

# HP 5920 & 5900 Switch Series

IP Multicast

Command Reference

Part number: 5998-6635

Software version: Release 2416

Document version: 6W100-20150130



**Legal and notice information**

© Copyright 2015 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 commands	1
display igmp-snooping	1
display igmp-snooping group	3
display igmp-snooping router-port	4
display igmp-snooping static-group	5
display igmp-snooping static-router-port	6
display igmp-snooping statistics	7
display l2-multicast ip	8
display l2-multicast ip forwarding	10
display l2-multicast mac	11
display l2-multicast mac forwarding	12
dot1p-priority (IGMP-snooping view)	13
enable (IGMP-snooping view)	14
entry-limit (IGMP-snooping view)	14
fast-leave (IGMP-snooping view)	15
group-policy (IGMP-snooping view)	16
host-aging-time (IGMP-snooping view)	17
igmp-snooping	18
igmp-snooping dot1p-priority	19
igmp-snooping drop-unknown	20
igmp-snooping enable	20
igmp-snooping fast-leave	21
igmp-snooping general-query source-ip	22
igmp-snooping group-limit	23
igmp-snooping group-policy	23
igmp-snooping host-aging-time	25
igmp-snooping host-join	26
igmp-snooping last-member-query-interval	27
igmp-snooping leave source-ip	28
igmp-snooping max-response-time	28
igmp-snooping overflow-replace	29
igmp-snooping querier	30
igmp-snooping query-interval	31
igmp-snooping report source-ip	32
igmp-snooping router-aging-time	33
igmp-snooping router-port-deny	34
igmp-snooping source-deny	34
igmp-snooping special-query source-ip	35
igmp-snooping static-group	36
igmp-snooping static-router-port	37
igmp-snooping version	37
last-member-query-interval (IGMP-snooping view)	38
max-response-time (IGMP-snooping view)	39
overflow-replace (IGMP-snooping view)	40
report-aggregation (IGMP-snooping view)	41
reset igmp-snooping group	41
reset igmp-snooping router-port	42
reset igmp-snooping statistics	42
router-aging-time (IGMP-snooping view)	43

source-deny (IGMP-snooping view) .....	43
version (IGMP-snooping view) .....	44
<b>PIM snooping commands .....</b>	<b>46</b>
display pim-snooping neighbor .....	46
display pim-snooping router-port .....	47
display pim-snooping routing-table .....	48
display pim-snooping statistics .....	49
pim-snooping enable .....	50
pim-snooping graceful-restart join-aging-time .....	51
pim-snooping graceful-restart neighbor-aging-time .....	52
reset pim-snooping statistics .....	52
<b>Multicast VLAN commands .....</b>	<b>54</b>
display multicast-vlan .....	54
display multicast-vlan group .....	55
display multicast-vlan forwarding-table .....	56
multicast-vlan .....	58
multicast-vlan entry-limit .....	59
port (multicast-VLAN view) .....	60
port multicast-vlan .....	60
reset multicast-vlan group .....	61
subvlan (multicast-VLAN view) .....	62
<b>Multicast routing and forwarding commands .....</b>	<b>63</b>
delete ip rpf-route-static .....	63
display mac-address multicast .....	63
display mrib interface .....	65
display multicast boundary .....	66
display multicast forwarding df-info .....	67
display multicast forwarding event .....	69
display multicast forwarding-table .....	70
display multicast forwarding-table df-list .....	72
display multicast routing-table .....	73
display multicast routing-table static .....	75
display multicast rpf-info .....	76
ip rpf-route-static .....	77
load-splitting (MRIB view) .....	78
longest-match (MRIB view) .....	79
mac-address multicast .....	79
multicast boundary .....	81
multicast forwarding supervlan community .....	81
multicast routing .....	82
reset multicast forwarding event .....	83
reset multicast forwarding-table .....	83
reset multicast routing-table .....	84
<b>IGMP commands .....</b>	<b>86</b>
display igmp group .....	86
display igmp interface .....	89
display igmp ssm-mapping .....	91
igmp .....	92
igmp enable .....	92
igmp fast-leave .....	93
igmp group-policy .....	94
igmp last-member-query-count .....	95

igmp last-member-query-interval	96
igmp max-response-time	96
igmp non-stop-routing	97
igmp other-querier-present-interval	98
igmp query-interval	98
igmp robust-count	99
igmp startup-query-count	100
igmp startup-query-interval	101
igmp static-group	102
igmp version	102
last-member-query-count (IGMP view)	103
last-member-query-interval (IGMP view)	104
max-response-time (IGMP view)	105
other-querier-present-interval (IGMP view)	105
query-interval (IGMP view)	106
reset igmp group	107
robust-count (IGMP view)	108
ssm-mapping (IGMP view)	109
startup-query-count (IGMP view)	110
startup-query-interval (IGMP view)	110

**PIM commands** ..... 112

auto-rp enable	112
bidir-pim enable (PIM view)	112
bidir-rp-limit (PIM view)	113
bsm-fragment enable (PIM view)	114
bsr-policy (PIM view)	114
c-bsr (PIM view)	115
c-rp (PIM view)	116
crp-policy (PIM view)	117
display interface register-tunnel	118
display pim bsr-info	121
display pim claimed-route	122
display pim c-rp	123
display pim df-info	125
display pim interface	126
display pim neighbor	128
display pim routing-table	130
display pim rp-info	132
display pim statistics	134
hello-option dr-priority (PIM view)	135
hello-option holdtime (PIM view)	136
hello-option lan-delay (PIM view)	137
hello-option neighbor-tracking (PIM view)	138
hello-option override-interval (PIM view)	138
holdtime join-prune (PIM view)	139
jp-pkt-size (PIM view)	140
pim	140
pim bfd enable	141
pim bsr-boundary	142
pim dm	142
pim hello-option dr-priority	143
pim hello-option holdtime	144
pim hello-option lan-delay	144
pim hello-option neighbor-tracking	145

pim hello-option override-interval	146
pim holdtime join-prune	147
pim neighbor-policy	147
pim passive	148
pim require-genid	149
pim sm	149
pim state-refresh-capable	150
pim timer graft-retry	151
pim timer hello	151
pim timer join-prune	152
pim triggered-hello-delay	153
register-policy (PIM view)	153
register-whole-checksum (PIM view)	154
source-lifetime (PIM view)	154
source-policy (PIM view)	155
spt-switch-threshold (PIM view)	156
ssm-policy (PIM view)	157
state-refresh-interval (PIM view)	158
state-refresh-rate-limit (PIM view)	158
state-refresh-ttl (PIM view)	159
static-rp (PIM view)	160
timer hello (PIM view)	161
timer join-prune (PIM view)	162
<b>MSDP commands</b>	<b>163</b>
cache-sa-enable	163
display msdp brief	163
display msdp peer-status	165
display msdp sa-cache	168
display msdp sa-count	169
encap-data-enable	170
import-source	171
msdp	172
originating-rp	173
peer connect-interface	173
peer description	174
peer mesh-group	175
peer minimum-ttl	175
peer password	176
peer request-sa-enable	177
peer sa-cache-maximum	178
peer sa-policy	178
peer sa-request-policy	179
reset msdp peer	180
reset msdp sa-cache	181
reset msdp statistics	181
shutdown (MSDP view)	182
static-rpf-peer	183
timer retry	183
<b>Multicast VPN commands</b>	<b>185</b>
data-delay	185
data-group	185
default-group	186
display multicast-domain data-group receive	187

display multicast-domain data-group send	189
display multicast-domain default-group	190
log data-group-reuse	191
multicast-domain	191
source	192

## MLD snooping commands 193

display ipv6 l2-multicast ip	193
display ipv6 l2-multicast ip forwarding	194
display ipv6 l2-multicast mac	195
display ipv6 l2-multicast mac forwarding	196
display mld-snooping	197
display mld-snooping group	199
display mld-snooping router-port	201
display mld-snooping static-group	202
display mld-snooping static-router-port	203
display mld-snooping statistics	204
dot1 p-priority (MLD-snooping view)	205
enable (MLD-snooping view)	206
entry-limit (MLD-snooping view)	207
fast-leave (MLD-snooping view)	207
group-policy (MLD-snooping view)	208
host-aging-time (MLD-snooping view)	209
last-listener-query-interval (MLD-snooping view)	210
max-response-time (MLD-snooping view)	211
mld-snooping	212
mld-snooping done source-ip	212
mld-snooping dot1 p-priority	213
mld-snooping drop-unknown	214
mld-snooping enable	215
mld-snooping fast-leave	216
mld-snooping general-query source-ip	217
mld-snooping group-limit	217
mld-snooping group-policy	218
mld-snooping host-aging-time	219
mld-snooping host-join	220
mld-snooping last-listener-query-interval	221
mld-snooping max-response-time	222
mld-snooping overflow-replace	223
mld-snooping querier	224
mld-snooping report source-ip	225
mld-snooping query-interval	226
mld-snooping router-aging-time	227
mld-snooping router-port-deny	228
mld-snooping source-deny	228
mld-snooping special-query source-ip	229
mld-snooping static-group	230
mld-snooping static-router-port	231
mld-snooping version	231
overflow-replace (MLD-snooping view)	232
report-aggregation (MLD-snooping view)	233
reset mld-snooping group	233
reset mld-snooping router-port	234
reset mld-snooping statistics	235
router-aging-time (MLD-snooping view)	235

source-deny (MLD-snooping view) .....	236
version (MLD-snooping view) .....	237
<b>IPv6 PIM snooping commands .....</b>	<b>238</b>
display ipv6 pim-snooping neighbor .....	238
display ipv6 pim-snooping router-port .....	239
display ipv6 pim-snooping routing-table .....	240
display ipv6 pim-snooping statistics .....	241
ipv6 pim-snooping enable .....	242
ipv6 pim-snooping graceful-restart join-aging-time .....	243
ipv6 pim-snooping graceful-restart neighbor-aging-time .....	244
reset ipv6 pim-snooping statistics .....	244
<b>IPv6 multicast VLAN commands .....</b>	<b>246</b>
display ipv6 multicast-vlan .....	246
display ipv6 multicast-vlan group .....	247
display ipv6 multicast-vlan forwarding-table .....	248
ipv6 multicast-vlan .....	250
ipv6 multicast-vlan entry-limit .....	251
ipv6 port multicast-vlan .....	252
port (IPv6 multicast VLAN view) .....	252
reset ipv6 multicast-vlan group .....	253
subvlan (IPv6 multicast VLAN view) .....	254
<b>IPv6 multicast routing and forwarding commands .....</b>	<b>255</b>
display ipv6 mrib interface .....	255
display ipv6 multicast boundary .....	256
display ipv6 multicast forwarding df-info .....	257
display ipv6 multicast forwarding event .....	259
display ipv6 multicast forwarding-table .....	260
display ipv6 multicast forwarding-table df-list .....	263
display ipv6 multicast routing-table .....	264
display ipv6 multicast rpf-info .....	265
ipv6 multicast boundary .....	266
ipv6 multicast forwarding supervlan community .....	268
ipv6 multicast routing .....	268
load-splitting (IPv6 MRIB view) .....	269
longest-match (IPv6 MRIB view) .....	270
reset ipv6 multicast forwarding event .....	270
reset ipv6 multicast forwarding-table .....	271
reset ipv6 multicast routing-table .....	272
<b>MLD commands .....</b>	<b>273</b>
display mld group .....	273
display mld interface .....	276
display mld ssm-mapping .....	278
last-listener-query-count (MLD view) .....	279
last-listener-query-interval (MLD view) .....	279
max-response-time (MLD view) .....	280
mld .....	281
mld enable .....	282
mld fast-leave .....	282
mld group-policy .....	283
mld last-listener-query-count .....	284
mld last-listener-query-interval .....	285
mld max-response-time .....	286



mld non-stop-routing	287
mld other-querier-present-timeout	287
mld query-interval	288
mld robust-count	289
mld startup-query-count	289
mld startup-query-interval	290
mld static-group	291
mld version	292
other-querier-present-timeout (MLD view)	292
query-interval (MLD view)	293
reset mld group	294
robust-count (MLD view)	295
ssm-mapping (MLD view)	296
startup-query-count (MLD view)	297
startup-query-interval (MLD view)	297

**IPv6 PIM commands** ..... 299

bidir-pim enable (IPv6 PIM view)	299
bidir-rp-limit (IPv6 PIM view)	299
bsm-fragment enable (IPv6 PIM view)	300
bsr-policy (IPv6 PIM view)	301
c-bsr (IPv6 PIM view)	301
c-rp (IPv6 PIM view)	302
crp-policy (IPv6 PIM view)	304
display ipv6 pim bsr-info	305
display ipv6 pim claimed-route	306
display ipv6 pim c-rp	307
display ipv6 pim df-info	308
display ipv6 pim interface	309
display ipv6 pim neighbor	312
display ipv6 pim routing-table	313
display ipv6 pim rp-info	316
display ipv6 pim statistics	318
hello-option dr-priority (IPv6 PIM view)	319
hello-option holdtime (IPv6 PIM view)	320
hello-option lan-delay (IPv6 PIM view)	321
hello-option neighbor-tracking (IPv6 PIM view)	321
ipv6 pim passive	322
hello-option override-interval (IPv6 PIM view)	323
holdtime join-prune (IPv6 PIM view)	323
ipv6 pim	324
ipv6 pim bfd enable	325
ipv6 pim bsr-boundary	326
ipv6 pim dm	326
ipv6 pim hello-option dr-priority	327
ipv6 pim hello-option holdtime	328
ipv6 pim hello-option lan-delay	328
ipv6 pim hello-option neighbor-tracking	329
ipv6 pim hello-option override-interval	330
ipv6 pim holdtime join-prune	331
ipv6 pim neighbor-policy	332
ipv6 pim require-genid	332
ipv6 pim sm	333
ipv6 pim state-refresh-capable	333
ipv6 pim timer graft-retry	334

ipv6 pim timer hello .....	335
ipv6 pim timer join-prune .....	335
ipv6 pim triggered-hello-delay .....	336
jp-pkt-size (IPv6 PIM view) .....	337
register-policy (IPv6 PIM view) .....	337
register-whole-checksum (IPv6 PIM view) .....	338
source-lifetime (IPv6 PIM view) .....	339
source-policy (IPv6 PIM view) .....	339
spt-switch-threshold (IPv6 PIM view) .....	340
ssm-policy (IPv6 PIM view) .....	341
state-refresh-hoplimit (IPv6 PIM view) .....	342
state-refresh-interval (IPv6 PIM view) .....	342
state-refresh-rate-limit (IPv6 PIM view) .....	343
static-rp (IPv6 PIM view) .....	344
timer hello (IPv6 PIM view) .....	345
timer join-prune (IPv6 PIM view) .....	346
<b>Support and other resources .....</b>	<b>347</b>
Contacting HP .....	347
Subscription service .....	347
Related information .....	347
Documents .....	347
Websites .....	347
Conventions .....	348
<b>Index .....</b>	<b>350</b>

---

# IGMP snooping commands

## display igmp-snooping

Use **display igmp-snooping** to display IGMP snooping status.

### Syntax

```
display igmp-snooping [ global | vlan vlan-id ]
```

### Views

Any view

### Predefined user roles

network-admin  
network-operator

### Parameters

**global**: Displays the global IGMP snooping status.

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

### Usage guidelines

If you do not specify any parameters, this command displays the global IGMP snooping status and the IGMP snooping status in all VLANs.

### Examples

```
# Display the global IGMP snooping status and the IGMP snooping status for all VLANs.
```

```
<Sysname> display igmp-snooping
IGMP snooping information: Global
  IGMP snooping: Enabled
  Drop-unknown: Disabled
  Host-aging-time: 260s
  Router-aging-time: 260s
  Max-response-time: 10s
  Last-member-query-interval: 1s
  Report-aggregation: Enabled
  Dot1p-priority: --

IGMP snooping information: VLAN 1
  IGMP snooping: Enabled
  Drop-unknown: Disabled
  Version: 2
  Host-aging-time: 260s
  Router-aging-time: 260s
  Max-response-time: 10s
  Last-member-query-interval: 1s
  Querier: Disabled
```

```

Query-interval: 125s
General-query source IP: 1.1.1.1
Special-query source IP: 2.2.2.2
Report source IP: 3.0.0.3
Leave source IP: 1.0.0.1
Dot1p-priority: 2

IGMP snooping information: VLAN 10
IGMP snooping: Enabled
Drop-unknown: Enabled
Version: 3
Host-aging-time: 260s
Router-aging-time: 260s
Max-response-time: 10s
Last-member-query-interval: 1s
Querier: Disabled
Query-interval: 125s
General-query source IP: 1.1.1.1
Special-query source IP: 2.2.2.2
Report source IP: 3.0.0.3
Leave source IP: 1.0.0.1
Dot1p-priority: --

```

**Table 1 Command output**

Field	Description
IGMP snooping	IGMP snooping status: <ul style="list-style-type: none"> <li>• Enabled.</li> <li>• Disabled.</li> </ul>
Drop-unknown	Status of dropping unknown multicast data: <ul style="list-style-type: none"> <li>• Enabled.</li> <li>• Disabled.</li> </ul>
Version	IGMP snooping version.
Host-aging-time	Aging timer for the dynamic member port.
Router-aging-time	Aging timer for the dynamic router port.
Max-response-time	Maximum response time for IGMP general queries.
Last-member-query-interval	Interval for sending IGMP group-specific queries.
Report-aggregation	Status of IGMP report suppression: <ul style="list-style-type: none"> <li>• Enabled.</li> <li>• Disabled.</li> </ul>
Dot1p-priority	802.1p priority for IGMP messages. If the priority is not configured, this field displays two hyphens (-).
Querier	Whether the IGMP snooping querier is enabled.
Query-interval	Interval for sending IGMP general queries.
General-query source IP	Source IP address of IGMP general queries.

Field	Description
Special-query source IP	Source IP address of IGMP group-specific queries.
Report source IP	Source IP address of IGMP reports.
Leave source IP	Source IP address of IGMP leave messages.

## display igmp-snooping group

Use **display igmp-snooping group** to display dynamic IGMP snooping forwarding entries.

### Syntax

```
display igmp-snooping group [ group-address | source-address ] * [ vlan vlan-id ] [ verbose ] [ slot slot-number ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**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 a multicast group, the command displays dynamic IGMP snooping forwarding entries for all multicast groups.

**source-address**: Specifies a multicast source by its IP address. If you do not specify a multicast source, the command displays dynamic IGMP snooping forwarding entries for all multicast sources.

**vlan** *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command displays dynamic IGMP snooping forwarding entries for all VLANs.

**verbose**: Displays detailed information. If you do not specify this keyword, the command displays brief information.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays dynamic IGMP snooping forwarding entries on the master device.

### Examples

# Display detailed information about the dynamic IGMP snooping forwarding entries for VLAN 2.

```
<Sysname> display igmp-snooping group vlan 2 verbose
Total 1 entries.
```

```
VLAN 2: Total 1 entries.
(0.0.0.0, 224.1.1.1)
Attribute: local port
FSM information: normal
Host slots (0 in total):
Host ports (1 in total):
XGE1/0/2          (00:03:23)
```

**Table 2 Command output**

Field	Description
Total 1 entries	Total number of dynamic IGMP snooping forwarding entries.
VLAN 2: Total 1 entries (0.0.0.0, 224.1.1.1)	Total number of dynamic IGMP snooping forwarding entries in VLAN 2. (S, G) entry, where <b>0.0.0.0</b> in the S position means any multicast sources.
Attribute	Entry attribute: <ul style="list-style-type: none"> <li>• <b>global port</b>—The entry has a global port.</li> <li>• <b>local port</b>—The entry has a port that resides on the specified device.</li> <li>• <b>slot</b>—The entry has a port that resides on a device other than the specified device.</li> </ul>
FSM information	Finite state machine information of the entry: <ul style="list-style-type: none"> <li>• <b>delete</b>—The entry attributes have been deleted.</li> <li>• <b>dummy</b>—The entry is a new and temporary entry.</li> <li>• <b>no info</b>—No entry exists.</li> <li>• <b>normal</b>—The entry is a correct entry.</li> </ul>
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (1 in total)	Member ports, and the total number of the member ports.
(00:03:23)	Remaining aging time for the dynamic member port. <ul style="list-style-type: none"> <li>• For a global port, this field is always displayed.</li> <li>• For a non-global port, this field is displayed if the port is on the master device. Otherwise, you must specify the <b>slot slot-number</b> option to display this field.</li> </ul>

## Related commands

**reset igmp-snooping group**

## display igmp-snooping router-port

Use **display igmp-snooping router-port** to display dynamic router port information.

### Syntax

**display igmp-snooping router-port** [ **vlan** *vlan-id* ] [ **slot** *slot-number* ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

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

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays dynamic router port information on the master device.

## Examples

```
# Display dynamic router port information for VLAN 2.
<Sysname> display igmp-snooping router-port vlan 2
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    XGE1/0/1                (00:01:30)
    XGE1/0/2                (00:00:23)
```

**Table 3 Command output**

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs of the member devices that have router ports and the total number of the member devices (excluding the specified member device).
Router ports (2 in total)	Dynamic router ports, and the total number of the dynamic router ports.
(00:01:30)	Remaining aging time for the dynamic router port. <ul style="list-style-type: none"><li>• For a global port, this field is always displayed.</li><li>• For a non-global port, this field is displayed if the port is on the master device. Otherwise, you must specify the <b>slot slot-number</b> option to display this field.</li></ul>

## Related commands

**reset igmp-snooping router-port**

## display igmp-snooping static-group

Use **display igmp-snooping static-group** to display static IGMP snooping forwarding entries.

### Syntax

```
display igmp-snooping static-group [ group-address | source-address ] * [ vlan vlan-id ] [ verbose ] [ slot slot-number ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**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 a multicast group, the command displays static IGMP snooping forwarding entries for all multicast groups.

**source-address**: Specifies a multicast source by its IP address. If you do not specify a multicast source, the command displays static IGMP snooping forwarding entries for all multicast sources.

**vlan vlan-id**: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command displays static IGMP snooping forwarding entries for all VLANs.

**verbose:** Displays detailed information. If you do not specify this keyword, the command displays brief information.

**slot slot-number:** Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays static IGMP snooping forwarding entries on the master device.

## Examples

# Display detailed information about the static IGMP snooping forwarding entries for VLAN 2.

```
<Sysname> display igmp-snooping static-group vlan 2 verbose
Total 1 entries.
```

```
VLAN 2: Total 1 entries.
(0.0.0.0, 224.1.1.1)
Attribute: local port
FSM information: normal
Host slots (0 in total):
Host ports (1 in total):
XGE1/0/2
```

**Table 4 Command output**

Field	Description
Total 1 entries	Total number of static IGMP snooping forwarding entries.
VLAN 2: Total 1 entries	Total number of static IGMP snooping forwarding entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where <b>0.0.0.0</b> in the S position means any multicast sources.
Attribute	Entry attribute: <ul style="list-style-type: none"> <li>• <b>global port</b>—The entry has a global port.</li> <li>• <b>local port</b>—The entry has a port that resides on the specified device.</li> <li>• <b>slot</b>—The entry has a port that resides on a device other than the specified device.</li> </ul>
FSM information	Finite state machine information of the entry: <ul style="list-style-type: none"> <li>• <b>delete</b>—The entry attributes have been deleted.</li> <li>• <b>dummy</b>—The entry is a new temporary entry.</li> <li>• <b>no info</b>—No entry exists.</li> <li>• <b>normal</b>—The entry is a correct entry.</li> </ul>
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (1 in total)	Member ports, and the total number of the member ports.

## display igmp-snooping static-router-port

Use **display igmp-snooping static-router-port** to display static router port information.

### Syntax

```
display igmp-snooping static-router-port [ vlan vlan-id ] [ slot slot-number ]
```



## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

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

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays static router port information on the master device.

## Examples

```
# Display static router port information for VLAN 2.
```

```
<Sysname> display igmp-snooping static-router-port vlan 2
```

```
VLAN 2:
```

```
Router slots (0 in total):
```

```
Router ports (2 in total):
```

```
  XGE1/0/1
```

```
  XGE1/0/2
```

**Table 5 Command output**

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs of the member devices that have router ports and the total number of the member devices (excluding the specified member device).
Router ports (2 in total)	Static router ports, and the total number of the static router ports.

# display igmp-snooping statistics

Use **display igmp-snooping statistics** to display statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping.

## Syntax

```
display igmp-snooping statistics
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Examples

```
# Display statistics for the IGMP messages and PIMv2 hello 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 PIMv2 hello: 0
Received error IGMP messages: 19

```

**Table 6 Command output**

Field	Description
general queries	Number of IGMP general queries.
specific queries	Number of IGMP group-specific queries.
reports	Number of IGMP reports.
leaves	Number of IGMP leave messages.
reports with right and wrong records	Number of IGMP reports with correct and incorrect records.
specific sg queries	Number of IGMP group-and-source-specific queries.
PIMv2 hello	Number of PIMv2 hello messages.
error IGMP messages	Number of IGMP messages with errors.

## Related commands

**reset igmp-snooping statistics**

## display l2-multicast ip

Use **display l2-multicast ip** to display information about Layer 2 IP multicast groups.

### Syntax

```
display l2-multicast ip [ group group-address | source source-address ] * [ vlan vlan-id ] [ slot slot-number ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**group** *group-address*: Specifies a multicast group by its IP address. If you do not specify a multicast group, the command displays information about all Layer 2 IP multicast groups.

**source** *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, the command displays information about Layer 2 IP multicast groups for all multicast sources.

**vlan** *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command displays information about Layer 2 IP multicast groups for all VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays information about the Layer 2 IP multicast groups on the master device.

## Examples

# Display information about the Layer 2 IP multicast groups for VLAN 2.

```
<Sysname> display l2-multicast ip vlan 2
```

```
Total 1 entries.
```

```
VLAN 2: Total 1 IP entries.
```

```
(0.0.0.0, 224.1.1.1)
```

```
Attribute: static, success
```

```
Host slots (0 in total):
```

```
Host ports (1 in total):
```

```
    XGE1/0/1                (S, SUC)
```

**Table 7 Command output**

Field	Description
Total 1 entries	Total number of Layer 2 IP multicast groups.
VLAN 2: Total 1 IP entries	Total number of Layer 2 IP multicast groups in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where <b>0.0.0.0</b> in the S position means any multicast sources.
Attribute	Entry attribute: <ul style="list-style-type: none"> <li>• <b>dynamic</b>—The entry is created by a dynamic protocol.</li> <li>• <b>static</b>—The entry is created by a static protocol.</li> <li>• <b>pim</b>—The entry is created by PIM.</li> <li>• <b>kernel</b>—The entry is obtained from the kernel.</li> <li>• <b>success</b>—Processing succeeds.</li> <li>• <b>fail</b>—Processing fails.</li> </ul>
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (1 in total)	Member ports, and the total number of the member ports.
(S, SUC)	Port attribute: <ul style="list-style-type: none"> <li>• <b>D</b>—Dynamic port.</li> <li>• <b>S</b>—Static port.</li> <li>• <b>P</b>—PIM port.</li> <li>• <b>K</b>—Port obtained from the kernel.</li> <li>• <b>R</b>—Port learned from (*, *) entries.</li> <li>• <b>W</b>—Port learned from (*, G) entries.</li> <li>• <b>SUC</b>—Processing succeeds.</li> <li>• <b>F</b>—Processing fails.</li> <li>• <b>BC</b>—Broadcast port. The TRILL port floods the multicast traffic after the topology changes.</li> </ul>

# display l2-multicast ip forwarding

Use **display l2-multicast ip forwarding** to display Layer 2 IP multicast group entries.

## Syntax

```
display l2-multicast ip forwarding [ group group-address | source source-address ] * [ vlan vlan-id ]  
[ slot slot-number ]
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**group** *group-address*: Specifies a multicast group by its IP address. If you do not specify a multicast group, the command displays Layer 2 IP multicast group entries for all multicast groups.

**source** *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, the command displays Layer 2 IP multicast group entries for all multicast sources.

**vlan** *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command displays Layer 2 IP multicast group entries for all VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays Layer 2 IP multicast group entries on the master device.

## Examples

```
# Display Layer 2 IP multicast group entries for VLAN 2.  
<Sysname> display l2-multicast ip forwarding vlan 2  
Total 1 entries.
```

```
VLAN 2: Total 1 IP entries.  
  (0.0.0.0, 224.1.1.1)  
  Host slots (0 in total):  
  Host ports (3 in total):  
    XGE1/0/1  
    XGE1/0/2  
    XGE1/0/3
```

**Table 8 Command output**

Field	Description
Total 1 entries	Total number of Layer 2 IP multicast group entries.
VLAN 2: Total 1 IP entries	Total number of Layer 2 IP multicast group entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where <b>0.0.0.0</b> in the S position means any multicast sources.
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).

Field	Description
Host ports (3 in total)	Member ports, and the total number of the member ports.

## display l2-multicast mac

Use **display l2-multicast mac** to display information about Layer 2 MAC multicast groups.

### Syntax

```
display l2-multicast mac [ mac-address ] [ vlan vlan-id ] [ slot slot-number ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**mac-address**: Specifies a MAC multicast group by its MAC address. If you do not specify a MAC multicast group, the command displays information about all Layer 2 MAC multicast groups.

**vlan** *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command displays information about Layer 2 MAC multicast groups for all VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays information about the Layer 2 MAC multicast groups on the master device.

### Examples

```
# Display information about the Layer 2 MAC multicast groups for VLAN 2.
```

```
<Sysname> display l2-multicast mac vlan 2
```

```
Total 1 MAC entries.
```

```
VLAN 2: Total 1 MAC entries.
```

```
MAC group address: 0100-5e01-0101
```

```
Attribute: success
```

```
Host slots (0 in total):
```

```
Host ports (1 in total):
```

```
XGE1/0/1
```

**Table 9 Command output**

Field	Description
Total 1 MAC entries	Total number of Layer 2 MAC multicast groups.
VLAN 2: Total 1 MAC entries	Total number of Layer 2 MAC multicast groups in VLAN 2.
Attribute	Entry attribute: <ul style="list-style-type: none"> <li><b>success</b>—Processing succeeds.</li> <li><b>fail</b>—Processing fails.</li> </ul>

Field	Description
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (1 in total)	Member ports, and the total number of the member ports.

## display l2-multicast mac forwarding

Use **display l2-multicast mac forwarding** to display Layer 2 MAC multicast group entries.

### Syntax

**display l2-multicast mac forwarding** [ *mac-address* ] [ **vlan** *vlan-id* ] [ **slot** *slot-number* ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**mac-address**: Specifies a MAC multicast group by its MAC address. If you do not specify a MAC multicast group, the command displays Layer 2 MAC multicast group entries for all MAC multicast groups.

**vlan** *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command displays Layer 2 MAC multicast group entries for all VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays Layer 2 MAC multicast group entries on the master device.

### Examples

```
# Display Layer 2 MAC multicast group entries for VLAN 2.
<Sysname> display l2-multicast mac forwarding vlan 2
Total 1 MAC entries.
```

```
VLAN 2: Total 1 MAC entries.
  MAC group address: 0100-5e01-0101
  Host slots (0 in total):
  Host ports (3 in total):
    XGE1/0/1
    XGE1/0/2
    XGE1/0/3
```

**Table 10 Command output**

Field	Description
Total 1 MAC entries	Total number of Layer 2 MAC multicast group entries.
VLAN 2: Total 1 MAC entries	Total number of Layer 2 MAC multicast group entries in VLAN 2.

Field	Description
MAC group address	Address of the MAC multicast group.
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (3 in total)	Member ports, and the total number of the member ports.

## dot1p-priority (IGMP-snooping view)

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

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

### Syntax

**dot1p-priority** *priority-number*

**undo dot1p-priority**

### Default

The 802.1p priority for IGMP messages is not configured.

### Views

IGMP-snooping view

### Predefined user roles

network-admin

### Parameters

*priority-number*: Sets an 802.1p priority for IGMP messages, in the range of 0 to 7. A higher value means a higher priority.

### Usage guidelines

This command and the **igmp-snooping dot1p-priority** command have the same function but different effective ranges:

- The **dot1p-priority** command in IGMP-snooping view takes effect on all VLANs.
- The **igmp-snooping dot1p-priority** command takes effect on the current VLAN.

For a VLAN, the **igmp-snooping dot1p-priority** command takes priority over the **dot1p-priority** command in IGMP-snooping view.

### Examples

# Set the 802.1p priority for IGMP messages to 3 globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dot1p-priority 3
```

### Related commands

**igmp-snooping dot1p-priority**

## enable (IGMP-snooping view)

Use **enable** to enable IGMP snooping for VLANs.

Use **undo enable** to disable IGMP snooping for VLANs.

### Syntax

**enable vlan** *vlan-list*

**undo enable vlan** *vlan-list*

### Default

IGMP snooping is disabled in a VLAN.

### Views

IGMP-snooping view

### Predefined user roles

network-admin

### Parameters

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The value range for the VLAN ID is 1 to 4094.

### Usage guidelines

You must enable IGMP snooping globally before you enable IGMP snooping for VLANs.

This command and the **igmp-snooping enable** command have the same function but different effective ranges:

- The **enable** command in IGMP-snooping view takes effect on the specified VLANs.
- The **igmp-snooping enable** command takes effect on the current VLAN.

For a VLAN, the **enable** command in IGMP-snooping view and the **igmp-snooping enable** command have the same priority, and the most recent configuration takes effect.

### Examples

```
# Enable IGMP snooping globally, and enable IGMP snooping for VLAN 2 through VLAN 10.
```

```
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] enable vlan 2 to 10
```

### Related commands

- **igmp-snooping**
- **igmp-snooping enable**

## entry-limit (IGMP-snooping view)

Use **entry-limit** to set the global maximum number of IGMP snooping forwarding entries, including dynamic entries and static entries.

Use **undo entry-limit** to restore the default.



## Syntax

**entry-limit** *limit*  
**undo entry-limit**

## Default

The setting is 4294967295.

## Views

IGMP-snooping view

## Predefined user roles

network-admin

## Parameters

*limit*: Sets the global maximum number of IGMP snooping forwarding entries, in the range of 0 to 4294967295.

## Examples

```
# Set the global maximum number of IGMP snooping forwarding entries to 512.  
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] entry-limit 512
```

# fast-leave (IGMP-snooping view)

Use **fast-leave** to enable fast-leave processing globally.

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

## Syntax

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

## Default

Fast-leave processing is disabled.

## Views

IGMP-snooping view

## Predefined user roles

network-admin

## Parameters

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command takes effect on all VLANs.

## Usage guidelines

This feature enables the switch to immediately remove a port from the forwarding entry for a multicast group when the port receives a leave message.

This command and the **igmp-snooping fast-leave** command have the same function but different effective ranges:

- The **fast-leave** command in IGMP-snooping view takes effect on all ports.
- The **igmp-snooping fast-leave** command takes effect on the current port.

For a port, the **igmp-snooping fast-leave** command takes priority over the **fast-leave** command in IGMP-snooping view.

## Examples

```
# Enable fast-leave processing globally for VLAN 2.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] fast-leave vlan 2
```

## Related commands

**igmp-snooping fast-leave**

# group-policy (IGMP-snooping view)

Use **group-policy** to configure a global multicast group policy to control the multicast groups that receiver hosts can join.

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

## Syntax

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

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

## Default

Global multicast group policies are not configured, and receiver hosts can join multicast groups.

## Views

IGMP-snooping view

## Predefined user roles

network-admin

## Parameters

**acl-number**: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Receiver hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or the ACL does not contain valid rules, receiver hosts cannot join multicast groups.

**vlan vlan-list**: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command takes effect on all VLANs.

## Usage guidelines

In an IPv4 basic ACL, the **source** keyword matches the multicast group address in IGMP reports. In an IPv4 advanced ACL, the **source** and **destination** keywords match the multicast source address and multicast group address in IGMP reports, respectively. The multicast source address is considered to be 0.0.0.0 for the following IGMP reports:

- IGMPv1 and IGMPv2 reports.

- IGMPv3 IS\_EX and IGMPv3 TO\_EX reports that do not carry multicast source addresses.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

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

This command takes effect only on the multicast groups that a port joins dynamically.

This command and the **igmp-snooping group-policy** command have the same function but different effective ranges:

- The **group-policy** command in IGMP-snooping view takes effect on all ports.
- The **igmp-snooping group-policy** command takes effect on the current port.

For a port, the **igmp-snooping group-policy** command takes priority over the **group-policy** command in IGMP-snooping view.

## Examples

```
# Globally configure a multicast group policy for VLAN 2 so that the hosts in this VLAN can join only the
multicast group 225.1.1.1.
<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
```

## Related commands

**igmp-snooping group-policy**

## host-aging-time (IGMP-snooping view)

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

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

## Syntax

**host-aging-time** *interval*

**undo host-aging-time**

## Default

The default setting is 260 seconds.

## Views

IGMP-snooping view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

## Usage guidelines

To avoid mistakenly deleting multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by the following formula:

$$[ \text{IGMP general query interval} ] + [ \text{maximum response time for IGMP general queries} ]$$

HP recommends that you set the aging timer of dynamic member ports to the value calculated by the following formula:

$$[ \text{IGMP general query interval} ] \times 2 + [ \text{maximum response time for IGMP general queries} ]$$

This command and the **igmp-snooping host-aging-time** command have the same function but different effective ranges:

- The **host-aging-time** command in IGMP-snooping view takes effect on all VLANs.
- The **igmp-snooping host-aging-time** command takes effect on the current VLAN.

For a VLAN, the **igmp-snooping host-aging-time** command takes priority over the **host-aging-time** command in IGMP-snooping view.

## 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
```

## Related commands

**igmp-snooping host-aging-time**

# igmp-snooping

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

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

## Syntax

**igmp-snooping**

**undo igmp-snooping**

## Default

IGMP snooping is globally disabled.

## Views

System view

## Predefined user roles

network-admin

## Examples

```
# Enable IGMP snooping globally and enter IGMP-snooping view.  
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping]
```

## Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

# igmp-snooping dot1p-priority

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

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

## Syntax

**igmp-snooping dot1p-priority** *priority-number*

**undo igmp-snooping dot1p-priority**

## Default

The 802.1p priority for IGMP messages is not configured.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*priority-number*: Sets an 802.1p priority for IGMP messages, in the range of 0 to 7. A higher value means a higher priority.

## Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

This command and the **dot1p-priority** command in IGMP-snooping view have the same function but different effective ranges:

- The **dot1p-priority** command in IGMP-snooping view takes effect on all VLANs.
- The **igmp-snooping dot1p-priority** command takes effect on the current VLAN.

For a VLAN, the **igmp-snooping dot1p-priority** command takes priority over the **dot1p-priority** command in IGMP-snooping view.

## Examples

# In VLAN 2, enable IGMP snooping, and set the 802.1p priority for IGMP messages 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
```

## Related commands

- **dot1p-priority** (IGMP-snooping view)
- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

## igmp-snooping drop-unknown

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.

### Syntax

**igmp-snooping drop-unknown**

**undo igmp-snooping drop-unknown**

### Default

Dropping unknown multicast data in a VLAN is disabled, and unknown multicast data is flooded in the VLAN.

### Views

VLAN view

### Predefined user roles

network-admin

### Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command for the VLAN.

### Examples

# In VLAN 2, enable IGMP snooping, and enable 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
```

### Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

## igmp-snooping enable

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

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

### Syntax

**igmp-snooping enable**

**undo igmp-snooping enable**

### Default

IGMP snooping is disabled in a VLAN.

### Views

VLAN view

## Predefined user roles

network-admin

## Usage guidelines

You must enable IGMP snooping globally before you enable IGMP snooping for a VLAN.

This command and the **enable** command in IGMP-snooping view have the same function but different effective ranges:

- The **enable** command in IGMP-snooping view takes effect on the specified VLANs.
- The **igmp-snooping enable** command takes effect on the current VLAN.

For a VLAN, the **igmp-snooping enable** command and the **enable** command in IGMP-snooping view have the same priority, and the most recent configuration takes effect.

## Examples

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

## Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping**

# igmp-snooping fast-leave

Use **igmp-snooping fast-leave** to enable fast-leave processing on a port.

Use **undo igmp-snooping fast-leave** to disable fast-leave processing on a port.

## Syntax

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

## Default

Fast-leave processing is disabled on a port.

## Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Parameters

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command takes effect on all VLANs.

## Usage guidelines

This feature enables the switch to immediately remove a port from the forwarding entry for a multicast group when the port receives a leave message.

This command and the **fast-leave** command in IGMP-snooping view have the same function but different effective ranges:

- The **fast-leave** command in IGMP-snooping view takes effect on all ports.
- The **igmp-snooping fast-leave** command takes effect on the current port.

For a port, the **igmp-snooping fast-leave** command takes priority over the **fast-leave** command in IGMP-snooping view.

