STATIC

00002. (1.1.1.1, 225.1.1.1), Flag: ACT
    List of 1 downstream interface in include mode
        Vlan-interface2 (30.1.1.1),
            Protocol: IGMP

00003. (*, 239.255.255.250)
    List of 1 downstream interface
        Vlan-interface3 (40.20.20.20),
            Protocol: IGMP
```

Table 23 Command output

Field	Description
Routing table of VPN-Instance: public net	Public network IGMP routing table.
00001	Sequence number of this (*, G) entry.
(*, 225.1.1.1)	(*, G) entry of the IGMP routing table.
Flag	IGMP route flags: <ul style="list-style-type: none">• ACT—Indicates IGMP routing entries that have been used for forwarding data packets but have the multicast group address out of the SSM group range.• SUC—Indicates IGMP routing entries that have been added to the forwarding table and have the multicast group address within the SSM group range.
List of 1 downstream interface	Downstream interface list—list of the interfaces to which multicast data for this group is forwarded.
in include mode	The downstream interface is in the include mode.

Field	Description
in exclude mode	The downstream interface is in the exclude mode.
Downstream interface is none	No downstream interfaces exist.
Protocol	Protocol type.

display igmp ssm-mapping

Syntax

```
display igmp [ all-instance | vpn-instance vpn-instance-name ] ssm-mapping group-address [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

group-address: Specifies a multicast group by its IP address, in the range of 224.0.1.0 to 239.255.255.255.

|: 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 igmp ssm-mapping** to display the configured IGMP SSM mappings for the specified multicast group.

If neither **all-instance** nor **vpn-instance** is specified, this command displays the information on the public network.

Related commands: **ssm-mapping**.

Examples

Display the IGMP SSM mappings for multicast group 232.1.1.1 on the public network.

```
<Sysname> display igmp ssm-mapping 232.1.1.1
VPN-Instance: public net
Group: 232.1.1.1
Source list:
    1.2.3.4
    5.5.5.5
```

```
10.1.1.1
100.1.1.10
```

Table 24 Command output

Field	Description
VPN-Instance: public net	Public network
Group	Multicast group address
Source list	List of multicast source addresses

display igmp ssm-mapping group

Syntax

```
display igmp [ all-instance | vpn-instance vpn-instance-name ] ssm-mapping group [ group-address |
interface interface-type interface-number ] [ verbose ] [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

group-address: Specifies a multicast group by its IP address, in the range of 224.0.1.0 to 239.255.255.255. If you do not specify any multicast group, the command displays the information of all multicast groups created based on the configured IGMP SSM mappings.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify any interface, the command displays the multicast group information created based on the configured IGMP SSM mappings on all the interfaces.

verbose: Displays the detailed multicast group information created based on the configured IGMP SSM mappings.

|: 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 igmp ssm-mapping group** to display the multicast group information created based on the configured IGMP SSM mappings.

If neither **all-instance** nor **vpn-instance** is specified, this command displays the information on the public network.

Examples

Display detailed information about multicast group 232.1.1.1 created based on the configured IGMP SSM mappings on the public network.

```
<Sysname> display igmp ssm-mapping group 232.1.1.1 verbose
Interface group report information of VPN-Instance: public net
Vlan-interface1(10.10.10.10):
  Total 1 IGMP SSM-mapping Group reported
  Group: 232.1.1.1
    Uptime: 00:00:31
    Expires: off
    Last reporter: 1.1.1.1
    Version1-host-present-timer-expiry: off
  Source list(Total 1 source):
    Source: 1.1.1.1
      Uptime: 00:00:31
      Expires: 00:01:39
      Last-member-query-counter: 0
      Last-member-query-timer-expiry: off
```

Table 25 Command output

Field	Description
Interface group report information of VPN-Instance: public net	Multicast group information created based on IGMP SSM mappings on a public network interface.
Total 1 IGMP SSM-mapping Group reported	One IGMP SSM mapping multicast group was reported.
Group	Multicast group address.
Uptime	Length of time since the multicast group was reported.
Expires	Remaining time of the multicast group, where "off" means that the multicast group never times out.
Last reporter	Address of the last host that reported its membership for this multicast group.
Version1-host-present-timer-expiry	Remaining time of the IGMPv1 host present timer, where "off" means that the timer never expires.
Source list(Total 1 source)	Multicast source list (one multicast source).
Source	Multicast source address.
Last-member-query-counter	Number of last-member queries sent.
Last-member-query-timer-expiry	Remaining time of the last-member query timer, where "off" means that the timer never expires.

display igmp ssm-mapping host interface

Syntax

```
display igmp ssm-mapping host interface interface-type interface-number group group-address source source-address [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Displays information about the hosts that join a multicast group based on the IGMP SSM mappings on the specified interface. The specified interface can be a Layer 3 Ethernet port, Layer 3 aggregate interface, or Tunnel interface.

group *group-address*: Displays information about the hosts that join the specified multicast group based on the IGMP SSM mappings. The *group-address* argument is in the range of 224.0.1.0 to 239.255.255.255.

source *source-address*: Displays information about the hosts that join the specified multicast source based on the IGMP SSM mappings, where *source-address* is a valid unicast address or 0.0.0.0. A source IP address of 0.0.0.0 specifies all multicast sources.

|: 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 igmp ssm-mapping host interface** to display information about the hosts that join a multicast group based on the IGMP SSM mappings on an interface.

Examples

```
# Displays information about the hosts that join multicast source group (10.1.1.1, 224.1.1.1) based on the IGMP SSM mappings on Layer 3 Ethernet port GigabitEthernet 1/0/1.
```

```
<Sysname> display igmp ssm-mapping host interface gigabitethernet 1/0/1 group 224.1.1.1 source 10.1.1.1
```

```
Host information of VPN-Instance: public net
```

```
GigabitEthernet1/0/1(192.168.1.1):
```

```
(10.1.1.1, 224.1.1.1)
```

Host	Uptime	Expires
1.1.1.1	00:02:20	00:00:40
2.2.2.2	00:02:21	00:00:39

Table 26 Command output

Field	Description
Host information of VPN-Instance: public net	Information about the hosts that join the group based on the IGMP SSM mappings on public network interface
GigabitEthernet1/0/1(192.168.1.1) (10.1.1.1, 224.1.1.1)	Interface and IP address (S, G) entry
Host	Host IP address
Uptime	Host running duration
Expires	Host expiration time, where <i>timeout</i> means that the host has expired

dscp (IGMP view)

Syntax

```
dscp dscp-value  
undo dscp
```

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value for IGMP messages, in the range of 0 to 63.

Description

Use **dscp** to set the DSCP value for IGMP messages.

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

The default DSCP value in IGMP messages is 48.

Examples

```
# Set the DSCP value to 63 for IGMP messages on the public network.
```

```
<Sysname> system-view  
[Sysname] igmp  
[Sysname-igmp] dscp 63
```

```
# Set the DSCP value to 63 for IGMP protocol packets in VPN instance mvpn
```

```
<Sysname> system-view  
[Sysname] igmp vpn-instance mvpn  
[Sysname-igmp-mvpn] dscp 63
```

fast-leave (IGMP view)

Syntax

```
fast-leave [ group-policy acl-number ]
```


undo fast-leave

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

acl-number: Basic ACL number, in the range of 2000 to 2999. If you do not include this option in your command, this command takes effect for all multicast groups.

Description

Use **fast-leave** to enable fast-leave processing globally.

Use **undo fast-leave** to disable fast-leave processing globally.

By default, fast-leave processing is disabled, and the IGMP querier sends IGMP group-specific queries or IGMP group-and-source-specific queries after receiving an IGMP leave message from a host, instead of sending a leave notification directly to the upstream.

When executed in IGMP view, this command takes effect only on Layer 3 interfaces except VLAN interfaces.

Related commands: **igmp fast-leave** and **last-member-query-interval**.

Examples

```
# Enable fast-leave processing globally on the public network.
```

```
<Sysname> system-view  
[Sysname] igmp  
[Sysname-igmp] fast-leave
```

```
# Enable fast-leave processing globally in VPN instance mvpn.
```

```
<Sysname> system-view  
[Sysname] igmp vpn-instance mvpn  
[Sysname-igmp-mvpn] fast-leave
```

host-tracking (IGMP view)

Syntax

host-tracking

undo host-tracking

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

None

Description

Use **host-tracking** to enable the IGMP host tracking function globally.

Use **undo host-tracking** to disable the IGMP host tracking function globally.

By default, this function is disabled.

Related command: **igmp host-tracking**.

Examples

Enable the IGMP host tracking function globally on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] host-tracking
```

Enable the IGMP host tracking function globally in VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn] host-tracking
```

igmp

Syntax

igmp [**vpn-instance** *vpn-instance-name*]

undo igmp [**vpn-instance** *vpn-instance-name*]

View

System view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If this option is not specified, the command applies to the public network.

Description

Use **igmp** to enter public network IGMP view or VPN instance IGMP view.

Use **undo igmp** to remove configurations in public network IGMP view or VPN instance IGMP view.

IP multicast routing must be enabled in the corresponding VPN instance before this command can take effect.

Related commands: **igmp enable** and **multicast routing-enable**.

Examples

Enable IP multicast routing on the public network and enter public network IGMP view.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] igmp
[Sysname-igmp]
```

Enable IP multicast routing in VPN instance **mvpn** and enter IGMP view for VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] route-distinguisher 100:1
```

```
[Sysname-vpn-instance-mvpn] multicast routing-enable
[Sysname-vpn-instance-mvpn] quit
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn]
```

igmp enable

Syntax

```
igmp enable
undo igmp enable
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **igmp enable** to enable IGMP on the current interface.

Use **undo igmp enable** to disable IGMP on the current interface.

By default, IGMP is disabled on all interfaces.

IP multicast routing must be enabled in the corresponding instance before this command can take effect.

IGMP must be enabled on an interface before any other IGMP feature configured on the interface can take effect.

Related commands: **igmp** and **multicast routing-enable**.

Examples

```
# Enable IP multicast routing on the public network, and then enable IGMP on VLAN-interface 100.
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp enable
```

igmp fast-leave

Syntax

```
igmp fast-leave [ group-policy acl-number ]
undo igmp fast-leave
```

View

Interface view

Default level

2: System level

Parameters

acl-number: Basic ACL number, in the range of 2000 to 2999. If you do not include this option in your command, this command takes effect for all multicast groups.

Description

Use **igmp fast-leave** to configure fast-leave processing on the current interface.

Use **undo igmp fast-leave** to disable fast-leave processing on the current interface.

By default, fast-leave processing is disabled, and the IGMP querier sends IGMP group-specific queries or IGMP group-and-source-specific queries after receiving an IGMP leave message from a host, instead of sending a leave notification directly to the upstream.

The **igmp fast-leave** command cannot be used in VLAN-interface view. To enable fast-leave processing on a specific Layer 2 port or ports, use the **igmp-snooping fast-leave** command or the **fast-leave** (IGMP-snooping view) command.

The **igmp-snooping fast-leave** and **fast-leave** (IGMP-snooping view) commands are effective for both IGMP snooping-enabled VLANs and VLANs with IGMP enabled on the corresponding VLAN interfaces.

Related commands: **fast-leave** (IGMP view), **fast-leave** (IGMP-snooping view), **igmp last-member-query-interval**, and **igmp-snooping fast-leave**.

Examples

```
# Enable fast-leave processing on Layer 3 Ethernet port GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-mode route
[Sysname-GigabitEthernet1/0/1] igmp fast-leave
```

igmp group-limit

Syntax

```
igmp group-limit limit
undo igmp group-limit
```

View

Interface view

Default level

2: System level

Parameters

limit: Maximum number of multicast groups that an interface can join, in the range of 1 to 2000.

Description

Use **igmp group-limit** to configure the maximum number of multicast groups that an interface can join.

Use **undo igmp group-limit** to restore the default.

By default, the upper limit is 2000.

This command is effective only for dynamically joined multicast groups but not statically joined multicast groups.

If the configured *limit* value is smaller than the number of the existing multicast groups on the current interface, the system does not automatically remove the multicast groups in excess. To bring this configuration into effect in this case, use the **reset igmp group** command to clear the IGMP group information manually.

You can also use the **igmp-snooping group-limit** command to limit the number of multicast groups that an interface can join. However, if you configure the limit both in a VLAN and on a VLAN interface of this VLAN by using these two commands, inconsistencies might exist between Layer 2 and Layer 3 table entries. HP recommends you to configure the limit only on the VLAN interface.

Related commands: **igmp static-group**, **igmp-snooping group-limit**, and **reset igmp group**.

Examples

```
# Allow VLAN-interface 100 to join up to 128 multicast groups.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp group-limit 128
```

igmp group-policy

Syntax

```
igmp group-policy acl-number [ version-number ]
undo igmp group-policy
```

View

Interface view

Default level

2: System level

Parameters

acl-number: Basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule matches the multicast source address or addresses specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX and TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

version-number: IGMP version, in the range of 1 to 3. If you do not specify an IGMP version, the configured group filter applies to IGMP reports of all versions.

Description

Use **igmp group-policy** to configure a multicast group filter on the current interface to control the multicast groups that the hosts on the current interface can join.

Use **undo igmp group-policy** to remove the configured multicast group filter.

By default, no multicast group filter is configured, and a host can join any valid multicast group.

You can also use the **group-policy** (IGMP-snooping view) command to control the multicast groups that hosts in a VLAN can join, achieving the same result as **igmp group-policy**. If you have configured a multicast group filter on a VLAN interface to control the multicast groups that the hosts on the interface can join, HP recommends you to configure the same multicast group filter in the corresponding VLAN.

Related commands: **group-policy** (IGMP-snooping view).

Examples

```
# Configure an ACL rule so that hosts on VLAN-interface 100 can join multicast group 225.1.1.1 only.
<Sysname> system-view
[Sysname] acl number 2005
[Sysname-acl-basic-2005] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2005] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp group-policy 2005
```

igmp host-tracking

Syntax

```
igmp host-tracking
undo igmp host-tracking
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **igmp host-tracking** to enable the IGMP host tracking function on an interface.

Use **undo igmp host-tracking** to disable the IGMP host tracking function on an interface

By default, this function is disabled.

Related commands: **host-tracking**.

Examples

```
# Enable the IGMP host tracking function on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp host-tracking
```

igmp last-member-query-interval

Syntax

```
igmp last-member-query-interval interval
undo igmp last-member-query-interval
```

View

Interface view

Default level

2: System level

Parameters

interval: IGMP last-member query interval in seconds, in the range of 1 to 5.

Description

Use **igmp last-member-query-interval** to configure the last-member query interval, the length of time that the switch waits between sending IGMP group-specific queries on the current interface.

Use **undo igmp last-member-query-interval** to restore the default.

By default, the IGMP last-member query interval is 1 second.

Related commands: **display igmp interface**, **igmp robust-count**, and **last-member-query-interval**.

Examples

```
# Set the IGMP last-member query interval to 3 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp last-member-query-interval 3
```

igmp max-response-time

Syntax

igmp max-response-time *interval*

undo igmp max-response-time

View

Interface view

Default level

2: System level

Parameters

interval: Maximum response time in seconds for IGMP general queries, in the range of 1 to 25.

Description

Use **igmp max-response-time** to configure the maximum response time for IGMP general queries on the current interface.

Use **undo igmp max-response-time** to restore the default.

By default, the maximum response time for IGMP general queries is 10 seconds.

Related commands: **display igmp interface**, **igmp timer other-querier-present**, and **max-response-time**.

Examples

```
# Set the maximum response time for IGMP general queries to 8 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp max-response-time 8
```

igmp proxying enable

Syntax

igmp proxying enable

undo igmp proxying enable

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **igmp proxying enable** to enable IGMP proxying on an interface.

Use **undo igmp proxying enable** to disable IGMP proxying on the interface.

By default, IGMP proxying is disabled.

This command takes effect only after IP multicast routing is enabled on the corresponding instance.

If IGMP proxying is enabled on a loopback interface, the proxy switch maintains only the IGMP routing table without adding the IGMP routes to the multicast routing table and forwarding table.

Related commands: **multicast routing-enable**.

Examples

```
# Enable IP multicast routing on the public network and enable IGMP proxying on VLAN-interface 100.  
<Sysname> system-view  
[Sysname] multicast routing-enable  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] igmp proxying enable
```

igmp proxying forwarding

Syntax

igmp proxying forwarding

undo igmp proxying forwarding

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **igmp proxying forwarding** to enable a non-querier downstream interface to forward multicast traffic.

Use **undo igmp proxying forwarding** to disable the forwarding capability of a non-querier downstream interface.

By default, a non-querier downstream interface does not forward multicast traffic.

Examples

Enable the multicast forwarding capability on VLAN-interface 100, a non-querier downstream interface on the IGMP proxy switch.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp proxying forwarding
```

igmp require-router-alert

Syntax

```
igmp require-router-alert
undo igmp require-router-alert
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **igmp require-router-alert** to configure the interface to discard IGMP messages that do not carry the Router-Alert option.

Use **undo igmp require-router-alert** to restore the default.

By default, the switch does not check the Router-Alert option but passes all the IGMP messages that it receives to the upper layer protocol for processing.

Related commands: **igmp send-router-alert** and **require-router-alert**.

Examples

Configure VLAN-interface 100 to discard IGMP messages that do not carry the Router-Alert option.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp require-router-alert
```

igmp robust-count

Syntax

```
igmp robust-count robust-value
undo igmp robust-count
```

View

Interface view

Default level

2: System level

Parameters

robust-value: IGMP querier's robustness variable, in the range of 2 to 5.

Description

Use **igmp robust-count** to configure the IGMP querier's robustness variable on the current interface.

Use **undo igmp robust-count** to restore the default.

By default, the IGMP querier's robustness variable is 2.

The IGMP querier's robustness variable defines the maximum number of attempts for transmitting IGMP general queries, group-specific queries or group-and-source-specific queries in case of packet loss because of network problems. A greater value of the robustness variable makes the IGMP querier more robust, but results in a longer multicast group timeout time.

The IGMP querier's robustness variable determines the following values:

- The default number of general queries that the IGMPv1/v2/v3 querier sends on startup
- The number of IGMP group-specific queries that the IGMPv2 querier sends after receiving an IGMP leave message
- The number of IGMP group-and-source-specific queries that the IGMPv3 querier sends after receiving an IGMP report that tells relation changes between IPv6 multicast groups and IPv6 multicast sources

Related commands: **display igmp interface**, **igmp last-member-query-interval**, **igmp startup-query-count**, **igmp timer other-querier-present**, **igmp timer query**, and **robust-count**.

Examples

```
# Set the IGMP querier's robustness variable to 3 on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp robust-count 3
```

igmp send-router-alert

Syntax

igmp send-router-alert

undo igmp send-router-alert

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **igmp send-router-alert** to enable insertion of the Router-Alert option in IGMP messages to send through a port.

Use **undo igmp send-router-alert** to disable insertion of the Router-Alert option in IGMP messages to send through a port.

By default, IGMP messages are sent with the Router-Alert option.

Related commands: **igmp require-router-alert** and **send-router-alert**.

Examples

```
# Disable insertion of the Router-Alert option into IGMP messages that leave VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo igmp send-router-alert
```

igmp ssm-mapping enable

Syntax

```
igmp ssm-mapping enable
undo igmp ssm-mapping enable
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **igmp ssm-mapping enable** to enable the IGMP SSM mapping feature on the current interface.

Use **undo igmp ssm-mapping enable** to disable the IGMP SSM mapping feature on the current interface.

By default, the IGMP SSM mapping feature is disabled on all interfaces.

Examples

```
# Enable the IGMP SSM mapping feature on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp ssm-mapping enable
```

igmp startup-query-count

Syntax

```
igmp startup-query-count value
undo igmp startup-query-count
```

View

Interface view

Default level

2: System level

Parameters

value: Startup query count, the number of queries the IGMP querier sends on startup. The range is from 2 to 5.

Description

Use **igmp startup-query-count** to configure the startup query count on the current interface.

Use **undo igmp startup-query-count** to restore the default.

By default, the startup query count is set to the IGMP querier's robustness variable.

Related commands: **igmp robust-count** and **startup-query-count**.

Examples

```
# Set the startup query count to 3 on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp startup-query-count 3
```

igmp startup-query-interval

Syntax

igmp startup-query-interval *interval*

undo igmp startup-query-interval

View

Interface view

Default level

2: System level

Parameters

interval: Startup query interval in seconds, the interval between general queries that the IGMP querier sends on startup. The range is from 1 to 18000.

Description

Use **igmp startup-query-interval** to configure the startup query interval on the current interface.

Use **undo igmp startup-query-interval** to restore the default.

By default, the startup query interval is 1/4 of the IGMP general query interval.

Related commands: **igmp timer query** and **startup-query-interval**.

Examples

```
# Set the startup query interval to 5 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp startup-query-interval 5
```

igmp static-group

Syntax

igmp static-group *group-address* [**source** *source-address*]

```
undo igmp static-group { all | group-address [ source source-address ] }
```

View

Interface view

Default level

2: System level

Parameters

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Multicast source address.

all: Removes all static multicast groups that the current interface has joined.

Description

Use **igmp static-group** to configure the current interface to be a statically connected member of the specified multicast group or multicast source and group.

Use **undo igmp static-group** to restore the default.

By default, an interface is not a static member of any multicast group or multicast source and group.

If the specified multicast address is in the SSM multicast address range, you must specify a multicast source address at the same time. Otherwise, IGMP routing table entries cannot be established. No such a restriction exists if the specified multicast group address is not in the SSM multicast address range.

To configure a VLAN interface as a static member of a multicast group or multicast source and group, execute the **igmp static-group** command on the VLAN interface, and configure the **igmp-snooping static-group** command on the member ports of the corresponding VLAN.

Related commands: **igmp-snooping static-group**.

Examples

```
# Configure VLAN-interface 100 to be a statically connected member of multicast group 224.1.1.1.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] igmp static-group 224.1.1.1
```

```
# Configure VLAN-interface 100 to be a statically connected member of multicast source and group  
(192.168.1.1, 232.1.1.1).
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] igmp static-group 232.1.1.1 source 192.168.1.1
```

igmp timer other-querier-present

Syntax

```
igmp timer other-querier-present interval
```

```
undo igmp timer other-querier-present
```

View

Interface view

Default level

2: System level

Parameters

interval: IGMP other querier present interval in seconds, in the range of 60 to 300.

Description

Use **igmp timer other-querier-present** to configure the IGMP other querier present interval on the current interface.

Use **undo igmp timer other-querier-present** to restore the default.

By default, the IGMP other querier present interval is [IGMP general query interval] × [IGMP querier's robustness variable] + [maximum response time for IGMP general queries] / 2.

Related commands: **display igmp interface**, **igmp max-response-time**, **igmp robust-count**, **igmp timer query**, and **timer other-querier-present**.

Examples

```
# Set the IGMP other querier present interval to 200 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp timer other-querier-present 200
```

igmp timer query

Syntax

```
igmp timer query interval
```

```
undo igmp timer query
```

View

Interface view

Default level

2: System level

Parameters

interval: IGMP general query interval in seconds, the interval between IGMP general queries. The range is from 1 to 18000.

Description

Use **igmp timer query** to configure the IGMP general query interval on the current interface.

Use **undo igmp timer query** to restore the default.

By default, the IGMP general query interval is 60 seconds.

Related commands: **display igmp interface**, **igmp timer other-querier-present**, and **timer query**.

Examples

```
# Set the IGMP general query interval to 125 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp timer query 125
```

igmp version

Syntax

```
igmp version version-number  
undo igmp version
```

View

Interface view

Default level

2: System level

Parameters

version-number: IGMP version, in the range of 1 to 3.

Description

Use **igmp version** to configure the IGMP version on the current interface.

Use **undo igmp version** to restore the default IGMP version.

The default IGMP version is version 2.

Related commands: **version**.

Examples

```
# Set the IGMP version to IGMPv1 on VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] igmp version 1
```

last-member-query-interval (IGMP view)

Syntax

```
last-member-query-interval interval  
undo last-member-query-interval
```

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

interval: Last-member query interval in seconds, in the range of 1 to 5.

Description

Use **last-member-query-interval** to configure the global IGMP last-member query interval.

Use **undo last-member-query-interval** to restore the default.

By default, the IGMP last-member query interval is 1 second.

Related commands: **display igmp interface**, **igmp last-member-query-interval**, and **robust-count**.

Examples

Set the global IGMP last-member interval to 3 seconds on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] last-member-query-interval 3
```

Set the global IGMP last-member interval to 3 seconds in VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn] last-member-query-interval 3
```

max-response-time (IGMP view)

Syntax

max-response-time *interval*

undo max-response-time

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

interval: Maximum response time for IGMP general queries in seconds, in the range of 1 to 25.

Description

Use **max-response-time** to configure the maximum response time for IGMP general queries globally.

Use **undo max-response-time** to restore the default.

By default, the maximum response time for IGMP general queries is 10 seconds.

Related commands: **display igmp interface**, **igmp max-response-time**, and **timer other-querier-present**.

Examples

Set the maximum response time for IGMP general queries to 8 seconds globally on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] max-response-time 8
```

Set the maximum response time for IGMP general queries to 8 seconds globally in VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn] max-response-time 8
```

require-router-alert (IGMP view)

Syntax

require-router-alert

undo require-router-alert

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

None

Description

Use **require-router-alert** to configure the router globally to discard IGMP messages that do not carry the Router-Alert option.

Use **undo require-router-alert** to restore the default.

By default, the switch does not check the Router-Alert option but passes all the IGMP messages that it received to the upper layer protocol for processing.

Related commands: **igmp require-router-alert** and **send-router-alert**.

Examples

Configure the router to discard IGMP messages that do not carry the Router-Alert option globally on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] require-router-alert
```

Configure the router to discard IGMP messages that do not carry the Router-Alert option globally in VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn] require-router-alert
```

reset igmp group

Syntax

```
reset igmp [ all-instance | vpn-instance vpn-instance-name ] group { all | interface interface-type interface-number } { all | group-address [ mask { mask | mask-length } ] [ source-address [ mask { mask | mask-length } ] ] }
```

View

User view

Default level

2: System level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

all: Specifies all interfaces (the first **all**) or all IGMP groups (the second **all**).

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

group-address: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

source-address: Multicast source address.

mask: Subnet mask of the multicast group address or multicast source address, 255.255.255.255 by default.

mask-length: Subnet mask length of the multicast group address or multicast source address. For a multicast group address, this argument has an effective value range of 4 to 32. For a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

Description

Use **reset igmp group** to remove dynamic IGMP group entries.

If neither **all-instance** nor **vpn-instance** is specified, this command removes the dynamic IGMP group entries on the public network.

This command cannot remove static IGMP group entries.

Related commands: **display igmp group**.

Examples

Remove the dynamic IGMP group entries on all interfaces on the public network.

```
<Sysname> reset igmp group all
```

Remove the dynamic IGMP group entries on VLAN-interface 100 on the public network.

```
<Sysname> reset igmp group interface vlan-interface 100 all
```

Remove the dynamic IGMP group entry for the IGMP group 225.0.0.1 on VLAN-interface 100 on the public network.

```
<Sysname> reset igmp group interface vlan-interface 100 225.0.0.1
```

reset igmp group port-info

Syntax

```
reset igmp group port-info { all | group-address } [ vlan vlan-id ]
```

View

User view

Default level

2: System level

Parameters

all: Specifies all the IGMP groups.

group-address: Specifies an IGMP group. *group-address* is in the range of 224.0.1.0 to 239.255.255.255.

vlan-id: Specifies a VLAN. *vlan-id* is in the range 1 to 4094.

Description

Use **reset igmp group port-info** to remove dynamic Layer 2 port entries for IGMP groups.

Layer 2 ports for IGMP groups include member ports and router ports.

This command cannot remove static Layer 2 port entries of IGMP groups.

Related commands: **display igmp group port-info**.

Examples

```
# Remove the dynamic Layer 2 port entries for all IGMP groups in all VLANs.
<Sysname> reset igmp group port-info all

# Remove the dynamic Layer 2 port entries for all IGMP groups in VLAN 100.
<Sysname> reset igmp group port-info all vlan 100

# Remove the dynamic Layer 2 port entry for the multicast group 225.0.0.1 in VLAN 100.
<Sysname> reset igmp group port-info 225.0.0.1 vlan 100
```

reset igmp ssm-mapping group

Syntax

```
reset igmp [ all-instance | vpn-instance vpn-instance-name ] ssm-mapping group { all | interface interface-type interface-number { all | group-address [ mask { mask | mask-length } ] [ source-address [ mask { mask | mask-length } ] ] } }
```

View

User view

Default level

2: System level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

all: Specifies the multicast group information created based on the configured IGMP SSM mappings on all interfaces (the first **all**), or all multicast group information created based on the configured IGMP SSM mappings (the second **all**).

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

group-address: Specifies a multicast group by its IP address, in the range of 224.0.0.0 to 239.255.255.255.

source-address: Specifies a multicast source by its IP address.

mask: Subnet mask of the multicast group address or multicast source address, 255.255.255.255 by default.

mask-length: Subnet mask length of the multicast group address or multicast source address. For a multicast group address, this argument is in the range of 4 to 32. For a multicast source address, this argument is in the range of 0 to 32. For both cases, the default value is 32.

Description

Use **reset igmp ssm-mapping group** to clear multicast group information created based on the configured IGMP SSM mappings.

If neither **all-instance** nor **vpn-instance** is specified, this command clears the information on the public network.

Related commands: **display igmp ssm-mapping group**.

Examples

```
# Clear all multicast group information created based on the configured IGMP SSM mappings on all interfaces on the public network.
```

```
<Sysname> reset igmp ssm-mapping group all
```

robust-count (IGMP view)

Syntax

```
robust-count robust-value
```

```
undo robust-count
```

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

robust-value: IGMP querier's robustness variable, in the range of 2 to 5.

Description

Use **robust-count** to configure the IGMP querier's robustness variable globally.

Use **undo robust-count** to restore the default.

By default, the IGMP querier's robustness variable is 2.

The IGMP querier's robustness variable defines the maximum number of attempts for transmitting IGMP general queries, group-specific queries or group-and-source-specific queries in case of packet loss because of network problems. A greater value of the robustness variable makes the IGMP querier more robust, but results in a longer multicast group timeout time.

The IGMP querier's robustness variable determines the following values:

- The default number of general queries that the IGMPv1/v2/v3 querier sends on startup
- The number of IGMP group-specific queries that the IGMPv2 querier sends after receiving an IGMP leave message
- The number of IGMP group-and-source-specific queries that the IGMPv3 querier sends after receiving an IGMP report that indicates relation changes between IPv6 multicast groups and IPv6 multicast sources

Related commands: **display igmp interface**, **igmp robust-count**, **last-member-query-interval**, **startup-query-count**, **timer other-querier-present**, and **timer query**.

Examples

```
# Set the IGMP querier's robustness variable to 3 globally on the public network.
```

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

```
[Sysname] igmp
```

```
[Sysname-igmp] robust-count 3
```

```
# Set the IGMP querier's robustness variable to 3 globally in VPN instance mvpn.
```

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

```
[Sysname] igmp vpn-instance mvpn
```

```
[Sysname-igmp-mvpn] robust-count 3
```

send-router-alert (IGMP view)

Syntax

```
send-router-alert  
undo send-router-alert
```

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

None

Description

Use **send-router-alert** to globally enable insertion of the Router-Alert option into IGMP messages to be sent.

Use **undo send-router-alert** to globally disable insertion of the Router-Alert option into IGMP messages to be sent.

By default, an IGMP message carries the Router-Alert option.

Related commands: **igmp send-router-alert** and **require-router-alert**.

Examples

Globally disable the insertion of the Router-Alert option in IGMP messages to be sent on the public network.

```
<Sysname> system-view  
[Sysname] igmp  
[Sysname-igmp] undo send-router-alert
```

Globally disable the insertion of the Router-Alert option in IGMP messages to be sent in VPN instance **mvpn**.

```
<Sysname> system-view  
[Sysname] igmp vpn-instance mvpn  
[Sysname-igmp-mvpn] undo send-router-alert
```

ssm-mapping (IGMP view)

Syntax

```
ssm-mapping group-address { mask | mask-length } source-address  
undo ssm-mapping { group-address { mask | mask-length } source-address | all }
```

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

group-address: Specifies a multicast group by its IP address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Subnet mask of the multicast group address.

mask-length: Subnet mask length of the multicast group address, in the range of 4 to 32.

source-address: Specifies a multicast source by its IP address.

all: Removes all IGMP SSM mappings.

Description

Use **ssm-mapping** to configure an IGMP SSM mapping.

Use **undo ssm-mapping** to remove IGMP SSM mappings.

By default, no IGMP SSM mappings are configured.

Related commands: **display igmp ssm-mapping** and **igmp ssm-mapping enable**.

Examples

```
# Configure an IGMP SSM mapping on the public network for multicast groups in the range of 225.1.1.0/24 and multicast source 125.1.1.1.
```

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] ssm-mapping 225.1.1.0 24 125.1.1.1
```

```
# Configure an IGMP SSM mapping in VPN instance mvpn for multicast groups in the range of 225.1.1.0/24 and multicast source 125.1.1.1.
```

```
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn] ssm-mapping 225.1.1.0 24 125.1.1.1
```

startup-query-count (IGMP view)

Syntax

startup-query-count *value*

undo startup-query-count

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

value: Startup query count, the number of queries that the IGMP querier sends on startup. The range is from 2 to 5.

Description

Use **startup-query-count** to configure the startup query count globally.

Use **undo startup-query-count** to restore the default.

By default, the startup query count is set to the IGMP querier's robustness variable.

Related commands: **igmp startup-query-count** and **robust-count**.

Examples

```
# Set the startup query count to 3 globally on the public network.
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] startup-query-count 3

# Set the startup query count to 3 globally in VPN instance mvpn.
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn] startup-query-count 3
```

startup-query-interval (IGMP view)

Syntax

```
startup-query-interval interval
undo startup-query-interval
```

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

interval: Startup query interval in seconds, the interval between general queries that the IGMP querier sends on startup. The range is from 1 to 18000.

Description

Use **startup-query-interval** to configure the startup query interval globally.

Use **undo startup-query-interval** to restore the default.

By default, the startup query interval is 1/4 of the "IGMP general query interval".

Related commands: **igmp-startup-query-interval** and **timer query**.

Examples

```
# Set the startup query interval to 5 seconds globally on the public network.
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] startup-query-interval 5

# Set the startup query interval to 5 seconds globally in VPN instance mvpn.
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn] startup-query-interval 5
```

timer other-querier-present (IGMP view)

Syntax

```
timer other-querier-present interval
```

undo timer other-querier-present

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

interval: IGMP other querier present interval, in the range of 60 to 300.

Description

Use **timer other-querier-present** to configure the IGMP other querier present interval globally.

Use **undo timer other-querier-present** to restore the default.

By default, the IGMP other querier present interval is [IGMP general query interval] × [IGMP querier's robustness variable] + [maximum response time for IGMP general queries] / 2.

Related commands: **display igmp interface**, **igmp timer other-querier-present**, **max-response-time**, **robust-count**, and **timer query**.

Examples

Set the IGMP other querier present interval to 200 seconds globally on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] timer other-querier-present 200
```

Set the IGMP other querier present interval to 200 seconds globally in VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn] timer other-querier-present 200
```

timer query (IGMP view)

Syntax

timer query *interval*

undo timer query

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

interval: IGMP general query interval in seconds, interval between IGMP general queries. The range is from 1 to 18000.

Description

Use **timer query** to configure the IGMP general query interval globally.

Use **undo timer query** to restore the default.

By default, the IGMP general query interval is 60 seconds.

Related commands: **display igmp interface**, **igmp timer query**, and **timer other-querier-present**.

Examples

```
# Set the IGMP general query interval to 125 seconds globally on the public network.
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] timer query 125

# Set the IGMP general query interval to 125 seconds globally in VPN instance mvpn.
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn] timer query 125
```

version (IGMP view)

Syntax

```
version version-number
```

```
undo version
```

View

Public network IGMP view, VPN instance IGMP view

Default level

2: System level

Parameters

version-number: IGMP version, in the range of 1 to 3.

Description

Use **version** to configure the IGMP version globally.

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

The default IGMP version is version 2.

Related commands: **igmp version**.

Examples

```
# Set the global IGMP version to IGMPv1 on the public network.
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] version 1

# Set the global IGMP version to IGMPv1 in VPN instance mvpn.
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn] version 1
```

PIM configuration commands (available only on the HP 5500 EI)

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

The term "interface" in this chapter collectively refers to Layer 3 interfaces, including VLAN 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*).

auto-rp enable

Syntax

```
auto-rp enable  
undo auto-rp enable
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

None

Description

Use **auto-rp enable** to enable auto-RP.

Use **undo auto-rp enable** to disable auto-RP.

By default, auto-RP is disabled.

Related commands: **static-rp**.

Examples

```
# Enable auto-RP in the public network.  
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] auto-rp enable  
  
# Enable auto-RP in VPN instance mvpn.  
<Sysname> system-view  
[Sysname] pim vpn-instance mvpn  
[Sysname-pim-mvpn] auto-rp enable
```

bidir-pim enable (PIM view)

Syntax

```
bidir-pim enable
```

undo bidir-pim enable

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

None

Description

Use **bidir-pim enable** to enable BIDIR-PIM.

Use **undo bidir-pim enable** to disable BIDIR-PIM.

By default, BIDIR-PIM is disabled.

This command is effective only after multicast routing is enabled.

Related commands: **pim** and **multicast routing-enable**.

Examples

Enable multicast routing in the public network, enter PIM view, and enable BIDIR-PIM.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] pim
[Sysname-pim] bidir-pim enable
```

Enable multicast routing in VPN instance **mvpn**, enter VPN instance PIM view, and enable BIDIR-PIM.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] route-distinguisher 100:1
[Sysname-vpn-instance-mvpn] multicast routing-enable
[Sysname-vpn-instance-mvpn] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] bidir-pim enable
```

bsm-fragment enable (PIM view)

Syntax

bsm-fragment enable

undo bsm-fragment enable

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

None

Description

Use **bsm-fragment enable** to enable bootstrap message (BSM) semantic fragmentation.

Use **undo bsm-fragment enable** to disable BSM semantic fragmentation.

By default, BSM semantic fragmentation is enabled.

Disable the BSM semantic fragmentation function if devices that do not support this function exist in the PIM-SM domain.

Related commands: **c-bsr admin-scope**.

Examples

```
# Disable BSM semantic fragmentation in the public network.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] undo bsm-fragment enable
```

```
# Disable BSM semantic fragmentation in VPN instance mvpn.
```

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] undo bsm-fragment enable
```

bsr-policy (PIM view)

Syntax

```
bsr-policy acl-number
```

```
undo bsr-policy
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

acl-number: Basic ACL number, in the range of 2000 to 2999. When an ACL is defined, the **source** keyword in the **rule** command specifies a legal BSR source address range.

Description

Use **bsr-policy** to configure a legal BSR address range to guard against BSR spoofing.

Use **undo bsr-policy** to remove the restriction of the BSR address range.

By default, no restrictions are defined for the BSR address range. Namely, the bootstrap messages from any source are considered eligible.

Examples

```
# Configure a legal BSR address range in the public network so that only devices on the segment 10.1.1.0/24 can become the BSR.
```

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
```

```

[Sysname] pim
[Sysname-pim] bsr-policy 2000

# Configure a legal BSR address range in VPN instance mvpn so that only devices on the segment
10.1.1.0/24 can become the BSR.

<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] bsr-policy 2000

```

c-bsr (PIM view)

Syntax

c-bsr *interface-type interface-number* [*hash-length* [*priority*]]

undo c-bsr

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

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

hash-length: Specifies a hash mask length, in the range of 0 to 32. If you do not specify this argument, the corresponding global setting is used.

priority: Specifies the priority of the C-BSR, in the range of 0 to 255. A larger value of this argument means a higher priority. If you do not specify this argument, the corresponding global setting is used.

Description

Use **c-bsr** to configure the specified interface as a C-BSR.

Use **undo c-bsr** to remove the related C-BSR configuration.

No C-BSR is configured by default.

You must enable PIM-SM on the interface that you want to configure as a C-BSR.

Related commands: **c-bsr hash-length**, **c-bsr priority**, **c-rp**, and **pim sm**.

Examples

Configure VLAN-interface 100 in the public network to be a C-BSR.

```

<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr vlan-interface 100

```

Configure VLAN-interface 100 in VPN instance **mvpn** to be a C-BSR.

```

<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] c-bsr vlan-interface 100

```

c-bsr admin-scope (PIM view)

Syntax

```
c-bsr admin-scope  
undo c-bsr admin-scope
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

None

Description

Use **c-bsr admin-scope** to enable administrative scoping.

Use **undo c-bsr admin-scope** to disable administrative scoping.

By default, BSR administrative scoping is disabled. Namely, only one BSR exists in a PIM-SM domain.

Related commands: **c-bsr**, **c-bsr global**, and **c-bsr group**.

Examples

```
# Enable administrative scoping in the public network.
```

```
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] c-bsr admin-scope
```

```
# Enable administrative scoping in VPN instance mvpn.
```

```
<Sysname> system-view  
[Sysname] pim vpn-instance mvpn  
[Sysname-pim-mvpn] c-bsr admin-scope
```

c-bsr global

Syntax

```
c-bsr global [ hash-length hash-length | priority priority ] *  
undo c-bsr global
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

hash-length: Hash mask length in the global scope zone, in the range of 0 to 32. If you do not specify this argument, the corresponding global setting is used.

priority: Priority of the C-BSR in the global scope zone, in the range of 0 to 255. A larger value of this argument means a higher priority. If you do not specify this argument, the corresponding global setting is used.

Description

Use **c-bsr global** to configure a C-BSR for the global scope zone.

Use **undo c-bsr global** to remove the C-BSR configuration for the global scope zone.

By default, no C-BSRs are configured for the global scope zone.

Related commands: **c-bsr group**, **c-bsr hash-length**, and **c-bsr priority**.

Examples

Configure the device to be a C-BSR for the global scope zone in the public network, with the priority of 1.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr global priority 1
```

Configure the device to be a C-BSR for the global scope zone in VPN instance **mvpn**, with the priority of 1.

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] c-bsr global priority 1
```

c-bsr group

Syntax

c-bsr group *group-address* { *mask* | *mask-length* } [**hash-length** *hash-length* | **priority** *priority*] *
undo c-bsr group *group-address*

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

group-address: Specifies a multicast group address, in the range of 239.0.0.0 to 239.255.255.255.

mask: Specifies the mask of the multicast group address.

mask-length: Specifies the mask length of the multicast group address, in the range of 8 to 32.

hash-length *hash-length*: Specifies the hash mask length in the admin-scope region that corresponds to the specified multicast group, in the range of 0 to 32. If you do not specify this argument, the corresponding global setting is used.

priority *priority*: Specifies the priority of the C-BSR in the admin-scope region that corresponds to a multicast group, in the range of 0 to 255. A larger value of this argument means a higher priority. If you do not specify this argument, the corresponding global setting is used.

Description

Use **c-bsr group** to configure a C-BSR for the admin-scope region associated with the specified group.

Use **undo c-bsr group** to remove the C-BSR configuration for the admin-scope region associated with the specified group.

By default, no C-BSRs are configured for admin-scope regions.

Related commands: **c-bsr admin-scope**, **c-bsr global**, **c-bsr hash-length**, and **c-bsr priority**.

Examples

In the public network, configure the device to be a C-BSR in the admin-scope region associated with the multicast group address 239.0.0.0/8, with the priority of 10.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr group 239.0.0.0 255.0.0.0 priority 10
```

In VPN instance **mvpn**, configure the device to be a C-BSR in the admin-scope region associated with the multicast group address 239.0.0.0/8, with the priority of 10.

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] c-bsr group 239.0.0.0 255.0.0.0 priority 10
```

c-bsr hash-length (PIM view)

Syntax

c-bsr hash-length *hash-length*

undo c-bsr hash-length

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

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

Description

Use **c-bsr hash-length** to configure the global hash mask length.

Use **undo c-bsr hash-length** to restore the default.

By default, the hash mask length is 30.

Related commands: **c-bsr**, **c-bsr global**, and **c-bsr group**.

Examples

Set the global hash mask length to 16 in the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr hash-length 16
```

Set the global hash mask length to 16 in VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] c-bsr hash-length 16
```


c-bsr holdtime (PIM view)

Syntax

```
c-bsr holdtime interval  
undo c-bsr holdtime
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: BS timeout in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use **c-bsr holdtime** to configure the BS timeout timer, namely, the length of time that a C-BSR waits before it must receive a bootstrap message from the BSR.

Use **undo c-bsr holdtime** to restore the default.

By default, this formula determines the bootstrap timeout value: BS timeout = BS period × 2 + 10.

The default BS period is 60 seconds, so the default BS timeout is 60 × 2 + 10 = 130 (seconds).

Related commands: **c-bsr** and **c-bsr interval**.

Examples

```
# Set the BS timeout timer to 150 seconds in the public network.
```

```
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] c-bsr holdtime 150
```

```
# Set the BS timeout timer to 150 seconds in VPN instance mvpn.
```

```
<Sysname> system-view  
[Sysname] pim vpn-instance mvpn  
[Sysname-pim-mvpn] c-bsr holdtime 150
```

c-bsr interval (PIM view)

Syntax

```
c-bsr interval interval  
undo c-bsr interval
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: BS period in seconds, with an effective range of 10 to 2,147,483,647.

Description

Use **c-bsr interval** to configure the BS period, namely, the interval at which the BSR sends bootstrap messages.

Use **undo c-bsr interval** to restore the default.

By default, this formula determines the BS period value: $\text{BS period} = (\text{BS timeout} - 10) \div 2$.

The default BS timeout is 130 seconds, so the default BS period is $(130 - 10) \div 2 = 60$ (seconds).

Related commands: **c-bsr** and **c-bsr holdtime**.

Examples

```
# Set the BS period to 30 seconds in the public network.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr interval 30

# Set the BS period to 30 seconds in VPN instance mvpn.
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] c-bsr interval 30
```

c-bsr priority (PIM view)

Syntax

```
c-bsr priority priority
undo c-bsr priority
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

priority: Priority of the C-BSR, in the range of 0 to 255. A larger value of this argument means a higher priority.

Description

Use **c-bsr priority** to configure the global C-BSR priority.

Use **undo c-bsr priority** to restore the default.

By default, the C-BSR priority is 64.

Related commands: **c-bsr**, **c-bsr global**, and **c-bsr group**.

Examples

```
# Set the global C-BSR priority to 5 in the public network.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr priority 5

# Set the global C-BSR priority to 5 in VPN instance mvpn.
```

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] c-bsr priority 5
```

c-rp (PIM view)

Syntax

```
c-rp interface-type interface-number [ group-policy acl-number | priority priority | holdtime hold-interval  
| advertisement-interval adv-interval ] * [ bidir ]
```

```
undo c-rp interface-type interface-number
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

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

acl-number: Specifies a basic ACL number, in the range of 2000 to 2999. This ACL defines a range of multicast groups to which the C-RP is designated, rather than defining a filtering rule. Any group range that matches the **permit** statement in the ACL is advertised as a group to which the RP is designated, but the configuration that matches other statements, like **deny**, does not take effect.

priority: Specifies the priority of the C-RP, in the range of 0 to 255. The default is 192. A larger value of this argument means a lower priority.

hold-interval: Specifies the C-RP timeout time, in seconds. The value ranges from 1 to 65,535. If you do not provide this argument in your command, the corresponding global setting is used.

adv-interval: Specifies the C-RP-Adv interval in seconds, with an effective range of 1 to 65,535. If you do not provide this argument in your command, the corresponding global setting is used.

bidir: Configures the C-RP to provide services for multicast groups in BIDIR-PIM. Without this argument, the C-RP provides services for multicast groups in PIM-SM.

Description

Use **c-rp** to configure the specified interface as a C-RP.

Use **undo c-rp** to remove the related C-RP configuration.

No C-RPs are configured by default.

You must enable PIM-SM on the interface that you want to configure as a C-RP.

If you do not specify a group range for the C-RP, the C-RP provides service for all multicast groups.

To configure a device as a C-RP for multiple group ranges, you must include these multiple group ranges in multiple rules in the ACL that corresponds to the **group-policy** keyword.

If you use this command repeatedly on the same interface, the last configuration takes effect.

Related commands: **c-bsr**.

Examples

```
# Configure VLAN-interface 100 in the public network to be a C-RP for multicast groups 225.1.0.0/16  
and 226.2.0.0/16, with a priority of 10.
```

```

<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule permit source 226.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] c-rp vlan-interface 100 group-policy 2000 priority 10

# Configure VLAN-interface 100 in VPN instance mvpn to be a C-RP for multicast groups 225.1.0.0/16
and 226.2.0.0/16, with a priority of 10.
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule permit source 226.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] c-rp vlan-interface 100 group-policy 2000 priority 10

```

c-rp advertisement-interval (PIM view)

Syntax

c-rp advertisement-interval *interval*

undo c-rp advertisement-interval

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535.

Description

Use **c-rp advertisement-interval** to configure the interval at which C-RP-Adv messages are sent.

Use **undo c-rp advertisement-interval** to restore the default.

By default, the C-RP-Adv interval is 60 seconds.

Related commands: **c-rp**.

Examples

Set the global C-RP-Adv interval to 30 seconds in the public network.

```

<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-rp advertisement-interval 30

```

Set the global C-RP-Adv interval to 30 seconds in VPN instance **mvpn**.

```

<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] c-rp advertisement-interval 30

```

c-rp holdtime (PIM view)

Syntax

```
c-rp holdtime interval  
undo c-rp holdtime
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: C-RP timeout in seconds, with an effective range of 1 to 65,535.

Description

Use **c-rp holdtime** to configure the global C-RP timeout time, namely, the length of time that the BSR waits before it must receive a C-RP-Adv message.

Use **undo c-rp holdtime** to restore the default.

By default, the C-RP timeout time is 150 seconds.

Because a non-BSR router refreshes its C-RP timeout time through BSR bootstrap messages, to prevent loss of C-RP information in BSR bootstrap messages, be sure that the C-RP timeout time is not smaller than the interval at which the BSR sends bootstrap messages. The recommended C-RP timeout setting is 2.5 times the BS period or longer.

Related commands: **c-bsr interval** and **c-rp**.

Examples

Set the global C-RP timeout time to 200 seconds in the public network.

```
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] c-rp holdtime 200
```

Set the global C-RP timeout time to 200 seconds in VPN instance **mvpn**.

```
<Sysname> system-view  
[Sysname] pim vpn-instance mvpn  
[Sysname-pim-mvpn] c-rp holdtime 200
```

crp-policy (PIM view)

Syntax

```
crp-policy acl-number  
undo crp-policy
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

acl-number: Advanced ACL number, in the range of 3000 to 3999. When the ACL is defined, the **source** keyword in the **rule** command specifies the address of a C-RP, and the **destination** keyword specifies the address range of the multicast groups to which the C-RP is designated.

Description

Use **crp-policy** to configure a legal C-RP address range and the range of multicast groups to which the C-RP is designated, in order to guard against C-RP spoofing.

Use **undo crp-policy** to remove the restrictions in C-RP address ranges and the ranges of multicast groups to which the C-RP is designated.

By default, no restrictions are defined for C-RP address ranges and the address ranges of groups to which the C-RP is designated. All received C-RP messages are accepted.

The **crp-policy** command filters the multicast group ranges advertised by C-RPs based on the group prefixes. For example, if the multicast group range that a C-RP advertises is 224.1.0.0/16 and the legal group range that the **crp-policy** command defines is 224.1.0.0/30, the multicast groups in the range of 224.1.0.0/16 can pass.

Related commands: **c-rp**.

Examples

In the public network, configure a C-RP policy so that only devices in the address range of 1.1.1.1/24 can be C-RPs that provide services for multicast groups in the address range of 225.1.1.0/24.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 1.1.1.1 0.0.0.255 destination 225.1.1.0
0.0.0.255
[Sysname-acl-adv-3000] quit
[Sysname] pim
[Sysname-pim] crp-policy 3000
```

In VPN instance **mvpn**, configure a C-RP policy, so that only devices in the address range of 1.1.1.1/24 can be C-RPs that provide services for multicast groups in the address range of 225.1.1.0/24.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 1.1.1.1 0.0.0.255 destination 225.1.1.0
0.0.0.255
[Sysname-acl-adv-3000] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] crp-policy 3000
```

display pim bsr-info

Syntax

```
display pim [ all-instance | vpn-instance vpn-instance-name ] bsr-info [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *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.

Description

Use **display pim bsr-info** to display BSR information in the PIM domain and the locally configured C-RP information in effect.

If neither **all-instance** nor **vpn-instance** is specified, this command displays the information in the public network.

Related commands: **c-bsr** and **c-rp**.

Examples

Display the BSR information of the PIM-SM domain in the public network and the locally configured C-RP information in effect.

```
<Sysname> display pim bsr-info
VPN-Instance: public net
Elected BSR Address: 12.12.12.9
  Priority: 64
  Hash mask length: 30
  State: Elected
  Scope: Global
  Uptime: 00:00:56
  Next BSR message scheduled at: 00:01:14
Candidate BSR Address: 12.12.12.9
  Priority: 64
  Hash mask length: 30
  State: Elected
  Scope: Global

Candidate RP: 12.12.12.9(LoopBack1)
  Priority: 192
  HoldTime: 150
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:48
Candidate RP: 3.3.3.3(Vlan-interface1)
  Priority: 200
```

```

HoldTime: 90
Advertisement Interval: 50
Next advertisement scheduled at: 00:00:28
Candidate RP: 5.5.5.5(Vlan-interface2)
Priority: 192
HoldTime: 80
Advertisement Interval: 60
Next advertisement scheduled at: 00:00:48

```

Table 27 Command output

Field	Description
VPN-Instance: public net	Public network
Elected BSR Address	Address of the elected BSR
Candidate BSR Address	Address of the candidate BSR
Priority	BSR priority
Hash mask length	Hash mask length
State	BSR state
Scope	Scope of the BSR
Uptime	Length of time for which this BSR has been up, in hh:mm:ss
Next BSR message scheduled at	Length of time in which the BSR will expire, in hh:mm:ss
Candidate RP	Address of the C-RP
Priority	Priority of the C-RP
HoldTime	Timeout time of the C-RP
Advertisement Interval	Interval at which the C-RP sends advertisement messages
Next advertisement scheduled at	Length of time in which the C-RP will send the next advertisement message, in hh:mm:ss

display pim claimed-route

Syntax

```

display pim [ all-instance | vpn-instance vpn-instance-name ] claimed-route [ source-address ] [ [
{ begin | exclude | include } regular-expression ]

```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

source-address: Displays the information of the unicast route to a particular multicast source. If you do not provide this argument, this command will display the information about all unicast routes that PIM uses.

|: 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 pim claimed-route** to display information about unicast routes that PIM uses.

If neither **all-instance** nor **vpn-instance** is specified, this command displays the information in the public network.

If an (S, G) is marked SPT, this (S, G) entry uses a unicast route.

Examples

Display the information of all unicast routes that PIM uses in the public network.