## Examples

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

## Related commands

**fast-leave** (IGMP-snooping view)

# igmp-snooping general-query source-ip

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

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

## Syntax

**igmp-snooping general-query source-ip** *ip-address*

**undo igmp-snooping general-query source-ip**

## Default

The source IP address of IGMP general queries is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*ip-address*: Specifies an IP address.

## Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

## Examples

```
# In VLAN 2, enable IGMP snooping, and configure 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
```

### Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

## igmp-snooping group-limit

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.

### Syntax

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

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

### Default

The default setting is 4294967295.

### Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

### Predefined user roles

network-admin

### Parameters

*limit*: Sets the maximum number of multicast groups that a port can join, in the range of 0 to 4294967295.

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command takes effect on all VLANs.

### Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

### Examples

```
# Set the maximum number of multicast groups that Ten-GigabitEthernet 1/0/1 in VLAN 2 can join to 10.
```

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

## igmp-snooping group-policy

Use **igmp-snooping group-policy** to configure a multicast group policy on a port to control the multicast groups that the receiver hosts attached to the port can join.

Use **undo igmp-snooping group-policy** to remove the multicast group policy on a port.

## Syntax

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

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

## Default

Multicast group policies are not configured on a port, and the hosts attached to the port can join multicast groups.

## Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Parameters

*acl-number*: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Receiver hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or the ACL does not contain valid rules, receiver hosts cannot join multicast groups.

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command takes effect on all VLANs.

## Usage guidelines

In an IPv4 basic ACL, the **source** keyword matches the multicast group address in IGMP reports. In an IPv4 advanced ACL, the **source** and **destination** keywords match the multicast source address and multicast group address in IGMP reports, respectively. The multicast source address is considered to be 0.0.0.0 for the following IGMP reports:

- IGMPv1 and IGMPv2 reports.
- IGMPv3 IS\_EX and IGMPv3 TO\_EX reports that do not carry multicast source addresses.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

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

This command takes effect only on the multicast groups that a port joins dynamically.

This command and the **group-policy** command in IGMP-snooping view have the same function but different effective ranges:

- The **group-policy** command in IGMP-snooping view takes effect on all ports.
- The **igmp-snooping group-policy** command takes effect on the current port.

For a port, the **igmp-snooping group-policy** command takes priority over the **group-policy** command in IGMP-snooping view.

## Examples

```
# Configure a multicast group policy for VLAN 2 on Ten-GigabitEthernet 1/0/1 so that hosts attached to the port in VLAN 2 can join only the multicast group 225.1.1.1.
```

```
<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 ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
```

## Related commands

**group-policy** (IGMP-snooping view)

# igmp-snooping host-aging-time

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

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

## Syntax

**igmp-snooping host-aging-time** *interval*

**undo igmp-snooping host-aging-time**

## Default

The default setting is 260 seconds.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an aging timer for the dynamic member ports in a VLAN, in the range of 1 to 8097894 seconds.

## Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command for the VLAN.

To avoid mistakenly deleting multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by the following formula:

[ IGMP general query interval ] + [ maximum response time for IGMP general queries ]

HP recommends that you set the aging timer of dynamic member ports to the value calculated by the following formula:

[ IGMP general query interval ] × 2 + [ maximum response time for IGMP general queries ]

This command and the **host-aging-time** command in IGMP-snooping view have the same function but different effective ranges:

- The **host-aging-time** command in IGMP-snooping view takes effect on all VLANs.
- The **igmp-snooping host-aging-time** command takes effect on the current VLAN.

For a VLAN, the **igmp-snooping host-aging-time** command takes priority over the **host-aging-time** command in IGMP-snooping view.

## Examples

```
# In VLAN 2, enable IGMP snooping, and set the aging timer for the dynamic member ports 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
```

### Related commands

- **enable** (IGMP-snooping view)
- **host-aging-time** (IGMP-snooping view)
- **igmp-snooping enable**

## igmp-snooping host-join

Use **igmp-snooping host-join** to configure a port as a simulated member host for a multicast group.

Use **undo igmp-snooping host-join** to remove the simulated joining configuration.

### 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 | all }
```

### Default

A port is not configured as a simulated member host for multicast groups.

### Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

### Predefined user roles

network-admin

### Parameters

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

**source-ip** *source-address*: Specifies a multicast source by its IP address. If you specify a multicast source, the command configures the port as a simulated member host for a multicast source and group. If you do not specify a multicast source, the command configures the port as a simulated member host for a multicast group. This option takes effect on IGMPv3 snooping devices.

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

**all**: Specifies all multicast groups.

### Usage guidelines

Unlike a static member port, a port configured as a simulated member host ages out like a dynamic member port.

The IGMP version and IGMP snooping version that the simulated member host runs must be the same.

### Examples

```
# Configure Ten-GigabitEthernet 1/0/1 as a simulated member host of the multicast source and group (1.1.1.1, 232.1.1.1) 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 version 3
[Sysname-vlan2] quit
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] igmp-snooping host-join 232.1.1.1 source-ip 1.1.1.1
vlan 2

```

## igmp-snooping last-member-query-interval

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

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

### Syntax

**igmp-snooping last-member-query-interval** *interval*

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

### Default

The default setting is 1 second.

### Views

VLAN view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets an IGMP last member query interval in the range of 1 to 25 seconds.

### Usage guidelines

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

You must enable IGMP snooping for a VLAN before you execute this command for the VLAN.

This command and the **last-member-query-interval** command in IGMP-snooping view have the same function but different effective ranges:

- The **last-member-query-interval** command in IGMP-snooping view takes effect on all VLANs.
- The **igmp-snooping last-member-query-interval** command takes effect on the current VLAN.

For a VLAN, the **igmp-snooping last-member-query-interval** command takes priority over the **last-member-query-interval** command in IGMP-snooping view.

### Examples

# In VLAN 2, enable IGMP snooping, and set the IGMP last member query interval to 3 seconds.

```

<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

```

## Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**
- **last-member-query-interval** (IGMP-snooping view)

## igmp-snooping leave source-ip

Use **igmp-snooping leave source-ip** to configure a source IP address for IGMP leave messages.

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

### Syntax

**igmp-snooping leave source-ip** *ip-address*

**undo igmp-snooping leave source-ip**

### Default

The source IP address of IGMP leave messages is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

### Views

VLAN view

### Predefined user roles

network-admin

### Parameters

*ip-address*: Specifies a source IP address for IGMP leave messages.

### Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

### Examples

# In VLAN 2, enable IGMP snooping, and configure 10.1.1.1 as the source IP address of IGMP leave messages.

```
<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
```

## Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

## igmp-snooping max-response-time

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

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

## Syntax

```
igmp-snooping max-response-time interval  
undo igmp-snooping max-response-time
```

## Default

The default setting is 10 seconds.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets the maximum response time for IGMP general queries, in the range of 1 to 3174 seconds.

## Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command for the VLAN.

To avoid mistakenly deleting multicast group members, set IGMP general query interval to be greater than the maximum response time for IGMP general queries.

This command and the **max-response-time** command in IGMP-snooping view have the same function but different effective ranges:

- The **max-response-time** command in IGMP-snooping view takes effect on all VLANs.
- The **igmp-snooping max-response-time** command takes effect on the current VLAN.

For a VLAN, the **igmp-snooping max-response-time** command takes priority over the **max-response-time** command in IGMP-snooping view.

## Examples

```
# In VLAN 2, enable IGMP snooping, and set the maximum response time for IGMP general queries to 5 seconds.
```

```
<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
```

## Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**
- **max-response-time** (IGMP-snooping view)

## igmp-snooping overflow-replace

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

Use **undo igmp-snooping overflow-replace** to disable the multicast group replacement feature on a port.

## Syntax

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

## Default

The multicast group replacement feature is disabled on a port.

## Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Parameters

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command takes effect on all VLANs.

## Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

This command and the **overflow-replace** command in IGMP-snooping view have the same function but different effective ranges:

- The **overflow-replace** command in IGMP-snooping view takes effect on all ports.
- The **igmp-snooping overflow-replace** command takes effect on the current port.

For a port, the **igmp-snooping overflow-replace** command takes priority over the **overflow-replace** command in IGMP-snooping view.

## Examples

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

## Related commands

**overflow-replace** (IGMP-snooping view)

# igmp-snooping querier

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

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

## Syntax

```
igmp-snooping querier  
undo igmp-snooping querier
```

## Default

The IGMP snooping querier is disabled.



## Views

VLAN view

## Predefined user roles

network-admin

## Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

This command takes effect on a sub-VLAN only after you remove the sub-VLAN from the multicast VLAN.

## Examples

```
# In VLAN 2, enable IGMP snooping, and enable the IGMP snooping querier.
```

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

## Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**
- **subvlan** (multicast VLAN view)

# igmp-snooping query-interval

Use **igmp-snooping query-interval** to set the IGMP general query interval for a VLAN.

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

## Syntax

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

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

## Default

The IGMP general query interval in a VLAN is 125 seconds.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an IGMP general query interval in the range of 2 to 31744 seconds.

## Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

To avoid mistakenly deleting multicast group members, set the IGMP general query interval to be greater than the maximum response time for IGMP general queries.

## Examples

```
# In VLAN 2, enable IGMP snooping, and set the IGMP general query interval to 20 seconds.
<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
```

## Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**
- **igmp-snooping max-response-time**
- **igmp-snooping querier**
- **max-response-time**

## igmp-snooping report source-ip

Use **igmp-snooping report source-ip** to configure a source IP address for IGMP reports.

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

## Syntax

**igmp-snooping report source-ip** *ip-address*

**undo igmp-snooping report source-ip**

## Default

The source IP address of IGMP reports is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*ip-address*: Specifies a source IP address for IGMP reports.

## Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

## Examples

```
# In VLAN 2, enable IGMP snooping, and configure 10.1.1.1 as the source IP address of IGMP reports.
<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
```

## Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

## igmp-snooping router-aging-time

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

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

### Syntax

**igmp-snooping router-aging-time** *interval*

**undo igmp-snooping router-aging-time**

### Default

The default setting is 260 seconds.

### Views

VLAN view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets an aging timer for the dynamic router ports in a VLAN, in the range of 1 to 8097894 seconds.

### Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command for the VLAN.

This command and the **router-aging-time** command in IGMP-snooping view have the same function but different effective ranges:

- The **router-aging-time** command in IGMP-snooping view takes effect on all VLANs.
- The **igmp-snooping router-aging-time** command takes effect on the current VLAN.

For a VLAN, the **igmp-snooping router-aging-time** command takes priority over the **router-aging-time** command in IGMP-snooping view.

### Examples

# In VLAN 2, enable IGMP snooping, and set the aging timer for the dynamic router ports to 100 seconds.

```
<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
```

## Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

- **router-aging-time** (IGMP-snooping view)

## igmp-snooping router-port-deny

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.

### Syntax

**igmp-snooping router-port-deny** [ **vlan** *vlan-list* ]

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

### Default

A port can become a dynamic router port.

### Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

### Predefined user roles

network-admin

### Parameters

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you specify VLANs, the command takes effect only when the port belongs to the specified VLANs. If you do not specify a VLAN, the command takes effect on all VLANs to which the port belongs.

### Examples

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

## igmp-snooping source-deny

Use **igmp-snooping source-deny** to enable multicast source port filtering on a port to discard all the received multicast data packets.

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

### Syntax

**igmp-snooping source-deny**

**undo igmp-snooping source-deny**

### Default

Multicast source port filtering is disabled, and the port can connect to both multicast sources and multicast receivers.

### Views

Layer 2 Ethernet interface view

## Predefined user roles

network-admin

## Usage guidelines

This command and the **source-deny** command in IGMP-snooping view have the same function but different effective ranges:

- The **source-deny** command in IGMP-snooping view takes effect on the specified ports.
- The **igmp-snooping source-deny** command takes effect on the current port.

For a port, the **igmp-snooping source-deny** command and the **source-deny** command in IGMP-snooping view have the same priority, and the most recent configuration takes effect.

## Examples

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

## Related commands

**source-deny** (IGMP-snooping view)

# igmp-snooping special-query source-ip

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

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

## Syntax

**igmp-snooping special-query source-ip** *ip-address*

**undo igmp-snooping special-query source-ip**

## Default

If the IGMP snooping querier has received IGMP general queries, the source IP address of IGMP group-specific queries is the source IP address of IGMP general queries. Otherwise, the source IP address of IGMP group-specific queries is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

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

## Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

## Examples

# In VLAN 2, enable IGMP snooping, and configure 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
```

## Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

## igmp-snooping static-group

Use **igmp-snooping static-group** to configure a port as a static group member of a multicast group.

Use **undo igmp-snooping static-group** to remove a static group member.

## 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* | **all** }

## Default

A port is not a static group member of multicast groups.

## Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Parameters

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

**source-ip** *source-address*: Specifies a multicast source by its IP address. If you specify a multicast source, the command configures the port as a static group member for a multicast source and group. If you do not specify a multicast source, the command configures the port as a static group member for a multicast group. This option takes effect on IGMPv3 snooping devices.

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

**all**: Specifies all VLANs.

## Examples

# Configure Ten-GigabitEthernet 1/0/1 as a static group member of the multicast source and group (1.1.1.1, 225.0.0.1) 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 version 3
[Sysname-vlan2] quit
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] igmp-snooping static-group 225.0.0.1 source-ip
1.1.1.1 vlan 2
```

## igmp-snooping static-router-port

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

Use **undo igmp-snooping static-router-port** to remove a static router port.

### Syntax

```
igmp-snooping static-router-port vlan vlan-id
undo igmp-snooping static-router-port { all | vlan vlan-id }
```

### Default

A port is not a static router port.

### Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

### Predefined user roles

network-admin

### Parameters

**all**: Specifies all VLANs.

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

### Examples

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

## igmp-snooping version

Use **igmp-snooping version** to specify an IGMP snooping version.

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

### Syntax

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

### Default

The IGMP snooping version in a VLAN is 2.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*version-number*: Specifies an IGMP snooping version, 2 or 3.

## Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command for the VLAN.

This command and the **version** command in IGMP-snooping view have the same function but different effective ranges:

- The **version** command in IGMP-snooping view takes effect on the specified VLANs.
- The **igmp-snooping version** command takes effect on the current VLAN.

For a VLAN, the **igmp-snooping version** command and the **version** command in IGMP-snooping view have the same priority, and the most recent configuration takes effect.

## Examples

# In VLAN 2, enable IGMP snooping, and specify IGMP snooping version 3.

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

## Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**
- **version** (IGMP-snooping view)

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

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

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

## Syntax

**last-member-query-interval** *interval*

**undo last-member-query-interval**

## Default

The global IGMP last member query is 1 second.

## Views

IGMP-snooping view

## Predefined user roles

network-admin



## Parameters

*interval*: Sets an IGMP last member query interval in the range of 1 to 25 seconds.

## Usage guidelines

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

This command and the **igmp-snooping last-member-query-interval** command have the same function but different effective ranges:

- The **last-member-query-interval** command in IGMP-snooping view takes effect on all VLANs.
- The **igmp-snooping last-member-query-interval** command takes effect on the current VLAN.

For a VLAN, the **igmp-snooping last-member-query-interval** command takes priority over the **last-member-query-interval** command in IGMP-snooping view.

## Examples

```
# Set the IGMP last member query interval to 3 seconds.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] last-member-query-interval 3
```

## Related commands

**igmp-snooping last-member-query-interval**

# max-response-time (IGMP-snooping view)

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

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

## Syntax

**max-response-time** *interval*

**undo max-response-time**

## Default

The global maximum response time for IGMP general queries is 10 seconds.

## Views

IGMP-snooping view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets the maximum response time for IGMP general queries, in the range of 1 to 3174 seconds.

## Usage guidelines

To avoid mistakenly deleting multicast group members, set IGMP general query interval to be greater than the maximum response time for IGMP general queries.

This command and the **igmp-snooping max-response-time** command have the same function but different effective ranges:

- The **max-response-time** command in IGMP-snooping view takes effect on all VLANs.

- The **igmp-snooping max-response-time** command takes effect on the current VLAN. For a VLAN, the **igmp-snooping max-response-time** command takes priority over the **max-response-time** command in IGMP-snooping view.

## Examples

```
# Set the global maximum response time for IGMP general queries to 5 seconds.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] max-response-time 5
```

## Related commands

**igmp-snooping max-response-time**

# overflow-replace (IGMP-snooping view)

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

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

## Syntax

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

## Default

The multicast group replacement feature is disabled globally.

## Views

IGMP-snooping view

## Predefined user roles

network-admin

## Parameters

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id to end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command takes effect on all VLANs.

## Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

This command and the **igmp-snooping overflow-replace** command have the same function but different effective ranges:

- The **overflow-replace** command in IGMP-snooping view takes effect on all ports.
- The **igmp-snooping overflow-replace** command takes effect on the current port.

For a port, the **igmp-snooping overflow-replace** command takes priority over the **overflow-replace** command in IGMP-snooping view.

## Examples

```
# Enable the multicast group replacement feature globally for VLAN 2.
<Sysname> system-view
[Sysname] igmp-snooping
```

```
[Sysname-igmp-snooping] overflow-replace vlan 2
```

## Related commands

**igmp-snooping overflow-replace**

# report-aggregation (IGMP-snooping view)

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

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

## Syntax

**report-aggregation**

**undo report-aggregation**

## Default

IGMP report suppression is enabled.

## Views

IGMP-snooping view

## Predefined user roles

network-admin

## Examples

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

# reset igmp-snooping group

Use **reset igmp-snooping group** to remove the dynamic IGMP snooping forwarding entries for multicast groups.

## Syntax

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

## Views

User view

## Predefined user roles

network-admin

## Parameters

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

*source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, the command removes the dynamic IGMP snooping forwarding entries for all multicast sources.

**all**: Specifies all multicast groups.

**vlan** *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command removes dynamic IGMP snooping forwarding entries for all VLANs.

## Examples

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

## Related commands

**display igmp-snooping group**

# reset igmp-snooping router-port

Use **reset igmp-snooping router-port** to remove dynamic router ports.

## Syntax

```
reset igmp-snooping router-port { all | vlan vlan-id }
```

## Views

User view

## Predefined user roles

network-admin

## Parameters

**all**: Specifies all dynamic router ports.

**vlan** *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command removes dynamic router ports for all VLANs.

## Examples

```
# Remove all dynamic router ports.
<Sysname> reset igmp-snooping router-port all
```

## Related commands

**display igmp-snooping router-port**

# reset igmp-snooping statistics

Use **reset igmp-snooping statistics** to clear statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping.

## Syntax

```
reset igmp-snooping statistics
```

## Views

User view

## Predefined user roles

network-admin

## Examples

```
# Clear the statistics for all IGMP messages and PIMv2 hello messages learned through IGMP snooping.
<Sysname> reset igmp-snooping statistics
```

## Related commands

**display igmp-snooping statistics**

## router-aging-time (IGMP-snooping view)

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

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

### Syntax

**router-aging-time** *interval*

**undo router-aging-time**

### Default

The global aging timer for dynamic router ports is 260 seconds.

### Views

IGMP-snooping view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

### Usage guidelines

This command and the **igmp-snooping router-aging-time** command have the same function but different effective ranges:

- The **router-aging-time** command in IGMP-snooping view takes effect on all VLANs.
- The **igmp-snooping router-aging-time** command takes effect on the current VLAN.

For a VLAN, the **igmp-snooping router-aging-time** command takes priority over the **router-aging-time** command in IGMP-snooping view.

### Examples

```
# Set the global aging timer for dynamic router ports to 100 seconds.
```

```
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] router-aging-time 100
```

## Related commands

**igmp-snooping router-aging-time**

## source-deny (IGMP-snooping view)

Use **source-deny** to enable multicast source port filtering on ports to discard all the received multicast data packets.

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

### Syntax

**source-deny port** *interface-list*

**undo source-deny port** *interface-list*

## Default

Multicast source port filtering is disabled, and the ports can connect to both multicast sources and multicast receivers.

## Views

IGMP-snooping view

## Predefined user roles

network-admin

## Parameters

**port** *interface-list*: Specifies a port list. Specifies a space-separated list of port items. Each item specifies a port by its port type and number or a range of ports in the form of *start-interface-type interface-number to end-interface-type interface-number*.

## Usage guidelines

This command and the **igmp-snooping source-deny** command have the same function but different effective ranges:

- The **source-deny** command in IGMP-snooping view takes effect on the specified ports.
- The **igmp-snooping source-deny** command takes effect on the current port.

For a port, the **igmp-snooping source-deny** command and the **source-deny** command in IGMP-snooping view have the same priority, and the most recent configuration takes effect.

## Examples

```
# Enable multicast source port filtering on ports Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/4.  
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] source-deny port ten-gigabitethernet 1/0/1 to  
ten-gigabitethernet 1/0/4
```

## Related commands

**igmp-snooping source-deny**

# version (IGMP-snooping view)

Use **version** to specify an IGMP snooping version for VLANs.

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

## Syntax

**version** *version-number* **vlan** *vlan-list*

**undo version** **vlan** *vlan-list*

## Default

The default setting in a VLAN is 2.

## Views

IGMP-snooping view

## Predefined user roles

network-admin

## Parameters

*version-number*: Specifies an IGMP snooping version, 2 or 3.

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id to end-vlan-id*. The value range for the VLAN ID is 1 to 4094.

## Usage guidelines

You must enable IGMP snooping for the specified VLANs before you execute this command.

This command and the **igmp-snooping version** command have the same function but different effective ranges:

- The **version** command in IGMP-snooping view takes effect on the specified VLANs.
- The **igmp-snooping version** command takes effect on the current VLAN.

For a VLAN, the **igmp-snooping version** command and the **version** command in IGMP-snooping view have the same priority, and the most recent configuration takes effect.

## Examples

# Enable IGMP snooping for VLAN 2 through VLAN 10, and specify IGMP snooping version 3 for these VLANs.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] enable vlan 2 to 10
[Sysname-igmp-snooping] version 3 vlan 2 to 10
```

## Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

# PIM snooping commands

## display pim-snooping neighbor

Use **display pim-snooping neighbor** to display PIM snooping neighbor information.

### Syntax

```
display pim-snooping neighbor [ vlan vlan-id ] [ slot slot-number ] [ verbose ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vlan** *vlan-id*: Specifies a VLAN in the range of 1 to 4094. If you do not specify a VLAN, the command displays PIM snooping neighbor information for all VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays PIM snooping neighbor information on the master device.

**verbose**: Displays detailed information. If you do not specify this keyword, the command displays brief information.

### Examples

```
# Display detailed PIM snooping neighbor information for VLAN 2.
```

```
<Sysname> display pim-snooping neighbor vlan 2 verbose  
Total 2 neighbors.
```

```
VLAN 2: Total 2 neighbors.
```

```
10.1.1.2
```

```
Slots (0 in total):
```

```
Ports (1 in total):
```

```
  XGE1/0/1                (02:02:23)    LAN Prune Delay(T)
```

```
10.1.1.3
```

```
Slots (0 in total):
```

```
Ports (1 in total):
```

```
  XGE1/0/2                (00:32:43)
```

### Table 11 Command output

Field	Description
Total 2 neighbors	Total number of PIM snooping neighbors.
VLAN 2: Total 2 neighbors	Total number of PIM snooping neighbors in VLAN 2.



Field	Description
10.1.1.2	IP address of the PIM snooping neighbor.
Ports (1 in total)	Ports that have PIM snooping neighbors, and the total number of the ports.
(02:02:23)	Remaining aging timer for a PIM snooping neighbor on the port. <ul style="list-style-type: none"> <li>For a global port, this field is always displayed.</li> <li>For a non-global port, this field is displayed if the port is on the master device. Otherwise, you must specify the <b>slot slot-number</b> option to display this field.</li> </ul>
LAN Prune Delay	The PIM hello message sent by the PIM snooping neighbor has the LAN_Prune_Delay option.
(T)	The join message suppression feature has been disabled for the PIM snooping neighbor.

## display pim-snooping router-port

Use **display pim-snooping router-port** to display PIM snooping router port information.

### Syntax

**display pim-snooping router-port** [ **vlan** *vlan-id* ] [ **slot** *slot-number* ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vlan** *vlan-id*: Specifies a VLAN in the range of 1 to 4094. If you do not specify a VLAN, the command displays PIM snooping router port information for all VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays PIM snooping router port information on the master device.

### Examples

```
# Display PIM snooping router port information for VLAN 2.
<Sysname> display pim-snooping router-port vlan 2
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    XGE1/0/1                (00:01:30)
    XGE1/0/2                (00:01:32)
```

**Table 12 Command output**

Field	Description
VLAN 2	VLAN ID.

Field	Description
Router ports (2 in total)	Router ports, and the total number of the router ports.
(00:01:30)	Remaining aging time for the router port. <ul style="list-style-type: none"> <li>For a global port, this field is always displayed.</li> <li>For a non-global port, this field is displayed if the port is on the master device. Otherwise, you must specify the <b>slot slot-number</b> option to display this field.</li> </ul>

## display pim-snooping routing-table

Use **display pim-snooping routing-table** to display PIM snooping routing entries.

### Syntax

```
display pim-snooping routing-table [ vlan vlan-id ] [ slot slot-number ] [ verbose ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vlan** *vlan-id*: Specifies a VLAN in the range of 1 to 4094. If you do not specify a VLAN, the command displays PIM snooping routing entries for all VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays PIM snooping routing entries on the master device.

**verbose**: Displays detailed information. If you do not specify this keyword, the command displays brief information.

### Examples

```
# Display detailed information about PIM snooping routing entries for VLAN 2.
```

```
<Sysname> display pim-snooping routing-table vlan 2 verbose
```

```
Total 1 entries.
```

```
FSM Flag: NI-no info, J-join, PP-prune pending
```

```
VLAN 2: Total 1 entries.
```

```
(172.10.10.1, 225.1.1.1)
```

```
Upstream neighbor: 20.1.1.1
```

```
FSM information: normal
```

```
Upstream Slots (0 in total):
```

```
Upstream Ports (1 in total):
```

```
  XGE1/0/1
```

```
Downstream Slots (0 in total):
```

```
Downstream Ports (2 in total):
```

```
  XGE1/0/2
```

```
Expires: 00:03:01, FSM: J
```

```

Downstream Neighbors (2 in total):
 7.1.1.1
   Expires: 00:59:19, FSM: J
 7.1.1.11
   Expires: 00:59:20, FSM: J
XGE1/0/3
   Expires: 00:02:21, FSM: PP

```

**Table 13 Command output**

Field	Description
Total 1 entries	Total number of (S, G) entries and (*, G) entries.
FSM Flag: NI-no info, J-join, PP-prune pending	State machine flag of the downstream port: <ul style="list-style-type: none"> <li>• <b>NI</b>—Initial state.</li> <li>• <b>J</b>—Join.</li> <li>• <b>PP</b>—Prune pending.</li> </ul>
(172.10.10.1, 225.1.1.1)	(S, G) entry.
FSM information	Finite state machine information of the entry: <ul style="list-style-type: none"> <li>• <b>delete</b>—The entry attributes have been deleted.</li> <li>• <b>dummy</b>—The entry is a new temporary entry.</li> <li>• <b>no info</b>—No entry exists.</li> <li>• <b>normal</b>—The entry is a correct entry.</li> </ul>
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry.
Upstream Ports (1 in total)	Upstream ports, and the total number of the upstream ports. This field is displayed if the upstream neighbor is on the master device. Otherwise, you must specify the <b>slot slot-number</b> option to display this field.
Downstream Ports (2 in total)	Downstream port of the upstream neighbor, and the total number of the downstream ports.
Downstream Neighbors (2 in total)	Downstream neighbors of the downstream port, and the total number of the downstream neighbors.
Expires: 00:03:01, FSM: J	Remaining aging time for the downstream port or downstream neighbor, and the finite state machine information. <ul style="list-style-type: none"> <li>• For a global port, this field is always displayed.</li> <li>• For a non-global port, this field is displayed if the port is on the master device. Otherwise, you must specify the <b>slot slot-number</b> option to display this field.</li> </ul>

## display pim-snooping statistics

Use **display pim-snooping statistics** to display statistics for the PIM messages learned through PIM snooping.

### Syntax

**display pim-snooping statistics**

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Examples

# Display statistics for the PIM messages learned through 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 14 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.

## Related commands

**reset pim-snooping statistics**

# pim-snooping enable

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

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

## Syntax

**pim-snooping enable**

**undo pim-snooping enable**

## Default

PIM snooping is disabled in a VLAN.

## Views

VLAN view

## Predefined user roles

network-admin

## Usage guidelines

You must enable IGMP snooping globally and for a VLAN before you execute this command the VLAN.

PIM snooping does not take effect on sub-VLANs of a multicast VLAN.

## Examples

```
# Enable IGMP snooping globally, and enable IGMP snooping and PIM snooping for 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
```

## Related commands

- **igmp-snooping**
- **igmp-snooping enable**

## pim-snooping graceful-restart join-aging-time

Use **pim-snooping graceful-restart join-aging-time** to set the aging time for PIM snooping global downstream ports and global router ports on the new master device in IRF master election.

Use **undo pim-snooping graceful-restart join-aging-time** to restore the default.

## Syntax

```
pim-snooping graceful-restart join-aging-time interval
undo pim-snooping graceful-restart join-aging-time
```

## Default

The default setting is 210 seconds.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an aging time in the range of 210 to 18000 seconds.

## Usage guidelines

A global downstream port or a global router port is a Layer 2 aggregate interface that acts as a downstream port or router port.

You must enable PIM snooping for a VLAN before you execute this command for the VLAN.

## Examples

```
# In VLAN 2, set the aging time for PIM snooping global downstream ports and global router ports to 600 seconds on the new master device in IRF master election.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
```

```
[Sysname-vlan2] pim-snooping enable
[Sysname-vlan2] pim-snooping graceful-restart join-aging-time 600
```

## Related commands

**pim-snooping enable**

# pim-snooping graceful-restart neighbor-aging-time

Use **pim-snooping graceful-restart neighbor-aging-time** to set the aging time for PIM snooping global neighbor ports on the new master device in IRF master election.

Use **undo pim-snooping graceful-restart neighbor-aging-time** to restore the default.

## Syntax

**pim-snooping graceful-restart neighbor-aging-time** *interval*

**undo pim-snooping graceful-restart neighbor-aging-time**

## Default

The default setting is 105 seconds.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an aging time in the range of 105 to 18000 seconds.

## Usage guidelines

A global neighbor port is a Layer 2 aggregate interface that acts as a neighbor port.

You must enable PIM snooping for a VLAN before you execute this command for the VLAN.

## Examples

# In VLAN 2, set the aging time for PIM snooping global neighbor ports to 300 seconds on the new master device in IRF master election.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] pim-snooping enable
[Sysname-vlan2] pim-snooping graceful-restart neighbor-aging-time 300
```

## Related commands

**pim-snooping enable**

# reset pim-snooping statistics

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

## Syntax

**reset pim-snooping statistics**

## Views

User view

## Predefined user roles

network-admin

## Examples

# Clear statistics for the PIM messages learned through PIM snooping.

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

## Related commands

**display pim-snooping statistics**

---

# Multicast VLAN commands

## display multicast-vlan

Use **display multicast-vlan** to display information about multicast VLANs.

### Syntax

```
display multicast-vlan [ vlan-id ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

*vlan-id*: Specifies a VLAN ID in the range of 1 to 4094. If you do not specify a VLAN ID, the command displays information about all multicast VLANs.

### Examples

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

```
<Sysname> display multicast-vlan
```

```
Total 2 multicast VLANs.
```

```
Multicast VLAN 100:
```

```
Sub-VLAN list(3 in total):
```

```
2-3, 6
```

```
Port list(3 in total):
```

```
XGE1/0/1
```

```
XGE1/0/2
```

```
XGE1/0/3
```

```
Multicast VLAN 200:
```

```
Sub-VLAN list(0 in total):
```

```
Port list(0 in total):
```

**Table 15 Command output**

Field	Description
Total 2 multicast VLANs	Total number of multicast VLANs.
Sub-VLAN list(3 in total)	Sub-VLAN list of the multicast VLAN, and the total number of the sub-VLANs.
Port list(3 in total)	Port list of the multicast VLAN, and the total number of the ports.



# display multicast-vlan group

Use **display multicast-vlan group** to display information about multicast groups in multicast VLANs.

## Syntax

```
display multicast-vlan group [ source-address | group-address | slot slot-number | verbose | vlan vlan-id ] *
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**source-address**: Specifies a multicast source by its IP address. If you do not specify a multicast source, the command displays information about multicast groups for all multicast sources in multicast VLANs.

**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 a multicast group, the command displays information about all multicast groups in multicast VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays information about multicast groups in multicast VLANs on the master device.

**verbose**: Displays detailed information.

**vlan** *vlan-id*: Specifies a multicast VLAN in the range of 1 to 4094. If you do not specify a VLAN, the command displays information about multicast groups in all multicast VLANs.

## Examples

```
# Display detailed information about all multicast groups in all multicast VLANs.
```

```
<Sysname> display multicast-vlan group verbose  
Total 6 entries.
```

```
Multicast VLAN 10: Total 3 entries.
```

```
(2.2.2.2, 225.1.1.2)  
Flags: 0x70000020  
Sub-VLANs (1 in total):  
VLAN 40  
(111.112.113.115, 225.1.1.4)  
Flags: 0x70000030  
Sub-VLANs (1 in total):  
VLAN 40  
(0.0.0.0, 226.1.1.6)  
Flags: 0x60000020  
Sub-VLANs (1 in total):  
VLAN 40
```

```
Multicast VLAN 20: Total 3 entries.
```

```

(2.2.2.2, 225.1.1.2)
  Flags: 0x70000010
  Sub-VLANs (0 in total):
(111.112.113.115, 225.1.1.4)
  Flags: 0x70000010
  Sub-VLANs (0 in total):
(0.0.0.0, 226.1.1.6)
  Flags: 0x50000010
  Sub-VLANs (0 in total):

```

**Table 16 Command output**

Field	Description
Total 6 entries	Total number of (S, G) entries.
Multicast VLAN 10: Total 3 entries	Total number of (S, G) entries in multicast VLAN 10.
(0.0.0.0, 226.1.1.6)	(S, G) entry, where <b>0.0.0.0</b> in the S position means any multicast sources.
Flags	Current state of the (S, G) entry. Different bits represent difference status. For values of this field, see <a href="#">Table 17</a> .
Sub-VLANs (1 in total)	Sub-VLAN list of the multicast VLAN, and the total number of the sub-VLANs.

**Table 17 Values of the Flags field**

Value	Meaning
0x10	The entry is created by a multicast VLAN.
0x20	The entry is created by a sub-VLAN of a multicast VLAN.
0x40	The entry is to be deleted.
0x10000000	This value represents one of the following situations: <ul style="list-style-type: none"> <li>The entry is newly created.</li> <li>The device receives an IGMP query that matches the (S, G) entry but does not receive any matching IGMPv1 reports within an IGMP general query interval.</li> </ul>
0x20000000	The switch does not receive any IGMPv2 or IGMPv3 reports that match the (S, G) entry within an IGMP general query interval.
0x40000000	The switch does not receive any IGMPv3 IS_EX (NULL) reports that match the (S, G) entry within an IGMP general query interval.

## Related commands

**reset multicast-vlan group**

## display multicast-vlan forwarding-table

Use **display multicast-vlan forwarding-table** to display multicast VLAN forwarding entries.

## Syntax

```
display multicast-vlan forwarding-table [ group-address [ mask { mask-length | mask } ] | source-address [ mask { mask-length | mask } ] | slot slot-number | subvlan vlan-id | vlan vlan-id ] *
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

*group-address*: Specifies a multicast group by its IP address in the range of 224.0.0.0 to 239.255.255.255. If you do not specify a multicast group, the command displays multicast VLAN forwarding entries for all multicast groups.

**mask** { *mask-length* | *mask* }: Specifies a mask length or subnet mask for the multicast group address. The value range for the *mask-length* argument is 4 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

*source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, the command displays information about multicast VLAN forwarding entries for all multicast sources.

**mask** { *mask-length* | *mask* }: Specifies a mask length or subnet mask for the multicast source address. The value range for the *mask-length* argument is 0 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays multicast VLAN forwarding entries on the master device.

**subvlan** *vlan-id*: Specifies a sub-VLAN by its ID. If you do not specify a sub-VLAN, the command displays multicast VLAN forwarding entries for all sub-VLANs.

**vlan** *vlan-id*: Specifies a multicast VLAN by its ID. The value range for the *vlan-id* argument is 1 to 4094. If you do not specify a multicast VLAN, the command displays multicast VLAN forwarding entries for all multicast VLANs.

## Examples

```
# Display all multicast VLAN forwarding entries.
```

```
<Sysname> display multicast-vlan forwarding-table
```

```
Multicast VLAN 100 Forwarding Table
```

```
Total 1 entries, 1 matched
```

```
00001. (1.1.1.1, 225.0.0.1)
```

```
Flags: 0x10000
```

```
Multicast VLAN: 100
```

```
List of sub-VLANs (3 in total):
```

```
1: VLAN 10
```

```
2: VLAN 20
```

```
3: VLAN 30
```

**Table 18 Command output**

Field	Description
Multicast VLAN 100 Forwarding Table	Forwarding table for multicast VLAN 100.
Total 1 entries, 1 matched	Total number of forwarding entries, and the number of matching entries.
00001	Sequence number of the (S, G) entry.
(1.1.1.1, 255.0.0.1)	(S, G) entry, where <b>0.0.0.0</b> in the S position means any multicast sources.
Flags	Current status of the (S, G) entry. Different bits represent different states of the entry. For values of this field, see <a href="#">Table 19</a> .
List of sub-VLANs (3 in total)	Sub-VLAN list of the multicast VLAN, and the total number of the sub-VLANs.

**Table 19 Values of the Flags field**

Value	Meaning
0x1	The entry is in inactive state.
0x4	The entry fails to update.
0x8	The sub-VLAN information fails to update for the entry.
0x200	The entry is in GR state.
0x10000	The entry is a forwarding entry for a multicast VLAN.

## multicast-vlan

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

Use **undo multicast-vlan** to remove a multicast VLAN.

### Syntax

**multicast-vlan** *vlan-id*

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

### Default

A VLAN is not configured as a multicast VLAN.

### Views

System view

### Predefined user roles

network-admin

### Parameters

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

**all**: Specifies all multicast VLANs.

## Usage guidelines

The specified VLAN must exist.

HP recommends not configuring a multicast VLAN on a device that is enabled with IP multicast routing.

The total number of multicast VLANs on a device must not exceed the system upper limit.

For a sub-VLAN-based multicast VLAN, you must enable IGMP snooping for the multicast VLAN and all its sub-VLANs. For a port-based multicast VLAN, you must enable IGMP snooping for the multicast VLAN and all user VLANs to which the user ports are connected.

## Examples

# Enable IGMP snooping for VLAN 100. Configure VLAN 100 as a multicast VLAN and enter its 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]
```

## Related commands

- **igmp-snooping enable**
- **multicast routing**

# multicast-vlan entry-limit

Use **multicast-vlan entry-limit** to set the maximum number of multicast VLAN forwarding entries.

Use **undo multicast-vlan entry-limit** to restore the default.

## Syntax

**multicast-vlan entry-limit** *limit*

**undo multicast-vlan entry-limit**

## Default

The setting is 4000.

## Views

System view

## Predefined user roles

network-admin

## Parameters

*limit*: Sets the maximum number of multicast VLAN forwarding entries, in the range of 0 to 4000.

## Examples

# Set the maximum number of multicast VLAN forwarding entries to 256.