```
<Sysname> display pim claimed-route
VPN-Instance: public net
RPF information about: 172.168.0.0
  RPF interface: Vlan-interface1, RPF neighbor: 172.168.0.2
  Referenced route/mask: 172.168.0.0/24
  Referenced route type: unicast (direct)
  RPF-route selecting rule: preference-preferred
  The (S,G) or (*,G) list dependent on this route entry
  (172.168.0.12, 227.0.0.1)
```

Table 28 Command output

Field	Description
VPN-Instance: public net	Public network.
RPF information about: 172.168.0.0	Information of the route to the multicast source 172.168.0.0.
RPF interface	RPF interface type and number.
RPF neighbor	IP address of the RPF neighbor.
Referenced route/mask	Address/mask of the referenced route.
Referenced route type	Type of the referenced route: <ul style="list-style-type: none"> • igp—IGP unicast route. • egp—EGP unicast route. • unicast (direct)—Direct unicast route. • unicast—Other unicast route (such as static unicast route). • mbgp—MBGP route. • multicast static—Static multicast route.
RPF-route selecting rule	Rule of RPF route selection.

Field	Description
The (S,G) or (*,G) list dependent on this route entry	(S,G) or (*, G) entry list dependent on this RPF route.

display pim control-message counters

Syntax

```
display pim [ all-instance | vpn-instance vpn-instance-name ] control-message counters [ message-type { probe | register | register-stop } | [ interface interface-type interface-number | message-type { assert | bsr | crp | graft | graft-ack | hello | join-prune | state-refresh } ] * ] [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

probe: Displays the number of null register messages.

register: Displays the number of register messages.

register-stop: Displays the number of register-stop messages.

interface *interface-type interface-number*: Displays the number of PIM control messages on the specified interface.

assert: Displays the number of assert messages.

bsr: Displays the number of bootstrap messages.

crp: Displays the number of C-RP-Adv messages.

graft: Displays the number of graft messages.

graft-ack: Displays the number of graft-ack messages.

hello: Displays the number of hello messages.

join-prune: Displays the number of join/prune messages.

state-refresh: Displays the number of state refresh messages.

|: 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 pim control-message counters** to display statistics for PIM control messages.

If neither **all-instance** nor **vpn-instance** is specified, this command displays statistics for PIM control messages on the public network.

Examples

Display statistics for PIM control messages on all interfaces on the public network.

```
<Sysname> display pim control-message counters
VPN-Instance: public net
PIM global control-message counters:

      Received      Sent      Invalid
Register      20        37         2
Register-Stop  25        20         1
Probe         10         5          0

PIM control-message counters for interface: Vlan-interface1

      Received      Sent      Invalid
Assert      10         5          0
Graft       20        37         2
Graft-Ack   25        20         1
Hello      1232      453         0
Join/Prune  15        30         21
State-Refresh  8         7          1
BSR        3243      589         1
C-RP       53        32          0
```

Table 29 Command output

Field	Description
VPN-Instance: public net	Public network
PIM global control-message counters	Statistics for PIM global control messages
PIM control-message counters for interface	Interface for which PIM control messages were counted
Received	Number of messages received
Sent	Number of messages sent
Invalid	Number of invalid messages
Register	Register messages
Register-Stop	Register-stop messages
Probe	Null register messages
Assert	Assert messages
Graft	Graft messages
Graft-Ack	Graft-ack messages
Hello	Hello messages
Join/Prune	Join/prune messages
State Refresh	State refresh messages

Field	Description
BSR	Bootstrap messages
C-RP	C-RP-Adv messages

display pim df-info

Syntax

```
display pim [ all-instance | vpn-instance vpn-instance-name ] df-info [ rp-address ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all instances.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case-sensitive string of up to 31 characters and must not contain any space.

rp-address: Specifies the RP address of BIDIR-PIM.

|: 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 the 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 pim df-info** to display the DF information of BIDIR-PIM.

If neither **all-instance** nor **vpn-instance** is specified, this command displays the DF information of BIDIR-PIM in the public network.

Examples

Display the DF information of BIDIR-PIM in the public network.

```
<Sysname> display pim df-info
```

```
VPN-Instance: public net
```

```
RP Address: 1.1.1.1
```

Interface	State	DF-Pref	DF-Metric	DF-Uptime	DF-Address
Vlan1	Win	100	1	01:24:09	192.168.2.1 (local)
Vlan2	Win	100	1	01:24:09	10.110.1.2 (local)
Vlan3	Lose	0	0	01:23:12	10.110.2.2

Table 30 Command output

Field	Description
VPN-Instance: public net	Public network
RP Address	BIDIR-PIM RP address
Interface	Interface type and number
State	DF election state, Win or Lose.
DF-Pref	Route priority of DF
DF-Metric	Route metric of DF
DF-Uptime	Existence duration of DF
DF-Address	IP address of DF, where local indicates a local address

display pim grafts

Syntax

```
display pim [ all-instance | vpn-instance vpn-instance-name ] grafts [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *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.

Description

Use **display pim grafts** to display information about unacknowledged PIM-DM graft messages.

If neither **all-instance** nor **vpn-instance** is specified, this command displays information about unacknowledged graft messages in the public network.

Examples

Display information about unacknowledged PIM-DM graft messages in the public network.

```
<Sysname> display pim grafts
VPN-Instance: public net
Source          Group          Age          RetransmitIn
```

192.168.10.1 224.1.1.1 00:00:24 00:00:02

Table 31 Command output

Field	Description
VPN-Instance: public net	Public network
Source	Multicast source address in the graft message
Group	Multicast group address in the graft message
Age	Time in which the graft message will age out, in hh:mm:ss
RetransmitIn	Time in which the graft message will be retransmitted, in hh:mm:ss

display pim interface

Syntax

```
display pim [ all-instance | vpn-instance vpn-instance-name ] interface [ interface-type interface-number ]
[ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

interface-type interface-number: Displays the PIM information on a particular interface.

verbose: Displays the detailed PIM 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 pim interface** to display PIM information on the specified interface or all interfaces.

If neither **all-instance** nor **vpn-instance** is specified, this command displays PIM information on all interfaces in the public network.

Examples

```
# Display the PIM information on all interfaces in the public network.
```

```
<Sysname> display pim interface
VPN-Instance: public net
Interface          NbrCnt HelloInt  DR-Pri  DR-Address
```

Vlan1	1	30	1	10.1.1.2	
Vlan2	0	30	1	172.168.0.2	(local)
Vlan3	1	30	1	20.1.1.2	

Table 32 Command output

Field	Description
VPN-Instance: public net	Public network
Interface	Interface name
NbrCnt	Number of PIM neighbors
HelloInt	Hello interval
DR-Pri	Priority for DR election
DR-Address	DR IP address, where "local" indicates a local address

Display detailed PIM information on VLAN-interface1 in the public network.

```
<Sysname> display pim interface vlan-interface 1 verbose
VPN-Instance: public net
Interface: Vlan-interface1, 10.1.1.1
  PIM version: 2
  PIM mode: Sparse
  PIM DR: 10.1.1.2
  PIM DR Priority (configured): 1
  PIM neighbor count: 1
  PIM hello interval: 30 s
  PIM LAN delay (negotiated): 500 ms
  PIM LAN delay (configured): 500 ms
  PIM override interval (negotiated): 2500 ms
  PIM override interval (configured): 2500 ms
  PIM neighbor tracking (negotiated): disabled
  PIM neighbor tracking (configured): disabled
  PIM generation ID: 0xF5712241
  PIM require generation ID: disabled
  PIM hello hold interval: 105 s
  PIM assert hold interval: 180 s
  PIM triggered hello delay: 5 s
  PIM J/P interval: 60 s
  PIM J/P hold interval: 210 s
  PIM BSR domain border: disabled
  Number of routers on network not using DR priority: 0
  Number of routers on network not using LAN delay: 0
  Number of routers on network not using neighbor tracking: 2
```

Table 33 Command output

Field	Description
VPN-Instance: public net	Public network
Interface	Interface name and its IP address

Field	Description
PIM version	Running PIM version
PIM mode	PIM mode, dense or sparse
PIM DR	DR IP address
PIM DR Priority (configured)	Configured priority for DR election
PIM neighbor count	Total number of PIM neighbors
PIM hello interval	Hello interval
PIM LAN delay (negotiated)	Negotiated prune message delay
PIM LAN delay (configured)	Configured prune message delay
PIM override interval (negotiated)	Negotiated prune override interval
PIM override interval (configured)	Configured prune override interval
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status (enabled/disabled)
PIM neighbor tracking (configured)	Configured neighbor tracking status (enabled/disabled)
PIM generation ID	Generation_ID value
PIM require generation ID	Rejection of hello messages without Generation_ID (enabled/disabled)
PIM hello hold interval	PIM neighbor timeout time
PIM assert hold interval	Assert timeout time
PIM triggered hello delay	Maximum delay of sending hello messages
PIM J/P interval	Join/prune interval
PIM J/P hold interval	Join/prune timeout time
PIM BSR domain border	Status of PIM domain border configuration (enabled/disabled)
Number of routers on network not using DR priority	Number of routers not using the DR priority field on the subnet where the interface resides
Number of routers on network not using LAN delay	Number of routers not using the LAN delay field on the subnet where the interface resides
Number of routers on network not using neighbor tracking	Number of routers not using neighbor tracking on the subnet where the interface resides

display pim join-prune

Syntax

```
display pim [ all-instance | vpn-instance vpn-instance-name ] join-prune mode { sm [ flags flag-value ]
| ssm } [ interface interface-type interface-number | neighbor neighbor-address ] * [ verbose ] [ | { begin
| exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

mode: Displays the information of join/prune messages to send in the specified PIM mode. PIM modes include **sm** and **ssm**, which represent PIM-SM and PIM-SSM respectively.

flags *flag-value*: Displays routing entries that contain the specified flag. Values and meanings of *flag-value* are as follows:

- **rpt:** Specifies routing entries on the RPT.
- **spt:** Specifies routing entries on the SPT.
- **wc:** Specifies wildcard routing entries.

interface-type interface-number: Displays the information of join/prune messages to send on the specified interface.

neighbor-address: Displays the information of join/prune messages to send to the specified PIM neighbor.

verbose: Displays the detailed information of join/prune messages to send.

|: 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 pim join-prune** to display information about the join/prune messages to send.

If neither **all-instance** nor **vpn-instance** is specified, this command displays information about the join/prune messages to send in the public network.

Examples

In the public network, view the information about join/prune messages to send in the PIM-SM mode.

```
<Sysname> display pim join-prune mode sm
```

```
VPN-Instance: public net
```

```
Expiry Time: 50 sec
```

```
Upstream nbr: 10.1.1.1 (Vlan-interface1)
```

```
1 (*, G) join(s), 0 (S, G) join(s), 1 (S, G, rpt) prune(s)
```

```
-----  
Total (*, G) join(s): 1, (S, G) join(s): 0, (S, G, rpt) prune(s): 1
```

Table 34 Command output

Field	Description
VPN-Instance: public net	Public network
Expiry Time:	Expiry time of sending join/prune messages

Field	Description
Upstream nbr:	IP address of the upstream PIM neighbor and the interface that connects to it
(*, G) join(s)	Number of (*, G) joins to send
(S, G) join(s)	Number of (S, G) joins to send
(S, G, rpt) prune(s)	Number of (S, G, rpt) prunes

display pim neighbor

Syntax

```
display pim [ all-instance | vpn-instance vpn-instance-name ] neighbor [ interface interface-type
interface-number | neighbor-address | verbose ] * [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

interface-type interface-number: Displays the PIM neighbor information on a particular interface.

neighbor-address: Displays the information of a particular PIM neighbor.

verbose: Displays the detailed PIM neighbor 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 pim neighbor** to display the PIM neighbor information.

If neither **all-instance** nor **vpn-instance** is specified, this command displays information about all PIM neighbors in the public network.

Examples

```
# Display information about all PIM neighbors in the public network.
```

```
<Sysname> display pim neighbor
VPN-Instance: public net
Total Number of Neighbors = 2
```

```
Neighbor          Interface          Uptime    Expires    Dr-Priority    Mode
```

```

10.1.1.2      Vlan1      02:50:49 00:01:31 1      B
20.1.1.2      Vlan2      02:49:39 00:01:42 1      B

```

In the public network, view the detailed information of the PIM neighbor whose IP address is 11.110.0.20.

```

<Sysname> display pim neighbor 11.110.0.20 verbose
VPN-Instance: public net
Neighbor: 11.110.0.20
  Interface: Vlan-interface3
  Uptime: 00:00:10
  Expiry time: 00:00:30
  DR Priority: 1
  Generation ID: 0x2ACEFE15
  Holdtime: 105 s
  LAN delay: 500 ms
  Override interval: 2500 ms
  State refresh interval: 60 s
  Neighbor tracking: Disabled
  Bidirectional PIM: Disabled

```

Table 35 Command output

Field	Description
VPN-Instance: public net	Public network.
Total Number of Neighbors	Total number of PIM neighbors.
Neighbor	IP address of the PIM neighbor.
Interface	Interface that connects to the PIM neighbor.
Uptime	Length of time for which the PIM neighbor has been up, in hh:mm:ss.
Expires/Expiry time	Remaining time of the PIM neighbor, in hh:mm:ss. "Never" means that the PIM neighbor is always up and reachable.
Dr-Priority/DR Priority	Priority of the PIM neighbor.
Mode	Mode of the PIM neighbor. The value "B" means the BIDIR-PIM mode. If nothing is displayed, it means the non-BIDIR-PIM mode.
Generation ID	Generation ID of the PIM neighbor. (A random value that indicates a status change of the PIM neighbor.)
Holdtime	Holdtime of the PIM neighbor; "forever" means that the PIM neighbor is always up and reachable.
LAN delay	Prune message delay.
Override interval	Prune override interval.
State refresh interval	Interval for sending state refresh messages. Displayed only when the PIM neighbor operates in PIM-DM mode and the state refresh capability is enabled.
Neighbor tracking	Neighbor tracking status (enabled/disabled).
Bidirectional PIM	BIDIR-PIM status (enabled/disabled).

display pim routing-table

Syntax

```
display pim [ all-instance | vpn-instance vpn-instance-name ] routing-table [ group-address [ mask { mask-length | mask } ] | source-address [ mask { mask-length | mask } ] | incoming-interface [ interface-type interface-number | register ] | outgoing-interface { include | exclude | match } { interface-type interface-number | register } | mode mode-type | flags flag-value | fsm ] * [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

group-address: Specifies a multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

source-address: Specifies a multicast source address.

mask: Specifies the mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Specifies the mask length of the multicast group/source address, in the range of 0 to 32. The default is 32.

incoming-interface: Displays PIM routing entries that contain the specified interface as the incoming interface.

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

register: Specifies the register interface. This keyword is valid only if *mode-type* is not specified or is **sm**.

outgoing-interface: Displays PIM routing entries, where the outgoing interface is the specified interface.

include: Displays PIM routing entries, where the outgoing interface list includes the specified interface.

exclude: Displays PIM routing entries, where the outgoing interface list excludes the specified interface.

match: Displays PIM routing entries, where the outgoing interface list includes only the specified interface.

mode *mode-type*: Specifies a PIM mode, where *mode-type* can have the following values:

- **dm**: Specifies PIM-DM.
- **sm**: Specifies PIM-SM.
- **ssm**: Specifies PIM-SSM.

flags *flag-value*: Displays PIM routing entries that contains the specified flags. The values of *flag-value* and their meanings are as follows:

- **2msdp**: Specifies PIM routing entries to be contained in the next SA message to notify an MSDP peer.
- **act**: Specifies PIM routing entries that have been used for routing data.
- **bidir**: Specifies PIM routing entries created by BIDIR-PIM.

- **del**: Specifies PIM routing entries scheduled to be deleted.
- **exprune**: Specifies PIM routing entries that contain outgoing interfaces pruned by other multicast routing protocols.
- **ext**: Specifies PIM routing entries that contain outgoing interfaces provided by other multicast routing protocols.
- **loc**: Specifies PIM routing entries on the devices that directly connect to the same subnet as the multicast source.
- **msdp**: Specifies PIM routing entries obtained from MSDP SA messages.
- **niif**: Specifies PIM routing entries that contain unknown incoming interfaces.
- **nonbr**: Specifies PIM routing entries with PIM neighbor searching failure.
- **rpt**: Specifies PIM routing entries on RPT branches where (S, G) prunes have been sent to the RP.
- **rq**: Specifies PIM routing entries of the receiving side of the switch-MDT switchover.
- **spt**: Specifies PIM routing entries on the SPT.
- **sq**: Specifies PIM routing entries of the originator side of switch-MDT switchover.
- **swt**: Specifies PIM routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies wildcard routing entries.

fsm: Displays the information of the state machine.

|: 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 pim routing-table** to display PIM routing table information.

If neither **all-instance** nor **vpn-instance** is specified, this command displays information about PIM routing tables in the public network.

Related commands: **display multicast routing-table**.

Examples

Display the content of the PIM routing table in the public network.

```
<Sysname> display pim routing-table
VPN-Instance: public net
Total 0 (*, G) entry; 1 (S, G) entry

(172.168.0.12, 227.0.0.1)
  RP: 2.2.2.2
  Protocol: pim-sm, Flag: SPT LOC ACT
  UpTime: 02:54:43
  Upstream interface: Vlan-interface1
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
```

```

Total number of downstreams: 1
  1: Vlan-interface2
      Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
# Display the state machine information in the PIM routing table in the public network.
<Sysname> display pim routing-table fsm
VPN-Instance: public net
Total 0 (*, G) entry; 1 (S, G) entry

Abbreviations for FSM states:
NI - no info, J - joined, NJ - not joined, P - pruned,
NP - not pruned, PP - prune pending, W - winner, L - loser,
F - forwarding, AP - ack pending, DR - designated router,
NDR - non-designated router, RCV - downstream receivers

(172.168.0.12, 227.0.0.1)
RP: 2.2.2.2
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 02:54:43
Upstream interface: Vlan-interface1
  Upstream neighbor: NULL
  RPF prime neighbor: NULL
  Join/Prune FSM: [SPT: J] [RPT: NP]
Downstream interface(s) information:
Total number of downstreams: 1
  1: Vlan-interface2
      Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
      DR state: [DR]
      Join/Prune FSM: [NI]
      Assert FSM: [NI]

FSM information for non-downstream interfaces: None

```

Table 36 Command output

Field	Description
VPN-Instance: public net	Public network.
Total 0 (*, G) entry; 1 (S, G) entry	Number of (S,G) and (*, G) entries in the PIM routing table.
(172.168.0.2, 227.0.0.1)	(S, G) entry in the PIM routing table.
RP	IP address of the RP.
Protocol	PIM mode.

Field	Description
Flag	<p>Flag of the (S, G) or (*, G) entry in the PIM routing table:</p> <ul style="list-style-type: none"> • 2MSDP—The entry is contained in the next SA message to notify an MSDP peer. • ACT—The entry has been used for routing data. • BIDIR—The entry was created by BIDIR-PIM. • DEL—The entry will be removed. • EXPRUNE—Some outgoing interfaces are pruned by other multicast routing protocols. • EXT—The entry contains outgoing interfaces provided by other multicast routing protocols. • LOC—The entry is on a router directly connected to the same subnet with the multicast source. • MSDP—The entry is learnt from MSDP SA messages. • NIIF—The entry contains unknown incoming interfaces. • NONBR—The entry has a PIM neighbor searching failure. • RPT—The entry is on a RPT branch where (S, G) prunes have been sent to the RP. • RQ—The entry is on the receiving side of the switch-MDT switchover. • SPT—The entry is on the SPT. • SQ—The entry is on the originator side of switch-MDT switchover. • SWT—The entry is in the process of RPT-to-SPT switchover. • WC—The entry is a wildcard routing entry.
Uptime	Length of time for which the (S, G) or (*, G) entry has existed.
Upstream interface	Upstream (incoming) interface of the (S, G) or (*, G) entry. If the upstream interface is an interface of another VPN, the VPN name is displayed.
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry.
RPF prime neighbor	<p>RPF neighbor of the (S, G) or (*, G) entry:</p> <ul style="list-style-type: none"> • For a (*, G) entry, if this router is the RP, the RPF neighbor of this (*, G) entry is NULL. • For an (S, G) entry, if this router directly connects to the multicast source, the RPF neighbor of this (S, G) entry is NULL.
Downstream interface(s) information	<p>Information of the downstream interfaces, including the following:</p> <ul style="list-style-type: none"> • Number of downstream interfaces. • Downstream interface name. If the downstream interface is an interface of another VPN, the VPN name is displayed. • Protocol type on the downstream interfaces. If the downstream interface is an interface of another VPN, extra_vpn is displayed. • Uptime of the downstream interfaces. • Expiry time of the downstream interfaces.

display pim rp-info

Syntax

```
display pim [ all-instance | vpn-instance vpn-instance-name ] rp-info [ group-address ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

group-address: Specifies the address of a multicast group, in the range of 224.0.1.0 to 239.255.255.255. If you do not provide a group address, this command displays information about the RPs that correspond to all multicast groups.

|: 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 pim rp-info** to display the RP information.

If neither **all-instance** nor **vpn-instance** is specified, this command displays information about RPs in the public network.

The RP information includes the information of RPs dynamically found by the BSR mechanism and static RPs.

Examples

```
# Display information about the RP that corresponds to the multicast group 224.0.1.1 in the public network.
```

```
<Sysname> display pim rp-info 224.0.1.1
  VPN-Instance: public net
  BSR RP Address is: 2.2.2.2
    Priority: 192
    HoldTime: 150
    Uptime: 03:01:10
    Expires: 00:02:30
  RP mapping for this group is: 2.2.2.2
```

```
# Display information about the RP that corresponds to all multicast groups in the public network.
```

```
<Sysname> display pim rp-info
```



```

VPN-Instance: public net
PIM-SM BSR RP information:
Group/MaskLen: 224.0.0.0/4 [B]
  RP: 2.2.2.2
  Priority: 192
  HoldTime: 150
  Uptime: 03:01:36
  Expires: 00:02:29

```

Table 37 Command output

Field	Description
VPN-Instance: public net	Public network.
BSR RP Address is	IP address of the RP.
Group/MaskLen	Multicast group to which the RP is designated.
[B]	The RP provides services for multicast groups in BIDIR-PIM. If this field is not displayed, it means that the RP provides services for groups in PIM-SM.
RP	IP address of the RP.
Priority	RP priority.
HoldTime	RP timeout time.
Uptime	Length of time for which the RP has been up, in hh:mm:ss.
Expires	Length of time in which the RP will expire, in hh:mm:ss.
RP mapping for this group	IP address of the RP that provides services for the current multicast group.

dscp (PIM view)

Syntax

```

dscp dscp-value
undo dscp

```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value for PIM messages, in the range of 0 to 63.

Description

Use **dscp** to set the DSCP value for PIM messages.

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

The default DSCP value in PIM messages is 48.

Examples

```
# Set the DSCP value to 63 for PIM messages on the public network.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] dscp 63
```

```
# Set the DSCP value to 63 for PIM messages in VPN instance mvpn.
```

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] dscp 63
```

hello-option dr-priority (PIM view)

Syntax

```
hello-option dr-priority priority
```

```
undo hello-option dr-priority
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

priority: Router priority for DR election, in the range of 0 to 4294967295. A larger value of this argument means a higher priority.

Description

Use **hello-option dr-priority** to configure the global value of the router priority for DR election.

Use **undo hello-option dr-priority** to restore the default.

By default, the router priority for DR election is 1.

Related commands: **pim hello-option dr-priority**.

Examples

```
# Set the router priority for DR election to 3 in the public network.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option dr-priority 3
```

```
# Set the router priority for DR election to 3 in VPN instance mvpn.
```

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] hello-option dr-priority 3
```

hello-option holdtime (PIM view)

Syntax

```
hello-option holdtime interval
```

```
undo hello-option holdtime
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535. A value of 65,535 makes the PIM neighbor always reachable.

Description

Use **hello-option holdtime** to configure the PIM neighbor timeout time.

Use **undo hello-option holdtime** to restore the default.

By default, the PIM neighbor timeout time is 105 seconds.

Related commands: **pim hello-option holdtime**.

Examples

Set the global value of the PIM neighbor timeout time to 120 seconds in the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option holdtime 120
```

Set the global value of the PIM neighbor timeout time to 120 seconds in VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] hello-option holdtime 120
```

hello-option lan-delay (PIM view)

Syntax

hello-option lan-delay *interval*

undo hello-option lan-delay

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

Description

Use **hello-option lan-delay** to configure the global value of the LAN-delay time, namely, the period of time that the device waits before it forwards a received prune message.

Use **undo hello-option lan-delay** to restore the default.

By default, the LAN-delay time is 500 milliseconds.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **hello-option override-interval**, **pim hello-option lan-delay**, and **pim hello-option override-interval**.

Examples

```
# Set the LAN-delay time to 200 milliseconds globally in the public network.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option lan-delay 200

# Set the LAN-delay time to 200 milliseconds globally in VPN instance mvpn.
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] hello-option lan-delay 200
```

hello-option neighbor-tracking (PIM view)

Syntax

```
hello-option neighbor-tracking
undo hello-option neighbor-tracking
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

None

Description

Use **hello-option neighbor-tracking** to disable join suppression globally, namely, enable neighbor tracking.

Use **undo hello-option neighbor-tracking** to enable join suppression.

By default, join suppression is enabled. Namely, neighbor tracking is disabled.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **pim hello-option neighbor-tracking**.

Examples

```
# Disable join suppression globally in the public network.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option neighbor-tracking

# Disable join suppression globally in VPN instance mvpn.
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] hello-option neighbor-tracking
```

hello-option override-interval (PIM view)

Syntax

```
hello-option override-interval interval  
undo hello-option override-interval
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

Description

Use **hello-option override-interval** to configure the global value of the prune override interval.

Use **undo hello-option override-interval** to restore the default.

By default, the prune override interval is 2500 milliseconds.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **hello-option lan-delay**, **pim hello-option lan-delay**, and **pim hello-option override-interval**.

Examples

```
# Set the prune override interval to 2000 milliseconds globally in the public network.
```

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

```
[Sysname] pim
```

```
[Sysname-pim] hello-option override-interval 2000
```

```
# Set the prune override interval to 2000 milliseconds globally in VPN instance mvpn.
```

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

```
[Sysname] pim vpn-instance mvpn
```

```
[Sysname-pim-mvpn] hello-option override-interval 2000
```

holdtime assert (PIM view)

Syntax

```
holdtime assert interval  
undo holdtime assert
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

Description

Use **holdtime assert** to configure the global value of the assert timeout time.

Use **undo holdtime assert** to restore the default.

By default, the assert timeout time is 180 seconds.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **holdtime join-prune**, **pim holdtime assert**, and **pim holdtime join-prune**.

Examples

```
# Set the global value of the assert timeout time to 100 seconds in the public network.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] holdtime assert 100
```

```
# Set the global value of the assert timeout time to 100 seconds in VPN instance mvpn.
```

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] holdtime assert 100
```

holdtime join-prune (PIM view)

Syntax

```
holdtime join-prune interval
```

```
undo holdtime join-prune
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

Description

Use **holdtime join-prune** to configure the global value of the join/prune timeout time.

Use **undo holdtime join-prune** to restore the default.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **pim holdtime assert**, and **pim holdtime join-prune**.

Examples

```
# Set the global value of the join/prune timeout time to 280 seconds in the public network.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] holdtime join-prune 280
```

```
# Set the global value of the join/prune timeout time to 280 seconds in VPN instance mvpn.
```

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
```

```
[Sysname-pim-mvpn] holdtime join-prune 280
```

jp-pkt-size (PIM view)

Syntax

```
jp-pkt-size packet-size
```

```
undo jp-pkt-size
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

packet-size: Maximum size of each join/prune message in bytes, in the range of 100 to 8100.

Description

Use **jp-pkt-size** to configure the maximum size of each join/prune message.

Use **undo jp-pkt-size** to restore the default.

By default, the maximum size of each join/prune message is 8100 bytes.

If PIM snooping-enabled switches are deployed in the PIM network, be sure to set a value no greater than the path MTU for the maximum size of each join/prune message on the receiver-side edge PIM devices

Related commands: **jp-queue-size**.

Examples

```
# Set the maximum size of each join/prune message to 1500 bytes in the public network.
```

```
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] jp-pkt-size 1500
```

```
# Set the maximum size of each join/prune message to 1500 bytes in VPN instance mvpn.
```

```
<Sysname> system-view  
[Sysname] pim vpn-instance mvpn  
[Sysname-pim-mvpn] jp-pkt-size 1500
```

jp-queue-size (PIM view)

Syntax

```
jp-queue-size queue-size
```

```
undo jp-queue-size
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

queue-size: Maximum number of (S, G) entries in a join/prune message, in the range of 1 to 4096.

Description

Use **jp-queue-size** to configure the maximum number of (S, G) entries in a join/prune message.

Use **undo jp-queue-size** to restore the default.

By default, a join/prune messages contains a maximum of 1020 (S, G) entries.

When you use this command, take the following into account:

- The size of the forwarding table. In a network that does not support packet fragmentation, if you configure a large queue size, a join/prune message might contain a large number of groups, which might cause the message length to exceed the MTU of the network. As a result, the products that do not support fragmentation will drop the join/prune message.
- The (S, G) join/prune timeout time on the upstream device. If you configure a small queue size, the outgoing interface of the corresponding entry might have been pruned because of timeout before the last join/prune message in a queue reaches the upstream device.

Related commands: **holdtime join-prune**, **jp-pkt-size**, and **pim holdtime join-prune**.

Examples

Configure a join/prune message to contain a maximum of 2000 (S, G) entries in the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] jp-queue-size 2000
```

Configure a join/prune message to contain a maximum of 2000 (S, G) entries in VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] jp-queue-size 2000
```

pim

Syntax

pim [**vpn-instance** *vpn-instance-name*]

undo pim [**vpn-instance** *vpn-instance-name*]

View

System view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If this option is not specified, the command applies to the public network.

Description

Use **pim** to enter public network PIM view or VPN instance PIM view.

Use **undo pim** to remove all configurations in public network PIM view or VPN instance PIM view.

IP multicast routing must be enabled in the corresponding instance before this command takes effect.

Related commands: **multicast routing-enable**.

Examples

```
# Enable IP multicast routing in the public network and enter public network PIM view.
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] pim
[Sysname-pim]

# Enable IP multicast routing in VPN instance mvpn and enter PIM view of VPN instance mvpn.
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] route-distinguisher 100:1
[Sysname-vpn-instance-mvpn] multicast routing-enable
[Sysname-vpn-instance-mvpn] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn]
```

pim bfd enable

Syntax

```
pim bfd enable
undo pim bfd enable
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim bfd enable** to enable PIM to work with Bidirectional Forwarding Detection (BFD).

Use **undo pim bfd enable** to disable this feature.

By default, this feature is disabled.

You must enable PIM-DM or PIM-SM on an interface before you configure this feature on the interface. Otherwise, this feature is not effective.

Related commands: **pim dm** and **pim sm**.

Examples

```
# Enable IP multicast routing in the public network, enable PIM-SM on interface VLAN-interface 100, and enable PIM to work with BFD on the interface.
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim sm
[Sysname-Vlan-interface100] pim bfd enable
```

pim bsr-boundary

Syntax

```
pim bsr-boundary  
undo pim bsr-boundary
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim bsr-boundary** to configure a PIM domain border, namely, a bootstrap message boundary.

Use **undo pim bsr-boundary** to remove the configured PIM domain border.

By default, no PIM domain border is configured.

Related commands: **c-bsr** and **multicast boundary**.

Examples

```
# Configure VLAN-interface 100 as a PIM domain border.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] pim bsr-boundary
```

pim dm

Syntax

```
pim dm  
undo pim dm
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim dm** to enable PIM-DM.

Use **undo pim dm** to disable PIM-DM.

By default, PIM-DM is disabled.

This command takes effect only after IP multicast routing is enabled in the corresponding instance.

PIM-DM cannot be used for multicast groups in the SSM group range.

Related commands: **multicast routing-enable**, **pim sm**, and **ssm-policy**.

Examples

```
# Enable IP multicast routing in the public network, and enable PIM-DM on VLAN-interface 100.
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim dm
```

pim hello-option dr-priority

Syntax

```
pim hello-option dr-priority priority
undo pim hello-option dr-priority
```

View

Interface view

Default level

2: System level

Parameters

priority: Router priority for DR election, in the range of 0 to 4294967295. A larger value of this argument means a higher priority.

Description

Use **pim hello-option dr-priority** to configure the router priority for DR election on the current interface.

Use **undo pim hello-option dr-priority** to restore the default.

By default, the router priority for DR election is 1.

Related commands: **hello-option dr-priority**.

Examples

```
# Set the router priority for DR election to 3 on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option dr-priority 3
```

pim hello-option holdtime

Syntax

```
pim hello-option holdtime interval
undo pim hello-option holdtime
```

View

Interface view

Default level

2: System level

Parameters

interval: PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535. A value of 65,535 makes the PIM neighbor always reachable.

Description

Use **pim hello-option holdtime** to configure the PIM neighbor timeout time on the current interface.

Use **undo pim hello-option holdtime** to restore the default.

By default, the PIM neighbor timeout time is 105 seconds.

Related commands: **hello-option holdtime**.

Examples

```
# Set the PIM neighbor timeout time to 120 seconds on VLAN-interface 100.
```

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

```
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] pim hello-option holdtime 120
```

pim hello-option lan-delay

Syntax

```
pim hello-option lan-delay interval
```

```
undo pim hello-option lan-delay
```

View

Interface view

Default level

2: System level

Parameters

interval: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

Description

Use **pim hello-option lan-delay** to configure the LAN-delay time—namely, the length of time that the device waits before forwarding a received prune message—on the current interface.

Use **undo pim hello-option lan-delay** to restore the default.

By default, the LAN-delay time is 500 milliseconds.

Related commands: **hello-option lan-delay**, **hello-option override-interval**, and **pim hello-option override-interval**.

Examples

```
# Set the LAN-delay time to 200 milliseconds on VLAN-interface 100.
```

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

```
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] pim hello-option lan-delay 200
```

pim hello-option neighbor-tracking

Syntax

```
pim hello-option neighbor-tracking  
undo pim hello-option neighbor-tracking
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim hello-option neighbor-tracking** to disable join suppression—namely, enable neighbor tracking—on the current interface.

Use **undo pim hello-option neighbor-tracking** to enable join suppression.

By default, join suppression is enabled. Namely, neighbor tracking is disabled.

Related commands: **hello-option neighbor-tracking**.

Examples

```
# Disable join suppression on VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] pim hello-option neighbor-tracking
```

pim hello-option override-interval

Syntax

```
pim hello-option override-interval interval  
undo pim hello-option override-interval
```

View

Interface view

Default level

2: System level

Parameters

interval: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

Description

Use **pim hello-option override-interval** to configure the prune override interval on the current interface.

Use **undo pim hello-option override-interval** to restore the default.

By default, the prune override interval is 2500 milliseconds.

Related commands: **hello-option lan-delay**, **hello-option override-interval**, and **pim hello-option lan-delay**.

Examples

```
# Set the prune override interval to 2000 milliseconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option override-interval 2000
```

pim holdtime assert

Syntax

```
pim holdtime assert interval
undo pim holdtime assert
```

View

Interface view

Default level

2: System level

Parameters

interval: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

Description

Use **pim holdtime assert** to configure the assert timeout time on the current interface.

Use **undo pim holdtime assert** to restore the default.

By default, the assert timeout time is 180 seconds.

Related commands: **holdtime assert**, **holdtime join-prune**, and **pim holdtime join-prune**.

Examples

```
# Set the assert timeout time to 100 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim holdtime assert 100
```

pim holdtime join-prune

Syntax

```
pim holdtime join-prune interval
undo pim holdtime join-prune
```

View

Interface view

Default level

2: System level

Parameters

interval: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

Description

Use **pim holdtime join-prune** to configure the join/prune timeout time on the interface.

Use **undo pim holdtime join-prune** to restore the default.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **holdtime join-prune**, and **pim holdtime assert**.

Examples

```
# Set the join/prune timeout time to 280 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim holdtime join-prune 280
```

pim neighbor-policy

Syntax

```
pim neighbor-policy acl-number
```

```
undo pim neighbor-policy
```

View

Interface view

Default level

2: System level

Parameters

acl-number: Basic ACL number, in the range of 2000 to 2999. When the ACL is defined, the **source** keyword in the **rule** command specifies a legal source address range for hello messages.

Description

Use **pim neighbor-policy** to configure a legal source address range for hello messages to guard against hello message spoofing.

Use **undo pim neighbor-policy** to restore the default.

By default, no source address range for hello messages is configured. That is, all the received hello messages are considered legal.

Examples

```
# Configure a legal source address range for hello messages on VLAN-interface 100 so that only the devices on the 10.1.1.0/24 subnet can become PIM neighbors of this switch.
```

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim neighbor-policy 2000
```

pim require-genid

Syntax

```
pim require-genid  
undo pim require-genid
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim require-genid** to enable rejection of hello messages without Generation_ID.

Use **undo pim require-genid** to restore the default.

By default, hello messages without Generation_ID are accepted.

Examples

```
# Enable VLAN-interface 100 to reject hello messages without Generation_ID.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] pim require-genid
```

pim sm

Syntax

```
pim sm  
undo pim sm
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim sm** to enable PIM-SM.

Use **undo pim sm** to disable PIM-SM.

By default, PIM-SM is disabled.

This command takes effect only after IP multicast routing is enabled in the corresponding instance.

Related commands: **multicast routing-enable** and **pim dm**.

Examples

```
# Enable IP multicast routing in the public network, and enable PIM-SM on VLAN-interface 100.
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim sm
```

pim state-refresh-capable

Syntax

```
pim state-refresh-capable
undo pim state-refresh-capable
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim state-refresh-capable** to enable the state refresh feature on the interface.

Use **undo pim state-refresh-capable** to disable the state refresh feature.

By default, the state refresh feature is enabled.

Related commands: **state-refresh-interval**, **state-refresh-rate-limit**, and **state-refresh-ttl**.

Examples

```
# Disable state refresh on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo pim state-refresh-capable
```

pim timer graft-retry

Syntax

```
pim timer graft-retry interval
undo pim timer graft-retry
```

View

Interface view

Default level

2: System level

Parameters

interval: Graft retry period in seconds, with an effective range of 1 to 65,535.

Description

Use **pim timer graft-retry** to configure the graft retry period.

Use **undo pim timer graft-retry** to restore the default.

By default, the graft retry period is 3 seconds.

Examples

```
# Set the graft retry period to 80 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer graft-retry 80
```

pim timer hello

Syntax

```
pim timer hello interval
```

```
undo pim timer hello
```

View

Interface view

Default level

2: System level

Parameters

interval: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use **pim timer hello** to configure the interval at which hello messages are sent on the current interface.

Use **undo pim timer hello** to restore the default.

By default, hello messages are sent at the interval of 30 seconds.

Related commands: **timer hello**.

Examples

```
# Set the hello interval to 40 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer hello 40
```

pim timer join-prune

Syntax

```
pim timer join-prune interval
```

```
undo pim timer join-prune
```

View

Interface view

Default level

2: System level

Parameters

interval: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use **pim timer join-prune** to configure the interval at which join/prune messages are sent on the current interface.

Use **undo pim timer join-prune** to restore the default.

By default, the join/prune interval is 60 seconds.

Related commands: **timer join-prune**.

Examples

```
# Set the join/prune interval to 80 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer join-prune 80
```

pim triggered-hello-delay

Syntax

```
pim triggered-hello-delay interval
undo pim triggered-hello-delay
```

View

Interface view

Default level

2: System level

Parameters

interval: Maximum delay in seconds between hello messages, with an effective range of 1 to 60.

Description

Use **pim triggered-hello-delay** to configure the maximum delay between hello messages.

Use **undo pim triggered-hello-delay** to restore the default.

By default, the maximum delay between hello messages is 5 seconds.

Examples

```
# Set the maximum delay between hello messages to 3 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim triggered-hello-delay 3
```

probe-interval (PIM view)

Syntax

```
probe-interval interval  
undo probe-interval
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: Register probe time in seconds, with an effective range of 1 to 1799.

Description

Use **probe-interval** to configure the register probe time.

Use **undo probe-interval** to restore the default.

By default, the register probe time is 5 seconds.

Related commands: **register-suppression-timeout**.

Examples

```
# Set the register probe time to 6 seconds in the public network.
```

```
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] probe-interval 6
```

```
# Set the register probe time to 6 seconds in VPN instance mvpn.
```

```
<Sysname> system-view  
[Sysname] pim vpn-instance mvpn  
[Sysname-pim-mvpn] probe-interval 6
```

prune delay (PIM view)

Syntax

```
prune delay interval  
undo prune delay
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: Prune delay time in the range of 1 to 128 seconds.

Description

Use **prune delay** to configure the prune delay time, namely, the length of time that the device waits between receiving a prune message and taking a prune action.

Use **undo prune delay** to restore the default.

By default, the prune delay is not configured.

Examples

```
# Set the prune delay time to 75 seconds in the public network.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] prune delay 75
```

```
# Set the prune delay time to 75 seconds in VPN instance mvpn.
```

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] prune delay 75
```

register-policy (PIM view)

Syntax

```
register-policy acl-number
```

```
undo register-policy
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

acl-number: Advanced ACL number, in the range of 3000 to 3999. The RP accepts only register messages that match the **permit** statement of the ACL.

Description

Use **register-policy** to configure an ACL rule to filter register messages.

Use **undo register-policy** to remove the configured register filtering rule.

By default, no register filtering rule is configured.

Related commands: **register-suppression-timeout**.

Examples

```
# In the public network, configure the RP to accept only those register messages from multicast sources on the subnet of 10.10.0.0/16 for multicast groups on the subnet of 225.1.0.0/16.
```

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[Sysname-acl-adv-3000] quit
[Sysname] pim
[Sysname-pim] register-policy 3000
```

```
# In VPN instance mvpn, configure the RP to accept only those register messages from multicast sources on the subnet of 10.10.0.0/16 for multicast groups on the subnet of 225.1.0.0/16.
```

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

```
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3000] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] register-policy 3000
```

register-suppression-timeout (PIM view)

Syntax

register-suppression-timeout *interval*

undo register-suppression-timeout

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: Register suppression time in seconds, in the range of 1 to 65535.

Description

Use **register-suppression-timeout** to configure the register suppression time.

Use **undo register-suppression-timeout** to restore the default.

By default, the register suppression time is 60 seconds.

Related commands: **probe-interval** and **register-policy**.

Examples

Set the register suppression time to 70 seconds in the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-suppression-timeout 70
```

Set the register suppression time to 70 seconds in VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] register-suppression-timeout 70
```

register-whole-checksum (PIM view)

Syntax

register-whole-checksum

undo register-whole-checksum

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

None

Description

Use **register-whole-checksum** to configure the router to calculate the checksum based on the entire register message.

Use **undo register-whole-checksum** to restore the default.

By default, the checksum is calculated based on the header in the register message.

Related commands: **register-policy** and **register-suppression-timeout**.

Examples

Configure the router to calculate the checksum based on the entire register message in the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-whole-checksum
```

Configure the router to calculate the checksum based on the entire register message in VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] register-whole-checksum
```

reset pim control-message counters

Syntax

```
reset pim [ all-instance | vpn-instance vpn-instance-name ] control-message counters [ interface interface-type interface-number ]
```

View

User view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters.

interface *interface-type interface-number*: Resets the PIM control message counter on a particular interface. If no interface is specified, this command resets PIM control message counters on all interfaces.

Description

Use **reset pim control-message counters** to clear statistics for PIM control messages.

If neither **all-instance** nor **vpn-instance** is specified, this command clear statistics for PIM control messages on the public network.

Examples

```
# Clear statistics for PIM control messages on all interfaces on the public network.
<Sysname> reset pim control-message counters
```

source-lifetime (PIM view)

Syntax

```
source-lifetime interval
undo source-lifetime
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: Multicast source lifetime in seconds, with an effective range of 1 to 31,536,000.

Description

Use **source-lifetime** to configure the multicast source lifetime.

Use **undo source-lifetime** to restore the default.

By default, the lifetime of a multicast source is 210 seconds.

Examples

```
# Set the multicast source lifetime to 200 seconds in the public network.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] source-lifetime 200

# Set the multicast source lifetime to 200 seconds in VPN instance mvpn.
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] source-lifetime 200
```

source-policy (PIM view)

Syntax

```
source-policy acl-number
undo source-policy
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

acl-number: Basic or advanced ACL number, in the range of 2000 to 3999.

Description

Use **source-policy** to configure a multicast data filter.

Use **undo source-policy** to remove the configured multicast data filter.

By default, no multicast data filter is configured.

If you specify a basic ACL, the device filters all the received multicast packets based on the source address, and discards packets that fail the source address match. If you specify an advanced ACL, the device filters all the received multicast packets based on the source and group addresses, and discards packets that fail the match.

If this command is executed repeatedly, the last configuration takes effect.

Examples

In the public network, configure the router to accept multicast packets that originate from 10.10.1.2 and discard multicast packets that originate from 10.10.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.10.1.2 0
[Sysname-acl-basic-2000] rule deny source 10.10.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] source-policy 2000
```

In VPN instance **mvpn**, configure the router to accept multicast packets originated from 10.10.1.2 and discard multicast packets originated from 10.10.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.10.1.2 0
[Sysname-acl-basic-2000] rule deny source 10.10.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] source-policy 2000
```

spt-switch-threshold infinity (PIM view)

Syntax

```
spt-switch-threshold infinity [ group-policy acl-number [ order order-value ] ]
```

```
undo spt-switch-threshold [ group-policy acl-number ]
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

group-policy *acl-number*: Specifies a basic ACL, in the range of 2000 to 2999. If you do not include this option in your command, the configuration applies to all multicast groups.

order *order-value*: Specifies the order of the ACL in the group-policy list, where *order-value* has an effective range of 1 to the largest order value in the existing group-policy list plus 1, but the value range

should not include the original order value of the ACL in the group-policy list. If you have assigned an *order-value* to a certain ACL, do not specify the same *order-value* for another ACL. Otherwise, the system gives error information. If you do not specify an *order-value*, the order value of the ACL remains the same in the group-policy list.

Description

Use **spt-switch-threshold infinity** to disable the switchover to SPT.

Use **undo spt-switch-threshold** to restore the default.

By default, the device switches to the SPT immediately after it receives the first multicast packet.

To adjust the order of an existing ACL in the group-policy list, you can use the *acl-number* argument to specify this ACL and set its *order-value*. This inserts the ACL to the position of *order-value* in the group-policy list. The order of the other existing ACLs in the group-policy list remains unchanged.

To use an ACL that does not exist in the group-policy list, you can use the *acl-number* argument to specify an ACL and set its *order-value*. This inserts the ACL to the position of *order-value* in the group-policy list. If you do not include the **order order-value** option in your command, the ACL is appended to the end of the group-policy list.

If you use this command multiple times on the same multicast group, the first traffic rate configuration matched in sequence takes effect.

If the switch is an RP, disabling switchover to SPT might cause multicast traffic forwarding failures on the source-side DR. When disabling switchover to SPT, be sure you fully understand its impact on your network.

Examples

In the public network, disable the switchover to SPT on the receiver-side DR.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] spt-switch-threshold infinity
```

In VPN instance **mvpn**, disable the switchover to SPT on the receiver-side DR.

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] spt-switch-threshold infinity
```

ssm-policy (PIM view)

Syntax

ssm-policy *acl-number*

undo ssm-policy

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

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

Description

Use **ssm-policy** to configure the SSM multicast group range.

Use **undo ssm-policy** to restore the default.

By default, the SSM group range is 232.0.0.0/8.

You can use this command to define an address range of permitted or denied multicast groups. If the match succeeds, the multicast mode is PIM-SSM. Otherwise, the multicast mode is PIM-SM.

Examples

```
# Configure the SSM group range to be 232.1.0.0/16 in the public network.
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] ssm-policy 2000

# Configure the SSM group range to be 232.1.0.0/16 in VPN instance mvpn.
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] ssm-policy 2000
```

state-refresh-interval (PIM view)

Syntax

state-refresh-interval *interval*

undo state-refresh-interval

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: State refresh interval in seconds, with an effective range of 1 to 255.

Description

Use **state-refresh-interval** to configure the interval between state refresh messages.

Use **undo state-refresh-interval** to restore the default.

By default, the state refresh interval is 60 seconds.

Related commands: **pim state-refresh-capable**, **state-refresh-rate-limit**, and **state-refresh-ttl**.

Examples

```
# Set the state refresh interval to 70 seconds in the public network.
<Sysname> system-view
```

```
[Sysname] pim
[Sysname-pim] state-refresh-interval 70

# Set the state refresh interval to 70 seconds in VPN instance mvpn.
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] state-refresh-interval 70
```

state-refresh-rate-limit (PIM view)

Syntax

state-refresh-rate-limit *interval*

undo state-refresh-rate-limit

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: Time to wait before receiving a new refresh message, in seconds and with an effective range of 1 to 65535.

Description

Use **state-refresh-rate-limit** to configure the time that the router must wait before receiving a new state refresh message.

Use **undo state-refresh-rate-limit** to restore the default.

By default, the device waits 30 seconds before it receives a new state refresh message.

Related commands: **pim state-refresh-capable**, **state-refresh-interval**, and **state-refresh-ttl**.

Examples

In the public network, configure the device to wait 45 seconds before it receives a new state refresh message.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-rate-limit 45
```

In VPN instance **mvpn**, configure the device to wait 45 seconds before receiving a new state refresh message.

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] state-refresh-rate-limit 45
```

state-refresh-ttl

Syntax

state-refresh-ttl *tvl-value*

undo state-refresh-ttl

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

tvl-value: TTL value of state refresh messages, in the range of 1 to 255.

Description

Use **state-refresh-ttl** to configure the TTL value of state refresh messages.

Use **undo state-refresh-ttl** to restore the default.

By default, the TTL value of state refresh messages is 255.

Related commands: **pim state-refresh-capable**, **state-refresh-interval**, and **state-refresh-rate-limit**.

Examples

In the public network, configure the device to send PIM state refresh messages with a TTL of 45.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-ttl 45
```

In VPN instance **mvpn**, configure the device to send PIM state refresh messages with a TTL of 45.

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] state-refresh-ttl 45
```

static-rp (PIM view)

Syntax

static-rp *rp-address* [*acl-number*] [**preferred**] [**bidir**]

undo static-rp *rp-address*

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

rp-address: Specifies the IP address of the static RP to be configured. This address must be a real, valid unicast IP address, rather than an address on the 127.0.0.0/8 segment. For a static RP serving BIDIR-PIM, you can specify a virtual IP address.

acl-number: Specifies a basic ACL number, in the range of 2000 to 2999. If you provide this argument, the configured static RP provides services for only those groups that pass the ACL filtering. Otherwise, the configured static RP provides services for the all-system group 224.0.0.0/4.

preferred: Gives priority to the static RP if the static RP conflicts with the dynamic RP. If you do not include the **preferred** keyword in your command, the dynamic RP receives priority, and the static RP takes effect only if no dynamic RP exists in the network or when the dynamic RP fails.

bidir: Configures the static RP to provide services for multicast groups in BIDIR-PIM. Without this argument, the static RP provides services for groups in PIM-SM.

Description

Use **static-rp** to configure a static RP.

Use **undo static-rp** to configure a static RP.

By default, no static RP is configured.

PIM-SM or PIM-DM cannot be enabled on an interface that acts as a static RP.

When the ACL rule applied on a static RP changes, a new RP must be elected for all the multicast groups.

You can configure multiple static RPs by using this command repeatedly. However, if you use this command multiple times and specify the same static RP address or reference the same ACL rule, the most recent configuration takes effect. If you have configured multiple static RPs for the same multicast group, the one with the highest IP address provides services for the multicast group.

You can configure up to 50 static RPs on the same device.

Related commands: **auto-rp enable** and **display pim rp-info**.

Examples

In the public network, configure the interface with the IP address 11.110.0.6 to be a static RP that provides services for the multicast groups in the address range of 225.1.1.0/24 defined in ACL 2001, and give priority to this static RP in the case of static/dynamic RP conflict.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] pim
[Sysname-pim] static-rp 11.110.0.6 2001 preferred
```

In VPN instance **mvpn**, configure the interface with the IP address 11.110.0.6 to be a static RP that provides services for the multicast groups in the address range of 225.1.1.0/24 defined in ACL 2001, and give priority to this static RP in the case of static/dynamic RP conflict.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] static-rp 11.110.0.6 2001 preferred
```

timer hello (PIM view)

Syntax

timer hello *interval*

undo timer hello

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use **timer hello** to configure the hello interval globally.

Use **undo timer hello** to restore the default.

By default, hello messages are sent at the interval of 30 seconds.

Related commands: **pim timer hello**.

Examples

```
# Set the global hello interval to 40 seconds in the public network.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer hello 40
```

```
# Set the global hello interval to 40 seconds in VPN instance mvpn.
```

```
<Sysname> system-view
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn] timer hello 40
```

timer join-prune (PIM view)

Syntax

```
timer join-prune interval
```

```
undo timer join-prune
```

View

Public network PIM view, VPN instance PIM view

Default level

2: System level

Parameters

interval: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use **timer join-prune** to configure the join/prune interval globally.

Use **undo timer join-prune** to restore the default.

By default, the join/prune interval is 60 seconds.

Related commands: **pim timer join-prune**.

Examples

```
# Set the global join/prune interval to 80 seconds in the public network.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer join-prune 80
```

```
# Set the global join/prune interval to 80 seconds in VPN instance mvpn.
```

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

```
[Sysname] pim vpn-instance mvpn  
[Sysname-pim-mvpn] timer join-prune 80
```

MSDP configuration commands (available only on the HP 5500 EI)

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

The term "interface" in this chapter 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*).

cache-sa-enable

Syntax

cache-sa-enable

undo cache-sa-enable

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

None

Description

Use **cache-sa-enable** to enable the SA cache mechanism to cache the (S, G) entries that the received SA messages contain.

Use **undo cache-sa-enable** to disable the SA cache mechanism.

By default, the SA cache mechanism is enabled. That is, the device caches the (S, G) entries that in the received SA messages contain.

Examples

Enable the SA message cache mechanism on the public network so that the device caches the (S, G) entries that the received SA messages contain.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] cache-sa-enable
```

Enable the SA message cache mechanism in VPN instance **mvpn**, so that the device caches the (S, G) entries that the received SA messages contain.

```
<Sysname> system-view
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] cache-sa-enable
```

display msdp brief

Syntax

```
display msdp [ all-instance | vpn-instance vpn-instance-name ] brief [ state { connect | down | listen | shutdown | up } ] [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

state: Displays the information of MSDP peers in the specified state.

connect: Displays the information of MSDP peers in the connecting state.

down: Displays the information of MSDP peers in the down state.

listen: Displays the information of MSDP peers in the listening state.

shutdown: Displays the information of MSDP peers in the terminated state.

up: Displays the information of MSDP peers in the in-session state.

|: 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 msdp brief** to display brief information about MSDP peers.

If neither **all-instance** nor **vpn-instance** is specified, this command displays brief information about MSDP peers on the public network.

Examples

```
# Display brief information about MSDP peers in all states on the public network.
```

```
<Sysname> display msdp brief
```

```
MSDP Peer Brief Information of VPN-Instance: public net
```

Configured	Up	Listen	Connect	Shutdown	Down
1	1	0	0	0	0

Peer's Address	State	Up/Down time	AS	SA Count	Reset Count
20.20.20.20	Up	00:00:13	100	0	0

Table 38 Command output

Field	Description
MSDP Peer Brief Information of VPN-Instance: public net	Brief information of MSDP peers on the public network.
Configured	Number of MSDP peers configured.
Up	Number of MSDP peers in up state.
Listen	Number of MSDP peers in listening state.
Connect	Number of MSDP peers in connecting state.
Shutdown	Number of MSDP peers in shutdown state.
Down	Number of MSDP peers in down state.
Peer's Address	MSDP peer address.
State	<p>MSDP peer status</p> <ul style="list-style-type: none"> • Up—The session has set up and MSDP peers are in session. • Listen—The session has set up. The local device acts as the server and is in listening state. • Connect—The session has not set up. The local device acts as a client and is in connecting state. • Shutdown—Deactivated. • Down—Connection failed.
Up/Down time	Length of time since the MSDP peer connection was established/failed.
AS	Number of the AS where the MSDP peer is located. A question mark indicates that the system could not obtain the AS number.
SA Count	Number of (S, G) entries
Reset Count	MSDP peer connection reset times

display msdp peer-status

Syntax

```
display msdp [ all-instance | vpn-instance vpn-instance-name ] peer-status [ peer-address ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

peer-address: Specifies an MSDP peer by its address. If you do not provide this argument, this command displays the detailed status information of all MSDP peers.

|: 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 msdp peer-status** to display detailed MSDP peer status information.