```
<Sysname> system-view
[Sysname] multicast-vlan entry-limit 256
```

## Related commands

**entry-limit** (IGMP-snooping view)

## port (multicast-VLAN view)

Use **port** to assign user ports to a multicast VLAN.

Use **undo port** to remove user ports from a multicast VLAN.

### Syntax

**port** *interface-list*

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

### Default

A multicast VLAN does not have user ports.

### Views

Multicast VLAN view

### Predefined user roles

network-admin

### Parameters

*interface-list*: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number to interface-type interface-number*.

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

### Usage guidelines

A port can belong to only one multicast VLAN.

You can assign Ethernet ports and Layer 2 aggregate interfaces as user ports of a multicast VLAN.

### Examples

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

## port multicast-vlan

Use **port multicast-vlan** to assign a port to a multicast VLAN.

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

### Syntax

**port multicast-vlan** *vlan-id*

**undo port multicast-vlan**

### Default

A port does not belong to multicast VLANs.

## Views

Ethernet interface view, Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Parameters

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

## Usage guidelines

A port can belong to only one multicast VLAN.

## Examples

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

# reset multicast-vlan group

Use **reset multicast-vlan group** to clear multicast groups in multicast VLANs.

## Syntax

Use **reset multicast-vlan group** [ *source-address* [ **mask** { *mask-length* | *mask* } ] | *group-address* [ **mask** { *mask-length* | *mask* } ] | **vlan** *vlan-id* ] \*

## Views

User view

## Predefined user roles

network-admin

## Parameters

*source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, the command clears multicast groups for all multicast sources in multicast VLANs.

**mask** { *mask-length* | *mask* }: Specifies the mask length or subnet mask for the multicast source address. The value range for the *mask-length* argument is 0 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

*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 a multicast group, the command clears all multicast groups in multicast VLANs.

**mask** { *mask-length* | *mask* }: Specifies a mask length or subnet mask for the multicast group address. The value range for the *mask-length* argument is 4 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

**vlan** *vlan-id*: Specifies a multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a multicast VLAN, the command clears multicast groups in all multicast VLANs.

## Examples

```
# Clear multicast groups in all multicast VLANs.
<Sysname> reset multicast-vlan group
```

## Related commands

**display multicast-vlan group**

# subvlan (multicast-VLAN view)

Use **subvlan** to assign sub-VLANs to a multicast VLAN.

Use **undo subvlan** to remove sub-VLANs from a multicast VLAN.

## Syntax

**subvlan** *vlan-list*

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

## Default

A multicast VLAN does not have sub-VLANs.

## Views

Multicast VLAN view

## Predefined user roles

network-admin

## Parameters

*vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The value range for the VLAN ID is 1 to 4094.

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

## Usage guidelines

The VLANs to be configured as sub-VLANs must exist and must not be multicast VLANs or sub-VLANs of any other multicast VLAN.

## 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 commands

The term "interface" in this chapter collectively refers to 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

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

### Syntax

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

### Views

System view

### Predefined user roles

network-admin

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command deletes static multicast routes on the public network.

### Usage guidelines

This command deletes static multicast routes, but the **undo ip rpf-route-static** command deletes a specific static multicast route.

### Examples

```
# Delete all static multicast 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]:y
```

### Related commands

```
ip rpf-route-static
```

## display mac-address multicast

Use **display mac-address multicast** to display static multicast MAC address entries.

### Syntax

```
display mac-address [ mac-address [ vlan vlan-id ] | [ multicast ] [ vlan vlan-id ] [ count ] ]
```

### Views

Any view

## Predefined user roles

network-admin  
network-operator

## Parameters

**mac-address:** Specifies a multicast MAC address. The MAC address can be any legal multicast MAC address. (A multicast MAC address is the MAC address in which the least significant bit of the most significant octet is 1.)

**vlan** *vlan-id:* Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command displays the static multicast MAC address entries for all VLANs.

**multicast:** Specifies static multicast MAC address entries.

**count:** Specifies the number of static multicast MAC address entries. If you specify this keyword, the command displays the number of matching static multicast MAC address entries. If you do not specify this keyword, the command displays the contents of the matching entries rather than the entry count.

## Usage guidelines

This command displays all MAC address table entries, including static multicast and unicast MAC address entries when one of the following conditions exists:

- You do not specify parameters.
- You specify either or both of the **vlan** and **count** keywords.

## Examples

# Display the static multicast MAC address entries for VLAN 2.

```
<Sysname> display mac-address multicast vlan 2
MAC Address      VLAN ID   State           Port/NickName      Aging
0100-0001-0001  2         Multicast      XGE1/0/1           N
                                     XGE1/0/2
```

# Display the number of static multicast MAC address entries.

```
<Sysname> display mac-address multicast count
1 mac address(es) found.
```

### Table 20 Command output

Field	Description
VLAN ID	ID of the VLAN to which the network device identified by the MAC address belongs.
State	Status of the MAC address. If the multicast MAC address entry is static, this field displays <b>Multicast</b> .
Port/NickName	Outgoing ports or nickname of the Egress RB in a TRILL network for the packet that is sent to the MAC address in this MAC address entry. For more information about the nickname, TRILL, and RB, see <i>TRILL Configuration Guide</i> . <b>NOTE:</b> The switch does not support the TRILL function.
Aging	Aging time state. If this entry never expires, this field displays <b>N</b> .
1 mac address(es) found	One static multicast MAC address entry is found.

## Related commands

**mac-address multicast**

# display mrib interface

Use **display mrib interface** to display information about interfaces maintained by the MRIB, including PIM interfaces, IGMP interfaces, register interfaces, InLoopBack0 interfaces, and null0 interfaces.

## Syntax

```
display mrib [ vpn-instance vpn-instance-name ] interface [ interface-type interface-number ]
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays information about interfaces maintained by the MRIB on the public network.

*interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays information about all interfaces maintained by the MRIB.

## Examples

# Display information about all interfaces maintained by the MRIB on the public network.

```
<Sysname> display mrib interface
Interface: Vlan-interface1
  Index: 0x00000001
  Current state: up
  MTU: 1500
  Type: BROADCAST
  Protocol: PIM-DM
  PIM protocol state: Enabled
  Address list:
    1. Local address : 8.12.0.2/16
       Remote address: 0.0.0.0
       Reference      : 1
       State          : NORMAL
```

**Table 21 Command output**

Field	Description
Interface	Interface name.
Index	Index number of the interface.
Current state	Current status of the interface: up or down.
MTU	MTU value.

Field	Description
Type	Interface type: <ul style="list-style-type: none"> <li>• <b>BROADCAST</b>—Broadcast link interface.</li> <li>• <b>LOOP</b>—Loopback interface.</li> <li>• <b>REGISTER</b>—Register interface.</li> <li>• <b>NBMA</b>—NBMA interface.</li> <li>• <b>MTUNNEL</b>—Multicast tunnel interface.</li> </ul>
Protocol	Protocol running on the interface: PIM-DM, PIM-SM, IGMP, or MD.
PIM protocol state	Whether PIM is enabled: <ul style="list-style-type: none"> <li>• Enabled.</li> <li>• Disabled.</li> </ul>
Address list	Interface address list.
Local address	Local IP address.
Remote address	Remote end IP address. This field is displayed when the interface is vlink type.
Reference	Number of times that the address has been referenced.
State	Status of the interface address: NORMAL or DEL.

## display multicast boundary

Use **display multicast boundary** to display multicast boundary information.

### Syntax

```
display multicast [ vpn-instance vpn-instance-name ] boundary [ group-address [ mask-length | mask ] ]
[ interface interface-type interface-number ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays multicast boundary information on the public network.

*group-address*: Specifies a multicast group by its IP address in the range of 224.0.0.0 to 239.255.255.255. If you do not specify a multicast group, the command displays the multicast boundary information of all multicast groups.

*mask-length*: Specifies an address mask length in the range of 4 to 32. The default is 32.

*mask*: Specifies an address mask. The default is 255.255.255.255.

**interface** *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays the multicast boundary information on all interfaces.

## Examples

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

```
<Sysname> display multicast boundary
Boundary          Interface
224.1.1.0/24      Vlan1
239.2.2.0/24      Vlan2
```

**Table 22 Command output**

Field	Description
Boundary	Multicast group that corresponds to the multicast boundary.
Interface	Boundary interface that corresponds to the multicast boundary.

## Related commands

**multicast boundary**

# display multicast forwarding df-info

Use **display multicast forwarding df-info** to display information about the DF for multicast forwarding.

## Syntax

```
display multicast [ vpn-instance vpn-instance-name ] forwarding df-info [ rp-address ] [ verbose ] [ slot slot-number ]
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays information about the DF for multicast forwarding on the public network.

*rp-address*: Specifies an RP of BIDIR-PIM by its IP address.

**verbose**: Displays detailed information. If you do not specify this keyword, the command displays brief information about the DF.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays information about the DF for multicast forwarding on the master device.

## Usage guidelines

The router that acts as a DF is the only multicast data forwarder to the RP in a BIDIR-PIM domain.

## Examples

```
# Display brief information about the DF for multicast routing on the public network.
<Sysname> display multicast forwarding df-info
```

Total 1 RP, 1 matched

```
00001. RP address: 7.11.0.2
  Flags: 0x0
  Uptime: 04:14:40
  RPF interface: Vlan-interface1
  List of 1 DF interface:
    1: Vlan-interface2
```

# Display detailed information about the DF for multicast routing on the public network.

```
<Sysname> display multicast forwarding df-info verbose
```

Total 1 RP, 1 matched

```
00001. RP address: 7.11.0.2
  MID: 2, Flags: 0x0
  Uptime: 03:37:22
  Product information: 0x7a2f762f, 0x718fee9f, 0x4b82f137, 0x71c32184
  RPF interface: Vlan-interface1
  Product information: 0xa567d6fc, 0xadeb03e3
  Tunnel information: 0xdfb107d4, 0x7aa5d510
  List of 1 DF interface:
    1: Vlan-interface2
      Product information: 0xa986152b, 0xb74a9a2f
      Tunnel information: 0x297ca208, 0x76985b89
```

**Table 23 Command output**

Field	Description
Total 1 RP, 1 matched	Total number of RPs and total number of matching RPs.
00001	Sequence number of the entry to which the RP is designated.
MID	ID of the entry to which the RP is designated. Each entry to which the RP is designated has a unique MID.
Flags	Current state of the entry to which the RP is designated. Different bits represent different states of the entry. For values of this field, see <a href="#">Table 24</a> .
Uptime	Existence duration for the entry to which the RP is designated.
RPF interface	RPF interface to the RP.
List of 1 DF interface	DF interface list.

**Table 24 Values of the Flags field**

Value	Meaning
0x0	The entry is in correct state.
0x4	The entry fails to update.
0x8	The DF interface information fails to update for the entry.
0x40	The entry is to be deleted.
0x100	The entry is being deleted.

Value	Meaning
0x200	The entry is in GR state.

## display multicast forwarding event

Use **display multicast forwarding event** to display statistics for multicast forwarding events.

### Syntax

```
display multicast [ vpn-instance vpn-instance-name ] forwarding event [ slot slot-number ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays statistics for the multicast forwarding events on the public network.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays statistics for the multicast forwarding events on the master device.

### Examples

# Display statistics for the multicast forwarding events on the public network.

```
<Sysname> display multicast forwarding event
Total entry active event sent: 0
Total entry inactive event sent: 0
Total NoCache event sent: 2
Total NoCache event dropped: 0
Total WrongIF event sent: 0
Total WrongIF event dropped: 0
Total SPT switch event sent: 0
NoCache rate limit: 1024 packets/s
WrongIF rate limit: 1 packets/10s
Total timer of register suppress timeout: 0
```

**Table 25 Command output**

Field	Description
Total entry active event sent	Number of times that the entry-active event has been sent.
Total entry inactive event sent	Number of times that the entry-inactive event has been sent.
Total NoCache event sent	Number of times that the NoCache event has been sent.
Total NoCache event dropped	Number of times that the NoCache event has been dropped.
Total WrongIF event sent	Number of times that the WrongIF event has been sent.

Field	Description
Total WrongIF event dropped	Number of times that the WrongIF event has been dropped.
Total SPT switch event sent	Number of times that the SPT-switch event has been sent.
NoCache rate limit	Rate limit for sending the NoCache event, in pps.
WrongIF rate limit	Rate limit for sending the WrongIF event, in packets per 10 seconds.
Total timer of register suppress timeout	Number of times that the registration suppression has timed out in total.

## Related commands

**reset multicast forwarding event**

# display multicast forwarding-table

Use **display multicast forwarding-table** to display multicast forwarding entries.

## Syntax

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

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays multicast forwarding entries on the public network.

*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-length*: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

*mask*: Specifies an address mask. The default value is 255.255.255.255.

**incoming-interface**: Specifies the multicast forwarding entries that contain the specified incoming interface.

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

**outgoing-interface**: Specifies the multicast forwarding entries that contain the specified outgoing interface.

**exclude**: Specifies the multicast forwarding entries that do not contain the specified interface in the outgoing interface list.



**include:** Specifies the multicast forwarding entries that contain the specified interface in the outgoing interface list.

**match:** Specifies the forwarding entries that contain only the specified interface in the outgoing interface list.

**slot slot-number:** Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays multicast forwarding entries on the master device.

**statistics:** Displays statistics for the multicast forwarding entries.

## Examples

```
# Display multicast forwarding entries on the public network.
```

```
<Sysname> display multicast forwarding-table
```

```
Total 1 entry, 1 matched
```

```
00001. (172.168.0.2, 227.0.0.1)
```

```
Flags: 0x0
```

```
Uptime: 00:08:32, Timeout in: 00:03:26
```

```
Incoming interface: Vlan-interface10
```

```
    Incoming sub-VLAN: VLAN 11
```

```
    Outgoing sub-VLAN: VLAN 12
```

```
                    VLAN 13
```

```
List of 1 outgoing interface:
```

```
    1: Vlan-interface20
```

```
        Sub-VLAN: VLAN 21
```

```
                VLAN 22
```

```
Matched 19648 packets(20512512 bytes), Wrong If 0 packet
```

```
Forwarded 19648 packets(20512512 bytes)
```

**Table 26 Command output**

Field	Description
Total 1 entry, 1 matched	Total number of (S, G) entries and total number of matching (S, G) entries.
00001	Sequence number of the (S, G) entry.
(172.168.0.2,227.0.0.1)	(S, G) entry.
Flags	Current state of the (S, G) entry. Different bits represent different states of (S, G) entries. For values of this field, see <a href="#">Table 27</a> .
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 expire.
Incoming interface	Incoming interface of the (S, G) entry.
Incoming sub-VLAN	Incoming sub-VLAN of the super VLAN when the incoming interface of the (S, G) entry is the VLAN interface of this super VLAN.
Outgoing sub-VLAN	Outgoing sub-VLAN of the super VLAN when the incoming interface of the (S, G) entry is the VLAN interface of this super VLAN.
List of 1 outgoing interface:	Outgoing interface list of the (S, G) entry.

Field	Description
Sub-VLAN	Outgoing sub-VLAN of the super VLAN when the outgoing interface of the (S, G) entry is the VLAN interface of this super VLAN.
Matched 19648 packets(20512512 bytes), Wrong If 0 packet	Number of packets (bytes) that match the (S, G) entry, and number of packets with incoming interface errors.
Forwarded 19648 packets(20512512 bytes)	Number of packets (bytes) that have been forwarded.

**Table 27 Values of the Flags field**

Value	Meaning
0x0	The entry is in correct state.
0x1	The entry is in inactive state.
0x2	The entry is null.
0x4	The entry fails to update.
0x8	The outgoing interface information fails to update for the entry.
0x10	The entry in the switch group fails to update.
0x20	A register outgoing interface is available.
0x40	The entry is to be deleted.
0x80	The entry is in state of registration suppression.
0x100	The entry is being deleted.
0x200	The entry is in GR state.
0x400	The entry has the VLAN interface of the super VLAN.
0x800	The entry has the associated ARP entry of the multicast source address.
0x20000000	The entry is a BIDIR-PIM entry.

## Related commands

**reset multicast forwarding-table**

## display multicast forwarding-table df-list

Use **display multicast forwarding-table df-list** to display information about the DF list in the multicast forwarding table.

### Syntax

```
display multicast [ vpn-instance vpn-instance-name ] forwarding-table df-list [ group-address ] [ verbose ] [ slot slot-number ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays information about the DF list in the multicast forwarding table on the public network.

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

**verbose**: Specifies detailed information about the DF list in the multicast forwarding table. If you do not specify this keyword, the command displays brief information about the DF list in the multicast forwarding table.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays information about the DF list in the multicast forwarding table on the master device.

## Examples

# Display brief information about the DF list in the multicast forwarding table on the public network.

```
<Sysname> display multicast forwarding-table df-list
Total 1 entry, 1 matched
```

```
00001. (0.0.0.0, 225.0.0.1)
  List of 1 DF interface:
    1: Vlan-interface1
```

# Display detailed information about the DF list in the multicast forwarding table on the public network.

```
<Sysname> display multicast forwarding-table df-list verbose
Total 1 entry, 1 matched
```

```
00001. (0.0.0.0, 225.0.0.1)
  List of 1 DF interface:
    1: Vlan-interface1
      Product information: 0x347849f6, 0x14bd6837
      Tunnel information: 0xc4857986, 0x128a9c8f
```

**Table 28 Command output**

Field	Description
Total 1 entry, 1 matched	Total number of entries, and the total number of matching entries.
00001	Sequence number of the entry.
(0.0.0.0, 225.0.0.1)	(* , G) entry.
List of 1 DF interface	DF interface list.

## display multicast routing-table

Use **display multicast routing-table** to display multicast routing entries.

## Syntax

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

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays multicast routing entries on the public network.

*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-length*: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

*mask*: Specifies an address mask. The default is 255.255.255.255.

**incoming-interface**: Specifies the multicast routing entries that contain the specified incoming interface.

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

**outgoing-interface**: Specifies the multicast routing entries that contain the specified outgoing interface.

**exclude**: Specifies the multicast routing entries that do not contain the specified interface in the outgoing interface list.

**include**: Specifies the multicast routing entries that contain the specified interface in the outgoing interface list.

**match**: Specifies the multicast routing entries that contain only the specified interface in the outgoing interface list.

## Usage guidelines

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

## Examples

```
# Display multicast routing entries on the public network.
```

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

```
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
```

**Table 29 Command output**

Field	Description
Total 1 entry	Total number of (S, G) entries.
00001	Sequence number of the (S, G) entry.
(172.168.0.2, 227.0.0.1)	(S, G) entry.
Uptime	Length of time for which the (S, G) entry has been up.
Upstream Interface	Upstream interface of the (S, G) entry that multicast packets should arrive at.
List of 2 downstream interfaces	List of downstream interfaces that need to forward multicast packets.

**Related commands****reset multicast routing-table****display multicast routing-table static**Use **display multicast routing-table static** to display static multicast routing entries.**Syntax**

```
display multicast [ vpn-instance vpn-instance-name ] routing-table static [ source-address { mask-length | mask } ]
```

**Views**

Any view

**Predefined user roles**

network-admin

network-operator

**Parameters**

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays static multicast routes on the public network.

*source-address*: Specifies a multicast source address.

*mask-length*: Specifies an address mask length in the range of 0 to 32.

*mask*: Specifies an address mask.

**Usage guidelines**

This command displays information about only valid static multicast routes.

**Examples**

```
# Display static multicast routing entries on the public network.
```

```
<Sysname> display multicast routing-table static
```

```
Destinations: 3          Routes: 4
```

```
Destination/Mask  Pre  RPF neighbor  Interface
```

1.1.0.0/16	10	7.12.0.1	Vlan12
		7.11.0.1	Vlan11
2.2.2.0/24	20	7.11.0.1	Vlan11
3.3.3.3/32	50	7.12.0.1	Vlan12

**Table 30 Command output**

Field	Description
Destinations	Number of the multicast destination addresses.
Routes	Number of routes.
Destination/Mask	Destination address and mask length.
Pre	Route preference.
RPF neighbor	IP address of the RPF neighbor to the reachable destination.
Interface	Outgoing interface to the reachable destination.

## display multicast rpf-info

Use **display multicast rpf-info** to display RPF information for multicast sources.

### Syntax

```
display multicast [ vpn-instance vpn-instance-name ] rpf-info source-address [ group-address ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays RPF information for multicast sources on the public network.

*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.

### 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:
  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 31 Command output**

Field	Description
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: <ul style="list-style-type: none"> <li>• <b>igp</b>—IGP unicast route.</li> <li>• <b>egp</b>—EGP unicast route.</li> <li>• <b>unicast (direct)</b>—Directly connected unicast route.</li> <li>• <b>unicast</b>—Other unicast routes, such as static unicast route.</li> <li>• <b>multicast static</b>—Static multicast route.</li> </ul>
Route selection rule	Rule for RPF route selection: <ul style="list-style-type: none"> <li>• Route preference.</li> <li>• Longest prefix match.</li> </ul>
Load splitting rule	Status of the load splitting rule: enabled or disabled.

**Related commands**

- **display multicast forwarding-table**
- **display multicast routing-table**

## ip rpf-route-static

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

Use **undo ip rpf-route-static** to delete a static multicast route.

**Syntax**

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

```
undo ip rpf-route-static [ vpn-instance vpn-instance-name ] source-address { mask-length | mask }
{ rpf-nbr-address | interface-type interface-number }
```

**Default**

No static multicast route exists.

**Views**

System view

**Predefined user roles**

network-admin

**Parameters**

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command configures a static multicast route on the public network.

*source-address*: Specifies a multicast source address.

*mask-length*: Specifies an address mask length in the range of 0 to 32.

*mask*: Specifies an address mask.

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

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

*preference*: Sets a route preference in the range of 1 to 255. The default value is 1.

## Usage guidelines

In the same multicast source address range, you can configure up to 16 RPF neighbors.

When you specify an RPF neighbor on a Layer 3 interface, you must specify the *rpf-nbr-address* argument rather than the *interface-type interface-number* argument. Layer 3 interfaces include Layer 3 Ethernet, Layer 3 aggregate, Loopback, and VLAN interfaces.

The configured static multicast route might not take effect due to one of the following reasons:

- The outgoing interface iteration fails.
- The specified interface is not in the public network or the same VPN instance as the current interface.
- The specified interface is not a point-to-point interface.
- The specified interface is in down state.

If multiple static multicast routes within the same multicast source address range are available, only the one with the highest route preference can become active. Therefore, after you configure a static multicast route, use the **display multicast routing-table static** command to verify that the configured static multicast route has taken effect.

The **undo ip rpf-route-static** command deletes the specified static multicast route, but the **delete ip rpf-route-static** command deletes all static multicast routes.

## Examples

# On the public network, configure a static multicast route to the multicast source groups 10.1.1.1/24, and 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
```

## Related commands

- **delete ip rpf-route-static**
- **display multicast routing-table static**

## load-splitting (MRIB view)

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

Use **undo load-splitting** to restore the default.

## Syntax

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

```
undo load-splitting
```

## Default

Load splitting of multicast traffic is disabled.



## Views

MRIB view

## Predefined user roles

network-admin

## Parameters

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

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

## Usage guidelines

This command does not take effect on BIDIR-PIM.

## Examples

```
# Enable load splitting of multicast traffic on a per-source basis on the public network.
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] load-splitting source
```

# longest-match (MRIB view)

Use **longest-match** to specify the longest prefix match principle for RPF route selection.

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

## Syntax

**longest-match**

**undo longest-match**

## Default

Route preference is used for RPF route selection

## Views

MRIB view

## Predefined user roles

network-admin

## Examples

```
# Specify the longest prefix match principle for RPF route selection on the public network.
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] multicast longest-match
```

# mac-address multicast

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.

## 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
```

## Default

No static multicast MAC address entry is configured.

## Views

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

## Predefined user roles

network-admin

## Parameters

**mac-address**: Specifies a multicast MAC address, in the format H-H-H. The multicast MAC address that can be manually configured in the multicast MAC address entry must be unused. A multicast MAC address is the MAC address in which the least significant bit of the most significant octet is 1.

**interface** *interface-list*: Specifies a list of interfaces. You can specify up to four 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 a VLAN by its VLAN ID 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.

## Usage guidelines

You can configure static multicast MAC address entries on the specified interface in system view or on the current interface in interface view.

If you do not specify the **multicast** keyword, the **undo mac-address** command deletes all MAC address entries, including static unicast and multicast MAC address entries.

## Examples

```
# Create a multicast entry for 0100-0001-0001 in VLAN 2, and configure Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/5 in VLAN 2 as outgoing ports.
```

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

```
[Sysname] mac-address multicast 0100-0001-0001 interface ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/5 vlan 2
```

```
# Configure a multicast entry for 0100-0001-0001 on Ten-GigabitEthernet 1/0/1 in VLAN 2.
```

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

```
[Sysname] interface ten-gigabitethernet 1/0/1
```

```
[Sysname-Ten-GigabitEthernet1/0/1] mac-address multicast 0100-0001-0001 vlan 2
```

## Related commands

```
display mac-address multicast
```

## multicast boundary

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

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

### Syntax

```
multicast boundary group-address { mask-length | mask }
```

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

### Default

No multicast forwarding boundary is configured.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

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

*mask-length*: Specifies an address mask length in the range of 4 to 32.

*mask*: Specifies an address mask.

**all**: Specifies all forwarding boundaries configured on the interface.

### Usage guidelines

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.

You do not need to enable IP multicast routing before executing this command.

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.

### 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
```

### Related commands

**display multicast boundary**

## multicast forwarding supervlan community

Use **multicast forwarding supervlan community** to configure multicast forwarding among sub-VLANs of a super VLAN.

Use **undo multicast forwarding supervlan community** to restore the default.

### Syntax

```
multicast forwarding supervlan community  
undo multicast forwarding supervlan community
```

### Default

Multicast data cannot be forwarded among sub-VLANs of the super VLAN.

### Views

VLAN interface view

### Predefined user roles

network-admin

### Usage guidelines

After you execute the **multicast forwarding supervlan community** command, you must clear all multicast forwarding entries with the super VLAN interface as the incoming interface. Otherwise, this command cannot take effect. To clear the required multicast forwarding entries, use the **reset multicast forwarding-table** command.

### Examples

```
# Configure multicast forwarding among sub-VLANs of the super VLAN 2.  
<Sysname> system-view  
[Sysname] interface vlan-interface 2  
[Sysname-Vlan-interface2] multicast forwarding supervlan community
```

### Related commands

**reset multicast forwarding-table**

## multicast routing

Use **multicast routing** to enable IP multicast routing and enter MRIB view.

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

### Syntax

```
multicast routing [ vpn-instance vpn-instance-name ]  
undo multicast routing [ vpn-instance vpn-instance-name ]
```

### Default

IP multicast routing is disabled.

### Views

System view

### Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command enables IP multicast routing on the public network.

## Usage guidelines

Other Layer 3 multicast commands take effect only when IP multicast routing is enabled.

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

## Examples

```
# Enable IP multicast routing and enter MRIB view on the public network.
```

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib]
```

```
# Enable IP multicast routing and enter MRIB view in the VPN instance mvpn.
```

```
<Sysname> system-view
[Sysname] multicast routing vpn-instance mvpn
[Sysname-mrib-mvpn]
```

# reset multicast forwarding event

Use **reset multicast forwarding event** to clear statistics for multicast forwarding events.

## Syntax

```
reset multicast [ vpn-instance vpn-instance-name ] forwarding event
```

## Views

User view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command clears statistics for the multicast forwarding events on the public network.

## Examples

```
# Clear statistics for the multicast forwarding events on the public network.
```

```
<Sysname> reset multicast forwarding event
```

## Related commands

```
display multicast forwarding event
```

# reset multicast forwarding-table

Use **reset multicast forwarding-table** to clear the multicast forwarding entries.

## Syntax

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

## Views

User view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears the multicast forwarding entries on the public network.

*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-length*: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

*mask*: Specifies an address mask. The default is 255.255.255.255.

**incoming-interface**: Specifies the multicast forwarding entries that contain the specified incoming interface.

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

**all**: Specifies all multicast forwarding entries.

## Usage guidelines

When a forwarding entry is deleted from the multicast forwarding table, the associated routing entry is also deleted from the multicast routing table.

## Examples

```
# On the public network, clear the multicast forwarding entries related to the multicast group 225.5.4.3 from the multicast forwarding table.
```

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

## Related commands

```
display multicast forwarding-table
```

# reset multicast routing-table

Use **reset multicast routing-table** to clear the multicast routing entries.

## Syntax

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

## Views

User view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command clears the multicast routing entries on the public network.

*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-length*: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

*mask*: Specifies an address mask. The default is 255.255.255.255.

**incoming-interface**: Specifies the routing entries that contain the specified incoming interface.

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

**all**: Specifies all multicast routing entries.

## Usage guidelines

When a routing entry is deleted from the multicast routing table, the associated forwarding entry is also deleted from the multicast forwarding table.

## Examples

```
# Clear the routing entries for the multicast group 225.5.4.3 from the multicast routing table on the public network.
```

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

## Related commands

**display multicast routing-table**

# IGMP commands

The term "interface" in this chapter collectively refers to 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

Use **display igmp group** to display IGMP information for multicast groups.

### Syntax

```
display igmp [ vpn-instance vpn-instance-name ] group [ group-address | interface interface-type interface-number ] [ static | verbose ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays IGMP information for multicast groups on the public network.

*group-address*: Specifies a multicast group by its address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, the command displays IGMP information for all multicast groups.

**interface** *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays the IGMP information for multicast groups on all interfaces.

**static**: Specifies IGMP information for the multicast groups that interfaces joined statically. If you do not specify this keyword, the command displays IGMP information for the multicast groups that interfaces joined dynamically.

**verbose**: Displays detailed information.

### Examples

```
# Display IGMP information for all multicast groups that interfaces dynamically joined on the public network.
```

```
<Sysname> display igmp group
IGMP groups in total: 3
Vlan-interface1(10.10.1.20):
IGMP groups reported in total: 3
  Group address   Last reporter   Uptime         Expires
  225.1.1.1       10.10.1.10     00:02:04      00:01:15
  225.1.1.2       10.10.1.10     00:02:04      00:01:15
  225.1.1.3       10.10.1.10     00:02:04      00:01:15
```



**Table 32 Command output**

Field	Description
IGMP groups in total	Total number of multicast groups.
IGMP groups reported in total	Total number of multicast groups that the interface joins dynamically.
Group address	Multicast group address.
Last reporter	Address of the last receiver host that reported its membership to the multicast group.
Uptime	Length of time since the multicast group was reported.
Expire	Remaining time for the multicast group. If the timer is disabled, this field displays <b>Off</b> .

# Display detailed IGMP information for the multicast group 225.1.1.1 that interfaces dynamically joined on the public network. In this example, IGMPv3 is running.

```
<Sysname> display igmp group 225.1.1.1 verbose
Vlan-interface1(10.10.1.20):
  IGMP groups reported in total: 1
  Group: 225.1.1.1
    Uptime: 00:00:34
    Expires: Off
    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
    Source list (sources in total: 1):
      Source: 10.1.1.1
        Uptime: 00:00:03
        Expires: 00:04:16
        Last-member-query-counter: 0
        Last-member-query-timer-expiry: Off
```

**Table 33 Command output**

Field	Description
IGMP groups reported in total	Total number of multicast groups that the interface joins dynamically.
Group	Multicast group address.
Uptime	Length of time since the multicast group was reported.
Expires	Remaining time for the multicast group. If the timer is disabled, this field displays <b>Off</b> .
Last reporter	Address of the last receiver host that reported its membership to this multicast group.
Last-member-query-counter	Number of group-specific queries or source-and-group-specific queries sent for the multicast group.

Field	Description
Last-member-query-timer-expiry	Remaining time for the last member query timer of the multicast group. If the timer is disabled, this field displays <b>Off</b> .
Group mode	Multicast source filtering mode: <ul style="list-style-type: none"> <li>• <b>Include.</b></li> <li>• <b>Exclude.</b></li> </ul> This field is displayed only when the switch runs IGMPv3.
Version1-host-present-timer-expiry	Remaining time for the IGMPv1 host present timer. If the timer is disabled, this field displays <b>Off</b> . This field is displayed only when the switch runs IGMPv2 or IGMPv3.
Version2-host-present-timer-expiry	Remaining time for the IGMPv2 host present timer. If the timer is disabled, this field displays <b>Off</b> . This field is displayed only when the switch runs IGMPv3.
Source list (sources in total)	List of multicast sources, and the total number of multicast sources. This field is displayed only when the switch runs IGMPv3.
Source	Multicast source address. This field is displayed only when the switch runs IGMPv3.
Uptime	Length of time since the multicast source was reported. This field is displayed only when the switch runs IGMPv3.
Expires	Remaining time for the multicast source. If the timer is disabled, this field displays <b>Off</b> . This field is displayed only when the switch runs IGMPv3.
Last-member-query-counter	Number of group-specific queries or group-and-source-specific queries sent for the multicast source and group. This field is displayed only when the switch runs IGMPv3.
Last-member-query-timer-expiry	Remaining time for the last member query timer for the multicast source and group. If the timer is disabled, this field displays <b>Off</b> . This field is displayed only when the switch runs IGMPv3.

# Display IGMP information for multicast groups that interfaces statically joined on the public network.

```
<Sysname> display igmp group static
```

```
Entries in total: 2
```

Group address	Source address	Interface	Expires
225.1.1.1	0.0.0.0	Vlan1	Never
225.2.2.2	1.1.1.1	Vlan1	Never

**Table 34 Command output**

Field	Description
Entries in total	Total number of multicast groups.
Group address	Multicast group address.

Field	Description
Source address	Multicast source address.
Interface	Interface name.
Expires	Remaining time for the multicast group. If the timer is disabled, this field displays <b>Off</b> .

## Related commands

**reset igmp group**

# display igmp interface

Use **display igmp interface** to display IGMP information for an interface.

## Syntax

**display igmp** [ **vpn-instance** *vpn-instance-name* ] **interface** [ *interface-type interface-number* ] [ **verbose** ]

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays IGMP information for an interface on the public network.

*interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays IGMP information for all IGMP-enabled interfaces.

**verbose**: Displays detailed IGMP information.

## Examples

# Display detailed IGMP information for VLAN-interface 1 on the public network.

```
<Sysname> display igmp interface vlan-interface 1 verbose
Vlan-interface1(10.10.1.20):
  IGMP is enabled.
  IGMP version: 2
  Query interval for IGMP: 125s
  Other querier present time for IGMP: 255s
  Maximum query response time for IGMP: 10s
  Last member query interval: 1s
  Last member query count: 2
  Startup query interval: 31s
  Startup query count: 2
  General query timer expiry (hh:mm:ss): 00:00:54
  Querier for IGMP: 10.10.1.20 (This router)
  IGMP activity: 1 join(s), 0 leave(s)
```

```

Multicast routing on this interface: Enabled
Robustness: 2
Require-router-alert: Disabled
Fast-leave: Disabled
SSM-mapping: Disabled
SSM-mapping: Disabled
Startup-query: Off
Other-querier-present-timer-expiry (hh:mm:ss): --:--:--
IGMP groups reported in total: 1

```

**Table 35 Command output**

Field	Description
Vlan-interface1(10.10.1.20)	Interface and its IP address.
Query interval for IGMP	IGMP general query interval, in seconds.
Other querier present time for IGMP	Other querier present interval, in seconds.
Maximum query response time for IGMP	Maximum response time for IGMP general queries, in seconds.
Last member query interval	IGMP last member query interval, in seconds.
Last member query count	Number of IGMP group-specific queries or IGMP group-and-source-specific queries sent for the multicast group.
Startup query interval	IGMP startup query interval, in seconds.
Startup query count	Number of IGMP general queries that the switch sends on startup.
General query timer expiry	Remaining time for the IGMP general query time. If the timer is disabled, this field displays <b>Off</b> .
Querier for IGMP	IP address of the IGMP querier. This field is not displayed when the switch runs IGMPv1 and the switch is not the IGMP querier. <b>NOTE:</b> In IGMPv1, the PIM DR acts as the IGMP querier. You can use the <b>display pim interface</b> command to display PIM information.
No querier elected	No IGMP querier is elected. This field is displayed only when the switch runs IGMPv1 and the switch is not the IGMP querier. <b>NOTE:</b> In IGMPv1, the PIM DR acts as the IGMP querier. You can use the <b>display pim interface</b> command to display PIM information.
IGMP activity: 1 join(s), 0 leave(s)	Statistics of IGMP activities: <ul style="list-style-type: none"> <li><b>join(s)</b>—Total number of multicast groups that this interface has joined.</li> <li><b>leave(s)</b>—Total number of multicast groups that this interface has left.</li> </ul>
Multicast routing on this interface	Whether multicast routing and forwarding is enabled.
Robustness	Robustness variable of the IGMP querier.
Require-router-alert	Whether the feature of dropping IGMP messages without Router-Alert is enabled.

Field	Description
Fast-leave	Whether the fast-leave processing feature is enabled.
SSM-mapping	Whether the IGMP SSM mapping feature is enabled.
Startup-query	Whether the IGMP querier sends IGMP general queries at the startup query interval on startup: <ul style="list-style-type: none"> <li>• <b>On</b>—The IGMP querier performs the above action.</li> <li>• <b>Off</b>—The IGMP querier does not perform the above action.</li> </ul>
Other-querier-present-timer-expiry	Remaining time for the other querier present timer. If the timer is disabled, this field displays <b>Off</b> .
IGMP groups reported in total	Total number of multicast groups that the interface has joined dynamically. This field is not displayed if the interface does not join multicast groups.

## display igmp ssm-mapping

Use **display igmp ssm-mapping** to display IGMP SSM mappings.

### Syntax

**display igmp** [ **vpn-instance** *vpn-instance-name* ] **ssm-mapping** *group-address*

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays information about the IGMP SSM mappings on the public network.

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

### Examples

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

```
<Sysname> display igmp ssm-mapping 232.1.1.1
Group: 232.1.1.1
Source list:
  1.2.3.4
  5.5.5.5
  10.1.1.1
  100.1.1.10
```

**Table 36 Command output**

Field	Description
Group	Multicast group address.
Source list	List of multicast source addresses.

## igmp

Use **igmp** to enter IGMP view.

Use **undo igmp** to remove the configurations made in IGMP view.

### Syntax

```
igmp [ vpn-instance vpn-instance-name ]  
undo igmp [ vpn-instance vpn-instance-name ]
```

### Views

System view

### Predefined user roles

network-admin

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command applies to the public network.

### Examples

```
# Enter IGMP view for the public network.  
<Sysname> system-view  
[Sysname] igmp  
[Sysname-igmp]  
  
# Enter IGMP view for VPN instance mvpn.  
<Sysname> system-view  
[Sysname] igmp vpn-instance mvpn  
[Sysname-igmp-mvpn]
```

## igmp enable

Use **igmp enable** to enable IGMP on an interface.

Use **undo igmp enable** to disable IGMP on an interface.

### Syntax

```
igmp enable  
undo igmp enable
```

### Default

IGMP is disabled on all interfaces.

## Views

Interface view

## Predefined user roles

network-admin

## Usage guidelines

This command takes effect only when IP multicast routing is enabled. If the interface belongs to a VPN instance, make sure IP multicast routing is enabled on the VPN instance.

IGMP configurations on an interface take effect only when IGMP is enabled on the interface.

## Examples

```
# Enable IP multicast routing, and enable IGMP on VLAN-interface 100 on the public network.
```

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp enable
```

## Related commands

**multicast routing**

# igmp fast-leave

Use **igmp fast-leave** to enable fast-leave processing on an interface.

Use **undo igmp fast-leave** to disable fast-leave processing on an interface.

## Syntax

```
igmp fast-leave [ group-policy acl-number ]
```

```
undo igmp fast-leave
```

## Default

Fast-leave processing is disabled. The IGMP querier sends IGMP group-specific or group-and-source-specific queries after receiving IGMP leave messages.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*acl-number*: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999. If you specify an ACL, the command takes effect only on the multicast groups that the ACL permits. The command takes effect on all multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not contain valid rules.

## Usage guidelines

This feature enables an IGMP querier to send leave notifications to the upstream routers without sending group-specific or group-and-source-specific queries after receiving leave messages.

In an IPv4 basic ACL, the **source** keyword matches the multicast group address in IGMP leave messages.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

## Examples

```
# Enable fast-leave processing on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp fast-leave
```

## igmp group-policy

Use **igmp group-policy** to configure a multicast group policy on an interface to control the multicast groups that receiver hosts attached to the interface can join.

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

## Syntax

```
igmp group-policy acl-number [ version-number ]
```

```
undo igmp group-policy
```

## Default

Multicast group policies are not configured on an interface, and receiver hosts attached to the interface can join multicast groups.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*acl-number*: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Receiver hosts can join only the multicast groups that the ACL permits. If the specified ACL does not exist or the specified ACL does not contain valid rules, receiver hosts cannot join multicast groups.

*version-number*: Specifies an IGMP version in the range of 1 to 3. By default, the configured group filter applies to IGMP reports of all versions.

## Usage guidelines

In an IPv4 basic ACL, the **source** keyword matches the multicast group address in IGMP reports. In an IPv4 advanced ACL, the **source** and **destination** keywords match the multicast source address and multicast group address in IGMP reports, respectively. The multicast source address is considered to be 0.0.0.0 for the following IGMP reports:

- IGMPv1 and IGMPv2 reports.
- IGMPv3 IS\_EX and IGMPv3 TO\_EX reports that do not carry multicast source addresses.



If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

If you configure the interface as a static member interface for a multicast group or a multicast source and group, this configuration has no effect on the multicast group or the multicast source and group.

## Examples

```
# Configure a multicast group policy on VLAN-interface 100 so that receiver hosts attached to
VLAN-interface 100 can join only the multicast group 225.1.1.1.
```

```
<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 last-member-query-count

Use **igmp last-member-query-count** to set the IGMP last member query count on an interface.

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

### Syntax

```
igmp last-member-query-count count
undo igmp last-member-query-count
```

### Default

The IGMP last member query count equals the IGMP querier's robustness variable.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

*count*: Sets an IGMP last member query count in the range of 1 to 255.

### Usage guidelines

This command and the **last-member-query-count** command have the same function but different effective ranges:

- The **last-member-query-count** command takes effect on all interfaces.
- The **igmp last-member-query-count** command takes effect on the current interface.