If neither **all-instance** nor **vpn-instance** is specified, this command displays detailed information about MSDP peer status on the public network.

Related commands: **peer connect-interface**, **peer description**, **peer mesh-group**, **peer minimum-ttl**, **peer request-sa-enable**, **peer sa-cache-maximum**, **peer sa-policy**, and **peer sa-request-policy**.

Examples

Display the detailed status information of the MSDP peer with the address of 10.110.11.11 on the public network.

```
<Sysname> display msdp peer-status 10.110.11.11
MSDP Peer Information of VPN-Instance: public net
  MSDP Peer 20.20.20.20, AS 100
  Description:
  Information about connection status:
    State: Up
    Up/down time: 14:41:08
    Resets: 0
    Connection interface: LoopBack0 (20.20.20.30)
    Number of sent/received messages: 867/947
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 14:42:40
  Information about (Source, Group)-based SA filtering policy:
    Import policy: none
    Export policy: none
  Information about SA-Requests:
    Policy to accept SA-Request messages: none
    Sending SA-Requests status: disable
  Minimum TTL to forward SA with encapsulated data: 0
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 0/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
```

Table 39 Command output

Field	Description
MSDP Peer Information of VPN-Instance: public net	Information of the MSDP peer on the public network.
MSDP Peer	MSDP peer address.
AS	Number of the AS where the MSDP peer is located. A question mark indicates that the system could not obtain the AS number.
State	<p>MSDP peer status</p> <ul style="list-style-type: none"> • Up—The session has set up and MSDP peers are in session. • Listen—The session has set up. The local device acts as the server and is in listening state. • Connect—The session has not set up. The local device acts as an client and is in connecting state. • Shutdown—Deactivated. • Down—Connection failed.
Resets	Number of times that the MSDP peer connection is reset.
Up/Down time	Length of time since the MSDP peer connection was established/failed.
Connection interface	Interface and its IP address used for setting up a TCP connection with the remote MSDP peer.
Number of sent/received messages	Number of SA messages sent and received through this connection.
Number of discarded output messages	Number of discarded outgoing messages.
Elapsed time since last connection or counters clear	Time passed since the information of the MSDP peer was last cleared.
Information about (Source, Group)-based SA filtering policy	<p>SA message filtering list information</p> <ul style="list-style-type: none"> • Import policy—Filter list for receiving SA messages from the specified MSDP peer. • Export policy—Filter list for forwarding SA messages from the specified MSDP peer.
Information about SA-Requests	<p>SA request information</p> <ul style="list-style-type: none"> • Policy to accept SA request messages—Filtering rule for receiving or forwarding SA messages from the specified MSDP peer. • Sending SA requests status—Whether enabled to send an SA request message to the designated MSDP peer after receiving a new join message.
Minimum TTL to forward SA with encapsulated data	Minimum TTL of multicast packet encapsulated in SA messages.
SAs learned from this peer	Number of cached (S, G) entries learned from this MSDP peer.
SA-cache maximum for the peer	Maximum number of (S, G) entries learned from this MSDP peer that the device can cache.
Input queue size	Data size cached in the input queue.
Output queue size	Data size cached in the output queue.

Field	Description
Counters for MSDP message	<p>MSDP peer statistics:</p> <ul style="list-style-type: none"> • Count of RPF check failure—Number of SA messages discarded because of RPF check failure. • Incoming/outgoing SA messages—Number of SA messages received and sent. • Incoming/outgoing SA requests—Number of SA requests received and sent. • Incoming/outgoing SA responses—Number of SA responses received and sent. • Incoming/outgoing data packets—Number of received and sent SA messages encapsulated with multicast data.

display msdp sa-cache

Syntax

```
display msdp [ all-instance | vpn-instance vpn-instance-name ] sa-cache [ group-address | source-address | as-number ] * [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

group-address: Specifies a multicast group address in the (S, G) entry, in the range of 224.0.1.0 to 239.255.255.255. If you do not provide any group address, this command displays the (S, G) entry information for all multicast groups.

source-address: Specifies a multicast source address in the (S, G) entry. If you do not provide any source address, this command displays the (S, G) entry information for all sources.

as-number: Specifies an AS number, in the range of 1 to 4294967295. If you do not provide any AS number, this command displays the (S, G) entry information of all ASs.

|: 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 msdp sa-cache** to display information about cached (S, G) entries.

If neither **all-instance** nor **vpn-instance** is specified, this command displays information about cached (S, G) entries on the public network.

This command gives the corresponding output only after the **cache-sa-enable** command is executed.

If you provide neither a group address nor a source address, this command displays information about all cached (S, G) entries.

Related commands: **cache-sa-enable**.

Examples

Display information about cached (S, G) entries on the public network.

```
<Sysname> display msdp sa-cache
```

```
MSDP Source-Active Cache Information of VPN-Instance: public net
```

```
MSDP Total Source-Active Cache - 5 entries
```

```
MSDP matched 5 entries
```

(Source, Group)	Origin RP	Pro	AS	Uptime	Expires
(10.10.1.2, 225.1.1.1)	10.10.10.10	BGP	100	00:00:11	00:05:49
(10.10.1.3, 225.1.1.1)	10.10.10.10	BGP	100	00:00:11	00:05:49
(10.10.1.2, 225.1.1.2)	10.10.10.10	BGP	100	00:00:11	00:05:49
(10.10.2.1, 225.1.1.2)	10.10.10.10	BGP	100	00:00:11	00:05:49
(10.10.1.2, 225.1.2.2)	10.10.10.10	BGP	100	00:00:11	00:05:49

Table 40 Command output

Field	Description
MSDP Source-Active Cache Information of VPN-Instance: public net	SA cache information on the public network.
MSDP Total Source-Active Cache - 5 entries	Total number of (S, G) entries in the SA cache.
MSDP matched 5 entries	Total number of (S, G) entries matched by MSDP.
(Source, Group)	(S, G) entry: (source address, group address).
Origin RP	Address of the RP that generated the (S, G) entry.
Pro	Type of protocol from which the AS number originates. A question mark indicates that the system could not obtain the protocol type.
AS	AS number of the origin RP. A question mark indicates that the system could not obtain the AS number.
Uptime	Length of time for which the cached (S, G) entry has existed, in hours:minutes:seconds.
Expires	Length of time in which the cached (S, G) entry will expire, in hours:minutes:seconds.

display msdp sa-count

Syntax

```
display msdp [ all-instance | vpn-instance vpn-instance-name ] sa-count [ as-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

as-number: Specifies an AS number, in the range of 1 to 4294967295.

|: 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 msdp sa-count** to display the number of (S, G) entries in the SA cache.

If neither **all-instance** nor **vpn-instance** is specified, this command displays the number of (S, G) entries on the public network.

This command gives the corresponding output only after you use the **cache-sa-enable** command.

Related commands: **cache-sa-enable**.

Examples

Display the number of (S, G) entries in the SA cache on the public network.

```
<Sysname> display msdp sa-count
MSDP Source-Active Count Information of VPN-Instance: public net
  Number of cached Source-Active entries, counted by Peer
  Peer's Address      Number of SA
  10.10.10.10         5

  Number of source and group, counted by AS
  AS      Number of source  Number of group
  ?       3                 3

  Total 5 Source-Active entries
```

Table 41 Command output

Field	Description
MSDP Source-Active Count Information of VPN-Instance: public net	Number of SA messages for the public network cache.
Number of cached Source-Active entries, counted by Peer	Number of (S, G) entries that the peer counted.

Field	Description
Peer's Address	Address of the MSDP peer that sent SA messages.
Number of SA	Number of (S, G) entries from this peer.
Number of source and group, counted by AS	Number of cached (S, G) entries that the AS counted.
AS	AS number. A question mark indicates that the system could not obtain the AS number.
Number of source	Number of multicast sources from this AS.
Number of group	Number of multicast groups from this AS.

encap-data-enable

Syntax

encap-data-enable

undo encap-data-enable

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

None

Description

Use **encap-data-enable** to enable encapsulation of multicast data in SA messages.

Use **undo encap-data-enable** to restore the default.

By default, an SA message contains only an (S, G) entry. No multicast data is encapsulated in an SA message.

Examples

Enable encapsulation of multicast data in SA messages on the public network.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] encap-data-enable
```

Enable encapsulation of multicast data in SA messages in VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] encap-data-enable
```

import-source

Syntax

import-source [**acl** *acl-number*]

undo import-source

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

acl-number: Specifies a basic or advanced ACL number, in the range of 2000 to 3999. A basic ACL filters multicast sources, and an advanced ACL filters multicast sources or multicast groups. If you do not provide this argument in your command, no multicast source information is advertised.

Description

Use **import-source** to configure a rule of creating (S, G) entries.

Use **undo import-source** to remove any rule of creating (S, G) entries.

By default, when an SA message is created, no restrictions are defined for the (S, G) entries to be advertised in it. Namely, all the (S, G) entries within the domain are advertised in the SA message.

During ACL matching, the protocol ID in the ACL rule is not verified.

In addition to controlling SA message creation by using this command, you can also configure a filtering rule for forwarding and receiving SA messages by using the **peer sa-policy** command.

Related commands: **peer sa-policy**.

Examples

Configure the MSDP peer on the public network to advertise only the (S, G) entries of multicast sources on the 10.10.0.0/16 subnet and with a multicast group address of 225.1.0.0/16 when creating an SA message.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3101] quit
[Sysname] msdp
[Sysname-msdp] import-source acl 3101
```

Configure the MSDP peer in VPN instance **mvpn** to advertise only the (S, G) entries of multicast sources on the 10.10.0.0/16 subnet and with a multicast group address of 225.1.0.0/16 when creating an SA message.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3101] quit
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] import-source acl 3101
```

msdp

Syntax

```
msdp [ vpn-instance vpn-instance-name ]  
undo msdp [ vpn-instance vpn-instance-name ]
```

View

System view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command applies to the public network.

Description

Use **msdp** to enable MSDP on the public network or the specified VPN instance and enter public network MSDP view or VPN instance MSDP view.

Use **undo msdp** to disable MSDP on the public network or the specified VPN instance and remove the configurations in public network MSDP view or VPN instance MSDP view to free the resources that MSDP occupies.

By default, MSDP is disabled.

You must enable IP multicast in the related instance before you use this command.

Related commands: **multicast routing-enable**.

Examples

Enable IP multicast routing on the public network, and enable MSDP on the public network to enter public network MSDP view.

```
<Sysname> system-view  
[Sysname] multicast routing-enable  
[Sysname] msdp  
[Sysname-msdp]
```

Enable IP multicast routing and MSDP in VPN instance **mvpn** to enter MSDP view of VPN instance **mvpn**.

```
<Sysname> system-view  
[Sysname] ip vpn-instance mvpn  
[Sysname-vpn-instance-mvpn] route-distinguisher 100:1  
[Sysname-vpn-instance-mvpn] multicast routing-enable  
[Sysname-vpn-instance-mvpn] quit  
[Sysname] msdp vpn-instance mvpn  
[Sysname-msdp-mvpn]
```

originating-rp

Syntax

```
originating-rp interface-type interface-number
```

undo originating-rp

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

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

Description

Use **originating-rp** to configure the address of the specified interface as the RP address of SA messages.

Use **undo originating-rp** to restore the default.

By default, the PIM RP address is used as the RP address of SA messages.

Examples

In public network, specify the IP address of VLAN-interface 100 as the RP address of SA messages.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] originating-rp vlan-interface 100
```

In VPN instance **mvpn**, specify the IP address of VLAN-interface 100 as the RP address of SA messages.

```
<Sysname> system-view
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] originating-rp vlan-interface 100
```

peer connect-interface

Syntax

peer *peer-address* **connect-interface** *interface-type interface-number*

undo peer *peer-address*

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

peer-address: Specifies an MSDP peer address.

interface-type interface-number: Specifies an interface by its type and number. The local device uses the IP address of the specified interface as the source IP address when setting up a TCP connection with the remote MSDP peer.

Description

Use **peer connect-interface** to create an MSDP peer connection.

Use **undo peer connect-interface** to remove an MSDP peer connection.

No MSDP peer connection is created by default.

Be sure to use this command before you use any other **peer** command. Otherwise, the system displays a prompt that the peer does not exist.

Related commands: **static-rpf-peer**.

Examples

On the public network, configure the router with the IP address of 125.10.7.6 as the MSDP peer of the local router, with interface VLAN-interface 100 as the local connection port.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
```

In VPN instance **mvpn**, configure the router with the IP address of 125.10.7.6 as the MSDP peer of the local router, with interface VLAN-interface 100 as the local connection port.

```
<Sysname> system-view
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] peer 125.10.7.6 connect-interface vlan-interface 100
```

peer description

Syntax

peer *peer-address* **description** *text*

undo peer *peer-address* **description**

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

peer-address: Specifies an MSDP peer address.

text: Specifies a description, a case-sensitive string of 1 to 80 characters including spaces.

Description

Use **peer description** to configure the description information for the specified MSDP peer.

Use **undo peer description** to delete the configured description information of the specified MSDP peer.

By default, an MSDP peer has no description information.

Related commands: **display msdp peer-status**.

Examples

On the public network, add the descriptive text "CustomerA" for the router with the IP address of 125.10.7.6 to indicate that this router is Customer A.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 description CustomerA
```

In VPN instance **mvpn**, add the descriptive text "CustomerA" for the router with the IP address of 125.10.7.6 to indicate that this router is Customer A.

```
<Sysname> system-view
[Sysname] msdp vpn-instance mvpn
```

```
[Sysname-msdp-mvpn] peer 125.10.7.6 description CustomerA
```

peer mesh-group

Syntax

```
peer peer-address mesh-group name
```

```
undo peer peer-address mesh-group
```

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

peer-address: Specifies an MSDP peer address.

name: Specifies a mesh group name, a case-sensitive string of 1 to 32 characters. A mesh group name must not contain any space.

Description

Use **peer mesh-group** to configure an MSDP peer as a mesh group member.

Use **undo peer mesh-group** to remove an MSDP peer as a mesh group member.

By default, an MSDP peer does not belong to any mesh group.

Examples

On the public network, configure the MSDP peer with the IP address of 125.10.7.6 as a member of the mesh group "Group1".

```
<Sysname> system-view  
[Sysname] msdp  
[Sysname-msdp] peer 125.10.7.6 mesh-group Group1
```

In VPN instance **mvpn**, configure the MSDP peer with the IP address of 125.10.7.6 as a member of the mesh group "Group1".

```
<Sysname> system-view  
[Sysname] msdp vpn-instance mvpn  
[Sysname-msdp-mvpn] peer 125.10.7.6 mesh-group Group1
```

peer minimum-ttl

Syntax

```
peer peer-address minimum-ttl t1l-value
```

```
undo peer peer-address minimum-ttl
```

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

peer-address: Specifies an MSDP peer address.

tvl-value: Specifies a Time-to-Live (TTL) threshold, in the range of 0 to 255.

Description

Use **peer minimum-ttl** to configure the TTL threshold for multicast data packet encapsulation in SA messages.

Use **undo peer minimum-ttl** to restore the default.

By default, the TTL threshold for a multicast packet to be encapsulated in an SA message is 0.

Related commands: **display msdp peer-status**.

Examples

On the public network, set the TTL threshold for multicast packets to be encapsulated in SA messages to 10 so that only multicast data packets whose TTL value is larger than or equal to 10 can be encapsulated in SA messages and forwarded to the MSDP peer 110.10.10.1.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 110.10.10.1 minimum-ttl 10
```

In VPN instance **mvpn**, set the TTL threshold for multicast packets to be encapsulated in SA messages to 10 so that only multicast data packets whose TTL value is larger than or equal to 10 can be encapsulated in SA messages and forwarded to the MSDP peer 110.10.10.1.

```
<Sysname> system-view
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] peer 110.10.10.1 minimum-ttl 10
```

peer password

Syntax

peer *peer-address* **password** { **cipher** | **simple** } *password*

undo peer *peer-address* **password**

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

peer-address: Specifies an MSDP peer address.

cipher: Specifies a ciphertext password.

simple: Specifies a plaintext password.

password: Specifies the password string. This argument is case sensitive.

- If the **simple** keyword is specified, the plaintext password comprises 1 to 80 characters.
- If the **cipher** keyword is specified, the ciphertext password comprises 1 to 137 characters.

Description

Use **peer password** to configure an MD5 authentication password for the TCP connection to be established with an MSDP peer.

Use **undo peer password** to restore the default.

By default, no MD5 authentication is performed for TCP connections to be established between MSDP peers.

The MSDP peers involved in the MD5 authentication must have the same authentication method and password. Otherwise, the authentication fails and the TCP connection cannot be established.

The plaintext password or ciphertext password is saved in cipher text in the configuration file.

Examples

On the public network, configure the MD5 authentication password to **aabbcc** in plain text for TCP connections to be established with MSDP peer 10.1.100.1. The configuration on the peer is similar.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 10.1.100.1 password simple aabbcc
```

In VPN instance **mvpn**, configure the MD5 authentication password to **aabbcc** in plain text for TCP connections to be established with MSDP peer 10.1.100.1. The configuration on the peer is similar.

```
<Sysname> system-view
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] peer 10.1.100.1 password simple aabbcc
```

peer request-sa-enable

Syntax

peer *peer-address* **request-sa-enable**

undo peer *peer-address* **request-sa-enable**

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

peer-address: Specifies an MSDP peer address.

Description

Use **peer request-sa-enable** to enable the device to send an SA request message to the specified MSDP peer after receiving a new join message.

Use **undo peer request-sa-enable** to disable the device from sending an SA request message to the specified MSDP peer.

By default, after receiving a new join message, the router does not send an SA request message to any MSDP peer. Instead, it waits for the next SA message to come.

Before you can enable the device to send SA requests, you must disable the SA message cache mechanism.

Related commands: **cache-sa-enable**.

Examples

Disable the SA message cache mechanism on the public network, and enable the router to send an SA request message to the MSDP peer 125.10.7.6 after receiving a new join message.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] undo cache-sa-enable
[Sysname-msdp] peer 125.10.7.6 request-sa-enable
```

Disable the SA message cache mechanism in VPN instance **mvpn**, and enable the router to send an SA request message to the MSDP peer 125.10.7.6 after receiving a new join message.

```
<Sysname> system-view
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] undo cache-sa-enable
[Sysname-msdp-mvpn] peer 125.10.7.6 request-sa-enable
```

peer sa-cache-maximum

Syntax

peer *peer-address* **sa-cache-maximum** *sa-limit*

undo peer *peer-address* **sa-cache-maximum**

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

peer-address: Specifies an MSDP peer address.

sa-limit: Specifies the maximum number of (S, G) entries that the device can cache, in the range of 1 to 8192.

Description

Use **peer sa-cache-maximum** to configure the maximum number of (S, G) entries learned from the specified MSDP peer that the device can cache.

Use **undo peer sa-cache-maximum** to restore the default.

By default, the device can cache up to 8192 (S, G) entries learned from MSDP peers.

Related commands: **display msdp brief**, **display msdp peer-status**, and **display msdp sa-count**.

Examples

On the public network, enable the device to cache a maximum of 100 (S, G) entries learned from its MSDP peer 125.10.7.6.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 sa-cache-maximum 100
```

In VPN instance **mvpn**, enable the device to cache a maximum of 100 (S, G) entries learned from its MSDP peer 125.10.7.6.

```
<Sysname> system-view
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] peer 125.10.7.6 sa-cache-maximum 100
```

peer sa-policy

Syntax

```
peer peer-address sa-policy { import | export } [ acl acl-number ]
undo peer peer-address sa-policy { import | export }
```

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

import: Filters SA messages from the specified MSDP peer.

export: Filters SA messages that are forwarded to the specified MSDP peer.

peer-address: Specifies an MSDP peer address.

acl-number: Specifies an advanced ACL number, in the range of 3000 to 3999. If you do not provide an ACL number, all SA messages that carry (S, G) entries are filtered out.

Description

Use **peer sa-policy** to configure a filtering rule for received or forwarded SA messages.

Use **undo peer sa-policy** to restore the default.

By default, the switch does not filter SA messages that are received or that will be forwarded. Namely, all SA messages are accepted and forwarded.

In addition to controlling SA message by using this command, you can also use the **import-source** command to configure a filtering rule for creating SA messages.

Related commands: **display msdp peer-status** and **import-source**.

Examples

On the public network, configure a filtering rule so that SA messages are forwarded to the MSDP peer 125.10.7.6 only if they match ACL 3100.

```
<Sysname> system-view
[Sysname] acl number 3100
[Sysname-acl-adv-3100] rule permit ip source 170.15.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3100] quit
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp] peer 125.10.7.6 sa-policy export acl 3100
```

In VPN instance **mvpn**, configure a filtering rule so that SA messages are forwarded to the MSDP peer 125.10.7.6 only if they match ACL 3100.

```
<Sysname> system-view
[Sysname] acl number 3100
```

```
[Sysname-acl-adv-3100] rule permit ip source 170.15.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3100] quit
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] peer 125.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp-mvpn] peer 125.10.7.6 sa-policy export acl 3100
```

peer sa-request-policy

Syntax

```
peer peer-address sa-request-policy [ acl acl-number ]
```

```
undo peer peer-address sa-request-policy
```

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

peer-address: Specifies an MSDP peer address.

acl-number: Specifies a basic ACL number, in the range of 2000 to 2999. If you provide this argument, the SA requests of only the multicast groups that match the ACL are accepted and other SA requests are ignored. If you do not provide this argument, all SA requests are ignored.

Description

Use **peer sa-request-policy** to configure a filtering rule for SA request messages.

Use **undo peer sa-request-policy** to remove the configured SA request filtering rule.

By default, SA request messages are not filtered.

Related commands: **display msdp peer-status**.

Examples

```
# Configure an SA request filtering rule on the public network so that SA messages from the MSDP peer
175.58.6.5 are accepted only if the multicast group address in the SA messages is in the range of
225.1.1.0/24.
```

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] msdp
[Sysname-msdp] peer 175.58.6.5 sa-request-policy acl 2001
```

```
# Configure an SA request filtering rule in VPN instance mvpn so that SA messages from the MSDP peer
175.58.6.5 are accepted only if the multicast group address in the SA messages is in the range of
225.1.1.0/24.
```

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Sysname-acl-basic-2001] quit
```

```
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] peer 175.58.6.5 sa-request-policy acl 2001
```

reset msdp peer

Syntax

```
reset msdp [ all-instance | vpn-instance vpn-instance-name ] peer [ peer-address ]
```

View

User view

Default level

2: System level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

peer-address: Specifies an MSDP peer by its address. If you do not provide this argument, the switch resets the TCP connections with all MSDP peers.

Description

Use **reset msdp peer** to reset the TCP connection with the specified MSDP peer and clear statistics for the MSDP peer.

If neither **all-instance** nor **vpn-instance** is specified, this command clears statistics for the specified MSDP peer on the public network.

Related commands: **display msdp peer-status**.

Examples

```
# Reset the TCP connection on the public network with the MSDP peer 125.10.7.6 and clear statistics for the MSDP peer.
```

```
<Sysname> reset msdp peer 125.10.7.6
```

reset msdp sa-cache

Syntax

```
reset msdp [ all-instance | vpn-instance vpn-instance-name ] sa-cache [ group-address ]
```

View

User view

Default level

2: System level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

group-address: Specifies a multicast group, in the range of 224.0.1.0 to 239.255.255.255. If you do not provide this argument, the command clears the cached (S, G) entries for all multicast groups from the SA cache.

Description

Use **reset msdp sa-cache** to remove the cached (S, G) entries.

If neither **all-instance** nor **vpn-instance** is specified, this command removes the cached (S, G) entries on the public network.

Related commands: **cache-sa-enable** and **display msdp sa-cache**.

Examples

Remove the cached (S, G) entries for multicast group 225.5.4.3 on the public network.

```
<Sysname> reset msdp sa-cache 225.5.4.3
```

reset msdp statistics

Syntax

```
reset msdp [ all-instance | vpn-instance vpn-instance-name ] statistics [ peer-address ]
```

View

User view

Default level

2: System level

Parameters

all-instance: Specifies all VPN instances.

vpn-instance *vpn-instance-name*: Specifies a VPN by its name, a case-sensitive string of 1 to 31 characters.

peer-address: Specifies the IP address of an MSDP peer. If you do not provide this argument, the command clears statistics for all MSDP peers.

Description

Use **reset msdp statistics** to clear statistics for the specified MSDP peer without resetting its connection.

If neither **all-instance** nor **vpn-instance** is specified, this command clears statistics for the specified MSDP peer on the public network.

Examples

Clear statistics for the MSDP peer 125.10.7.6 on the public network.

```
<Sysname> reset msdp statistics 125.10.7.6
```

shutdown (MSDP view)

Syntax

```
shutdown peer-address
```

```
undo shutdown peer-address
```

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

peer-address: MSDP peer address.

Description

Use **shutdown** to terminate the connection with the specified MSDP peer.

Use **undo shutdown** to re-activate the connection with the specified MSDP peer.

By default, the connections with all MSDP peers are active.

Related commands: **display msdp peer-status**.

Examples

```
# Terminate the connection with the MSDP peer 125.10.7.6 on the public network.
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] shutdown 125.10.7.6

# Terminate the connection with the MSDP peer 125.10.7.6 in VPN instance mvpn.
<Sysname> system-view
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] shutdown 125.10.7.6
```

static-rpf-peer

Syntax

```
static-rpf-peer peer-address [ rp-policy ip-prefix-name ]
undo static-rpf-peer peer-address
```

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

peer-address: MSDP peer address.

rp-policy *ip-prefix-name*: Specifies a filtering policy based on the RP address in SA messages, where *ip-prefix-name* is the filtering policy name, a case-sensitive string of 1 to 19 characters.

Description

Use **static-rpf-peer** to configure a static RPF peer.

Use **undo static-rpf-peer** to remove a static RPF peer.

No static RPF peer is configured by default.

When you configure multiple static RPF peers, observe the follow rules:

- If you use the **rp-policy** keyword for all the static RPF peers, all the static RPF peers take effect concurrently. SA messages are filtered according to the configured prefix list and only those SA messages whose RP addresses pass the filtering are accepted. If multiple static RPF peers use the

same filtering policy at the same time, when a peer receives an SA message, it forwards the SA message to the other peers.

- If you use the `rp-policy` keyword for none of the static RPF peers, according to the configuration sequence, only the first static RPF peer whose connection is in up state is activated, and all SA messages from this peer are accepted but the SA messages from other static RPF peers are discarded. When this active static RPF peer fails (for example, when the configuration is removed or when the connection is torn down), still the first RPF peer whose connection is in up state is selected as the activated RPF peer according to the configuration sequence.

Related commands: **display msdp peer-status** and **ip prefix-list**.

Examples

Configure static RPF peers on the public network.

```
<Sysname> system-view
[Sysname] ip ip-prefix list1 permit 130.10.0.0 16 great-equal 16 less-equal 32
[Sysname] msdp
[Sysname-msdp] peer 130.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp] static-rpf-peer 130.10.7.6 rp-policy list1
```

Configure static RPF peers in VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] ip ip-prefix list1 permit 130.10.0.0 16 great-equal 16 less-equal 32
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] peer 130.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp-mvpn] static-rpf-peer 130.10.7.6 rp-policy list1
```

timer retry

Syntax

timer retry *interval*

undo timer retry

View

Public network MSDP view, VPN instance MSDP view

Default level

2: System level

Parameters

interval: Interval between MSDP peer connection retries, in seconds. The value ranges from 1 to 60.

Description

Use **timer retry** to configure the interval between MSDP peer connection retries.

Use **undo timer retry** to restore the default.

By default, the interval between MSDP peer connection retries is 30 seconds.

Related commands: **display msdp peer-status**.

Examples

Set the MSDP peer connection retry interval to 60 seconds on the public network.

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

```
[Sysname] msdp
[Sysname-msdp] timer retry 60
# Set the MSDP peer connection retry interval to 60 seconds in VPN instance mvpn.
<Sysname> system-view
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn] timer retry 60
```


MBGP configuration commands (available only on the HP 5500 EI)

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

For more information about routing policy commands, see *Layer 3—IP Routing Command Reference*.

aggregate (MBGP address family view)

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

IPv4 MBGP address family view

Default level

2: System level

Parameters

ip-address: Specifies a summary address.

mask: Specifies the summary mask, in dotted decimal notation.

mask-length: Specifies the summary mask length, 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: Advertises the summary route only.

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 determine routes for summarization. The routing policy name is a case-sensitive string of 1 to 63 characters.

The keywords of the command are described as follows:

Table 42 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 must be summarized, because the frequent changes of these specific routes might lead to route flaps.

Keywords	Function
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.
suppress-policy	Used to create a summary route and suppress the advertisement of some summarized routes. 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 that satisfy the routing policy for route summarization
attribute-policy	Sets attributes except the AS_PATH attribute for the summary route. You accomplish the same task by using the peer route-policy command.

Description

Use **aggregate** to create a summary route in the IPv4 MBGP routing table.

Use **undo aggregate** to remove a summary route.

By default, no summary route is configured.

Examples

In IPv4 MBGP address family view, create a summary of 192.213.0.0/16 in the IPv4 MBGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] aggregate 10.40.0.0 255.255.0.0
```

balance (MBGP address family view)

Syntax

balance *number*

undo balance

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

number: Specifies the number of MBGP 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 MBGP routes for load balancing.

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

By default, no load balancing is configured.

Unlike IGP, MBGP has no explicit metric for implementing load balancing. Instead, it implements load balancing by using route selection rules.

Related commands: **display ip multicast routing-table**.

Examples

```
# In IPv4 MBGP address family view, set the number of routes for BGP load balancing to 2.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] balance 2
```

bestroute as-path-neglect (MBGP address family view)

Syntax

```
bestroute as-path-neglect
undo bestroute as-path-neglect
```

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

None

Description

Use **bestroute as-path-neglect** to configure MBGP not to consider AS_PATH during best route selection.

Use **undo bestroute as-path-neglect** to restore the default.

By default, MBGP considers AS_PATH during best route selection.

Examples

```
# In IPv4 MBGP address family view, configure BGP to ignore AS_PATH during best route selection.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] bestroute as-path-neglect
```

bestroute compare-med (MBGP address family view)

Syntax

```
bestroute compare-med
undo bestroute compare-med
```

View

IPv4 MBGP 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 during best route selection.

Use **undo bestroute compare-med** to disable this comparison.

The comparison is not enabled by default.

Examples

In IPv4 MBGP address family view, enable the comparison of the MED for paths from each AS during best route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] bestroute compare-med
```

bestroute med-confederation (MBGP address family view)

Syntax

bestroute med-confederation

undo bestroute med-confederation

View

IPv4 MBGP 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 during best route selection.

Use **undo bestroute med-confederation** to disable the comparison.

The comparison is not enabled by default.

The system compares only MED values for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

Examples

In IPv4 MBGP address family view, enable the comparison of the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] bestroute med-confederation
```

compare-different-as-med (MBGP address family view)

Syntax

compare-different-as-med

undo compare-different-as-med

View

IPv4 MBGP 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 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 and routing selection method.

Examples

In IPv4 MBGP address family view, enable the comparison of the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] compare-different-as-med
```

dampening (MBGP address family view)

Syntax

dampening [*half-life-reachable* *half-life-unreachable* *reuse* *suppress* *ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

half-life-reachable: Specifies a half-life for active routes, in the range of 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Specifies a half-life for suppressed routes, in the range of 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Specifies a reuse threshold value for suppressed routes, in the range of 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, in the range of 1 to 20000. The route with a penalty value higher than the threshold is suppressed. The default is 2000.

ceiling: Specifies a ceiling penalty value, in the range of 1001 to 20000. The value must be greater than the *suppress* value. By default, the value is 16000.

route-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Description

Use **dampening** to configure IPv4 MBGP route dampening.

Use **undo dampening** to disable route dampening.

By default, no IPv4 MBGP route dampening is configured.

The command dampens only eBGP routes rather than iBGP routes.

Examples

In IPv4 MBGP address family view, configure IPv4 MBGP route dampening.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] dampening 15 15 1000 2000 10000
```

default local-preference (MBGP address family view)

Syntax

default local-preference *value*

undo default local-preference

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

value: Specifies the default local preference, in the range of 0 to 4294967295. A larger value indicates a higher preference.

Description

Use **default local-preference** to configure the default local preference.

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

By default, the default local preference is 100.

Using this command can affect MBGP route selection.

Examples

In IPv4 MBGP address family view, set the default local preference to 180.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] default local-preference 180
```

default med (MBGP address family view)

Syntax

```
default med med-value
undo default med
```

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

med-value: Specifies the default 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.

Multi-exit discriminator (MED) is an external metric for routes. Different from local preference, MED is exchanged between ASs and stays in the AS after it enters the AS. The route with a lower MED is preferred. When a router that is running BGP obtains several routes with an identical destination but different next hops from various external peers, it selects the best route depending on the MED value. If all other conditions are the same, the system selects the route with the smallest MED as the best external route.

Examples

In IPv4 MBGP address family view, configure the default MED as 25.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] default med 25
```

default-route imported (MBGP address family view)

Syntax

```
default-route imported
undo default-route imported
```

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

None

Description

Use **default-route imported** to allow default route redistribution into the MBGP routing table.

Use **undo default-route imported** to restore the default.

By default, default route redistribution is not allowed.

To redistribute default routes of other protocols into the MBGP routing table, you must use the **default-route imported** command together with the **import-route** command.

Related commands: **import-route**.

Examples

```
# In IPv4 MBGP address family view, allow default route redistribution from OSPF into MBGP.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] default-route imported
[Sysname-bgp-af-mul] import-route ospf 1
```

display ip multicast routing-table

Syntax

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

View

Any view

Default level

2: Monitor level

Parameters

verbose: Displays detailed information about the multicast routing table, including both inactive and active multicast routes. Without the keyword, the command displays brief information about only the active MBGP 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 multicast routing-table** to display the multicast BGP routing table.

All the active MBGP routes in the MBGP routing table are used for RPF check, but inactive MBGP routes are not.

Examples

Display brief information about the active routes in the multicast BGP routing table.

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

```
Routing Tables: Public
```

```
Destinations : 6          Routes : 6
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
2.2.2.0/24	Direct	0	0	2.2.2.1	Vlan-interface2
2.2.2.1/32	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	Vlan-interfacel
192.168.80.10/32	Direct	0	0	127.0.0.1	InLoop0

Table 43 Command output

Field	Description
Destinations	Number of destinations
Routes	Number of routes
Destination/Mask	Destination address/mask length
Proto	Routing protocol that discovered the route
Pre	Route preference
Cost	Route cost
NextHop	Next hop of the route
Interface	Outgoing interface to reach the destination

Display the detailed information of the multicast routing table.

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

```
Routing Table : Public
```

```
Destinations : 2          Routes : 2
```

```
Destination: 192.168.80.0/24
```

```
Protocol: Direct          Process ID: 0
```

```
Preference: 0            Cost: 0
```

```
IpPrecedence:           QoSLeId:
```

```
NextHop: 192.168.80.10   Interface: Vlan-interfacel
```

```
BkNextHop: 0.0.0.0       BkInterface:
```

```
RelyNextHop: 0.0.0.0     Neighbour: 0.0.0.0
```

```
Tunnel ID: 0x0           Label: NULL
```

```
State: Active Adv        Age: 00h14m49s
```

```
Tag: 0
```

```
Destination: 192.168.80.10/32
```

```
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      Neighbour: 0.0.0.0
    Tunnel ID: 0x0            Label: NULL
    State: Active NoAdv       Age: 00h14m49s
    Tag: 0

```

Table 44 Command output

Field	Description
Destination	Destination/mask
Protocol	Routing protocol that discovered the route
Process ID	Process ID
Preference	Route preference
Cost	Route cost
IpPrecedence	IP precedence
QoSLocalId	QoS local ID
NextHop	Nexthop of the route
Interface	Outgoing interface to reach the destination
BkNextHop	Backup next hop
BkInterface	Backup outgoing interface
RelyNextHop	Recursive next hop
Neighbour	Neighbor address
Tunnel ID	Tunnel ID
Label	Label
State	Route state: Active, Inactive, Adv (can be advertised), NoAdv (cannot be advertised), GotQ (route recursion succeeded), WaitQ (route recursion has not succeeded yet)
Age	Age of the route, in the sequence of hours, minutes, and seconds from left to right
Tag	Route tag

display ip multicast routing-table *ip-address*

Syntax

```

display ip multicast routing-table ip-address [mask-length | mask] [longer-match] [verbose] [ [ begin
| exclude | include ] regular-expression ]

```

View

Any view

Default level

2: Monitor level

Parameters

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

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

mask: Specifies the IP address mask in dotted decimal format.

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

verbose: Displays detailed information about both active and inactive routes. With this argument absent, 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 multicast routing-table** *ip-address* to display information about multicast routes to a specified destination address.

Executing the command with different parameters yields different outputs:

display ip multicast routing-table *ip-address*

It displays all multicast routes that fall into the natural network of the IP address. If no such multicast routes are available, it displays only the longest matched active multicast route.

display ip multicast routing-table *ip-address mask*

It displays the multicast route that exactly matches the IP address and mask.

Examples

Display brief information about all multicast routes that fall into the natural network of the IP address (A multicast route is available).

```
<Sysname> display ip multicast routing-table 169.0.0.0
Routing Table : Public
Summary Count : 1
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
169.0.0.0/16	Direct	0	0	127.0.0.1	InLoop0

For more information about the fields, see [Table 43](#).

Display brief information about the longest matched active multicast route (No multicast route falls into the natural network of the IP address).

```
<Sysname> display ip multicast routing-table 169.253.0.0
Routing Table : Public
Summary Count : 1
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
169.0.0.0/16	Direct	0	0	127.0.0.1	InLoop0

For more information about the fields, see [Table 43](#).

Display detailed information about multicast routes that fall into the natural network of the IP address (A multicast route is available).

```
<Sysname> display ip multicast routing-table 2.2.2.1 verbose
Routing Table : Public
Summary Count : 1
```

```
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    Neighbour: 0.0.0.0
  Tunnel ID: 0x0          Label: NULL
  State: Active NoAdv     Age: 05h38m46s
  Tag: 0
```

For more information about the fields, see [Table 44](#).

Display detailed information about the longest matched active multicast route (No multicast route falls into the natural network of the IP address).

```
<Sysname> display ip multicast routing-table 169.253.2.1 verbose
Routing Table : Public
Summary Count : 1
```

```
Destination: 169.0.0.0/8
  Protocol: Direct          Process ID: 0
  Preference: 0            Cost: 0
  IpPrecedence:           QoSLeId:
  NextHop: 169.1.1.1       Interface: Vlan-interface1
  BkNextHop: 0.0.0.0      BkInterface:
  RelyNextHop: 0.0.0.0    Neighbour: 0.0.0.0
  Tunnel ID: 0x0          Label: NULL
  State: Active Adv       Age: 00h00m32s
  Tag: 0
```

For more information about the fields, see [Table 44](#).

display bgp multicast group

Syntax

```
display bgp multicast group [ group-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

2: Monitor level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its 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 multicast group** to display IPv4 MBGP peer group information.

Examples

Display the information of the IPv4 MBGP peer group **aaa**.

```
<Sysname> display bgp multicast 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 45 Command output

Field	Description
BGP peer-group	Name of the peer group.
Remote AS	AS number of the peer group.
Type	Type of the peer group: iBGP or eBGP.
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.
Configured hold timer value	Holdtime interval.
Keepalive timer value	Keepalive interval.
Minimum time between advertisement runs	Minimum interval for route advertisement.
Peer Preferred Value	Preferred value specified for the routes from the peer.
No routing policy is configured	No routing policy is configured.

Field	Description
Members	Detailed information of the members in the peer group.
Peer	IPv4 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.
PrefRcv	Number of prefixes received.
Up/Down	Time elapsed.
State	State machine of the peer.

display bgp multicast network

Syntax

```
display bgp multicast network [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

2: 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 multicast network** to display IPv4 MBGP routing information advertised with the **network** command.

Examples

Display IPv4 MBGP routing information advertised with the **network** command.

```
<Sysname> display bgp multicast 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 46 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 referenced
Short-cut	Shortcut route

display bgp multicast paths

Syntax

```
display bgp multicast paths [ as-regular-expression | | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

2: Monitor level

Parameters

as-regular-expression: Specifies an AS path regular expression, a case-sensitive string of 1 to 80 characters, including spaces.

|: 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 multicast paths** to display the AS path information of IPv4 MBGP routes.

Examples

```
# Display the AS path information of IPv4 MBGP routes.
```

```
<Sysname> display bgp multicast paths ^200
```

```
Address      Hash      Refcount  MED      Path/Origin
0x5917100    11        1         0        200 300i
```

Table 47 Command output

Field	Description
Address	Route address in the local database, in dotted hexadecimal notation.
Hash	Hash index.

Field	Description
Refcount	Count of routes that reference the path.
MED	MED of the path.
Path	AS_PATH attribute of the path, recording the ASs that it has passed to avoid routing loops.
Origin	<p>ORIGIN attribute of the path:</p> <ul style="list-style-type: none"> • i—Indicates that the route is interior to the AS. Summary routes and routes injected through the network command are considered IGP routes. • e—Indicates that the route is learned from the Exterior Gateway Protocol (EGP). • ?—Indicates that the origin of the route is unknown. Routes redistributed from other routing protocols have this origin attribute.

display bgp multicast peer

Syntax

```
display bgp multicast peer [ [ ip-address ] verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

2: Monitor level

Parameters

ip-address: Specifies the IP address of an IPv4 MBGP peer to be displayed, in dotted decimal notation.

verbose: Displays the detailed information of the peer or the 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 multicast peer** to display IPv4 MBGP peer information.

Examples

```
# Display the detailed information of the IPv4 MBGP peer 10.110.25.20.
```

```
<Sysname> display bgp multicast 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
Peer support bgp route AS4 capability
Address family IPv4 Unicast: advertised and received
Address family IPv4 Multicast: 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 48 Command output

Field	Description
Peer	IP address of the peer.
Local	Local router ID.
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.
Configured: Active Hold Time: 180 sec Keepalive Time: 60 sec	Local holdtime interval and keepalive interval.
Received: Active Hold Time	Remote holdtime interval.
Negotiated: Active Hold Time Keepalive Time:60 sec	Negotiated holdtime interval and keepalive interval.

Field	Description
Peer optional capabilities	Optional capabilities that the peer supports, including multiprotocol BGP extensions and route refresh.
Peer support bgp multi-protocol extended	The peer supports multiprotocol BGP extensions.
Peer support bgp route refresh capability	The peer supports route refresh.
Peer support bgp route AS4 capability	The peer supports 4-byte router IDs.
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	Threshold value.
Minimum time between advertisement runs	Minimum route advertisement interval.
Optional capabilities	Optional capabilities that the peer enables (displayed only after optional capabilities are configured).
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. (This field is displayed only after the ORF capability is enabled for the BGP peer.)
Local: both	The local BGP router supports both the ORF sending and receiving capabilities. (This field is displayed only after the ORF capability is enabled for the BGP peer.)
Negotiated: send	<p>Negotiation result: The local BGP router can send route-refresh messages that carry the ORF information, and the peer can receive route-refresh messages that carry the ORF information.</p> <ul style="list-style-type: none"> • If receive is displayed, the local BGP router can receive route-refresh messages that carry the ORF information, and the peer can send route-refresh messages that carry the ORF information. • If both send and receive are displayed, the local BGP router and the peer can both send and receive route-refresh messages that carry the ORF information • This field is not displayed if neither the send nor the receive capability is supported. • This field is displayed only after the ORF capability is enabled for the BGP peer.
Peer Preferred Value	Preferred value specified for the routes from the peer.
BFD	Status of BGP (enabled/disabled).
Routing policy configured	Local routing policy.

display bgp multicast peer received ip-prefix

Syntax

```
display bgp multicast peer ip-address received ip-prefix [ | { begin | exclude | include }  
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ip-address: Specifies the 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 multicast peer received ip-prefix** to display the prefix entries in the ORF information of the specified BGP peer.

Examples

```
# Display the prefix information received from the BGP peer 10.110.25.20.
```

```
<Sysname> display bgp multicast 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 49 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, which indicates that the mask length must be greater than or equal to the specific value.
Le	Less-equal, which indicates that the mask length must be less than or equal to the specific value.

display bgp multicast routing-table

Syntax

```
display bgp multicast 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: Specifies a destination IP address.

mask: Specifies the network mask, in dotted decimal notation.

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

longer-prefixes: 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 multicast routing-table** to display IPv4 MBGP routing information.

Examples

```
# Display the IPv4 MBGP routing table.
```

```
<Sysname> display bgp multicast 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	200 300i

Table 50 Command output

Field	Description
Total Number of Routes	Total number of routes.
BGP Local router ID	BGP local router ID.

Field	Description
Status codes	Status codes, including: <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	ORIGIN attributes, including: <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.
MED	Measurement value of the route.
LocPrf	Local preference value.
PrefVal	Preferred value of the route.
Path	AS_PATH attribute, which records the ASs that the packet has passed to avoid routing loops.
Ogn	ORIGIN attribute of the route, which can be one of the following values: <ul style="list-style-type: none"> • i—Indicates that the route is interior to the AS. Summary routes and the routes injected through 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 some other means. BGP marks routes redistributed from IGP as incomplete.

display bgp multicast routing-table as-path-acl

Syntax

```
display bgp multicast routing-table as-path-acl as-path-acl-number [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

2: Monitor level

Parameters

as-path-acl-number: Displays IPv4 MBGP routing information that matches 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 multicast routing-table as-path-acl** to display IPv4 MBGP routes that match an AS path list.

Examples

Display IPv4 MBGP routes that match AS path list 1.

```
<Sysname> display bgp multicast 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 more information about the output, see [Table 50](#).

display bgp multicast routing-table cidr

Syntax

```
display bgp multicast routing-table cidr [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

2: 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 multicast routing-table cidr** to display IPv4 MBGP Classless Inter-Domain Routing (CIDR) routing information.

Examples

```
# Display IPv4 MBGP CIDR routing information.
```

```
<Sysname> display bgp multicast 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 more information about the output, see [Table 50](#).

display bgp multicast routing-table community

Syntax

```
display bgp multicast 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

2: Monitor level

Parameters

aa:nn: Specifies a community by its number. Both *aa* and *nn* are in the range of 0 to 65535.

&<1-13>: Specifies an argument before it can be entered up to 13 times.

no-advertise: Displays MBGP routes that cannot be advertised to any peer.

no-export: Displays MBGP routes that cannot be advertised out of the AS. If a confederation is configured, it displays the routes that cannot be advertised out of the confederation, but can be advertised to other sub ASs in the confederation.

no-export-subconfed: Displays the MBGP routes that cannot be advertised out of the AS or to other sub ASs in the confederation.

whole-match: Displays the MBGP routes that exactly match the specified COMMUNITY attributes.

|: 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 multicast routing-table community** to display IPv4 MBGP routing information with the specified BGP COMMUNITY attribute.

Examples

Display IPv4 MBGP routing information with the specified BGP COMMUNITY attribute.

```
<Sysname> display bgp multicast 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          0       i
*> 40.40.40.0/24     20.20.20.1           0          0          200 300i
```

For more information about the output, see [Table 50](#).

display bgp multicast routing-table community-list

Syntax

```
display bgp multicast 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

2: 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 the routes that exactly match 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 multicast routing-table community-list** to display IPv4 MBGP routing information that matches the specified BGP community list.

Examples

```
# Display MBGP routing information that matches the community list 100.
```

```
<Sysname> display bgp multicast routing-table community-list 100
```

```
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	1.2.3.4	0		0	i
*>	40.40.40.0/24	1.2.3.4	0		0	i

For more information about the output, see [Table 50](#).

display bgp multicast routing-table dampened

Syntax

```
display bgp multicast routing-table dampened [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

2: 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 multicast routing-table dampened** to display dampened IPv4 MBGP routes.

Examples

```
# Display dampened IPv4 MBGP routes.
```

```
<Sysname> display bgp multicast 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 51 Command output

Field	Description
From	IP address from which the route was received
Reuse	Reuse time of the route

For more information about the output, see [Table 50](#).

display bgp multicast routing-table dampening parameter

Syntax

```
display bgp multicast routing-table dampening parameter [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

2: 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 multicast routing-table dampening parameter** to display IPv4 MBGP route dampening parameters.

Related commands: **dampening**.

Examples

```
# Display IPv4 MBGP route dampening parameters.
```

```
<Sysname> display bgp multicast 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 52 Command output

Field	Description
Maximum Suppress Time	Maximum suppression time
Ceiling Value	Ceiling penalty value
Reuse Value	Reuse value
HalfLife Time	Half-life time of active routes
Suppress-Limit	Threshold at which a route is suppressed

display bgp multicast routing-table different-origin-as

Syntax

```
display bgp multicast routing-table different-origin-as [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

2: 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 multicast routing-table different-origin-as** to display the IPv4 MBGP routes that originate from different autonomous systems.

Examples

```
# Display the IPv4 MBGP routes that originate from different autonomous systems.
```

```
<Sysname> display bgp multicast 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 more information about the output, see [Table 50](#).

display bgp multicast routing-table flap-info

Syntax

```
display bgp multicast 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

2: Monitor level

Parameters

as-regular-expression: Displays route flap information that matches the AS path regular expression.

as-path-acl-number: Displays route flap information that matches the AS path list. The number is in the range of 1 to 256.

ip-address: Specifies a destination IP address.

mask: Specifies the network mask, in dotted decimal notation.

mask-length: Specifies the 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 multicast routing-table flap-info** to display IPv4 MBGP route flap statistics. If no parameter is specified, this command displays all IPv4 MBGP route flap statistics.

Examples

```
# Display IPv4 MBGP route flap statistics.
```

```
<Sysname> display bgp multicast 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 53 Command output

Field	Description
From	Source IP address of the route
Flaps	Number of routing flaps
Duration	Route flap duration
Reuse	Reuse time of the route

For more information about the output, see [Table 50](#).

display bgp multicast routing-table peer

Syntax

```
display bgp multicast 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

2: Monitor level

Parameters

ip-address: Specifies the IP address of an IPv4 MBGP peer.

advertised-routes: Displays routing information advertised to the specified peer.

received-routes: Displays routing information received from the specified peer.

network-address: Specifies the IP address of the destination network.

mask: Specifies the mask of the destination network, in dotted decimal notation.

mask-length: Specifies the 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 multicast routing-table peer** to display IPv4 MBGP routing information advertised to or received from the specified IPv4 MBGP peer.

Related commands: **display bgp multicast peer**.

Examples

```
# Display IPv4 MBGP routing information advertised to the peer 20.20.20.1.
```

```
<Sysname> display bgp multicast 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 more information about the output, see [Table 50](#).

display bgp multicast routing-table regular-expression

Syntax

```
display bgp multicast routing-table regular-expression as-regular-expression
```

View

Any view

Default level

2: Monitor level

Parameters

as-regular-expression: AS path regular expression, a case-sensitive string of 1 to 80 characters, including spaces.

Description

Use **display bgp multicast routing-table regular-expression** to display IPv4 MBGP routing information that matches the specified AS path regular expression.

Examples

```
# Display IPv4 MBGP routing information that matches AS path regular expression 300$.
```

```
<Sysname> display bgp multicast 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 more information about the output, see [Table 50](#).

display bgp multicast routing-table statistic

Syntax

```
display bgp multicast routing-table statistic [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

2: 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 multicast routing-table statistic** to display IPv4 MBGP routing statistics.

Examples

```
# Display IPv4 MBGP routing statistics.
```

```
<Sysname> display bgp multicast routing-table statistic
```

```
Total Number of Routes: 4
```

filter-policy export (MBGP address family 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

IPv4 MBGP address family view

Default level

2: System level

Parameters

acl-number: Specifies the number of an ACL used to filter outgoing routing information, ranging from 2000 to 3999.

ip-prefix-name: Specifies the 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 process ID is in the range of 1 to 65535.

ospf process-id: Filters outgoing routes redistributed from the OSPF process. The process ID is in the range of 1 to 65535.

rip process-id: Filters outgoing routes redistributed from a RIP process. The process 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.

By default, the filtering is not configured.

If no routing protocol is specified, all redistributed routes are filtered.

Examples

In IPv4 MBGP address family view, reference ACL 2000 to filter all outgoing routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] filter-policy 2000 export
```

filter-policy import (MBGP address family view)

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy import

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

acl-number: Specifies the number of an ACL used to filter incoming routing information, in the range of 2000 to 3999.

ip-prefix-name: Specifies the 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.

Examples

In IPv4 MBGP address family view, reference ACL 2000 to filter incoming routing information.

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



```
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] filter-policy 2000 import
```

import-route (MBGP address family 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

IPv4 MBGP address family view

Default level

2: System level

Parameters

protocol: Redistributes routes from the routing protocol, which can be **direct**, **isis**, **ospf**, **rip**, or **static** at present.

process-id: Specifies a process by its ID, in the range of 1 to 65535. It is available only when the protocol is **isis**, **ospf**, or **rip**.

all-processes: Redistributes routes from all the processes of the specified routing protocol. It is available only when the specified protocol is **isis**, **ospf**, or **rip**.

allow-direct: Redistributes direct routes from the specified routing protocol. This keyword is available only when the specified routing 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 a redistributed route is used as its MED in the BGP routing domain.

route-policy-name: Specifies the name of a routing policy used to filter redistributed routes, a case-sensitive string of 1 to 63 characters.

Description

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

Use **undo import-route** to disable route redistribution from a routing protocol.

By default, MBGP does not redistribute routes from other protocols.

The ORIGIN attribute of routes redistributed through the **import-route** command is incomplete.

The **undo import-route** *protocol* **all-processes** command can cancel only the configuration that you make by using the **import-route** *protocol* **all-processes** command. To cancel the configuration that you make by using the **import-route** *protocol* *process-id* command, you must use the **undo import-route** *protocol* *process-id* command.

Examples

```
# In IPv4 MBGP address family view, enable route redistribution from RIP.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] import-route rip
```

ipv4-family multicast

Syntax

```
ipv4-family multicast
undo ipv4-family multicast
```

View

BGP view

Default level

2: System level

Parameters

None

Description

Use **ipv4-family multicast** to enter IPv4 MBGP address family view.

Use **undo ipv4-family multicast** to remove all configurations made in IPv4 MBGP address family view and return to BGP view.

Examples

```
# Enter IPv4 MBGP address family view.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul]
```

network (MBGP address family view)

Syntax

```
network ip-address [ mask | mask-length ] [ short-cut | route-policy route-policy-name ]
undo network ip-address [ mask | mask-length ] [ short-cut ]
```

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

ip-address: Specifies a destination IP address.

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

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

short-cut: Specifies the route to use the local preference. If the route is an eBGP route whose preference is higher than the local preference, using this keyword can configure the eBGP route to use the local preference, and thus the route cannot become the optimal route.

route-policy-name: Specifies the 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 IPv4 MBGP routing table.

Use **undo network** to remove a network from the IPv4 MBGP 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 through the **network** command is IGP.

Examples

```
# In IPv4 MBGP address family view, inject the network 10.0.0.0/16.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] network 10.0.0.0 255.255.0.0
```

peer advertise-community (MBGP address family view)

Syntax

peer { *group-name* | *ip-address* } **advertise-community**

undo peer { *group-name* | *ip-address* } **advertise-community**

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies an IPv4 MBGP peer by its IP address.

Description

Use **peer advertise-community** to advertise the COMMUNITY attribute to a peer or a peer group.

Use **undo peer advertise-community** to disable the COMMUNITY attribute advertisement to a peer or a peer group.

By default, no COMMUNITY attribute is advertised to any peer or peer group.

Related commands: **apply community**, **if-match community**, and **ip community-list** (*Layer 3—IP Routing Command Reference*).

Examples

In IPv4 MBGP address family view, advertise the COMMUNITY attribute to the existing peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test advertise-community
```

peer advertise-ext-community (MBGP address family view)

Syntax

```
peer { group-name | ip-address } advertise-ext-community
undo peer { group-name | ip-address } advertise-ext-community
```

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies an IPv4 MBGP peer by its IP address.

Description

Use **peer advertise-ext-community** to advertise the extended community attribute to a peer or a peer group.

Use **undo peer advertise-ext-community** to disable the extended community attribute advertisement to a peer or a peer group.

By default, no extended community attribute is advertised to a peer or a peer group.

Related commands: **apply extcommunity**, **if-match extcommunity**, and **ip extcommunity-list** (*Layer 3—IP Routing Command Reference*).

Examples

In IPv4 MBGP address family view, advertise the extended community attribute to the existing peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test advertise-ext-community
```

peer allow-as-loop (MBGP address family view)

Syntax

```
peer { group-name | ip-address } allow-as-loop [ number ]
```

```
undo peer { group-name | ip-address } allow-as-loop
```

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies the IP address of an IPv4 MBGP peer.

number: Specifies the number of times the local AS number can appear in routes from the peer or the 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 or a peer group, and to configure the number of times that 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.

Related commands: **display bgp multicast routing-table peer**.

Examples

In IPv4 MBGP address family view, configure the number of times that the local AS number can appear in routes from the peer 1.1.1.1 as 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 as-number 200
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer 1.1.1.1 enable
[Sysname-bgp-af-mul] peer 1.1.1.1 allow-as-loop 2
```

peer as-path-acl (MBGP address family 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

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies the IP address of an IPv4 MBGP peer.

as-path-acl-number: Specifies an AS path list by its 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 an MBGP peer or a peer group based on a specified AS path list.

Use **undo peer as-path-acl** to remove the filtering.

By default, no AS path list based filtering is configured.

Related commands: **apply as-path**, **if-match as-path**, and **ip as-path** (*Layer 3—IP Routing Command Reference*).

Examples

In IPv4 MBGP address family view, reference the AS path list 1 to filter routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test as-path-acl 1 export
```

peer capability-advertise orf (MBGP address family view)

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

MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies an IPv4 MBGP peer by its IP address.

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 an MBGP peer or peer group.

Use **undo peer capability-advertise orf** to disable the ORF capability for the MBGP peer or peer group.

By default, the ORF capability is not enabled for an MBGP 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 that carry the standard ORF information from the peer or send route-refresh messages that carry the standard ORF information to the peer. For nonstandard ORF capability negotiation, you must also configure the **peer capability-advertise orf non-standard** command in IPv4 unicast view.
- After you disable the ORF capability, the local BGP router does not negotiate the ORF capability with the specified peer or peer group.

Table 54 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, respectively.

Examples

Enable the ORF capability for the BGP peer 18.10.0.9. Then, after negotiation, the local router can exchange multicast 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] ipv4-family multicast
[Sysname-bgp-af-mul] peer 18.10.0.9 enable
[Sysname-bgp-af-mul] peer 18.10.0.9 capability-advertise orf ip-prefix both
```

peer default-route-advertise (MBGP address family 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

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies an IPv4 MBGP peer by its IP address.

route-policy-name: Specifies an routing policy by its name, a case-sensitive string of 1 to 63 characters.

Description

Use **peer default-route-advertise** to advertise a default route to a peer or a peer group.

Use **undo peer default-route-advertise** to disable default route advertisement to a peer or a peer group.

By default, no default route is advertised to a peer or a peer group.

When you use this command, the router unconditionally sends a default route with the next hop as itself to the peer or peer group regardless of whether the default route is available in the routing table.

Examples

In IPv4 MBGP address family view, advertise a default route to the existing peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test default-route-advertise
```

peer enable (MBGP address family view)

Syntax

peer { *group-name* | *ip-address* } **enable**

undo peer { *group-name* | *ip-address* } **enable**

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies an IPv4 MBGP peer by its IP address.

Description

Use **peer enable** to enable the specified peer or peer group that has been created in BGP view.

Use **undo peer enable** to disable the specified peer or peer group that has been created in BGP view.

If a peer is disabled, the router does not exchange routing information with the peer.

Examples

Enable the peer 18.10.0.9.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 18.10.0.9 as-number 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer 18.10.0.9 enable
```


peer filter-policy (MBGP address family 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

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies the IP address of an IPv4 MBGP peer.

acl-number: Specifies an ACL by its number, in the range of 2000 to 3999.

export: Uses the ACL to filter routes outgoing to the peer or the peer group.

import: Uses the ACL to filter routes incoming from the peer or the 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 filtering.

By default, no ACL-based filter policy is configured for a peer or a peer group.

Related commands: **peer as-path-acl**.

Examples

```
# In IPv4 MBGP address family view, reference ACL 2000 to filter routes sent to the peer group test.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] group test external  
[Sysname-bgp] peer test as-number 200  
[Sysname-bgp] ipv4-family multicast  
[Sysname-bgp-af-mul] peer test enable  
[Sysname-bgp-af-mul] peer test filter-policy 2000 export
```

peer group (MBGP address family view)

Syntax

```
peer ip-address group group-name  
undo peer ip-address group group-name
```

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies an IPv4 MBGP peer by its IP address.

Description

Use **peer group** to add an IPv4 MBGP peer to an IPv4 MBGP peer group.

Use **undo peer group** to delete a specified peer from a peer group.

By default, no peer is added to a peer group.

Examples

```
# In IPv4 MBGP address family view, add the peer 10.1.1.1 to the multicast eBGP peer group test.
<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] ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer 10.1.1.1 group test
```

peer ip-prefix (MBGP address family view)

Syntax

peer { *group-name* | *ip-address* } **ip-prefix** *ip-prefix-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **ip-prefix** { **export** | **import** }

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies an IPv4 MBGP peer by its IP address.

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

export: Applies the filter to routes outgoing to the specified peer or peer group.

import: Applies the filter to routes from the specified peer or peer group.

Description

Use **peer ip-prefix** to reference an IP prefix list to filter routes received from or advertised to a peer or a peer group.

Use **undo peer ip-prefix** to remove the configuration.

By default, no IP prefix list-based filtering is configured.

Examples

```
# In IPv4 MBGP address family view, use the IP prefix list 1 to filter routes outgoing to the peer group test.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test ip-prefix list1 export
```

peer keep-all-routes (MBGP address family view)

Syntax

```
peer { group-name | ip-address } keep-all-routes
undo peer { group-name | ip-address } keep-all-routes
```

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies an IPv4 MBGP peer by its IP address.

Description

Use **peer keep-all-routes** to save original routing information from a peer or a peer group, including the routes that fail to pass the inbound policy (if configured).

Use **undo peer keep-all-routes** to disable this feature.

By default, the feature is not enabled.

Examples

```
# In IPv4 MBGP address family view, save all the routing information from peer 131.108.1.1.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.108.1.1 as-number 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer 131.108.1.1 enable
[Sysname-bgp-af-mul] peer 131.108.1.1 keep-all-routes
```

peer next-hop-local (MBGP address family view)

Syntax

```
peer { group-name | ip-address } next-hop-local
undo peer { group-name | ip-address } next-hop-local
```

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies an IPv4 MBGP peer by its IP address.

Description

Use **peer next-hop-local** to specify the router as the next hop for routes sent to a peer or a peer group.

Use **undo peer next-hop-local** to remove the configuration.

By default, the routes advertised to an eBGP peer or a peer group take the local router as the next hop, but the routes outgoing to an iBGP peer or a peer group do not take the local router as the next hop.

Examples

In IPv4 MBGP address family view, specify the router as the next hop for routes sent to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test internal
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test next-hop-local
```

peer preferred-value (MBGP address family view)

Syntax

peer { *group-name* | *ip-address* } **preferred-value** *value*

undo peer { *group-name* | *ip-address* } **preferred-value**

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies the IP address of an IPv4 MBGP peer.

value: Specifies a preferred value, in the range of 0 to 65535.

Description

Use **peer preferred-value** to specify a preferred value for routes received from a peer or peer group.

Use **undo peer preferred-value** to restore the default.

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 or a peer group, the routing policy sets the specified preferred value for the routes that match it. Other routes that do not match the routing policy use the value set through the **peer preferred-value** command. If the preferred value specified in the routing policy is zero, the routes that match it also use the value set through the **peer preferred-value** command.

To learn how to use 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*. For more information about the command, see *Layer 3—IP Routing Command Reference*.

Examples

```
# In IPv4 MBGP address family 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 as-number 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer 131.108.1.1 enable
[Sysname-bgp-af-mul] peer 131.108.1.1 preferred-value 50
```

peer public-as-only (MBGP address family view)

Syntax

```
peer { group-name | ip-address } public-as-only
undo peer { group-name | ip-address } public-as-only
```

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies an IPv4 MBGP peer by its IP address.

Description

Use **peer public-as-only** to not keep private AS numbers in BGP updates sent to a peer or a peer group.

Use **undo peer public-as-only** to keep private AS numbers in BGP updates sent to a peer or a peer group.

By default, outgoing BGP updates can carry private AS numbers.

The command does not take effect for BGP updates with both public and private AS numbers. The range of private AS numbers is from 64512 to 65535.

Examples

```
# In IPv4 MBGP address family view, disable updates sent to the peer group test from carrying private AS numbers.
```

```

<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test public-as-only

```

peer reflect-client (MBGP address family view)

Syntax

```

peer { group-name | peer-address } reflect-client
undo peer { group-name | peer-address } reflect-client

```

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

peer-address: IP address of an IPv4 MBGP peer.

Description

Use **peer reflect-client** to configure the router as a route reflector and specify a peer or a 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 IPv4 MBGP address family 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] group test internal
[Sysname-bgp] peer test as-number 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test reflect-client

```

peer route-limit (MBGP address family view)

Syntax

```

peer { group-name | ip-address } route-limit limit [ percentage ]
undo peer { group-name | ip-address } route-limit

```

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies the IP address of an IPv4 MBGP peer.

limit: Specifies the upper limit of IP prefixes that can be received from the peer or peer group, in the range of 1 to 12288.

percentage: Specifies the percentage that will cause the system to generate alarm information if the number of received routes divided by the upper limit reaches it. The percentage is in the range of 1 to 100. The default is 75.

Description

Use **peer route-limit** to set the maximum number of the routes that can be received from a peer or a peer group.

Use **undo peer route-limit** to restore the default.

The number is unlimited by default.

Examples

```
# In IPv4 MBGP address family view, set the number of the routes that can be received from peer 131.108.1.1 to 10000.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.108.1.1 as-number 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer 131.108.1.1 enable
[Sysname-bgp-af-mul] peer 131.108.1.1 route-limit 10000
```

peer route-policy (MBGP address family 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

IPv4 MBGP address family view

Default level

2: System level

Parameters

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

ip-address: Specifies an IPv4 MBGP peer by its IP address.

route-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

export: Applies the routing policy to routes advertised to the peer or the peer group.

import: Applies the routing policy to routes received from the peer or 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 applied to routes from/to the peer or the peer group.

The **peer route-policy** command does not apply the **if-match interface** clause in the referenced routing policy. For more information, see *Layer 3—IP Routing Command Reference*.

Examples

In IPv4 MBGP address family view, apply the routing policy **test-policy** to routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test route-policy test-policy export
```

preference (MBGP address family view)

Syntax

preference { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }

undo preference

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

external-preference: Specifies the preference of eBGP routes, in the range of 1 to 255.

internal-preference: Specifies the preference of iBGP routes, in the range of 1 to 255.

local-preference: Specifies the preference of local routes, in the range of 1 to 255.

route-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. Using a routing policy can set preferences for the routes that match it. As for the unmatched routes, the default preferences are adopted.

Description

Use **preference** to configure preferences for external, internal, and local routes.

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

The default preference values of external, internal and local BGP routes are 255, 255, and 130, respectively.

Examples

In IPv4 MBGP address family view, configure preferences for eBGP, iBGP, and local IPv4 MBGP routes as 20, 20, and 200.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] preference 20 20 200
```

reflect between-clients (MBGP address family view)

Syntax

reflect between-clients

undo reflect between-clients

View

IPv4 MBGP 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 the routes of a client to other clients. If the clients of a route reflector are fully meshed, you must 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] ipv4-family multicast
[Sysname-bgp-af-mul] undo reflect between-clients
```

reflector cluster-id (MBGP address family view)

Syntax

reflector cluster-id { *cluster-id* | *ip-address* }

undo reflector cluster-id

View

IPv4 MBGP address family view

Default level

2: System level

Parameters

cluster-id: Specifies a route reflector by its cluster ID, in the range of 1 to 4294967295.

ip-address: Specifies a route reflector by its IP address, in the format of an IP 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, each route reflector uses its router ID as the cluster ID.

A route reflector reflects a route from a client to another client. The router ID of the route reflector is the ID of the cluster. You can configure multiple route reflectors to improve network stability. If a cluster has multiple route reflectors, you must use the **reflector cluster-id** command to specify the same cluster ID for these route reflectors, in order to avoid routing loops.

Related commands: **reflect between-clients** and **peer reflect-client**.

Examples

Specify 80 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] ipv4-family multicast
[Sysname-bgp-af-mul] reflector cluster-id 80
```

refresh bgp ipv4 multicast

Syntax

```
refresh bgp ipv4 multicast { all | ip-address | group group-name | external | internal } { export | import }
```

View

User view

Default level

2: Monitor level

Parameters

all: Soft-resets all BGP connections.

ip-address: Specifies an IPv4 MBGP peer by its IP address.

group-name: Specifies an IPv4 MBGP peer group by its name, a string of 1 to 47 characters.

external: Soft-resets eBGP connections.

internal: Soft-resets iBGP connections.

export: Specifies an outbound soft reset.

import: Specifies an inbound soft reset.

Description

Use **refresh bgp ipv4 multicast** to perform a soft reset on specified IPv4 MBGP connections. This method can also refresh the MBGP routing table and apply a new routing policy seamlessly.

To perform a BGP soft reset, be sure that all routers in the network support route refresh. If a router does not support the route-refresh function, you must configure the **peer keep-all-routes** command to save all the routing information of the peer before BGP soft reset.

Examples

```
# Soft-reset all the IPv4 MBGP connections.
<Sysname> refresh bgp ipv4 multicast all import
```

reset bgp ipv4 multicast

Syntax

```
reset bgp ipv4 multicast { all | as-number | ip-address | group group-name | external | internal }
```

View

User view

Default level

2: System level

Parameters

all: Resets all MBGP connections.

as-number: Resets MBGP connections to peers in the AS.

ip-address: Resets the connection with an IPv4 MBGP peer.

group *group-name*: Resets connections with the specified BGP peer group.

external: Resets all the multicast eBGP connections.

internal: Resets all the multicast iBGP connections.

Description

Use **reset bgp ipv4 multicast** to reset specified MBGP connections.

Examples

```
# Reset all the IPv4 MBGP connections.
<Sysname> reset bgp ipv4 multicast all
```

reset bgp ipv4 multicast dampening

Syntax

```
reset bgp ipv4 multicast dampening [ ip-address [ mask | mask-length ] ]
```

View

User view

Default level

1: Monitor level

Parameters

ip-address: Specifies a destination IP address.

mask: Specifies the network mask, in dotted decimal notation. The default is 255.255.255.255.

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

Description

Use **reset bgp ipv4 multicast dampening** to clear route dampening information and release suppressed routes.

Related commands: **dampening** and **display bgp multicast routing-table dampened**.

Examples

```
# Clear damping information of route 20.1.0.0/16 and release the suppressed route.
```

```
<Sysname> reset bgp ipv4 multicast dampening 20.1.0.0 255.255.0.0
```

reset bgp ipv4 multicast flap-info

Syntax

```
reset bgp ipv4 multicast flap-info [ regex as-path-regular-expression | as-path-acl as-path-acl-number | ip-address [ mask | mask-length ] ]
```

View

User view

Default level

1: Monitor level

Parameters

as-path-regular-expression: Clears the flap statistics of the routes that match the AS path regular expression, a case-sensitive string of 1 to 80 characters with spaces included.

as-path-acl-number: Clears the flap statistics for the routes that match the AS path list, number of which is in the range of 1 to 256.

ip-address: Specifies an IP address.

mask: Specifies the network mask, in dotted decimal notation. The default is 255.255.255.255.

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

Description

Use **reset bgp ipv4 multicast flap-info** to clear IPv4 MBGP routing flap statistics.

The flap statistics of all the routes is cleared if no parameter is specified.

Examples

```
# Clear the flap statistics of all IPv4 MBGP routes that match AS path list 10.
```

```
<Sysname> reset bgp ipv4 multicast flap-info as-path-acl 10
```

summary automatic (MBGP address family view)

Syntax

```
summary automatic
```

undo summary automatic

View

IPv4 MBGP address family 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.

The default routes and the routes imported through the **network** command cannot be automatically summarized.

The **summary automatic** command helps IPv4 MBGP limit the number of routes redistributed from IGP.

Examples

In IPv4 MBGP address family view, enable automatic route summarization.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] summary automatic
```

MLD snooping configuration commands

display mld-snooping group

Syntax

```
display mld-snooping group [ vlan vlan-id ] [ slot slot-number ] [ verbose ] [ | { begin | exclude | include }  
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the MLD snooping group information in the specified VLAN, where *vlan-id* is in the range of 1 to 4094. If you do not specify a VLAN, this command displays MLD snooping group information in all VLANs.

slot *slot-number*: Displays information about MLD snooping multicast groups on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

verbose: Displays the detailed MLD snooping group 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 mld-snooping group** to display MLD snooping group information, including both dynamic and static MLD snooping group entries.

Examples

```
# Display detailed MLD snooping group information in VLAN 2.
```

```
<Sysname> display mld-snooping group vlan 2 verbose
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
```

```
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):2.
```

```

Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port(s).
    GE1/0/1                (D) ( 00:01:30 )
IP group(s):the following ip group(s) match to one mac group.
IP group address:FF1E::101
  (::, FF1E::101):
    Attribute:      Host Port
    Host port(s):total 1 port(s).
        GE1/0/2                (D) ( 00:03:23 )
MAC group(s):
MAC group address:3333-0000-0101
Host port(s):total 1 port(s).
    GE1/0/2

```

Table 55 Command output

Field	Description
Total 1 IP Group(s).	Total number of IPv6 multicast groups.
Total 1 IP Source(s).	Total number of IPv6 multicast sources.
Total 1 MAC Group(s).	Total number of MAC multicast groups.
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port	Port flags: D —Dynamic port. S —Static port. C —Port copied from a (*, G) entry to an (S, G) entry. P —Port that IPv6 PIM snooping adds.
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R —Real egress sub-VLAN under the current entry. C —Sub-VLAN copied from a (*, G) entry to an (S, G) entry.
Router port(s)	Number of router ports.
(00:01:30)	Remaining time of the aging timer for the dynamic member port or router port.
IP group address	Address of IPv6 multicast group.
(::, FF1E::101)	(S, G) entry, double colon represents all the multicast sources.
MAC group address	Address of MAC multicast group.
Attribute	Attribute of IPv6 multicast group.
Host port(s)	Number of member ports.

display mld-snooping host

Syntax

```

display mld-snooping host vlan vlan-id group ipv6-group-address [ source ipv6-source-address ] [ slot
slot-number ] [ { begin | exclude | include } regular-expression ]

```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays information about the hosts tracked by MLD snooping in the specified VLAN, where *vlan-id* is in the range of 1 to 4094.

group *ipv6-group-address*: Displays information about the hosts tracked by MLD snooping that are in the specified IPv6 multicast group. The value of *ipv6-group-address* is in the range of FFx::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

source *ipv6-source-address*: Displays information about the hosts tracked by MLD snooping that are in the specified IPv6 multicast source.

slot *slot-number*: Displays information about the hosts tracked by MLD snooping on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device 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 mld-snooping host** to display information about the hosts tracked by MLD snooping.

Examples

```
# Display information about the hosts tracked by MLD snooping in multicast group FF1E::101 in VLAN 2.
```

```
<Sysname> display mld-snooping host vlan 2 group ff1e::101
```

```
VLAN(ID) : 2
```

```
(:, FF1E::101)
```

```
Port : GigabitEthernet1/0/1
```

Host	Uptime	Expires
1::1	00:02:20	00:00:40
2::2	00:02:21	00:00:39

```
Port : GigabitEthernet1/0/2
```

Host	Uptime	Expires
3::3	00:02:20	00:00:40

Table 56 Command output

Field	Description
(:, FF1E::101)	(S, G) entry, where :: indicates all IPv6 multicast sources
Port	Member port

Field	Description
Host	Host IPv6 address
Uptime	Host running duration
Expires	Host expiration time, where <i>timeout</i> means that the host has expired

display mld-snooping statistics

Syntax

```
display mld-snooping 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 mld-snooping statistics** to display statistics for the MLD messages learned through MLD snooping.

Examples

```
# Display statistics for the MLD messages learned through MLD snooping.
```

```
<Sysname> display mld-snooping statistics
  Received MLD general queries:0.
  Received MLDv1 specific queries:0.
  Received MLDv1 reports:0.
  Received MLD dones:0.
  Sent      MLDv1 specific queries:0.
  Received MLDv2 reports:0.
  Received MLDv2 reports with right and wrong records:0.
  Received MLDv2 specific queries:0.
  Received MLDv2 specific sg queries:0.
  Sent      MLDv2 specific queries:0.
  Sent      MLDv2 specific sg queries:0.
  Received error MLD messages:0.
```

Table 57 Command output

Field	Description
general queries	General query messages
specific queries	Multicast-address-specific query messages
reports	Report messages
done	Done messages
reports with right and wrong records	Reports that contain correct and incorrect records
specific sg queries	Multicast-address-and-source-specific queries

dot1p-priority (MLD-snooping view)

Syntax

dot1p-priority *priority-number*

undo dot1p-priority

View

MLD-snooping view

Default level

2: System level

Parameters

priority-number: Specifies an 802.1p precedence for MLD messages, in the range of 0 to 7. A higher number indicates a higher precedence.

Description

Use **dot1p-priority** to set the 802.1p precedence for MLD messages globally.

Use **undo dot1p-priority** to restore the default.

The default 802.1p precedence for MLD messages is 0.

Examples

```
# Set the 802.1p precedence for MLD messages to 3 globally.  
<Sysname> system-view  
[Sysname] mld-snooping  
[Sysname-mld-snooping] dot1p-priority 3
```

dscp (MLD-snooping view)

Syntax

dscp *dscp-value*

undo dscp

View

MLD-snooping view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value for MLD messages, in the range of 0 to 63.

Description

Use **dscp** to set the DSCP value for MLD messages.

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

The default DSCP value in MLD messages is 48.

This command applies to only the MLD messages that the local switch generates when the switch or its port acts as a member host, rather than those forwarded ones.

Examples

```
# Set the DSCP value to 63 for MLD messages.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] dscp 63
```

fast-leave (MLD-snooping view)

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

View

MLD-snooping view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command applies to all VLANs. If you specify one or multiple VLANs, the command applies to the specified VLANs only.

Description

Use **fast-leave** to enable fast-leave processing globally. With this function enabled, when the switch receives an MLD done message on a port, it directly removes that port from the forwarding table entry for the specific group.

Use **undo fast-leave** to disable fast-leave processing globally.

By default, fast-leave processing is disabled.

For the HP 5500 EI switches, this command takes effect in both MLD snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in MLD snooping-enabled VLANs.

Related commands: **mld-snooping fast-leave**.

Examples

```
# Enable fast-leave processing globally in VLAN 2.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] fast-leave vlan 2
```

group-policy (MLD-snooping view)

Syntax

```
group-policy acl6-number [ vlan vlan-list ]
undo group-policy [ vlan vlan-list ]
```

View

MLD-snooping view

Default level

2: System level

Parameters

acl6-number: Specifies a basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced IPv6 ACL rule matches the IPv6 multicast source address or addresses specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX or TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command applies to all VLANs. If you specify one or multiple VLANs, the command applies to the specified VLANs only.

Description

Use **group-policy** to configure a global IPv6 multicast group filter, namely, to control the IPv6 multicast groups that a host can join.

Use **undo group-policy** to remove the configured global IPv6 multicast group filter.

By default, no IPv6 multicast group filter is configured globally. Namely, any host can join any valid IPv6 multicast group.

If the specified IPv6 ACL does not exist or the ACL rule is null, all IPv6 multicast groups are filtered out.

You can configure different IPv6 ACL rules for each port in different VLANs. For a given VLAN, a newly configured IPv6 ACL rule overrides the existing one.

Related commands: **mld-snooping group-policy**.

Examples

```
# Apply ACL 2000 as an IPv6 multicast group filter so that hosts in VLAN 2 can join FF03::101 only.
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff03::101 16
```

```
[Sysname-acl6-basic-2000] quit
[Sysname] mld-snooping
[Sysname-mld-snooping] group-policy 2000 vlan 2
```

host-aging-time (MLD-snooping view)

Syntax

host-aging-time *interval*

undo host-aging-time

View

MLD-snooping view

Default level

2: System level

Parameters

interval: Specifies an aging timer for dynamic member ports in seconds. The value range is 200 to 1000.

Description

Use **host-aging-time** to set the aging timer for dynamic member ports globally.

Use **undo host-aging-time** to restore the default.

By default, the aging timer of a dynamic member port is 260 seconds.

This command takes effect only in MLD snooping-enabled VLANs.

Related commands: **mld-snooping host-aging-time**.

Examples

Set the aging timer for dynamic member ports to 300 seconds globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] host-aging-time 300
```

host-tracking (MLD-snooping view)

Syntax

host-tracking

undo host-tracking

View

MLD-snooping view

Default level

2: System level

Parameters

None

Description

Use **host-tracking** to enable the MLD snooping host tracking function globally.

Use **undo host-tracking** to disable the MLD snooping host tracking function globally.

By default, this function is disabled.

This command takes effect only in MLD snooping-enabled VLANs.

Related commands: **display mld-snooping host** and **mld-snooping host-tracking**.

Examples

```
# Enable the MLD snooping host tracking function globally.
```

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] host-tracking
```

last-listener-query-interval (MLD-snooping view)

Syntax

last-listener-query-interval *interval*

undo last-listener-query-interval

View

MLD-snooping view

Default level

2: System level

Parameters

interval: Sets the MLD last-listener query interval in seconds. The value range is 1 to 5.

Description

Use **last-listener-query-interval** to configure the MLD last-listener query interval globally.

Use **undo last-listener-query-interval** to restore the default.

By default, the MLD last-listener query interval is 1 second.

The MLD last-listener query interval determines the interval for sending MLD multicast-address-specific queries and the maximum response delay for MLD multicast-address-specific queries.

This command takes effect only in MLD snooping-enabled VLANs.

Related commands: **mld-snooping last-listener-query-interval**.

Examples

```
# Set the MLD last listener query interval to 3 seconds globally.
```

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] last-listener-query-interval 3
```

max-response-time (MLD-snooping view)

Syntax

max-response-time *interval*

undo max-response-time

View

MLD-snooping view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for MLD general queries in seconds. The value ranges from 1 to 25.

Description

Use **max-response-time** to configure the maximum response time for MLD general queries globally.

Use **undo max-response-time** to restore the default.

By default, the maximum response delay for MLD general queries is 10 seconds.

This command takes effect only in MLD snooping-enabled VLANs.

Related commands: **mld-snooping max-response-time** and **mld-snooping query-interval**.

Examples

```
# Set the maximum response delay for MLD general queries to 5 seconds globally.  
<Sysname> system-view  
[Sysname] mld-snooping  
[Sysname-mld-snooping] max-response-time 5
```

mld-snooping

Syntax

mld-snooping

undo mld-snooping

View

System view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping** to enable MLD snooping globally and enter MLD-snooping view.

Use **undo mld-snooping** to disable MLD snooping globally.

By default, MLD snooping is disabled.

Related commands: **mld-snooping enable**.

Examples

```
# Enable MLD snooping globally and enter MLD-snooping view.  
<Sysname> system-view  
[Sysname] mld-snooping
```

[Sysname-mld-snooping]

mld-snooping access-policy

Syntax

```
mld-snooping access-policy acl6-number  
undo mld-snooping access-policy { acl6-number | all }
```

View

User profile view

Default level

2: System level

Parameters

acl6-number: Specifies a basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL matches the multicast source address or addresses specified in MLDv2 reports, rather than the source address in the IP packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX and TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

all: Specifies all IPv6 ACLs.

Description

Use **mld-snooping access-policy** to configure an IPv6 multicast user control policy.

Use **undo mld-snooping access-policy** to remove the configuration.

By default, no IPv6 user control policy is configured. Namely, a user can join any valid IPv6 multicast group.

You can use this command repeatedly to configure multiple IPv6 multicast user control policies.

Examples

Create and enable a user profile named **abc**, and configure the user profile so that users in this user profile can join FF03::101 only.

```
<Sysname> system-view  
[Sysname] acl ipv6 number 2001  
[Sysname-acl6-basic-2001] rule permit source ff03::101 16  
[Sysname-acl6-basic-2001] quit  
[Sysname] user-profile abc  
[Sysname-user-profile-abc] mld-snooping access-policy 2001  
[Sysname-user-profile-abc] quit  
[Sysname] user-profile abc enable
```

mld-snooping done source-ip

Syntax

```
mld-snooping done source-ip { ipv6-address | current-interface }  
undo mld-snooping done source-ip
```


View

VLAN view

Default level

2: System level

Parameters

ipv6-address: Specifies a source IPv6 address for the MLD done messages that the MLD snooping proxy sends, which can be any legal IPv6 link-local address.

current-interface: Specifies the IPv6 link-local address of the current VLAN interface as the source address of MLD done messages that the MLD snooping proxy sends. If no IPv6 address has been assigned to the current interface, the default IPv6 address FE80::02FF:FFFF:FE00:0001 is used.

Description

Use **mld-snooping done source-ip** to configure the source IPv6 address of the MLD done messages that the MLD snooping proxy sends.

Use **undo mld-snooping done source-ip** to restore the default.

By default, the source IPv6 address of the MLD done messages that the MLD snooping proxy sends is FE80::02FF:FFFF:FE00:0001.

Before you configure this command in a VLAN, enable MLD snooping for the VLAN.

The source IPv6 address configured in the **mld-snooping done source-ip** command also applies when the simulated host sends MLD done messages.

Related commands: **mld-snooping enable**.

Examples

```
# Enable MLD snooping in VLAN 2 and configure the source IPv6 address of MLD done messages that the MLD snooping proxy sends in VLAN 2 to FE80:0:0:1::1.
```

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping done source-ip fe80:0:0:1::1
```

mld-snooping dot1p-priority

Syntax

mld-snooping dot1p-priority *priority-number*

undo mld-snooping dot1p-priority

View

VLAN view

Default level

2: System level

Parameters

priority-number: Specifies an 802.1p precedence for MLD messages, in the range of 0 to 7. A higher number indicates a higher precedence.

Description

Use **mld-snooping dot1p-priority** to set the 802.1p precedence for the MLD messages in a VLAN.

Use **undo mld-snooping dot1p-priority** to restore the default.

The default 802.1p precedence for the MLD messages in a VLAN is 0.

Before you configure this command in a VLAN, enable MLD snooping for the VLAN.

Related commands: **mld-snooping enable**.

Examples

Enable MLD snooping in VLAN 2 and set the 802.1p precedence for the MLD messages in the VLAN to 3.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping dot1p-priority 3
```

mld-snooping drop-unknown

Syntax

mld-snooping drop-unknown

undo mld-snooping drop-unknown

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping drop-unknown** to enable dropping unknown IPv6 multicast data for a VLAN.

Use **undo mld-snooping drop-unknown** to disable dropping unknown IPv6 multicast data for a VLAN.

By default, this function is disabled, and unknown IPv6 multicast data is flooded in the VLAN.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **mld-snooping enable**.

Examples

Enable MLD snooping and the function for dropping unknown IPv6 multicast data in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
```

```
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping drop-unknown
```

mld-snooping enable

Syntax

```
mld-snooping enable
undo mld-snooping enable
```

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping enable** to enable MLD snooping for a VLAN.

Use **undo mld-snooping enable** to disable MLD snooping for a VLAN.

By default, MLD snooping is disabled in a VLAN.

MLD snooping must be enabled globally before it can be enabled in a VLAN

Related commands: **mld-snooping**.

Examples

```
# Enable MLD snooping in VLAN 2.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
```

mld-snooping fast-leave

Syntax

```
mld-snooping fast-leave [ vlan vlan-list ]
undo mld-snooping fast-leave [ vlan vlan-list ]
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **mld-snooping fast-leave** to enable fast-leave processing on the current port or group of ports. With this function enabled, when the switch receives an MLD done message on a port, it directly removes that port from the forwarding table entry for the specific group.

Use **undo mld-snooping fast-leave** to disable fast-leave processing on the current port or group of ports. By default, fast-leave processing is disabled.

For the HP 5500 EI switches, this command takes effect in both MLD snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in MLD snooping-enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **fast-leave**.

Examples

```
# Enable fast-leave processing on GigabitEthernet 1/0/1 in VLAN 2.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping fast-leave vlan 2
```

mld-snooping general-query source-ip

Syntax

```
mld-snooping general-query source-ip { ipv6-address | current-interface }
undo mld-snooping general-query source-ip
```

View

VLAN view

Default level

2: System level

Parameters

ipv6-address: Specifies the source IPv6 address of MLD general queries, which can be any legal IPv6 link-local address.

current-interface: Sets the source IPv6 link-local address of MLD general queries to the IPv6 address of the current VLAN interface. If the current VLAN interface does not have an IPv6 address, the default IPv6 address FE80::02FF:FFFF:FE00:0001 is used as the source IPv6 address of MLD general queries.

Description

Use **mld-snooping general-query source-ip** to configure the source IPv6 address of MLD general queries.

Use **undo mld-snooping general-query source-ip** to restore the default.

By default, the source IPv6 address of MLD general queries is FE80::02FF:FFFF:FE00:0001.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **mld-snooping enable**.

Examples

In VLAN 2, enable MLD snooping and specify FE80:0:0:1::1 as the source IPv6 address of MLD general queries.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping general-query source-ip fe80:0:0:1::1
```

mld-snooping group-limit

Syntax

mld-snooping group-limit *limit* [**vlan** *vlan-list*]

undo mld-snooping group-limit [**vlan** *vlan-list*]

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

limit: Specifies the maximum number of IPv6 multicast groups that a port can join. The value ranges from 1 to 1000.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **mld-snooping group-limit** to configure the maximum number of IPv6 multicast groups that a port can join.

Use **undo mld-snooping group-limit** to restore the default.

By default, the upper limit is 1000.

For the HP 5500 EI switches, you can also use the **mld group-limit** command to limit the number of IPv6 multicast groups that an interface can join. However, if you configure the limit both in a VLAN and on a VLAN interface of this VLAN by using these two commands, inconsistencies might exist between Layer 2 and Layer 3 table entries. Therefore, HP recommends you to configure the limit only on the VLAN interface.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **mld group-limit**.

Examples

```
# Configure to allow up to 10 IPv6 multicast groups that GigabitEthernet 1/0/1 in VLAN 2 can join.
```

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

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mld-snooping group-limit 10 vlan 2
```

mld-snooping group-policy

Syntax

```
mld-snooping group-policy acl6-number [ vlan vlan-list ]
```

```
undo mld-snooping group-policy [ vlan vlan-list ]
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

acl6-number: Specifies a basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The IPv6 source address or address range specified in the advanced IPv6 ACL rule is the IPv6 multicast source addresses specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX or TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **mld-snooping group-policy** to configure an IPv6 multicast group filter on the current ports, namely, to control the multicast groups that the hosts on the port can join.

Use **undo mld-snooping group-policy** to remove the configured IPv6 multicast group filter on the current port or ports.

By default, no IPv6 multicast group filter is configured on a port. Namely, a host can join any valid IPv6 multicast group.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

If the specified ACL does not exist or the ACL rule is null, all IPv6 multicast groups are filtered out.

You can configure different IPv6 ACL rules for each port in different VLANs. For a given VLAN, a newly configured IPv6 ACL rule overrides the existing one.

Related commands: **group-policy**.

Examples

Apply ACL 2000 as an IPv6 multicast group filter so that hosts on GigabitEthernet 1/0/1 in VLAN 2 can join FF03::101 only.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff03::101 16
[Sysname-acl6-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping group-policy 2000 vlan 2
```

mld-snooping host-aging-time

Syntax

mld-snooping host-aging-time *interval*

undo mld-snooping host-aging-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an aging timer for dynamic member ports in seconds. The value range is 200 to 1000.

Description

Use **mld-snooping host-aging-time** to set the aging timer for the dynamic member ports for a VLAN.

Use **undo mld-snooping host-aging-time** to restore the default.

By default, the aging timer of a dynamic member port is 260 seconds.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **display mld-snooping host, host-aging-time** and **mld-snooping enable**.

Examples

```
# Enable MLD snooping and set the aging timer for dynamic member ports to 300 seconds in VLAN 2.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping host-aging-time 300
```

mld-snooping host-join

Syntax

```
mld-snooping host-join ipv6-group-address [ source-ip ipv6-source-address ] vlan vlan-id
undo mld-snooping host-join ipv6-group-address [ source-ip ipv6-source-address ] vlan vlan-id
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

ipv6-group-address: Specifies the address of the IPv6 multicast group that the simulated host will join. The value ranges from FFXy::/16 (excluding FFX0::/16, FFX1::/16, FFX2::/16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive.

ipv6-source-address: Specifies the address of the IPv6 multicast source that the simulated host will join.

vlan *vlan-id*: Specifies a VLAN that comprises the port or ports, where *vlan-id* is in the range of 1 to 4094.

Description

Use **mld-snooping host-join** to enable simulated joining on a port. Namely, you configure a port as a simulated member host for the specified IPv6 multicast group or source and group.

Use **undo mld-snooping host-join** to remove the simulated member host from the specified IPv6 multicast group or source and group.

By default, this function is disabled.

For the HP 5500 EI switches, this command takes effect in both MLD snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces. The version of MLD on the simulated member host is consistent with the version of MLD snooping that runs in the VLAN or the version of MLD that runs on the VLAN interface.

For the HP 5500 SI switches, this command takes effect in MLD snooping-enabled VLANs. The version of MLD on the simulated member host is consistent with the version of MLD snooping that runs in the VLAN.

The **source-ip** *ipv6-source-address* option in the command is meaningful only for MLDv2 snooping. If MLDv1 snooping is running, the **source-ip** *ipv6-source-address* option does not take effect although you can include **source-ip** *ipv6-source-address* in the command.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN. In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Examples

```
# Configure GigabitEthernet 1/0/1 in VLAN 2 to join (2002::22, FF3E::101) as a simulated host.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping host-join ff3e::101 source-ip 2002::22 vlan
2
```

mld-snooping host-tracking

Syntax

```
mld-snooping host-tracking
undo mld-snooping host-tracking
```

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping host-tracking** to enable the MLD snooping host tracking function in a VLAN.

Use **undo mld-snooping host-tracking** to disable the MLD snooping host tracking function in a VLAN.

By default, this function is disabled.

Before you configure this command, enable MLD snooping for the VLAN first.

Related commands: **host-tracking**, and **mld-snooping enable**.

Examples

```
# Enable MLD snooping and the MLD snooping host tracking function for VLAN 2.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping host-tracking
```

mld-snooping last-listener-query-interval

Syntax

```
mld-snooping last-listener-query-interval interval
```

undo mld-snooping last-listener-query-interval

View

VLAN view

Default level

2: System level

Parameters

interval: Sets the MLD last-listener query interval in seconds. The value ranges from 1 to 5.

Description

Use **mld-snooping last-listener-query-interval** to set the MLD last-listener query interval for a VLAN.

Use **undo mld-snooping last-listener-query-interval** to restore the default.

By default, the MLD last listener query interval is 1 second.

The MLD last-listener query interval determines the interval for sending MLD multicast-address-specific queries and the maximum response delay for MLD multicast-address-specific queries in a VLAN.

You must enable MLD snooping for a VLAN before you configure this command for the VLAN.

Related commands: **last-listener-query-interval** and **mld-snooping enable**.

Examples

```
# Enable MLD snooping and set the MLD last listener query interval to 3 seconds in VLAN 2.
```

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping last-listener-query-interval 3
```

mld-snooping max-response-time

Syntax

```
mld-snooping max-response-time interval
```

```
undo mld-snooping max-response-time
```

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for MLD general queries in seconds. The value ranges from 1 to 25.

Description

Use **mld-snooping max-response-time** to configure the maximum response delay for MLD general queries in the VLAN.

Use **undo mld-snooping max-response-time** to restore the default.

By default, the maximum response delay for MLD general queries is 10 seconds.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **max-response-time**, **mld-snooping enable**, and **mld-snooping query-interval**.

Examples

```
# Enable MLD snooping and set the maximum response delay for MLD general queries to 5 seconds in VLAN 2.
```

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping max-response-time 5
```

mld-snooping overflow-replace

Syntax

```
mld-snooping overflow-replace [ vlan vlan-list ]
```

```
undo mld-snooping overflow-replace [ vlan vlan-list ]
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **mld-snooping overflow-replace** to enable the IPv6 multicast group replacement function on the current port.

Use **undo mld-snooping overflow-replace** to disable the IPv6 multicast group replacement function.

By default, the IPv6 multicast group replacement function is disabled.

For the HP 5500 EI switches, this command takes effect in both MLD snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in MLD snooping-enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **overflow-replace**.

Examples

```
# Enable the IPv6 multicast group replacement function on GigabitEthernet 1/0/1 in VLAN 2.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping overflow-replace vlan 2
```

mld-snooping proxying enable

Syntax

```
mld-snooping proxying enable
undo mld-snooping proxying enable
```

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping proxying enable** to enable the MLD snooping proxying function in a VLAN.

Use **undo mld-snooping proxying enable** to disable the MLD snooping proxying function in a VLAN.

By default, MLD snooping proxying is disabled in all VLANs.

Before you configure this command in a VLAN, enable MLD snooping for the VLAN.

Related commands: **mld-snooping enable**.

Examples

```
# Enable MLD snooping and then MLD snooping proxying in VLAN 2.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping proxying enable
```

mld-snooping querier

Syntax

```
mld-snooping querier
undo mld-snooping querier
```

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping querier** to enable the MLD snooping querier function.

Use **undo mld-snooping querier** to disable the MLD snooping querier function.

By default, the MLD snooping querier function is disabled.

This command takes effect only if MLD snooping is enabled for the VLAN, and it does not take effect in a sub-VLAN of an IPv6 multicast VLAN.

Related commands: **mld-snooping enable** and **subvlan**.

Examples

```
# Enable MLD snooping and the MLD snooping querier function in VLAN 2.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping querier
```

mld-snooping query-interval

Syntax

```
mld-snooping query-interval interval
undo mld-snooping query-interval
```

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an MLD query interval in seconds, namely, the length of time that the device waits between sending MLD general queries. The value ranges from 2 to 300.

Description

Use **mld-snooping query-interval** to configure the MLD query interval.

Use **undo mld-snooping query-interval** to restore the default.

By default, the MLD query interval is 125 seconds.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **max-response-time**, **mld-snooping enable**, **mld-snooping max-response-time**, and **mld-snooping querier**.

Examples

```
# Enable MLD snooping and set the MLD query interval to 20 seconds in VLAN 2.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping query-interval 20
```

mld-snooping report source-ip

Syntax

```
mld-snooping report source-ip { ipv6-address | current-interface }
undo mld-snooping report source-ip
```

View

VLAN view

Default level

2: System level

Parameters

ipv6-address: Specifies a source IPv6 address for the MLD reports that the MLD snooping proxy sends, which can be any legal IPv6 link-local address.

current-interface: Specifies the IPv6 link-local address of the current VLAN interface as the source address of MLD reports that the MLD snooping proxy sends. If no IPv6 address has been assigned to the current interface, the default IPv6 address FE80::02FF:FFFF:FE00:0001 is used.

Description

Use **mld-snooping report source-ip** to configure the source IPv6 address of the MLD reports that the MLD snooping proxy sends.

Use **undo mld-snooping report source-ip** to restore the default.

By default, the source IPv6 address of the MLD reports that the MLD snooping proxy sends is FE80::02FF:FFFF:FE00:0001.

Before you configure this command in a VLAN, enable MLD snooping for the VLAN.

The source IPv6 address configured in the **mld-snooping report source-ip** command also applies when the simulated host sends MLD reports.

Related commands: **mld-snooping enable**.

Examples

```
# Enable MLD snooping in VLAN 2 and configure the source IPv6 address of MLD reports that the MLD
snooping proxy sends in VLAN 2 to FE80:0:0:1::1.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
```

```
[Sysname-vlan2] mld-snooping report source-ip fe80:0:0:1::1
```

mld-snooping router-aging-time

Syntax

```
mld-snooping router-aging-time interval
```

```
undo mld-snooping router-aging-time
```

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an aging timer for dynamic router ports, in seconds. The value ranges from 1 to 1,000.

Description

Use **mld-snooping router-aging-time** to set the aging timer for the dynamic router ports for a VLAN.

Use **undo mld-snooping router-aging-time** to restore the default.

By default, the aging timer of a dynamic router port is 260 seconds.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **mld-snooping enable** and **router-aging-time**.

Examples

```
# Enable MLD snooping and set the aging timer for the dynamic router ports to 100 seconds in VLAN 2.
```

```
<Sysname> system-view  
[Sysname] mld-snooping  
[Sysname-mld-snooping] quit  
[Sysname] vlan 2  
[Sysname-vlan2] mld-snooping enable  
[Sysname-vlan2] mld-snooping router-aging-time 100
```

mld-snooping router-port-deny

Syntax

```
mld-snooping router-port-deny [ vlan vlan-list ]
```

```
undo mld-snooping router-port-deny [ vlan vlan-list ]
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to*

end-vlan-id, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **mld-snooping router-port-deny** to disable a port from becoming a dynamic router port.

Use **undo mld-snooping router-port-deny** to restore the default.

By default, a port can become a dynamic router port.

For the HP 5500 EI switches, this command takes effect in both MLD snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

For the HP 5500 EI switches, this command takes effect in MLD snooping-enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Examples

```
# Disable GigabitEthernet 1/0/1 from becoming a dynamic router port in VLAN 2.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping router-port-deny vlan 2
```

mld-snooping source-deny

Syntax

mld-snooping source-deny

undo mld-snooping source-deny

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping source-deny** to enable IPv6 multicast source port filtering.

Use **undo mld-snooping source-deny** to disable IPv6 multicast source port filtering.

By default, IPv6 multicast source port filtering is disabled.

For the HP 5500 EI switches, this command takes effect in both MLD snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in MLD snooping-enabled VLANs.

Examples

```
# Enable source port filtering for IPv6 multicast data on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping source-deny
```

mld-snooping special-query source-ip

Syntax

```
mld-snooping special-query source-ip { ipv6-address | current-interface }
undo mld-snooping special-query source-ip
```

View

VLAN view

Default level

2: System level

Parameters

ipv6-address: Specifies an IPv6 link-local address as the source IPv6 address of MLD multicast-address-specific queries.

current-interface: Specifies the source IPv6 link-local address of the VLAN interface of the current VLAN as the source IPv6 address of MLD multicast-address-specific queries. If the current VLAN interface does not have an IPv6 address, the default IPv6 address FE80::02FF:FFFF:FE00:0001 is used as the source IPv6 address of MLD multicast-address-specific queries.

Description

Use **mld-snooping special-query source-ip** to configure the source IPv6 address of MLD multicast-address-specific queries.

Use **undo mld-snooping special-query source-ip** to restore the default.

By default, the source IPv6 address of MLD multicast-address-specific queries is FE80::02FF:FFFF:FE00:0001.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **mld-snooping enable**.

Examples

```
# In VLAN 2, enable MLD snooping and specify FE80:0:0:1::1 as the source IPv6 address of MLD
multicast-address-specific queries.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping special-query source-ip fe80:0:0:1::1
```

mld-snooping static-group

Syntax

```
mld-snooping static-group ipv6-group-address [ source-ip ipv6-source-address ] vlan vlan-id  
undo mld-snooping static-group ipv6-group-address [ source-ip ipv6-source-address ] vlan vlan-id
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

ipv6-group-address: Specifies the address of the IPv6 multicast group that the port will join as a static member port. The value ranges from FFxy::/16—excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::, where x and y represent any hexadecimal number between 0 and F, inclusive.

ipv6-source-address: Specifies the address of the IPv6 multicast source that the port will join as a static member port.

vlan *vlan-id*: Specifies the VLAN that comprises the Ethernet ports, where *vlan-id* is in the range of 1 to 4094.

Description

Use **mld-snooping static-group** to configure the static IPv6 (*, G) or (S, G) joining function, that is, to configure the port as a static member port of an IPv6 multicast group or source and group.

Use **undo mld-snooping static-group** to restore the default.

By default, no ports are static member ports.