For an interface, the **igmp last-member-query-count** command takes priority over the **last-member-query-count** command.

## Examples

```
# Set the IGMP last member query count to 6 on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp last-member-query-count 6
```

## Related commands

**last-member-query-count** (IGMP view)

# igmp last-member-query-interval

Use **igmp last-member-query-interval** to set the IGMP last member query interval on an interface.

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

## Syntax

**igmp last-member-query-interval** *interval*

**undo igmp last-member-query-interval**

## Default

The IGMP last member query interval is 1 second.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an IGMP last member query interval in the range of 1 to 25 seconds.

## Usage guidelines

This command and the **last-member-query-interval** command in IGMP view have the same function but different effective ranges:

- The **last-member-query-interval** command in IGMP view takes effect on all interfaces.
- The **igmp last-member-query-interval** command takes effect on the current interface.

For an interface, the **igmp last-member-query-interval** command takes priority over the **last-member-query-interval** command in IGMP view.

## Examples

```
# Set the IGMP last member query interval to 6 seconds on VLAN-interface 100.
```

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

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

```
[Sysname-Vlan-interface100] igmp last-member-query-interval 6
```

## Related commands

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

# igmp max-response-time

Use **igmp max-response-time** to set the maximum response time for IGMP general queries on an interface.

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

## Syntax

**igmp max-response-time** *time*

**undo igmp max-response-time**

## Default

The maximum response time for IGMP general queries is 10 seconds.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*time*: Sets the maximum response time for IGMP general queries, in the range of 1 to 3174 seconds.

## Usage guidelines

This command and the **max-response-time** command in IGMP view have the same function but different effective ranges:

- The **max-response-time** command in IGMP view takes effect on all interfaces.
- The **igmp max-response-time** command takes effect on the current interface.

For an interface, the **igmp max-response-time** command takes priority over the **max-response-time** command in IGMP view.

## Examples

```
# Set the maximum response time for IGMP general queries to 25 seconds on VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] igmp max-response-time 25
```

## Related commands

**max-response-time** (IGMP view)

# igmp non-stop-routing

Use **igmp non-stop-routing** to enable IGMP NSR.

Use **undo igmp non-stop-routing** to disable IGMP NSR.

## Syntax

**igmp non-stop-routing**

**undo igmp non-stop-routing**

## Default

IGMP NSR is disabled.

## Views

System view

## Predefined user roles

network-admin

## Examples

```
# Enable IGMP NSR.
```

```
<Sysname> system-view
[Sysname] igmp non-stop-routing
```

## igmp other-querier-present-interval

Use **igmp other-querier-present-interval** to set the IGMP other querier present timer on an interface.

Use **undo igmp other-querier-present-interval** to restore the default.

### Syntax

```
igmp other-querier-present-interval interval
```

```
undo igmp other-querier-present-interval
```

### Default

The IGMP other querier present timer is calculated by the following formula:

$$[ \text{IGMP general query interval} ] \times [ \text{IGMP querier's robustness variable} ] + [ \text{maximum response time for IGMP general queries} ] / 2.$$

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets an IGMP other querier present timer in the range of 1 to 31744 seconds.

### Usage guidelines

This command and the **other-querier-present-interval** command have the same function but different effective ranges:

- The **other-querier-present-interval** command takes effect on all interfaces.
- The **igmp other-querier-present-interval** command takes effect on the current interface.

For an interface, the **igmp other-querier-present-interval** command takes priority over the **other-querier-present-interval** command.

### Examples

```
# Set the IGMP other querier present timer to 125 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp other-querier-present-interval 125
```

### Related commands

**other-querier-present-interval** (IGMP view)

## igmp query-interval

Use **igmp query-interval** to set the IGMP general query interval on an interface.

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

## Syntax

**igmp query-interval** *interval*

**undo igmp query-interval**

## Default

The IGMP general query interval is 125 seconds.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an IGMP general query interval in the range of 1 to 31744 seconds.

## Usage guidelines

This command and the **query-interval** command in IGMP view have the same function but different effective ranges:

- The **query-interval** command in IGMP view takes effect on all interfaces.
- The **igmp query-interval** command takes effect on the current interface.

For an interface, the **igmp query-interval** command takes priority over the **query-interval** command in IGMP view.

## Examples

```
# Set the IGMP general query interval to 60 seconds on VLAN-interface 100.
```

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

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

```
[Sysname-Vlan-interface100] igmp query-interval 60
```

## Related commands

**query-interval** (IGMP view)

# igmp robust-count

Use **igmp robust-count** to set the IGMP querier's robustness variable on an interface.

Use **undo igmp robust-count** to restore the default.

## Syntax

**igmp robust-count** *count*

**undo igmp robust-count**

## Default

The IGMP querier's robustness variable is 2.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*count*: Sets an IGMP querier's robustness variable in the range of 1 to 255.

## Usage guidelines

The IGMP querier's robustness variable defines the number of times to retransmit queries if packet loss occurs. A higher robustness variable makes the IGMP querier more robust, but it increases timeout time for multicast groups.

This command and the **robust-count** command in IGMP view have the same function but different effective ranges:

- The **robust-count** command in IGMP view takes effect on all interfaces.
- The **igmp robust-count** command takes effect on the current interface.

For an interface, the **igmp robust-count** command takes priority over the **robust-count** command in IGMP view.

## Examples

```
# Set the IGMP querier's robustness variable to 5 on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp robust-count 5
```

## Related commands

**robust-count** (IGMP view)

# igmp startup-query-count

Use **igmp startup-query-count** to set the IGMP startup query count on an interface.

Use **undo igmp startup-query-count** to restore the default.

## Syntax

**igmp startup-query-count** *count*

**undo igmp startup-query-count**

## Default

The IGMP startup query count equals the IGMP querier's robustness variable.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*count*: Sets an IGMP startup query count in the range of 1 to 255.

## Usage guidelines

This command and the **startup-query-count** command in IGMP view have the same function but different effective ranges:

- The **startup-query-count** command in IGMP view takes effect on all interfaces.
- The **igmp startup-query-count** command takes effect on the current interface.

For an interface, the **igmp startup-query-count** command takes priority over the **startup-query-count** command in IGMP view.

## Examples

```
# Set the IGMP startup query count to 5 on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp startup-query-count 5
```

## Related commands

**startup-query-count** (IGMP view)

# igmp startup-query-interval

Use **igmp startup-query-interval** to set the IGMP startup query interval on an interface.

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

## Syntax

```
igmp startup-query-interval interval
undo igmp startup-query-interval
```

## Default

The IGMP startup query interval equals one quarter of the IGMP general query interval.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an IGMP startup query interval in the range of 1 to 31744 seconds.

## Usage guidelines

This command and the **startup-query-interval** command in IGMP view have the same function but different effective ranges:

- The **startup-query-interval** command in IGMP view takes effect on all interfaces.
- The **igmp startup-query-interval** command takes effect on the current interface.

For an interface, the **igmp startup-query-interval** command takes priority over the **startup-query-interval** command in IGMP view.

## Examples

```
# Set the IGMP startup query interval to 100 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp startup-query-interval 100
```

## Related commands

**startup-query-interval** (IGMP view)

## igmp static-group

Use **igmp static-group** to configure an interface as a static group member of a multicast group.

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

### Syntax

```
igmp static-group group-address [ source source-address ]  
undo igmp static-group { all | group-address [ source source-address ] }
```

### Default

An interface is not a static group member of multicast groups.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

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

*source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, the command configures an interface as a static group member of the multicast groups with all multicast source addresses.

**all**: Specifies all multicast groups that the interface has statically joined.

### Usage guidelines

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 entries cannot be established. No such a restriction exists if the specified multicast group address is not in the SSM multicast address range.

### Examples

```
# Configure VLAN-interface 100 as a static group member of the 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 as a static group member of the 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 version

Use **igmp version** to specify an IGMP version for an interface.

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



## Syntax

**igmp version** *version-number*  
**undo igmp version**

## Default

The default IGMP version is 2.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*version-number*: Specifies an IGMP version in the range of 1 to 3.

## Examples

```
# Specify IGMP version 1 for VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] igmp version 1
```

# last-member-query-count (IGMP view)

Use **last-member-query-count** to set the global IGMP last member query count.

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

## Syntax

**last-member-query-count** *count*  
**undo last-member-query-count**

## Default

The global IGMP last member query count equals the IGMP querier's robustness variable.

## Views

IGMP view

## Predefined user roles

network-admin

## Parameters

*count*: Sets an IGMP last member query count in the range of 1 to 255.

## Usage guidelines

This command and the **igmp last-member-query-count** command have the same function but different effective ranges:

- The **last-member-query-count** command in IGMP view takes effect on all interfaces.
- The **igmp last-member-query-count** command takes effect on the current interface.

For an interface, the **igmp last-member-query-count** command takes priority over the **last-member-query-count** command in IGMP view.

## Examples

```
# Set the global IGMP last member query count to 6 on the public network.
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] last-member-query-count 6
```

## Related commands

**igmp last-member-query-count**

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

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

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

## Syntax

**last-member-query-interval** *interval*

**undo last-member-query-interval**

## Default

The global IGMP last member query interval is 1 second.

## Views

IGMP view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an IGMP last member query interval in the range of 1 to 25 seconds.

## Usage guidelines

This command and the **igmp last-member-query-interval** command have the same function but different effective ranges:

- The **last-member-query-interval** command in IGMP view takes effect on all interfaces.
- The **igmp last-member-query-interval** command takes effect on the current interface.

For an interface, the **igmp last-member-query-interval** command takes priority over the **last-member-query-interval** command in IGMP view.

## Examples

```
# Set the global IGMP last member query interval to 6 seconds on the public network.
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] last-member-query-interval 6
```

## Related commands

**igmp last-member-query-interval**

## max-response-time (IGMP view)

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

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

### Syntax

**max-response-time** *time*

**undo max-response-time**

### Default

The global maximum response time for IGMP general queries is 10 seconds.

### Views

IGMP view

### Predefined user roles

network-admin

### Parameters

*time*: Sets the maximum response time for IGMP general queries in the range of 1 to 3174 seconds.

### Usage guidelines

This command and the **igmp max-response-time** command have the same function but different effective ranges:

- The **max-response-time** command in IGMP view takes effect on all interfaces.
- The **igmp max-response-time** command takes effect on the current interface.

For an interface, the **igmp max-response-time** command takes priority over the **max-response-time** command in IGMP view.

### Examples

```
#Set the global maximum response time for IGMP general queries to 25 seconds on the public network.
```

```
<Sysname> system-view  
[Sysname] igmp  
[Sysname-igmp] max-response-time 25
```

### Related commands

**igmp max-response-time**

## other-querier-present-interval (IGMP view)

Use **other-querier-present-interval** to set the global IGMP other querier present timer.

Use **undo other-querier-present-interval** to restore the default.

### Syntax

**other-querier-present-interval** *interval*

**undo other-querier-present-interval**

### Default

The IGMP other querier present timer is calculated by the following formula:

$[ \text{IGMP general query interval} ] \times [ \text{IGMP querier's robustness variable} ] + [ \text{maximum response time for IGMP general queries} ] / 2.$

## Views

IGMP view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an IGMP other querier present timer in the range of 1 to 31744 seconds.

## Usage guidelines

This command and the **igmp other-querier-present-interval** command have the same function but different effective ranges:

- The **other-querier-present-interval** command takes effect on all interfaces.
- The **igmp other-querier-present-interval** command takes effect on the current interface.

For an interface, the **igmp other-querier-present-interval** command takes priority over the **other-querier-present-interval** command.

## Examples

```
# Set the global IGMP other querier present timer to 125 seconds on the public network.
```

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

```
[Sysname] igmp
```

```
[Sysname-igmp] other-querier-present-interval 125
```

## Related commands

**igmp other-querier-present-interval**

# query-interval (IGMP view)

Use **query-interval** to set the global IGMP general query interval.

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

## Syntax

**query-interval** *interval*

**undo query-interval**

## Default

The global IGMP general query interval is 125 seconds.

## Views

IGMP view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an IGMP general query interval in the range of 1 to 31744 seconds.

## Usage guidelines

This command and the **igmp query-interval** command have the same function but different effective ranges:

- The **query-interval** command in IGMP view takes effect on all interfaces.
- The **igmp query-interval** command takes effect on the current interface.

For an interface, the **igmp query-interval** command takes priority over the **query-interval** command in IGMP view.

## Examples

```
# Set the global IGMP general query interval to 60 seconds on the public network.
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] query-interval 60
```

## Related commands

**igmp query-interval**

## reset igmp group

Use **reset igmp group** to remove dynamic IGMP group entries.

## Syntax

```
reset igmp [ 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 } ] ] }
```

## Views

User view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command removes dynamic IGMP group entries on the public network.

**all**: Specifies all interfaces (the first **all**), or all multicast groups (the second **all**).

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

*group-address*: Specifies a multicast group by its address in the range of 224.0.0.0 to 239.255.255.255.

*source-address*: Specifies a multicast source address. If this argument is not specified, the command removes dynamic IGMP group entries of all multicast source addresses.

*mask*: Specifies an address mask. The default is 255.255.255.255.

*mask-length*: Specifies an address mask length. The default is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

## Usage guidelines

This command might interrupt the multicast information transmission.

## Examples

```
# Remove the dynamic group entries for all IGMP groups on all interfaces on the public network.
<Sysname> reset igmp group all

# Remove the dynamic group entries for all IGMP groups on VLAN-interface 100 on the public network.
<Sysname> reset igmp group interface vlan-interface 100 all

# Remove the dynamic 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
```

## Related commands

**display igmp group**

# robust-count (IGMP view)

Use **robust-count** to set the global IGMP querier's robustness variable.

Use **undo robust-count** to restore the default.

## Syntax

**robust-count** *count*

**undo robust-count**

## Default

The global IGMP querier's robustness variable is 2.

## Views

IGMP view

## Predefined user roles

network-admin

## Parameters

*count*: Sets an IGMP querier's robustness variable in the range of 1 to 255.

## Usage guidelines

The IGMP querier's robustness variable defines the number of times to retransmit queries if packet loss occurs. A higher robustness variable makes the IGMP querier more robust, but it increases the timeout time for multicast groups.

This command and the **igmp robust-count** command have the same function but different effective ranges:

- The **robust-count** command in IGMP view takes effect on all interfaces.
- The **igmp robust-count** command takes effect on the current interface.

For an interface, the **igmp robust-count** command takes priority over the **robust-count** command in IGMP view.

## Examples

```
# Set the global IGMP querier's robustness variable to 5 on the public network.
<Sysname> system-view
[Sysname] igmp
```

```
[Sysname-igmp] robust-count 5
```

## Related commands

**igmp robust-count**

# ssm-mapping (IGMP view)

Use **ssm-mapping** to configure IGMP SSM mappings.

Use **undo ssm-mapping** to remove IGMP SSM mappings.

## Syntax

```
ssm-mapping source-address acl-number
```

```
undo ssm-mapping { source-address | all }
```

## Default

IGMP SSM mappings are not configured.

## Views

IGMP view

## Predefined user roles

network-admin

## Parameters

*source-address*: Specifies a multicast source by its IP address.

*acl-number*: Specifies a basic ACL number in the range of 2000 to 2999. The specified multicast source is mapped only to multicast groups that the ACL permits. If the ACL does not exist or the ACL does not have valid rules, the specified multicast source is not mapped to multicast groups.

**all**: Removes all the IGMP SSM mappings.

## Usage guidelines

In an IPv4 basic ACL, the **source** keyword matches the multicast group address in IGMP reports.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

## Examples

# Map the multicast source **125.1.1.1** to the multicast groups in the range of **232.1.1.0/24** on the public network.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 232.1.1.1 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] igmp
[Sysname-igmp] ssm-mapping 125.1.1.1 2001
```

## Related commands

**display igmp ssm-mapping**

## startup-query-count (IGMP view)

Use **startup-query-count** to set the global IGMP startup query count.

Use **undo startup-query-count** to restore the default.

### Syntax

**startup-query-count** *count*

**undo startup-query-count**

### Default

The global IGMP startup query count equals the IGMP querier's robustness variable.

### Views

IGMP view

### Predefined user roles

network-admin

### Parameters

*count*: Sets an IGMP startup query count in the range of 1 to 255.

### Usage guidelines

This command and the **igmp startup-query count** command have the same function but different effective ranges:

- The **startup-query-count** command in IGMP view takes effect on all interfaces.
- The **igmp startup-query count** command takes effect on the current interface.

For an interface, the **igmp startup-query count** command takes priority over the **startup-query-count** command in IGMP view.

### Examples

```
# Set the global IGMP startup query count to 5 on the public network.
```

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

```
[Sysname] igmp
```

```
[Sysname-igmp] startup-query-count 5
```

### Related commands

**igmp startup-query-count**

## startup-query-interval (IGMP view)

Use **startup-query-interval** to set the global IGMP startup query interval.

Use **undo startup-query-interval** to restore the default.

### Syntax

**startup-query-interval** *interval*

**undo startup-query-interval**

### Default

The global IGMP startup query interval equals one quarter of the IGMP general query interval.



## Views

IGMP view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an IGMP startup query interval in the range of 1 to 31744 seconds.

## Usage guidelines

This command and the **igmp startup-query-interval** command have the same function but different effective ranges:

- The **startup-query-interval** command in IGMP view takes effect on all interfaces.
- The **igmp startup-query-interval** command takes effect on the current interface.

For an interface, the **igmp startup-query-interval** command takes priority over the **startup-query-interval** command in IGMP view.

## Examples

```
# Set the global IGMP startup query interval to 100 seconds on the public network.  
<Sysname> system-view  
[Sysname] igmp  
[Sysname-igmp] startup-query-interval 100
```

## Related commands

**igmp startup-query-interval**

---

# PIM commands

The term "interface" in this chapter collectively refers to 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*).

## auto-rp enable

Use **auto-rp enable** to enable Auto-RP listening.

Use **undo auto-rp enable** to disable Auto-RP listening.

### Syntax

**auto-rp enable**

**undo auto-rp enable**

### Default

Auto-RP listening is disabled.

### Views

PIM view

### Predefined user roles

network-admin

### Examples

```
# Enable Auto-RP listening on the public network.  
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] auto-rp enable
```

## bidir-pim enable (PIM view)

Use **bidir-pim enable** to enable BIDIR-PIM.

Use **undo bidir-pim enable** to disable BIDIR-PIM.

### Syntax

**bidir-pim enable**

**undo bidir-pim enable**

### Default

BIDIR-PIM is disabled.

### Views

PIM view

## Predefined user roles

network-admin

## Usage guidelines

This command takes effect only when IP multicast routing is enabled.

## Examples

```
# Enable IP multicast routing on the public network, and enable BIDIR-PIM.
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] pim
[Sysname-pim] bidir-pim enable
```

## Related commands

**multicast routing**

# bidir-rp-limit (PIM view)

Use **bidir-rp-limit** to configure the maximum number of BIDIR-PIM RPs.

Use **undo bidir-rp-limit** to restore the default.

## Syntax

**bidir-rp-limit** *limit*

**undo bidir-rp-limit**

## Default

The default setting is 6.

## Views

PIM view

## Predefined user roles

network-admin

## Parameters

*limit*: Sets the maximum number of RPs in BIDIR-PIM, in the range of 1 to 32.

## Usage guidelines

In a BIDIR-PIM domain, one DF election per RP is implemented on all PIM-enabled interfaces. To avoid unnecessary DF elections, HP recommends not configuring multiple RPs for BIDIR-PIM.

This command sets a limit on the number of BIDIR-PIM RPs. If the number of RPs exceeds the limit, excess RPs do not take effect and can be used only for DF election rather than multicast data forwarding.

## Examples

```
# Set the maximum number of BIDIR-PIM RPs to 3 on the public network.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] bidir-rp-limit 3
```

## bsm-fragment enable (PIM view)

Use **bsm-fragment enable** to enable bootstrap message (BSM) semantic fragmentation.

Use **undo bsm-fragment enable** to disable BSM semantic fragmentation.

### Syntax

**bsm-fragment enable**

**undo bsm-fragment enable**

### Default

BSM semantic fragmentation is enabled.

### Views

PIM view

### Predefined user roles

network-admin

### Usage guidelines

Disable BSM semantic fragmentation if the PIM-SM domain contains a device that does not support this feature.

### Examples

```
# Disable BSM semantic fragmentation on the public network.
```

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

```
[Sysname] pim
```

```
[Sysname-pim] undo bsm-fragment enable
```

## bsr-policy (PIM view)

Use **bsr-policy** to configure a BSR policy to define the legal bootstrap router (BSR) address range.

Use **undo bsr-policy** to remove the configuration.

### Syntax

**bsr-policy** *acl-number*

**undo bsr-policy**

### Default

BSR policies are not configured, and bootstrap messages from any multicast sources are regarded valid.

### Views

PIM view

### Predefined user roles

network-admin

### Parameters

*acl-number*: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999.

## Usage guidelines

You can use this command to guard against BSR spoofing.

In an IPv4 basic ACL, the **source** keyword matches the source address in bootstrap messages.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

## Examples

# On the public network, configure a BSR policy so that only the devices on the subnet 10.1.1.0/24 can act as 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
```

## Related commands

**c-bsr** (PIM view)

## c-bsr (PIM view)

Use **c-bsr** to configure a candidate-BSR (C-BSR).

Use **undo c-bsr** to remove a C-BSR.

## Syntax

**c-bsr** *ip-address* [ **scope** *group-address* { *mask-length* | *mask* } ] [ **hash-length** *hash-length* | **priority** *priority* ] \*

**undo c-bsr** *ip-address* [ **scope** *group-address* { *mask-length* | *mask* } ]

## Default

No C-BSR is configured.

## Views

PIM view

## Predefined user roles

network-admin

## Parameters

*ip-address*: Specifies the IP address of a C-BSR.

**scope** *group-address*: Specifies a multicast group address by its IP address in the range of 239.0.0.0 to 239.255.255.255. If you do not specify a multicast group, the command designates the C-BSR to the global-scoped zone.

*mask-length*: Specifies an address mask length in the range of 8 to 32.

*mask*: Specifies an address mask.

**hash-length** *hash-length*: Specifies a hash mask length in the range of 0 to 32. The default setting is 30.

**priority** *priority*: Sets a C-BSR priority in the range of 0 to 255. The default setting is 64. A larger value represents a higher priority.

## Usage guidelines

The IP address of a C-BSR must be the IP address of a local PIM enabled interface on the C-BSR. Otherwise, the configuration does not take effect.

If you execute this command for a zone multiple times, the most recent configuration takes effect.

You can configure the same C-BSR for different zones.

## Examples

```
# Configure the interface with the IP address of 1.1.1.1 as the C-BSR for the global-scoped zone on the public network.
```

```
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] c-bsr 1.1.1.1
```

## c-rp (PIM view)

Use **c-rp** to configure a candidate-RP (C-RP).

Use **undo c-rp** to remove the configuration of a C-RP.

## Syntax

```
c-rp ip-address [ advertisement-interval adv-interval | group-policy acl-number | holdtime hold-time | priority priority ] * [ bidir ]
```

```
undo c-rp ip-address
```

## Default

No C-RPs are configured.

## Views

PIM view

## Predefined user roles

network-admin

## Parameters

*ip-address*: Specifies the IP address of a C-RP.

**advertisement-interval** *adv-interval*: Sets a C-RP advertisement interval in the range of 1 to 65535 seconds. The default value is 60 seconds.

**group-policy** *acl-number*: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. The C-RP is designated only to IPv4 multicast groups that the ACL permits. The C-RP is designated to all IPv4 multicast groups 224.0.0.0/4 when the one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

**holdtime** *hold-time*: Sets a C-RP lifetime in the range of 1 to 65535 seconds. The default value is 150 seconds.

**priority** *priority*: Sets a C-RP priority in the range of 0 to 255. The default setting is 192. A larger value represents a lower priority.

**bidir**: Specifies BIDIR-PIM. If you do not specify this keyword, the C-RP provides services for PIM-SM.

## Usage guidelines

The IP address of a C-RP must be the IP address of a local PIM enabled interface on the C-RP. Otherwise, the configuration does not take effect.

In an IPv4 basic ACL, the **source** keyword matches the multicast group address in C-RP advertisement messages, and the other parameters are ignored. If the specified addresses are not multicast group addresses, the ACL rule is not valid. Only groups that the ACL permits are advertised.

To use a C-RP for multiple multicast group ranges, specify them by multiple **permit** statements in an ACL and reference the ACL in the **group-policy** keyword.

If you execute this command using the same C-RP IP address multiple times, the most recent configuration takes effect.

## Examples

# On the public network, configure the interface with the IP address of 1.1.1.1 as the C-RP for multicast group ranges 225.1.0.0/16 and 226.2.0.0/16, and set its priority to 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 1.1.1.1 group-policy 2000 priority 10
```

## crp-policy (PIM view)

Use **crp-policy** to configure a C-RP policy to define the legal C-RP address range and the multicast group range to which the C-RP is designated.

Use **undo crp-policy** to remove the configuration.

## Syntax

**crp-policy** *acl-number*

**undo crp-policy**

## Default

C-RP policies are not configured, and all received C-RP messages are regarded legal.

## Views

PIM view

## Predefined user roles

network-admin

## Parameters

*acl-number*: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999.

## Usage guidelines

You can use this command to guard against C-RP spoofing.

In an IPv4 advanced ACL, the **source** and **destination** keywords match the RP address and multicast group address in C-RP advertisement messages, respectively. If you do not specify the **source** keyword in rules, all C-RPs are considered to be legal. If you do not specify the **destination** keyword in any rules, the C-RPs are designated to all multicast groups.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

When the switch compares the advertisement message against the destination field in the ACL, it uses only the prefix of the multicast group range in the advertisement message. For example, the multicast group range specified in a C-RP advertisement message is 224.1.0.0/16. If the prefix 224.1.0.0 is in the multicast group range specified in the destination field of the ACL, the advertisement message passes the filtering. Otherwise, the advertisement message is discarded.

## Examples

```
# On 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 for groups in the 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
```

## Related commands

**c-rp** (PIM view)

# display interface register-tunnel

Use **display interface register-tunnel** to display register-tunnel interface information.

## Syntax

```
display interface [ register-tunnel [ interface-number ] ] [ brief [ description | down ] ]
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**register-tunnel**: Displays information about the register-tunnel interface. If you do not specify this keyword, the command displays information about all interfaces.

*interface-number*: Specifies a register-tunnel interface by its number. The switch has only one register-tunnel interface, and the value for this argument is fixed at 0. The command always displays information about Register-Tunnel 0 when you specify the **register-tunnel** keyword, regardless of whether you specify an interface number.



**brief:** Displays brief information. If you do not specify this keyword, the command displays detailed information.

**description:** Displays the full interface description. If you do not specify this keyword, the command displays only the first 27 characters of the interface description.

**down:** Displays information about the interfaces in down state and the reasons why the interfaces are down. If you do not specify this keyword, the command displays information about interfaces in all states.

## Usage guidelines

The register-tunnel interface is a virtual interface that is automatically created by the system. You cannot configure it or delete it, but you can display the interface information by using this command.

In the initial stage of multicast source registration, the register-tunnel interface is used to establish a channel between the source-side DR and the RP to transmit multicast register messages. The process of initial source registration is as follows:

1. After receiving the first multicast data from the source, the source-side DR encapsulates the multicast data into a register message. The register message is forwarded to the RP through the register-tunnel interface.
2. The register message reaches RP on the register-tunnel interface on the RP. The RP decapsulates the register message and forwards the multicast data to the receiver hosts. At the same time, the RP learns the IP address of the multicast source.
3. The RP sends a join message toward the multicast source to build an SPT.
4. After the SPT is built, the multicast data travels to the RP along the SPT rather than through the register-tunnel interface.

## Examples

```
# Display detailed information about Register-Tunnel 0.
```

```
<Sysname> display interface register-tunnel 0
Register-Tunnel0
Current state: UP
Line protocol state: DOWN
Description: Register-Tunnel0 Interface
Bandwidth: 0kbps
Maximum Transmit Unit: 1536
Internet protocol processing: disabled
Physical: Unknown
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

```
# Display brief information about Register-Tunnel 0.
```

```
<Sysname> display interface register-tunnel 0 brief
Brief information on interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Main IP      Description
REG0               UP    --      --
```

**Table 37 Command output**

<b>Field</b>	<b>Description</b>
Current state	Physical state of the register-tunnel interface. This field always displays <b>UP</b> .
Line protocol state	Link state of the register-tunnel interface. This field always displays <b>DOWN</b> .
Description	Description of the register-tunnel interface. It is not configurable.
Bandwidth	Expected bandwidth of the register-tunnel interface. It is not configurable.
Maximum Transmit Unit	MTU of the register-tunnel interface. It is not configurable.
Internet protocol processing	IP protocol processing capability. This field always displays <b>disabled</b> .
Physical	Physical type of the register-tunnel interface. This field always displays <b>Unknown</b> .
Last 300 seconds input rate	Average incoming rate in the last 300 seconds. This field always displays <b>0</b> .
Last 300 seconds output rate	Average outgoing rate in the last 300 seconds. This field always displays <b>0</b> .
Input	Number of incoming packets, incoming bytes, and discarded packets. This field always displays <b>0</b> .
Output	Number of outgoing packets, outgoing bytes, and discarded packets. This field always displays <b>0</b> .
Brief information on interface(s) under route mode	Brief information about Layer 3 interfaces.
Link: ADM - administratively down; Stby - standby	<p>Physical state of the interface:</p> <ul style="list-style-type: none"> <li>• <b>UP</b>—The interface is physically up.</li> <li>• <b>DOWN</b>—The interface is physically down.</li> <li>• <b>ADM</b>—The interface has been administratively shut down. To recover its physical state, use the <b>undo shutdown</b> command.</li> <li>• <b>Stby</b>—The interface is a backup interface. To display information about the primary interface, use the <b>display interface-backup</b> command.</li> </ul>
Protocol: (s) - spoofing	<p>If the Protocol field contains "(s)", it means one of the following conditions:</p> <ul style="list-style-type: none"> <li>• The data link protocol state of the interface is up, but no link is present on the interface.</li> <li>• The link is created on demand.</li> </ul> <p>Typically, null interfaces or loopback interfaces have this attribute.</p>
Protocol	Protocol connection state of the interface. This field always displays double hyphens (-).
Main IP	IP address of the interface. This field always displays double hyphens (-).
Cause	Causes why the physical state of the interface is down. This field always displays <b>Not connected</b> .

# display pim bsr-info

Use **display pim bsr-info** to display BSR information in the PIM-SM domain.

## Syntax

```
display pim [ vpn-instance vpn-instance-name ] bsr-info
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays BSR information on the public network.

## Examples

```
# Display BSR information in the PIM-SM domain on the public network.
```

```
<Sysname> display pim bsr-info
Scope: non-scoped
  State: Accept Preferred
  Bootstrap timer: 00:01:44
  Elected BSR address: 12.12.12.1
    Priority: 64
    Hash mask length: 30
    Uptime: 00:21:56

Scope: 239.4.0.0/16
  State: Accept Any
  Scope-zone expiry timer: 00:21:12

Scope: 239.1.0.0/16
  State: Elected
  Bootstrap timer: 00:00:26
  Elected BSR address: 17.1.11.1
    Priority: 64
    Hash mask length: 30
    Uptime: 02:53:37
  Candidate BSR address: 17.1.11.1
    Priority: 64
    Hash mask length: 30

Scope: 239.2.2.0/24
  State: Candidate
  Bootstrap timer: 00:01:56
  Elected BSR address: 61.2.37.1
```

```

    Priority: 64
    Hash mask length: 30
    Uptime: 02:53:32
    Candidate BSR address: 17.1.12.1
    Priority: 64
    Hash mask length: 30

Scope: 239.3.3.0/24
    State: Pending
    Bootstrap timer: 00:00:07
    Candidate BSR address: 17.1.13.1
    Priority: 64
    Hash mask length: 30

```

**Table 38 Command output**

Field	Description
Scope-zone expiry timer	Scoped zone aging timer.
Elected BSR address	Address of the elected BSR.
Candidate BSR address	Address of the candidate BSR.
Priority	BSR priority.
Uptime	Length of time the BSR has been up.

## display pim claimed-route

Use **display pim claimed-route** to display information about all routes that PIM uses.

### Syntax

```
display pim [ vpn-instance vpn-instance-name ] claimed-route [ source-address ]
```

### Views

Any view

### Predefined user roles

```
network-admin
network-operator
```

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays information about all routes that PIM uses on the public network.

*source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, the command displays information about all routes that PIM uses.

### Examples

# Display information about all routes that PIM uses on the public network.

```
<Sysname> display pim claimed-route
RPF-route selecting rule: longest-match
```

```

Route/mask: 7.11.0.0/16 (unicast (direct))
  RPF interface: Vlan-interface2, RPF neighbor: 8.0.0.2
  Total number of (S,G) or (*,G) dependent on this route entry: 4
  (7.11.0.10, 225.1.1.1)
  (7.11.0.10, 226.1.1.1)
  (7.11.0.10, 227.1.1.1)
  (*, 228.1.1.1)
Route/mask: 7.12.0.0/16 (multicast static)
  RPF interface: Vlan-interface2, RPF neighbor: 8.0.0.3,
  Config NextHop: 8.0.0.5
  Total number of (S,G) or (*,G) dependent on this route entry: 2
  (7.12.0.10, 226.1.1.1)
  (7.12.0.10, 225.1.1.1)

```

**Table 39 Command output**

Field	Description
Route/mask	Route entry. Route types in parentheses include: <ul style="list-style-type: none"> <li>• <b>igp</b>—IGP unicast route.</li> <li>• <b>egp</b>—EGP unicast route.</li> <li>• <b>unicast (direct)</b>—Direct unicast route.</li> <li>• <b>unicast</b>—Other unicast route, such as static unicast route.</li> <li>• <b>multicast static</b>—Static multicast route.</li> </ul>
RPF interface	Name of the RPF interface.
RPF neighbor	IP address of the RPF neighbor.
Config NextHop	Address of the configured next hop. This field is displayed only when the static multicast route is configured with a next hop.
Total number of (S,G) or (*,G) dependent on this route entry	Total number of (S, G) or (*, G) entries dependent on the RPF route and their details.

## display pim c-rp

Use **display pim c-rp** to display C-RP information in the PIM-SM domain.

### Syntax

```
display pim [ vpn-instance vpn-instance-name ] c-rp [ local ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays information about learned C-RPs on the public network.

**local**: Specifies local C-RPs. If you do not specify this keyword, the command displays information about all C-RPs.

## Usage guidelines

You can view information about learned C-RPs only on the BSR. On other devices, you can view information about the locally configured C-RPs.

## Examples

# Display information about learnt C-RPs on the public network.

```
<Sysname> display pim c-rp
Scope: non-scoped
  Group/MaskLen: 224.0.0.0/4
    C-RP address          Priority  HoldTime  Uptime    Expires
    1.1.1.1 (local)      192     150      03:01:36  00:02:29
    2.2.2.2              192     150      1d:13h    00:02:02
  Group/MaskLen: 226.1.1.0/24 [B] Expires: 00:00:33
  Group/MaskLen: 225.1.0.0/16 [B]
    C-RP Address         Priority  HoldTime  Uptime    Expires
    3.3.3.3              192     150      12w:5d    00:02:05
```

# Display information about the locally configured C-RPs.

```
<Sysname> display pim c-rp local
Candidate RP: 12.12.12.9(Loop1)
  Priority: 192
  HoldTime: 150
  Advertisement interval: 60
  Next advertisement scheduled at: 00:00:48
```

**Table 40 Command output**

Field	Description
Group/MaskLen	Multicast group to which the C-RP is designated.
[B]	The C-RP provides services for BIDIR-PIM. If this field is not displayed, the C-RP provides services for PIM-SM.
C-RP address	IP address of the C-RP. If the C-RP resides on the device where the command is executed, this field displays <b>(local)</b> after the address.
HoldTime	C-RP lifetime.
Uptime	Length of time the C-RP has been up: <ul style="list-style-type: none"><li>• <b>w</b>—Weeks.</li><li>• <b>d</b>—Days.</li><li>• <b>h</b>—Hours.</li></ul>
Expires	Remaining lifetime for the C-RP and the multicast group.
Candidate RP	IP address of the locally configured C-RP.

Field	Description
Advertisement interval	Interval between two advertisement messages sent by the locally configured C-RP.
Next advertisement scheduled at	Remaining time for the locally configured C-RP to send the next advertisement message.

## display pim df-info

Use **display pim df-info** to display the DF information of BIDIR-PIM.

### Syntax

**display pim** [ **vpn-instance** *vpn-instance-name* ] **df-info** [ *rp-address* ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays the DF information of BIDIR-PIM on the public network.

*rp-address*: Specifies the RP address of BIDIR-PIM.

### Examples

# Display the DF information of BIDIR-PIM on the public network.

```
<Sysname> display pim df-info
RP address: 1.1.0.3
  Interface      State  DF-Pref  DF-Metric  DF-Uptime  DF-Address
  Vlan1          Lose   0         0          00:20:13   8.13.0.3
  Vlan2          Win    10        1          00:20:12   7.11.0.1 (local)
```

**Table 41 Command output**

Field	Description
State	DF election state: <ul style="list-style-type: none"> <li>• <b>Win</b>—The interface wins the DF election.</li> <li>• <b>Lose</b>—The interface loses the DF election.</li> <li>• <b>Offer</b>—The interface is in the initial state of the DF election.</li> <li>• <b>Backoff</b>—The interface is acting as the DF, but there are more appropriate devices running for the DF.</li> <li>• <b>--</b>—The interface does not participate in the DF election.</li> </ul>
DF-Pref	Advertised route preference for DF election.
DF-Metric	Advertised route metric for DF election.
DF-Uptime	Length of time the DF has been up.

Field	Description
DF-Address	IP address of DF. If the DF resides on the device where the command is executed, this field displays <b>(local)</b> after the address.

## display pim interface

Use **display pim interface** to display PIM information on an interface.

### Syntax

**display pim** [ **vpn-instance** *vpn-instance-name* ] **interface** [ *interface-type interface-number* ] [ **verbose** ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays PIM information on the public network.

*interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays PIM information on all interfaces.

**verbose**: Displays detailed PIM information. If you do not specify this keyword, the command displays brief PIM information.

### Examples

# Display brief PIM information on all interfaces on the public network.

```
<Sysname> display pim interface
  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 42 Command output**

Field	Description
NbrCnt	Number of PIM neighbors.
HelloInt	Interval for sending hello messages.
DR-Pri	DR priority.
DR-Address	IP address of the DR. If the DR resides on the device where the command is executed, this field displays <b>(local)</b> after the address.

# Display detailed PIM information on VLAN-interface 1 on the public network.

```
<Sysname> display pim interface vlan-interface 1 verbose
  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
PIM BFD: disabled
PIM passive: 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 43 Command output**

Field	Description
PIM mode	PIM mode: <ul style="list-style-type: none"> <li>• <b>Dense.</b></li> <li>• <b>Sparse.</b></li> </ul>
PIM DR	IP address of the DR.
PIM DR Priority (configured)	Configured DR priority.
PIM neighbor count	Total number of PIM neighbors.
PIM hello interval	Interval between two hello messages.
PIM LAN delay (negotiated)	Negotiated PIM message propagation delay.
PIM LAN delay (configured)	Configured PIM message propagation delay.
PIM override interval (negotiated)	Negotiated interval for overriding prune messages.
PIM override interval (configured)	Configured interval for overriding prune messages.
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status: enabled or disabled.
PIM neighbor tracking (configured)	Configured neighbor tracking status: enabled or disabled.
PIM require generation ID	Whether the feature of discarding hello messages without Generation_ID is enabled.
PIM hello hold interval	PIM neighbor lifetime.

Field	Description
PIM assert hold interval	Assert holdtime timer.
PIM triggered hello delay	Maximum delay for sending hello messages.
PIM J/P interval	Interval between two join/prune messages.
PIM J/P hold interval	Joined/pruned state holdtime timer.
PIM BSR domain border	Whether a PIM domain border is configured.
PIM BFD	Whether PIM is enabled to work with BFD.
PIM passive	Whether PIM passive mode is enabled.
Number of routers on network not using DR priority	Number of routers that do not use the DR priority field on the subnet where the interface resides.
Number of routers on network not using LAN delay	Number of routers that do not use the LAN delay field on the subnet where the interface resides.
Number of routers on network not using neighbor tracking	Number of routers that are not enabled with neighbor tracking on the subnet where the interface resides.

## display pim neighbor

Use **display pim neighbor** to display PIM neighbor information.