The **source-ip** *ipv6-source-address* option in the command is meaningful only for MLDv2 snooping. If MLDv1 snooping is running, the **source-ip** *ipv6-source-address* option does not take effect although you can include **source-ip** *ipv6-source-address* in the command.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN. In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Examples

```
# Configure GigabitEthernet 1/0/1 in VLAN 2 as a static member port for (2002::22, FF3E::101).  
<Sysname> system-view  
[Sysname] mld-snooping  
[Sysname-mld-snooping] quit  
[Sysname] vlan 2  
[Sysname-vlan2] mld-snooping enable  
[Sysname-vlan2] mld-snooping version 2  
[Sysname-vlan2] quit  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] mld-snooping static-group ff3e::101 source-ip 2002::22  
vlan 2
```

mld-snooping static-router-port

Syntax

```
mld-snooping static-router-port vlan vlan-id  
undo mld-snooping static-router-port vlan vlan-id
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-id*: Specifies a VLAN by its ID, in the range of 1 to 4094.

Description

Use **mld-snooping static-router-port** to configure the current port as a static router port.

Use **undo mld-snooping static-router-port** to restore the default.

By default, no ports are static router ports.

For the HP 5500 EI switches, this command takes effect in both MLD snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in MLD snooping-enabled VLANs.

This command does not take effect in a sub-VLAN of an IPv6 multicast VLAN.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN. In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Related commands: **subvlan**.

Examples

```
# Enable the static router port function on GigabitEthernet 1/0/1 in VLAN 2.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] mld-snooping static-router-port vlan 2
```

mld-snooping version

Syntax

```
mld-snooping version version-number  
undo mld-snooping version
```

View

VLAN view

Default level

2: System level

Parameters

version-number: Specifies an MLD snooping version. The value can be 1 or 2.

Description

Use **mld-snooping version** to configure the MLD snooping version.

Use **undo mld-snooping version** to restore the default.

By default, the MLDv1 snooping is used.

This command can take effect only if MLD snooping is enabled for the VLAN, and it does not take effect in a sub-VLAN of an IPv6 multicast VLAN.

Related commands: **mld-snooping enable** and **subvlan**.

Examples

```
# Enable MLD snooping in VLAN 2, and specify MLDv2 snooping.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
```

overflow-replace (MLD-snooping view)

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

View

MLD-snooping view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command applies to all VLANs. If you specify one or multiple VLANs, the command applies to the specified VLANs only.

Description

Use **overflow-replace** to enable the IPv6 multicast group replacement function globally.

Use **undo overflow-replace** to disable the IPv6 multicast group replacement function globally.

By default, the IPv6 multicast group replacement function is disabled globally.

For the HP 5500 EI switches, this command takes effect in both MLD snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in MLD snooping-enabled VLANs.

Related commands: **mld-snooping overflow-replace**.

Examples

```
# Enable the IPv6 multicast group replacement function globally in VLAN 2.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] overflow-replace vlan 2
```

report-aggregation (MLD-snooping view)

Syntax

```
report-aggregation
undo report-aggregation
```

View

MLD-snooping view

Default level

2: System level

Parameters

None

Description

Use **report-aggregation** to enable MLD report suppression.

Use **undo report-aggregation** to disable MLD report suppression.

By default, MLD report suppression is enabled.

For the HP 5500 EI switches, this command takes effect in both MLD snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in MLD snooping-enabled VLANs.

Examples

```
# Disable MLD report suppression.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] undo report-aggregation
```

reset mld-snooping group

Syntax

```
reset mld-snooping group { ipv6-group-address | all } [ vlan vlan-id ]
```

View

User view

Default level

2: System level

Parameters

ipv6-group-address: Specifies an IPv6 multicast group. The value range of *ipv6-group-address* is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive.

all: Specifies all IPv6 multicast groups.

vlan *vlan-id*: Specifies a VLAN. The value range of *vlan-id* is 1 to 4094.

Description

Use **reset mld-snooping group** to remove the dynamic group entries of a specified MLD snooping group or all MLD snooping groups.

This command takes effect only in MLD snooping-enabled VLANs.

This command cannot remove the static group entries of MLD snooping groups.

Examples

```
# Remove the dynamic group entries of all MLD snooping groups.
```

```
<Sysname> reset mld-snooping group all
```

reset mld-snooping statistics

Syntax

```
reset mld-snooping statistics
```

View

User view

Default level

2: System level

Parameters

None

Description

Use **reset mld-snooping statistics** to clear statistics for the MLD messages learned by MLD snooping.

Examples

```
# Clear statistics for the MLD messages learned by MLD snooping.
```

```
<Sysname> reset mld-snooping statistics
```

router-aging-time (MLD-snooping view)

Syntax

```
router-aging-time interval
```

```
undo router-aging-time
```

View

MLD-snooping view

Default level

2: System level

Parameters

interval: Specifies an aging timer in seconds for dynamic router ports. The value ranges from 1 to 1,000.

Description

Use **router-aging-time** to set the aging timer for dynamic router ports globally.

Use **undo router-aging-time** to restore the default.

By default, the aging time of a dynamic router port is 260 seconds.

This command takes effect only in MLD snooping-enabled VLANs.

Related commands: **mld-snooping router-aging-time**.

Examples

Set the aging timer for dynamic router ports to 100 seconds globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] router-aging-time 100
```

source-deny (MLD-snooping view)

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

View

MLD-snooping view

Default level

2: System level

Parameters

interface-list: Specifies a list of ports. You can specify multiple ports or port ranges by providing the this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }, where *interface-type* is the port type and *interface-number* is the port number.

Description

Use **source-deny** to enable IPv6 multicast source port filtering, namely, to filter out all the received IPv6 multicast packets.

Use **undo source-deny** to disable IPv6 multicast source port filtering.

By default, IPv6 multicast source port filtering is disabled.

For the HP 5500 EI switches, this command takes effect in both MLD snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

For the HP 5500 SI switches, this command takes effect in MLD snooping-enabled VLANs.

Examples

Enable source port filtering for IPv6 multicast data on interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Sysname> system-view
[Sysname] mld-snooping
```

```
[Sysname-mld-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```


IPv6 PIM snooping configuration commands

display pim-snooping ipv6 neighbor

Syntax

```
display pim-snooping ipv6 neighbor [ vlan vlan-id ] [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the IPv6 PIM snooping neighbor information of the specified VLAN. The *vlan-id* argument is in the range of 1 to 4094. If no VLAN is specified, this command displays the IPv6 PIM snooping neighbor information in all VLANs.

slot *slot-number*: Displays the IPv6 PIM snooping neighbor information on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device 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 pim-snooping ipv6 neighbor** to display IPv6 PIM snooping neighbor information.

Examples

```
# Display the IPv6 PIM snooping neighbor information of VLAN 2.
```

```
<Sysname> display pim-snooping ipv6 neighbor vlan 2
```

```
Total number of neighbors: 2
```

```
VLAN ID: 2
```

```
Total number of neighbors: 2
```

Neighbor	Port	Expires	Option Flags
FE80::6401:101	GE1/0/1	02:02:23	LAN Prune Delay(T)
FE80::C801:101	GE1/0/2	03:00:05	LAN Prune Delay

Table 58 Command output

Field	Description
Total number of neighbors	Total number of IPv6 PIM snooping neighbors.
Neighbor	IP address of the IPv6 PIM snooping neighbor.
Port	Name of the port that connects to the IPv6 PIM snooping neighbor.
Expires	Remaining time before the IPv6 PIM snooping neighbor expires. <i>Never</i> means the IPv6 PIM snooping neighbor never expires.
Option Flags	<p>Possible values includes the following items:</p> <ul style="list-style-type: none"> • LAN Prune Delay—Indicates that the IPv6 PIM hello messages received from the neighbor carry the LAN_Prune_Delay option. • LAN Prune Delay(T)—Indicates that the IPv6 PIM hello messages received from the neighbor carry the LAN_Prune_Delay option, and the join suppression function has been disabled.

display pim-snooping ipv6 routing-table

Syntax

```
display pim-snooping ipv6 routing-table [ vlan vlan-id ] [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the IPv6 PIM snooping routing entries of the specified VLAN. The *vlan-id* argument is in the range of 1 to 4094.

slot *slot-number*: Displays the IPv6 PIM snooping routing entries on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device 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 pim-snooping ipv6 routing-table** to display the IPv6 PIM snooping routing table.

Examples

```
# Display the IPv6 PIM snooping routing entries of VLAN 2.
<Sysname> display pim-snooping ipv6 routing-table vlan 2 slot 1
```

```

Total 1 entry(ies)
FSM Flag: NI-no info, J-join, PP-prune pending

VLAN ID: 2
  Total 2 entry(ies)
  (2000::1, FF1E::1)
    Upstream neighbor: FE80::101
    Upstream port: GE1/0/1
    Total number of downstream ports: 2
      1: GE1/0/3
        Expires: 00:03:01, FSM: J
    Upstream neighbor: FE80::102
    Upstream port: GE1/0/2
    Total number of downstream ports: 1
      1: GE1/0/4
        Expires: 00:01:05, FSM: J

```

Table 59 Command output

Field	Description
Total 1 entry(ies)	Total number of (S, G) entries and (*, G) entries in the IPv6 PIM snooping routing table.
FSM Flag: NI-no info, J-join, PP-prune pending	State machine flag of the downstream port. Possible values include: <ul style="list-style-type: none"> • NI—Initial state. • J—Join. • PP—Prune pending.
(2000::1, FF1E::1)	(S, G) entry.
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry.
Upstream port	Upstream port of the (S, G) entry or (*, G) entry).
Expires	Expiration time of the downstream port.
FSM	State machine of the downstream port.

display pim-snooping ipv6 statistics

Syntax

```
display pim-snooping ipv6 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 pim-snooping ipv6 statistics** to display statistics for the IPv6 PIM messages learned by IPv6 PIM snooping.

Examples

Display statistics for the IPv6 PIM messages learned by IPv6 PIM snooping.

```
<Sysname> display pim-snooping ipv6 statistics
Received IPv6 PIM IPv6 hello: 100
Received IPv6 PIM IPv6 join/prune: 100
Received IPv6 PIM IPv6 error: 0
Received IPv6 PIM IPv6 messages in total: 200
```

Table 60 Command output

Field	Description
Received IPv6 PIM IPv6 hello	Number of received IPv6 PIM hello messages
Received IPv6 PIM IPv6 join/prune	Number of received IPv6 PIM join/prune messages
Received IPv6 PIM IPv6 error	Number of received IPv6 PIM messages with errors
Received IPv6 PIM IPv6 messages in total	Total number of received IPv6 PIM messages

pim-snooping ipv6 enable

Syntax

pim-snooping ipv6 enable

undo pim-snooping ipv6 enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **pim-snooping ipv6 enable** to enable IPv6 PIM snooping in a VLAN.

Use **undo pim-snooping ipv6 enable** to disable IPv6 PIM snooping in a VLAN.

By default, IPv6 PIM snooping is disabled.

Before you enable IPv6 PIM snooping in a VLAN, be sure to enable MLD snooping globally and specially in the VLAN.

IPv6 PIM snooping does not work in a sub-VLAN of a multicast VLAN.

Related commands: **mld-snooping enable**.

Examples

```
# Enable MLD snooping globally, and enable MLD snooping and IPv6 PIM snooping in VLAN 2.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] pim-snooping ipv6 enable
```

reset pim-snooping ipv6 statistics

Syntax

reset pim-snooping ipv6 statistics

View

User view

Default level

2: System level

Parameters

None

Description

Use **reset pim-snooping ipv6 statistics** to clear statistics for the IPv6 PIM messages learned by IPv6 PIM snooping.

Examples

```
# Clear statistics for the IPv6 PIM messages learned by IPv6 PIM snooping.
<Sysname> reset pim-snooping ipv6 statistics
```

IPv6 multicast VLAN configuration commands

display multicast-vlan ipv6

Syntax

```
display multicast-vlan ipv6 [ vlan-id ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan-id: Specifies an IPv6 multicast VLAN, in the range of 1 to 4094. If this argument is not specified, this command displays information about all IPv6 multicast VLANs.

|: 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 multicast-vlan ipv6** to display information about the specified IPv6 multicast VLAN or all IPv6 multicast VLANs.

Examples

```
# Display information about all IPv6 multicast VLANs.
```

```
<Sysname> display multicast-vlan ipv6
Total 2 IPv6 multicast-vlan(s)
```

```
IPv6 Multicast vlan 100
  subvlan list:
    vlan 2  4-6
  port list:
    no port
```

```
IPv6 Multicast vlan 200
  subvlan list:
    no subvlan
  port list:
    GE1/0/1          GE1/0/2
```

Table 61 Command output

Field	Description
subvlan list	List of sub-VLANs of the IPv6 multicast VLAN
port list	Port list of the IPv6 multicast VLAN

multicast-vlan ipv6

Syntax

```
multicast-vlan ipv6 vlan-id  
undo multicast-vlan ipv6 { all | vlan-id }
```

View

System view

Default level

2: System level

Parameters

vlan-id: Specifies a VLAN by its ID, in the range of 1 to 4094.

all: Specifies all IPv6 multicast VLANs.

Description

Use **multicast-vlan ipv6** to configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.

Use **undo multicast-vlan ipv6** to remove the specified VLAN as an IPv6 multicast VLAN.

No VLAN is an IPv6 multicast VLAN by default.

The specified VLAN to be configured as an IPv6 multicast VLAN must exist.

For the HP 5500 EI switches, the IPv6 multicast VLAN feature cannot be enabled on a device with IPv6 multicast routing enabled.

For a sub-VLAN-based IPv6 multicast VLAN, you must enable MLD snooping only in the IPv6 multicast VLAN. For a port-based IPv6 multicast VLAN, you must enable MLD snooping in both the IPv6 multicast VLAN and all the user VLANs.

Related commands: **mld-snooping enable** and **multicast ipv6 routing-enable**.

Examples

Enable MLD snooping in VLAN 100. Configure it as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.

```
<Sysname> system-view  
[Sysname] mld-snooping  
[Sysname-mld-snooping] quit  
[Sysname] vlan 100  
[Sysname-vlan100] mld-snooping enable  
[Sysname-vlan100] quit  
[Sysname] multicast-vlan ipv6 100  
[Sysname-ipv6-mvlan-100]
```

port (IPv6 multicast VLAN view)

Syntax

```
port interface-list  
undo port { all | interface-list }
```

View

IPv6 multicast VLAN view

Default level

2: System level

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number* to *interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

all: Specifies all the ports in the current IPv6 multicast VLAN.

Description

Use **port** to assign the specified ports to the current IPv6 multicast VLAN.

Use **undo port** to delete the specified ports from the current IPv6 multicast VLAN.

By default, an IPv6 multicast VLAN has no ports.

A port can belong to only one IPv6 multicast VLAN.

You can assign only Ethernet ports, and Layer 2 aggregate interfaces to a multicast VLAN.

Examples

```
# Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to IPv6 multicast VLAN 100.  
<Sysname> system-view  
[Sysname] multicast-vlan ipv6 100  
[Sysname-ipv6-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

port multicast-vlan ipv6

Syntax

```
port multicast-vlan ipv6 vlan-id  
undo port multicast-vlan ipv6
```

View

Ethernet interface view, Layer 2 aggregate interface view, port group view.

Default level

2: System level

Parameters

vlan-id: Specifies an IPv6 multicast VLAN by its ID, in the range of 1 to 4094.

Description

Use **port multicast-vlan ipv6** to assign the current port to the specified IPv6 multicast VLAN.

Use **undo port multicast-vlan ipv6** to restore the default.

By default, a port does not belong to any IPv6 multicast VLAN.

A port can belong to only one IPv6 multicast VLAN.

Examples

```
# Assign GigabitEthernet 1/0/1 to IPv6 multicast VLAN 100.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port multicast-vlan ipv6 100
```

subvlan (IPv6 multicast VLAN view)

Syntax

```
subvlan vlan-list
undo subvlan { all | vlan-list }
```

View

IPv6 multicast VLAN view

Default level

2: System level

Parameters

vlan-list: Specifies a VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

all: Specifies all the sub-VLANs of the current IPv6 multicast VLAN.

Description

Use **subvlan** to configure sub-VLANs for the current IPv6 multicast VLAN.

Use **undo subvlan** to remove the specified sub-VLANs or all sub-VLANs from the current IPv6 multicast VLAN.

An IPv6 multicast VLAN has no sub-VLANs by default.

The VLANs to be configured as the sub-VLANs of the IPv6 multicast VLAN must exist and must not be IPv6 multicast VLANs or sub-VLANs of any other IPv6 multicast VLAN.

The number of sub-VLANs of the IPv6 multicast VLAN must not exceed the system-defined limit.

Examples

```
# Configure VLAN 10 through VLAN 15 as sub-VLANs of IPv6 multicast VLAN 100.
<Sysname> system-view
[Sysname] multicast-vlan ipv6 100
[Sysname-ipv6-mvlan-100] subvlan 10 to 15
```

IPv6 multicast routing and forwarding configuration commands (available only on the HP 5500 EI)

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

The term "interface" in the IPv6 multicast routing and forwarding 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*).

display multicast ipv6 boundary

Syntax

```
display multicast ipv6 boundary { group [ ipv6-group-address [ prefix-length ] ] | scope [ scope-id ] }  
[ interface interface-type interface-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

group: Displays the IPv6 multicast boundary information for the specified group.

ipv6-group-address: Specifies an IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

prefix-length: Specifies the prefix length of an IPv6 multicast group address, in the range of 8 to 128. The default is 128.

scope: Displays the IPv6 multicast group boundary information in the admin-scope zone.

scope-id: Specifies the ID of an admin-scope zone in the range of 3 to 15, which is identified by the scope field in the IPv6 multicast group address.

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 multicast ipv6 boundary** to display the IPv6 multicast boundary information on the specified interface or all interfaces.

Related commands: **multicast ipv6 boundary**.

Examples

```
# Display IPv6 multicast boundary information on all interfaces.
```

```
<Sysname> display multicast ipv6 boundary group
IPv6 multicast boundary information
Boundary          Interface
FF03::/16         Vlan1
FF09::/16         Vlan2
```

Table 62 Command output

Field	Description
Boundary	IPv6 multicast group that corresponds to the IPv6 multicast boundary
Interface	Boundary interface that corresponds to the IPv6 multicast boundary

display multicast ipv6 forwarding-table

Syntax

```
display multicast ipv6 forwarding-table [ ipv6-source-address [ prefix-length ] | ipv6-group-address [ prefix-length ] | incoming-interface { interface-type interface-number | register } | outgoing-interface { exclude | include | match } { interface-type interface-number | register } | statistics | slot slot-number ] * [ port-info ] [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

prefix-length: Specifies the prefix length of an IPv6 multicast group address or an IPv6 multicast source address. For an IPv6 multicast group address, the value ranges from 8 to 128. For an IPv6 multicast source address, the value ranges from 0 to 128. The default is 128 in both cases.

incoming-interface: Displays the forwarding entries whose incoming interface is the specified one.

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

register: Represents a registered interface.

outgoing-interface: Displays the forwarding entries whose outgoing interface is the specified one.

exclude: Displays the forwarding entries whose outgoing interface list excludes the specified interface.

include: Displays the forwarding entries whose outgoing interface list includes the specified interface.

match: Displays the forwarding entries whose outgoing interface list includes and includes only the specified interface.

statistics: Displays statistics for the IPv6 multicast forwarding table.

slot slot-number: Displays IPv6 multicast forwarding entries for the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

port-info: Displays Layer 2 port 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 multicast ipv6 forwarding-table** to display information about the IPv6 multicast forwarding table.

IPv6 multicast forwarding tables guide multicast forwarding. You can determine the state of IPv6 multicast traffic forwarding by viewing the IPv6 multicast forwarding table.

Related commands: **display multicast ipv6 routing-table**, **multicast ipv6 forwarding-table downstream-limit**, and **multicast ipv6 forwarding-table route-limit**.

Examples

```
# Display information about the IPv6 multicast forwarding table.
```

```
<Sysname> display multicast ipv6 forwarding-table
```

```
IPv6 Multicast Forwarding Table
```

```
Total 1 entry
```

```
Total 1 entry matched
```

```
00001. (2000:5::1:1000, FF1E::1234)
```

```
  MID: 0, Flags: 0x100000:0
```

```
  Uptime: 04:04:37, Timeout in: 00:03:26
```

```
  Incoming interface: Vlan-interface1
```

```
  List of 1 outgoing interfaces:
```

```
    1: Vlan-interface2
```

```
  Matched 146754 packets(10272780 bytes), Wrong If 0 packets
```

```
  Forwarded 139571 packets(9769970 bytes)
```

Table 63 Command output

Field	Description
Total 1 entry	Total number of (S, G) entries in the IPv6 multicast forwarding table.
Total 1 entry matched	Total number of matched (S, G) entries in the IPv6 multicast forwarding table.

Field	Description
00001	Sequence number of the (S, G) entry.
(2000:5::1:1000, FF1E::1234)	(S, G) entry in the IPv6 multicast forwarding table.
MID	MID of the (S, G). Each (S, G) entry has a unique MID.
Flags	Current state of the (S, G) entry. Different bits indicate different states of (S, G) entries. The flags field comprises two hexadecimal numbers separated by a colon (:). Major values of the flags field before the colon are described in Table 64 . The value of the flags field after the colon is 0.
Uptime	Length of time for which the (S, G) entry has been up.
Timeout in	Length of time in which the (S, G) entry will time out.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces: 1: Vlan-interface2	Outgoing interface list. Interface type and number.
Matched 146754 packets(10272780 bytes), Wrong If 0 packets	(S, G)-matched packets (bytes), packets with incoming interface errors.
Forwarded 139571 packets(9769970 bytes)	(S, G) forwarded IPv6 multicast packets (bytes).

Table 64 Major values of the Flags field (before the colon)

Value	Meaning
0x1	A register-stop message must be sent.
0x2	Whether the IPv6 multicast source that corresponds to the (S, G) entry is active.
0x4	Null forwarding entry.
0x8	Whether the RP is a border router in an IPv6 PIM domain.
0x10	A register outgoing interface is available.
0x400	(S, G) entry to be deleted.
0x8000	The (S, G) entry is in smoothing process after active/standby switchover.
0x10000	The (S, G) entry has been updated during the smoothing process.
0x80000	The (S, G) entry has been repeatedly updated and need to be deleted before a new entry is added.
0x100000	The (S, G) entry was added successfully.
0x1000000	Multicast forwarding entry for IPv6 BIDIR-PIM.
0x2000000	RP for IPv6 BIDIR-PIM.

display multicast ipv6 forwarding-table df-info

Syntax

```
display multicast ipv6 forwarding-table df-info [ rp-address ] [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

rp-address: Specifies an RP address of IPv6 BIDIR-PIM.

slot *slot-number*: Displays the DF information of the IPv6 multicast forwarding table for the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device 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 the 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 multicast ipv6 forwarding-table df-info** to display the DF information of the IPv6 multicast forwarding table.

Examples

```
# Display the DF information of the IPv6 multicast forwarding table.
<Sysname> display multicast ipv6 forwarding-table df-info
IPv6 Multicast DF information
Total 1 RP

Total 1 RP matched

00001. RP Address: 2010::1
    MID: 0, Flags: 0x2100000:0
    Uptime: 00:08:32
    RPF interface: Vlan-interface1
    List of 1 DF interfaces:
        1: Vlan-interface2
```

Table 65 Command output

Field	Description
Total 1 RP	Total number of RPs.

Field	Description
Total 1 RP matched	Total number of matched RPs.
00001	Sequence number of the RP.
MID	ID of the RP. Each RP has a unique MID.
Flags	Current state of the RP. Different bits indicate different states of an RP. Major values of the flags field before the colon are described in Table 64 . The value of the flags field after the colon is 0.
Uptime	Length of time for which the RP has been up, in the format hours:minutes:seconds.
RPF interface	RPF interface to the RP.
List of 1 DF interfaces	DF interface list.

display multicast ipv6 routing-table

Syntax

```
display multicast ipv6 routing-table [ ipv6-source-address [ prefix-length ] | ipv6-group-address [ prefix-length ] | incoming-interface { interface-type interface-number | register } | outgoing-interface { exclude | include | match } { interface-type interface-number | register } ] * [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-source-address: Specifies a multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

prefix-length: Specifies the length of the prefix of a multicast group address or an IPv6 multicast source address. For an IPv6 multicast group address, the value ranges from 8 to 128. For an IPv6 multicast source address, the value ranges from 0 to 128. The default is 128 in both cases.

incoming-interface: Displays routing entries whose incoming interface is the specified one.

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

register: Represents a registered interface.

outgoing-interface: Displays routing entries whose the outgoing interface is the specified one.

exclude: Displays routing entries whose outgoing interface list excludes the specified interface.

include: Displays routing entries whose outgoing interface list includes the specified interface.

match: Displays routing entries whose outgoing interface list includes only the specified interface.

|: 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 multicast ipv6 routing-table** to display information about the IPv6 multicast routing table.

IPv6 multicast routing tables are the basis of IPv6 multicast forwarding. You can determine the establishment state of an (S, G) entry by viewing the IPv6 multicast routing table.

Related commands: **display multicast ipv6 forwarding-table**.

Examples

Display information about the IPv6 multicast routing table.

```
<Sysname> display multicast ipv6 routing-table
IPv6 multicast routing table
Total 1 entry

00001. (2001::2, FFE3::101)
  Uptime: 00:00:14
  Upstream Interface: Vlan-interface1
  List of 1 downstream interface
    1: Vlan-interface2
```

Table 66 Command output

Field	Description
Total 1 entry	Total number of (S, G) entries in the IPv6 multicast routing table.
00001	Sequence number of the (S, G) entry.
(2001::2, FFE3::101)	(S, G) entry in the IPv6 multicast forwarding table.
Uptime	Length of time for which the (S, G) entry has been up.
Upstream interface	Upstream interface of the (S, G) entry. Multicast packets should arrive through this interface.
List of 2 downstream interfaces	Downstream interface list. These interfaces must forward multicast packets.

display multicast ipv6 rpf-info

Syntax

```
display multicast ipv6 rpf-info ipv6-source-address [ ipv6-group-address ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number from 0 to F.

|: 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 multicast ipv6 rpf-info** to display RPF information of an IPv6 multicast source.

Related commands: **display multicast ipv6 forwarding-table** and **display multicast ipv6 routing-table**.

Examples

```
# Display all RPF information of the multicast source with an IPv6 address 2001::101.
```

```
<Sysname> display multicast ipv6 rpf-info 2001::101
RPF information about source 2001::101:
  RPF interface: Vlan-interface1, RPF neighbor: 2002::201
  Referenced prefix/prefix length: 2001::/64
  Referenced route type: igp
  Route selection rule: preference-preferred
  Load splitting rule: disable
```

Table 67 Command output

Field	Description
RPF interface	Interface type and number of the RPF interface.
RPF neighbor	IPv6 address of the RPF neighbor.
Referenced prefix/prefix length	Referenced route and prefix length.
Referenced route type	Type of the referenced route, which can be any of the following: <ul style="list-style-type: none">• igp—IPv6 unicast route (IGB).• egp—IPv6 unicast (EGP).• unicast (direct)—IPv6 unicast route (directly connected).• unicast—Other IPv6 unicast route (such as IPv6 unicast static route).• mbgp—IPv6 MBGP route.
Route selection rule	RPF route selection rule: An RPF route can be selected by the priority of the routing protocol or by the longest match of the destination address in the routing table.
Load splitting rule	Load sharing rule.

multicast ipv6 boundary

Syntax

```
multicast ipv6 boundary { ipv6-group-address prefix-length | scope { scope-id | admin-local | global | organization-local | site-local } }
```

```
undo multicast ipv6 boundary { ipv6-group-address prefix-length | scope { scope-id | admin-local | global | organization-local | site-local } | all }
```

View

Interface view

Default level

2: System level

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

prefix-length: Specifies the Prefix length of an IPv6 multicast group address, in the range of 8 to 128.

scope-id: Specifies the ID of an admin-scope zone in the range of 3 to 15, which is identified by the scope field in the IPv6 multicast group address.

admin-local: Specifies the scope zone as admin-local, which has a scope ID of 4.

global: Specifies the scope zone as global, which has a scope ID of 14.

organization-local: Specifies the scope zone as organization-local, which has a scope ID of 8.

site-local: Specifies the scope zone as site-local, which has a scope ID of 5.

all: Deletes all IPv6 multicast boundaries configured on the interface.

Description

Use **multicast ipv6 boundary** to configure an IPv6 multicast forwarding boundary.

Use **undo multicast ipv6 boundary** to delete the specified IPv6 multicast forwarding boundary or all IPv6 multicast forwarding boundaries.

By default, no multicast forwarding boundary is configured.

A multicast forwarding boundary sets the boundary condition for the IPv6 multicast groups in the specified address range. If the destination address of an IPv6 multicast packet matches the set boundary condition, the packet is not forwarded.

An interface can act as a forwarding boundary for multiple IPv6 multicast groups in different address ranges. You can implement this by using this command on the interface for each multicast address range. These multicast groups must be in the same scope. The latest configuration of a scope overwrites the previous one.

Assume that Set A and Set B are both multicast forwarding boundary sets with different address ranges, and that B is a subset of A. If B is configured after A, A still takes effect. If A is configured after B, B will be removed.

Related commands: **display multicast ipv6 boundary**.

Examples

Configure VLAN-interface 100 to be the forwarding boundary of the IPv6 multicast groups in the range of FF03::/16.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] multicast ipv6 boundary ff03:: 16
```

Configure VLAN-interface 100 to be the forwarding boundary of the IPv6 multicast groups in the admin-local scope.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] multicast ipv6 boundary scope 4
```

multicast ipv6 forwarding-table downstream-limit

Syntax

multicast ipv6 forwarding-table downstream-limit *limit*

undo multicast ipv6 forwarding-table downstream-limit

View

System view

Default level

2: System level

Parameters

limit: Specifies the maximum number of downstream node (the maximum number of outgoing interfaces) for a single entry in the IPv6 multicast forwarding table. The value ranges from 0 to 128.

Description

Use **multicast ipv6 forwarding-table downstream-limit** to configure the maximum number of downstream nodes for a single entry in the IPv6 multicast forwarding table.

Use **undo multicast ipv6 forwarding-table downstream-limit** to restore the default.

By default, the maximum number of downstream nodes for a single entry in the IPv6 multicast forwarding table is 128.

Related commands: **display multicast ipv6 forwarding-table**.

Examples

Set the maximum number of downstream nodes for a single entry in the IPv6 multicast forwarding table to 120.

```
<Sysname> system-view
[Sysname] multicast ipv6 forwarding-table downstream-limit 120
```

multicast ipv6 forwarding-table route-limit

Syntax

multicast ipv6 forwarding-table route-limit *limit*

undo multicast ipv6 forwarding-table route-limit

View

System view

Default level

2: System level

Parameters

limit: Specifies the maximum number of entries in the IPv6 multicast forwarding table. The value ranges from 0 to 1000.

Description

Use **multicast ipv6 forwarding-table route-limit** to configure the maximum number of entries in the IPv6 multicast forwarding table.

Use **undo multicast ipv6 forwarding-table route-limit** to restore the default.

By default, the upper limit is 1000.

Related commands: **display multicast ipv6 forwarding-table**.

Examples

Set the maximum number of entries in the IPv6 multicast forwarding table to 200.

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

```
[Sysname] multicast ipv6 forwarding-table route-limit 200
```

multicast ipv6 load-splitting

Syntax

multicast ipv6 load-splitting {source | source-group }

undo multicast ipv6 load-splitting

View

System view

Default level

2: System level

Parameters

source: Specifies IPv6 multicast load splitting on a per-source basis.

source-group: Specifies IPv6 multicast load splitting on a per-source and per-group basis.

Description

Use **multicast ipv6 load-splitting** to enable load splitting of IPv6 multicast traffic.

Use **undo multicast ipv6 load-splitting** to disable load splitting of IPv6 multicast traffic.

By default, load splitting of IPv6 multicast traffic is disabled.

This command does not take effect in IPv6 BIDIR-PIM.

Examples

Enable load splitting of IPv6 multicast traffic on a per-source basis.

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

```
[Sysname] multicast ipv6 load-splitting source
```

multicast ipv6 longest-match

Syntax

```
multicast ipv6 longest-match
undo multicast ipv6 longest-match
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **multicast ipv6 longest-match** to configure RPF route selection based on the longest match principle, namely, to select the route with the longest prefix as the RPF route.

Use **undo multicast ipv6 longest-match** to restore the default.

By default, the route with the highest priority is selected as the RPF route.

Examples

```
# Configure RPF route selection based on the longest match.
<Sysname> system-view
[Sysname] multicast ipv6 longest-match
```

multicast ipv6 routing-enable

Syntax

```
multicast ipv6 routing-enable
undo multicast ipv6 routing-enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **multicast ipv6 routing-enable** to enable IPv6 multicast routing.

Use **undo multicast ipv6 routing-enable** to disable IPv6 multicast routing.

IPv6 multicast routing is disabled by default.

You must enable IPv6 multicast routing before you can use other Layer 3 IPv6 multicast commands.

The device does not forward any IPv6 multicast packets before IPv6 multicast routing is enabled.

Examples

```
# Enable IPv6 multicast routing.
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
```

reset multicast ipv6 forwarding-table

Syntax

```
reset multicast ipv6 forwarding-table { { ipv6-source-address [ prefix-length ] | ipv6-group-address [ prefix-length ] | incoming-interface { interface-type interface-number | register } } * | all }
```

View

User view

Default level

2: System level

Parameters

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 to F.

prefix-length: Specifies the prefix length of an IPv6 multicast group or an IPv6 multicast source address. For an IPv6 multicast group address, the value ranges from 8 to 128. For an IPv6 multicast source address, the value ranges from 0 to 128. The default is 128 in both cases.

incoming-interface: Specifies the IPv6 multicast forwarding entries whose incoming interface is the specified one.

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

register: Specifies the register interface.

all: Specifies all forwarding entries.

Description

Use **reset multicast ipv6 forwarding-table** to remove IPv6 multicast forwarding entries.

When an IPv6 forwarding entry is removed, the associated IPv6 multicast routing entry is also removed.

Related commands: **display multicast ipv6 forwarding-table**, **display multicast ipv6 routing-table**, and **reset multicast IPv6 routing-table**.

Examples

```
# Remove the IPv6 multicast forwarding entry for the IPv6 multicast group FF03::101.
<Sysname> reset multicast ipv6 forwarding-table ff03::101
```

reset multicast ipv6 routing-table

Syntax

```
reset multicast ipv6 routing-table { { ipv6-source-address [ prefix-length ] | ipv6-group-address [ prefix-length ] | incoming-interface { interface-type interface-number | register } } * | all }
```

View

User view

Default level

2: System level

Parameters

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 to F.

prefix-length: Specifies the prefix length of an IPv6 multicast group address or an IPv6 multicast source address. For an IPv6 multicast group address, the value ranges from 8 to 128. For an IPv6 multicast source address, the value ranges from 0 to 128. The default is 128 in both cases.

incoming-interface: Specifies the IPv6 multicast routing entries whose incoming interface is the specified one.

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

register: Specifies a register interface.

all: Specifies all IPv6 multicast routing entries.

Description

Use **reset multicast ipv6 routing-table** to remove IPv6 multicast routing entries.

When an IPv6 multicast routing entry is removed, the associated IPv6 multicast forwarding entry is also removed.

Related commands: **display multicast ipv6 forwarding-table**, **display multicast ipv6 routing-table**, and **reset multicast ipv6 forwarding-table**.

Examples

```
# Remove the IPv6 multicast routing entry for the IPv6 multicast group FF03::101.
```

```
<Sysname> reset multicast ipv6 routing-table ff03::101
```

MLD configuration commands (available only on the HP 5500 EI)

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

The term "interface" in this chapter 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*).

display mld group

Syntax

```
display mld group [ ipv6-group-address | interface interface-type interface-number ] [ static | verbose ]  
[ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-group-address: Specifies an MLD group address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F. If you do not specify any IPv6 multicast group address, this command displays the information of all MLD groups.

interface *interface-type interface-number*: Displays the information of MLD groups on the specified interface. If you do not specify *interface-type interface-number*, the command displays the MLD group information on all the interfaces.

static: Displays the information of static MLD group entries. If you do not specify this keyword, the command displays the dynamic MLD group entries.

verbose: Displays detailed information of MLD groups.

|: 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 mld group** to display information about MLD groups.

Examples

```
# Display detailed information about dynamically joined MLD groups on all interfaces.
```



```

<Sysname> display mld group verbose
Interface group report information
Vlan-interface1(FE80::101)
  Total 1 MLD Groups reported
  Group: FF03::101
    Uptime: 00:01:46
    Expires: 00:01:30
    Last reporter: FE80::10
    Last-listener-query-counter: 0
    Last-listener-query-timer-expiry: off
    Group mode: include
    Version1-host-present-timer-expiry: off

```

Table 68 Command output

Field	Description
Interface group report information	MLD group information on the interface.
Total 1 MLD Groups reported	One MLD group was reported.
Group	IPv6 multicast group address.
Uptime	Length of time since the IPV6 multicast group was joined.
Expires	Remaining time of the IPv6 multicast group, where "off" means that the multicast group never times out.
Last reporter	IPv6 address of the host that last reported membership for this group.
Last-listener-query-counter	Number of MLD last listener queries sent.
Last-listener-query-timer-expiry	Remaining time of the MLD last listener query timer, where "off" means that the timer never times out.
Group mode	Multicast source filtering mode: <ul style="list-style-type: none"> • Include. • Exclude. This field is displayed only when the device is running MLDv2.
Version1-host-present-timer-expiry	Remaining time of the MLDv1 host present timer, where "off" means that the timer never times out. This field is displayed only when the device is running MLDv2.

display mld group port-info

Syntax

```

display mld group port-info [ vlan vlan-id ] [ slot slot-number ] [ verbose ] [ { begin | exclude | include }
regular-expression ]

```

View

Any view

Default level

1: Monitor level

Parameters

vlan-id: Specifies a VLAN by its ID, in the range of 1 to 4094. If you do not specify any VLAN, this command displays the Layer 2 port information of MLD groups in all VLANs.

slot slot-number: Displays the Layer 2 port information of MLD multicast groups on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

verbose: Displays the detailed information about Layer 2 ports of MLD groups.

|: 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 mld group port-info** to display Layer 2 port information of MLD groups, including Layer 2 information of dynamic and static MLD group entries.

Examples

```
# Display detailed layer 2 port information of MLD groups.
<Sysname> display mld group port-info verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):2.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port unit board: Mask(0x0000)
    Router port(s):total 1 port(s).
      GE1/0/1                (D) ( 00:01:30 )
  IP group(s):the following ip group(s) match to one mac group.
    IP group address: FF03::101
      (FE80::1, FF03::101):
        Attribute:    Host Port
        Host port unit board: Mask(0x0000)
        Host port(s):total 1 port(s).
          GE1/0/2                (D) ( 00:03:23 )
  MAC group(s):
    MAC group address:3333-0000-0101
    Host port unit board: Mask(0x0000)
    Host port(s):total 1 port(s).
      GE1/0/2
```

Table 69 Command output

Field	Description
Total 1 IP Group(s).	Total number of IPv6 multicast groups.
Total 1 IP Source(s).	Total number of IPv6 multicast sources.
Total 1 MAC Group(s).	Total number of MAC multicast groups.
Port flags: D-Dynamic port, S-Static port, C-Copy port	Port flag: D —Dynamic port. S —Static port. C —Port copied from a (*, G) entry to an (S, G) entry.
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flag: R stands for real egress sub-VLAN under the current entry, and C for sub-VLAN copied from a (*, G) entry to an (S, G) entry.
Router port unit board	Mask indicating an IRF member switch with a router port residing on it. If no IRF fabric exists, Mask (0x0000) is displayed.
Router port(s)	Number of router ports.
(00:01:30)	Remaining time of the aging timer for the dynamic member ports or router ports. On an IRF member switch, to display the remaining life of a non-aggregation port that does not belong to the Master device, you must specify the member ID of the IRF member switch by using slot slot-number . For an aggregation port, you do not need to do this.
IP group address	Address of an IPv6 multicast group.
MAC group address	Address of a MAC multicast group.
Attribute	Attribute of an IPv6 multicast group.
Host port unit board	Mask indicating an IRF member switch with a member port residing on it. If no IRF fabric exists, Mask (0x0000) is displayed.
Host port(s)	Number of member ports.

display mld host interface

Syntax

```
display mld host interface interface-type interface-number group ipv6-group-address [ source
ipv6-source-address ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Displays information about the hosts tracked by MLD on the specified interface. The specified interface can be a Layer 3 Ethernet port, Layer 3 aggregate interface, or Tunnel interface.

group *ipv6-group-address*: Displays information about the hosts tracked by MLD that are in the specified IPv6 multicast group. The value of *ipv6-group-address* is in the range of FFxy::/16 (excluding FFx0::/16,

FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

source *ipv6-source-address*: Displays information about the hosts tracked by MLD that are in the specified IPv6 multicast source.

|: 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 mld host interface** to display information about the hosts tracked by MLD on the specified interface.

Examples

```
# Display information about the hosts tracked by MLD in multicast group FF1E::101 on layer 3 Ethernet port GigabitEthernet1/0/1.
```

```
<Sysname> display mld host interface gigabitethernet1/0/1 group ff1e::101
GigabitEthernet1/0/1(1::1):
  (::, FF1E::101)
  Host                Uptime                Expires
  1::1                 00:02:20              00:00:40
  2::2                 00:02:21              00:00:39
```

Table 70 Command output

Field	Description
GigabitEthernet1/0/1(1::1)	Interface and IPv6 address
(::, FF1E::101)	(S, G) entry, where "::" indicates all IPv6 multicast sources
Host	Host IPv6 address
Uptime	Host running duration
Expires	Host expiration time, where "timeout" means that the host has expired

display mld host port-info

Syntax

```
display mld host port-info vlan vlan-id group ipv6-group-address [ source ipv6-source-address ] [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays information about the hosts tracked by MLD on the Layer 2 ports in the specified VLAN, where *vlan-id* is in the range of 1 to 4094.

group *ipv6-group-address*: Displays information about the hosts tracked by MLD that are in the specified IPv6 multicast group on the Layer 2 ports. The value of *ipv6-group-address* is in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

source *ipv6-source-address*: Displays information about the hosts tracked by MLD that are in the specified IPv6 multicast source on the Layer 2 ports.

slot *slot-number*: Displays information about the hosts tracked by MLD on the Layer 2 ports on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device 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 mld host port-info** to display information about the hosts tracked by MLD on the Layer 2 ports.

Examples

```
# Display information about the hosts tracked by MLD that are in IPv6 multicast group FF1E::101 2 on the Layer 2 ports in VLAN.
```

```
<Sysname> display mld host port-info vlan 2 group ff1e::101
```

```
VLAN(ID) : 2
```

```
(::, FF1E::101)
```

```
Port : GigabitEthernet1/0/1
```

Host	Uptime	Expires
1::1	00:02:20	00:00:40
2::2	00:02:21	00:00:39

```
Port : GigabitEthernet1/0/2
```

Host	Uptime	Expires
3::3	00:02:20	00:00:40

Table 71 Command output

Field	Description
(::, FF1E::101)	(S, G) entry, where "::" indicates all IPv6 multicast sources
Port	Member port
Host	Host IPv6 address
Uptime	Host running duration
Expires	Host expiration time, where "timeout" means that the host has expired

display mld interface

Syntax

```
display mld interface [ interface-type interface-number ] [ verbose ] [ | { 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. If you do not specify any interface, this command displays information about all interfaces that runs MLD.

verbose: Displays detailed MLD configuration and operation 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 mld interface** to display MLD configuration and operation information on the specified interface or all MLD-enabled interfaces.

Examples

```
# Display detailed MLD configuration and operation information on VLAN-interface1 (downstream interface).
```

```
<Sysname> display mld interface vlan-interface 1 verbose
Vlan-interface1(FE80::200:AFF:FE01:101):
  MLD is enabled
  Current MLD version is 1
  Value of query interval for MLD(in seconds): 125
  Value of other querier present interval for MLD(in seconds): 255
  Value of maximum query response time for MLD(in seconds): 10
  Value of last listener query interval(in seconds): 1
  Value of startup query interval(in seconds): 31
  Value of startup query count: 2
  General query timer expiry (hours:minutes:seconds): 00:00:23
  Querier for MLD: FE80::200:AFF:FE01:101 (this router)
  MLD activity: 1 joins, 0 leaves
  Multicast ipv6 routing on this interface: enabled
  Robustness: 2
  Require-router-alert: disabled
```

```

Fast-leave: disabled
Ssm-mapping: disabled
Startup-query-timer-expiry: off
Other-querier-present-timer-expiry: off
Proxying interface: Vlan-interface2(FE80::100:CEF:FE01:101)
Total 1 MLD Group reported

```

Display detailed MLD configuration and operation information on VLAN-interface2 (upstream interface).

```

<Sysname> display mld interface vlan-interface 2 verbose
Vlan-interface2(FE80::100:CEF:FE01:101):
  MLD proxy is enabled
  Current MLD version is 2
  Multicast ipv6 routing on this interface: enabled
  Require-router-alert: disabled
  Version1-querier-present-timer-expiry: off

```

Table 72 Command output

Field	Description
vlan-interface1(FE80::200:AFF:FE01:101)	Interface and IPv6 link-local address
Current MLD version	MLD version running on the interface
Value of query interval for MLD (in seconds)	MLD query interval, in seconds
Value of other querier present interval for MLD (in seconds)	MLD other querier present interval, in seconds
Value of maximum query response time for MLD (in seconds)	Maximum response delay for general query messages (in seconds)
Value of last listener query interval (in seconds)	MLD last listener query interval, in seconds
Value of startup query interval(in seconds)	MLD startup query interval, in seconds
Value of startup query count	Number of MLD general queries sent on startup
General query timer expiry	Remaining time of the MLD general query timer, where "off" means that the timer never times out
Querier for MLD	IPv6 link-local address of the MLD querier
MLD activity	MLD activity statistics (number of join and done messages)
Robustness	MLD querier's robustness variable
Require-router-alert	Dropping MLD messages without Router-Alert (enabled/disabled)
Fast-leave	MLD fast-leave processing status (enabled/disabled)
Ssm-mapping	MLD SSM mapping status (enabled/disabled)
Startup-query-timer-expiry	Remaining time of MLD startup query timer, where "off" means that the timer never times out
Other-querier-present-timer-expiry	Remaining time of MLD other querier present timer, where "off" means that the timer never times out

Field	Description
Proxying interface	MLD proxy interface, where "none" means that no proxy interface exists
Total 1 MLD Group reported	Total number of MLD groups the interface has dynamically joined
Version1-querier-present-timer-expiry	Remaining time of the MLDv1 querier present timer, where "off" means that the timer never times out

display mld proxying group

Syntax

```
display mld proxying group [ ipv6-group-address ] [ verbose ] [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-group-address: Displays the information of the specified MLD proxying group. The group address is in the form of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, through FF0y::), where x and y represent any hexadecimal number ranging from 0 to F. If this argument is not specified, this command displays the information of all the MLD proxying groups.

verbose: Displays detailed MLD proxying group 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 mld proxying group** to display MLD proxying group information.

Examples

```
# Display MLD proxying group information on all interfaces.
```

```
<Sysname> display mld proxying group verbose
Proxying group record(s) information
  Total 1 MLD-Proxying group record(s)
  Group: FF03::101
  Group mode: include
  Member state: Delay
  Expires: 00:00:02
  Source list (total 1 source(s))
```


Source: 30::1

Table 73 Command output

Field	Description
Proxying group record(s) information	Information of MLD proxying groups on the interfaces.
Total 1 MLD-Proxying group record(s)	One MLD proxying group is recorded.
Group	IPv6 multicast group address.
Member state	State of the member hosts: <ul style="list-style-type: none">• Delay.• Idle.
Expires	Remaining time of the IPv6 multicast group, where "off" means that the group never times out.
Group mode	IPv6 multicast source filtering modes: <ul style="list-style-type: none">• Include.• Exclude.
Source list	List of IPv6 multicast sources (only including the sources from which the hosts want to receive IPv6 multicast data).

display mld routing-table

Syntax

```
display mld routing-table [ ipv6-source-address [ prefix-length ] | ipv6-group-address [ prefix-length ] | flags { act | suc } ] * [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-source-address: Specifies a multicast source by its IPv6 address.

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address, in the form of FFxy::/16, where x and y represent any hexadecimal number ranging from 0 to F.

prefix-length: Prefix length of the multicast source or multicast group address. For a multicast source address, this argument has an effective value range of 0 to 128. For a multicast group address, it has an effective value range of 8 to 128. The default is 128 in both cases.

flags: Specifies the route flag.

act: Specifies the MLD routes with the ACT flag

suc: Specifies the MLD routes with the SUC flag.

|: 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 mld routing-table** to display information about the MLD routing table.

Examples

```
# Display information about the MLD routing table.
```

```
<Sysname> display mld routing-table
Routing table
Total 2 entries

00001. (*, FF1E::101)
    List of 1 downstream interface
        Vlan-interface1 (FE80::200:5EFF:FE71:3800),
            Protocol: MLD

00002. (100::1, FF1E::101), Flag: ACT
    List of 1 downstream interface in include mode
        Vlan-interface2 (FE80::100:5E16:FEC0:1010),
            Protocol: MLD
```

Table 74 Command output

Field	Description
Routing table	MLD routing table.
00001	Sequence number of this (*, G) entry.
(*, FF1E::101)	(*, G) entry in the MLD routing table.
Flag	MLD route flags: <ul style="list-style-type: none">• ACT—Indicates MLD routing entries that have been used for forwarding data packets but have the multicast group address out of the SSM group range.• SUC—Indicates MLD routing entries that have been added to the forwarding table and have the multicast group address within the SSM group range.
List of 1 downstream interface	List of downstream interfaces, namely, the interfaces to which multicast data for this group is forwarded.
in include mode	The downstream interface is in the include mode.
in exclude mode	The downstream interface is in the exclude mode.
Downstream interface is none	No downstream interfaces exist.
Protocol	Protocol type.

display mld ssm-mapping

Syntax

```
display mld ssm-mapping ipv6-group-address [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

|: 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 mld ssm-mapping** to display the configured MLD SSM mappings for the specified IPv6 multicast group.

Related commands: **ssm-mapping**.

Examples

```
# Display the MLD SSM mappings for multicast group FF1E::101.
```

```
<Sysname> display mld ssm-mapping ff1e::101
Group: FF1E::101
Source list:
    1::1
    1::2
    10::1
    100::10
```

Table 75 Command output

Field	Description
Group	IPv6 multicast group address
Source list	List of IPv6 multicast source addresses

display mld ssm-mapping group

Syntax

```
display mld ssm-mapping group [ ipv6-group-address | interface interface-type interface-number ]  
[ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-group-address: Specifies a multicast group by its IPv6 address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F. If you do not specify any IPv6 multicast group, this command displays the information of all IPv6 multicast groups created based on the configured MLD SSM mappings.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify any interface, this command displays the multicast group information created based on the configured MLD SSM mappings on all interfaces.

verbose: Displays detailed information about multicast groups created based on the configured MLD SSM mappings.

|: 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 mld ssm-mapping group** to display information about the multicast groups created based on the configured MLD SSM mappings.

Examples

```
# Display detailed information about IPv6 multicast group FF3E::101 created based on the configured  
MLD SSM mappings on all interfaces.
```

```
<Sysname> display mld ssm-mapping group ff3e::101 verbose  
Interface group report information  
Vlan-interface1(FE80::101):  
Total 1 MLD SSM-mapping Group reported  
Group: FF3E::101  
Uptime: 00:01:46  
Expires: off  
Last reporter: FE80::10  
Group mode: include  
Source list(Total 1 source):  
Source: 30::1  
Uptime: 00:01:46
```

```
Expires: 00:02:34
Last-listener-query-counter: 0
Last-listener-query-timer-expiry: off
```

Table 76 Command output

Field	Description
Interface group report information	IPv6 multicast group information created based on MLD SSM mappings on the interface.
Total 1 MLD SSM-mapping Group reported	One MLD SSM mapping multicast group was reported.
Group	IPv6 multicast group address.
Uptime	Length of time since the IPv6 multicast group was reported.
Expires	Remaining time of the IPv6 multicast group, where "off" means that the group never times out.
Last reporter	IPv6 address of the host that last reported membership for this group.
Group mode	IPv6 multicast sources filter mode.
Source list(Total 1 source)	IPv6 multicast source list (one IPv6 multicast source).
Source	IPv6 multicast source address.
Last-listener-query-counter	Number of MLD last listener queries sent.
Last-listener-query-timer-expiry	Remaining time of the MLD last listener query timer, where "off" means that the timer never expires.

display mld ssm-mapping host interface

Syntax

```
display mld ssm-mapping host interface interface-type interface-number group ipv6-group-address
source ipv6-source-address [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Displays information about the hosts that join based on the MLD SSM mappings on the specified interface. The specified interface can be a Layer 3 Ethernet port, Layer 3 aggregate interface, or Tunnel interface.

group *ipv6-group-address*: Displays information about the hosts that join the specified IPv6 multicast group based on the MLD SSM mappings. The value of *ipv6-group-address* is in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

source *ipv6-source-address*: Displays information about the hosts that join the specified IPv6 multicast source based on the MLD SSM mappings.

|: 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 mld ssm-mapping host interface** to display information about the hosts that join based on the MLD SSM mappings on the specified interface.

Examples

Displays information about the hosts that join multicast source group (10::1, FF1E::101) based on the MLD SSM mappings on layer 3 Ethernet port GigabitEthernet1/0/1.

```
<Sysname> display mld ssm-mapping host interface gigabitethernet 1/0/1 group ff1e::101
source 10::1
GigabitEthernet1/0/1(1::1):
  (10::1, FF1E::101)
  Host                Uptime                Expires
  1::1                00:02:20              00:00:40
  2::2                00:02:21              00:00:39
```

Table 77 Command output

Field	Description
GigabitEthernet1/0/1(1::1)	Interface and IPv6 address
(10::1, FF1E::101)	(S, G) entry
Host	Host IPv6 address
Uptime	Host running duration
Expires	Host expiration time, where "timeout" means that the host has expired

dscp (MLD view)

Syntax

dscp *dscp-value*

undo dscp

View

MLD view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value for MLD messages, in the range of 0 to 63.

Description

Use **dscp** to set the DSCP value for MLD messages.

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

The default DSCP value in MLD messages is 48.

Examples

```
# Set the DSCP value to 63 for MLD messages.
<Sysname> system-view
[Sysname] mld
[Sysname-mld] dscp 63
```

fast-leave (MLD view)

Syntax

fast-leave [**group-policy** *acl6-number*]

undo fast-leave

View

MLD view

Default level

2: System level

Parameters

acl6-number: Specifies a basic IPv6 ACL, in the range of 2000 to 2999. If you do not include this argument in your command, this command takes effect for all IPv6 multicast groups.

Description

Use **fast-leave** to configure MLD fast-leave processing globally.

Use **undo fast-leave** to disable MLD fast-leave processing globally.

By default, MLD fast-leave processing is disabled. That is, the MLD querier sends multicast-address-specific queries or multicast-address-and-source-specific queries after receiving an MLD done message from a host, instead of sending a leave notification directly to the upstream.

When this command is executed in MLD view, this command takes effect only on Layer 3 interfaces except VLAN interfaces.

Related commands: **last-listener-query-interval** and **mld fast-leave**.

Examples

```
# Enable MLD fast-leave processing globally.
<Sysname> system-view
[Sysname] mld
[Sysname-mld] fast-leave
```

host-tracking (MLD view)

Syntax

host-tracking

undo host-tracking

View

MLD view

Default level

2: System level

Parameters

None

Description

Use **host-tracking** to enable the MLD host tracking function globally.

Use **undo host-tracking** to disable the MLD host tracking function globally.

By default, this function is disabled.

Related command: **mld host-tracking**.

Examples

```
# Enable the MLD host tracking function globally.  
<Sysname> system-view  
[Sysname] mld  
[Sysname-mld] host-tracking
```

last-listener-query-interval (MLD view)

Syntax

last-listener-query-interval *interval*

undo last-listener-query-interval

View

MLD view

Default level

2: System level

Parameters

interval: Specifies an MLD last listener query interval in seconds, namely, the length of time that the device waits between sending MLD multicast-address-specific queries. The value ranges from 1 to 5.

Description

Use **last-listener-query-interval** to configure the MLD last listener query interval globally.

Use **undo last-listener-query-interval** to restore the default.

By default, the MLD last listener query interval is 1 second.

Related commands: **display mld interface**, **mld last-listener-query-interval**, and **robust-count**.

Examples

```
# Set the MLD last listener query interval to 3 seconds globally.  
<Sysname> system-view  
[Sysname] mld
```



```
[Sysname-mld] last-listener-query-interval 3
```

max-response-time (MLD view)

Syntax

max-response-time *interval*

undo max-response-time

View

MLD view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for MLD general query messages in seconds, in the range of 1 to 25.

Description

Use **max-response-time** to configure the maximum response delay for MLD general queries globally.

Use **undo max-response-time** to restore the default.

By default, the maximum response delay for MLD general queries is 10 seconds.

Related commands: **display mld interface**, **mld max-response-time**, and **timer other-querier-present**.

Examples

```
# Set the maximum response delay for MLD general queries to 8 seconds globally.
```

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] max-response-time 8
```

mld

Syntax

mld

undo mld

View

System view

Default level

2: System level

Parameters

None

Description

Use **mld** to enter MLD view.

Use **undo mld** to remove the configurations made in MLD view.

This command can take effect only after IPv6 multicast routing is enabled on the device.

Related commands: **mld enable** and **multicast ipv6 routing-enable**.

Examples

```
# Enable IPv6 multicast routing and enter MLD view.  
<Sysname> system-view  
[Sysname] multicast ipv6 routing-enable  
[Sysname] mld  
[Sysname-mld]
```

mld enable

Syntax

```
mld enable  
undo mld enable
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **mld enable** to enable MLD on the current interface.

Use **undo mld enable** to disable MLD on the current interface.

By default, MLD is disabled on the current interface.

This command can take effect only after IPv6 multicast routing is enabled on the device.

Other MLD configurations performed on the interface can take effect only after MLD is enabled on the interface.

Related commands: **mld** and **multicast ipv6 routing-enable**.

Examples

```
# Enable IPv6 multicast routing and enable MLD on VLAN-interface 100.  
<Sysname> system-view  
[Sysname] multicast ipv6 routing-enable  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] mld enable
```

mld fast-leave

Syntax

```
mld fast-leave [ group-policy acl6-number ]  
undo mld fast-leave
```

View

Interface view

Default level

2: System level

Parameters

acl6-number: Specifies a basic IPv6 ACL, in the range of 2000 to 2999. If you do not specify any IPv6 ACL number, this command takes effect for all IPv6 multicast groups.

Description

Use **mld fast-leave** to configure MLD fast-leave processing on the current interface.

Use **undo mld fast-leave** to disable MLD fast-leave processing on the current interface.

By default, MLD fast-leave processing is disabled. That is, the MLD querier sends multicast-address-specific queries or multicast-address-and-source-specific queries after receiving an MLD done message from a host, instead of sending a leave notification directly to the upstream.

The **mld fast-leave** command cannot be used in VLAN interface view. To enable fast-leave processing on a specific Layer 2 port or ports, use the **mld-snooping fast-leave** command or the **fast-leave** (MLD-snooping view) command.

The **mld-snooping fast-leave** and **fast-leave** (MLD-snooping view) commands are effective for both MLD snooping-enabled VLANs and VLANs with MLD enabled on the corresponding VLAN interfaces.

Related commands: **fast-leave** (MLD view), **fast-leave** (MLD-snooping view), **mld last-listener-query-interval**, and **mld-snooping fast-leave**.

Examples

```
# Enable MLD fast-leave processing on layer 3 Ethernet port GigabitEthernet1/0/1.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-mode route
[Sysname-GigabitEthernet1/0/1] mld fast-leave
```

mld group-limit

Syntax

mld group-limit *limit*

undo mld group-limit

View

Interface view

Default level

2: System level

Parameters

limit: Specifies the maximum number of IPv6 multicast groups that an interface can join, in the range of 1 to 1000.

Description

Use **mld group-limit** to configure the maximum number of IPv6 multicast groups that an interface can join.

Use **undo mld group-limit** to restore the default.

By default, the upper limit is 1000.

This command is effective only for dynamically joined IPv6 multicast groups but not statically joined IPv6 multicast groups.

If the configured *limit* value is smaller than the number of the existing IPv6 multicast groups on the current interface, the system does not automatically remove the IPv6 multicast groups in excess. To bring this configuration into effect in this case, you need to use the **reset mld group** command to clear the IPv6 multicast groups information manually.

You can also use the **mld-snooping group-limit** command to limit the number of IPv6 multicast groups that an interface can join. However, if you configure the limit both in a VLAN and on a VLAN interface of this VLAN by using these two commands, inconsistencies might exist between Layer 2 and Layer 3 table entries. Therefore, HP recommends you to configure the limit only on the VLAN interface.

Related commands: **mld static-group**, **mld-snooping group-limit**, and **reset mld group**.

Examples

```
# Allow VLAN-interface 100 to join up to 128 IPv6 multicast groups.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld group-limit 128
```

mld group-policy

Syntax

```
mld group-policy acl6-number [ version-number ]
undo mld group-policy
```

View

Interface view

Default level

2: System level

Parameters

acl6-number: Specifies a basic or advanced IPv6 ACL, in the range of 2000 to 3999. The source address or address range specified in the advanced IPv6 ACL rule is the IPv6 multicast source address or addresses specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX or TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

version-number: MLD version number, 1 or 2. If you do not specify an MLD version, the configured group filter is effective for MLD reports of both version 1 and version 2.

Description

Use **mld group-policy** to configure an IPv6 multicast group filter on the current interface to control the IPv6 multicast groups that the hosts on the current interface can join.

Use **undo mld group-policy** to remove the configured IPv6 multicast group filter.

By default, no IPv6 multicast group filter is configured. That is, a host can join any valid IPv6 multicast group.

You can also use the **group-policy** (MLD-snooping view) command to control the IPv6 multicast groups that hosts in a VLAN can join, achieving the same result as **mld group-policy**. If you have configured a multicast group filter on a VLAN interface to control the multicast groups that the hosts on the interface can join, HP recommends you to configure the same multicast group filter in the corresponding VLAN.

Related commands: **group-policy** (MLD-snooping view).

Examples

```
# Configure an IPv6 ACL so that hosts on VLAN-interface 100 can join the IPv6 multicast group FF03::101 only.
```

```
<Sysname> system-view
[Sysname] acl ipv6 number 2005
[Sysname-acl6-basic-2005] rule permit source ff03::101 16
[Sysname-acl6-basic-2005] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld group-policy 2005
```

mld host-tracking

Syntax

mld host-tracking

undo mld host-tracking

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **mld host-tracking** to enable the MLD host tracking function on an interface.

Use **undo mld host-tracking** to disable the MLD host tracking function on an interface

By default, this function is disabled.

Related commands: **host-tracking**.

Examples

```
# Enable the MLD host tracking function on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld host-tracking
```

mld last-listener-query-interval

Syntax

mld last-listener-query-interval *interval*

undo mld last-listener-query-interval

View

Interface view

Default level

2: System level

Parameters

interval: Specifies an MLD last listener query interval in seconds, in the range of 1 to 5.

Description

Use **mld last-listener-query-interval** to configure the MLD last listener query interval on the current interface.

Use **undo mld last-listener-query-interval** to restore the default.

By default, the MLD last listener query interval is 1 second.

Related commands: **display mld interface**, **last-listener-query-interval**, and **mld robust-count**.

Examples

```
# Set the MLD last listener query interval to 3 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld last-listener-query-interval 3
```

mld max-response-time

Syntax

mld max-response-time *interval*

undo mld max-response-time

View

Interface view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for MLD general query messages in seconds, in the range of 1 to 25.

Description

Use **mld max-response-time** to configure the maximum response delay for MLD general query messages on the interface.

Use **undo mld max-response-time** to restore the default.

By default, the maximum response delay for MLD general query messages is 10 seconds.

The maximum response delay determines the time that the device takes to detect directly attached group members in the LAN.

Related commands: **display mld interface**, **max-response-time**, and **mld timer other-querier-present**.

Examples

```
# Set the maximum response delay for MLD general query messages to 8 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld max-response-time 8
```

mld proxying enable

Syntax

```
mld proxying enable
undo mld proxying enable
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **mld proxying enable** to enable MLD proxying on an interface.

Use **undo mld proxying enable** to disable MLD proxying on the interface.

By default, MLD proxying is disabled.

This command takes effect only after IPv6 multicast routing is enabled.

If MLD proxying is enabled on a loopback interface, the proxy device maintains only the MLD routing table without adding the MLD routes to the multicast routing table and forwarding table.

Related commands: **multicast ipv6 routing-enable**.

Examples

```
# Enable IPv6 multicast routing and enable MLD proxying on VLAN-interface 100.
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld proxying enable
```

mld proxying forwarding

Syntax

```
mld proxying forwarding
undo mld proxying forwarding
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **mld proxying forwarding** to enable a non-querier downstream interface to forward multicast traffic.

Use **undo mld proxying forwarding** to disable the forwarding capability of a non-querier downstream interface.

By default, a non-querier downstream interface does not forward multicast traffic.

Examples

Enable the multicast forwarding capability on VLAN-interface 100, a non-querier downstream interface on the MLD proxy device.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld proxying forwarding
```

mld require-router-alert

Syntax

mld require-router-alert

undo mld require-router-alert

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **mld require-router-alert** to configure the interface to discard MLD messages without the Router-Alert option.

Use **undo mld require-router-alert** to restore the default.

By default, the device does not check the Router-Alert option. That is, it forwards all received MLD messages to the upper layer protocol for processing.

Related commands: **mld send-router-alert** and **require-router-alert**.

Examples

Configure VLAN-interface 100 to discard MLD messages without the Router-Alert option.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld require-router-alert
```


mld robust-count

Syntax

mld robust-count *robust-value*

undo mld robust-count

View

Interface view

Default level

2: System level

Parameters

robust-value: Specifies an MLD querier's robustness variable, in the range of 2 to 5.

Description

Use **mld robust-count** to configure the MLD querier's robustness variable on the current interface.

Use **undo mld robust-count** to restore the default.

By default, the MLD querier's robustness variable is 2.

The MLD querier's robustness variable defines the maximum number of attempts for transmitting MLD general queries, multicast-address-specific queries, or multicast-address-and-source-specific queries in case of packet loss because of network problems. A greater value of the robustness variable makes the MLD querier "more robust", but results in a longer IPv6 multicast group timeout time.

The MLD querier's robustness variable determines the following values:

- The default number of MLD general queries the MLDv1/v2 querier sends on startup.
- The number of multicast-address-specific queries the MLDv1 querier sends after receiving an MLD done message.
- The number of multicast-address-and-source-specific queries the MLDv2 querier sends after receiving an MLD report that tells relation changes between IPv6 multicast groups and IPv6 multicast sources.

Related commands: **display mld interface**, **mld last-listener-query-interval**, **mld startup-query-count**, **mld timer other-querier-present**, **mld timer query**, and **robust-count**.

Examples

```
# Set the MLD querier's robustness variable to 3 on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld robust-count 3
```

mld send-router-alert

Syntax

mld send-router-alert

undo mld send-router-alert

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **mld send-router-alert** to enable insertion of the Router-Alert option into MLD messages to be sent from the current interface.

Use **undo mld send-router-alert** to disable insertion of the Router-Alert option into MLD messages to be sent from the current interface.

By default, MLD messages carry the Router-Alert option.

Related commands: **mld require-router-alert** and **send-router-alert**.

Examples

```
# Disable insertion of the Router-Alert option into MLD messages to be sent from VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo mld send-router-alert
```

mld ssm-mapping enable

Syntax

mld ssm-mapping enable

undo mld ssm-mapping enable

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **mld ssm-mapping enable** to enable the MLD SSM mapping feature on the current interface.

Use **undo mld ssm-mapping enable** to disable the MLD SSM mapping feature on the current interface.

By default, the MLD SSM mapping feature is disabled on all interfaces.

Examples

```
# Enable the MLD SSM mapping feature on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld ssm-mapping enable
```

mld startup-query-count

Syntax

mld startup-query-count *value*

undo mld startup-query-count

View

Interface view

Default level

2: System level

Parameters

value: Specifies a startup query count, namely, the number of queries that the MLD querier sends on startup, in the range of 2 to 5.

Description

Use **mld startup-query-count** to configure the startup query count on the current interface.

Use **undo mld startup-query-count** to restore the default.

By default, the startup query count is set to the MLD querier's robustness variable.

Related commands: **mld robust-count** and **startup-query-count**.

Examples

```
# Set the startup query count to 3 on VLAN-interface 100.
```

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

```
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] mld startup-query-count 3
```

mld startup-query-interval

Syntax

mld startup-query-interval *interval*

undo mld startup-query-interval

View

Interface view

Default level

2: System level

Parameters

interval: Specifies a startup query interval in seconds, namely, the interval between general queries that the MLD querier sends on startup, in the range of 1 to 18000.

Description

Use **mld startup-query-interval** to configure the startup query interval on the current interface.

Use **undo mld startup-query-interval** to restore the default.

By default, the startup query interval is 1/4 of the MLD query interval.

Related commands: **mld timer query** and **startup-query-interval**.

Examples

```
# Set the startup query interval to 5 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld startup-query-interval 5
```

mld static-group

Syntax

```
mld static-group ipv6-group-address [ source ipv6-source-address ]
undo mld static-group { all | ipv6-group-address [ source ipv6-source-address ] }
```

View

Interface view

Default level

2: System level

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

ipv6-source-address: IPv6 address of the specified multicast source.

all: Removes all static IPv6 multicast groups that the current interface has joined.

Description

Use **mld static-group** to configure the current interface to be a statically-connected member of the specified IPv6 multicast group or IPv6 multicast source and group.

Use **undo mld static-group** to remove the configuration.

By default, an interface is not a statically-connected member of any IPv6 multicast group or IPv6 multicast source and group.

If the IPv6 multicast address is in the SSM multicast address range, you must specify an IPv6 multicast source address at the same time. Otherwise MLD routing table entries cannot be established. No such a restriction exists if the specified IPv6 multicast group address is not in the SSM multicast address range.

To configure a VLAN interface as a static member of an IPv6 multicast group or IPv6 multicast source and group, execute the **mld static-group** command on the VLAN interface, and configure the **mld-snooping static-group** command on the member ports of the corresponding VLAN.

Related commands: **mld-snooping static-group**.

Examples

```
# Configure VLAN-interface 100 to be a statically-connected member of the IPv6 multicast group FF03::101.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld static-group ff03::101
```

```
# Configure VLAN-interface 100 to be a statically connected member of multicast source and group (2001::101, FF3E::202).
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld static-group ff3e::202 source 2001::101
```

mld timer other-querier-present

Syntax

```
mld timer other-querier-present interval
undo mld timer other-querier-present
```

View

Interface view

Default level

2: System level

Parameters

interval: Specifies an MLD other querier present interval in seconds, in the range of 60 to 300.

Description

Use **mld timer other-querier-present** to configure the MLD other querier present interval on the current interface.

Use **undo mld timer other-querier-present** to restore the default.

By default, MLD other querier present interval = [MLD query interval] × [MLD querier's robustness variable] + [maximum response delay for MLD general queries] / 2.

Related commands: **display mld interface**, **mld max-response-time**, **mld robust-count**, **mld timer query**, and **timer other-querier-present**.

Examples

```
# Set the MLD other querier present interval to 200 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface100
[Sysname-Vlan-interface100] mld timer other-querier-present 200
```

mld timer query

Syntax

```
mld timer query interval
undo mld timer query
```

View

Interface view

Default level

2: System level

Parameters

interval: Specifies an MLD query interval, namely, the amount of time in seconds between MLD general query messages, in the range of 1 to 18,000.

Description

Use **mld timer query** to configure the MLD query interval on the current interface.

Use **undo mld timer query** to restore the default.

By default, the MLD query interval is 125 seconds.

Related commands: **display mld interface**, **mld timer other-querier-present**, and **timer query**.

Examples

```
# Set the MLD query interval to 200 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld timer query 200
```

mld version

Syntax

```
mld version version-number
```

```
undo mld version
```

View

Interface view

Default level

2: System level

Parameters

version-number: MLD version, 1 or 2.

Description

Use **mld version** to configure the MLD version on the current interface.

Use **undo mld version** to restore the default MLD version.

By default, the MLD version is MLDv1.

Related commands: **version**.

Examples

```
# Set the MLD version to MLDv2 on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld version 2
```

require-router-alert (MLD view)

Syntax

```
require-router-alert
```

undo require-router-alert

View

MLD view

Default level

2: System level

Parameters

None

Description

Use **require-router-alert** to globally configure the device to discard MLD messages without the Router-Alert option.

Use **undo require-router-alert** to restore the default.

By default, the device does not check the Router-Alert option. That is, it forwards all received MLD messages to the upper layer protocol for processing.

Related commands: **mld require-router-alert** and **send-router-alert**.

Examples

```
# Configure the device to discard MLD messages without the Router-Alert option.
```

```
<Sysname> system-view  
[Sysname] mld  
[Sysname-mld] require-router-alert
```

reset mld group

Syntax

```
reset mld group { all | interface interface-type interface-number { all | ipv6-group-address [ prefix-length ]  
[ ipv6-source-address [ prefix-length ] ] }
```

View

User view

Default level

2: System level

Parameters

all: The first **all** specifies all interfaces, and the second **all** specifies all MLD groups.

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

ipv6-group-address: Specifies an IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number ranging from 0 to F.

ipv6-source-address: Specifies an IPv6 multicast source address.

prefix-length: Specifies the Prefix length of the specified multicast source or multicast group. For a multicast source address, this argument has an effective value range of 0 to 128. For a multicast group address, it has an effective value range of 8 to 128. The default is 128 in both cases.

Description

Use **reset mld group** to remove the dynamic group entries of the specified MLD groups.

This command cannot remove the static group entries of MLD groups.

Related commands: **display mld group**.

Examples

Remove the dynamic MLD group entries on all interfaces.

```
<Sysname> reset mld group all
```

Remove the dynamic MLD group entries on VLAN-interface 100.

```
<Sysname> reset mld group interface vlan-interface 100 all
```

Remove the dynamic group entry for MLD group FF03::101:10 on VLAN-interface 100.

```
<Sysname> reset mld group interface vlan-interface 100 ff03::101:10
```

reset mld group port-info

Syntax

```
reset mld group port-info { all | ipv6-group-address } [ vlan vlan-id ]
```

View

User view

Default level

2: System level

Parameters

all: Specifies all IPv6 multicast groups.

ipv6-group-address: Specifies an IPV6 multicast group. The value range of *group-address* is FFxy::/16, where x and y represent any hexadecimal number between 0 and F, inclusive.

vlan-id: Specifies a VLAN. The value range of *vlan-id* is 1 to 4094.

Description

Use **reset mld group port-info** to remove the dynamic Layer 2 port entries of the specified MLD groups.

Layer 2 ports for MLD groups include member ports and router ports.

This command cannot remove static Layer 2 port entries of MLD groups.

Related commands: **display mld group port-info**.

Examples

Remove the dynamic Layer 2 port entries of all MLD groups in all VLANs.

```
<Sysname> reset mld group port-info all
```

Remove the dynamic Layer 2 port entries of all MLD groups in VLAN 100.

```
<Sysname> reset mld group port-info all vlan 100
```

Remove the dynamic Layer 2 port entry for the multicast group FF03::101:10 in VLAN 100.

```
<Sysname> reset mld group port-info ff03::101:10 vlan 100
```


reset mld ssm-mapping group

Syntax

```
reset mld ssm-mapping group { all | interface interface-type interface-number { all | ipv6-group-address [ prefix-length ] [ ipv6-source-address [ prefix-length ] ] } }
```

View

User view

Default level

2: System level

Parameters

all: The first **all** specifies to clear IPv6 multicast group information created based on the configured MLD SSM mappings on all interfaces, and the second **all** specifies to clear all IPv6 multicast group information created based on the configured MLD SSM mappings.

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

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address, in the form of FFxy::/16, where x and y represent any hexadecimal number ranging from 0 to F.

ipv6-source-address: Specifies a multicast source by its IPv6 address.

prefix-length: Prefix length of the multicast source or multicast group address. For a multicast source address, this argument has an effective value range of 0 to 128. For a multicast group address, it has an effective value range of 8 to 128. The default is 128 in both cases.

Description

Use **reset mld ssm-mapping group** to clear IPv6 multicast group information created based on the configured MLD SSM mappings.

Related commands: **display mld ssm-mapping group**.

Examples

```
# Clear all IPv6 multicast group information created based on the configured MLD SSM mappings on all interfaces.
```

```
<Sysname> reset mld ssm-mapping group all
```

robust-count (MLD view)

Syntax

```
robust-count robust-value
```

```
undo robust-count
```

View

MLD view

Default level

2: System level

Parameters

robust-value: Specifies an MLD querier's robustness variable, in the range of 2 to 5.

Description

Use **robust-count** to configure the MLD querier's robustness variable globally.

Use **undo robust-count** to restore the default.

By default, the MLD querier's robustness variable is 2.

The MLD querier's robustness variable defines the maximum number of attempts for transmitting MLD general queries, multicast-address-specific queries, or multicast-address-and-source-specific queries in case of packet loss because of network problems. A greater value of the robustness variable makes the MLD querier "more robust", but results in a longer IPv6 multicast group timeout time.

The MLD querier's robustness variable determines the following values:

- The default number of MLD general queries that the MLDv1/v2 querier sends on startup.
- The number of multicast-address-specific queries that the MLDv1 querier sends after receiving an MLD done message.
- The number of multicast-address-and-source-specific queries that the MLDv2 querier sends after receiving an MLD report that tells relation changes between IPv6 multicast groups and IPv6 multicast sources.

Related commands: **display mld interface**, **last-listener-query-interval**, **mld robust-count**, **startup-query-count**, **timer other-querier-present**, and **timer query**.

Examples

```
# Set the MLD querier's robustness variable to 3 globally.
```

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] robust-count 3
```

send-router-alert (MLD view)

Syntax

send-router-alert

undo send-router-alert

View

MLD view

Default level

2: System level

Parameters

None

Description

Use **send-router-alert** to globally enable the insertion of the Router-Alert option into MLD messages to be sent.

Use **undo send-router-alert** to globally disable the insertion of the Router-Alert option into MLD messages to be sent.

By default, MLD messages carry the Router-Alert option.

Related commands: **mld send-router-alert** and **require-router-alert**.

Examples

```
# Disable insertion of the Router-Alert option into MLD messages to be sent.
<Sysname> system-view
[Sysname] mld
[Sysname-mld] undo send-router-alert
```

ssm-mapping (MLD view)

Syntax

```
ssm-mapping ipv6-group-address prefix-length ipv6-source-address
undo ssm-mapping { ipv6-group-address prefix-length ipv6-source-address | all }
```

View

MLD view

Default level

2: System level

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address, in the form of FFxy::/16, where x and y represent any hexadecimal number ranging from 0 to F.

prefix-length: Specifies the Prefix length of the IPv6 multicast group address, in the range of 8 to 128.

ipv6-source-address: Specifies a multicast source by its IPv6 address.

all: Removes all MLD SSM mappings.

Description

Use **ssm-mapping** to configure an MLD SSM mapping.

Use **undo ssm-mapping** to remove one or all MLD SSM mappings.

By default, no MLD SSM mappings are configured.

Related commands: **display mld ssm-mapping** and **mld ssm-mapping enable**.

Examples

```
# Configure an MLD SSM mapping for multicast groups in the range of FF1E::/64 and multicast source 1::1.
<Sysname> system-view
[Sysname] mld
[Sysname-mld] ssm-mapping ff1e:: 64 1::1
```

startup-query-count (MLD view)

Syntax

```
startup-query-count value
undo startup-query-count
```

View

MLD view

Default level

2: System level

Parameters

value: Specifies a startup query count, namely, the number of queries that the MLD querier sends on startup, in the range of 2 to 5.

Description

Use **startup-query-count** to configure the startup query count globally.

Use **undo startup-query-count** to restore the default.

By default, the startup query count is set to the MLD querier's robustness variable.

Related commands: **mld startup-query-count** and **robust-count**.

Examples

```
# Set the startup query count to 3 globally.
<Sysname> system-view
[Sysname] mld
[Sysname-mlld] startup-query-count 3
```

startup-query-interval (MLD view)

Syntax

startup-query-interval *interval*

undo startup-query-interval

View

MLD view

Default level

2: System level

Parameters

interval: Specifies a startup query interval in seconds, namely, the interval between general queries that the MLD querier sends on startup, in the range of 1 to 18000.

Description

Use **startup-query-interval** to configure the startup query interval globally.

Use **undo startup-query-interval** to restore the default.

By default, the startup query interval is 1/4 of the "MLD query interval".

Related commands: **mld startup-query-interval** and **timer query**.

Examples

```
# Set the startup query interval to 5 seconds globally.
<Sysname> system-view
[Sysname] mld
[Sysname-mlld] startup-query-interval 5
```

timer other-querier-present (MLD view)

Syntax

```
timer other-querier-present interval  
undo timer other-querier-present
```

View

MLD view

Default level

2: System level

Parameters

interval: Specifies an MLD other querier present interval in seconds, in the range of 60 to 300.

Description

Use **timer other-querier-present** to configure the MLD other querier present interval globally.

Use **undo timer other-querier-present** to restore the default.

By default, MLD other querier present interval = [MLD query interval] × [MLD querier's robustness variable] + [maximum response delay for MLD general queries] / 2.

Related commands: **display mld interface**, **max-response-time**, **mld timer other-querier-present**, **robust-count**, and **timer query**.

Examples

```
# Set the MLD other querier present interval to 200 seconds globally.  
<Sysname> system-view  
[Sysname] mld  
[Sysname-mld] timer other-querier-present 200
```

timer query (MLD view)

Syntax

```
timer query interval  
undo timer query
```

View

MLD view

Default level

2: System level

Parameters

interval: Specifies an MLD query interval, namely, amount of time in seconds between MLD general queries, in the range of 1 to 18,000.

Description

Use **timer query** to configure the MLD query interval globally.

Use **undo timer query** to restore the default.

By default, the MLD query interval is 125 seconds.

Related commands: **display mld interface**, **mld timer query**, and **timer other-querier-present**.

Examples

```
# Set the MLD query interval to 200 seconds globally.
<Sysname> system-view
[Sysname] mld
[Sysname-mld] timer query 200
```

version (MLD view)

Syntax

version *version-number*

undo version

View

MLD view

Default level

2: System level

Parameters

version-number: Specifies an MLD version number, 1 or 2.

Description

Use **version** to configure the MLD version globally.

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

By default, the MLD version is MLDv1.

Related commands: **mld version**.

Examples

```
# Set the MLD version to MLDv2 globally.
<Sysname> system-view
[Sysname] mld
[Sysname-mld] version 2
```

IPv6 PIM configuration commands (available only on the HP 5500 EI)

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

The term "interface" in this chapter collectively refers to Layer 3 interfaces, including VLAN 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*).

bidir-pim enable (IPv6 PIM view)

Syntax

```
bidir-pim enable  
undo bidir-pim enable
```

View

IPv6 PIM view

Default level

2: System level

Parameters

None

Description

Use **bidir-pim enable** to enable IPv6 BIDIR-PIM.

Use **undo bidir-pim enable** to disable IPv6 BIDIR-PIM.

By default, IPv6 BIDIR-PIM is disabled.

This command is effective only after IPv6 multicast routing is enabled.

Related commands: **multicast ipv6 routing-enable** and **pim ipv6**.

Examples

```
# Enable IPv6 multicast routing, enter IPv6 PIM view, and enable IPv6 BIDIR-PIM.
```

```
<Sysname> system-view  
[Sysname] multicast ipv6 routing-enable  
[Sysname] pim ipv6  
[Sysname-pim6] bidir-pim enable
```

bsm-fragment enable (IPv6 PIM view)

Syntax

```
bsm-fragment enable  
undo bsm-fragment enable
```

View

IPv6 PIM view

Default level

2: System level

Parameters

None

Description

Use **bsm-fragment enable** to enable bootstrap message (BSM) semantic fragmentation.

Use **undo bsm-fragment enable** to disable BSM semantic fragmentation.

By default, BSM semantic fragmentation is enabled.

The BSM semantic fragmentation function should be disabled if devices not supporting this function exist in the IPv6 PIM-SM domain.

Related commands: **c-bsr admin-scope**.

Examples

```
# Disable BSM semantic fragmentation in the public network.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] undo bsm-fragment enable
```

bsr-policy (IPv6 PIM view)

Syntax

```
bsr-policy acl6-number
undo bsr-policy
```

View

IPv6 PIM view

Default level

2: System level

Parameters

acl6-number: Basic IPv6 ACL number, in the range of 2000 to 2999. When an IPv6 ACL is defined, the **source** keyword in the **rule** command specifies a legal BSR source IPv6 address range.

Description

Use **bsr-policy** to configure a legal BSR address range to guard against BSR spoofing.

Use **undo bsr-policy** to remove the restriction of the BSR address range.

By default, no restrictions are defined for the BSR address range. Namely, the BSR messages from any source are considered eligible.

Examples

```
# Configure a legal BSR address range so that only devices on the segment 2001::2/64 can become the BSR.
<Sysname> system-view
```



```
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2001::2 64
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] bsr-policy 2000
```

c-bsr (IPv6 PIM view)

Syntax

```
c-bsr ipv6-address [ hash-length [ priority ] ]
undo c-bsr
```

View

IPv6 PIM view

Default level

2: System level

Parameters

ipv6-address: IPv6 address of the interface that will act as a C-BSR.

hash-length: Hash mask length, in the range of 0 to 128. If you do not specify this argument, the corresponding global setting is used.

priority: Priority of the C-BSR, in the range of 0 to 255. A larger value means a higher priority. If you do not specify this argument, the corresponding global setting is used.

Description

Use **c-bsr** to configure the specified interface as a C-BSR.

Use **undo c-bsr** to remove the related C-BSR configuration.

No C-BSR is configured by default.

You must enable IPv6 PIM-SM on the interface that you want to configure as a C-BSR.

Related commands: **c-bsr hash-length**, **c-bsr priority**, **c-rp**, and **pim ipv6 sm**.

Examples

```
# Configure the interface with an IPv6 address of 1101::1 as a C-BSR.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr 1101::1
```

c-bsr admin-scope (IPv6 PIM view)

Syntax

```
c-bsr admin-scope
undo c-bsr admin-scope
```

View

IPv6 PIM view

Default level

2: System level

Parameters

None

Description

Use **c-bsr admin-scope** to enable IPv6 administrative scoping.

Use **undo c-bsr admin-scope** to disable IPv6 administrative scoping.

IPv6 administrative scoping is disabled by default.

Related commands: **c-bsr** and **c-bsr scope**.

Examples

```
# Enable IPv6 administrative scoping.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr admin-scope
```

c-bsr hash-length (IPv6 PIM view)

Syntax

c-bsr hash-length *hash-length*

undo c-bsr hash-length

View

IPv6 PIM view

Default level

2: System level

Parameters

hash-length: Hash mask length, in the range of 0 to 128.

Description

Use **c-bsr hash-length** to configure the global hash mask length.

Use **undo c-bsr hash-length** to restore the default.

By default, the hash mask length is 126.

Related commands: **c-bsr**.

Examples

```
# Set the global hash mask length to 16.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr hash-length 16
```

c-bsr holdtime (IPv6 PIM view)

Syntax

```
c-bsr holdtime interval  
undo c-bsr holdtime
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: BS timeout in seconds, in the range of 1 to 2,147,483,647.

Description

Use **c-bsr holdtime** to configure the BS timeout, namely, the length of time that the C-BSRs wait for a bootstrap message from the BSR.

Use **undo c-bsr holdtime** to restore the default.

By default, the BS timeout value is determined by this formula: BS timeout = BS period × 2 + 10.

The default BS period is 60 seconds, so the default BS timeout is 60 × 2 + 10 = 130 (seconds).

Related commands: **c-bsr** and **c-bsr interval**.

Examples

```
# Set the BS timeout to 150 seconds.  
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] c-bsr holdtime 150
```

c-bsr interval (IPv6 PIM view)

Syntax

```
c-bsr interval interval  
undo c-bsr interval
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: BS period in seconds, with an effective range of 10 to 2,147,483,647.

Description

Use **c-bsr interval** to configure the BS period, namely, the interval at which the BSR sends bootstrap messages.

Use **undo c-bsr interval** to restore the default.

By default, the BS period value is determined by this formula: $BS\ period = (BS\ timeout - 10) / 2$.
The default BS timeout is 130 seconds, so the default BS period is $(130 - 10) / 2 = 60$ (seconds).

Related commands: **c-bsr** and **c-bsr holdtime**.

Examples

```
# Set the BS period to 30 seconds.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr interval 30
```

c-bsr priority (IPv6 PIM view)

Syntax

```
c-bsr priority priority
undo c-bsr priority
```

View

IPv6 PIM view

Default level

2: System level

Parameters

priority: Priority of the C-BSR, in the range of 0 to 255. A larger value means a higher priority.

Description

Use **c-bsr priority** to configure the global C-BSR priority.

Use **undo c-bsr priority** to restore the default.

By default, the C-BSR priority is 64.

Related commands: **c-bsr**.

Examples

```
# Set the global C-BSR priority to 5.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr priority 5
```

c-bsr scope

Syntax

```
c-bsr scope { scope-id | admin-local | global | organization-local | site-local } [ hash-length hash-length | priority priority ] *
undo c-bsr scope { scope-id | admin-local | global | organization-local | site-local }
```

View

IPv6 PIM view

Default level

2: System level

Parameters

scope-id: Specifies the value of the scope field, in the range of 3 to 15.

admin-local: Specifies the scope field value as admin-local, which has a scope value of 4.

global: Specifies the scope field value as global, which has a scope value of 14.

organization-local: Specifies the scope field value as organization-local, which has a scope value of 8.

site-local: Specifies the scope field value as site-local, which has a scope value of 5.

hash-length: Specifies the hash mask length of the IPv6 admin-scope zone indicated by the scope value, in the range of 0 to 128. If you do not specify this argument, the corresponding global setting is used.

priority: Specifies the priority of the C-BSR in the IPv6 admin-scope zone indicated by the scope value, in the range of 0 to 255. A larger value means a higher priority. If you do not specify this argument, the corresponding global setting is used.

Description

Use **c-bsr scope** to configure the C-BSR in the IPv6 admin-scope zone.

Use **undo c-bsr scope** to remove the C-BSR configuration.

Related commands: **c-bsr admin-scope**, **c-bsr hash-length**, and **c-bsr priority**.

Examples

Configure local device as the C-BSR of the IPv6 admin-scope zone with a scope value of 14 and set the C-BSR priority to 10.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr scope global priority 10
```

c-rp (IPv6 PIM view)

Syntax

c-rp *ipv6-address* [{ **group-policy** *acl6-number* | **scope** *scope-id* } | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] * [**bidir**]

undo c-rp *ipv6-address*

View

IPv6 PIM view

Default level

2: System level

Parameters

ipv6-address: Specifies the IPv6 address of the interface that will act as a C-RP.

acl6-number: Specifies a basic IPv6 ACL number, in the range of 2000 to 2999. This IPv6 ACL defines a range of IPv6 multicast groups to which the C-RP is designated, rather than defining a filtering rule. Any IPv6 multicast group range that matches the **permit** statement in the ACL is advertised as a group to which the RP is designated, but the configuration that matches other statements, like **deny**, does not take effect.

scope-id: Specifies the value of the scope field, in the range of 3 to 15.

priority: Specifies the priority of the C-RP, in the range of 0 to 255 and defaulting to 192. A larger value means a lower priority.

hold-interval: Specifies the C-RP timeout time, in seconds. The value ranges from 1 to 65,535. If you do not specify this argument, the corresponding global setting is used.

adv-interval: Specifies the C-RP-Adv interval in seconds, with an effective range of 1 to 65,535. If you do not specify this argument, the corresponding global setting is used.

bidir: Configures the C-RP to provide services for multicast groups in the bidirectional PIM mode. If you do not specify this argument, the C-RP provides services for multicast groups in the IPv6 PIM-SM mode.

Description

Use **c-rp** to configure the specified interface as a C-RP.

Use **undo c-rp** to remove the related C-RP configuration.

No C-RPs are configured by default.

You must enable IPv6 PIM-SM on the interface that you want to configure as a C-RP.

If you do not specify an IPv6 multicast group range for the C-RP, the C-RP provides services for all IPv6 multicast groups in the IPv6 non-scoped zone, or it provides services for IPv6 multicast groups in the IPv6 global admin-scope zone if IPv6 administrative scoping is configured.

To configure a device as a C-RP for multiple group ranges, you must include these group ranges in multiple rules in the IPv6 ACL that corresponds to the **group-policy** keyword.

If you use this command repeatedly on the same interface, the last configuration takes effect.

Related commands: **c-bsr**.

Examples

```
# Configure the interface with the IPv6 address of 2001::1 to be a C-RP for IPv6 multicast group FFOE:0:1391::/96, with a priority of 10.
```

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff0e:0:1391:: 96
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] c-rp 2001::1 group-policy 2000 priority 10
```

c-rp advertisement-interval (IPv6 PIM view)

Syntax

```
c-rp advertisement-interval interval
```

```
undo c-rp advertisement-interval
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535.

Description

Use **c-rp advertisement-interval** to configure the interval at which C-RP-Adv messages are sent.

Use **undo c-rp advertisement-interval** to restore the default.

By default, the C-RP-Adv interval is 60 seconds.

Related commands: **c-rp**.

Examples

```
# Set the global C-RP-Adv interval to 30 seconds.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-rp advertisement-interval 30
```

c-rp holdtime (IPv6 PIM view)

Syntax

c-rp holdtime *interval*

undo c-rp holdtime

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: C-RP timeout in seconds, with an effective range of 1 to 65,535.

Description

Use **c-rp holdtime** to configure the global C-RP timeout time, namely, the length of time that the BSR waits for a C-RP-Adv message from C-RPs.

Use **undo c-rp holdtime** to restore the default.

By default, the C-RP timeout time is 150 seconds.

Because a non-BSR router refreshes its C-RP timeout time through bootstrap messages, to prevent loss of C-RP information in bootstrap messages, be sure that the C-RP timeout time is not smaller than the interval at which the BSR sends bootstrap messages. The recommended C-RP timeout setting is 2.5 times the BS period or longer.

Related commands: **c-bsr interval** and **c-rp**.

Examples

```
# Set the global C-RP timeout time to 200 seconds.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-rp holdtime 200
```

crp-policy (IPv6 PIM view)

Syntax

```
crp-policy acl6-number  
undo crp-policy
```

View

IPv6 PIM view

Default level

2: System level

Parameters

acl6-number: Advanced IPv6 ACL number, in the range of 3000 to 3999. When the IPv6 ACL is defined, the **source** keyword in the **rule** command specifies the IPv6 address of a C-RP, and the **destination** keyword specifies the IPv6 address range of the IPv6 multicast groups to which the C-RP is designated.

Description

Use **crp-policy** to configure a legal C-RP address range and the range of IPv6 multicast groups to which the C-RP is designated, in order to guard against C-RP spoofing.

Use **undo crp-policy** to remove the restrictions in C-RP address ranges and the ranges of IPv6 multicast groups to which the C-RP is designated.

By default, no restrictions are defined for C-RP address ranges and the address ranges of groups to which the C-RP is designated. All received C-RP messages are regarded legal.

The **crp-policy** command filters the IPv6 multicast group ranges advertised by C-RPs based on the group prefixes. For example, if the IPv6 multicast group range advertised by a C-RP is FF0E:0:1::/96 and the legal IPv6 multicast group range defined by the **crp-policy** command is FF0E:0:1::/120, the IPv6 multicast groups in the range of FF0E:0:1::/96 can pass.

Related commands: **c-rp**.

Examples

```
# Configure a C-RP policy so that only devices in the IPv6 address range of 2001::2/64 can be C-RPs  
that provides services for IPv6 multicast groups in the address range of FF03::101/64.
```

```
<Sysname> system-view  
[Sysname] acl ipv6 number 3000  
[Sysname-acl6-adv-3000] rule permit ipv6 source 2001::2 64 destination ff03::101 64  
[Sysname-acl6-adv-3000] quit  
[Sysname] pim ipv6  
[Sysname-pim6] crp-policy 3000
```

display pim ipv6 bsr-info

Syntax

```
display pim ipv6 bsr-info [ | { 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 pim ipv6 bsr-info** to display the BSR information in the IPv6 PIM domain and the locally configured C-RP information in effect.

Related commands: **c-bsr** and **c-rp**.

Examples

Display the BSR information in the IPv6 PIM-SM domain and the locally configured C-RP information in effect.

```
<Sysname> display pim ipv6 bsr-info
Elected BSR Address: 2004::2
  Priority: 64
  Hash mask length: 126
  State: Elected
  Scope: 14
  Uptime: 00:01:10
  Next BSR message scheduled at: 00:00:48
Candidate BSR Address: 2004::2
  Priority: 64
  Hash mask length: 126
  State: Elected
  Scope: 14

Candidate RP: 2001::1(LoopBack1)
  Priority: 192
  HoldTime: 130
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:48
Candidate RP: 2002::1(Vlan-interface1)
  Priority: 200
  HoldTime: 90
  Advertisement Interval: 50
  Next advertisement scheduled at: 00:00:28
Candidate RP: 2003::1(Vlan-interface2)
  Priority: 192
  HoldTime: 80
  Advertisement Interval: 60
```

Next advertisement scheduled at: 00:00:48

Table 78 Command output

Field	Description
Elected BSR Address	IPv6 address of the elected BSR
Candidate BSR Address	Address of the candidate BSR
Priority	BSR priority
Hash mask length	Hash mask length
State	BSR state
Scope	Scope of the BSR
Uptime	Length of time since this BSR was elected
Next BSR message scheduled at	Remaining time of this BSR
Candidate RP	Address of the C-RP
Priority	Priority of the C-RP
HoldTime	Timeout time of the C-RP
Advertisement Interval	Interval between C-RP-Adv messages
Next BSR message scheduled at	Remaining time before the C-RP will send the next C-RP-Adv message

display pim ipv6 claimed-route

Syntax

```
display pim ipv6 claimed-route [ ipv6-source-address ] [ | { begin | exclude | include }  
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-source-address: Displays the information of the IPv6 unicast route to a particular IPv6 multicast source. If you do not provide this argument, this command displays information about all IPv6 unicast routes that IPv6 PIM uses.

|: 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 pim ipv6 claimed-route** to display information about IPv6 unicast routes that IPv6 PIM uses. If an (S, G) is marked SPT, this (S, G) entry uses an IPv6 unicast route.

Examples

Display the information of all IPv6 unicast routes that IPv6 PIM uses.

```
<Sysname> display pim ipv6 claimed-route
RPF information about: 2001::2
  RPF interface: Vlan-interface1, RPF neighbor: FE80::A01:100:1
  Referenced prefix/prefix length: 2001::/64
  Referenced route type: igp
  RPF-route selecting rule: preference-preferred
  The (S, G) or (*, G) list dependent on this route entry
  (2001::2, FF03::101)
```

Table 79 Command output

Field	Description
RPF information about: 2001::2	Information of the RPF route to IPv6 multicast source 2001::2
RPF interface	RPF interface type and number
RPF neighbor	IPv6 address of the RPF neighbor
Referenced prefix/prefix length	Address/mask of the reference route
Referenced route type	Type of the referenced route: <ul style="list-style-type: none">• igp—IGP IPv6 unicast route• egp—EGP IPv6 unicast route• unicast (direct)—Direct IPv6 unicast route• unicast—Other IPv6 unicast route (such as IPv6 static unicast route)• mbgp—IPv6 MBGP route
RPF-route selecting rule	Rule of RPF route selection.
The (S,G) or (*,G) list dependent on this route entry	(S, G) or (*, G) entry list dependent on this RPF route

display pim ipv6 control-message counters

Syntax

```
display pim ipv6 control-message counters [ message-type { probe | register | register-stop } | [ interface interface-type interface-number | message-type { assert | bsr | crp | graft | graft-ack | hello | join-prune | state-refresh } ] * ] [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

probe: Displays the number of null register messages.

register: Displays the number of register messages.

register-stop: Displays the number of register-stop messages.

interface-type interface-number: Displays the number of IPv6 PIM control messages on the specified interface.

assert: Displays the number of assert messages.

bsr: Displays the number of bootstrap messages.

crp: Displays the number of C-RP-Adv messages.

graft: Displays the number of graft messages.

graft-ack: Displays the number of graft-ack messages.

hello: Displays the number of hello messages.

join-prune: Displays the number of join/prune messages.

state-refresh: Displays the number of state refresh messages.

|: 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 pim ipv6 control-message counters** to display statistics for IPv6 PIM control messages.

Examples

```
# Display statistics for all IPv6 PIM control messages on all interfaces.
```

```
<Sysname> display pim ipv6 control-message counters
PIM global control-message counters:

              Received          Sent              Invalid
Register      20                37                2
Register-Stop 25                20                1
Probe         10                 5                 0

PIM control-message counters for interface: Vlan-interfaces
              Received          Sent              Invalid
Assert        10                 5                 0
Graft         20                37                2
Graft-Ack     25                20                1
Hello         1232               453               0
Join/Prune    15                 30                21
State-Refresh 8                   7                 1
BSR           3243               589               1
C-RP          53                 32                0
```

Table 80 Command output

Field	Description
PIM global control-message counters	Statistics of IPv6 PIM global control messages
PIM control-message counters for interface	Interface for which IPv6 PIM control messages were counted
Received	Number of messages received
Sent	Number of messages sent
Invalid	Number of invalid messages
Register	Register messages
Register-Stop	Register-stop messages
Probe	Null register messages
Assert	Assert messages
Graft	Graft messages
Graft-Ack	Graft-ack messages
Hello	Hello messages
Join/Prune	Join/prune messages
State Refresh	State refresh messages
BSR	Bootstrap messages
C-RP	C-RP-Adv messages

display pim ipv6 df-info

Syntax

```
display pim ipv6 df-info [ rp-address ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

rp-address: Specifies the RP address of IPv6 BIDIR-PIM.

|: 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 the 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 pim ipv6 df-info** to display the DF information of IPv6 BIDIR-PIM.

Examples

Display the DF information of IPv6 BIDIR-PIM.

```
<Sysname> display pim ipv6 df-info
```

```
RP Address: 2010::1
```

Interface	State	DF-Pref	DF-Metric	DF-Uptime	DF-Address
Vlan1	Win	100	1	01:24:09	FE80::20F:E2FF: FE38:4E01 (local)
Vlan2	Win	100	1	01:24:09	FE80::200:5EFF: FE71:2801 (local)
Vlan3	Lose	0	0	01:23:12	FE80::20F:E2FF: FE15:5601

Table 81 Command output

Field	Description
RP Address	IPv6 BIDIR-PIM RP address
Interface	Interface type and number
State	DF election state: <ul style="list-style-type: none">• Win• Lose
DF-Pref	Route priority of DF
DF-Metric	Route metric of DF
DF-Uptime	Existence duration of DF
DF-Address	IPv6 address of DF, where "local" indicates a local IPv6 address

display pim ipv6 grafts

Syntax

```
display pim ipv6 grafts [ | { 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 pim ipv6 grafts** to display information about unacknowledged IPv6 PIM-DM graft messages.

Examples

```
# Display information about unacknowledged IPv6 PIM-DM graft messages.
```

```
<Sysname> display pim ipv6 grafts
Source           Group           Age             RetransmitIn
1004::2         ff03::101      00:00:24       00:00:02
```

Table 82 Command output

Field	Description
Source	IPv6 multicast source address in the graft message
Group	IPv6 multicast group address in the graft message
Age	Time in which the graft message will age out, in hours:minutes:seconds
RetransmitIn	Time in which the graft message will be retransmitted, in hours:minutes:seconds

display pim ipv6 interface

Syntax

```
display pim ipv6 interface [ interface-type interface-number ] [ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Displays the IPv6 PIM information on a particular interface.

verbose: Displays the detailed PIM 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 pim ipv6 interface** to display IPv6 PIM information on the specified interface or all interfaces.

Examples

```
# Display the detailed IPv6 PIM information on Vlan-interface1.
<Sysname> display pim ipv6 interface vlan-interface 1 verbose
Interface: Vlan-interface1, FE80::200:5EFF:FE04:8700
```

```

PIM version: 2
PIM mode: Sparse
PIM DR: FE80::200:AFF:FE01:101
PIM DR Priority (configured): 1
PIM neighbor count: 1
PIM hello interval: 30 s
PIM LAN delay (negotiated): 500 ms
PIM LAN delay (configured): 500 ms
PIM override interval (negotiated): 2500 ms
PIM override interval (configured): 2500 ms
PIM neighbor tracking (negotiated): disabled
PIM neighbor tracking (configured): disabled
PIM generation ID: 0xF5712241
PIM require generation ID: disabled
PIM hello hold interval: 105 s
PIM assert hold interval: 180 s
PIM triggered hello delay: 5 s
PIM J/P interval: 60 s
PIM J/P hold interval: 210 s
PIM BSR domain border: disabled
Number of routers on network not using DR priority: 0
Number of routers on network not using LAN delay: 0
Number of routers on network not using neighbor tracking: 2

```

Table 83 Command output

Field	Description
Interface	Interface name and its IPv6 address
PIM version	IPv6 PIM version
PIM mode	IPv6 PIM mode, dense or sparse
PIM DR	IPv6 address of the DR
PIM DR Priority (configured)	Priority for DR election
PIM neighbor count	Total number of IPv6 PIM neighbors
PIM hello interval	Interval between IPv6 PIM hello messages
PIM LAN delay (negotiated)	Negotiated prune message delay
PIM LAN delay (configured)	Configured prune message delay
PIM override interval (negotiated)	Negotiated prune override interval
PIM override interval (configured)	Configured prune override interval
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status (enabled/disabled)
PIM neighbor tracking (configured)	Configured neighbor tracking status (enabled/disabled)
PIM generation ID	Generation_ID value
PIM require generation ID	Rejection of hello messages without Generation_ID (enabled/disabled)

Field	Description
PIM hello hold interval	IPv6 PIM neighbor timeout time.
PIM assert hold interval	Assert timeout time.
PIM triggered hello delay	Maximum delay of sending hello messages.
PIM J/P interval	Join/prune interval.
PIM J/P hold interval	Join/prune timeout time.
PIM BSR domain border	Status of PIM domain border configuration (enabled/disabled).
Number of routers on network not using DR priority	Number of routers not using the DR priority field on the subnet where the interface resides.
Number of routers on network not using LAN delay	Number of routers not using the LAN delay field on the subnet where the interface resides.
Number of routers on network not using neighbor tracking	Number of routers not using neighbor tracking on the subnet where the interface resides.

display pim ipv6 join-prune

Syntax

```
display pim ipv6 join-prune mode { sm [ flags flag-value ] | ssm } [ interface interface-type
interface-number | neighbor ipv6-neighbor-address ] * [ verbose ] [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

mode: Displays the information of join/prune messages to send in the specified IPv6 PIM mode. IPv6 PIM modes include **sm** and **ssm**, which represent IPv6 PIM-SM and IPv6 PIM-SSM respectively.

flags flag-value: Displays IPv6 PIM routing entries that contain the specified flags. Values and meanings of *flag-value* are as follows:

- **rpt:** Specifies routing entries on the RPT.
- **spt:** Specifies routing entries on the SPT.
- **wc:** Specifies wildcard routing entries.

interface-type interface-number: Displays the information of join/prune messages to send on the specified interface.

ipv6-neighbor-address: Displays the information of join/prune messages to send to the specified IPv6 PIM neighbor.

verbose: Displays the detailed information of join/prune messages to send.

|: 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 pim ipv6 join-prune** to display information about the join/prune messages to send.

Examples

```
# Display the information of join/prune messages to send in the IPv6 PIM-SM mode.
```

```
<Sysname> display pim ipv6 join-prune mode sm
```

```
Expiry Time: 50 sec
```

```
Upstream nbr: FE80::2E0:FCFF:FE03:1004 (Vlan-interface1)
```

```
1 (*, G) join(s), 0 (S, G) join(s), 1 (S, G, rpt) prune(s)
```

```
-----  
Total (*, G) join(s): 1, (S, G) join(s): 0, (S, G, rpt) prune(s): 1
```

Table 84 Command output

Field	Description
Expiry Time:	Expiry time of sending join/prune messages
Upstream nbr:	IPv6 address of the upstream IPv6 PIM neighbor and the interface that connects to it
(*, G) join(s)	Number of (*, G) joins to send
(S, G) join(s)	Number of (S, G) joins to send
(S, G, rpt) prune(s)	Number of (S, G, rpt) prunes

display pim ipv6 neighbor

Syntax

```
display pim ipv6 neighbor [ interface interface-type interface-number | ipv6-neighbor-address | verbose ] * [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Displays the IPv6 PIM neighbor information on a particular interface.

ipv6-neighbor-address: Displays the information of a particular IPv6 PIM neighbor.

verbose: Displays the detailed IPv6 PIM neighbor 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 pim ipv6 neighbor** to display IPv6 PIM neighbor information.

Examples

```
# Display the information of all IPv6 PIM neighbors.
```

```
<Sysname> display pim ipv6 neighbor
Total Number of Neighbors = 2
```

Neighbor	Interface	Uptime	Expires	Dr-Priority	Mode
FE80::A01:101:1	Vlan1	02:50:49	00:01:31	1	B
FE80::A01:102:1	Vlan2	02:49:39	00:01:42	1	B

```
# Display the detailed information of the IPv6 PIM neighbor whose IPv6 address is FE80::A01:101:1.
```

```
<Sysname> display pim ipv6 neighbor fe80::a01:101:1 verbose
```

```
Neighbor: FE80::A01:101:1
  Interface: Vlan-interface3
  Uptime: 00:00:10
  Expiry time: 00:00:30
  DR Priority: 1
  Generation ID: 0x2ACEFE15
  Holdtime: 105 s
  LAN delay: 500 ms
  Override interval: 2500 ms
  State refresh interval: 60 s
  Neighbor tracking: Disabled
  Bidirectional PIM: Disabled
  Neighbor Secondary Address(es):
  1::1
```

Table 85 Command output

Field	Description
Total Number of Neighbors	Total number of IPv6 PIM neighbors.
Neighbor	Primary IPv6 address of the PIM neighbor (link-local address).
Interface	Interface that connects to the IPv6 PIM neighbor.
Uptime	Length of time since the IPv6 PIM neighbor was discovered.
Expires/Expiry time	Remaining time of the IPv6 PIM neighbor. "Never" means that the IPv6 PIM neighbor is always up and reachable.
Dr-Priority/DR Priority	Priority of the IPv6 PIM neighbor.
Mode	Mode of the IPv6 PIM neighbor, where B means IPv6 BIDIR-PIM mode, and if nothing is displayed, it means non-IPv6 BIDIR-PIM mode.
Generation ID	Generation ID of the IPv6 PIM neighbor. (A random value that indicates status change of the IPv6 PIM neighbor.)

Field	Description
Holdtime	Hold time of the IPv6 PIM neighbor; "forever" means that the IPv6 PIM neighbor is always up and reachable.
LAN delay	Prune message delay.
Override interval	Prune override interval.
State refresh interval	Interval for sending state refresh messages. Displayed only when the IPv6 PIM neighbor works in IPv6 PIM_DM mode and state refresh capability is enabled.
Neighbor tracking	Neighbor tracking status (enabled/disabled).
Bidirectional PIM	IPv6 BIDIR-PIM status (enabled/disabled).
Neighbor Secondary Address(es)	Secondary IPv6 address of the PIM neighbor (non-link-local address).

display pim ipv6 routing-table

Syntax

```
display pim ipv6 routing-table [ ipv6-group-address [ prefix-length ] | ipv6-source-address
[ prefix-length ] | incoming-interface [ interface-type interface-number | register ] | outgoing-interface
{ include | exclude | match } { interface-type interface-number | register } | mode mode-type | flags
flag-value | fsm ] * [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its address, in the range of FFxy::/16, where x and y represent any hexadecimal number between 0 and F, inclusive.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address.

prefix-length: Specifies the prefix length of the IPv6 multicast group/source address prefix. For an IPv6 multicast group address, the effective range is 8 to 128 and the default value is 128. For an IPv6 multicast source address, the effective range is 0 to 128 and the default value is 128.

incoming-interface: Displays routing entries that contain the specified interface as the incoming interface.