### Syntax

```
display pim [ vpn-instance vpn-instance-name ] neighbor [ neighbor-address | interface interface-type interface-number | verbose ] *
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays PIM neighbor information on the public network.

*neighbor-address*: Specifies a PIM neighbor by its IP address. If you do not specify a PIM neighbor, the command displays information about all PIM neighbors.

**interface** *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays PIM neighbor information on all interfaces.

**verbose**: Displays detailed PIM neighbor information. If you do not specify this keyword, the command displays brief PIM neighbor information.

### Examples

# Display brief information about all PIM neighbors on the public network.

```
<Sysname> display pim neighbor
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
```

# Display detailed information about the PIM neighbor with the IP address 11.110.0.20 on the public network.

```
<Sysname> display pim neighbor 11.110.0.20 verbose
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: Enabled
```

**Table 44 Command output**

Field	Description
Neighbor	IP address of the PIM neighbor.
Interface	Interface that connects to the PIM neighbor.
Uptime	Length of time the PIM neighbor has been up.
Expires/Expiry time	Remaining lifetime for the PIM neighbor. If the PIM neighbor is always up and reachable, this field displays <b>never</b> .
DR-Priority/DR Priority	Priority of the PIM neighbor.
Mode	PIM mode. If the PIM mode is BIDIR-PIM, this field displays <b>B</b> . If a PIM mode other than BIDIR-PIM is used, this field is blank.
Generation ID	Generation ID of the PIM neighbor. (A random value represents a status change of the PIM neighbor.)
Holdtime	Lifetime of the PIM neighbor. If the PIM neighbor is always up and reachable, this field displays <b>forever</b> .
LAN delay	PIM message propagation delay.
Override interval	Interval for overriding prune messages.
State refresh interval	Interval for refreshing state. This field is displayed only when the PIM neighbor operates in PIM-DM mode and the state refresh capability is enabled.
Neighbor tracking	Neighbor tracking status: enabled or disabled.
Bidirectional PIM	Whether BIDIR-PIM is enabled.

# display pim routing-table

Use **display pim routing-table** to display PIM routing entries.

## Syntax

```
display pim [ vpn-instance vpn-instance-name ] routing-table [ group-address [ mask { mask-length | mask } ] | source-address [ mask { mask-length | mask } ] | flags flag-value | fsm | incoming-interface interface-type interface-number | mode mode-type | outgoing-interface { exclude | include | match } interface-type interface-number ] *
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays PIM routing entries on the public network.

*group-address*: Specifies a multicast group by its IP address in the range of 224.0.0.0 to 239.255.255.255. If you do not specify a multicast group, the command displays PIM routing entries for all multicast groups.

*source-address*: Specifies a multicast source by its IP address.

*mask-length*: Specifies an address mask length in the range of 0 to 32. The default value is 32.

*mask*: Specifies an address mask. The default value is 255.255.255.255.

**flags** *flag-value*: Specifies a flag. If you do not specify a flag, the command displays PIM routing entries that contain all flags. The following lists the values for the *flag-value* argument and their meanings:

- **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.
- **del**: Specifies PIM routing entries 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 reside on the same subnet as the multicast source.
- **msdp**: Specifies PIM routing entries learned from MSDP SA messages.
- **niif**: Specifies PIM routing entries that contain unknown incoming interfaces.
- **nonbr**: Specifies PIM routing entries with PIM neighbor lookup failure.
- **rpt**: Specifies PIM routing entries on the RPT branches where (S, G) prunes have been sent to the RP.
- **spt**: Specifies PIM routing entries on the SPT.
- **swt**: Specifies PIM routing entries in the process of RPT-to-SPT switchover.

- **wc**: Specifies PIM routing entries with wildcards.

**fsm**: Displays detailed information about the finite state machine.

**incoming-interface** *interface-type interface-number*: Specifies an incoming interface. If you do not specify an incoming interface, the command displays PIM routing entries that contain all incoming interfaces.

**mode** *mode-type*: Specifies a PIM mode. If you do not specify a PIM mode, the command displays PIM routing entries in all PIM modes. The available PIM modes include:

- **bidir**: Specifies BIDIR-PIM.
- **dm**: Specifies PIM-DM.
- **sm**: Specifies PIM-SM.
- **ssm**: Specifies PIM-SSM.

**outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*: Specifies an outgoing interface. If you do not specify an outgoing interface, the command displays PIM routing entries that contain all outgoing interfaces. Whether an outgoing interface is contained in the PIM routing entries depends on the following conditions:

- If you specify an excluded interface, the command displays PIM routing entries that do not contain the specified outgoing interface.
- If you specify an included interface, the command displays PIM routing entries that contain the specified outgoing interface.
- If you specify a matching interface, the command displays PIM routing entries that contain only the specified outgoing interface.

## Examples

# Display PIM routing entries on the public network.

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

**Table 45 Command output**

Field	Description
Total 0 (*, G) entry; 1 (S, G) entry	Total number of (*, G) entries, and the total number of (S, G) entries.
(172.168.0.12, 227.0.0.1)	(S, G) entry.
Protocol	PIM mode.

Field	Description
Flag	<p>Flag of the (S, G) entry or (*, G) entry:</p> <ul style="list-style-type: none"> <li>• <b>ACT</b>—The entry has been used for routing data.</li> <li>• <b>DEL</b>—The entry will be removed.</li> <li>• <b>EXPRUNE</b>—Some outgoing interfaces are pruned by other multicast routing protocols.</li> <li>• <b>EXT</b>—The entry contains outgoing interfaces provided by other multicast routing protocols.</li> <li>• <b>LOC</b>—The entry is on a router directly connected to the same subnet with the multicast source.</li> <li>• <b>NIIF</b>—The entry contains unknown incoming interfaces.</li> <li>• <b>NONBR</b>—The entry has a PIM neighbor lookup failure.</li> <li>• <b>RPT</b>—The entry is on an RPT branch where (S, G) prunes have been sent to the RP.</li> <li>• <b>SPT</b>—The entry is on the SPT.</li> <li>• <b>SWT</b>—The entry is in the process of RPT-to-SPT switchover.</li> <li>• <b>WC</b>—The entry contains a wildcard.</li> </ul>
Uptime	Length of time since the (S, G) entry or (*, G) entry was installed.
Upstream interface	Upstream (incoming) interface of the (S, G) entry or (*, G) entry.
Upstream neighbor	Upstream neighbor of the (S, G) entry or (*, G) entry.
RPF prime neighbor	<p>RPF neighbor of the (S, G) or (*, G) entry:</p> <ul style="list-style-type: none"> <li>• For a (*, G) entry, if the RPF neighbor is the RP, the field displays <b>NULL</b>.</li> <li>• For an (S, G) entry, if the RPF neighbor is a router that directly connects to the multicast source, this field displays <b>NULL</b>.</li> </ul>
Downstream interface(s) information	<p>Information about the downstream interfaces:</p> <ul style="list-style-type: none"> <li>• Total number of downstream interfaces.</li> <li>• Names of the downstream interfaces.</li> <li>• Protocol type on the downstream interfaces.</li> <li>• Uptime of the downstream interfaces.</li> <li>• Expiration time of the downstream interfaces.</li> </ul>

## display pim rp-info

Use **display pim rp-info** to display RP information in the PIM-SM domain.

### Syntax

```
display pim [ vpn-instance vpn-instance-name ] rp-info [ group-address ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays RP information on the public network.

*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 a multicast group, the command displays RP information for all multicast groups.

## Examples

# Display RP information for the multicast group 224.0.1.1 on the public network.

```
<Sysname> display pim rp-info 224.0.1.1
```

```
Auto RP address is: 1.1.1.1
```

```
  HoldTime: 181
```

```
  Uptime: 00:20:19
```

```
  Expires: 00:02:42
```

```
BSR RP address is: 2.2.2.2
```

```
  Priority: 192
```

```
  HoldTime: 150
```

```
  Uptime: 03:01:10
```

```
  Expires: 00:02:30
```

```
Static RP address is: 3.3.3.5
```

```
  Preferred: Yes
```

```
  Configured ACL: 2003
```

```
RP mapping for this group is: 3.3.3.5
```

# Display RP information for all multicast groups on the public network.

```
<Sysname> display pim rp-info
```

```
Auto RP information:
```

```
  RP agent address: 4.4.4.4
```

```
  Group/MaskLen: 224.0.0.0/4
```

RP address	HoldTime	Uptime	Expires
1.1.1.1	181	00:20:19	00:02:42

```
  Group/MaskLen: 225.1.0.0/16 [B]
```

RP address	HoldTime	Uptime	Expires
1.1.1.2	181	00:20:19	00:02:42

```
BSR RP information:
```

```
Scope: non-scoped
```

```
Group/MaskLen: 224.0.0.0/4
```

RP address	Priority	HoldTime	Uptime	Expires
1.1.1.1 (local)	192	150	03:01:36	00:02:29
2.2.2.2	192	150	1d:13h	00:02:02

```
Group/MaskLen: 225.1.0.0/16 [B]
```

RP address	Priority	HoldTime	Uptime	Expires
3.3.3.3	192	150	12w:5d	00:02:05

Static RP information:

RP address	ACL	Mode	Preferred
3.3.3.1	2000	pim-sm	No
3.3.3.2	2001	bidir	Yes
3.3.3.3	2002	pim-sm	No
3.3.3.4		pim-sm	No
3.3.3.5	2002	pim-sm	Yes

**Table 46 Command output**

Field	Description
Auto RP address is	IP address of the Auto-RP.
RP agent address	IP address of the Auto-RP agent.
Group/MaskLen	Multicast group to which the RP is designated.
[B]	The RP provides services for multicast groups in the BIDIR-PIM domain. If this field is not displayed, the RP provides services for groups in the PIM-SM domain.
RP address	IP address of the RP. If the RP resides on the device where the command is executed, this field displays <b>(local)</b> after the address.
Priority	Priority of the RP.
HoldTime	RP lifetime.
Uptime	Length of time the RP has been up.
Expires	Remaining lifetime for the RP.
Preferred	Whether the static RP is preferred.
Configured ACL/ACL	ACL defining the multicast groups to which the static RP is designated.
Mode	RP service mode: PIM-SM or BIDIR-PIM.
RP mapping for this group	IP address of the RP that provides services for the multicast group.

## display pim statistics

Use **display pim statistics** to display statistics for PIM packets.

### Syntax

**display pim statistics**

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Examples

```
# Display statistics for PIM packets.  
<Sysname> display pim statistics  
Received PIM packets: 3295  
Sent PIM packets      : 5975
```



	Valid	Invalid	Succeeded	Failed
Hello	: 3128	0	4333	0
Reg	: 14	0	0	0
Reg-stop	: 0	0	0	0
JP	: 151	0	561	0
BSM	: 0	0	1081	0
Assert	: 0	0	0	0
Graft	: 0	0	0	0
Graft-ACK	: 0	0	0	0
C-RP	: 0	0	0	0
SRM	: 0	0	0	0
DF	: 0	0	0	0

**Table 47 Command output**

Field	Description
Received PIM packets	Total number of received PIM packets.
Sent PIM packets	Total number of sent PIM packets.
Valid	Number of received valid PIM packets.
Invalid	Number of received invalid PIM packets.
Succeeded	Number of valid PIM packets that were sent successfully.
Failed	Number of valid PIM packets that failed to be sent.
Hello	Hello message statistics.
Reg	Register message statistics.
Reg-stop	Register-stop message statistics.
JP	Join/prune message statistics.
BSM	BSM statistics.
Assert	Assert message statistics.
Graft	Graft message statistics.
Graft-ACK	Graft-ACK message statistics.
C-RP	C-RP message statistics.
SRM	State refresh message statistics.
DF	Designated forwarder message statistics.

## hello-option dr-priority (PIM view)

Use **hello-option dr-priority** to set the global DR priority.

Use **undo hello-option dr-priority** to restore the default.

### Syntax

**hello-option dr-priority** *priority*

**undo hello-option dr-priority**

## Default

The global DR priority is 1.

## Views

PIM view

## Predefined user roles

network-admin

## Parameters

*priority*: Sets a DR priority in the range of 0 to 4294967295. A larger value represents a higher priority.

## Usage guidelines

You can set the DR priority for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

## Examples

```
# Set the global DR priority to 3 on the public network.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option dr-priority 3
```

## Related commands

**pim hello-option dr-priority**

# hello-option holdtime (PIM view)

Use **hello-option holdtime** to set the global PIM neighbor lifetime.

Use **undo hello-option holdtime** to restore the default.

## Syntax

**hello-option holdtime** *time*

**undo hello-option holdtime**

## Default

The global PIM neighbor lifetime is 105 seconds.

## Views

PIM view

## Predefined user roles

network-admin

## Parameters

*time*: Sets a PIM neighbor lifetime in the range of 1 to 65535 seconds. If you set the value to 65535 seconds, PIM neighbors are always reachable.

## Usage guidelines

You can set the PIM neighbor lifetime for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

## Examples

```
# Set the global PIM neighbor lifetime to 120 seconds on the public network.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option holdtime 120
```

## Related commands

**pim hello-option holdtime**

# hello-option lan-delay (PIM view)

Use **hello-option lan-delay** to set the global PIM message propagation delay on a shared-media LAN.

Use **undo hello-option lan-delay** to restore the default.

## Syntax

**hello-option lan-delay** *delay*

**undo hello-option lan-delay**

## Default

The global PIM message propagation delay on a shared-media LAN is 500 milliseconds.

## Views

PIM view

## Predefined user roles

network-admin

## Parameters

*delay*: Sets a PIM message propagation delay on a shared-media LAN in the range of 1 to 32767 milliseconds.

## Usage guidelines

You can set the global PIM message propagation delay on a shared-media LAN for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

## Examples

```
# Set the global PIM message propagation delay on a shared-media LAN to 200 milliseconds on the
public network.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option lan-delay 200
```

## Related commands

- **hello-option override-interval** (PIM view)
- **pim hello-option lan-delay**
- **pim hello-option override-interval**

## hello-option neighbor-tracking (PIM view)

Use **hello-option neighbor-tracking** to enable neighbor tracking and disable join message suppression globally.

Use **undo hello-option neighbor-tracking** to restore the default.

### Syntax

**hello-option neighbor-tracking**

**undo hello-option neighbor-tracking**

### Default

Neighbor tracking is disabled, and join message suppression is enabled.

### Views

PIM view

### Predefined user roles

network-admin

### Usage guidelines

You can enable neighbor tracking for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

### Examples

```
# Enable neighbor tracking globally on the public network.
```

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

```
[Sysname] pim
```

```
[Sysname-pim] hello-option neighbor-tracking
```

### Related commands

**pim hello-option neighbor-tracking**

## hello-option override-interval (PIM view)

Use **hello-option override-interval** to set the global override interval.

Use **undo hello-option override-interval** to restore the default.

### Syntax

**hello-option override-interval** *interval*

**undo hello-option override-interval**

### Default

The global override interval is 2500 milliseconds.

### Views

PIM view

### Predefined user roles

network-admin

## Parameters

*interval*: Sets an override interval in the range of 1 to 65535 milliseconds.

## Usage guidelines

You can set the override interval for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

## Examples

```
# Set the global override interval to 2000 milliseconds on the public network.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option override-interval 2000
```

## Related commands

- **hello-option lan-delay** (PIM view)
- **pim hello-option lan-delay**
- **pim hello-option override-interval**

# holdtime join-prune (PIM view)

Use **holdtime join-prune** to set the global joined/pruned state holdtime timer.

Use **undo holdtime join-prune** to restore the default.

## Syntax

```
holdtime join-prune time
undo holdtime join-prune
```

## Default

The global joined/pruned state holdtime timer is 210 seconds.

## Views

PIM view

## Predefined user roles

network-admin

## Parameters

*time*: Sets a joined/pruned state holdtime timer in the range of 1 to 65535 seconds.

## Usage guidelines

You can set the joined/pruned state holdtime timer for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

To prevent the upstream neighbors from aging out, you must configure the interval for sending join/prune messages to be less than the joined/pruned state holdtime timer.

## Examples

```
# Set the global joined/pruned state holdtime timer to 280 seconds on the public network.
<Sysname> system-view
[Sysname] pim
```

```
[Sysname-pim] holdtime join-prune 280
```

## Related commands

- **pim holdtime join-prune**
- **timer join-prune** (PIM view)

## jp-pkt-size (PIM view)

Use **jp-pkt-size** to set the maximum size of each join/prune message.

Use **undo jp-pkt-size** to restore the default.

### Syntax

```
jp-pkt-size size
```

```
undo jp-pkt-size
```

### Default

The maximum size of a join/prune message is 8100 bytes.

### Views

PIM view

### Predefined user roles

network-admin

### Parameters

*size*: Sets the maximum size of each join/prune message, in the range of 100 to 8100 bytes.

### Examples

```
# Set the maximum size of each join/prune message to 1500 bytes on the public network.  
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] jp-pkt-size 1500
```

## pim

Use **pim** to enter PIM view.

Use **undo pim** to remove all configurations in PIM view.

### Syntax

```
pim [ vpn-instance vpn-instance-name ]
```

```
undo pim [ vpn-instance vpn-instance-name ]
```

### Views

System view

### Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, you enter public network PIM view.

## Examples

# Enable IP multicast routing on the public network and enter public network PIM view.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] pim
[Sysname-pim]
```

# Enable IP multicast routing in VPN instance **mvpn** and enter PIM view of VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] multicast routing vpn-instance mvpn
[Sysname-mrib-mvpn] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn]
```

## Related commands

**multicast routing-enable**

# pim bfd enable

Use **pim bfd enable** to enable BFD for PIM.

Use **undo pim bfd enable** to disable BFD for PIM.

## Syntax

**pim bfd enable**

**undo pim bfd enable**

## Default

BFD is disabled for PIM.

## Views

Interface view

## Predefined user roles

network-admin

## Usage guidelines

This command takes effect only when PIM-DM or PIM-SM is enabled on an interface.

## Examples

# On the public network, enable IP multicast routing, enable PIM-DM on VLAN-interface 100, and enable BFD for PIM on the interface.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim dm
```

```
[Sysname-Vlan-interface100] pim bfd enable
```

### Related commands

- **pim dm**
- **pim sm**

## pim bsr-boundary

Use **pim bsr-boundary** to configure a PIM-SM domain border, namely, a bootstrap message boundary.

Use **undo pim bsr-boundary** to remove the configured PIM-SM domain border.

### Syntax

```
pim bsr-boundary
```

```
undo pim bsr-boundary
```

### Default

No PIM-SM domain border is configured.

### Views

Interface view

### Predefined user roles

network-admin

### Examples

```
# Configure VLAN-interface 100 as a PIM-SM domain border.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] pim bsr-boundary
```

### Related commands

- **c-bsr** (PIM view)
- **multicast boundary**

## pim dm

Use **pim dm** to enable PIM-DM.

Use **undo pim dm** to disable PIM-DM.

### Syntax

```
pim dm
```

```
undo pim dm
```

### Default

PIM-DM is disabled.

### Views

Interface view



## Predefined user roles

network-admin

## Usage guidelines

This command takes effect only when IP multicast routing is enabled. If the interface belongs to a VPN instance, make sure IP multicast routing is enabled on the VPN instance.

## Examples

```
# On the public network, enable IP multicast routing, and enable PIM-DM on VLAN-interface 100.
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim dm
```

## Related commands

**multicast routing**

# pim hello-option dr-priority

Use **pim hello-option dr-priority** to set the DR priority on an interface.

Use **undo pim hello-option dr-priority** to restore the default.

## Syntax

**pim hello-option dr-priority** *priority*

**undo pim hello-option dr-priority**

## Default

The DR priority is 1.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*priority*: Sets a DR priority in the range of 0 to 4294967295. A larger value represents a higher priority.

## Usage guidelines

You can set the DR priority for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

## Examples

```
# Set the DR priority to 3 on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option dr-priority 3
```

## Related commands

**hello-option dr-priority** (PIM view)

## pim hello-option holdtime

Use **pim hello-option holdtime** to set the PIM neighbor lifetime on an interface.

Use **undo pim hello-option holdtime** to restore the default.

### Syntax

**pim hello-option holdtime** *time*

**undo pim hello-option holdtime**

### Default

The PIM neighbor lifetime is 105 seconds.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

*time*: Sets a PIM neighbor lifetime in the range of 1 to 65535 seconds. If you set the value to 65535 seconds, the PIM neighbor is always reachable.

### Usage guidelines

You can set the PIM neighbor lifetime for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

### Examples

```
# Sets the PIM neighbor lifetime to 120 seconds on VLAN-interface 100.
```

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

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

```
[Sysname-Vlan-interface100] pim hello-option holdtime 120
```

### Related commands

**hello-option holdtime** (PIM view)

## pim hello-option lan-delay

Use **pim hello-option lan-delay** to set the PIM message propagation delay on a shared-media LAN for an interface.

Use **undo pim hello-option lan-delay** to restore the default.

### Syntax

**pim hello-option lan-delay** *delay*

**undo pim hello-option lan-delay**

### Default

The PIM message propagation delay is 500 milliseconds.

### Views

Interface view

## Predefined user roles

network-admin

## Parameters

*delay*: Sets a PIM message propagation delay on a shared-media LAN in the range of 1 to 32767 milliseconds.

## Usage guidelines

You can set the PIM message propagation delay on a shared-media LAN for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

## Examples

```
# Set the PIM message propagation delay on a shared-media LAN to 200 milliseconds on
VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option lan-delay 200
```

## Related commands

- **hello-option lan-delay** (PIM view)
- **hello-option override-interval** (PIM view)
- **pim hello-option override-interval**

# pim hello-option neighbor-tracking

Use **pim hello-option neighbor-tracking** to enable neighbor tracking and disable join message suppression on an interface.

Use **pim hello-option neighbor-tracking disable** to disable neighbor tracking on an interface when neighbor tracking is enabled globally.

Use **undo pim hello-option neighbor-tracking** to restore neighbor tracking on an interface to be consistent with the global setting.

## Syntax

```
pim hello-option neighbor-tracking
pim hello-option neighbor-tracking disable
undo pim hello-option neighbor-tracking
```

## Default

Neighbor tracking is disabled and join message suppression is enabled.

## Views

Interface view

## Predefined user roles

network-admin

## Usage guidelines

You can enable neighbor tracking for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

## Examples

```
# Enable neighbor tracking on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option neighbor-tracking
```

```
# On the public network, disable neighbor tracking on VLAN-interface 100 when neighbor tracking is enabled globally.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option neighbor-tracking
[Sysname-pim] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option neighbor-tracking disable
```

## Related commands

**hello-option neighbor-tracking** (PIM view)

# pim hello-option override-interval

Use **pim hello-option override-interval** to set the override interval on an interface.

Use **undo pim hello-option override-interval** to restore the default.

## Syntax

```
pim hello-option override-interval interval
```

```
undo pim hello-option override-interval
```

## Default

The override interval is 2500 milliseconds.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an override interval in the range of 1 to 65535 milliseconds.

## Usage guidelines

You can set the override interval for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

## Examples

```
# Set the 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
```

### Related commands

- **hello-option lan-delay** (PIM view)
- **hello-option override-interval** (PIM view)
- **pim hello-option lan-delay**

## pim holdtime join-prune

Use **pim holdtime join-prune** to set the joined/pruned state holdtime timer on an interface.

Use **undo pim holdtime join-prune** to restore the default.

### Syntax

```
pim holdtime join-prune time
```

```
undo pim holdtime join-prune
```

### Default

The joined/pruned state holdtime timer is 210 seconds.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

*time*: Sets a joined/pruned state holdtime timer in the range of 1 to 65535 seconds.

### Usage guidelines

You can set the joined/pruned state holdtime timer for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

To prevent the upstream neighbors from aging out, you must configure the interval for sending join/prune messages to be less than the joined/pruned state holdtime timer.

### Examples

```
# Set the joined/pruned state holdtime timer to 280 seconds on VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] pim holdtime join-prune 280
```

### Related commands

- **holdtime join-prune** (PIM view)
- **pim timer join-prune**

## pim neighbor-policy

Use **pim neighbor-policy** to configure a PIM hello policy to define the legal source address range for hello messages.

Use **undo pim neighbor-policy** to restore the default.

### Syntax

```
pim neighbor-policy acl-number  
undo pim neighbor-policy
```

### Default

PIM hello policies are not configured, and all received hello messages are considered legal.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

*acl-number*: Specifies an IPv4 basic ACL number in the range of 2000 to 2999.

### Usage guidelines

You can use this command to guard against hello message spoofing.

In an IPv4 basic ACL, the **source** keyword matches the source address in hello messages.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

### Examples

# Configure a PIM hello policy 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 passive

Use **pim passive** to enable PIM passive mode on an interface.

Use **undo pim passive** to restore the default.

### Syntax

```
pim passive  
undo pim passive
```

### Default

The PIM passive mode is disabled for an interface.

### Views

Interface view

## Predefined user roles

network-admin

## Usage guidelines

This command takes effect only when PIM-DM or PIM-SM is enabled on the interface.

## Examples

# On the public network, enable IP multicast routing. Then, enable PIM-DM and PIM passive mode on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim dm
[Sysname-Vlan-interface100] pim passive
```

# pim require-genid

Use **pim require-genid** to enable dropping hello messages without the generation ID options.

Use **undo pim require-genid** to restore the default.

## Syntax

**pim require-genid**

**undo pim require-genid**

## Default

Hello messages without the generation ID options are accepted.

## Views

Interface view

## Predefined user roles

network-admin

## Examples

# Enable VLAN-interface 100 to drop hello messages without the generation ID options.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim require-genid
```

# pim sm

Use **pim sm** to enable PIM-SM.

Use **undo pim sm** to disable PIM-SM.

## Syntax

**pim sm**

**undo pim sm**

## Default

PIM-SM is disabled.

## Views

Interface view

## Predefined user roles

network-admin

## Usage guidelines

This command takes effect only when IP multicast routing is enabled. If the interface belongs to a VPN instance, make sure IP multicast routing is enabled on the VPN instance.

## Examples

# On the public network, enable IP multicast routing, and enable PIM-SM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim sm
```

## Related commands

**multicast routing**

# pim state-refresh-capable

Use **pim state-refresh-capable** to enable the state refresh feature on an interface.

Use **undo pim state-refresh-capable** to disable the state refresh feature.

## Syntax

**pim state-refresh-capable**

**undo pim state-refresh-capable**

## Default

The state refresh feature is enabled.

## Views

Interface view

## Predefined user roles

network-admin

## Examples

# Disable state refresh on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo pim state-refresh-capable
```

## Related commands

- **state-refresh-interval** (PIM view)
- **state-refresh-rate-limit** (PIM view)



- **state-refresh-ttl** (PIM view)

## pim timer graft-retry

Use **pim timer graft-retry** to set a graft retry timer.

Use **undo pim timer graft-retry** to restore the default.

### Syntax

**pim timer graft-retry** *interval*

**undo pim timer graft-retry**

### Default

The graft retry timer is 3 seconds.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets a graft retry timer in the range of 1 to 65535 seconds.

### Examples

```
# Set the graft retry timer 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

Use **pim timer hello** to set the hello interval on an interface.

Use **undo pim timer hello** to restore the default.

### Syntax

**pim timer hello** *interval*

**undo pim timer hello**

### Default

The hello interval on an interface is 30 seconds.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets a hello interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send hello messages.

## Usage guidelines

You can set the hello interval for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

## 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
```

## Related commands

**timer hello** (PIM view)

# pim timer join-prune

Use **pim timer join-prune** to set join/prune interval on an interface.

Use **undo pim timer join-prune** to restore the default.

## Syntax

```
pim timer join-prune interval
undo pim timer join-prune
```

## Default

The join/prune interval on an interface is 60 seconds.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets a join/prune interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send join or prune messages.

## Usage guidelines

You can set the join/prune interval for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

The configuration takes effect after the current interval ends.

To prevent the upstream neighbors from aging out, you must configure the join/prune interval to be less than the joined/pruned state holdtime timer.

## 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
```

## Related commands

- **pim holdtime join-prune**

- **timer join-prune** (PIM view)

## pim triggered-hello-delay

Use **pim triggered-hello-delay** to set the triggered hello delay.

Use **undo pim triggered-hello-delay** to restore the default.

### Syntax

**pim triggered-hello-delay** *delay*

**undo pim triggered-hello-delay**

### Default

The triggered hello delay is 5 seconds.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

*delay*: Sets a triggered hello delay in the range of 1 to 60 seconds.

### Usage guidelines

The triggered hello delay defines the maximum delay for sending a hello message.

### Examples

```
# Set the triggered hello delay to 3 seconds on VLAN-interface 100.
```

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

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

```
[Sysname-Vlan-interface100] pim triggered-hello-delay 3
```

## register-policy (PIM view)

Use **register-policy** to configure a PIM register policy.

Use **undo register-policy** to remove the configured PIM register policy.

### Syntax

**register-policy** *acl-number*

**undo register-policy**

### Default

PIM register policies are not configured.

### Views

PIM view

### Predefined user roles

network-admin

## Parameters

*acl-number*: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999.

## Usage guidelines

In an IPv4 advanced ACL, the **source** and **destination** keywords match the multicast source address and multicast group address in register messages, respectively.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

## Examples

# On the public network, configure a PIM register policy to accept only register messages from sources on the subnet of 10.10.0.0/16 for 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
```

## register-whole-checksum (PIM view)

Use **register-whole-checksum** to configure the switch to calculate the checksum based on an entire register message.

Use **undo register-whole-checksum** to restore the default.

## Syntax

**register-whole-checksum**

**undo register-whole-checksum**

## Default

The switch calculates the checksum based on the register message header.

## Views

PIM view

## Predefined user roles

network-admin

## Examples

# Configure the switch to calculate the checksum based on an entire register message on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-whole-checksum
```

## source-lifetime (PIM view)

Use **source-lifetime** to set the multicast source lifetime.

Use **undo source-lifetime** to restore the default.

### Syntax

**source-lifetime** *time*  
**undo source-lifetime**

### Default

The multicast source lifetime is 210 seconds.

### Views

PIM view

### Predefined user roles

network-admin

### Parameters

*time*: Sets a multicast source lifetime in the range of 0 to 31536000 seconds. If you set the value to 0 seconds, multicast sources are never aged out.

### Examples

```
# Set the multicast source lifetime to 200 seconds on the public network.  
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] source-lifetime 200
```

## source-policy (PIM view)

Use **source-policy** to configure a multicast source policy.

Use **undo source-policy** to remove the configured multicast source policy.

### Syntax

**source-policy** *acl-number*  
**undo source-policy**

### Default

Multicast source policies are not configured.

### Views

PIM view

### Predefined user roles

network-admin

### Parameters

*acl-number*: Specifies an IPv4 basic or advanced ACL number in the range of 2000 to 3999.

### Usage guidelines

In an IPv4 basic ACL, the **source** keyword matches the source address in multicast data packets. In an IPv4 advanced ACL, the **source** and **destination** keywords match the source address and multicast group address in multicast data packets, respectively.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

If you execute this command multiple times, the most recent configuration takes effect.

## Examples

# On the public network, configure a multicast source policy to accept multicast data from the source 10.10.1.2 and to discard multicast data from the source 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
```

## spt-switch-threshold (PIM view)

Use **spt-switch-threshold** to configure the switchover to SPT.

Use **undo spt-switch-threshold** to restore the default.

### Syntax

```
spt-switch-threshold { immediacy | infinity } [ group-policy acl-number ]
undo spt-switch-threshold [ immediacy | infinity ] [ group-policy acl-number ]
```

### Default

The switch immediately triggers the switchover to SPT after receiving the first multicast packet.

### Views

PIM view

### Predefined user roles

network-admin

### Parameters

**immediacy**: Triggers the switchover to SPT immediately.

**infinity**: Disables the switchover to SPT.

**group-policy** *acl-number*: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. If you specify an ACL, the configuration applies to only the multicast groups that the ACL permits. The configuration applies to all multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

### Usage guidelines

---

#### CAUTION:

If the switch is an RP, disabling the switchover to SPT might cause multicast traffic forwarding failures on the source-side DR. When disabling the switchover to SPT, be sure you fully understand its impact on your network.

---

In an IPv4 basic ACL, the **source** keyword matches multicast group address in multicast packets.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

## Examples

```
# Disable the switchover to SPT on a receiver-side DR on the public network.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] spt-switch-threshold infinity
```

## ssm-policy (PIM view)

Use **ssm-policy** to configure the SSM group range.

Use **undo ssm-policy** to restore the default.

## Syntax

```
ssm-policy acl-number
undo ssm-policy
```

## Default

The SSM group range is 232.0.0.0/8.

## Views

PIM view

## Predefined user roles

network-admin

## Parameters

*acl-number*: Specifies an IPv4 basic ACL number in the range of 2000 to 2999.

## Usage guidelines

In an IPv4 basic ACL, the **source** keyword matches the multicast group address in IGMP reports.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

You can use this command to define a multicast group address range. If a packet to a multicast group is permitted by the used ACL, the multicast mode for the packet is PIM-SSM. Otherwise, the multicast mode is PIM-SM.

## Examples

```
# Configure the SSM group range to be 232.1.0.0/16.
<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
```

## state-refresh-interval (PIM view)

Use **state-refresh-interval** to set the state refresh interval.

Use **undo state-refresh-interval** to restore the default.

### Syntax

**state-refresh-interval** *interval*

**undo state-refresh-interval**

### Default

The state refresh interval is 60 seconds.

### Views

PIM view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets a state refresh interval in the range of 1 to 255 seconds.

### Examples

```
# Set the state refresh interval to 70 seconds on the public network.
```

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

```
[Sysname] pim
```

```
[Sysname-pim] state-refresh-interval 70
```

### Related commands

- **pim state-refresh-capable**
- **state-refresh-rate-limit** (PIM view)
- **state-refresh-ttl** (PIM view)

## state-refresh-rate-limit (PIM view)

Use **state-refresh-rate-limit** to configure the amount of time that the switch waits before receiving a new state refresh message.

Use **undo state-refresh-rate-limit** to restore the default.

### Syntax

**state-refresh-rate-limit** *time*

**undo state-refresh-rate-limit**

### Default

The switch waits 30 seconds before it receives a new state refresh message.

### Views

PIM view



## Predefined user roles

network-admin

## Parameters

*time*: Sets an amount of time that the switch waits before receiving a new refresh message, in the range of 1 to 65535 seconds.

## Examples

# Configure the switch to wait 45 seconds before it receives a new state refresh message on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-rate-limit 45
```

## Related commands

- **pim state-refresh-capable**
- **state-refresh-interval** (PIM view)
- **state-refresh-ttl** (PIM view)

# state-refresh-ttl (PIM view)

Use **state-refresh-ttl** to set the TTL value for state refresh messages.

Use **undo state-refresh-ttl** to restore the default.

## Syntax

**state-refresh-ttl** *ttl-value*

**undo state-refresh-ttl**

## Default

The TTL value of state refresh messages is 255.

## Views

PIM view

## Predefined user roles

network-admin

## Parameters

*ttl-value*: Sets a TTL value for state refresh messages, in the range of 1 to 255.

## Examples

# Set the TTL value for state refresh messages to be 45 on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-ttl 45
```

## Related commands

- **pim state-refresh-capable** (PIM view)
- **state-refresh-interval** (PIM view)
- **state-refresh-rate-limit** (PIM view)

## static-rp (PIM view)

Use **static-rp** to configure a static RP.

Use **undo static-rp** to remove a static RP.

### Syntax

```
static-rp rp-address [ acl-number | bidir | preferred ] *
```

```
undo static-rp rp-address
```

### Default

Static RPs are not configured.

### Views

PIM view

### Predefined user roles

network-admin

### Parameters

**rp-address**: Specifies the IP address of the static RP. This address must be a real, valid unicast IP address, rather than an address on the 127.0.0.0/8 subnet. For a static RP serving BIDIR-PIM, you can specify a virtual IP address.

**acl-number**: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. The static RP is designated only to IPv4 multicast groups that the ACL permits. The static RP is designated to all multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not contain valid rules.

**bidir**: Specifies BIDIR-PIM to which the static RP is designated. If you do not specify this keyword, the PIM mode is PIM-SM.

**preferred**: Gives priority to the static RP if the static RP and the dynamic RP exist at the same time in the network. The dynamic RP takes effect only if no static RP exists in the network. If you do not specify this keyword, the dynamic RP has priority. The static RP takes effect only if no dynamic RP exists in the network or when the dynamic RP fails.

### Usage guidelines

You do not need to enable PIM on an interface that acts as a static RP.

In an IPv4 basic ACL, the **source** keyword matches the multicast group address in multicast packets.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

When the ACL rules used by a static RP change, new RPs must be elected for all multicast groups.

You can configure multiple static RPs by using this command multiple times. However, if you specify the same static RP address or reference the same ACL in the command, the most recent configuration takes effect. If you configure multiple static RPs for the same multicast group, the static RP with the highest IP address is used.

## Examples

# On the public network, configure the interface with the IP address of 11.110.0.6 as a static RP for multicast group range 225.1.1.0/24, and give priority to this static RP.

```
<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
```

## Related commands

**display pim rp-info**

## timer hello (PIM view)

Use **timer hello** to set the global hello interval.

Use **undo timer hello** to restore the default.

## Syntax

**timer hello** *interval*

**undo timer hello**

## Default

The global hello interval is 30 seconds.

## Views

PIM view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets a hello interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the switch does not send hello messages.

## Usage guidelines

You can set the hello interval for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

## Examples

# Set the global hello interval to 40 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer hello 40
```

## Related commands

**pim timer hello**

## timer join-prune (PIM view)

Use **timer join-prune** to set the global join/prune interval.

Use **undo timer join-prune** to restore the default.

### Syntax

```
timer join-prune interval
```

```
undo timer join-prune
```

### Default

The global join/prune interval is 60 seconds.

### Views

PIM view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets a join/prune interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the switch does not send join or prune messages.

### Usage guidelines

You can set the join/prune interval for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

The configuration takes effect after the current interval ends.

To prevent the upstream neighbors from expiring, you must configure the interval for sending join/prune messages to be less than the joined/pruned state holdtime timer.

### Examples

```
# Set the global join/prune interval to 80 seconds on the public network.
```

```
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] timer join-prune 80
```

### Related commands

- **holdtime join-prune** (PIM view)
- **pim timer join-prune**

---

# MSDP commands

## cache-sa-enable

Use **cache-sa-enable** to enable the SA message cache mechanism to cache the (S, G) entries contained in SA messages.

Use **undo cache-sa-enable** to disable the SA message cache mechanism.

### Syntax

**cache-sa-enable**

**undo cache-sa-enable**

### Default

The SA message cache mechanism is enabled. The device caches the (S, G) entries contained in received SA messages.

### Views

MSDP view

### Predefined user roles

network-admin

### Examples

# Enable the SA message cache mechanism on the public network, so that the device caches the (S, G) entries contained in the received SA messages.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] cache-sa-enable
```

### Related commands

- **display msdp sa-cache**
- **display msdp sa-count**

## display msdp brief

Use **display msdp brief** to display brief information about MSDP peers.

### Syntax

**display msdp** [ **vpn-instance** *vpn-instance-name* ] **brief** [ **state** { **connect** | **disabled** | **established** | **listen** | **shutdown** } ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays brief information about MSDP peers on the public network.

**state**: Specifies a state. If you do not specify this keyword, the command displays brief information about MSDP peers in all states.

**connect**: Specifies the connecting state.

**disabled**: Specifies the connection failure state.

**established**: Specifies the session state.

**listen**: Specifies the listening state.

**shutdown**: Specifies the shutdown state.

## Examples

# Display brief information about MSDP peers in all states on the public network.

```
<Sysname> display msdp brief
```

Configured	Established	Listen	Connect	Shutdown	Disabled
1	1	0	0	0	0

Peer address	State	Up/Down time	AS	SA count	Reset count
20.20.20.20	Established	00:00:13	100	0	0

**Table 48 Command output**

Field	Description
Configured	Number of MSDP peers that have been configured.
Established	Number of MSDP peers in established 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.
Disabled	Number of MSDP peers in disabled state.
Peer address	MSDP peer address.
State	MSDP peer status: <ul style="list-style-type: none"><li>• <b>Established</b>—A session has been established and the MSDP peer is in session.</li><li>• <b>Listen</b>—A session has been established and the local device acts as the server in listening state.</li><li>• <b>Connect</b>—A session is not established and the local device acts as a client in connecting state.</li><li>• <b>Shutdown</b>—The session has been torn down.</li><li>• <b>Down</b>—The connection failed.</li></ul>
Up/Down time	Length of time since the MSDP peering connection was established or torn down.

Field	Description
AS	Number of the AS where the MSDP peer is located. If the system could not obtain the AS number, this field displays a question mark (?).
SA count	Number of (S, G) entries.
Reset count	MSDP peering connection reset times.

## display msdp peer-status

Use **display msdp peer-status** to display detailed status of MSDP peers.

### Syntax

**display msdp** [ **vpn-instance** *vpn-instance-name* ] **peer-status** [ *peer-address* ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays detailed status of the MSDP peers on the public network.

*peer-address*: Specifies an MSDP peer by its address. If you do not specify an MSDP peer, the command displays the detailed status of all MSDP peers.

### Examples

# Display the detailed status of the MSDP peer 20.20.20.20 on the public network.

```
<Sysname> display msdp peer-status 20.20.20.20
```

```
MSDP peer 20.20.20.20; AS 100
```

```
Description:
```

```
Information about connection status:
```

```
State: Disabled
```

```
Up/down time: 14:41:08
```

```
Resets: 0
```

```
Connection interface: LoopBack0 (20.20.20.30)
```

```
Received/sent messages: 867/867
```

```
Discarded input messages: 0
```

```
Discarded output messages: 0
```

```
Elapsed time since last connection or counters clear: 14:42:40
```

```
Mesh group peer joined: momo
```

```
Last disconnect reason: Hold timer expired with truncated message
```

```
Truncated packet: 5 bytes in buffer, type: 1, length: 20, without packet time: 75s
```

```
Information about (Source, Group)-based SA filtering policy:
```

```
Import policy: None
```

```
Export policy: None
```

Information about SA-Requests:

```

Policy to accept SA-Requests: 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: 4294967295
Input queue size: 0, Output queue size: 0
Counters for MSDP messages:
RPF check failure: 0
Incoming/outgoing SA: 0/0
Incoming/outgoing SA-Request: 0/0
Incoming/outgoing SA-Response: 0/0
Incoming/outgoing Keepalive: 867/867
Incoming/outgoing Notification: 0/0
Incoming/outgoing Traceroutes in progress: 0/0
Incoming/outgoing Traceroute reply: 0/0
Incoming/outgoing Unknown: 0/0
Incoming/outgoing data packet: 0/0

```

**Table 49 Command output**

Field	Description
MSDP peer	MSDP peer address.
AS	Number of the AS where the MSDP peer is located. If the system could not obtain the AS number, this field displays a question mark (?).
State	<p>MSDP peer status:</p> <ul style="list-style-type: none"> <li>• <b>Established</b>—A session has been established and the MSDP peer is in session.</li> <li>• <b>Listen</b>—A session has been established and the local device acts as the server in listening state.</li> <li>• <b>Connect</b>—A session is not established and the local device acts as a client in connecting state.</li> <li>• <b>Shutdown</b>—The session has been torn down.</li> <li>• <b>Disabled</b>—The connection failed.</li> </ul>
Up/Down time	Length of time since the MSDP peering connection was established or torn down.
Resets	MSDP peering connection reset times.
Connection interface	Interface and IP address used for setting up a TCP connection with the remote MSDP peer.
Received/sent messages	Number of SA messages sent and received through this connection.
Discarded input messages	Number of discarded incoming messages.
Discarded output messages	Number of discarded outgoing messages.
Elapsed time since last connection or counters clear	Elapsed time since the MSDP peer information was last cleared.
Mesh group peer joined	Mesh group that the MSDP peer has joined. This field is not displayed if the MSDP peer does not join a mesh group.



Field	Description
Last disconnect reason	<p>Reason why last MSDP peering connection was torn down. If the connection is not terminated, this field is not displayed.</p> <ul style="list-style-type: none"> <li>• <b>Hold timer expired without message</b>—Hold timer expires and the receiving cache has no messages.</li> <li>• <b>Hold timer expired with truncated message</b>—Hold timer expires and messages in the receiving cache are not intact. <ul style="list-style-type: none"> <li>○ <b>bytes in buffer</b>—Size of data in the receiving cache when the connection was terminated.</li> <li>○ <b>type</b>—Type of packets in the receiving cache when the connection was terminated.</li> <li>○ <b>length</b>—Length of packets in the receiving cache when the connection was terminated. If the packet is too small in size, this field cannot be resolved and is not displayed.</li> <li>○ <b>without packet time</b>—Length of time since packets were last processed.</li> </ul> </li> <li>• <b>Remote peer has been closed</b>—The MSDP peering connection has been torn down.</li> <li>• <b>TCP ERROR/HUP event received</b>—Error/hup event received by the TCP socket when the MSDP peer sent messages.</li> <li>• <b>Illegal message received</b>—The MSDP peer received illegal messages.</li> <li>• <b>Notification received</b>—The MSDP peer received notification messages.</li> <li>• <b>Reset command executed</b>—The user executed the <b>reset msdp peer</b> command.</li> <li>• <b>Shutdown command executed</b>—The user executed the <b>shutdown</b> command.</li> <li>• <b>Interface downed</b>—The MSDP peer received the interface down event when connecting to the remote MSDP peer.</li> </ul>
Information about (Source, Group)-based SA filtering policy	<p>SA message filtering list information:</p> <ul style="list-style-type: none"> <li>• <b>Import policy</b>—Filter list for receiving SA messages from the specified MSDP peer.</li> <li>• <b>Export policy</b>—Filter list for forwarding SA messages from the specified MSDP peer.</li> </ul>
Information about SA-Requests	<p>SA request information:</p> <ul style="list-style-type: none"> <li>• <b>Policy to accept SA request messages</b>—Filtering rule for receiving or forwarding SA request messages from the specified MSDP peer. If SA request messages are not filtered, this field displays <b>None</b>.</li> <li>• <b>Sending SA requests status</b>—Whether the MSDP peer is enabled to send an SA request message to the designated MSDP peer after receiving a new join message.</li> </ul>
Minimum TTL to forward SA with encapsulated data	Minimum TTL value for the multicast packets encapsulated in SA messages.
SAs learned from this peer	Number of cached (S, G) entries learned from the specified MSDP peer.
SA-cache maximum for the peer	Maximum number of (S, G) entries learned from the specified MSDP peer that the device can cache.
Input queue size	Data size cached in the input queue.

Field	Description
Output queue size	Data size cached in the output queue.
Counters for MSDP message	<p>MSDP peer statistics:</p> <ul style="list-style-type: none"> <li>• <b>RPF check failure</b>—Number of SA messages discarded because of RPF check failure.</li> <li>• <b>Incoming/outgoing SA</b>—Number of received and sent SA messages.</li> <li>• <b>Incoming/outgoing SA-Request</b>—Number of received and sent SA requests.</li> <li>• <b>Incoming/outgoing SA-Response</b>—Number of received and sent SA responses.</li> <li>• <b>Incoming/outgoing Keepalive</b>—Number of received and sent keepalive messages.</li> <li>• <b>Incoming/outgoing Notification</b>—Number of received and sent notification messages.</li> <li>• <b>Incoming/outgoing Traceroutes in progress</b>—Number of received and sent traceroute-in-progress messages.</li> <li>• <b>Incoming/outgoing Traceroute reply</b>—Number of received and sent traceroute replies.</li> <li>• <b>Incoming/outgoing Unknown</b>—Number of received and sent unknown messages.</li> <li>• <b>Incoming/outgoing data packet</b>—Number of received and sent SA messages encapsulated with multicast data.</li> </ul>

## display msdp sa-cache

Use **display msdp sa-cache** to display (S, G) entries in the SA cache.

### Syntax

```
display msdp [ vpn-instance vpn-instance-name ] sa-cache [ group-address | source-address | as-number ] *
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays (S, G) entries in the SA cache on the public network.

*group-address*: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, the command displays (S, G) entries for all multicast groups.

*source-address*: Specifies a multicast source address. If you do not specify a multicast source, the command displays (S, G) entries for all sources.

*as-number*: Specifies an AS number in the range of 1 to 4294967295. If you do not specify an AS number, the command displays (S, G) entries for all ASs.

## Usage guidelines

You must execute the **cache-sa-enable** command before you execute this command. Otherwise, this command does not give any output.

## Examples

# Display information about the (S, G) entries in the SA cache on the public network.

```
<Sysname> display msdp sa-cache
Total Source-Active Cache - 5 entries
Matched 5 entries
```

Source	Group	Origin RP	Pro	AS	Uptime	Expires
10.10.1.2	225.0.0.1	10.10.10.10	BGP	100	00:00:11	00:05:49
10.10.1.2	225.0.0.2	10.10.10.10	BGP	100	00:00:11	00:05:49
10.10.1.2	225.0.0.3	10.10.10.10	BGP	100	00:00:11	00:05:49
10.10.1.2	225.0.0.4	10.10.10.10	BGP	100	00:00:11	00:05:49
10.10.1.2	225.0.0.5	10.10.10.10	BGP	100	00:00:11	00:05:49

**Table 50 Command output**

Field	Description
Total Source-Active Cache	Total number of multicast sources in the SA cache.
Matched	Total number of (S, G) entries that match a multicast source.
Source	Multicast source address.
Group	Multicast group address.
Origin RP	Address of the RP that generated the (S, G) entry.
Pro	Type of protocol from which the AS number of the origin RP originates. If the system could not obtain the AS number, this field displays a question mark (?).
AS	AS number of the origin RP. If the system could not obtain the AS number, this field displays a question mark (?).
Uptime	Length of time for which the cached (S, G) entry has existed.
Expires	Length of time in which the cached (S, G) entry will expire.

## Related commands

**cache-sa-enable**

## display msdp sa-count

Use **display msdp sa-count** to display the number of (S, G) entries in the SA cache.

## Syntax

**display msdp** [ **vpn-instance** *vpn-instance-name* ] **sa-count** [ *as-number* ]

## Views

Any view

## Predefined user roles

network-admin  
network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays the number of (S, G) entries in the SA cache on the public network.

*as-number*: Specifies an AS number in the range of 1 to 4294967295. If you do not specify an AS number, the command displays the number of (S, G) entries in the SA cache of all ASs.

## Usage guidelines

You must execute the **cache-sa-enable** command before you execute this command. Otherwise, this command does not give any output.

## Examples

# Display the number of (S, G) entries in the SA cache on the public network.

```
<Sysname> display msdp sa-count
(S, G) entries statistics, counted by peer
  Peer address      SA count
  10.10.10.10      5

(S, G) entries statistics, counted by AS
  AS      Source count      Group count
  ?       3                  3

5 (S, G) entries in total
```

**Table 51 Command output**

Field	Description
(S, G) entries statistics, counted by peer	Number of (S, G) entries on an MSDP peer basis.
Peer address	Address of the MSDP peer that sent SA messages.
SA count	Number of (S, G) entries from this MSDP peer.
(S, G) entries statistics, counted by AS	Number of cached (S, G) entries on an AS basis.
AS	AS number. If the system could not obtain the AS number, this field displays a question mark (?).
Source count	Number of multicast sources from this AS.
Group count	Number of multicast groups from this AS.
(S, G) entries in total	Total number of (S, G) entries.

## Related commands

**cache-sa-enable**

## encap-data-enable

Use **encap-data-enable** to enable multicast data encapsulation in SA messages.

Use **undo encap-data-enable** to restore the default.

### Syntax

**encap-data-enable**

**undo encap-data-enable**

### Default

An SA message contains only (S, G) entries. No multicast data is encapsulated in an SA message.

### Views

MSDP view

### Predefined user roles

network-admin

### Examples

# Enable multicast data encapsulation in SA messages on the public network.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] encap-data-enable
```

## import-source

Use **import-source** to configure an SA message creation policy.

Use **undo import-source** to remove the configured SA message creation policy.

### Syntax

**import-source** [ **acl** *acl-number* ]

**undo import-source**

### Default

When an SA message is created, all the (S, G) entries within the domain are advertised in the SA message.

### Views

MSDP view

### Predefined user roles

network-admin

### Parameters

*acl-number*: Specifies an IPv4 basic or advanced ACL number in the range of 2000 to 3999. If you specify an ACL, the command advertises only the (S, G) entries that the ACL permits. The command does not advertise any (S, G) entries when any of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

### Usage guidelines

During ACL matching, the protocol ID in the ACL rule is not verified.

In an IPv4 basic ACL, the **source** keyword matches against multicast group addresses in register messages. In an IPv4 advanced ACL, the **source** keyword and the **destination** keyword match against the multicast source addresses and multicast group addresses in register messages, respectively.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

This command controls the creation of SA messages. You can also use the **peer sa-policy** command to configure a filtering rule to control forwarding and acceptance of SA messages.

## Examples

# On the public network, configure an SA creation policy to advertise only the (10.10.0.0/16, 225.1.0.0/16) entries when an SA message is created.

```
<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
```

## Related commands

**peer sa-policy**

## msdp

Use **msdp** to enable MSDP and enter MSDP view.

Use **undo msdp** to disable MSDP and remove the configurations in MSDP view to release the resources occupied by MSDP.

## Syntax

```
msdp [ vpn-instance vpn-instance-name ]
undo msdp [ vpn-instance vpn-instance-name ]
```

## Default

MSDP is disabled.

## Views

System view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command applies to the public network.

## Usage guidelines

This command takes effect only when IP multicast routing is enabled.

## Examples

```
# Enable IP multicast routing on the public network, and enable MSDP on the public network and enter public network MSDP view.
```

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] msdp
[Sysname-msdp]
```

## Related commands

**multicast routing**

# originating-rp

Use **originating-rp** to configure an interface address as the RP address of SA messages.

Use **undo originating-rp** to remove the configuration.

## Syntax

**originating-rp** *interface-type interface-number*

**undo originating-rp**

## Default

The PIM RP address is used as the RP address of SA messages.

## Views

MSDP view

## Predefined user roles

network-admin

## Parameters

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

## Examples

```
# On the 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
```

# peer connect-interface

Use **peer connect-interface** to create an MSDP peering connection.

Use **undo peer connect-interface** to remove an MSDP peering connection.

## Syntax

**peer** *peer-address* **connect-interface** *interface-type interface-number*

**undo peer** *peer-address*

## Default

MSDP peering connection is not created.

## Views

MSDP view

## Predefined user roles

network-admin

## Parameters

*peer-address*: Specifies an MSDP peer by its IP address.

*interface-type interface-number*: Specifies an interface by its type and number. The local device uses the primary IP address of the specified interface as the source IP address when setting up a TCP connection with the remote MSDP peer.

## Usage guidelines

You must execute this command before you use any other **peer** command. Otherwise, the system notifies you that the MSDP peer does not exist.

## Examples

# On the public network, configure the router with the IP address 125.10.7.6 as the MSDP peer of the local router, and configure 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
```

# peer description

Use **peer description** to configure the description for an MSDP peer.

Use **undo peer description** to delete the description for an MSDP peer.

## Syntax

**peer** *peer-address* **description** *text*

**undo peer** *peer-address* **description**

## Default

No description is configured for an MSDP peer.

## Views

MSDP view

## Predefined user roles

network-admin

## Parameters

*peer-address*: Specifies an MSDP peer by its IP address.

*text*: Specifies a description, a case-sensitive string of 1 to 80 characters, including spaces.

## Examples

# On the public network, configure the description for the device at 125.10.7.6 as **CustomerA**.



```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 description CustomerA
```

## peer mesh-group

Use **peer mesh-group** to configure an MSDP peer as a mesh group member.

Use **undo peer mesh-group** to remove an MSDP peer from the mesh group.

### Syntax

```
peer peer-address mesh-group name
```

```
undo peer peer-address mesh-group
```

### Default

An MSDP peer does not belong to any mesh group.

### Views

MSDP view

### Predefined user roles

network-admin

### Parameters

*peer-address*: Specifies an MSDP peer by its IP address.

*name*: Specifies a mesh group, a case-sensitive string of 1 to 32 characters. A mesh group name must not contain any spaces.

### Examples

# On the public network, configure the MSDP peer 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
```

## peer minimum-ttl

Use **peer minimum-ttl** to configure the lower TTL threshold for multicast data packets encapsulated in SA messages.

Use **undo peer minimum-ttl** to restore the default.

### Syntax

```
peer peer-address minimum-ttl tth-value
```

```
undo peer peer-address minimum-ttl
```

### Default

The lower TTL threshold for a multicast packet to be encapsulated in an SA message is 0.

### Views

MSDP view

## Predefined user roles

network-admin

## Parameters

*peer-address*: Specifies an MSDP peer by its IP address.

*ttl-value*: Specifies the lower TTL threshold in the range of 0 to 255.

## Examples

# On the public network, set the lower TTL threshold for multicast packets to be encapsulated in SA messages to 10. 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
```

# peer password

Use **peer password** to configure an MD5 authentication key used by both MSDP peers to establish a TCP connection.

Use **undo peer password** to restore the default.

## Syntax

**peer** *peer-address* **password** { **cipher** | **simple** } *password*

**undo peer** *peer-address* **password**

## Default

MSDP peers do not perform MD5 authentication to establish TCP connections.

## Views

MSDP view

## Predefined user roles

network-admin

## Parameters

*peer-address*: Specifies an MSDP peer by its IP address.

**cipher**: Sets a ciphertext MD5 authentication key.

**simple**: Sets a plaintext MD5 authentication key.

*password*: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 80 characters. If **cipher** is specified, it must be a ciphertext string of 33 to 137 characters.

## Usage guidelines

The MSDP peers involved in MD5 authentication must be configured with the same authentication method and key. Otherwise, the authentication fails and the TCP connection cannot be established.

For security purposes, all keys, including keys configured in plain text, are saved in cipher text.

## Examples

# On the public network, configure an MD5 authentication key in plaintext as **aabbcc** for the TCP connections between the local end and the MSDP peer 10.1.100.1. The configuration on the remote peer is similar.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 10.1.100.1 password simple aabbcc
```

## peer request-sa-enable

Use **peer request-sa-enable** to enable the device to send an SA request message to an 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.

### Syntax

```
peer peer-address request-sa-enable
undo peer peer-address request-sa-enable
```

### Default

After receiving a new join message, the device does not send an SA request message to any MSDP peer. Instead, it waits for the next SA message to come.

### Views

MSDP view

### Predefined user roles

network-admin

### Parameters

*peer-address*: Specifies an MSDP peer by its IP address.

### Usage guidelines

You must disable SA message cache mechanism before you execute this command. Otherwise, the device does not send out SA request messages.

## Examples

# On the public network, disable the SA message cache mechanism. Enable the device to send an SA request message to the MSDP peer 125.10.7.6 after it receives 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
```

### Related commands

- **cache-sa-enable**
- **display msdp peer-status**

## peer sa-cache-maximum

Use **peer sa-cache-maximum** to configure the maximum number of cached (S, G) entries learned from an MSDP peer.

Use **undo peer sa-cache-maximum** to restore the default.

### Syntax

```
peer peer-address sa-cache-maximum sa-limit
```

```
undo peer peer-address sa-cache-maximum
```

### Default

The device can cache a maximum of 4294967295 (S, G) entries learned from any MSDP peer.

### Views

MSDP view

### Predefined user roles

network-admin

### Parameters

*peer-address*: Specifies an MSDP peer by its IP address.

*sa-limit*: Specifies the maximum number of (S, G) entries that the device can cache, in the range of 1 to 4294967295.

### Examples

```
# On the public network, enable the device to cache up to 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
```

### Related commands

- **display msdp brief**
- **display msdp peer-status**
- **display msdp sa-count**

## peer sa-policy

Use **peer sa-policy** to configure an SA incoming or outgoing policy.

Use **undo peer sa-policy** to remove the configured SA incoming or outgoing policy.

### Syntax

```
peer peer-address sa-policy { export | import } [ acl acl-number ]
```

```
undo peer peer-address sa-policy { export | import }
```

### Default

All SA messages are accepted or forwarded.

## Views

MSDP view

## Predefined user roles

network-admin

## Parameters

**export**: Specifies the outgoing direction.

**import**: Specifies the incoming direction.

*peer-address*: Specifies an MSDP peer by its IP address.

*acl-number*: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999. If you specify an ACL, the device accepts and forwards only SA messages that the ACL permits. If you do not specify an ACL, the device discards all SA messages when any of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

## Usage guidelines

In an IPv4 advanced ACL, the **source** keyword and the **destination** keyword match against multicast source addresses and multicast group addresses in SA messages, respectively.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

This command controls the acceptance and forwarding of SA messages. You can also use the **import-source** command to configure a filtering rule to control the creation of SA messages.

## Examples

# On the public network, configure an SA outgoing policy to forward only SA messages that ACL 3100 permits to the MSDP peer 125.10.7.6.

```
<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
```

## Related commands

- **display msdp peer-status**
- **import-source**

## peer sa-request-policy

Use **peer sa-request-policy** to configure an SA request policy.

Use **undo peer sa-request-policy** to remove the configured SA request policy.

## Syntax

```
peer peer-address sa-request-policy [ acl acl-number ]
```

```
undo peer peer-address sa-request-policy
```

## Default

SA request messages are not filtered.

## Views

MSDP view

## Predefined user roles

network-admin

## Parameters

*peer-address*: Specifies an MSDP peer by its IP address.

*acl-number*: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. If you specify an ACL, the switch accepts only SA requests that the ACL permits. All SA requests are filtered out when any of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

## Usage guidelines

In an IPv4 basic rule, the **source** keyword matches the multicast group addresses in SA request messages.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

## Examples

```
# On the public network, configure an SA request policy to process SA requests originated from the MSDP peer 175.58.6.5 with multicast groups 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
```

## reset msdp peer

Use **reset msdp peer** to reset the TCP connection with an MSDP peer and clear statistics for the MSDP peer.

## Syntax

```
reset msdp [ vpn-instance vpn-instance-name ] peer [ peer-address ]
```

## Views

User view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command resets the TCP connection with the specified MSDP peer and clears statistics for the MSDP peer on the public network.

*peer-address*: Specifies an MSDP peer by its IP address. If you do not specify an MSDP peer, the command resets the TCP connections with all MSDP peers.

## Examples

# On the public network, reset the TCP connection with the MSDP peer 125.10.7.6, and clear all statistics for this MSDP peer.

```
<Sysname> reset mstp peer 125.10.7.6
```

# reset mstp sa-cache

Use **reset mstp sa-cache** to clear (S, G) entries from the SA cache.

## Syntax

```
reset mstp [ vpn-instance vpn-instance-name ] sa-cache [ group-address ]
```

## Views

User view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command clears (S, G) entries from the SA cache on the public network.

*group-address*: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, the command clears the cached (S, G) entries for all multicast groups from the SA cache.

## Examples

# Clear the (S, G) entries for the multicast group 225.5.4.3 from the SA cache on the public network.

```
<Sysname> reset mstp sa-cache 225.5.4.3
```

## Related commands

- **cache-sa-enable**
- **display mstp sa-cache**

# reset mstp statistics

Use **reset mstp statistics** to clear statistics for the specified MSDP peer without resetting the TCP connection with the MSDP peer.

## Syntax

```
reset msdp [ vpn-instance vpn-instance-name ] statistics [ peer-address ]
```

## Views

User view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command clears statistics for the specified MSDP peer without resetting the TCP connection with the MSDP peer on the public network.

*peer-address*: Specifies an MSDP peer by its IP address. If you do not specify an MSDP peer, the command clears statistics for all MSDP peers.

## 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)

Use **shutdown** to tear down the connection with an MSDP peer.

Use **undo shutdown** to re-establish the connection with an MSDP peer.

## Syntax

```
shutdown peer-address
```

```
undo shutdown peer-address
```

## Default

The connections with all MSDP peers are active.

## Views

MSDP view

## Predefined user roles

network-admin

## Parameters

*peer-address*: Specifies an MSDP peer by its IP address.

## Examples

```
# Tear down 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
```

## Related commands

- **display msdp brief**
- **display msdp peer-status**



## static-rpf-peer

Use **static-rpf-peer** to configure a static RPF peer.

Use **undo static-rpf-peer** to remove a static RPF peer.

### Syntax

```
static-rpf-peer peer-address [ rp-policy ip-prefix-name ]
```

```
undo static-rpf-peer peer-address
```

### Default

No static RPF peer is configured.

### Views

MSDP view

### Predefined user roles

network-admin

### Parameters

*peer-address*: Specifies an MSDP peer by its IP address.

**rp-policy** *ip-prefix-name*: Specifies a filtering policy based on the RP addresses in SA messages. The *ip-prefix-name* argument is the filtering policy name, a case-sensitive string of 1 to 63 characters.

### Usage guidelines

When you configure multiple static RPF peers at the same time, observe the following rules:

- If the **rp-policy** keyword is specified for all the static RPF peers, SA messages from the active static RPF peers are filtered according to the configured filtering policy. The router receives only SA messages that have passed the filtering.
- If the **rp-policy** keyword is not specified for the static RPF peers, the router receives all SA messages from the active static RPF peers.

### Examples

```
# Configure a static RPF peer on the public network.
```

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

```
[Sysname] ip prefix-list list1 permit 130.10.0.0 16 greater-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
```

### Related commands

- **display msdp peer-status**
- **ip prefix-list**

## timer retry

Use **timer retry** to configure the interval between MSDP peering connection attempts.

Use **undo timer retry** to restore the default.

## Syntax

**timer retry** *interval*

**undo timer retry**

## Default

The interval between MSDP peering connection attempts is 30 seconds.

## Views

MSDP view

## Predefined user roles

network-admin

## Parameters

*interval*: Specifies an interval between MSDP peering connection attempts, in the range of 1 to 60 seconds.

## Examples

# Set the MSDP peering connection attempt interval to 60 seconds on the public network.

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

```
[Sysname] msdp
```

```
[Sysname-msdp] timer retry 60
```

---

# Multicast VPN commands

## data-delay

Use **data-delay** to configure the data-delay period (delay period before the default-MDT switches to the data-MDT).

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

### Syntax

**data-delay** *delay*

**undo data-delay**

### Default

The default setting is 3 seconds.

### Views

MD view

### Predefined user roles

network-admin

### Parameters

*delay*: Specifies a data-delay period in the range of 1 to 60 seconds.

### Examples

```
# Set the data-delay period to 20 seconds in the VPN instance mvpn.
```

```
<Sysname> system-view  
[Sysname] multicast-domain vpn-instance mvpn  
[Sysname-md-mvpn] data-delay 20
```

## data-group

Use **data-group** to configure the data-group address range and the switchover criteria.

Use **undo data-group** to restore the default.

### Syntax

**data-group** *group-address* { *mask-length* | *mask* } [ **acl** *acl-number* ]

**undo data-group**

### Default

The data-group address range is not configured, and multicast traffic never switches to a data-MDT.

### Views

MD view

## Predefined user roles

network-admin

## Parameters

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

*mask-length*: Specifies an address mask length in the range of 25 to 32.

*mask*: Specifies the address mask.

**acl** *acl-number*: Specifies an advanced ACL number in the range of 3000 to 3999. If you specify an ACL, the configured MDT switchover criteria applies to the (S, G) entries that the ACL permits. If you do not specify an ACL, the configured MDT switchover criteria apply to all (S, G) entries. To make the ACL effective, specify the protocol type as IP, and include the **source** and **destination** keywords when creating an ACL rule. The **source** and **destination** keywords specify a multicast source address range and a multicast group address range, respectively.

## Usage guidelines

On a PE device, the data-group address range must meet the following requirements:

- It must not include the default-group address of the MD.
- It must not overlap with the data-group address range of any other MDs.

On different devices, if the public network is not in PIM-SSM mode, the data-group address ranges for different MDs cannot overlap.

If you execute the command multiple times in an MD, the most recent configuration takes effect.

If you configure this command on the device, switchover from the default-MDT to data-MDT will take place when the following conditions are met:

- The device receives the multicast traffic that has passed the ACL rule filtering.
- The multicast traffic is maintained for the data-delay period.

## Examples

```
# Configure the data-group address range in VPN instance mvpn as 239.1.2.128 to 239.1.2.255.  
<Sysname> system-view  
[Sysname] multicast-domain vpn-instance mvpn  
[Sysname-md-mvpn] data-group 239.1.2.128 25
```

## default-group

Use **default-group** to specify a default-group address.

Use **undo default-group** to restore the default.

## Syntax

**default-group** *group-address*

**undo default-group**

## Default

The default-group address is not specified.

## Views

MD view

## Predefined user roles

network-admin

## Parameters

*group-address*: Specifies a default-group address in the range of 224.0.1.0 to 239.255.255.255.

## Usage guidelines

The same default-group address must be used by the MD of the same VPN instance on different PE device. In addition, the default-group address must be different from the default-group address and the data-group address used by other MDs.

## Examples

# Specify the default-group address as 239.1.1.1 for VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] multicast-domain vpn-instance mvpn
[Sysname-md-mvpn] default-group 239.1.1.1
```

# display multicast-domain data-group receive

Use **display multicast-domain data-group receive** to display data-group information received by a VPN instance in the MD.

## Syntax

```
display multicast-domain vpn-instance vpn-instance-name data-group receive [ brief | [ active | group group-address | sender source-address | vpn-source-address [ mask { mask-length | mask } ] ] | vpn-group-address [ mask { mask-length | mask } ] ] *
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance, a case-sensitive string of 1 to 31 characters.

**brief**: Specifies brief information. If you do not specify this keyword, the command displays detailed information.

**active**: Specifies the data-group that has joined the data-MDT.

**group** *group-address*: Specifies a public network multicast group address in the range of 224.0.1.0 to 239.255.255.255.

**sender** *source-address*: Specifies a public network multicast source address.

*vpn-source-address*: Specifies a VPN multicast source address.

*mask-length*: Specifies a mask length of the specified VPN multicast source/group address, in the range of 0 to 32. The default value is 32.

*mask*: Specifies a subnet mask of the specified VPN multicast source/group address, 255.255.255.255 by default.

*vpn-group-address*: Specifies a VPN multicast group address in the range of 224.0.0.0 to 239.255.255.255.

## Examples

# Display data-group information received by VPN instance **mvpn** in the MD.

```
<Sysname> display multicast-domain vpn-instance mvpn data-group receive
MD data-group information received by VPN instance: mvpn
Total 2 data-groups for 8 entries
Total 2 data-groups and 8 entries matched
```

```
Data-group: 226.1.1.0   Reference count: 4   Active count: 2
  Sender: 172.100.1.1   Active count: 1
    (192.6.1.5, 239.1.1.1)   expires: 00:03:10 active
    (192.6.1.5, 239.1.1.158) expires: 00:03:10
  Sender: 181.100.1.1, active count: 1
    (195.6.1.2, 239.1.2.12)  expires: 00:03:10 active
    (195.6.1.2, 239.1.2.197) expires: 00:03:10
Data-group: 229.1.1.0   Reference count: 4   Active count: 2
  Sender: 185.100.1.1   Active count: 1
    (198.6.1.5, 239.1.3.62)  expires: 00:03:10 active
    (198.6.1.5, 225.1.1.109) expires: 00:03:10
  Sender: 190.100.1.1   Active count: 1
    (200.6.1.2, 225.1.4.80)  expires: 00:03:10 active
    (200.6.1.2, 225.1.4.173) expires: 00:03:10
```

# Display brief data-group information received by VPN instance **mvpn** in the MD.

```
<Sysname> display multicast-domain vpn-instance mvpn data-group receive brief
MD data-group information received by VPN instance: mvpn
Total 2 data-groups for 8 entries
Total 2 data-groups and 8 entries matched
```

```
Data group: 226.1.1.0   Reference count: 4   Active count: 2
Data group: 229.1.1.0   Reference count: 4   Active count: 2
```

**Table 52 Command output**

Field	Description
MD data-group information received by VPN instance: mvpn	Data-group information received by VPN instance <b>mvpn</b> .
Total 2 data-groups for 8 entries	A total of two data-groups, associated with eight (S, G) entries.
Total 2 data-groups and 8 entries matched	A total of two data-groups are matched, associated with eight (S, G) entries.
Data-group	Data-group address received.
Sender	BGP peer address of the PE device that sent the data-group information.
Reference count	Number of VPN multicast groups referenced by the data-group.
Active count	Number of active VPN multicast groups (multicast groups with active receivers) referenced by the data-group.

Field	Description
expires	Remaining time for the VPN (S, G) entry referenced by the data-group.

## display multicast-domain data-group send

Use **display multicast-domain data-group send** to display data-group information sent by a VPN instance in the MD.

### Syntax

**display multicast-domain vpn-instance** *vpn-instance-name* **data-group send** [ **group** *group-address* | **reuse interval** | *vpn-source-address* [ **mask** { *mask-length* | *mask* } ] | *vpn-group-address* [ **mask** { *mask-length* | *mask* } ] ] \*

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance, a case-sensitive string of 1 to 31 characters.

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

**reuse interval**: Specifies an interval during which the data-group address reuses occur, in the range of 1 to 2147483647 seconds.

*vpn-source-address*: Specifies a VPN multicast source address.

*mask-length*: Specifies a mask length of the specified multicast source/group address, in the range of 0 to 32. The default is 32.

*mask*: Specifies a subnet mask of the specified VPN multicast source/group address, 255.255.255.255 by default.

*vpn-group-address*: Specifies a VPN multicast group address in the range of 224.0.0.0 to 239.255.255.255.

### Examples

# Display data-group information sent by VPN instance **mvpn** in the MD.

```
<Sysname> display multicast-domain vpn-instance mvpn data-group send
```

```
MD data-group information sent by VPN instance: mvpn
```

```
Total 2 data-groups for 6 entries
```

```
Total 2 data-groups and 6 entries matched
```

```
Reference count of 226.1.1.0: 3
```

```
(192.6.1.5, 239.1.1.1)
```

```
switch time: 00:00:21
```

```
(192.6.1.5, 239.1.1.158)
```

```
switch time: 00:00:21
```

```
(192.6.1.5, 239.1.2.50)
```

```
switch time: 00:00:05
```

```

Reference count of 226.1.1.1: 3
(192.6.1.2, 225.1.1.1)          switch time: 00:00:21
(192.6.1.2, 225.1.2.50)         switch time: 00:00:05
(192.6.1.5, 239.1.1.159)        switch time: 00:00:21

# Display the data-group reuse information sent by VPN instance mvpn within 30 seconds in the MD.
<Sysname> display multicast-domain vpn-instance mvpn data-group send reuse 30
MD data-group information sent by VPN instance: mvpn
Total 2 data-groups for 3 entries
Total 2 data-groups and 3 entries matched

Reuse count of 226.1.1.0: 1
Reuse count of 226.1.1.1: 1
Reuse count of 226.1.1.2: 1

```

**Table 53 Command output**

Field	Description
MD data-group information sent by VPN instance: mvpn	Data-group information sent by VPN instance <b>mvpn</b> .
Total 2 data-groups for 6 entries	A total of two data-groups, associated with six (S, G) entries.
Total 2 data-groups and 6 entries matched	A total of two data-groups are matched, associated with six (S, G) entries.
Reference count of 226.1.1.0	Number of VPN multicast groups referenced by the sent data-group.
switch time	Switchover time of the VPN (S, G) entry referenced by the data-group.
Reuse count of 226.1.1.0	Number of data-group reuses during the specified length of time.

## display multicast-domain default-group

Use **display multicast-domain default-group** to display the default-group information.

### Syntax

```
display multicast-domain [ vpn-instance vpn-instance-name ] default-group
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays the default-group information for all VPN instances.



## Examples

```
# Display information about default-groups for all VPN instances.
```

```
<Sysname> display multicast-domain default-group
Group address      Source address     Interface          VPN instance
239.1.1.1          1.1.1.1           MTunnel0           mvpna
239.2.1.1          1.1.1.1           MTunnel1           mvpnb
239.3.1.1          --                 MTunnel2           mvpnc
```

**Table 54 Command output**

Field	Description
Group address	Address of the default-group.
Source address	IP address of the MD source interface, which is used by the MTI as the source address to encapsulate the VPN multicast packets.
Interface	MTI interface.
VPN instance	VPN instance to which the default-group belongs.

## log data-group-reuse

Use **log data-group-reuse** to enable data-group reuse logging.

Use **undo log data-group-reuse** to disable data-group reuse logging.

### Syntax

```
log data-group-reuse
```

```
undo log data-group-reuse
```

### Default

The data-group reuse logging function is disabled.

### Views

MD view

### Predefined user roles

network-admin

### Examples

```
# Enable data-group reuse logging in VPN instance mvpn.
```

```
<Sysname> system-view
[Sysname] multicast-domain vpn-instance mvpn
[Sysname-md-mvpn] log data-group-reuse
```

## multicast-domain

Use **multicast-domain** to create the MD for a VPN instance and enter MD view.

Use **undo multicast-domain** to clear the configurations that are made in MD view for a VPN instance.

### Syntax

```
multicast-domain vpn-instance vpn-instance-name
```

**undo multicast-domain vpn-instance** *vpn-instance-name*

## Default

No MD exists for a VPN instance.

## Views

System view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

## Examples

```
# Create the MD for the VPN instance mvpn and enter MD view.  
<Sysname> system-view  
[Sysname] multicast-domain vpn-instance mvpn  
[Sysname-md-mvpn]
```

## source

Use **source** to specify the MD source interface.

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

## Syntax

**source** *interface-type interface-number*

**undo source**

## Default

No MD source interface is specified.

## Views

MD view

## Predefined user roles

network-admin

## Parameters

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

## Usage guidelines

The IP address of the MD source interface must be the same as the source address used for establishing BGP peer relationship. Otherwise, correct routing information cannot be obtained.

## Examples

```
# The source interface used for establishing BGP peer relationship is Loopback 1. Specify this interface  
as the MD source interface for the VPN instance mvpn.  
<Sysname> system-view  
[Sysname] multicast-domain vpn-instance mvpn  
[Sysname-md-mvpn] source loopback 1
```

# MLD snooping commands

## display ipv6 l2-multicast ip

Use **display ipv6 l2-multicast ip** to display information about Layer 2 IPv6 multicast groups.

### Syntax

```
display ipv6 l2-multicast ip [ group ipv6-group-address | source ipv6-source-address ] * [ vlan vlan-id ]  
[ slot slot-number ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**group** *ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. If you do not specify an IPv6 multicast group, the command displays information about all Layer 2 IPv6 multicast groups.

**source** *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, the command displays information about Layer 2 IPv6 multicast groups for all IPv6 multicast sources.

**vlan** *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command displays information about Layer 2 IPv6 multicast groups for all VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays information about the Layer 2 IPv6 multicast groups on the master device.

### Examples

```
# Display information about the Layer 2 IPv6 multicast groups for VLAN 2.
```

```
<Sysname> display ipv6 l2-multicast ip vlan 2
```

```
Total 1 entries.
```

```
VLAN 2: Total 1 IP entries.  
 (::, FF1E::101)  
Attribute: static, success  
Host slots (0 in total):  
Host ports (1 in total):  
XGE1/0/1 (S, SUC)
```

**Table 55 Command output**

Field	Description
Total 1 entries	Total number of Layer 2 IPv6 multicast groups.

Field	Description
VLAN 2: Total 1 IP entries	Total number of Layer 2 IPv6 multicast groups in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means any IPv6 multicast sources.
Attribute	Entry attribute: <ul style="list-style-type: none"> <li>• <b>dynamic</b>—The entry is created by a dynamic protocol.</li> <li>• <b>static</b>—The entry is created by a static protocol.</li> <li>• <b>pim</b>—The entry is created by IPv6 PIM.</li> <li>• <b>kernel</b>—The entry is obtained from the kernel.</li> <li>• <b>success</b>—Processing succeeds.</li> <li>• <b>fail</b>—Processing fails.</li> </ul>
Host ports (1 in total)	Member ports, and the total number of the member ports.
(S, SUC)	Port attribute: <ul style="list-style-type: none"> <li>• <b>D</b>—Dynamic port.</li> <li>• <b>S</b>—Static port.</li> <li>• <b>P</b>—IPv6 PIM port.</li> <li>• <b>K</b>—Port obtained from the kernel.</li> <li>• <b>R</b>—Port learned from (*, *) entries.</li> <li>• <b>W</b>—Port learned from (*, G) entries.</li> <li>• <b>SUC</b>—Processing succeeds.</li> <li>• <b>F</b>—Processing fails.</li> <li>• <b>BC</b>—Broadcast port. The TRILL port floods the IPv6 multicast data after the topology changes.</li> </ul>

## display ipv6 l2-multicast ip forwarding

Use **display ipv6 l2-multicast ip forwarding** to display Layer 2 IPv6 multicast group entries.

### Syntax

```
display ipv6 l2-multicast ip forwarding [ group ipv6-group-address | source ipv6-source-address ] *
[ vlan vlan-id ] [ slot slot-number ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**group** *ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. If you do not specify an IPv6 multicast group, the command displays Layer 2 IPv6 multicast group entries for all IPv6 multicast groups.

**source** *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, the command displays Layer 2 IPv6 multicast group entries for all IPv6 multicast sources.

**vlan** *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command displays Layer 2 IPv6 multicast group entries for all VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays Layer 2 IPv6 multicast group entries on the master device.

## Examples

```
# Display Layer 2 IPv6 multicast group entries for VLAN 2.
```

```
<Sysname> display ipv6 l2-multicast ip forwarding vlan 2
Total 1 entries.
```

```
VLAN 2: Total 1 IP entries.
 (::, FF1E::101)
 Host slots (0 in total):
 Host ports (3 in total):
   XGE1/0/1
   XGE1/0/2
   XGE1/0/3
```

**Table 56 Command output**

Field	Description
Total 1 entries	Total number of Layer 2 IPv6 multicast group entries.
VLAN 2: Total 1 IP entries	Total number of Layer 2 IPv6 multicast group entries in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means any IPv6 multicast sources.
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (3 in total)	Member ports, and the total number of the member ports.

## display ipv6 l2-multicast mac

Use **display ipv6 l2-multicast mac** to display information about Layer 2 IPv6 MAC multicast groups.

### Syntax

```
display ipv6 l2-multicast mac [ mac-address ] [ vlan vlan-id ] [ slot slot-number ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

*mac-address*: Specifies an IPv6 MAC multicast group by its IPv6 MAC address. If you do not specify an IPv6 MAC multicast group, the command displays information about all Layer 2 IPv6 MAC multicast groups.