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

register: Specifies the register interface. This keyword is valid only if *mode-type* is not specified or is **sm**.

outgoing-interface: Displays routing entries that contain the specified interface as the outgoing interface.

include: Displays routing entries, where the outgoing interface list includes the specified interface.

exclude: Displays routing entries, where the outgoing interface list excludes the specified interface.

match: Displays routing entries, where the outgoing interface list includes only the specified interface.

mode mode-type: Specifies an IPv6 PIM mode, where *mode-type* can have the following values:

- **dm**: Specifies IPv6 PIM-DM.
- **sm**: Specifies IPv6 PIM-SM.
- **ssm**: Specifies IPv6 PIM-SSM.

flags *flag-value*: Displays IPv6 PIM routing entries that contain the specified flags. The values of *flag-value* and their meanings are as follows:

- **act**: Specifies IPv6 multicast routing entries that have been used for routing data.
- **bidir**: Specifies IPv6 multicast routing entries created by IPv6 BIDIR-PIM.
- **del**: Specifies IPv6 multicast routing entries scheduled to be deleted.
- **exprune**: Specifies multicast routing entries that contain outgoing interfaces pruned by other IPv6 multicast routing protocols.
- **ext**: Specifies IPv6 routing entries that contain outgoing interfaces provided by other IPv6 multicast routing protocols.
- **loc**: Specifies IPv6 multicast routing entries on that devices that directly connect to the same subnet as the IPv6 multicast source.
- **niif**: Specifies IPv6 multicast routing entries that contain unknown incoming interfaces.
- **nonbr**: Specifies routing entries with IPv6 PIM neighbor searching failure.
- **rpt**: Specifies routing entries on RPT branches where (S, G) prunes have been sent to the RP.
- **spt**: Specifies routing entries on the SPT.
- **swt**: Specifies routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies wildcard routing entries.

fsm: Displays the information of the state machine.

|: 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 pim ipv6 routing-table** to display IPv6 PIM routing table information.

Related commands: **display ipv6 multicast routing-table**.

Examples

Display the content of the IPv6 PIM routing table.

```
<Sysname> display pim ipv6 routing-table
Total 0 (*, G) entry; 1 (S, G) entry
```

```
(2001::2, FFE3::101)
  RP: FE80::A01:100:1
  Protocol: pim-sm, Flag: SPT LOC ACT
  UpTime: 02:54:43
  Upstream interface: Vlan-interface1
  Upstream neighbor: NULL
```

```

    RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
    1: Vlan-interface2
        Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
# Display the state machine information of the IPv6 PIM routing table.
<Sysname> display pim ipv6 routing-table fsm
Total 0 (*, G) entry; 1 (S, G) entry

Abbreviations for FSM states:
NI - no info, J - joined, NJ - not joined, P - pruned,
NP - not pruned, PP - prune pending, W - winner, L - loser,
F - forwarding, AP - ack pending, DR - designated router,
NDR - non-designated router, RCV - downstream receivers

(2001::2, FFE3::101)
RP: FE80::A01:100:1
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 02:54:43
Upstream interface: Vlan-interface1
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
    Join/Prune FSM: [SPT: J] [RPT: NP]
Downstream interface(s) information:
Total number of downstreams: 1
    1: Vlan-interface2
        Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
        DR state: [DR]
        Join/Prune FSM: [NI]
        Assert FSM: [NI]

FSM information for non-downstream interfaces: None

```

Table 86 Command output

Field	Description
Total 0 (*, G) entry; 1 (S, G) entry	Number of (S, G) and (*, G) entries in the IPv6 PIM routing table.
(2001::2, FFE3::101)	(S, G) entry in the IPv6 PIM routing table.
RP	IP address of the RP.
Protocol	IPv6 PIM mode.

Field	Description
Flag	<p>Flag of the (S, G) or (*, G) entry in the IPv6 PIM routing table:</p> <ul style="list-style-type: none"> • ACT—The entry has been used for routing data. • BIDIR—The entry was created by IPv6 BIDIR-PIM. • DEL—The entry will be removed. • EXPRUNE—Some outgoing interfaces are pruned by other IPv6 multicast routing protocols. • EXT—The entry contains outgoing interfaces provided by other IPv6 multicast routing protocols. • LOC—The entry is on a router directly connected to the same subnet with the IPv6 multicast source. • NIIF—The entry contains unknown incoming interfaces. • NONBR—The entry has an IPv6 PIM neighbor searching failure. • RPT—The entry is on a RPT branch where (S, G) prunes have been sent to the RP. • SPT—The entry is on the SPT. • SWT—The entry is in the process of RPT-to-SPT switchover. • WC—The entry is a wildcard routing entry.
Uptime	Length of time since the (S, G) or (*, G) entry was installed.
Upstream interface	Upstream (incoming) interface of the (S, G) or (*, G) entry.
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry.
RPF prime neighbor	<p>RPF neighbor of the (S, G) or (*, G) entry.</p> <ul style="list-style-type: none"> • For a (*, G) entry, if this router is the RP, the RPF neighbor of this (*, G) entry is NULL. • For a (S, G) entry, if this router directly connects to the IPv6 multicast source, the RPF neighbor of this (S, G) entry is NULL.
Downstream interface(s) information	<p>Information of the downstream interfaces, including the following:</p> <ul style="list-style-type: none"> • Number of downstream interfaces. • Downstream interface name. • Protocol type configured on the downstream interface. • Uptime of the downstream interfaces. • Expiry time of the downstream interfaces.

display pim ipv6 rp-info

Syntax

```
display pim ipv6 rp-info [ ipv6-group-address ] [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal

number between 0 and F, inclusive. If you do not provide a group address, this command displays information about the RPs that corresponds to all IPv6 multicast groups.

|: 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 pim ipv6 rp-info** to display RP information.

The RP information includes the information of RPs dynamically found by the BSR mechanism and static RPs.

Examples

Display the RP information that corresponds to the IPv6 multicast group FF0E::101.

```
<Sysname> display pim ipv6 rp-info ff0e::101
PIM-SM BSR RP information:
prefix/prefix length: FF0E::101/64 [B]
  RP: 2004::2
  Priority: 192
  HoldTime: 130
  Uptime: 00:05:19
  Expires: 00:02:11
```

Table 87 Command output

Field	Description
prefix/prefix length	IPv6 multicast group to which the RP is designated.
[B]	RP provides services for multicast groups in the IPv6 bidirectional PIM mode. Without this field displayed, the RP provides services for multicast groups in the IPv6 PIM-SM mode.
RP	IPv6 address of the RP.
Priority	RP priority.
HoldTime	Timeout time of the RP.
Uptime	Length of time since the RP was elected.
Expires	Remaining time of the RP.

dscp (IPv6 PIM view)

Syntax

dscp *dscp-value*

undo dscp

View

IPv6 PIM view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value for IPv6 PIM messages, in the range of 0 to 63.

Description

Use **dscp** to set the DSCP value for IPv6 PIM messages.

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

The default DSCP value in IPv6 PIM messages is 48.

Examples

Set the DSCP value to 63 for IPv6 PIM messages.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] dscp 63
```

embedded-rp

Syntax

embedded-rp [*acl6-number*]

undo embedded-rp [*acl6-number*]

View

IPv6 PIM view

Default level

2: System level

Parameters

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

Description

Use **embedded-rp** to enable embedded RP.

Use **undo embedded-rp** to disable embedded RP or restore the default.

By default, embedded RP is enabled for IPv6 multicast groups in the default embedded RP address scopes.

The default embedded RP address scopes are FF7x::/12 and FFFx::/12, where x represents any legal address scope. For more information about the scope field, see *Multicast overview*.

When you use the **embedded-rp** command without specifying *acl6-number*, the embedded RP feature is enabled for all the IPv6 multicast groups in the default embedded RP address scopes. If you specify *acl6-number*, the embedded RP feature is enabled for only those IPv6 multicast groups that are within the default embedded RP address scopes and pass the ACL check.

When you use the **undo embedded-rp** command without specifying *acl6-number*, the embedded RP feature is disabled for all the IPv6 multicast groups. If you specify *acl6-number*, this command restores the default.

Examples

```
# Enable embedded RP for only those IPv6 multicast groups in the address scope FF7E:140:20::101/64.
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff7e:140:20::101 64
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] embedded-rp 2000
```

hello-option dr-priority (IPv6 PIM view)

Syntax

hello-option dr-priority *priority*

undo hello-option dr-priority

View

IPv6 PIM view

Default level

2: System level

Parameters

priority: Router priority for DR election, in the range of 0 to 4294967295. A larger value means a higher priority.

Description

Use **hello-option dr-priority** to configure the global value of the router priority for DR election.

Use **undo hello-option dr-priority** to restore the default.

By default, the router priority for DR election is 1.

Related commands: **pim ipv6 hello-option dr-priority**.

Examples

```
# Set the router priority for DR election to 3.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option dr-priority 3
```

hello-option holdtime (IPv6 PIM view)

Syntax

hello-option holdtime *interval*

undo hello-option holdtime

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: IPv6 PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535. A value of 65,535 makes the IPv6 PIM neighbor always reachable.

Description

Use **hello-option holdtime** to configure the IPv6 PIM neighbor timeout time.

Use **undo hello-option holdtime** to restore the default.

By default, the IPv6 PIM neighbor timeout time is 105 seconds.

Related commands: **pim ipv6 hello-option holdtime**.

Examples

```
# Set the IPv6 PIM neighbor timeout time to 120 seconds globally.
```

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option holdtime 120
```

hello-option lan-delay (IPv6 PIM view)

Syntax

hello-option lan-delay *interval*

undo hello-option lan-delay

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

Description

Use **hello-option lan-delay** to configure the global value of the LAN-delay time, namely, the period of time that the device waits before it forwards a received prune message.

Use **undo hello-option lan-delay** to restore the default.

By default, the LAN-delay time is 500 milliseconds.

Related commands: **hello-option override-interval**, **pim ipv6 hello-option lan-delay**, and **pim ipv6 hello-option override-interval**.

Examples

```
# Set the LAN-delay time to 200 milliseconds globally.
```

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option lan-delay 200
```

hello-option neighbor-tracking (IPv6 PIM view)

Syntax

```
hello-option neighbor-tracking  
undo hello-option neighbor-tracking
```

View

IPv6 PIM view

Default level

2: System level

Parameters

None

Description

Use **hello-option neighbor-tracking** to globally disable join suppression, namely, to enable neighbor tracking.

Use **undo hello-option neighbor-tracking** to enable join suppression.

By default, join suppression is enabled. Namely, neighbor tracking is disabled.

Related commands: **pim ipv6 hello-option neighbor-tracking**.

Examples

```
# Disable join suppression globally.  
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] hello-option neighbor-tracking
```

hello-option override-interval (IPv6 PIM view)

Syntax

```
hello-option override-interval interval  
undo hello-option override-interval
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

Description

Use **hello-option override-interval** to configure the global value of the prune override interval.

Use **undo hello-option override-interval** to restore the default.

By default, the prune override interval is 2500 milliseconds.

Related commands: **hello-option lan-delay**, **pim ipv6 hello-option lan-delay**, and **pim ipv6 hello-option override-interval**.

Examples

```
# Set the prune override interval to 2000 milliseconds globally.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option override-interval 2000
```

holdtime assert (IPv6 PIM view)

Syntax

```
holdtime assert interval
undo holdtime assert
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

Description

Use **holdtime assert** to configure the global value of the assert timeout time.

Use **undo holdtime assert** to restore the default.

By default, the assert timeout time is 180 seconds.

Related commands: **holdtime join-prune**, **pim ipv6 holdtime assert**, and **pim ipv6 holdtime join-prune**.

Examples

```
# Set the global value of the assert timeout time to 100 seconds.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] holdtime assert 100
```

holdtime join-prune (IPv6 PIM view)

Syntax

```
holdtime join-prune interval
undo holdtime join-prune
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

Description

Use **holdtime join-prune** to configure the global value of the join/prune timeout time.

Use **undo holdtime join-prune** to restore the default.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **pim ipv6 holdtime assert**, and **pim ipv6 holdtime join-prune**.

Examples

```
# Set the global value of the join/prune timeout time to 280 seconds.
```

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] holdtime join-prune 280
```

jp-pkt-size (IPv6 PIM view)

Syntax

jp-pkt-size *packet-size*

undo jp-pkt-size

View

IPv6 PIM view

Default level

2: System level

Parameters

packet-size: Maximum size of each join/prune message in bytes, with an effective range of 100 to 64000.

Description

Use **jp-pkt-size** to configure the maximum size of each join/prune message.

Use **undo jp-pkt-size** to restore the default.

By default, the maximum size of each join/prune message is 8100 bytes.

If IPv6 PIM snooping-enabled switches are deployed in the IPv6 PIM network, be sure to set a value no greater than the IPv6 path MTU for the maximum size of each join/prune message on the receiver-side edge IPv6 PIM devices.

Related commands: **jp-queue-size**.

Examples

```
# Set the maximum size of each join/prune message to 1500 bytes.
```

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] jp-pkt-size 1500
```

jp-queue-size (IPv6 PIM view)

Syntax

jp-queue-size *queue-size*

undo jp-queue-size

View

IPv6 PIM view

Default level

2: System level

Parameters

queue-size: Maximum number of (S, G) entries in a join/prune message, in the range of 1 to 4096.

Description

Use **jp-queue-size** to configure the maximum number of (S, G) entries in a join/prune message.

Use **undo jp-queue-size** to restore the default.

By default, a join/prune messages contains a maximum of 1,020 (S, G) entries.

When you use this command, take the following into account:

- The size of the forwarding table. In a network that does not support packet fragmentation, if you configure a large *queue-size*, a join/prune message might contain a large number of groups, which might cause the message length to exceed the MTU of the network. As a result, the products that do not support fragmentation drop the join/prune message.
- The (S, G) join/prune state hold time on the upstream device. If you configure a small queue size, the outgoing interface of the corresponding entry might have been pruned because of timeout before the last join/prune message in a queue reaches the upstream device.

Related commands: **holdtime join-prune**, **jp-pkt-size**, and **pim ipv6 holdtime join-prune**.

Examples

```
# Configure a join/prune messages to contain a maximum of 2,000 (S, G) entries.
```

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

```
[Sysname] pim ipv6
```

```
[Sysname-pim6] jp-queue-size 2000
```

pim ipv6

Syntax

pim ipv6

undo pim ipv6

View

System view

Default level

2: System level

Parameters

None

Description

Use **pim ipv6** to enter IPv6 PIM view.

Use **undo pim ipv6** to remove all configurations in IPv6 PIM view.

You must enable IPv6 multicast routing on the device before this command can take effect.

Related commands: **multicast ipv6 routing-enable**.

Examples

```
# Enable IPv6 multicast routing and enter IPv6 PIM view.
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] pim ipv6
[Sysname-pim6]
```

pim ipv6 bfd enable

Syntax

pim ipv6 bfd enable

undo pim ipv6 bfd enable

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim ipv6 bfd enable** to enable IPv6 PIM to work with Bidirectional Forwarding Detection (BFD).

Use **undo pim ipv6 bfd enable** to disable this feature.

By default, this feature is disabled.

You must enable IPv6 PIM-DM or IPv6 PIM-SM on an interface before you configure this feature on the interface. Otherwise, this feature is not effective.

Related commands: **pim ipv6 dm** and **pim ipv6 sm**.

Examples

```
# Enable IPv6 multicast routing in the public network, enable IPv6 PIM-SM on interface VLAN-interface
100, and enable IPv6 PIM to work with BFD on the interface.
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 sm
[Sysname-Vlan-interface100] pim ipv6 bfd enable
```


pim ipv6 bsr-boundary

Syntax

```
pim ipv6 bsr-boundary
undo pim ipv6 bsr-boundary
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim ipv6 bsr-boundary** to configure an IPv6 PIM domain border, namely, a bootstrap message boundary.

Use **undo pim ipv6 bsr-boundary** to remove the configured IPv6 PIM domain border.

By default, no PIM domain border is configured.

Related commands: **c-bsr** and **multicast ipv6 boundary**.

Examples

```
# Configure VLAN-interface 100 as a PIM domain border.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 bsr-boundary
```

pim ipv6 dm

Syntax

```
pim ipv6 dm
undo pim ipv6 dm
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim ipv6 dm** to enable IPv6 PIM-DM.

Use **undo pim ipv6 dm** to disable IPv6 PIM-DM.

By default, IPv6 PIM-DM is disabled.

This command can take effect only after IPv6 multicast routing is enabled on the device.

IPv6 PIM-DM cannot be used for IPv6 multicast groups in the IPv6 SSM group range.

Related commands: **multicast ipv6 routing-enable**, **pim ipv6 sm**, and **ssm-policy**.

Examples

```
# Enable IPv6 multicast routing, and enable IPv6 PIM-DM on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 dm
```

pim ipv6 hello-option dr-priority

Syntax

```
pim ipv6 hello-option dr-priority priority
undo pim ipv6 hello-option dr-priority
```

View

Interface view

Default level

2: System level

Parameters

priority: Router priority for DR election, in the range of 0 to 4294967295. A larger value means a higher priority.

Description

Use **pim ipv6 hello-option dr-priority** to configure the router priority for DR election on the current interface.

Use **undo pim ipv6 hello-option dr-priority** to restore the default.

By default, the router priority for DR election is 1.

Related commands: **hello-option dr-priority**.

Examples

```
# Set the router priority for DR election to 3 on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option dr-priority 3
```

pim ipv6 hello-option holdtime

Syntax

```
pim ipv6 hello-option holdtime interval
undo pim ipv6 hello-option holdtime
```

View

Interface view

Default level

2: System level

Parameters

interval: IPv6 PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535. A value of 65,535 makes the PIM neighbor always reachable.

Description

Use **pim ipv6 hello-option holdtime** to configure the PIM neighbor timeout time on the current interface.

Use **undo pim ipv6 hello-option holdtime** to restore the default.

By default, the IPv6 PIM neighbor timeout time is 105 seconds.

Related commands: **hello-option holdtime**.

Examples

```
# Set the IPv6 PIM neighbor timeout time to 120 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option holdtime 120
```

pim ipv6 hello-option lan-delay

Syntax

pim ipv6 hello-option lan-delay *interval*

undo pim ipv6 hello-option lan-delay

View

Interface view

Default level

2: System level

Parameters

interval: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

Description

Use **pim ipv6 hello-option lan-delay** to configure the LAN-delay time—namely, the time that the device waits before it forwards a received prune message—on the current interface.

Use **undo pim ipv6 hello-option lan-delay** to restore the default.

By default, the LAN-delay time is 500 milliseconds.

Related commands: **hello-option lan-delay**, **hello-option override-interval**, and **pim ipv6 hello-option override-interval**.

Examples

```
# Set the LAN-delay time to 200 milliseconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option lan-delay 200
```

pim ipv6 hello-option neighbor-tracking

Syntax

```
pim ipv6 hello-option neighbor-tracking  
undo pim ipv6 hello-option neighbor-tracking
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim ipv6 hello-option neighbor-tracking** to disable join suppression—namely, to enable neighbor tracking—on the current interface.

Use **undo pim ipv6 hello-option neighbor-tracking** to enable join suppression.

By default, join suppression is enabled. Namely, neighbor tracking is disabled.

Related commands: **hello-option neighbor-tracking**.

Examples

```
# Disable join suppression on VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] pim ipv6 hello-option neighbor-tracking
```

pim ipv6 hello-option override-interval

Syntax

```
pim ipv6 hello-option override-interval interval  
undo pim ipv6 hello-option override-interval
```

View

Interface view

Default level

2: System level

Parameters

interval: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

Description

Use **pim ipv6 hello-option override-interval** to configure the prune override interval on the current interface.

Use **undo pim ipv6 hello-option override-interval** to restore the default.

By default, the prune override interval is 2500 milliseconds.

Related commands: **hello-option lan-delay**, **hello-option override-interval**, and **pim ipv6 hello-option lan-delay**.

Examples

```
# Set the prune override interval to 2000 milliseconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option override-interval 2000
```

pim ipv6 holdtime assert

Syntax

```
pim ipv6 holdtime assert interval
undo pim ipv6 holdtime assert
```

View

Interface view

Default level

2: System level

Parameters

interval: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

Description

Use **pim ipv6 holdtime assert** to configure the assert timeout time on the current interface.

Use **undo pim ipv6 holdtime assert** to restore the default.

By default, the assert timeout time is 180 seconds.

Related commands: **holdtime assert**, **holdtime join-prune**, and **pim ipv6 holdtime join-prune**.

Examples

```
# Set the assert timeout time to 100 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 holdtime assert 100
```

pim ipv6 holdtime join-prune

Syntax

```
pim ipv6 holdtime join-prune interval
undo pim ipv6 holdtime join-prune
```

View

Interface view

Default level

2: System level

Parameters

interval: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

Description

Use **pim ipv6 holdtime join-prune** to configure the join/prune timeout time on the interface.

Use **undo pim ipv6 holdtime join-prune** to restore the default.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **holdtime join-prune**, and **pim ipv6 holdtime assert**.

Examples

```
# Set the join/prune timeout time to 280 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 holdtime join-prune 280
```

pim ipv6 neighbor-policy

Syntax

```
pim ipv6 neighbor-policy acl6-number
undo pim ipv6 neighbor-policy
```

View

Interface view

Default level

2: System level

Parameters

acl6-number: Basic IPv6 ACL number, in the range of 2000 to 2999. When the IPv6 ACL is defined, the **source** keyword in the **rule** command specifies a legal source address range for hello messages.

Description

Use **pim ipv6 neighbor-policy** to configure a legal source address range for hello messages to guard against hello message spoofing.

Use **undo pim ipv6 neighbor-policy** to restore the default.

By default, no source address range for hello messages is configured. That is, all the received hello messages are considered legal.

Examples

```
# Configure a legal source address range for hello messages on VLAN-interface 100 so that only the
devices on the FE80:101::101/64 subnet can become PIM neighbors of this switch.
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source fe80:101::101 64
[Sysname-acl6-basic-2000] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 neighbor-policy 2000
```

pim ipv6 require-genid

Syntax

```
pim ipv6 require-genid
undo pim ipv6 require-genid
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim ipv6 require-genid** to enable rejection of hello messages without Generation_ID.

Use **undo pim ipv6 require-genid** to restore the default.

By default, hello messages without Generation_ID are accepted.

Examples

```
# Enable VLAN-interface 100 to reject hello messages without Generation_ID.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 require-genid
```

pim ipv6 sm

Syntax

```
pim ipv6 sm
undo pim ipv6 sm
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim ipv6 sm** to enable IPv6 PIM-SM.

Use **undo pim ipv6 sm** to disable IPv6 PIM-SM.

By default, IPv6 PIM-SM is disabled.

This command can take effect only after IPv6 multicast routing is enabled on the device.

Related commands: **multicast ipv6 routing-enable** and **pim ipv6 dm**.

Examples

```
# Enable IPv6 multicast routing, and enable IPv6 PIM-SM on VLAN-interface 100.
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 sm
```

pim ipv6 state-refresh-capable

Syntax

```
pim ipv6 state-refresh-capable
undo pim ipv6 state-refresh-capable
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **pim ipv6 state-refresh-capable** to enable the state refresh feature on the interface.

Use **undo pim ipv6 state-refresh-capable** to disable the state refresh feature.

By default, the state refresh feature is enabled.

Related commands: **state-refresh-hoplimit**, **state-refresh-interval**, and **state-refresh-rate-limit**.

Examples

```
# Disable state refresh on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo pim ipv6 state-refresh-capable
```

pim ipv6 timer graft-retry

Syntax

```
pim ipv6 timer graft-retry interval
undo pim ipv6 timer graft-retry
```

View

Interface view

Default level

2: System level

Parameters

interval: Graft retry period in seconds, with an effective range of 1 to 65,535.

Description

Use **pim ipv6 timer graft-retry** to configure the graft retry period.

Use **undo pim ipv6 timer graft-retry** to restore the default.

By default, the graft retry period is 3 seconds.

Examples

```
# Set the graft retry period to 80 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 timer graft-retry 80
```

pim ipv6 timer hello

Syntax

```
pim ipv6 timer hello interval
```

```
undo pim ipv6 timer hello
```

View

Interface view

Default level

2: System level

Parameters

interval: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use **pim ipv6 timer hello** to configure the interval at which hello messages are sent on the current interface.

Use **undo pim ipv6 timer hello** to restore the default.

By default, hello messages are sent at the interval of 30 seconds.

Related commands: **timer hello**.

Examples

```
# Set the hello interval to 40 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 timer hello 40
```

pim ipv6 timer join-prune

Syntax

```
pim ipv6 timer join-prune interval
```

```
undo pim ipv6 timer join-prune
```

View

Interface view

Default level

2: System level

Parameters

interval: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use **pim ipv6 timer join-prune** to configure the interval at which join/prune messages are sent on the current interface.

Use **undo pim ipv6 timer join-prune** to restore the default.

By default, the join/prune interval is 60 seconds.

Related commands: **timer join-prune**.

Examples

```
# Set the join/prune interval to 80 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 timer join-prune 80
```

pim ipv6 triggered-hello-delay

Syntax

pim ipv6 triggered-hello-delay *interval*

undo pim ipv6 triggered-hello-delay

View

Interface view

Default level

2: System level

Parameters

interval: Maximum delay in seconds between hello messages, with an effective range of 1 to 60.

Description

Use **pim ipv6 triggered-hello-delay** to configure the maximum delay between hello messages.

Use **undo pim ipv6 triggered-hello-delay** to restore the default.

By default, the maximum delay between hello messages is 5 seconds.

Examples

```
# Set the maximum delay between hello messages to 3 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 triggered-hello-delay 3
```

probe-interval (IPv6 PIM view)

Syntax

```
probe-interval interval  
undo probe-interval
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: Register probe time in seconds, with an effective range of 1 to 1799.

Description

Use **probe-interval** to configure the register probe time.

Use **undo probe-interval** to restore the default.

By default, the register probe time is 5 seconds.

Related commands: **register-suppression-timeout**.

Examples

```
# Set the register probe time to 6 seconds.  
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] probe-interval 6
```

prune delay (IPv6 PIM view)

Syntax

```
prune delay interval  
undo prune delay
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: Prune delay time in the range of 1 to 128 seconds.

Description

Use **prune delay** to configure the prune delay time, namely, the length of time that the device waits between receiving a prune message and taking a prune action.

Use **undo prune delay** to restore the default.

By default, the prune delay time is not configured.

Examples

```
# Set the prune delay time to 75 seconds in the public network.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] prune delay 75
```

register-policy (IPv6 PIM view)

Syntax

```
register-policy acl6-number
undo register-policy
```

View

IPv6 PIM view

Default level

2: System level

Parameters

acl6-number: Advanced IPv6 ACL number, in the range of 3000 to 3999. The RP can accept only register messages that match the **permit** statement of the IPv6 ACL.

Description

Use **register-policy** to configure an IPv6 ACL rule to filter register messages.

Use **undo register-policy** to remove the configured register filtering rule.

By default, no register filtering rule is configured.

Related commands: **register-suppression-timeout**.

Examples

```
# Configure a register filtering policy on the RP so that the RP accepts only those register messages from
IPv6 multicast sources on the 3:1::/64 subnet for IPv6 multicast groups on the FF0E:13::/64 subnet.
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit ipv6 source 3:1:: 64 destination ff0e:13:: 64
[Sysname-acl6-adv-3000] quit
[Sysname] pim ipv6
[Sysname-pim6] register-policy 3000
```

register-suppression-timeout (IPv6 PIM view)

Syntax

```
register-suppression-timeout interval
undo register-suppression-timeout
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: Register suppression time in seconds, in the range of 1 to 65535.

Description

Use **register-suppression-timeout** to configure the register suppression time.

Use **undo register-suppression-timeout** to restore the default.

By default, the register suppression time is 60 seconds.

Related commands: **probe-interval** and **register-policy**.

Examples

```
# Set the register suppression time to 70 seconds.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] register-suppression-timeout 70
```

register-whole-checksum (IPv6 PIM view)

Syntax

```
register-whole-checksum
undo register-whole-checksum
```

View

IPv6 PIM view

Default level

2: System level

Parameters

None

Description

Use **register-whole-checksum** to configure the router to calculate the checksum based on the entire register message.

Use **undo register-whole-checksum** to restore the default.

By default, the router calculates the checksum based only on the header in the register message.

Related commands: **register-policy** and **register-suppression-timeout**.

Examples

```
# Configure the router to calculate the checksum based on the entire register message.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] register-whole-checksum
```

reset pim ipv6 control-message counters

Syntax

```
reset pim ipv6 control-message counters [ interface interface-type interface-number ]
```

View

User view

Default level

1: Monitor level

Parameters

interface-type interface-number: Resets the IPv6 PIM control message counter on a particular interface. If no interface is specified, this command clears statistics for IPv6 PIM control messages on all interfaces.

Description

Use **reset pim ipv6 control-message counters** to clear statistics for IPv6 PIM control messages.

Examples

```
# Clear statistics for IPv6 PIM control messages on all interfaces.  
<Sysname> reset pim ipv6 control-message counters
```

source-lifetime (IPv6 PIM view)

Syntax

```
source-lifetime interval  
undo source-lifetime
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: IPv6 multicast source lifetime in seconds, with an effective range of 1 to 31,536,000.

Description

Use **source-lifetime** to configure the IPv6 multicast source lifetime.

Use **undo source-lifetime** to restore the default.

By default, the lifetime of an IPv6 multicast source is 210 seconds.

Examples

```
# Set the IPv6 multicast source lifetime to 200 seconds.  
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] source-lifetime 200
```

source-policy (IPv6 PIM view)

Syntax

```
source-policy acl6-number  
undo source-policy
```

View

IPv6 PIM view

Default level

2: System level

Parameters

acl6-number: Basic or advanced IPv6 ACL number, in the range of 2000 to 3999.

Description

Use **source-policy** to configure an IPv6 multicast data filter.

Use **undo source-policy** to remove the configured IPv6 multicast data filter.

By default, no IPv6 multicast data filter is configured.

If you specify a basic ACL, the device filters all the received IPv6 multicast packets based on the source address, and discards packets that fail the source address match.

If you specify an advanced ACL, the device filters all the received IPv6 multicast packets based on the source and group addresses, and discards packets that fail the match.

If you use this command repeatedly, the last configuration takes effect.

Examples

```
# Configure the router to accept IPv6 multicast packets that originate from 3121::1 and discard IPv6 multicast packets that originate from 3121::2.
```

```
<Sysname> system-view  
[Sysname] acl ipv6 number 2000  
[Sysname-acl6-basic-2000] rule permit source 3121::1 128  
[Sysname-acl6-basic-2000] rule deny source 3121::2 128  
[Sysname-acl6-basic-2000] quit  
[Sysname] pim ipv6  
[Sysname-pim6] source-policy 2000  
[Sysname-pim6] quit
```

spt-switch-threshold infinity (IPv6 PIM view)

Syntax

```
spt-switch-threshold infinity [ group-policy acl6-number [ order order-value ] ]  
undo spt-switch-threshold [ group-policy acl6-number ]
```

View

IPv6 PIM view

Default level

2: System level

Parameters

group-policy *acl6-number*: Specifies a basic IPv6 ACL number, in the range of 2000 to 2999. If you do not include this option in your command, the configuration applies to all IPv6 multicast groups.

order *order-value*: Specifies the order of the IPv6 ACL in the group-policy list, where *order-value* has an effective range of 1 to (the largest order value in the existing group-policy list + 1), but the value range should not include the original order value of the IPv6 ACL in the group-policy list. If you have assigned an *order-value* to a certain IPv6 ACL, do not specify the same *order-value* for another IPv6 ACL. Otherwise the system gives error information. If you do not specify an *order-value*, the order value of the IPv6 ACL remains the same in the group-policy list.

Description

Use **spt-switch-threshold infinity** to disable the switchover to SPT.

Use **undo spt-switch-threshold** to restore the default.

By default, the device switches to the SPT immediately after it receives the first IPv6 multicast packet.

To adjust the order of an IPv6 ACL that already exists in the group-policy list, you can use the *acl6-number* argument to specify this IPv6 ACL and set its order value. This inserts the IPv6 ACL to the position of *order-value* in the group-policy list. The order of the other existing IPv6 ACLs in the group-policy list remains unchanged.

To use an IPv6 ACL that does not exist in the group-policy list, you can use the *acl6-number* argument to specify an IPv6 ACL and set its order value. This inserts the IPv6 ACL to the position of *order-value* in the group-policy list. If you do not include the **order** *order-value* option in your command, the ACL is appended to the end of the group-policy list.

If you use this command multiple times on the same IPv6 multicast group, the first traffic rate configuration matched in sequence takes effect.

If the switch is an RP, disabling switchover to SPT might cause multicast traffic forwarding failures on the source-side DR. When disabling switchover to SPT, be sure you fully understand its impact on your network.

Examples

```
# Disable the switchover to SPT on the receiver-side DR
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] spt-switch-threshold infinity
```

ssm-policy (IPv6 PIM view)

Syntax

```
ssm-policy acl6-number
undo ssm-policy
```

View

IPv6 PIM view

Default level

2: System level

Parameters

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

Description

Use **ssm-policy** to configure the IPv6 SSM group range.

Use **undo ssm-policy** to restore the default.

By default, the IPv6 SSM group range is FF3x::/32, where x represents any legal scope.

You can use this command to define an address range of permitted or denied IPv6 multicast groups. If the match succeeds, the running multicast mode is IPv6 PIM-SSM. Otherwise, the multicast mode is IPv6 PIM-SM.

Examples

```
# Configure the IPv6 SSM group range to be FF3E:0:8192::/96.
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff3e:0:8192:: 96
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] ssm-policy 2000
```

state-refresh-hoplimit

Syntax

```
state-refresh-hoplimit hoplimit-value
undo state-refresh-hoplimit
```

View

IPv6 PIM view

Default level

2: System level

Parameters

hoplimit-value: Hop limit value of state refresh messages, in the range of 1 to 255.

Description

Use **state-refresh-hoplimit** to configure the hop limit value of state refresh messages.

Use **undo state-refresh-hoplimit** to restore the default.

By default, the hop limit value of state refresh messages is 255.

Related commands: **pim ipv6 state-refresh-capable**, **state-refresh-interval**, and **state-refresh-rate-limit**.

Examples

```
# Set the hop limit value of state refresh messages to 45.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] state-refresh-hoplimit 45
```

state-refresh-interval (IPv6 PIM view)

Syntax

```
state-refresh-interval interval  
undo state-refresh-interval
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: State refresh interval in seconds, with an effective range of 1 to 255.

Description

Use **state-refresh-interval** to configure the interval between state refresh messages.

Use **undo state-refresh-interval** to restore the default.

By default, the state refresh interval is 60 seconds.

Related commands: **pim ipv6 state-refresh-capable**, **state-refresh-hoplimit**, and **state-refresh-rate-limit**.

Examples

```
# Set the state refresh interval to 70 seconds.  
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] state-refresh-interval 70
```

state-refresh-rate-limit (IPv6 PIM view)

Syntax

```
state-refresh-rate-limit interval  
undo state-refresh-rate-limit
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: Time to wait before receiving a new refresh message, in seconds and with an effective range of 1 to 65535.

Description

Use **state-refresh-rate-limit** to configure the time that the router must wait before it receives a new state refresh message.

Use **undo state-refresh-rate-limit** to restore the default.

By default, the device waits 30 seconds before it receives a new state refresh message.

Related commands: **pim ipv6 state-refresh-capable**, **state-refresh-hoplimit**, and **state-refresh-interval**.

Examples

```
# Configure the device to wait 45 seconds before it receives a new state refresh message.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] state-refresh-rate-limit 45
```

static-rp (IPv6 PIM view)

Syntax

```
static-rp ipv6-rp-address [ acl6-number ] [ preferred ] [ bidir ]
undo static-rp ipv6-rp-address
```

View

IPv6 PIM view

Default level

2: System level

Parameters

ipv6-rp-address: Specifies the IPv6 address of the static RP to be configured. This address must be a real, valid, globally scoped IPv6 unicast address. For a static RP serving IPv6 BIDIR-PIM, you can specify a virtual IPv6 address.

acl6-number: Specifies a basic IPv6 ACL number, in the range of 2000 to 2999. If you provide this argument, the configured static RP provides services for only those IPv6 multicast groups that pass the filtering. Otherwise, the configured static RP provides services for the all IPv6 multicast groups.

preferred: Gives priority to the static RP if the static RP conflicts with the dynamic RP. If you do not include the **preferred** keyword in your command, the dynamic RP receives priority, and the static RP takes effect only if no dynamic RP exists in the network or when the dynamic RP fails.

bidir: Configures the static RP to provide services for multicast groups in IPv6 BIDIR-PIM. Without this argument, the static RP provides services for groups in IPv6 PIM-SM.

Description

Use **static-rp** to configure a static RP.

Use **undo static-rp** to configure a static RP.

By default, no static RP is configured.

IPv6 PIM-SM or IPv6 PIM-DM cannot be enabled on an interface that acts as a static RP.

When the IPv6 ACL rule applied on a static RP changes, a new RP must be elected for all IPv6 multicast groups.

You can configure multiple static RPs by using this command repeatedly. However, if you use this command multiple times and specify the same static RP address or reference the same IPv6 ACL rule, the last configuration overrides the previous one. If you have configured multiple static RPs for the same IPv6 multicast group, the one with the highest IPv6 address provides services for the group.

You can configure up to 50 static RPs on the same device.

Related commands: **display pim ipv6 rp-info**.

Examples

Configure the interface with an IPv6 address of 2001::2 as a static RP to provide services for the IPv6 multicast groups in the address range of FF03::101/64 defined in IPv6 ACL 2001, and give priority to this static RP in the case of static/dynamic RP conflict.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source ff03::101 64
[Sysname-acl6-basic-2001] quit
[Sysname] pim ipv6
[Sysname-pim6] static-rp 2001::2 2001 preferred
```

timer hello (IPv6 PIM view)

Syntax

```
timer hello interval
undo timer hello
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use **timer hello** to configure the hello interval globally.

Use **undo timer hello** to restore the default.

By default, hello messages are sent at the interval of 30 seconds.

Related commands: **pim ipv6 timer hello**.

Examples

```
# Set the global hello interval to 40 seconds.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] timer hello 40
```

timer join-prune (IPv6 PIM view)

Syntax

```
timer join-prune interval
undo timer join-prune
```

View

IPv6 PIM view

Default level

2: System level

Parameters

interval: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

Description

Use **timer join-prune** to configure the join/prune interval globally.

Use **undo timer join-prune** to restore the default.

By default, the join/prune interval is 60 seconds.

Related commands: **pim ipv6 timer join-prune**.

Examples

Set the global join/prune interval to 80 seconds.

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

```
[Sysname] pim ipv6
```

```
[Sysname-pim6] timer join-prune 80
```

IPv6 MBGP configuration commands (available only on the HP 5500 EI)

aggregate (IPv6 MBGP 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 MBGP address family view

Default level

2 System level

Parameters

ipv6-address: Specifies a summary address.

prefix-length: Specifies the 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 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.

The keywords of the command are described as follows:

Table 88 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 must be summarized, because the frequent changes to these specific routes might lead to route oscillation.
detail-suppressed	Does not suppress the summary route, but suppresses the advertisement of all the more specific routes. To summarize only some specific routes, use the peer filter-policy command.
suppress-policy	Used to create a summary route and suppress the advertisement of some summarized routes. To suppress some routes selectively and leave other routes advertised, use the if-match clause of the route-policy command.

Keywords	Function
origin-policy	Selects only the routes that satisfy the routing policy for route summarization.
attribute-policy	Sets attributes, except the AS_PATH attribute, for the summary route. You can accomplish the same task by using the peer route-policy command.

Description

Use **aggregate** to create an IPv6 summary route in the IPv6 MBGP routing table.

Use **undo aggregate** to remove an IPv6 summary route.

By default, no summary route is configured.

Examples

In IPv6 MBGP address family view, create a summary of 12::/64 in the IPv6 MBGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] aggregate 12:: 64
```

balance (IPv6 MBGP address family view)

Syntax

balance *number*

undo balance

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

number: Specifies the number of IPv6 MBGP 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 IPv6 MBGP routes used for load balancing.

Use **undo balance** to disable load balancing.

By default, load balancing is disabled.

Unlike IGP, IPv6 MBGP has no explicit metric for load balancing. Instead, it implements load balancing by using IPv6 MBGP route selection rules.

Related commands: **display ipv6 multicast routing-table**.

Examples

In IPv6 MBGP address family view, set the number of IPv6 MBGP routes for load balancing to 2.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
```

```
[Sysname-bgp-af-ipv6-mul] balance 2
```

bestroute as-path-neglect (IPv6 MBGP address family view)

Syntax

```
bestroute as-path-neglect  
undo bestroute as-path-neglect
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

None

Description

Use **bestroute as-path-neglect** to configure IPv6 MBGP not to consider the AS_PATH during best route selection.

Use **undo bestroute as-path-neglect** to configure IPv6 MBGP to consider the AS_PATH during best route selection.

By default, IPv6 MBGP considers the AS_PATH during best route selection.

Examples

In IPv6 MBGP address family view, configure IPv6 MBGP to ignore the AS_PATH during best route selection.

```
<Sysname> system-view  
[Sysname]bgp 100  
[Sysname-bgp]ipv6-family multicast  
[Sysname-bgp-af-ipv6-mul]bestroute as-path-neglect
```

bestroute compare-med (IPv6 MBGP address family view)

Syntax

```
bestroute compare-med  
undo bestroute compare-med
```

View

IPv6 MBGP 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.

By default, the comparison of the MED for paths from each AS is disabled.

After you use the **bestroute compare-med** command, the **balance** command does not take effect.

Examples

In IPv6 MBGP address family view, enable the comparison of MED for paths from each AS during best route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] bestroute compare-med
```

bestroute med-confederation (IPv6 MBGP address family view)

Syntax

```
bestroute med-confederation
undo bestroute med-confederation
```

View

IPv6 MBGP 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 during best route selection.

Use **undo bestroute med-confederation** to disable the comparison.

Such comparison is disabled by default.

When you use this command used, the system compares MED values only for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

Examples

In IPv6 MBGP address family view, enable the comparison of the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]bestroute med-confederation
```

compare-different-as-med (IPv6 MBGP address family view)

Syntax

```
compare-different-as-med
undo compare-different-as-med
```

View

IPv6 MBGP 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.

By default, MED comparison is not allowed among the routes from the peers in different ASs.

If several paths are available for one destination, the path with the smallest MED is selected.

Do not use this command unless associated ASs adopt the same IGP and routing selection method.

Examples

In IPv6 MBGP address family view, enable the comparison of the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]compare-different-as-med
```

dampening (IPv6 MBGP address family view)

Syntax

dampening [*half-life-reachable* *half-life-unreachable* *reuse* *suppress* *ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

half-life-reachable: Specifies the half-life for reachable routes, in the range of 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Specifies the half-life for unreachable routes, in the range of 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Specifies the reuse threshold value for suppressed routes, in the range of 1 to 20000. A suppressed route that has the penalty value decreased under the value is reused. By default, the value is 750.

suppress: Specifies the threshold for a route to be suppressed, in the range of 1 to 20000. A route is suppressed if its penalty value exceeds this value. The value must be greater than the *reuse* value. By default, the value is 2000.

ceiling: Specifies a ceiling penalty value from 1001 to 20000. The value must be greater than the *suppress* value. The default is 16000.

route-policy-name: Specifies a routing policy name, a case-sensitive string of 1 to 63 characters.

The arguments *half-life-reachable*, *half-life-unreachable*, *reuse*, *suppress*, and *ceiling* are mutually dependent. After you configure any one of them, you must specify all the others accordingly.

Description

Use **dampening** to configure IPv6 MBGP route dampening.

Use **undo dampening** to disable route dampening.

By default, route dampening is not configured.

Related commands: **display bgp ipv6 multicast routing-table dampened**, **display bgp ipv6 multicast routing-table dampening parameter**, **display bgp ipv6 multicast routing-table flap-info**, **reset bgp ipv6 dampening**, and **reset bgp ipv6 flap-info**.

Examples

```
# In IPv6 MBGP address family view, configure route dampening.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] dampening 10 10 1000 3000 10000
```

default local-preference (IPv6 MBGP address family view)

Syntax

default local-preference *value*

undo default local-preference

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

value: Specifies the 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.

By default, the default local preference is 100.

Using this command can affect IPv6 MBGP route selection.

Examples

```
# In IPv6 MBGP address family view, set the default local preference to 180.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] default local-preference 180
```

default med (IPv6 MBGP address family view)

Syntax

default med *med-value*

undo default med

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

med-value: Specifies the default 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 the local preference, the MED is exchanged between ASs and stays in the AS after 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 selects the best route depending on the MED value. If all the other conditions are the same, the system selects the route with the lowest MED as the best external route.

Examples

```
# Devices A and B belong to AS 100 and device C belongs to AS 200. Device 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 multicast
[Sysname-bgp-af-ipv6-mul] default med 25
```

default-route imported (IPv6 MBGP address family view)

Syntax

default-route imported

undo default-route imported

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

None

Description

Use **default-route imported** to enable default route redistribution into the IPv6 MBGP routing table.

Use **undo default-route imported** to disable the redistribution.

By default, default route redistribution is disabled.

Examples

Enable default and OSPFv3 route redistribution into IPv6 MBGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] default-route imported
[Sysname-bgp-af-ipv6-mul] import-route ospfv3 1
```

display bgp ipv6 multicast group

Syntax

```
display bgp ipv6 multicast group [ ipv6-group-name ] [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-group-name: Specifies a 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 multicast group** to display IPv6 MBGP peer group information.

If no *ipv6-group-name* is specified, information about all peer groups is displayed.

Examples

Display information about the IPv6 MBGP peer group **aaa**.

```
<Sysname> display bgp ipv6 multicast group aaa
```

```

BGP peer-group is aaa
remote AS number not specified
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
20:20::20:1  200      170      141      0      2 02:13:35  Established

```

Table 89 Command output

Field	Description
BGP peer-group	Name of the IPv6 MBGP peer group.
remote AS	AS number of the IPv6 MBGP peer group.
Type	Type of the IPv6 MBGP peer group.
Maximum allowed prefix number	Maximum number of prefixes allowed to be received from the IPv6 MBGP peer group.
Threshold	Threshold value.
Configured hold timer value	Hold-timer value.
Keepalive timer value	Keepalive interval.
Minimum time between advertisement runs	Minimum interval for route advertisement.
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 route-refresh messages that carry the ORF information, and the peer can receive route-refresh messages that carry the ORF information. If receive is displayed, the local BGP router can receive route-refresh messages that carry the ORF information, and the peer can send route-refresh messages that carry 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.
Members	Group members.
Peer	IPv6 address of the peer.
AS	AS number.

Field	Description
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 a session/lasting time of present state (when no session is established).
State	Peer state machine .

display bgp ipv6 multicast network

Syntax

display bgp ipv6 multicast 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 multicast network** to display the IPv6 MBGP routes advertised with the **network** command.

Examples

Display IPv6 MBGP routes advertised with the **network** command.

```
<Sysname> display bgp ipv6 multicast network
  BGP Local Router ID is 1.1.1.2.
  Local AS Number is 200.
  Network          Mask          Route-policy      Short-cut
  -----
  2002::           64
  2001::           64                Short-cut
```

Table 90 Command output

Field	Description
BGP Local Router ID	BGP local router ID

Field	Description
Local AS Number	Local AS number
Network	Network address
Mask	Prefix length of the address
Route-policy	Routing policy configured
Short-cut	Shortcut route

display bgp ipv6 multicast paths

Syntax

```
display bgp ipv6 multicast paths [ as-regular-expression | | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

as-regular-expression: Specifies an AS path regular expression.

|: 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 multicast paths** to display AS path information.

If no parameter is specified, this command displays all AS path information.

Examples

```
# Display AS path information.
```

```
<Sysname> display bgp ipv6 multicast paths
```

Address	Hash	Refcount	MED	Path/Origin
0x5917098	1	1	0	i
0x59171D0	9	2	0	100i

Table 91 Command output

Field	Description
Address	Route address in the local database, in dotted hexadecimal notation.
Hash	Hash index.

Field	Description
Refcount	Count of the routes that referenced the path.
MED	MED of the path.
Path	AS_PATH attribute of the route, recording the ASs that it has passed, used to avoid routing loops.
Origin	<p>ORIGIN attribute of the route:</p> <ul style="list-style-type: none"> i—Indicates that the route is interior to the AS. Summary routes and routes injected via the network command are considered IGP routes. e—Indicates that a route is learned from the exterior gateway protocol (EGP). ?—Indicates that the origin of the route is unknown and the route is learned through some other means. BGP sets the ORIGIN attribute of routes learned from other IGP protocols to incomplete.

display bgp ipv6 multicast peer

Syntax

```
display bgp ipv6 multicast peer [ [ ipv6-address ] verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Specifies an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

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 multicast peer** to display IPv6 MBGP peer information or peer group information.

If no parameter is specified, information about all IPv6 MBGP peers and peer groups is displayed.

Examples

```
# Display all IPv6 MBGP peer information.
<Sysname> display bgp ipv6 multicast peer
```

```

BGP local router ID : 2.2.2.2
Local AS number : 100
Total number of peers : 1                Peers in established state : 0

Peer                AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
2000::1            100      1         1       0      0 00:00:51 Active

```

Table 92 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 BGP peers in established state
Peer	IPv6 address of the peer
V	Peer BGP version
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	Lasting time of the session/Lasting time of the present state (when no session is established)
State	Peer state machine

display bgp ipv6 multicast peer received ipv6-prefix

Syntax

```

display bgp ipv6 multicast peer ipv6-address received ipv6-prefix [ | { begin | exclude | include }
regular-expression ]

```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Specifies the 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 multicast 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 multicast 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 93 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, which indicates that the mask length must be greater than or equal to the specific value
le	Less-equal, which indicates that the mask length must be less than or equal to the specific value

display bgp ipv6 multicast routing-table

Syntax

```
display bgp ipv6 multicast routing-table [ ipv6-address prefix-length ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Specifies a destination IPv6 address.

prefix-length: Specifies the 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 multicast routing-table** to display IPv6 MBGP routing information.

Examples

Display IPv6 MBGP routing information.

```
<Sysname> display bgp ipv6 multicast 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 94 Command output

Field	Description
Local router ID	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.
Origin	ORIGIN attributes: <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.

Field	Description
PrefixLen	Prefix length of the address.
NextHop	Next hop IP address.
MED	Multi-Exit Discriminator.
LocPrf	Local precedence.
Path	AS_PATH attribute of the path, recording the ASs that it has passed to avoid routing loops.
PrefVal	Preferred value for a route.
Label	Label.
Ogn	<p>ORIGIN attribute of the route:</p> <ul style="list-style-type: none"> • i—Indicates that the route is interior to the AS. Summary routes and routes injected via the network command are considered IGP routes. • e—Indicates that the route is learned from the Exterior Gateway Protocol (EGP). • ?—Indicates that the origin of the route is unknown and the route is learned by some other means. BGP sets the ORIGIN attribute of routes learned from other IGP protocols to incomplete.

display bgp ipv6 multicast routing-table as-path-acl

Syntax

```
display bgp ipv6 multicast 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 that matches an AS path list numbered 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 multicast routing-table as-path-acl** to display the IPv6 MBGP routes that match the specified AS path list.

Examples

```
# Display the IPv6 MBGP routes that match AS path list 20.
<Sysname> display bgp ipv6 multicast 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 more information about the fields, see [Table 94](#).

display bgp ipv6 multicast routing-table community

Syntax

```
display bgp ipv6 multicast 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: Specifies a community number. Both *aa* and *nn* are in the range of 0 to 65535.

&<1-13>: Specifies that you can provide up to 13 community numbers.

no-advertise: Displays the IPv6 MBGP routes that cannot be advertised to any peer.

no-export: Displays the IPv6 MBGP routes that cannot be advertised out of the AS. If a confederation is configured, it displays the routes that cannot be advertised out of the confederation, but can be advertised to other sub-ASs in the confederation.

no-export-subconfed: Displays the IPv6 MBGP routes that cannot be advertised out of the local AS, or to other sub-ASs in the confederation.

whole-match: Displays the IPv6 MBGP routes exactly that match 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 multicast routing-table community** to display the IPv6 MBGP routing information with the specified IPv6 MBGP COMMUNITY attribute.

Examples

Display IPv6 MBGP routing information with the community attribute NO_EXPORT.

```
<Sysname> display bgp ipv6 multicast 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 more information about the fields, see [Table 94](#).

display bgp ipv6 multicast routing-table community-list

Syntax

```
display bgp ipv6 multicast 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 the IPv6 MBGP routes exactly that match the COMMUNITY attributes defined in 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 ipv6 multicast routing-table community-list** to display the IPv6 MBGP routing information that matches the specified IPv6 MBGP community list.

Examples

```
# Display the IPv6 MBGP routing information that matches the community list
<Sysname> display bgp ipv6 multicast 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 more information about the fields, see [Table 94](#).

display bgp ipv6 multicast routing-table dampened

Syntax

```
display bgp ipv6 multicast 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 multicast routing-table dampened** to display the dampened IPv6 MBGP routes.