**vlan** *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command displays information about Layer 2 IPv6 MAC multicast groups for all VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays information about the Layer 2 IPv6 MAC multicast groups on the master device.

## Examples

```
# Display information about the Layer 2 IPv6 MAC multicast groups for VLAN 2.
```

```
<Sysname> display ipv6 l2-multicast mac vlan 2  
Total 1 MAC entries.
```

```
VLAN 2: Total 1 MAC entries.  
MAC group address: 3333-0000-0101  
Attribute: success  
Host slots (0 in total):  
Host ports (1 in total):  
XGE1/0/1
```

**Table 57 Command output**

Field	Description
Total 1 MAC entries	Total number of Layer 2 IPv6 MAC multicast groups.
VLAN 2: Total 1 MAC entries	Total number of Layer 2 IPv6 MAC multicast groups in VLAN 2.
MAC group address	IPv6 address of the Layer 2 IPv6 MAC multicast group.
Attribute	Entry attribute: <ul style="list-style-type: none"><li>• <b>success</b>—Processing succeeds.</li><li>• <b>fail</b>—Processing fails.</li></ul>
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (1 in total)	Member ports, and the total number of the member ports.

## display ipv6 l2-multicast mac forwarding

Use **display ipv6 l2-multicast mac forwarding** to display IPv6 MAC multicast group entries.

### Syntax

```
display ipv6 l2-multicast mac forwarding [ mac-address ] [ vlan vlan-id ] [ slot slot-number ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

## Parameters

**mac-address:** Specifies an IPv6 MAC multicast group by its IPv6 MAC address. If you do not specify an IPv6 MAC multicast group, the command displays IPv6 MAC multicast group entries for all IPv6 MAC multicast groups.

**vlan *vlan-id*:** Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command displays IPv6 MAC multicast group entries for all VLANs.

**slot *slot-number*:** Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays IPv6 MAC multicast group entries on the master device.

## Examples

```
# Display IPv6 MAC multicast group entries for VLAN 2.
```

```
<Sysname> display ipv6 l2-multicast mac forwarding vlan 2
Total 1 MAC entries.
```

```
VLAN 2: Total 1 MAC entries.
```

```
MAC group address: 3333-0000-0101
```

```
Host slots (0 in total):
```

```
Host ports (3 in total):
```

```
  XGE1/0/1
```

```
  XGE1/0/2
```

```
  XGE1/0/3
```

**Table 58 Command output**

Field	Description
Total 1 MAC entries	Total number of IPv6 MAC multicast group entries.
VLAN 2: Total 1 MAC entries	Total number of IPv6 MAC multicast group entries in VLAN 2.
MAC group address	Address of the IPv6 MAC multicast group.
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (3 in total)	Member ports, and the total number of the member ports.

## display mld-snooping

Use **display mld-snooping** to display MLD snooping status.

### Syntax

```
display mld-snooping [ global | vlan vlan-id ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

## Parameters

**global**: Displays the global MLD snooping status.

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

## Usage guidelines

If you do not specify any parameters, the command displays the global MLD snooping status and the MLD snooping status in all VLANs.

## Examples

# Display the global MLD snooping status and the MLD snooping status for all VLANs.

```
<Sysname> display mld-snooping
MLD snooping information: Global
  MLD snooping: Enabled
  Drop-unknown: Disabled
  Host-aging-time: 260s
  Router-aging-time: 260s
  Max-response-time: 10s
  Last-listener-query-interval: 1s
  Report-aggregation: Enabled
  Dot1p-priority: --

MLD snooping information: VLAN 1
  MLD snooping: Enabled
  Drop-unknown: Disabled
  Version: 1
  Host-aging-time: 260s
  Router-aging-time: 260s
  Max-response-time: 10s
  Last-listener-query-interval: 1s
  Querier: Disabled
  Query-interval: 125s
  General-query source IP: FE80::2FF:FFFF:FE00:1
  Special-query source IP: FE80::2FF:FFFF:FE00:1
  Report source IP: FE80::2FF:FFFF:FE00:2
  Done source IP: FE80::2FF:FFFF:FE00:3
  Dot1p-priority: 2

MLD snooping information: VLAN 10
  MLD snooping: Enabled
  Drop-unknown: Enabled
  Version: 2
  Host-aging-time: 260s
  Router-aging-time: 260s
  Max-response-time: 10s
  Last-listener-query-interval: 1s
  Query-interval: 125s
  General-query source IP: FE80::2FF:FFFF:FE00:1
  Special-query source IP: FE80::2FF:FFFF:FE00:1
```



```

Report source IP: FE80::2FF:FFFF:FE00:2
Done source IP: FE80::2FF:FFFF:FE00:3
Dot1p-priority: --

```

**Table 59 Command output**

Field	Description
MLD snooping	MLD snooping status: <ul style="list-style-type: none"> <li>• Enabled.</li> <li>• Disabled.</li> </ul>
Drop-unknown	Status of dropping unknown IPv6 multicast data: <ul style="list-style-type: none"> <li>• Enabled.</li> <li>• Disabled.</li> </ul>
Version	MLD snooping version.
Host-aging-time	Aging timer for the dynamic member port.
Router-aging-time	Aging timer for the dynamic router port.
Max-response-time	Maximum time for responding to MLD general queries.
Last-listener-query-interval	Interval for sending MLD multicast-address-specific queries.
Report-aggregation	Status of MLD report suppression: <ul style="list-style-type: none"> <li>• Enabled.</li> <li>• Disabled.</li> </ul>
Dot1p-priority	802.1p priority for MLD messages, where two hyphens (-) mean that it is not configured.
Querier	Whether the MLD snooping querier is enabled.
Query-interval	Interval for sending MLD general queries.
General-query source IP	Source IPv6 address of MLD general queries.
Special-query source IP	Source IPv6 address of MLD multicast-address-specific queries.
Report source IP	Source IPv6 address of MLD reports.
Done source IP	Source IPv6 address of MLD done messages.

## display mld-snooping group

Use **display mld-snooping group** to display dynamic MLD snooping forwarding entries.

### Syntax

```
display mld-snooping group [ ipv6-group-address | ipv6-source-address ] * [ vlan vlan-id ] [ verbose ]
[ slot slot-number ]
```

### Views

Any view

### Predefined user roles

network-admin  
network-operator

## Parameters

*ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where "x" and "y" represent any hexadecimal numbers from 0 to F. If you do not specify an IPv6 multicast group, the command displays dynamic MLD snooping forwarding entries for all IPv6 multicast groups.

*ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, the command displays dynamic MLD snooping forwarding entries for all IPv6 multicast sources.

**vlan** *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command displays dynamic MLD snooping forwarding entries for all VLANs.

**verbose**: Displays detailed information. If you do not specify this keyword, the command displays brief information.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays dynamic MLD snooping forwarding entries on the master device.

## Examples

# Display detailed information about the dynamic MLD snooping forwarding entries for VLAN 2.

```
<Sysname> display mld-snooping group vlan 2 verbose
Total 1 entries.
```

```
VLAN 2: Total 1 entries.
  (::,FF1E::101)
  Attribute: local port
  FSM information: normal
  Host slots (0 in total):
  Host ports (1 in total):
    XGE1/0/2          (00:03:23)
```

**Table 60 Command output**

Field	Description
Total 1 entries	Total number of dynamic MLD snooping forwarding entries.
VLAN 2: Total 1 entries	Total number of dynamic MLD snooping forwarding entries in VLAN.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means any IPv6 multicast sources.
Attribute	Entry attribute: <ul style="list-style-type: none"><li>• <b>global port</b>—The entry has a global port.</li><li>• <b>local port</b>—The entry has a port that resides on the specified device.</li><li>• <b>slot</b>—The entry has a port that resides on a device other than the specified device.</li></ul>
FSM information	Finite state machine information of the entry: <ul style="list-style-type: none"><li>• <b>delete</b>—The entry attributes have been deleted.</li><li>• <b>dummy</b>—The entry is a new temporary entry.</li><li>• <b>no info</b>—No entry exists.</li><li>• <b>normal</b>—The entry is a correct entry.</li></ul>

Field	Description
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (1 in total)	Member ports, and the total number of the member ports.
(00:03:23)	Remaining aging time for the dynamic member port. <ul style="list-style-type: none"> <li>For a global port (including Layer 2 aggregate interfaces), this field is always displayed.</li> <li>For a non-global port, this field is displayed if the port is on the master device. Otherwise, you must specify the <b>slot slot-number</b> option to display this field.</li> </ul>

## Related commands

**reset mld-snooping group**

## display mld-snooping router-port

Use **display mld-snooping router-port** to display dynamic router port information.

### Syntax

**display mld-snooping router-port** [ **vlan** *vlan-id* ] [ **slot** *slot-number* ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

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

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays dynamic router port information on the master device.

### Examples

```
# Display dynamic router port information for VLAN 2.
<Sysname> display mld-snooping router-port vlan 2
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    XGE1/0/1                (00:01:30)
    XGE1/0/2                (00:00:23)
```

**Table 61 Command output**

Field	Description
Router slots (0 in total)	Member IDs of the member devices that have router ports and the total number of the member devices (excluding the specified member device).
Router ports (2 in total)	Dynamic router ports, and the total number of the dynamic router ports.

Field	Description
(00:01:30)	<p>Remaining aging time for the dynamic router port.</p> <ul style="list-style-type: none"> <li>For a global port, this field is always displayed.</li> <li>For a non-global port, this field is displayed if the port is on the master device. Otherwise, you must specify the <b>slot slot-number</b> option to display this field.</li> </ul>

## Related commands

**reset mld-snooping router-port**

# display mld-snooping static-group

Use **display mld-snooping static-group** to display static MLD snooping forwarding entries.

## Syntax

```
display mld-snooping static-group [ ipv6-group-address | ipv6-source-address ] * [ vlan vlan-id ]
[ verbose ] [ slot slot-number ]
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

*ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where "x" and "y" represent any hexadecimal numbers from 0 to F. If you do not specify an IPv6 multicast group, the command displays static MLD snooping forwarding entries for all IPv6 multicast groups.

*ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, the command displays static MLD snooping forwarding entries for all IPv6 multicast sources.

**vlan** *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command displays static MLD snooping forwarding entries for all VLANs.

**verbose**: Displays detailed information. If you do not specify this keyword, the command displays brief information.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays static MLD snooping forwarding entries on the master device.

## Examples

```
# Display detailed information about the static MLD snooping forwarding entries for VLAN 2.
```

```
<Sysname> display mld-snooping static-group vlan 2 verbose
```

```
Total 1 entries.
```

```
VLAN 2: Total 1 entries.
```

```
(::,FF1E::101)
```

```
Attribute: local port
```

```

FSM information: normal
Host slots (0 in total):
Host ports (1 in total):
  XGE1/0/2

```

**Table 62 Command output**

Field	Description
Total 1 entries	Total number of static MLD snooping forwarding entries.
VLAN 2: Total 1 entries	Total number of static MLD snooping forwarding entries in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means any IPv6 multicast sources.
Attribute	Entry attribute: <ul style="list-style-type: none"> <li>• <b>global port</b>—The entry has a global port.</li> <li>• <b>local port</b>—The entry has a port that resides on the specified device.</li> <li>• <b>slot</b>—The entry has a port that resides on a device other than the specified device.</li> </ul>
FSM information	Finite state machine information of the entry: <ul style="list-style-type: none"> <li>• <b>delete</b>—The entry attributes have been deleted.</li> <li>• <b>dummy</b>—The entry is a new temporary entry.</li> <li>• <b>no info</b>—No entry exists.</li> <li>• <b>normal</b>—The entry is a correct entry.</li> </ul>
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (1 in total)	Member ports, and the total number of the member ports.

## display mld-snooping static-router-port

Use **display mld-snooping static-router-port** to display static router port information.

### Syntax

```
display mld-snooping static-router-port [ vlan vlan-id ] [ slot slot-number ]
```

### Views

Any view

### Predefined user roles

```

network-admin
network-operator

```

### Parameters

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

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays static router port information on the master device.

### Examples

```
# Display static router port information for VLAN 2.
```

```

<Sysname> display mld-snooping static-router-port vlan 2
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    XGE1/0/1
    XGE1/0/2

```

**Table 63 Command output**

Field	Description
Router slots (0 in total)	Member IDs of the member devices that have router ports and the total number of the member devices (excluding the specified member device).
Router ports (2 in total)	Static router ports, and the total number of the static router ports.

## display mld-snooping statistics

Use **display mld-snooping statistics** to display statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping.

### Syntax

**display mld-snooping statistics**

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Examples

# Display statistics for the MLD messages and IPv6 PIM hello 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 IPv6 PIM hello: 0
Received error MLD messages: 0

```

Table 64 Command output

Field	Description
general queries	Number of MLD general queries.
specific queries	Number of MLD multicast-address-specific queries.
reports	Number of MLD reports.
done	Number of MLD done messages.
reports with right and wrong records	Number of MLD reports with correct and incorrect records.
specific sg queries	Number of MLD multicast-address-and-source-specific queries.
IPv6 PIM hello	Number of IPv6 PIM hello messages.
error MLD messages	Number of MLD messages with errors.

## Related commands

**reset mld-snooping statistics**

## dot1p-priority (MLD-snooping view)

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

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

### Syntax

**dot1p-priority** *priority-number*

**undo dot1p-priority**

### Default

The 802.1p priority for MLD messages is not configured.

### Views

MLD-snooping view

### Predefined user roles

network-admin

### Parameters

*priority-number*: Sets an 802.1p priority for MLD messages, in the range of 0 to 7. A higher value means a higher priority.

### Usage guidelines

This command and the **mld-snooping dot1p-priority** command have the same function but different effective ranges:

- The **dot1p-priority** command in MLD-snooping view takes effect on all VLANs.
- The **mld-snooping dot1p-priority** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping dot1p-priority** command takes priority over the **dot1p-priority** command in MLD-snooping view.

### Examples

```
# Set the 802.1p priority for MLD messages to 3 globally.
```

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] dot1p-priority 3
```

## Related commands

**mld-snooping dot1p-priority**

# enable (MLD-snooping view)

Use **enable** to enable MLD snooping for VLANs.

Use **undo enable** to disable MLD snooping for VLANs.

## Syntax

**enable vlan** *vlan-list*

**undo enable vlan** *vlan-list*

## Default

MLD snooping is disabled in a VLAN.

## Views

MLD-snooping view

## Predefined user roles

network-admin

## Parameters

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The value range for the VLAN ID is 1 to 4094.

## Usage guidelines

You must globally enable MLD snooping before you execute this command.

This command and the **mld-snooping enable** command have the same function but different effective ranges:

- The **enable** command in MLD-snooping view takes effect on the specified VLANs.
- The **mld-snooping enable** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping enable** command and the **enable** command in MLD-snooping view have the same priority, and the most recent configuration takes effect.

## Examples

```
# Enable MLD snooping globally, and enable MLD snooping for VLAN 2 through VLAN 10.
```

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] enable vlan 2 to 10
```

## Related commands

- **mld-snooping**
- **mld-snooping enable**



## entry-limit (MLD-snooping view)

Use **entry-limit** to set the global maximum number of MLD snooping forwarding entries, including dynamic entries and static entries.

Use **undo entry-limit** to restore the default.

### Syntax

**entry-limit** *limit*

**undo entry-limit**

### Default

The default setting is 4294967295.

### Views

MLD-snooping view

### Predefined user roles

network-admin

### Parameters

*limit*: Sets the global maximum number of MLD snooping forwarding entries, in the range of 0 to 4294967295.

### Examples

```
# Set the global maximum number of MLD snooping forwarding entries to 512.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] entry-limit 512
```

## fast-leave (MLD-snooping view)

Use **fast-leave** to enable fast-leave processing globally.

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

### Syntax

**fast-leave** [ **vlan** *vlan-list* ]

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

### Default

Fast-leave processing is disabled.

### Views

MLD-snooping view

### Predefined user roles

network-admin

## Parameters

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command applies to all VLANs.

## Usage guidelines

This feature enables the switch to immediately remove a port from the forwarding entry for an IPv6 multicast group when the port receives a done message.

This command and the **mld-snooping fast-leave** command have the same function but different effective ranges:

- The **fast-leave** command in MLD-snooping view takes effect on all ports.
- The **mld-snooping fast-leave** command takes effect on the current port.

For a port, the **mld-snooping fast-leave** command takes priority over the **fast-leave** command in MLD-snooping view.

## Examples

```
# Globally enable fast-leave processing for VLAN 2.  
<Sysname> system-view  
[Sysname] mld-snooping  
[Sysname-mld-snooping] fast-leave vlan 2
```

## Related commands

**mld-snooping fast-leave**

# group-policy (MLD-snooping view)

Use **group-policy** to configure a global IPv6 multicast group policy to control the IPv6 multicast groups that receiver hosts can join.

Use **undo group-policy** to remove the configured global IPv6 multicast group policy.

## Syntax

```
group-policy acl6-number [ vlan vlan-list ]  
undo group-policy [ vlan vlan-list ]
```

## Default

IPv6 multicast group policies are not configured, and receiver hosts can join IPv6 multicast groups.

## Views

MLD-snooping view

## Predefined user roles

network-admin

## Parameters

*acl6-number*: Specifies an IPv6 basic or advanced ACL by its number in the range of 2000 to 3999. Receiver hosts can join only IPv6 multicast groups that the ACL permits. If the ACL does not exist or the ACL does not contain valid rules, receiver hosts cannot join IPv6 multicast groups.

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command applies to all VLANs.

## Usage guidelines

In an IPv6 basic ACL, the **source** keyword matches the multicast group address in MLD reports. In an IPv6 advanced ACL, the **source** and **destination** keywords match the multicast source address and multicast group address in MLD reports, respectively. The multicast source address is considered to be 0::0 for the following MLD reports:

- MLDv1 reports.
- MLDv2 IS\_EX and MLDv2 TO\_EX reports that do not carry IPv6 multicast source addresses.

If you specify the **VPN-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

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

This configuration takes effect only on the IPv6 multicast groups that the port joins dynamically.

This command and the **mld-snooping group-policy** command have the same function but different effective ranges:

- The **group-policy** command in MLD-snooping view takes effect on all ports.
- The **mld-snooping group-policy** command takes effect on the current port.

For a port, the **mld-snooping group-policy** command takes priority over the **group-policy** command in MLD-snooping view.

## Examples

```
# Globally configure an IPv6 multicast group policy for VLAN 2 so that the hosts in this VLAN can join only the IPv6 multicast group FF03::101.
```

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff03::101 128
[Sysname-acl6-basic-2000] quit
[Sysname] mld-snooping
[Sysname-mld-snooping] group-policy 2000 vlan 2
```

## Related commands

**mld-snooping group-policy**

## host-aging-time (MLD-snooping view)

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

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

## Syntax

**host-aging-time** *interval*

**undo host-aging-time**

## Default

The default setting is 260 seconds.

## Views

MLD-snooping view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

## Usage guidelines

To avoid mistakenly deleting IPv6 multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by the following formula:

[ MLD general query interval ] + [ maximum response time for MLD general queries ]

HP recommends that you set the aging timer of dynamic member ports to the value calculated by the following formula:

[ MLD general query interval ] × 2 + [ maximum response time for MLD general queries ]

This command and the **mld-snooping host-aging-time** command have the same function but different effective ranges:

- The **host-aging-time** command in MLD-snooping view takes effect on all VLANs.
- The **mld-snooping host-aging-time** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping host-aging-time** command takes priority over the **host-aging-time** command in MLD-snooping view.

## 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
```

## Related commands

**mld-snooping host-aging-time**

# last-listener-query-interval (MLD-snooping view)

Use **last-listener-query-interval** to set the global MLD last listener query interval.

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

## Syntax

**last-listener-query-interval** *interval*

**undo last-listener-query-interval**

## Default

The global MLD last listener query interval is 1 second.

## Views

MLD-snooping view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an MLD last listener query interval in the range of 1 to 25 seconds.

## Usage guidelines

The MLD last listener query interval determines the interval for sending MLD multicast-address-specific queries and the maximum response time for MLD multicast-address-specific queries.

This command and the **mld-snooping last-listener-query-interval** command have the same function but different effective ranges:

- The **last-listener-query-interval** command in MLD-snooping view takes effect on all VLANs.
- The **mld-snooping last-listener-query-interval** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping last-listener-query-interval** command takes priority over the **last-listener-query-interval** command in MLD-snooping view.

## Examples

```
# Set the global MLD last listener query interval to 3 seconds.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] last-listener-query-interval 3
```

## Related commands

**mld-snooping last-listener-query-interval**

# max-response-time (MLD-snooping view)

Use **max-response-time** to set the global maximum response time for MLD general queries.

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

## Syntax

**max-response-time** *interval*

**undo max-response-time**

## Default

The global maximum response time for MLD general queries is 10 seconds.

## Views

MLD-snooping view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets the maximum response time for MLD general queries, in the range of 1 to 3174 seconds.

## Usage guidelines

To avoid mistakenly deleting IPv6 multicast group members, set the MLD general query interval to be greater than the maximum response time for MLD general queries.

This command and the **mld-snooping max-response-time** command have the same function but different effective ranges:

- The **max-response-time** command in MLD-snooping view takes effect on all VLANs.
- The **mld-snooping max-response-time** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping max-response-time** command takes priority over the **max-response-time** command in MLD-snooping view.

## Examples

```
# Set the global maximum response time for MLD general queries to 5 seconds.
```

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

## Related commands

**mld-snooping max-response-time**

# mld-snooping

Use **mld-snooping** to enable MLD snooping globally and enter MLD-snooping view.

Use **undo mld-snooping** to disable MLD snooping globally.

## Syntax

**mld-snooping**

**undo mld-snooping**

## Default

MLD snooping is globally disabled.

## Views

System view

## Predefined user roles

network-admin

## Examples

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

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

## Related commands

- **enable** (MLD-snooping view)
- **mld-snooping enable**

# mld-snooping done source-ip

Use **mld-snooping done source-ip** to configure a source IPv6 address for MLD done messages.

Use **undo mld-snooping done source-ip** to restore the default.

## Syntax

**mld-snooping done source-ip** *ipv6-address*

**undo mld-snooping done source-ip**

## Default

The source IPv6 address of the MLD done messages is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*ipv6-address*: Specifies a source IPv6 address for MLD done messages.

## Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

## Examples

# In VLAN 2, enable MLD snooping, and configure FE80:0:0:1::1 as the source IPv6 address of MLD done messages.

```
<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
```

## Related commands

- **enable** (MLD-snooping view)
- **mld-snooping enable**

# mld-snooping dot1p-priority

Use **mld-snooping dot1p-priority** to set the 802.1p priority for MLD messages in a VLAN.

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

## Syntax

**mld-snooping dot1p-priority** *priority-number*

**undo mld-snooping dot1p-priority**

## Default

The 802.1p priority for MLD messages is not configured.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*priority-number*: Sets an 802.1p priority for MLD messages, in the range of 0 to 7. A higher value means a higher priority.

## Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

This command and the **dot1p-priority** command in MLD-snooping view have the same function but different effective ranges:

- The **dot1p-priority** command in MLD-snooping view takes effect on all VLANs.
- The **mld-snooping dot1p-priority** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping dot1p-priority** command takes priority over the **dot1p-priority** command in MLD-snooping view.

## Examples

# In VLAN 2, enable MLD snooping, and set the 802.1p priority for MLD messages 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
```

## Related commands

- **dot1p-priority** (MLD-snooping view)
- **enable** (MLD-snooping view)
- **mld-snooping enable**

# mld-snooping drop-unknown

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.

## Syntax

**mld-snooping drop-unknown**

**undo mld-snooping drop-unknown**

## Default

Dropping unknown IPv6 multicast data in a VLAN is disabled, and unknown IPv6 multicast data is flooded in the VLAN.

## Views

VLAN view

## Predefined user roles

network-admin



## Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

## Examples

```
# In VLAN 2, enable MLD snooping, and enable dropping unknown IPv6 multicast data.
```

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

## Related commands

- **enable** (MLD-snooping view)
- **mld-snooping enable**

# mld-snooping enable

Use **mld-snooping enable** to enable MLD snooping for a VLAN.

Use **undo mld-snooping enable** to disable MLD snooping for a VLAN.

## Syntax

**mld-snooping enable**

**undo mld-snooping enable**

## Default

MLD snooping is disabled in a VLAN.

## Views

VLAN view

## Predefined user roles

network-admin

## Usage guidelines

You must enable MLD snooping globally before you enable MLD snooping for a VLAN.

This command and the **enable** command in MLD-snooping view have the same function but different effective ranges:

- The **enable** command in MLD-snooping view takes effect on the specified VLANs.
- The **mld-snooping enable** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping enable** command and the **enable** command in MLD-snooping view have the same priority, and the most recent configuration takes effect.

## Examples

```
# Enable MLD snooping globally and for VLAN 2.
```

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
```

```
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
```

## Related commands

- **enable** (MLD-snooping view)
- **mld-snooping**

## mld-snooping fast-leave

Use **mld-snooping fast-leave** to enable fast-leave processing on a port.

Use **undo mld-snooping fast-leave** to disable fast-leave processing on a port.

## Syntax

```
mld-snooping fast-leave [ vlan vlan-list ]
```

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

## Default

Fast-leave processing is disabled on a port.

## Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Parameters

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command applies to all VLANs.

## Usage guidelines

This feature enables the switch to immediately remove a port from the forwarding entry for a multicast group specified when the port receives a done message.

This command and the **fast-leave** command in MLD-snooping view have the same function but different effective ranges:

- The **fast-leave** command in MLD-snooping view takes effect on all ports.
- The **mld-snooping fast-leave** command takes effect on the current port.

For a port, the **mld-snooping fast-leave** command takes priority over the **fast-leave** command in MLD-snooping view.

## Examples

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

## Related commands

**fast-leave** (MLD-snooping view)

## mld-snooping general-query source-ip

Use **mld-snooping general-query source-ip** to configure a source IPv6 address for MLD general queries.

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

### Syntax

**mld-snooping general-query source-ip** *ipv6-address*

**undo mld-snooping general-query source-ip**

### Default

The source IPv6 address for MLD general queries is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

### Views

VLAN view

### Predefined user roles

network-admin

### Parameters

*ipv6-address*: Specifies a source IPv6 address for MLD general queries.

### Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command for the VLAN.

### Examples

# In VLAN 2, enable MLD snooping, and configure 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
```

### Related commands

- **enable** (MLD-snooping view)
- **mld-snooping enable**

## mld-snooping group-limit

Use **mld-snooping group-limit** to set the maximum number of IPv6 multicast groups that a port can join.

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

### Syntax

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

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

## Default

The default setting is 4294967295.

## Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Parameters

*limit*: Sets the maximum number of multicast groups that a port can join, in the range of 0 to 4294967295.

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id to end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command applies to all VLANs.

## Usage guidelines

This command takes effect only on the IPv6 multicast groups that a port joins dynamically.

## Examples

# Set the maximum number of IPv6 multicast groups that Ten-GigabitEthernet 1/0/1 in VLAN 2 can join to 10.

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

# mld-snooping group-policy

Use **mld-snooping group-policy** to configure an IPv6 multicast group policy on a port to control the IPv6 multicast groups that the receiver hosts attached to the port can join.

Use **undo mld-snooping group-policy** to remove the IPv6 multicast group policy on a port.

## Syntax

**mld-snooping group-policy** *acl6-number* [ **vlan** *vlan-list* ]

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

## Default

IPv6 multicast group policies are not configured on a port, and the hosts attached to the port can join IPv6 multicast groups.

## Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Parameters

*acl6-number*: Specifies an IPv6 basic or advanced ACL by its number in the range of 2000 to 3999. Receiver hosts can join only IPv6 multicast groups that the ACL permits. If the ACL does not exist or the ACL does not contain valid rules, receiver hosts cannot join IPv6 multicast groups.

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command applies to all VLANs.

## Usage guidelines

In an IPv6 basic ACL, the **source** keyword matches the multicast group address in MLD reports. In an IPv6 advanced ACL, the **source** and **destination** keywords match the multicast source address and multicast group address in MLD reports, respectively. The multicast source address is considered to be 0::0 for the following MLD reports:

- MLDv1 reports.
- MLDv2 IS\_EX and MLDv2 TO\_EX reports that do not carry IPv6 multicast source addresses.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

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

This command takes effect only on the IPv6 multicast groups that a port joins dynamically.

This command and the **group policy** command in MLD-snooping view have the same function but different effective ranges:

- The **group policy** command in MLD-snooping view takes effect on all ports.
- The **mld-snooping group-policy** command takes effect on the current port.

For a port, the **mld-snooping group-policy** command takes priority over the **group policy** command in MLD-snooping view.

## Examples

```
# Configure an IPv6 multicast group policy for VLAN 2 on Ten-GigabitEthernet 1/0/1 so that hosts attached to the port can join only the multicast group FF03::101.
```

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff03::101 128
[Sysname-acl6-basic-2000] quit
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mld-snooping group-policy 2000 vlan 2
```

## Related commands

**group-policy** (MLD-snooping view)

## mld-snooping host-aging-time

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

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

## Syntax

**mld-snooping host-aging-time** *interval*

**undo mld-snooping host-aging-time**

## Default

The default setting is 260 seconds.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an aging timer for the dynamic member ports in a VLAN, in the range of 1 to 8097894 seconds.

## Usage guidelines

You must enable MLD snooping for a VLAN before you configure this command for the VLAN.

To avoid mistakenly deleting IPv6 multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by the following formula:

[ MLD general query interval ] + [ maximum response time for MLD general queries ]

HP recommends that you set the aging timer of dynamic member ports to the value calculated by the following formula:

[ MLD general query interval ] × 2 + [ maximum response time for MLD general queries ]

This command and the **host-aging-time** command in MLD-snooping view have the same function but different effective ranges:

- The **host-aging-time** command in MLD-snooping view takes effect on all VLANs.
- The **mld-snooping host-aging-time** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping host-aging-time** command takes priority over the **host-aging-time** command in MLD-snooping view.

## Examples

# In VLAN 2, enable MLD snooping, and set the aging timer for the dynamic member ports to 300 seconds.

```
<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
```

## Related commands

- **enable** (MLD-snooping view)
- **host-aging-time** (MLD-snooping view)
- **mld-snooping enable**

## mld-snooping host-join

Use **mld-snooping host-join** to configure a port as a simulated member host for an IPv6 multicast group.

Use **undo mld-snooping host-join** to restore the default.

## 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* | **all** }

## Default

This function is disabled.

## Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Parameters

**ipv6-group-address**: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where "x" and "y" represent any hexadecimal numbers from 0 to F.

**source-ip** *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you specify an IPv6 multicast source, the command configures the port as a simulated member host for an IPv6 multicast source and group. If you do not specify an IPv6 multicast source, the command configures the port as a simulated member host for an IPv6 multicast group. This option takes effect on MLDv2 snooping devices.

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

**all**: Specifies all IPv6 multicast groups.

## Usage guidelines

Unlike a static member port, a port configured as a simulated member host ages out like a dynamic member port.

The MLD version and the MLD snooping version that the simulated member host runs must be the same.

## Examples

```
# Configure Ten-GigabitEthernet 1/0/1 as a simulated member host for the IPv6 multicast source and group (2002::22, FF3E::101) 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 version 2
[Sysname-vlan2] quit
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mld-snooping host-join ff3e::101 source-ip 2002::22
vlan 2
```

# mld-snooping last-listener-query-interval

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.

## Syntax

**mld-snooping last-listener-query-interval** *interval*

**undo mld-snooping last-listener-query-interval**

## Default

The MLD last listener query interval in a VLAN is 1 second.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an MLD last listener query interval in the range of 1 to 25 seconds.

## Usage guidelines

The MLD last listener query interval determines the interval for sending MLD multicast-address-specific queries and the maximum response time 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.

This command and the **last-listener-query-interval** command in MLD-snooping view have the same function but different effective ranges:

- The **last-listener-query-interval** command in MLD-snooping view takes effect on all VLANs.
- The **mld-snooping last-listener-query-interval** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping last-listener-query-interval** command takes priority over the **last-listener-query-interval** command in MLD-snooping view.

## Examples

# In VLAN 2, enable MLD snooping, and set the MLD last listener query interval to 3 seconds.

```
<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
```

## Related commands

- **enable** (MLD-snooping view)
- **last-listener-query-interval** (MLD-snooping view)
- **mld-snooping enable**

# mld-snooping max-response-time

Use **mld-snooping max-response-time** to set the maximum response time for MLD general queries in a VLAN.

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

## Syntax

**mld-snooping max-response-time** *interval*

**undo mld-snooping max-response-time**



## Default

The maximum response time for MLD general queries in a VLAN is 10 seconds.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets the maximum response time for MLD general queries, in the range of 1 to 3174 seconds.

## Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command for the VLAN.

To avoid mistakenly deleting IPv6 multicast group members, set the MLD general query interval to be greater than the maximum response time for MLD general queries.

This command and the **max-response-time** command in MLD-snooping view have the same function but different effective ranges:

- The **max-response-time** command in MLD-snooping view takes effect on all VLANs.
- The **mld-snooping max-response-time** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping max-response-time** command takes priority over the **max-response-time** command in MLD-snooping view.

## Examples

# In VLAN 2, enable MLD snooping, and set the maximum response time for MLD general queries to 5 seconds.

```
<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
```

## Related commands

- **enable** (MLD-snooping view)
- **max-response-time** (MLD-snooping view)
- **mld-snooping enable**

# mld-snooping overflow-replace

Use **mld-snooping overflow-replace** to enable the IPv6 multicast group replacement feature on a port.

Use **undo mld-snooping overflow-replace** to disable the multicast group replacement feature on a port.

## Syntax

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

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

## Default

The IPv6 multicast group replacement feature is disabled on a port.

## Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Parameters

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id to end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command applies to all VLANs.

## Usage guidelines

This command takes effect only on the IPv6 multicast groups that a port dynamically joins.

This command and the **overflow-replace** command in MLD-snooping view have the same feature but different effective ranges:

- The **overflow-replace** command in MLD-snooping view takes effect on all ports.
- The **mld-snooping overflow-replace** command takes effect on the current port.

For a port, the **mld-snooping overflow-replace** command takes priority over the **overflow-replace** command in MLD-snooping view.

## Examples

```
# Enable the IPv6 multicast group replacement feature for VLAN 2 on Ten-GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mld-snooping overflow-replace vlan 2
```

## Related commands

**overflow-replace** (MLD-snooping view)

# mld-snooping querier

Use **mld-snooping querier** to enable the MLD snooping querier for a VLAN.

Use **undo mld-snooping querier** to disable the MLD snooping querier.

## Syntax

**mld-snooping querier**

**undo mld-snooping querier**

## Default

The MLD snooping querier for a VLAN is disabled.

## Views

VLAN view

## Predefined user roles

network-admin

## Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command for the VLAN.

This command takes effect on a sub-VLAN only after you remove the sub-VLAN from the IPv6 multicast VLAN.

## Examples

```
# In VLAN 2, enable MLD snooping, and enable the MLD snooping querier.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping querier
```

## Related commands

- **enable** (MLD-snooping view)
- **mld-snooping enable**
- **subvlan** (IPv6 multicast VLAN view)

# mld-snooping report source-ip

Use **mld-snooping report source-ip** to configure a source IPv6 address for MLD reports.

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

## Syntax

**mld-snooping report source-ip** *ipv6-address*

**undo mld-snooping report source-ip**

## Default

The source IPv6 address for MLD reports is the IPv6 link-local address of current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*ipv6-address*: Specifies a source IPv6 address for MLD reports.

## Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

## Examples

```
# In VLAN 2, enable MLD snooping, and configure FE80:0:0:1::1 as the source IPv6 address of the MLD reports.
<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
```

### Related commands

- **enable** (MLD-snooping view)
- **mld-snooping enable**

## mld-snooping query-interval

Use **mld-snooping query-interval** to set the MLD general query interval in a VLAN.

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

### Syntax

```
mld-snooping query-interval interval
```

```
undo mld-snooping query-interval
```

### Default

The MLD general query interval in a VLAN is 125 seconds.

### Views

VLAN view

### Predefined user roles

network-admin

### Parameters

*interval*: Set an MLD general query interval, in the range of 2 to 31744 seconds.

### Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command for the VLAN.

To avoid mistakenly deleting IPv6 multicast group members, set the MLD general query interval to be greater than the maximum response time for MLD general queries.

### Examples

```
# In VLAN 2, enable MLD snooping, and set the MLD general query interval to 20 seconds.
```

```
<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
```

### Related commands

- **enable** (MLD-snooping view)
- **max-response-time**
- **mld-snooping enable**
- **mld-snooping max-response-time**

- **mld-snooping querier**

## mld-snooping router-aging-time

Use **mld-snooping router-aging-time** to set the aging timer for the dynamic router ports in a VLAN.

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

### Syntax

**mld-snooping router-aging-time** *interval*

**undo mld-snooping router-aging-time**

### Default

The default setting is 260 seconds.

### Views

VLAN view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets an aging timer for the dynamic router ports in a VLAN, in the range of 1 to 8097894 seconds.

### Usage guidelines

You must enable MLD snooping for a VLAN before you configure this command for the VLAN.

This command and the **routing-aging-time** command in MLD-snooping view have the same function but different effective ranges:

- The **routing-aging-time** command in MLD-snooping view takes effect on all VLANs.
- The **mld-snooping router-aging-time** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping router-aging-time** command takes priority over the **routing-aging-time** command in MLD-snooping view.

### Examples

# In VLAN 2, enable MLD snooping, and set the aging timer for the dynamic router ports to 100 seconds.

```
<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
```

### Related commands

- **enable** (MLD-snooping view)
- **mld-snooping enable**
- **router-aging-time** (MLD-snooping view)

## mld-snooping router-port-deny

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.

### Syntax

**mld-snooping router-port-deny** [ **vlan** *vlan-list* ]

**undo mld-snooping router-port-deny** [ **vlan** *vlan-list* ]

### Default

A port can become a dynamic router port.

### Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

### Predefined user roles

network-admin

### Parameters

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you specify VLANs, the command takes effect only when the port belongs to the specified VLANs. If you do not specify a VLAN, the command takes effect on all VLANs.

### Examples

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

## mld-snooping source-deny

Use **mld-snooping source-deny** to enable IPv6 multicast source port filtering on a port to discard all the received IPv6 multicast data packets.

Use **undo mld-snooping source-deny** to disable IPv6 multicast source port filtering on a port.

### Syntax

**mld-snooping source-deny**

**undo mld-snooping source-deny**

### Default

IPv6 multicast source port filtering is disabled, and the port can connect to both IPv6 multicast sources and IPv6 multicast receivers.

### Views

Layer 2 Ethernet interface view

### Predefined user roles

network-admin

## Usage guidelines

This command and the **source-deny** command in MLD-snooping view have the same function but different effective ranges:

- The **source-deny** command in MLD-snooping view takes effect on the specified ports.
- The **mld-snooping source-deny** command takes effect on the current port.

For a port, the **mld-snooping source-deny** command and the **source-deny** command in MLD-snooping view have the same priority, and the most recent configuration takes effect.

## Examples

```
# Enable source port filtering for IPv6 multicast data on Ten-GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mld-snooping source-deny
```

## Related commands

**source-deny** (MLD-snooping view)

# mld-snooping special-query source-ip

Use **mld-snooping special-query source-ip** to configure a source IPv6 address for MLD multicast-address-specific queries.

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

## Syntax

```
mld-snooping special-query source-ip ipv6-address
undo mld-snooping special-query source-ip
```

## Default

If the MLD snooping querier has received MLD general queries, the source IP address of MLD multicast-address-specific queries is the IPv6 address of the MLD general queries. Otherwise, the source IP address is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*ipv6-address*: Specifies a source IPv6 address for MLD multicast-address-specific queries.

## Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command for the VLAN.

## Examples

```
# In VLAN 2, enable MLD snooping, and configure 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
```

### Related commands

- **enable** (MLD-snooping view)
- **mld-snooping enable**

## mld-snooping static-group

Use **mld-snooping static-group** to configure a port as a static member port of an IPv6 multicast group.

Use **undo mld-snooping static-group** to remove the static member port.