Examples

```
# Display dampened IPv6 MBGP routing information
<Sysname> display bgp ipv6 multicast 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 95 Command output

Field	Description
From	IP address from which the route was received.
Reuse	Route reuse time, namely, the period of time before the unusable route becomes usable.

For more information about the fields, see [Table 94](#).

display bgp ipv6 multicast routing-table dampening parameter

Syntax

```
display bgp ipv6 multicast 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 multicast routing-table dampening parameter** to display IPv6 MBGP routing dampening parameters.

Related commands: **dampening**.

Examples

```
# Display IPv6 MBGP dampening parameter information.
<Sysname> display bgp ipv6 multicast 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 96 Command output

Field	Description
Maximum Suppress Time	Maximum suppress time
Ceiling Value	Ceiling penalty value
Reuse Value	Limit for a route to be desuppressed
Reach HalfLife Time(in second)	Half-life of reachable routes
Unreach HalfLife Time(in second)	Half-life of unreachable routes
Suppress-Limit	Limit for routes to be suppressed

display bgp ipv6 multicast routing-table different-origin-as

Syntax

```
display bgp ipv6 multicast 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 multicast routing-table different-origin-as** to display IPv6 MBGP routes originating from different autonomous systems.

Examples

```
# Display IPv6 MBGP routing information from different ASs  
<Sysname> display bgp ipv6 multicast 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 more information about the fields, see [Table 94](#).

display bgp ipv6 multicast routing-table flap-info

Syntax

```
display bgp ipv6 multicast 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: Specifies an AS path regular expression to be matched.

as-path-acl-number: Specifies the number of the specified AS path list to be matched, ranging from 1 to 256.

ipv6-address: Specifies the IPv6 address of a route to be displayed.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 1 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 multicast routing-table flap-info** to display IPv6 MBGP routing flap statistics.

Examples

```
# Display IPv6 MBGP routing flap statistics
```

```
<Sysname> display bgp ipv6 multicast 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 97 Command output

Field	Description
Flaps	Number of flaps
Duration	Duration of the flapping
Reuse	Reuse value

For more information about the fields, see [Table 94](#).

display bgp ipv6 multicast routing-table peer

Syntax

```
display bgp ipv6 multicast routing-table peer 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

ipv6-address: Specifies the IPv6 peer to be displayed.

advertised-routes: Specifies routing information advertised to the specified peer.

received-routes: Specifies routing information received from the specified peer.

network-address prefix-length: Specifies 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 multicast routing-table peer** to display the routing information advertised to or received from the specified IPv6 MBGP peer.

Examples

```
# Display the routing information advertised to the specified IPv6 MBGP peer.
```

```
<Sysname> display bgp ipv6 multicast 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 more information about the fields, see [Table 94](#).

display bgp ipv6 multicast routing-table regular-expression

Syntax

```
display bgp ipv6 multicast routing-table regular-expression as-regular-expression
```

View

Any view

Default level

1: Monitor level

Parameters

as-regular-expression: Specifies an AS path regular expression.

Description

Use **display bgp ipv6 multicast routing-table regular-expression** to display the IPv6 MBGP routes that match the specified AS regular expression.

Examples

```
# Display IPv6 MBGP routing information that matches the specified AS regular expression.
```

```
<Sysname> display bgp ipv6 multicast 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 more information about the fields, see [Table 94](#).

display bgp ipv6 multicast routing-table statistic

Syntax

```
display bgp ipv6 multicast 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 multicast routing-table statistic** to display IPv6 MBGP routing statistics.

Examples

```
# Display IPv6 MBGP routing statistics
<Sysname> display bgp ipv6 multicast routing-table statistic

Total Number of Routes: 1
```

display ipv6 multicast routing-table

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

verbose: Displays detailed routing table information, including both active and inactive routes. With this argument absent, the command displays brief information about active IPv6 MBGP routes only.

|: 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 multicast routing-table** to display the IPv6 MBGP routing table.

Active and inactive routes might coexist in the IPv6 MBGP routing table. Active routes are the optimal routes used for RPF check.

Examples

```
# Display brief IPv6 MBGP routing table information.
<Sysname> display ipv6 multicast routing-table
Routing Table :
                Destinations : 4          Routes : 4
```

```
Destination: 100::1/128                Protocol : Direct
NextHop      : ::1                      Preference: 0
Interface    : InLoop0                  Cost      : 0
```

Table 98 Command output

Field	Description
Destination	Destination IPv6 address
Protocol	Routing protocol
Nexthop	Next hop IP address
Preference	Route preference
Interface	Outbound interface
Cost	Route cost

```
# Display detailed IPv6 MBGP routing table information.
<Sysname> display ipv6 multicast routing-table verbose
Routing Table :
                Destinations : 1          Routes : 1
```

```
Destination      : ::1                PrefixLength : 128
NextHop          : ::1                Preference   : 0
RelayNextHop     : ::                Tag          : 0H
Neighbour        : ::                ProcessID    : 0
Interface        : InLoopBack0        Protocol     : Direct
State            : Active NoAdv       Cost         : 0
Tunnel ID        : 0x0                Label        : NULL
Age              : 17073sec
```

Table 99 Command output

Field	Description
Destination	Destination IPv6 address
PrefixLength	Prefix length of the address

Field	Description
NextHop	Next hop IP address
Preference	Route preference
RelayNextHop	Recursive next hop
Tag	Route tag
Neighbour	Neighbor address
ProcessID	Process ID
Interface	Outbound interface
Protocol	Routing protocol
State	Status of the route: Active, Inactive, Adv, or NoAdv
Cost	Route cost
Tunnel ID	Tunnel ID
Label	Label
Age	Time elapsed since the route was generated

display ipv6 multicast routing-table *ipv6-address*

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Specifies a destination IPv6 address.

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

longer-match: Displays the routes that match the specified prefix.

verbose: Displays both detailed active and inactive routing information permitted by the ACL. Without this keyword, only the brief information about active routes permitted by the ACL 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 multicast routing-table** *ipv6-address* to display the multicast routing information for the specified destination IPv6 address.

Examples

Display brief information about the specified multicast route.

```
<Sysname> display ipv6 multicast routing-table 100::1 128
Routing Table:
Summary Count 1
Destination: 100::1/128                Protocol   : Direct
NextHop      : ::1                      Preference: 0
Interface   : InLoop0                  Cost       : 0
```

Display the brief route information that falls into the specified network.

```
<Sysname> display ipv6 multicast routing-table 4:: 16 longer-match
Routing Tables:
Summary Count 2
Destination: 4::                        Protocol   : Static
NextHop      : ::1                      Preference: 0
Interface   : Vlan-interface1          Cost       : 0

Destination: 4:4::                      Protocol   : Static
NextHop      : 3::1                     Preference: 60
Interface   : Vlan-interface1          Cost       : 0
```

Display the detailed route information that falls into the specified network.

```
<Sysname> display ipv6 multicast routing-table 4:4:: 32 verbose
Routing Tables:
Summary count:1
Destination: 4:4::                      Protocol   : Static
NextHop      : 3::1                     Preference: 60
Interface   : Vlan-interface1          Cost       : 0
```

filter-policy export (IPv6 MBGP address family view)

Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } export [ protocol process-id ]
undo filter-policy export [ protocol process-id ]
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

acl6-number: Specifies a basic or advanced ACL 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** at present. If no protocol is specified, all routes will be filtered when advertised.

process-id: Specifies the process ID of the routing protocol, in the range of 1 to 65535. This argument is available when the protocol is **isisv6**, **ospfv3**, or **ripng**.

Description

Use **filter-policy export** to filter outgoing routes by using a specified filter.

Use **undo filter-policy export** to cancel the filtering of outgoing routes.

By default, no outgoing 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 are filtered.

Examples

```
# Reference IPv6 ACL 2001 to filter all outgoing IPv6 MBGP routes.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] filter-policy 2001 export
```

filter-policy import (IPv6 MBGP address family view)

Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } import
undo filter-policy import
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

acl6-number: Specifies the number of a basic or advanced IPv6 ACL 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.

Description

Use **filter-policy import** to configure the filtering of inbound routing information using a specified filter.

Use **undo filter-policy import** to cancel the filtering of inbound routing information.

By default, inbound IPv6 MBGP routes are not filtered.

Examples

```
# Reference IPv6 ACL 2000 to filter all inbound IPv6 MBGP routes.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] filter-policy 2000 import
```

import-route (IPv6 MBGP address family view)

Syntax

```
import-route protocol [ process-id [ med med-value | route-policy route-policy-name ] * ]  
undo import-route protocol [ process-id ]
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

protocol: Redistributes routes from the protocol, which can be **direct**, **isisv6**, **ospfv3**, **ripng** or **static** at present.

process-id: Specifies a process ID, in the range of 1 to 65535. This argument is available when the protocol is **isisv6**, **ospfv3**, or **ripng**.

med-value: Specifies the default MED value, in the range of 0 to 4294967295. If no MED is specified, the cost of a redistributed route will be used as its MED in the BGP routing domain.

route-policy-name: Specifies the name of a routing policy used to filter redistributed routes, a case-sensitive string of 1 to 63 characters.

Description

Use **import-route** to redistribute routes from another routing protocol.

Use **undo import-route** to disable route redistribution from a routing protocol.

By default, IPv6 MBGP does not redistribute routes from any routing protocol.

The ORIGIN attribute of routes redistributed through the **import-route** command is incomplete.

Examples

```
# Redistribute routes from RIPng 1.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family multicast  
[Sysname-bgp-af-ipv6-mul] import-route ripng 1
```

ipv6-family multicast

Syntax

```
ipv6-family multicast  
undo ipv6-family multicast
```

View

BGP view

Default level

2: System level

Parameters

None

Description

Use **ipv6-family multicast** to enter IPv6 MBGP address family view.

Use **undo ipv6-family multicast** to remove all the configurations in the IPv6 MBGP address family view.

IPv4 BGP unicast view is the default.

If the **ipv6-family** command is not configured in BGP view, you cannot directly configure the **ipv6-family multicast** command in BGP view (see example I). If the **ipv6-family** command is configured in BGP view, you can directly configure the **ipv6-family multicast** command in BGP view (see example II).

Examples

- Example I

Enter IPv6 MBGP address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
Error: Please configure IPv6 Unicast address-family first
```

The error information indicates that the **ipv6-family** command is not configured.

```
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]
```

- Example II

Enter IPv6 MBGP address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]
```

network (IPv6 MBGP address family view)

Syntax

network *ipv6-address prefix-length* [**route-policy** *route-policy-name* | **short-cut**]

undo network *ipv6-address prefix-length* [**short-cut**]

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

ipv6-address: IPv6 address prefix.

prefix-length: Prefix length of the IPv6 address, in the range of 0 to 128.

short-cut: If the keyword is specified for an IPv6 multicast eBGP route, the route will use the local preference rather than its own preference, and therefore it probably does not become the optimal route.

route-policy-name: Name of a routing policy, a case-sensitive string of 1 to 63 characters.

Description

Use **network** to inject a network to the IPv6 MBGP routing table.

Use **undo network** to remove a network from the routing table.

By default, no network is injected.

The network to be injected must exist in the local IPv6 routing table. You can use a routing policy to control the advertisement of the route with more flexibility.

The route injected through the **network** command has the IGP origin attribute.

Examples

```
# Inject the network 2002::/16.
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] network 2002:: 16
```

peer advertise-community (IPv6 MBGP address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } advertise-community
undo peer { ipv6-group-name | ipv6-address } advertise-community
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

Description

Use **peer advertise-community** to advertise the COMMUNITY attribute to an IPv6 MBGP peer or a peer group.

Use **undo peer advertise-community** to remove the configuration.

By default, no COMMUNITY attribute is advertised to any IPv6 MBGP peer group/peer.

Examples

```
# Advertise the COMMUNITY attribute to the IPv6 MBGP 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] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
```

```
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 advertise-community
```

peer advertise-ext-community (IPv6 MBGP address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } advertise-ext-community
```

```
undo peer { ipv6-group-name | ipv6-address } advertise-ext-community
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

group-name: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

Description

Use **peer advertise-ext-community** to advertise the extended community attribute to an IPv6 MBGP peer or a peer group.

Use **undo peer advertise-ext-community** to remove the configuration.

By default, no extended community attribute is advertised to any IPv6 MBGP peer or peer group.

Examples

```
# Advertise the extended community attribute to the IPv6 MBGP 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] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 advertise-ext-community
```

peer allow-as-loop (IPv6 MBGP address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } allow-as-loop [ number ]
```

```
undo peer { ipv6-group-name | ipv6-address } allow-as-loop
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

number: Specifies the number of times that the local AS number can appear in the AS PATH of routes from the peer or the 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 or a peer group, and to configure the times that the local AS number can appear.

Use **undo peer allow-as-loop** to disable the function.

The local AS number cannot appear in routes from the peer or the peer group.

Examples

Configure the number of times that the local AS number can appear in the AS path of routes from the peer as 2.

```
<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] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 allow-as-loop 2
```

peer as-path-acl (IPv6 MBGP address family view)

Syntax

```
peer { ipv6-address | ipv6-group-name } as-path-acl as-path-acl-number { export | import }
undo peer { ipv6-address | ipv6-group-name } as-path-acl as-path-acl-number { export | import }
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

as-path-acl-number: Specifies an AS path list number, in the range of 1 to 256.

import: Filters incoming IPv6 MBGP routes.

export: Filters outgoing IPv6 MBGP routes.

Description

Use **peer as-path-acl** to specify an AS path list to filter routes incoming from or outgoing to an IPv6 MBGP peer or a peer group.

Use **undo peer as-path-acl** to remove the configuration.

By default, no AS path list is specified for filtering the routes from/to an IPv6 MBGP peer or a peer group.

Examples

```
# Specify AS path list 3 to filter routes outgoing to the IPv6 MBGP 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] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 as-path-acl 3 export
```

peer capability-advertise orf (IPv6 MBGP address family view)

Syntax

```
peer { group-name | ipv6-address } capability-advertise orf ipv6-prefix { both | receive | send }
undo peer { group-name | ipv6-address } capability-advertise orf ipv6-prefix { both | receive | send }
```

View

IPv6 address family view

Default level

2: System level

Parameters

group-name: Specifies a peer group by its name, a string of 1 to 47 characters.

ipv6-address: Specifies a peer by its IPv6 address.

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 that carry the standard ORF information from the peer or send route-refresh messages that carry the standard ORF information to the peer. For non-standard ORF capability negotiation, you must also 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 100 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, respectively.

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] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 capability-advertise orf ipv6-prefix both
```

peer default-route-advertise (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **default-route-advertise** [**route-policy** *route-policy-name*]
undo peer { *ipv6-group-name* | *ipv6-address* } **default-route-advertise**

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

route-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Description

Use **peer default-route-advertise** to advertise a default route to an IPv6 MBGP peer or a peer group.

Use **undo peer default-route-advertise** to disable default route advertisement to an IPv6 MBGP peer or a peer group.

By default, no default route is advertised to any IPv6 MBGP peer or peer group.

When you use this command used, the router unconditionally sends a default route with the next hop as itself to the IPv6 MBGP peer or peer group, regardless of whether the default route is available in the routing table.

Examples

```
# Advertise a default route to the IPv6 MBGP 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] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 default-route-advertise
```

peer enable (IPv6 MBGP address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } enable
undo peer { ipv6-group-name | ipv6-address } enable
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters. You must create the IPv6 MBGP peer group in IPv6 MBGP view before you can activate it here.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

Description

Use **peer enable** to enable an IPv6 MBGP peer or peer group.

Use **undo peer enable** to disable an IPv6 MBGP peer or peer group.

By default, no IPv6 MBGP peer or peer group is enabled.

If an IPv6 MBGP peer or peer group is disabled, the router does not exchange routing information with it.

Examples

```
# Enable IPv6 MBGP 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] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
```

peer filter-policy (IPv6 MBGP address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } filter-policy acl6-number { import | export }  
undo peer { ipv6-group-name | ipv6-address } filter-policy [ acl6-number ] { import | export }
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

acl6-number: Specifies an IPv6 ACL number, in the range of 2000 to 3999.

import: Applies the filter to routes received from the IPv6 MBGP peer or the peer group.

export: Applies the filter to routes advertised to the IPv6 MBGP peer or the peer group.

Description

Use **peer filter-policy** to configure an IPv6 ACL-based filter policy for an IPv6 MBGP peer or peer group.

Use **undo peer filter-policy** to remove the configuration.

By default, no IPv6 ACL-based filter policy is configured for any IPv6 MBGP peer or peer group.

Examples

```
# Apply IPv6 ACL 2000 to filter routes advertised to the IPv6 MBGP 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 as-number 100  
[Sysname-bgp-af-ipv6] quit  
[Sysname-bgp] ipv6-family multicast  
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable  
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 filter-policy 2000 export
```

peer group (IPv6 MBGP address family view)

Syntax

```
peer ipv6-address group ipv6-group-name  
undo peer ipv6-address group ipv6-group-name
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

Description

Use **peer group** to add an IPv6 MBGP peer to a configured IPv6 MBGP peer group.

Use **undo peer group** to delete a specified IPv6 MBGP peer from an IPv6 MBGP peer group.

By default, no IPv6 MBGP peer is added to any IPv6 MBGP peer group.

Examples

Create an IPv6 MBGP peer group named **test** and add the IPv6 MBGP 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
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer test enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 group test
```

peer ipv6-prefix (IPv6 MBGP address family view)

Syntax

peer { *ipv6-group-name* | *ipv6-address* } **ipv6-prefix** *ipv6-prefix-name* { **import** | **export** }

undo peer { *ipv6-group-name* | *ipv6-address* } **ipv6-prefix** { **import** | **export** }

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

ipv6-prefix-name: Specifies an IPv6 prefix list name, a string of 1 to 19 characters.

import: Applies the IPv6 prefix list to filter routes received from the IPv6 MBGP peer or the peer group.

export: Applies the IPv6 prefix list to filter routes advertised to the IPv6 MBGP peer or the peer group.

Description

Use **peer ipv6-prefix** to specify an IPv6 prefix list to filter routes incoming from or outgoing to an IPv6 MBGP peer or peer group.

Use **undo peer ipv6-prefix** to remove the configuration.

By default, no IPv6 prefix list-based filtering is configured.

Examples

```
# Apply the IPv6 ACL list1 to filter routes advertised to the IPv6 MBGP 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 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 ipv6-prefix list1 export
```

peer keep-all-routes (IPv6 MBGP address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } keep-all-routes
```

```
undo peer { ipv6-group-name | ipv6-address } keep-all-routes
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters.

ipv6-address: IPv6 address of an IPv6 MBGP peer.

Description

Use **peer keep-all-routes** to save the original routing information from an IPv6 MBGP peer or peer group, including the routes that fail to pass the inbound filtering policy (if configured).

Use **undo peer keep-all-routes** to disable this function.

By default, the original routing information from an IPv6 MBGP peer or peer group is not saved.

Examples

```
# Save the original routing information from IPv6 MBGP 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] quit
[Sysname-bgp] ipv6-family multicast
```

```
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 keep-all-routes
```

peer next-hop-local (IPv6 MBGP 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 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

Description

Use **peer next-hop-local** to configure the next hop of routes advertised to an IPv6 MBGP peer or a peer group as the local router.

Use **undo peer next-hop-local** to restore the default.

By default, an IPv6 MBGP speaker specifies itself as the next hop for routes outgoing to an IPv6 multicast eBGP peer or a peer group rather than an IPv6 multicast iBGP peer or a peer group.

Examples

```
# Set the next hop of routes advertised to iBGP peer group test to the advertising router.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test internal
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer test enable
[Sysname-bgp-af-ipv6-mul] peer test next-hop-local
```

peer preferred-value (IPv6 MBGP address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } preferred-value value
undo peer { ipv6-group-name | ipv6-address } preferred-value
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

value: Specifies a preferred value, in the range of 0 to 65535.

Description

Use **peer preferred-value** to assign a preferred value to routes received from an IPv6 MBGP peer or peer group.

Use **undo peer preferred-value** to restore the default.

The preferred value defaults to 0.

Routes learned from peers each have a preferred value. Among multiple routes to the same destination, the route with the greatest preferred value is selected.

If you both reference a routing policy and use the **peer { ipv6-group-name | ipv6-address } preferred-value value** command to set a preferred value for routes from a peer, the routing policy sets the specified preferred value for the routes that match it. Other routes that do not match the routing policy use the value set with the **peer preferred-value** command. If the preferred value specified in the routing policy is zero, the routes that match it also use the value set with the **peer preferred-value** command.

To learn how to use a routing policy to set a preferred value, see the command **peer { group-name | ipv6-address } route-policy route-policy-name { import | export }** in this document, and the command **apply preferred-value preferred-value** in the *Layer 3—IP Routing Command Reference*.

Examples

```
# Configure a preferred value of 50 for routes from IPv6 MBGP 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] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 preferred-value 50
```

peer public-as-only (IPv6 MBGP 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 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

Description

Use **peer public-as-only** to disable IPv6 MBGP updates to a peer or a peer group from carrying private AS numbers.

Use **undo peer public-as-only** to allow IPv6 MBGP updates to a peer or a peer group to carry private AS numbers.

By default, private AS numbers can be carried in outbound IPv6 MBGP update packets.

The command does not take effect for IPv6 MBGP updates with both public and private AS numbers. The range of private AS numbers is from 64512 to 65535.

Examples

```
# Disable updates sent to IPv6 MBGP peer 1:2::3:4 from carrying private AS numbers.
```

```
<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] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 public-as-only
```

peer reflect-client (IPv6 MBGP address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } reflect-client
```

```
undo peer { ipv6-group-name | ipv6-address } reflect-client
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

Description

Use **peer reflect-client** to configure the router as a route reflector and specify an IPv6 MBGP peer or a peer group as its 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 internal
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer test enable
[Sysname-bgp-af-ipv6-mul] peer test reflect-client
```

peer route-limit (IPv6 MBGP address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } route-limit limit [ percentage ]
undo peer { ipv6-group-name | ipv6-address } route-limit
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

limit: Specifies the upper limit of IPv6 address prefixes that can be received from the peer or peer group, in the range of 1 to 6144.

percentage: Percentage at which the system will generate alarm information if the number of received routes divided by the upper limit reaches it. The percentage is in the range of 1 to 100. The default is 75.

Description

Use **peer route-limit** to set the maximum number of IPv6 prefixes that can be received from an IPv6 MBGP peer or a peer group.

Use **undo peer route-limit** to restore the default.

By default, the IPv6 prefixes from an IPv6 MBGP peer or a peer group are unlimited.

The router removes the TCP connection when the number of IPv6 prefixes received from the peer exceeds the limit.

Examples

```
# Set the number of IPv6 address prefixes allowed to be received from the IPv6 MBGP peer 1:2::3:4 to 5000.
```

```
<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] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 route-limit 5000
```

peer route-policy (IPv6 MBGP address family view)

Syntax

```
peer { ipv6-group-name | ipv6-address } route-policy route-policy-name { import | export }  
undo peer { ipv6-group-name | ipv6-address } route-policy route-policy-name { import | export }
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

ipv6-group-name: Specifies an IPv6 MBGP peer group by its name, a string of 1 to 47 characters.

ipv6-address: Specifies an IPv6 MBGP peer by its IP address.

route-policy-name: Specifies a routing policy name, a case-sensitive string of 1 to 63 characters.

import: Applies the routing policy to routes received from the IPv6 MBGP peer or the peer group.

export: Applies the routing policy to routes advertised to the IPv6 MBGP peer or the peer group.

Description

Use **peer route-policy** to apply a routing policy to routes incoming from or outgoing to an IPv6 MBGP peer or peer group.

Use **undo peer route-policy** to remove the configuration.

By default, no routing policy is applied to the routes incoming from or outgoing to an IPv6 MBGP peer or peer group.

The **if-match interface** clause in the routing policy referenced by the **peer route-policy** command is not applied.

For more information, see *Layer 3—IP Routing Command Reference*.

Examples

Apply the routing policy **test-policy** to routes received from the IPv6 MBGP 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] quit  
[Sysname-bgp] ipv6-family multicast  
[Sysname-bgp-af-ipv6-mul] peer test enable  
[Sysname-bgp-af-ipv6-mul] peer test route-policy test-policy import
```

preference (IPv6 MBGP address family view)

Syntax

```
preference { external-preference internal-preference local-preference | route-policy route-policy-name }  
undo preference
```

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

external-preference: Specifies the preference of IPv6 multicast eBGP routes, in the range of 1 to 255. An IPv6 multicast eBGP route is learned from an IPv6 multicast eBGP peer.

internal-preference: Specifies the preference of IPv6 multicast iBGP routes, in the range of 1 to 255. An IPv6 multicast iBGP route is learned from an IPv6 multicast iBGP peer.

local-preference: Specifies the preference of locally generated IPv6 MBGP routes, in the range of 1 to 255.

route-policy-name: Specifies a routing policy name, a case-sensitive string of 1 to 63 characters. By using a routing policy, you can configure the preferences for the routes that match the filtering conditions. For the unmatched routes, the default preferences are adopted.

Description

Use **preference** to configure preferences for IPv6 multicast eBGP, IPv6 multicast iBGP, and local IPv6 MBGP routes.

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

The default preference values of external, internal and local IPv6 MBGP routes are 255, 255, and 130, respectively.

The greater the preference value is, the lower the preference is.

Examples

```
# Configure preferences for IPv6 multicast eBGP, IPv6 multicast iBGP, and local IPv6 MBGP routes as 20,  
20, and 200.
```

```
<Sysname> system-view  
[Sysname]bgp 100  
[Sysname-bgp] ipv6-family multicast  
[Sysname-bgp-af-ipv6-mul] preference 20 20 200
```

reflect between-clients (IPv6 MBGP address family view)

Syntax

```
reflect between-clients  
undo reflect between-clients
```

View

IPv6 MBGP 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 you configure a route reflector, it reflects the routes of a client to the other clients. If the clients of a route reflector are fully meshed, you must disable route reflection between clients to reduce routing costs.

Related commands: **peer reflect-client** and **reflector cluster-id**.

Examples

```
# Enable route reflection between clients
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] reflect between-clients
```

reflector cluster-id (IPv6 MBGP address family view)

Syntax

reflector cluster-id *cluster-id*

undo reflector cluster-id

View

IPv6 MBGP address family view

Default level

2: System level

Parameters

cluster-id: 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, each route reflector uses its router ID as the cluster ID.

The router ID of the route reflector is the ID of the cluster. You can configure multiple route reflectors to improve network stability. If a cluster has multiple route reflectors, you must use the **reflector cluster-id** command to specify the same cluster ID for these route reflectors to avoid routing loops.

Related commands: **peer reflect-client** and **reflect between-clients**.

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 multicast
[Sysname-bgp-af-ipv6-mul] reflector cluster-id 50
```

refresh bgp ipv6 multicast

Syntax

```
refresh bgp ipv6 multicast { ipv6-address | all | external | group ipv6-group-name | internal } { export | import }
```

View

User view

Default level

1: Monitor level

Parameters

ipv6-address: Soft-resets the connection to the specified IPv6 MBGP peer.

all: Soft-resets all IPv6 MBGP connections.

external: Soft-resets IPv6 multicast eBGP connections.

group *ipv6-group-name*: Soft-resets connections to an IPv6 multicast peer group. The name of the peer group is a string of 1 to 47 characters.

internal: Soft-resets IPv6 multicast iBGP connections.

export: Performs a soft-reset in an outbound direction.

import: Performs a soft-reset in an inbound direction.

Description

Use **refresh bgp ipv6 multicast** to soft-reset specified IPv6 MBGP connections. This command allows you to refresh the IPv6 MBGP routing table and apply a new policy without removing IPv6 MBGP connections.

To perform an IPv6 MBGP soft reset, be sure that all routers in the network should support route-refresh. If a peer that does not support route refresh exists in the network, use the **peer keep-all-routes** command on the local router to save all route updates from the peer before performing a soft reset.

Examples

```
# Soft-reset inbound IPv6 MBGP connections.
<Sysname> refresh bgp ipv6 multicast all import
```

reset bgp ipv6 multicast

Syntax

```
reset bgp ipv6 multicast { as-number | ipv6-address [ flap-info ] | all | group ipv6-group-name | external | internal }
```

View

User view

Default level

2: System level

Parameters

as-number: Resets the connections to IPv6 MBGP peers in the specified AS.

ipv6-address: Resets the connection to the specified peer.

flap-info: Clears routing flap information.

all: Resets all IPv6 MBGP connections.

group *ipv6-group-name*: Resets the connections to the specified IPv6 MBGP peer group.

external: Resets all the IPv6 multicast eBGP connections.

internal: Resets all the IPv6 multicast iBGP connections.

Description

Use **reset bgp ipv6 multicast** to reset specified IPv6 MBGP connections to reconnect to the peers.

Examples

```
# Reset all the IPv6 MBGP connections.  
<Sysname> reset bgp ipv6 multicast all
```

reset bgp ipv6 multicast dampening

Syntax

```
reset bgp ipv6 multicast dampening [ ipv6-address prefix-length ]
```

View

User view

Default level

1: Monitor level

Parameters

ipv6-address: Specifies a destination IPv6 address.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

Description

Use **reset bgp ipv6 multicast dampening** to clear route dampening information and release suppressed routes.

If no *ipv6-address prefix-length* is specified, all IPv6 MBGP route dampening information is cleared.

Examples

```
# Clear the dampening information of the route 2345::/64 and release the suppressed route.  
<Sysname> reset bgp ipv6 multicast dampening 2345::64
```

reset bgp ipv6 multicast flap-info

Syntax

```
reset bgp ipv6 multicast flap-info [ ipv6-address/prefix-length | regex as-path-regexp | as-path-acl as-path-acl-number ]
```

View

User view

Default level

1: Monitor level

Parameters

ipv6-address: Specifies an IPv6 address.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 1 to 128.

as-path-regexp: Clears the routing flap statistics for the routes that match the AS path regular expression.

as-path-acl-number: Clears the routing flap statistics for the routes that match the AS path list. The value of this argument is in the range of 1 to 256.

Description

Use **reset bgp ipv6 multicast flap-info** to clear IPv6 MBGP routing flap statistics.

If no parameters are specified, the flap statistics of all the routes will be cleared

Examples

Clear the flap statistics of all routes that match AS path list 10.

```
<Sysname> reset bgp ipv6 multicast flap-info as-path-acl 10
```

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](#) [J](#) [L](#) [M](#) [N](#) [O](#) [P](#) [R](#) [S](#) [T](#) [V](#)

A

aggregate (IPv6 MBGP address family view), [401](#)
aggregate (MBGP address family view), [196](#)
auto-rp enable, [109](#)

B

balance (IPv6 MBGP address family view), [402](#)
balance (MBGP address family view), [197](#)
bestroute as-path-neglect (IPv6 MBGP address family view), [403](#)
bestroute as-path-neglect (MBGP address family view), [198](#)
bestroute compare-med (IPv6 MBGP address family view), [403](#)
bestroute compare-med (MBGP address family view), [198](#)
bestroute med-confederation (IPv6 MBGP address family view), [404](#)
bestroute med-confederation (MBGP address family view), [199](#)
bidir-pim enable (IPv6 PIM view), [346](#)
bidir-pim enable (PIM view), [109](#)
bsm-fragment enable (IPv6 PIM view), [346](#)
bsm-fragment enable (PIM view), [110](#)
bsr-policy (IPv6 PIM view), [347](#)
bsr-policy (PIM view), [111](#)

C

cache-sa-enable, [172](#)
c-bsr (IPv6 PIM view), [348](#)
c-bsr (PIM view), [112](#)
c-bsr admin-scope (IPv6 PIM view), [348](#)
c-bsr admin-scope (PIM view), [113](#)
c-bsr global, [113](#)
c-bsr group, [114](#)
c-bsr hash-length (IPv6 PIM view), [349](#)
c-bsr hash-length (PIM view), [115](#)
c-bsr holdtime (IPv6 PIM view), [350](#)
c-bsr holdtime (PIM view), [116](#)

c-bsr interval (IPv6 PIM view), [350](#)
c-bsr interval (PIM view), [116](#)
c-bsr priority (IPv6 PIM view), [351](#)
c-bsr priority (PIM view), [117](#)
c-bsr scope, [351](#)
compare-different-as-med (IPv6 MBGP address family view), [404](#)
compare-different-as-med (MBGP address family view), [200](#)
c-rp (IPv6 PIM view), [352](#)
c-rp (PIM view), [118](#)
c-rp advertisement-interval (IPv6 PIM view), [353](#)
c-rp advertisement-interval (PIM view), [119](#)
c-rp holdtime (IPv6 PIM view), [354](#)
c-rp holdtime (PIM view), [120](#)
crp-policy (IPv6 PIM view), [355](#)
crp-policy (PIM view), [120](#)

D

dampening (IPv6 MBGP address family view), [405](#)
dampening (MBGP address family view), [200](#)
default local-preference (IPv6 MBGP address family view), [406](#)
default local-preference (MBGP address family view), [201](#)
default med (IPv6 MBGP address family view), [407](#)
default med (MBGP address family view), [202](#)
default-route imported (IPv6 MBGP address family view), [407](#)
default-route imported (MBGP address family view), [202](#)
delete ip rpf-route-static, [47](#)
display bgp ipv6 multicast group, [408](#)
display bgp ipv6 multicast network, [410](#)
display bgp ipv6 multicast paths, [411](#)
display bgp ipv6 multicast peer, [412](#)
display bgp ipv6 multicast peer received ipv6-prefix, [413](#)
display bgp ipv6 multicast routing-table, [414](#)

display bgp ipv6 multicast routing-table as-path-acl, [416](#)
display bgp ipv6 multicast routing-table community, [417](#)
display bgp ipv6 multicast routing-table community-list, [418](#)
display bgp ipv6 multicast routing-table dampened, [419](#)
display bgp ipv6 multicast routing-table dampening parameter, [420](#)
display bgp ipv6 multicast routing-table different-origin-as, [421](#)
display bgp ipv6 multicast routing-table flap-info, [422](#)
display bgp ipv6 multicast routing-table peer, [423](#)
display bgp ipv6 multicast routing-table regular-expression, [424](#)
display bgp ipv6 multicast routing-table statistic, [425](#)
display bgp multicast group, [207](#)
display bgp multicast network, [209](#)
display bgp multicast paths, [210](#)
display bgp multicast peer, [211](#)
display bgp multicast peer received ip-prefix, [214](#)
display bgp multicast routing-table, [215](#)
display bgp multicast routing-table as-path-acl, [216](#)
display bgp multicast routing-table cidr, [217](#)
display bgp multicast routing-table community, [218](#)
display bgp multicast routing-table community-list, [219](#)
display bgp multicast routing-table dampened, [220](#)
display bgp multicast routing-table dampening parameter, [221](#)
display bgp multicast routing-table different-origin-as, [222](#)
display bgp multicast routing-table flap-info, [223](#)
display bgp multicast routing-table peer, [224](#)
display bgp multicast routing-table regular-expression, [225](#)
display bgp multicast routing-table statistic, [226](#)
display igmp group, [67](#)
display igmp group port-info, [69](#)
display igmp host interface, [71](#)
display igmp host port-info, [72](#)
display igmp interface, [73](#)
display igmp proxying group, [75](#)
display igmp routing-table, [77](#)
display igmp ssm-mapping, [79](#)
display igmp ssm-mapping group, [80](#)
display igmp ssm-mapping host interface, [82](#)
display igmp-snooping group, [1](#)
display igmp-snooping host, [2](#)
display igmp-snooping statistics, [4](#)
display ip multicast routing-table, [203](#)
display ip multicast routing-table ip-address, [205](#)
display ipv6 multicast routing-table, [425](#)
display ipv6 multicast routing-table ipv6-address, [427](#)
display mac-address multicast, [5](#)
display mld group, [307](#)
display mld group port-info, [308](#)
display mld host interface, [310](#)
display mld host port-info, [311](#)
display mld interface, [313](#)
display mld proxying group, [315](#)
display mld routing-table, [316](#)
display mld ssm-mapping, [318](#)
display mld ssm-mapping group, [319](#)
display mld ssm-mapping host interface, [320](#)
display mld-snooping group, [249](#)
display mld-snooping host, [250](#)
display mld-snooping statistics, [252](#)
display msdp brief, [173](#)
display msdp peer-status, [174](#)
display msdp sa-cache, [177](#)
display msdp sa-count, [178](#)
display multicast boundary, [47](#)
display multicast forwarding-table, [49](#)
display multicast forwarding-table df-info, [51](#)
display multicast ipv6 boundary, [293](#)
display multicast ipv6 forwarding-table, [294](#)
display multicast ipv6 forwarding-table df-info, [297](#)
display multicast ipv6 routing-table, [298](#)
display multicast ipv6 rpf-info, [299](#)
display multicast routing-table, [53](#)
display multicast routing-table static, [55](#)
display multicast rpf-info, [56](#)
display multicast-vlan, [43](#)
display multicast-vlan ipv6, [289](#)
display pim bsr-info, [121](#)
display pim claimed-route, [123](#)
display pim control-message counters, [125](#)
display pim df-info, [127](#)
display pim grafts, [128](#)
display pim interface, [129](#)

- display pim ipv6 bsr-info, 355
- display pim ipv6 claimed-route, 357
- display pim ipv6 control-message counters, 358
- display pim ipv6 df-info, 360
- display pim ipv6 grafts, 361
- display pim ipv6 interface, 362
- display pim ipv6 join-prune, 364
- display pim ipv6 neighbor, 365
- display pim ipv6 routing-table, 367
- display pim ipv6 rp-info, 370
- display pim join-prune, 131
- display pim neighbor, 133
- display pim routing-table, 135
- display pim rp-info, 139
- display pim-snooping ipv6 neighbor, 284
- display pim-snooping ipv6 routing-table, 285
- display pim-snooping ipv6 statistics, 286
- display pim-snooping neighbor, 38
- display pim-snooping routing-table, 39
- display pim-snooping statistics, 40
- dot1 p-priority (IGMP-snooping view), 6
- dot1 p-priority (MLD-snooping view), 253
- dscp (IGMP view), 83
- dscp (IGMP-snooping view), 7
- dscp (IPv6 PIM view), 371
- dscp (MLD view), 321
- dscp (MLD-snooping view), 253
- dscp (PIM view), 140

E

- embedded-rp, 372
- encap-data-enable, 180

F

- fast-leave (IGMP view), 83
- fast-leave (IGMP-snooping view), 7
- fast-leave (MLD view), 322
- fast-leave (MLD-snooping view), 254
- filter-policy export (IPv6 MBGP address family view), 428
- filter-policy export (MBGP address family view), 226
- filter-policy import (IPv6 MBGP address family view), 429
- filter-policy import (MBGP address family view), 227

G

- group-policy (IGMP-snooping view), 8
- group-policy (MLD-snooping view), 255

H

- hello-option dr-priority (IPv6 PIM view), 373
- hello-option dr-priority (PIM view), 141
- hello-option holdtime (IPv6 PIM view), 373
- hello-option holdtime (PIM view), 141
- hello-option lan-delay (IPv6 PIM view), 374
- hello-option lan-delay (PIM view), 142
- hello-option neighbor-tracking (IPv6 PIM view), 375
- hello-option neighbor-tracking (PIM view), 143
- hello-option override-interval (IPv6 PIM view), 375
- hello-option override-interval (PIM view), 144
- holdtime assert (IPv6 PIM view), 376
- holdtime assert (PIM view), 144
- holdtime join-prune (IPv6 PIM view), 376
- holdtime join-prune (PIM view), 145
- host-aging-time (IGMP-snooping view), 9
- host-aging-time (MLD-snooping view), 256
- host-tracking (IGMP view), 84
- host-tracking (IGMP-snooping view), 10
- host-tracking (MLD view), 322
- host-tracking (MLD-snooping view), 256

I

- igmp, 85
- igmp enable, 86
- igmp fast-leave, 86
- igmp group-limit, 87
- igmp group-policy, 88
- igmp host-tracking, 89
- igmp last-member-query-interval, 89
- igmp max-response-time, 90
- igmp proxying enable, 90
- igmp proxying forwarding, 91
- igmp require-router-alert, 92
- igmp robust-count, 92
- igmp send-router-alert, 93
- igmp ssm-mapping enable, 94
- igmp startup-query-count, 94
- igmp startup-query-interval, 95
- igmp static-group, 95
- igmp timer other-querier-present, 96
- igmp timer query, 97
- igmp version, 98

- igmp-snooping, [10](#)
- igmp-snooping access-policy, [11](#)
- igmp-snooping dot1p-priority, [12](#)
- igmp-snooping drop-unknown, [12](#)
- igmp-snooping enable, [13](#)
- igmp-snooping fast-leave, [14](#)
- igmp-snooping general-query source-ip, [14](#)
- igmp-snooping group-limit, [15](#)
- igmp-snooping group-policy, [16](#)
- igmp-snooping host-aging-time, [17](#)
- igmp-snooping host-join, [18](#)
- igmp-snooping host-tracking, [19](#)
- igmp-snooping last-member-query-interval, [20](#)
- igmp-snooping leave source-ip, [20](#)
- igmp-snooping max-response-time, [21](#)
- igmp-snooping overflow-replace, [22](#)
- igmp-snooping proxying enable, [23](#)
- igmp-snooping querier, [23](#)
- igmp-snooping query-interval, [24](#)
- igmp-snooping report source-ip, [25](#)
- igmp-snooping router-aging-time, [26](#)
- igmp-snooping router-port-deny, [26](#)
- igmp-snooping source-deny, [27](#)
- igmp-snooping special-query source-ip, [28](#)
- igmp-snooping static-group, [29](#)
- igmp-snooping static-router-port, [30](#)
- igmp-snooping version, [30](#)
- import-route (IPv6 MBGP address family view), [430](#)
- import-route (MBGP address family view), [228](#)
- import-source, [180](#)
- ip rpf-route-static, [57](#)
- ipv4-family multicast, [229](#)
- ipv6-family multicast, [430](#)

J

- jp-pkt-size (IPv6 PIM view), [377](#)
- jp-pkt-size (PIM view), [146](#)
- jp-queue-size (IPv6 PIM view), [378](#)
- jp-queue-size (PIM view), [146](#)

L

- last-listener-query-interval (MLD view), [323](#)
- last-listener-query-interval (MLD-snooping view), [257](#)
- last-member-query-interval (IGMP view), [98](#)
- last-member-query-interval (IGMP-snooping view), [31](#)

M

- mac-address multicast, [32](#)
- max-response-time (IGMP view), [99](#)
- max-response-time (IGMP-snooping view), [33](#)
- max-response-time (MLD view), [324](#)
- max-response-time (MLD-snooping view), [257](#)
- mld, [324](#)
- mld enable, [325](#)
- mld fast-leave, [325](#)
- mld group-limit, [326](#)
- mld group-policy, [327](#)
- mld host-tracking, [328](#)
- mld last-listener-query-interval, [328](#)
- mld max-response-time, [329](#)
- mld proxying enable, [330](#)
- mld proxying forwarding, [330](#)
- mld require-router-alert, [331](#)
- mld robust-count, [332](#)
- mld send-router-alert, [332](#)
- mld ssm-mapping enable, [333](#)
- mld startup-query-count, [334](#)
- mld startup-query-interval, [334](#)
- mld static-group, [335](#)
- mld timer other-querier-present, [336](#)
- mld timer query, [336](#)
- mld version, [337](#)
- mld-snooping, [258](#)
- mld-snooping access-policy, [259](#)
- mld-snooping done source-ip, [259](#)
- mld-snooping dot1p-priority, [260](#)
- mld-snooping drop-unknown, [261](#)
- mld-snooping enable, [262](#)
- mld-snooping fast-leave, [262](#)
- mld-snooping general-query source-ip, [263](#)
- mld-snooping group-limit, [264](#)
- mld-snooping group-policy, [265](#)
- mld-snooping host-aging-time, [266](#)
- mld-snooping host-join, [267](#)
- mld-snooping host-tracking, [268](#)
- mld-snooping last-listener-query-interval, [268](#)
- mld-snooping max-response-time, [269](#)
- mld-snooping overflow-replace, [270](#)
- mld-snooping proxying enable, [271](#)
- mld-snooping querier, [271](#)

- mld-snooping query-interval, [272](#)
- mld-snooping report source-ip, [273](#)
- mld-snooping router-aging-time, [274](#)
- mld-snooping router-port-deny, [274](#)
- mld-snooping source-deny, [275](#)
- mld-snooping special-query source-ip, [276](#)
- mld-snooping static-group, [277](#)
- mld-snooping static-router-port, [278](#)
- mld-snooping version, [278](#)
- msdp, [182](#)
- mtracert, [59](#)
- multicast boundary, [60](#)
- multicast forwarding-table downstream-limit, [61](#)
- multicast forwarding-table route-limit, [62](#)
- multicast ipv6 boundary, [301](#)
- multicast ipv6 forwarding-table downstream-limit, [302](#)
- multicast ipv6 forwarding-table route-limit, [302](#)
- multicast ipv6 load-splitting, [303](#)
- multicast ipv6 longest-match, [304](#)
- multicast ipv6 routing-enable, [304](#)
- multicast load-splitting, [62](#)
- multicast longest-match, [63](#)
- multicast routing-enable, [64](#)
- multicast-vlan, [44](#)
- multicast-vlan ipv6, [290](#)

N

- network (IPv6 MBGP address family view), [431](#)
- network (MBGP address family view), [229](#)

O

- originating-rp, [182](#)
- overflow-replace (IGMP-snooping view), [33](#)
- overflow-replace (MLD-snooping view), [279](#)

P

- peer advertise-community (IPv6 MBGP address family view), [432](#)
- peer advertise-community (MBGP address family view), [230](#)
- peer advertise-ext-community (IPv6 MBGP address family view), [433](#)
- peer advertise-ext-community (MBGP address family view), [231](#)
- peer allow-as-loop (IPv6 MBGP address family view), [433](#)
- peer allow-as-loop (MBGP address family view), [232](#)

- peer as-path-acl (IPv6 MBGP address family view), [434](#)
- peer as-path-acl (MBGP address family view), [232](#)
- peer capability-advertise orf (IPv6 MBGP address family view), [435](#)
- peer capability-advertise orf (MBGP address family view), [233](#)
- peer connect-interface, [183](#)
- peer default-route-advertise (IPv6 MBGP address family view), [436](#)
- peer default-route-advertise (MBGP address family view), [234](#)
- peer description, [184](#)
- peer enable (IPv6 MBGP address family view), [437](#)
- peer enable (MBGP address family view), [235](#)
- peer filter-policy (IPv6 MBGP address family view), [438](#)
- peer filter-policy (MBGP address family view), [236](#)
- peer group (IPv6 MBGP address family view), [438](#)
- peer group (MBGP address family view), [236](#)
- peer ip-prefix (MBGP address family view), [237](#)
- peer ipv6-prefix (IPv6 MBGP address family view), [439](#)
- peer keep-all-routes (IPv6 MBGP address family view), [440](#)
- peer keep-all-routes (MBGP address family view), [238](#)
- peer mesh-group, [185](#)
- peer minimum-ttl, [185](#)
- peer next-hop-local (IPv6 MBGP address family view), [441](#)
- peer next-hop-local (MBGP address family view), [238](#)
- peer password, [186](#)
- peer preferred-value (IPv6 MBGP address family view), [441](#)
- peer preferred-value (MBGP address family view), [239](#)
- peer public-as-only (IPv6 MBGP address family view), [442](#)
- peer public-as-only (MBGP address family view), [240](#)
- peer reflect-client (IPv6 MBGP address family view), [443](#)
- peer reflect-client (MBGP address family view), [241](#)
- peer request-sa-enable, [187](#)
- peer route-limit (IPv6 MBGP address family view), [444](#)
- peer route-limit (MBGP address family view), [241](#)
- peer route-policy (IPv6 MBGP address family view), [445](#)
- peer route-policy (MBGP address family view), [242](#)
- peer sa-cache-maximum, [188](#)
- peer sa-policy, [189](#)

- peer sa-request-policy, [190](#)
- pim, [147](#)
- pim bfd enable, [148](#)
- pim bsr-boundary, [149](#)
- pim dm, [149](#)
- pim hello-option dr-priority, [150](#)
- pim hello-option holdtime, [150](#)
- pim hello-option lan-delay, [151](#)
- pim hello-option neighbor-tracking, [152](#)
- pim hello-option override-interval, [152](#)
- pim holdtime assert, [153](#)
- pim holdtime join-prune, [153](#)
- pim ipv6, [378](#)
- pim ipv6 bfd enable, [379](#)
- pim ipv6 bsr-boundary, [380](#)
- pim ipv6 dm, [380](#)
- pim ipv6 hello-option dr-priority, [381](#)
- pim ipv6 hello-option holdtime, [381](#)
- pim ipv6 hello-option lan-delay, [382](#)
- pim ipv6 hello-option neighbor-tracking, [383](#)
- pim ipv6 hello-option override-interval, [383](#)
- pim ipv6 holdtime assert, [384](#)
- pim ipv6 holdtime join-prune, [384](#)
- pim ipv6 neighbor-policy, [385](#)
- pim ipv6 require-genid, [386](#)
- pim ipv6 sm, [386](#)
- pim ipv6 state-refresh-capable, [387](#)
- pim ipv6 timer graft-retry, [387](#)
- pim ipv6 timer hello, [388](#)
- pim ipv6 timer join-prune, [388](#)
- pim ipv6 triggered-hello-delay, [389](#)
- pim neighbor-policy, [154](#)
- pim require-genid, [155](#)
- pim sm, [155](#)
- pim state-refresh-capable, [156](#)
- pim timer graft-retry, [156](#)
- pim timer hello, [157](#)
- pim timer join-prune, [157](#)
- pim triggered-hello-delay, [158](#)
- pim-snooping enable, [41](#)
- pim-snooping ipv6 enable, [287](#)
- port (IPv6 multicast VLAN view), [291](#)
- port (multicast VLAN view), [45](#)
- port multicast-vlan, [45](#)
- port multicast-vlan ipv6, [291](#)

- preference (IPv6 MBGP address family view), [446](#)
- preference (MBGP address family view), [243](#)
- probe-interval (IPv6 PIM view), [390](#)
- probe-interval (PIM view), [159](#)
- prune delay (IPv6 PIM view), [390](#)
- prune delay (PIM view), [159](#)

R

- reflect between-clients (IPv6 MBGP address family view), [446](#)
- reflect between-clients (MBGP address family view), [244](#)
- reflector cluster-id (IPv6 MBGP address family view), [447](#)
- reflector cluster-id (MBGP address family view), [244](#)
- refresh bgp ipv4 multicast, [245](#)
- refresh bgp ipv6 multicast, [448](#)
- register-policy (IPv6 PIM view), [391](#)
- register-policy (PIM view), [160](#)
- register-suppression-timeout (IPv6 PIM view), [391](#)
- register-suppression-timeout (PIM view), [161](#)
- register-whole-checksum (IPv6 PIM view), [392](#)
- register-whole-checksum (PIM view), [161](#)
- report-aggregation (IGMP-snooping view), [34](#)
- report-aggregation (MLD-snooping view), [280](#)
- require-router-alert (IGMP view), [99](#)
- require-router-alert (MLD view), [337](#)
- reset bgp ipv4 multicast, [246](#)
- reset bgp ipv4 multicast dampening, [246](#)
- reset bgp ipv4 multicast flap-info, [247](#)
- reset bgp ipv6 multicast, [448](#)
- reset bgp ipv6 multicast dampening, [449](#)
- reset bgp ipv6 multicast flap-info, [449](#)
- reset igmp group, [100](#)
- reset igmp group port-info, [101](#)
- reset igmp ssm-mapping group, [102](#)
- reset igmp-snooping group, [35](#)
- reset igmp-snooping statistics, [35](#)
- reset mld group, [338](#)
- reset mld group port-info, [339](#)
- reset mld ssm-mapping group, [340](#)
- reset mld-snooping group, [280](#)
- reset mld-snooping statistics, [281](#)
- reset msdp peer, [191](#)
- reset msdp sa-cache, [191](#)
- reset msdp statistics, [192](#)

reset multicast forwarding-table, [64](#)
reset multicast ipv6 forwarding-table, [305](#)
reset multicast ipv6 routing-table, [305](#)
reset multicast routing-table, [65](#)
reset pim control-message counters, [162](#)
reset pim ipv6 control-message counters, [393](#)
reset pim-snooping ipv6 statistics, [288](#)
reset pim-snooping statistics, [42](#)
robust-count (IGMP view), [103](#)
robust-count (MLD view), [340](#)
router-aging-time (IGMP-snooping view), [36](#)
router-aging-time (MLD-snooping view), [281](#)

S

send-router-alert (IGMP view), [104](#)
send-router-alert (MLD view), [341](#)
shutdown (MSDP view), [192](#)
source-deny (IGMP-snooping view), [36](#)
source-deny (MLD-snooping view), [282](#)
source-lifetime (IPv6 PIM view), [393](#)
source-lifetime (PIM view), [163](#)
source-policy (IPv6 PIM view), [394](#)
source-policy (PIM view), [163](#)
spt-switch-threshold infinity (IPv6 PIM view), [394](#)
spt-switch-threshold infinity (PIM view), [164](#)
ssm-mapping (IGMP view), [104](#)
ssm-mapping (MLD view), [342](#)
ssm-policy (IPv6 PIM view), [395](#)
ssm-policy (PIM view), [165](#)
startup-query-count (IGMP view), [105](#)

startup-query-count (MLD view), [342](#)
startup-query-interval (IGMP view), [106](#)
startup-query-interval (MLD view), [343](#)
state-refresh-hoplimit, [396](#)
state-refresh-interval (IPv6 PIM view), [397](#)
state-refresh-interval (PIM view), [166](#)
state-refresh-rate-limit (IPv6 PIM view), [397](#)
state-refresh-rate-limit (PIM view), [167](#)
state-refresh-ttl, [167](#)
static-rp (IPv6 PIM view), [398](#)
static-rp (PIM view), [168](#)
static-rpf-peer, [193](#)
subvlan (IPv6 multicast VLAN view), [292](#)
subvlan (multicast VLAN view), [46](#)
summary automatic (MBGP address family view), [247](#)

T

timer hello (IPv6 PIM view), [399](#)
timer hello (PIM view), [169](#)
timer join-prune (IPv6 PIM view), [399](#)
timer join-prune (PIM view), [170](#)
timer other-querier-present (IGMP view), [106](#)
timer other-querier-present (MLD view), [344](#)
timer query (IGMP view), [107](#)
timer query (MLD view), [344](#)
timer retry, [194](#)

V

version (IGMP view), [108](#)
version (MLD view), [345](#)