### 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 | all }
```

### Default

A port is not a static member port of IPv6 multicast groups.

### Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

### Predefined user roles

network-admin

### Parameters

*ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. The value can be 0::0 or in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where "x" and "y" represent any hexadecimal numbers from 0 to F.

**source-ip** *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you specify an IPv6 multicast source, the command configures the port as a static member port of an IPv6 multicast source and group. If you do not specify an IPv6 multicast source, the command configures the port as a static member port of an IPv6 multicast group. This option takes effect on MLDv2 snooping devices.

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

**all**: Specifies all VLANs.

### Examples

# Configure Ten-GigabitEthernet 1/0/1 as a static member port for the IPv6 multicast source and group (2002::22, FF3E::101) 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 version 2
[Sysname-vlan2] quit
```



```
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] mld-snooping static-group ff3e::101 source-ip
2002::22 vlan 2
```

## mld-snooping static-router-port

Use **mld-snooping static-router-port** to configure a port as a static router port.

Use **undo mld-snooping static-router-port** to remove a static router port.

### Syntax

```
mld-snooping static-router-port vlan vlan-id
undo mld-snooping static-router-port { all | vlan vlan-id }
```

### Default

A port is not a static router port.

### Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

### Predefined user roles

network-admin

### Parameters

**all**: Specifies all VLANs.

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

### Examples

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

## mld-snooping version

Use **mld-snooping version** to specify an MLD snooping version in a VLAN.

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

### Syntax

```
mld-snooping version version-number
undo mld-snooping version
```

### Default

The MLD snooping version in a VLAN is 1.

### Views

VLAN view

### Predefined user roles

network-admin

## Parameters

*version-number*: Specifies an MLD snooping version, 1 or 2.

## Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

This command and the **version** command in MLD-snooping view have the same function but different effective ranges:

- The **version** command in MLD-snooping view takes effect on the specified VLANs.
- The **mld-snooping version** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping version** command and the **version** command in MLD-snooping view have the same priority, and the most recent configuration takes effect.

## Examples

```
# In VLAN 2, enable MLD snooping, and specify MLD snooping version 2.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
```

## Related commands

- **enable** (MLD-snooping view)
- **mld-snooping enable**
- **version** (MLD-snooping view)

# overflow-replace (MLD-snooping view)

Use **overflow-replace** to enable the IPv6 multicast group replacement feature globally.

Use **undo overflow-replace** to disable the IPv6 multicast group replacement feature globally.

## Syntax

```
overflow-replace [ vlan vlan-list ]
```

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

## Default

The IPv6 multicast group replacement feature is disabled globally.

## Views

MLD-snooping view

## Predefined user roles

network-admin

## Parameters

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, the command applies to all VLANs.

## Usage guidelines

This command takes effect only on the IPv6 multicast groups that a port joins dynamically.

This command and the **mld-snooping overflow-replace** command have the same function but different effective ranges:

- The **overflow-replace** command in MLD-snooping view takes effect on all ports.
- The **mld-snooping overflow-replace** command takes effect on the current port.

For a port, the **mld-snooping overflow-replace** command takes priority over the **overflow-replace** command in MLD-snooping view.

## Examples

```
# Enable the IPv6 multicast group replacement feature globally for VLAN 2.
```

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

## Related commands

**mld-snooping overflow-replace**

# report-aggregation (MLD-snooping view)

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

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

## Syntax

**report-aggregation**

**undo report-aggregation**

## Default

MLD report suppression is enabled.

## Views

MLD-snooping view

## Predefined user roles

network-admin

## Examples

```
# Disable MLD report suppression.
```

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] undo report-aggregation
```

# reset mld-snooping group

Use **reset mld-snooping group** to remove the dynamic MLD snooping forwarding entries for IPv6 multicast groups.

## Syntax

**reset mld-snooping group** { *ipv6-group-address* [ *ipv6-source-address* ] | **all** } [ **vlan** *vlan-id* ]

## Views

User view

## Predefined user roles

network-admin

## Parameters

*ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where "x" and "y" represent any hexadecimal numbers from 0 to F.

*ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, the command removes the dynamic MLD snooping forwarding entries for all IPv6 multicast sources.

**all**: Specifies all IPv6 multicast groups.

**vlan** *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, the command removes dynamic MLD snooping forwarding entries for all VLANs.

## Examples

```
# Remove the dynamic MLD snooping forwarding entries for all IPv6 multicast groups.
```

```
<Sysname> reset mld-snooping group all
```

## Related commands

**display mld-snooping group**

# reset mld-snooping router-port

Use **reset mld-snooping router-port** to remove dynamic router ports.

## Syntax

**reset mld-snooping router-port** { **all** | **vlan** *vlan-id* }

## Views

User view

## Predefined user roles

network-admin

## Parameters

**all**: Specifies all dynamic router ports.

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

## Examples

```
# Remove all dynamic router ports.
```

```
<Sysname> reset mld-snooping router-port all
```

## Related commands

**display mld-snooping router-port**

## reset mld-snooping statistics

Use **reset mld-snooping statistics** to clear statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping.

### Syntax

```
reset mld-snooping statistics
```

### Views

User view

### Predefined user roles

network-admin

### Examples

```
# Clear statistics for all MLD messages and IPv6 PIM hello messages learned through MLD snooping.  
<Sysname> reset mld-snooping statistics
```

### Related commands

```
display mld-snooping statistics
```

## router-aging-time (MLD-snooping view)

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

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

### Syntax

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

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

### Default

The global aging timer for dynamic router ports is 260 seconds.

### Views

MLD-snooping view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

### Usage guidelines

This command and the **mld-snooping router-aging-time** command have the same function but different effective ranges:

- The **router-aging-time** command in MLD-snooping view takes effect on all VLANs.
- The **mld-snooping router-aging-time** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping router-aging-time** command takes priority over the **router-aging-time** command in MLD-snooping view.

## Examples

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

## Related commands

**mld-snooping router-aging-time**

# source-deny (MLD-snooping view)

Use **source-deny** to enable IPv6 multicast source port filtering on ports to discard all the received IPv6 multicast data packets.

Use **undo source-deny** to disable IPv6 multicast source port filtering on ports.

## Syntax

**source-deny port** *interface-list*

**undo source-deny port** *interface-list*

## Default

IPv6 multicast source port filtering is disabled, and the ports can connect to both IPv6 multicast sources and IPv6 multicast receivers.

## Views

MLD-snooping view

## Predefined user roles

network-admin

## Parameters

**port** *interface-list*: Specifies a space-separated list of port items. Each item specifies a port by its port type and number or a range of ports in the form of *start-interface-type interface-number to end-interface-type interface-number*.

## Usage guidelines

This command and the **mld-snooping source-deny** command have the same function but different effective ranges:

- The **source-deny** command in MLD-snooping view takes effect on the specified ports.
- The **mld-snooping source-deny** command takes effect on the current port.

For a port, the **mld-snooping source-deny** command and the **source-deny** command in MLD-snooping view have the same priority, and the most recent configuration takes effect.

## Examples

```
# Enable source port filtering for IPv6 multicast data on ports Ten-GigabitEthernet 1/0/1 through
Ten-GigabitEthernet 1/0/4.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] source-deny port ten-gigabitethernet 1/0/1 to ten-gigabitethernet
1/0/4
```

## Related commands

**mld-snooping source-deny**

## version (MLD-snooping view)

Use **version** to specify an MLD snooping version for VLANs.

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

### Syntax

**version** *version-number* **vlan** *vlan-list*

**undo version** **vlan** *vlan-list*

### Default

The MLD snooping version is 1.

### Views

MLD-snooping view

### Predefined user roles

network-admin

### Parameters

*version-number*: Specifies an MLD snooping version, 1 or 2.

**vlan** *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id to end-vlan-id*. The value range for the VLAN ID is 1 to 4094.

### Usage guidelines

You must enable MLD snooping for the specified VLANs before you execute this command.

This command and the **mld-snooping version** command in VLAN view have the same function but different effective ranges:

- The **version** command in MLD-snooping view takes effect on the specified VLANs.
- The **mld-snooping version** command takes effect on the current VLAN.

For a VLAN, the **mld-snooping version** command and the **version** command in MLD-snooping view have the same priority, and the most recent configuration takes effect.

### Examples

# Enable MLD snooping for VLAN 2 through VLAN 10, and specify MLD snooping version 2 for these VLANs.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] enable vlan 2 to 10
[Sysname-mld-snooping] version 2 vlan 2 to 10
```

### Related commands

- **enable** (MLD-snooping view)
- **mld-snooping enable**
- **mld-snooping version**

# IPv6 PIM snooping commands

## display ipv6 pim-snooping neighbor

Use **display ipv6 pim-snooping neighbor** to display IPv6 PIM snooping neighbor information.

### Syntax

```
display ipv6 pim-snooping neighbor [ vlan vlan-id ] [ slot slot-number ] [ verbose ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vlan** *vlan-id*: Specifies a VLAN in the range of 1 to 4094. If you do not specify a VLAN, the command displays information about IPv6 PIM snooping neighbors for all VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays IPv6 PIM snooping neighbor information on the master device.

**verbose**: Displays detailed information. If you do not specify this keyword, the command displays brief information.

### Examples

```
# Display detailed IPv6 PIM snooping neighbor information for VLAN 2.
```

```
<Sysname> display ipv6 pim-snooping neighbor vlan 2 verbose  
Total 2 neighbors.
```

```
VLAN 2: Total 2 neighbors.
```

```
FE80::6401:101
```

```
Slots (0 in total):
```

```
Ports (1 in total):
```

```
XGE1/0/1 (02:02:23) LAN Prune Delay(T)
```

```
FE80::C801:101
```

```
Slots (0 in total):
```

```
Ports (1 in total):
```

```
XGE1/0/2 (00:32:43)
```

### Table 65 Command output

Field	Description
Total 2 neighbors	Total number of IPv6 PIM snooping neighbors.
VLAN 2: Total 2 neighbors	Total number of IPv6 PIM snooping neighbors in VLAN 2.



Field	Description
FE80::6401:101	IP address of the IPv6 PIM snooping neighbor.
Ports (1 in total)	Ports that have IPv6 PIM snooping neighbors, and the total number of the ports.
(02:02:23)	Remaining aging time for an IPv6 PIM snooping neighbor on the port. <ul style="list-style-type: none"> <li>For a global port, this field is always displayed.</li> <li>For a non-global port, this field is displayed if the port is on the master device. Otherwise, you must specify the <b>slot slot-number</b> option to display this field.</li> </ul>
LAN Prune Delay	PIM hello message sent by the IPv6 PIM snooping neighbor has the LAN_Prune_Delay option.
(T)	The join report suppression function has been disabled for the IPv6 PIM snooping neighbor.

## display ipv6 pim-snooping router-port

Use **display ipv6 pim-snooping router-port** to display IPv6 PIM snooping router port information.

### Syntax

**display ipv6 pim-snooping router-port** [ **vlan** *vlan-id* ] [ **slot** *slot-number* ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vlan** *vlan-id*: Specifies a VLAN in the range of 1 to 4094. If you do not specify a VLAN, the command displays information about IPv6 PIM snooping router ports for all VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays IPv6 PIM snooping router port information on the master device.

### Examples

# Display IPv6 PIM snooping router port information for VLAN 2.

```
<Sysname> display ipv6 pim-snooping router-port vlan 2
```

```
VLAN 2:
```

```
Router slots (0 in total):
```

```
Router ports (2 in total):
```

```
  XGE1/0/1                (00:01:30)
```

```
  XGE1/0/2                (00:01:32)
```

### Table 66 Command output

Field	Description
Router ports (2 in total)	Router port and total number.

Field	Description
(00:01:30)	<p>Remaining aging time for the router port.</p> <ul style="list-style-type: none"> <li>For a global port, this field is always displayed.</li> <li>For a non-global port, this field is displayed when the port is on the master device. Otherwise, you must specify the <b>slot slot-number</b> option to display this field.</li> </ul>

## display ipv6 pim-snooping routing-table

Use **display ipv6 pim-snooping routing-table** to display IPv6 PIM snooping routing entries.

### Syntax

```
display ipv6 pim-snooping routing-table [ vlan vlan-id ] [ slot slot-number ] [ verbose ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vlan** *vlan-id*: Specifies a VLAN in the range of 1 to 4094. If you do not specify a VLAN, the command displays IPv6 PIM snooping routing entries for all VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays IPv6 PIM snooping routing entries on the master device.

**verbose**: Displays detailed information. If you do not specify this keyword, the command displays brief information.

### Examples

# Display detailed information about IPv6 PIM snooping routing entries for VLAN 2.

```
<Sysname> display ipv6 pim-snooping routing-table vlan 2 verbose
```

```
Total 1 entries.
```

```
FSM Flag: NI-no info, J-join, PP-prune pending
```

```
VLAN 2: Total 1 entries.
```

```
(2000::1, FF1E::1)
```

```
FSM information: normal
```

```
Upstream neighbor: FE80::101
```

```
Upstream Slots (0 in total):
```

```
Upstream Ports (1 in total):
```

```
  XGE1/0/1
```

```
Downstream Slots (0 in total):
```

```
Downstream Ports (2 in total):
```

```
  XGE1/0/2
```

```
Expires: 00:03:01, FSM: J
```

```
Downstream Neighbors (2 in total):
```

```

1001::1
    Expires: 00:59:19, FSM: J
1001::2
    Expires: 00:59:20, FSM: J
XGE1/0/3
    Expires: 00:02:21, FSM: PP

```

**Table 67 Command output**

Field	Description
Total 1 entries	Total number of (S, G) entries and (*, G) entries.
FSM Flag: NI-no info, J-join, PP-prune pending	State machine flag of the downstream port: <ul style="list-style-type: none"> <li>• <b>NI</b>—Initial state.</li> <li>• <b>J</b>—Join.</li> <li>• <b>PP</b>—Prune pending.</li> </ul>
(2000::1, FF1E::1)	(S, G) entry.
FSM information	Finite state machine information of the entry: <ul style="list-style-type: none"> <li>• <b>delete</b>—The entry attributes have been deleted.</li> <li>• <b>dummy</b>—The entry is a new temporary entry.</li> <li>• <b>no info</b>—No entry exists.</li> <li>• <b>normal</b>—The entry is a correct entry.</li> </ul>
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry.
Upstream Ports (1 in total)	Upstream ports, and the total number of the ports. This field is displayed if the port is on the master device. Otherwise, you must specify the <b>slot slot-number</b> option to display this field.
Downstream Ports (2 in total)	Downstream port of the upstream neighbor, and the total number of the downstream ports.
Downstream Neighbors (2 in total)	Downstream neighbors of the downstream port, and the total number of the downstream neighbors.
Expires: 00:03:01, FSM: J	Remaining aging time for the downstream port or downstream neighbor, and the finite state machine information. <ul style="list-style-type: none"> <li>• For a global port, this field is always displayed.</li> <li>• For a non-global port, this field is displayed if the port is on the master device. Otherwise, you must specify the <b>slot slot-number</b> option to display this field.</li> </ul>

## display ipv6 pim-snooping statistics

Use **display ipv6 pim-snooping statistics** to display statistics for the IPv6 PIM messages learned through IPv6 PIM snooping.

### Syntax

```
display ipv6 pim-snooping statistics
```

### Views

Any view

## Predefined user roles

network-admin  
network-operator

## Examples

```
# Display statistics for the IPv6 PIM messages learned through IPv6 PIM snooping.  
<Sysname> display ipv6 pim-snooping statistics  
Received IPv6 PIM hello: 100  
Received IPv6 PIM join/prune: 100  
Received IPv6 PIM error: 0  
Received IPv6 PIM messages in total: 200
```

**Table 68 Command output**

Field	Description
Received IPv6 PIM hello	Number of received IPv6 PIM hello messages.
Received IPv6 PIM join/prune	Number of received IPv6 PIM join/prune messages.
Received IPv6 PIM error	Number of received IPv6 PIM messages with errors.
Received IPv6 PIM messages in total	Total number of received IPv6 PIM messages.

## Related commands

**reset ipv6 pim-snooping statistics**

# ipv6 pim-snooping enable

Use **ipv6 pim-snooping enable** to enable IPv6 PIM snooping for a VLAN.

Use **undo ipv6 pim-snooping enable** to disable IPv6 PIM snooping for a VLAN.

## Syntax

**ipv6 pim-snooping enable**

**undo ipv6 pim-snooping enable**

## Default

IPv6 PIM snooping is disabled in a VLAN.

## Views

VLAN view

## Predefined user roles

network-admin

## Usage guidelines

You must enable MLD snooping globally and for a VLAN before you execute this command for the VLAN.

IPv6 PIM snooping does not take effect on sub-VLANs of a multicast VLAN.

## Examples

```
# Enable MLD snooping globally, and enable MLD snooping and IPv6 PIM snooping for VLAN 2.
```

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] ipv6 pim-snooping enable
```

### Related commands

- **mld-snooping**
- **mld-snooping enable**

## ipv6 pim-snooping graceful-restart join-aging-time

Use **ipv6 pim-snooping graceful-restart join-aging-time** to set the aging time for IPv6 PIM snooping global downstream ports and global router ports on the new master device in IRF master election.

Use **undo ipv6 pim-snooping graceful-restart join-aging-time** to restore the default.

### Syntax

```
ipv6 pim-snooping graceful-restart join-aging-time interval
undo ipv6 pim-snooping graceful-restart join-aging-time
```

### Default

The default setting is 210 seconds.

### Views

VLAN view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets an aging time in the range of 210 to 18000 seconds.

### Usage guidelines

A global downstream port or a global router port is a Layer 2 aggregate interface that acts as a downstream port or router port.

You must enable IPv6 PIM snooping for a VLAN before you execute this command for the VLAN.

### Examples

# In VLAN 2, set the aging time for IPv6 PIM snooping global downstream ports and global router ports to 600 seconds on the new master device in IRF master election.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] ipv6 pim-snooping enable
[Sysname-vlan2] ipv6 pim-snooping graceful-restart join-aging-time 300
```

## Related commands

**ipv6 pim-snooping enable**

# ipv6 pim-snooping graceful-restart neighbor-aging-time

Use **ipv6 pim-snooping graceful-restart neighbor-aging-time** to set the aging time for IPv6 PIM snooping global neighbor ports on the new master device in IRF master election.

Use **undo ipv6 pim-snooping graceful-restart neighbor-aging-time** to restore the default.

## Syntax

**ipv6 pim-snooping graceful-restart neighbor-aging-time** *interval*

**undo ipv6 pim-snooping graceful-restart neighbor-aging-time**

## Default

The default setting is 105 seconds.

## Views

VLAN view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an aging time in the range of 105 to 18000 seconds.

## Usage guidelines

A global neighbor port is a Layer 2 aggregate interface that acts as a neighbor port.

You must enable IPv6 PIM snooping for a VLAN before you execute this command for the VLAN.

## Examples

# In VLAN 2, set the aging time for IPv6 PIM snooping global neighbor ports to 300 seconds on the new master device in IRF master election.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] ipv6 pim-snooping enable
[Sysname-vlan2] ipv6 pim-snooping graceful-restart neighbor-aging-time 300
```

## Related commands

**ipv6 pim-snooping enable**

# reset ipv6 pim-snooping statistics

Use **reset ipv6 pim-snooping statistics** to clear statistics for the IPv6 PIM messages learned through IPv6 PIM snooping.

## Syntax

**reset ipv6 pim-snooping statistics**

## Views

User view

## Predefined user roles

network-admin

## Examples

# Clear statistics for the IPv6 PIM messages learned through IPv6 PIM snooping.

```
<Sysname> reset ipv6 pim-snooping statistics
```

## Related commands

**display ipv6 pim-snooping statistics**

---

# IPv6 multicast VLAN commands

## display ipv6 multicast-vlan

Use **display ipv6 multicast-vlan** to display information about IPv6 multicast VLANs.

### Syntax

```
display ipv6 multicast-vlan [ vlan-id ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

*vlan-id*: Specifies a VLAN ID in the range of 1 to 4094. If you do not specify a VLAN ID, the command displays information about all IPv6 multicast VLANs.

### Examples

```
# Display information about all IPv6 multicast VLANs.
```

```
<Sysname> display ipv6 multicast-vlan
```

```
Total 2 IPv6 multicast VLANs.
```

```
IPv6 multicast VLAN 100:
```

```
Sub-VLAN list(3 in total):
```

```
2-3, 6
```

```
Port list(3 in total):
```

```
XGE1/0/1
```

```
XGE1/0/2
```

```
XGE1/0/3
```

```
IPv6 multicast VLAN 200:
```

```
Sub-VLAN list(0 in total):
```

```
Port list(0 in total):
```

**Table 69 Command output**

Field	Description
Total 2 IPv6 multicast VLANs	Total number of IPv6 multicast VLANs.
Sub-VLAN list(3 in total)	Sub-VLAN list of the IPv6 multicast VLAN, and the total number of the sub-VLANs.
Port list(3 in total)	Port list of the IPv6 multicast VLAN, and the total number of the ports.



# display ipv6 multicast-vlan group

Use **display ipv6 multicast-vlan group** to display information about IPv6 multicast groups in IPv6 multicast VLANs.

## Syntax

```
display ipv6 multicast-vlan group [ ipv6-source-address | ipv6-group-address | slot slot-number | verbose | vlan vlan-id ] *
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

*ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, the command displays information about IPv6 multicast groups in IPv6 multicast VLANs for all IPv6 multicast sources.

*ipv6-group-address*: Specifies an IPv6 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 numbers from 0 to F. If you do not specify an IPv6 multicast group, the command displays information about all IPv6 multicast groups in IPv6 multicast VLANs.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays information about IPv6 multicast groups in IPv6 multicast VLANs on the master device.

**verbose**: Displays detailed information. If you do not specify this keyword, the command displays brief information.

**vlan** *vlan-id*: Specifies an IPv6 multicast VLAN in the range of 1 to 4094. If you do not specify a multicast VLAN, the command displays information about IPv6 multicast groups in all IPv6 multicast VLANs.

## Examples

```
# Display detailed information about all IPv6 multicast groups in all IPv6 multicast VLANs.
```

```
<Sysname> display ipv6 multicast-vlan group verbose  
Total 6 entries.
```

```
IPv6 multicast VLAN 10: Total 3 entries.
```

```
(2::2, FF0E::2)
```

```
Flags: 0x70000020
```

```
Sub-VLANs (1 in total):
```

```
VLAN 40
```

```
(22::22, FF0E::4)
```

```
Flags: 0x70000030
```

```
Sub-VLANs (1 in total):
```

```
VLAN 40
```

```
(::, FF0E::10)
```

```
Flags: 0x10000030
```

```

Sub-VLANs (1 in total):
    VLAN 40

IPv6 multicast VLAN 20: Total 3 entries.
(2::2, FF0E::2)
  Flags: 0x70000010
  Sub-VLANs (0 in total):
(22::22, FF0E::4)
  Flags: 0x70000010
  Sub-VLANs (0 in total):
(:, FF0E::10)
  Flags: 0x50000010
  Sub-VLANs (0 in total):

```

**Table 70 Command output**

Field	Description
Total 6 entries	Total number of (S, G) entries.
IPv6 multicast VLAN 10: Total 3 entries	Total number of (S, G) in IPv6 multicast VLAN 10.
(:, FFOE::10)	(S, G) entry, where a double colon (::) in the S position means any IPv6 multicast source.
Flags	State of the (S, G) entry. Different bits represent different states of the entry. For values of this field, see <a href="#">Table 71</a> .
Sub-VLANs (1 in total)	Sub-VLAN list of the IPv6 multicast VLAN, and the total number of the sub-VLANs.

**Table 71 Values for the Flags field**

Value	Meaning
0x10	The entry is created by the IPv6 multicast VLAN.
0x20	The entry is created by a sub-VLAN of the IPv6 multicast VLAN.
0x40	The entry is to be deleted.
0x10000000	This value represents one of the following situations: <ul style="list-style-type: none"> <li>The entry is newly created.</li> <li>The device receives an MLD query within an MLD general query interval.</li> </ul>
0x20000000	The device does not receive MLDv1 or MLDv2 reports that match the entry within an MLD general query interval.
0x40000000	The device does not receive MLDv2 IS_EX (NULL) reports that match the entry within an MLD general query interval.

## Related commands

**reset ipv6 multicast-vlan group**

## display ipv6 multicast-vlan forwarding-table

Use **display ipv6 multicast-vlan forwarding-table** to display IPv6 multicast VLAN forwarding entries.

## Syntax

```
display ipv6 multicast-vlan forwarding-table [ ipv6-source-address [ prefix-length ] | ipv6-group-address [ prefix-length ] | slot slot-number | subvlan vlan-id | vlan vlan-id ] *
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

*ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, the command displays IPv6 multicast VLAN forwarding entries for all IPv6 multicast sources.

*prefix-length*: Specifies a prefix length of the IPv6 multicast source address. The value range is 0 to 128 and the default value is 128.

*ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers from 0 to F. If you do not specify an IPv6 multicast group, the command displays information about IPv6 multicast VLAN forwarding entries for all IPv6 multicast groups.

*prefix-length*: Specifies a prefix length of the IPv6 multicast group address. The value range is 8 to 128 and the default value is 128.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays IPv6 multicast VLAN forwarding entries on the master device.

**subvlan** *vlan-id*: Specifies a sub-VLAN by its ID. If you do not specify a sub-VLAN, the command displays IPv6 multicast VLAN forwarding entries for all sub-VLANs.

**vlan** *vlan-id*: Specifies an IPv6 multicast VLAN by its ID in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, the command displays IPv6 multicast VLAN forwarding entries for all IPv6 multicast VLANs.

## Examples

```
# Display all IPv6 multicast VLAN forwarding entries.
```

```
<Sysname> display ipv6 multicast-vlan forwarding-table
IPv6 multicast VLAN 100 Forwarding Table
Total 1 entries, 1 matched

00001. (1::1, FF0E::1)
  Flags: 0x10000
  IPv6 multicast VLAN: 100
  List of sub-VLANs (3 in total):
    1: VLAN 10
    2: VLAN 20
    3: VLAN 30
```

**Table 72 Command output**

Field	Description
IPv6 multicast VLAN 100 Forwarding Table	Forwarding table for IPv6 multicast VLAN 100.
Total 1 entries, 1 matched	Total number of forwarding entries, and the number of matching entries.
00001	Sequence number of the (S, G) entry.
(1::1, FF0E::1)	(S, G) entry, where a double colon (::) in the S position means any IPv6 multicast source.
Flags	Current status of the (S, G) entry. Different bits represent different states of the entry. For values of the field, see <a href="#">Table 73</a> .
List of sub-VLANs (3 in total)	Sub-VLAN list of the IPv6 multicast VLAN, and the total number of the sub-VLANs.

**Table 73 Values of the Flags field**

Value	Meaning
0x1	The entry is in inactive state.
0x4	The entry fails to update.
0x8	The sub-VLAN information fails to update for the entry.
0x200	The entry is in GR state.
0x10000	The entry is a forwarding entry for the IPv6 multicast VLAN.

## ipv6 multicast-vlan

Use **ipv6 multicast-vlan** to configure an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.

Use **undo ipv6 multicast-vlan** to remove an IPv6 multicast VLAN.

### Syntax

```

ipv6 multicast-vlan vlan-id
undo ipv6 multicast-vlan { all | vlan-id }

```

### Default

A VLAN is not configured as an IPv6 multicast VLAN.

### Views

System view

### Predefined user roles

network-admin

### Parameters

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

**all**: Specifies all IPv6 multicast VLANs.

## Usage guidelines

The specified VLAN must exist.

HP recommends not configuring an IPv6 multicast VLAN on a device that is enabled with IPv6 multicast routing.

The total number of IPv6 multicast VLANs on a device must not exceed the system upper limit.

For a sub-VLAN-based IPv6 multicast VLAN, you must enable MLD snooping for the IPv6 multicast VLAN and all its sub-VLANs. For a port-based IPv6 multicast VLAN, you must enable MLD snooping for the IPv6 multicast VLAN and all user VLANs to which the user ports are connected.

## Examples

# Enable MLD snooping for VLAN 100. Configure VLAN 100 as an IPv6 multicast VLAN and enter its view.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 100
[Sysname-vlan100] mld-snooping enable
[Sysname-vlan100] quit
[Sysname] ipv6 multicast-vlan 100
[Sysname-ipv6-mvlan-100]
```

## Related commands

- **mld-snooping enable**
- **ipv6 multicast routing**

# ipv6 multicast-vlan entry-limit

Use **ipv6 multicast-vlan entry-limit** to set the maximum number of IPv6 multicast VLAN forwarding entries.

Use **undo ipv6 multicast-vlan entry-limit** to restore the default.

## Syntax

```
ipv6 multicast-vlan entry-limit limit
undo ipv6 multicast-vlan entry-limit
```

## Default

The setting is 4000.

## Views

System view

## Predefined user roles

network-admin

## Parameters

*limit*: Sets the maximum number of IPv6 multicast VLAN forwarding entries, in the range of 0 to 4000.

## Examples

# Set the maximum number of IPv6 multicast VLAN forwarding entries to 256.

```
<Sysname> system-view
[Sysname] ipv6 multicast-vlan entry-limit 256
```

## Related commands

**entry-limit** (MLD-snooping view)

# ipv6 port multicast-vlan

Use **ipv6 port multicast-vlan** to assign a port to an IPv6 multicast VLAN.

Use **undo ipv6 port multicast-vlan** to restore the default.

## Syntax

```
ipv6 port multicast-vlan vlan-id
undo ipv6 port multicast-vlan
```

## Default

A port does not belong to IPv6 multicast VLANs.

## Views

Ethernet interface view, Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Parameters

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

## Usage guidelines

A port can belong to only one IPv6 multicast VLAN.

## Examples

```
# Assign Ten-GigabitEthernet 1/0/1 to IPv6 multicast VLAN 100.
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] ipv6 port multicast-vlan 100
```

# port (IPv6 multicast VLAN view)

Use **port** to assign user ports to an IPv6 multicast VLAN.

Use **undo port** to remove user ports from the IPv6 multicast VLAN.

## Syntax

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

## Default

An IPv6 multicast VLAN does not have user ports.

## Views

IPv6 multicast VLAN view

## Predefined user roles

network-admin

## Parameters

*interface-list*: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number to interface-type interface-number*.

**all**: Specifies all user ports in the current IPv6 multicast VLAN.

## Usage guidelines

A port can belong to only one IPv6 multicast VLAN.

You can assign Ethernet interfaces and Layer 2 aggregate interfaces as user ports to an IPv6 multicast VLAN.

## Examples

```
# Assign Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/5 to IPv6 multicast VLAN 100.
<Sysname> system-view
[Sysname] ipv6 multicast-vlan 100
[Sysname-ipv6-mvlan-100] port ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/5
```

# reset ipv6 multicast-vlan group

Use **reset ipv6 multicast-vlan group** to clear IPv6 multicast groups in IPv6 multicast VLANs.

## Syntax

```
reset ipv6 multicast-vlan group [ ipv6-group-address [ prefix-length ] | ipv6-source-address [ prefix-length ] | vlan vlan-id ] *
```

## Views

User view

## Predefined user roles

network-admin

## Parameters

*ipv6-group-address*: Specifies an IPv6 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 numbers from 0 to F. If you do not specify an IPv6 multicast group, the command clears all IPv6 multicast groups in IPv6 multicast VLANs.

*prefix-length*: Specifies a prefix length of the IPv6 multicast group address. The value range is 8 to 128 and the default value is 128.

*ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, the command clears IPv6 multicast groups for all IPv6 multicast sources in IPv6 multicast VLANs.

*prefix-length*: Specifies a prefix length of the IPv6 multicast source address. The value range is 0 to 128 and the default value is 128.

**vlan** *vlan-id*: Specifies an IPv6 multicast VLAN in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, the command clears IPv6 multicast groups in all IPv6 multicast VLANs.

## Examples

```
# Clear all IPv6 multicast groups in all IPv6 multicast VLANs.  
<Sysname> reset ipv6 multicast-vlan group
```

## Related commands

**display ipv6 multicast-vlan group**

# subvlan (IPv6 multicast VLAN view)

Use **subvlan** to assign sub-VLANs to an IPv6 multicast VLAN.

Use **undo subvlan** to remove sub-VLANs from an IPv6 multicast VLAN.

## Syntax

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

## Default

An IPv6 multicast VLAN does not have sub-VLANs.

## Views

IPv6 multicast VLAN view

## Predefined user roles

network-admin

## Parameters

*vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The value range for the VLAN ID is 1 to 4094.

**all**: Specifies all sub-VLANs of the current IPv6 multicast VLAN.

## Usage guidelines

The VLANs to be configured as sub-VLANs must exist and must not be IPv6 multicast VLANs or sub-VLANs of any other IPv6 multicast VLANs.

## Examples

```
# Configure VLAN 10 through VLAN 15 as sub-VLANs of multicast VLAN 100.  
<Sysname> system-view  
[Sysname] ipv6 multicast-vlan 100  
[Sysname-ipv6-mvlan-100] subvlan 10 to 15
```



---

# IPv6 multicast routing and forwarding commands

The term "interface" in this chapter collectively refers to 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 ipv6 mrib interface

Use **display ipv6 mrib interface** to display information about interfaces maintained by the IPv6 MRIB, including IPv6 PIM interfaces, MLD interfaces, register interfaces, InLoopBack0 interfaces, and null0 interfaces.

### Syntax

```
display ipv6 mrib [ vpn-instance vpn-instance-name ] interface [ interface-type interface-number ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays information about interfaces maintained by the IPv6 MRIB on the public network.

*interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays information about all interfaces maintained by the IPv6 MRIB.

### Examples

# Display information about all interfaces maintained by the IPv6 MRIB on the public network.

```
<Sysname> display ipv6 mrib interface
Interface: Vlan-interfaces1
  Index: 0x00000001
  Current state: up
  MTU: 1500
  Type: BROADCAST
  Protocol: PIM-DM
  PIM protocol state: Enabled
  Address list:
    1. Local address : FE80:7:11::1/10
       Remote address: ::
       Reference      : 1
       State          : NORMAL
```

**Table 74 Command output**

Field	Description
Interface	Interface name.
Index	Index number of the interface.
Current state	Current status of the interface: up or down.
MTU	MTU value.
Type	Interface type: <ul style="list-style-type: none"> <li>• <b>BROADCAST</b>—Broadcast link interface.</li> <li>• <b>LOOP</b>—Loopback interface.</li> <li>• <b>REGISTER</b>—Register interface.</li> <li>• <b>NBMA</b>—NBMA interface.</li> <li>• <b>MTUNNEL</b>—Multicast tunnel interface.</li> </ul>
Protocol	Protocol running on the interface: PIM-DM, PIM-SM, or MLD.
PIM protocol state	Whether IPv6 PIM is enabled: <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
Address list	Interface address list.
Local address	Local IP address.
Remote address	Remote end IP address. This field is displayed when the interface is vlink type.
Reference	Number of times that the address has been referenced.
State	Status of the interface address: NORMAL or DEL.

## display ipv6 multicast boundary

Use **display ipv6 multicast boundary** to display IPv6 multicast boundary information.

### Syntax

```
display ipv6 multicast [ vpn-instance vpn-instance-name ] boundary { group [ ipv6-group-address [ prefix-length ] ] | scope [ scope-id ] } [ interface interface-type interface-number ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays IPv6 multicast boundary information on the public network.

**group**: Displays the IPv6 multicast boundary information for the specified group.

*ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers from 0 to F. If you do not specify an IPv6 multicast group, the command displays the IPv6 multicast boundary information of all IPv6 multicast groups.

*prefix-length*: Specifies an address prefix length 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 an admin-scope zone by its ID in the range of 3 to 15, which is identified by the scope field in the IPv6 multicast group address. If you do not specify an admin-scoped zone, the command displays the IPv6 multicast boundary information of all IPv6 admin-scope zones.

**interface** *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays IPv6 multicast boundary information on all interfaces.

## Examples

# Display the IPv6 multicast boundary information of all IPv6 multicast groups on all interfaces on the public network.

```
<Sysname> display ipv6 multicast boundary group
Boundary                                     Interface
FF1E::/64                                   Vlan1
```

# Display IPv6 multicast boundary information in all IPv6 admin-scope zones on all interfaces on the public network.

```
<Sysname> display ipv6 multicast boundary scope
Boundary      Interface
              3          Vlan-interface1
```

**Table 75 Command output**

Field	Description
Boundary	IPv6 multicast group or IPv6 admin-scope zone that corresponds to the IPv6 multicast boundary.
Interface	Boundary interface that corresponds to the IPv6 multicast boundary.

## Related commands

**ipv6 multicast boundary**

# display ipv6 multicast forwarding df-info

Use **display ipv6 multicast forwarding df-info** to display information about the DF for IPv6 multicast forwarding.

## Syntax

```
display ipv6 multicast [ vpn-instance vpn-instance-name ] forwarding df-info [ ipv6-rp-address ]
[ verbose ] [ slot slot-number ]
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays information about the DF for IPv6 multicast forwarding on the public network.

*ipv6-rp-address*: Specifies an RP of IPv6 BIDIR-PIM by its IPv6 address.

**verbose**: Displays detailed information. If you do not specify this keyword, the command displays brief information.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays information about the DF for IPv6 multicast forwarding on the master device.

## Usage guidelines

The router that acts as a DF is the only IPv6 multicast data forwarder to the RP in an IPv6 BIDIR-PIM domain.

## Examples

# Display brief information about the DF for IPv6 multicast forwarding on the public network.

```
<Sysname> display ipv6 multicast forwarding df-info  
Total 1 RP, 1 matched
```

```
00001. RP address: 7:11::1  
  Flags: 0x0  
  Uptime: 01:46:40  
  RPF interface: Vlan-interface1  
  List of 1 DF interface:  
    1: Vlan-interface2
```

# Display detailed information about the DF for IPv6 multicast forwarding on the public network.

```
<Sysname> display ipv6 multicast forwarding df-info verbose  
Total 1 RP, 1 matched
```

```
00001. RP address: 7:11::1  
  MID: 2, Flags: 0x0  
  Uptime: 00:03:53  
  Product information: 0x7a2f762f, 0x718fee9f, 0x4b82f137, 0x71c32184  
  RPF interface: Vlan-interface1  
  Product information: 0xa567d6fc, 0xadeb03e3  
  Tunnel information: 0xdfb107d4, 0x7aa5d510  
  List of 1 DF interface:  
    1: Vlan-interface2  
      Product information: 0xa986152b, 0xb74a9a2f  
      Tunnel information: 0x297ca208, 0x76985b89
```

**Table 76 Command output**

Field	Description
Total 1 RP, 1 matched	Total number of RPs and total number of matched RPs.

Field	Description
00001	Sequence number of the entry to which the RP is designated.
MID	ID of the entry to which the RP is designated. Each entry to which the RP is designated has a unique MID.
Flags	Current state of the entry to which the RP is designated. Different bits represent different states of the entry. For values of this field, see <a href="#">Table 77</a> .
Uptime	Existence duration for the entry to which the RP is designated.
RPF interface	RPF interface to the RP.
List of 1 DF interface	DF interface list.

**Table 77 Values of the Flags field**

Value	Description
0x0	The entry is in correct state.
0x4	The entry fails to update.
0x8	The DF interface information fails to update for the entry.
0x40	The entry is to be deleted.
0x100	The entry is being deleted.
0x200	The entry is in GR state.

## display ipv6 multicast forwarding event

Use **display ipv6 multicast forwarding event** to display statistics for IPv6 multicast forwarding events.

### Syntax

```
display ipv6 multicast [ vpn-instance vpn-instance-name ] forwarding event [ slot slot-number ]
```

### Views

Any view

### Predefined user roles

network-admin  
network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays statistics for the IPv6 multicast forwarding events on the public network.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays statistics for the IPv6 multicast forwarding events on the master device.

### Examples

```
# Display statistics for the IPv6 multicast forwarding events on the public network.
<Sysname> display ipv6 multicast forwarding event
```

```

Total entry active event sent: 0
Total entry inactive event sent: 0
Total NoCache event sent: 2
Total NoCache event dropped: 0
Total WrongIF event sent: 0
Total WrongIF event dropped: 0
Total SPT switch event sent: 0
NoCache rate limit: 1024 packets/s
WrongIF rate limit: 1 packets/10s
Total timer of register suppress timeout: 0

```

**Table 78 Command output**

Field	Description
Total entry active event sent	Number of times that the entry-active event has been sent.
Total entry inactive event sent	Number of times that the entry-inactive event has been sent.
Total NoCache event sent	Number of times that the NoCache event has been sent.
Total NoCache event dropped	Number of times that the NoCache event has been dropped.
Total WrongIF event sent	Number of times that the WrongIF event has been sent.
Total WrongIF event dropped	Number of times that the WrongIF event has been dropped.
Total SPT switch event sent	Number of times that the SPT-switch event has been sent.
NoCache rate limit	Rate limit for sending the NoCache event, in pps.
WrongIF rate limit	Rate limit for sending the WrongIF event, in packets per 10 seconds.
Total timer of register suppress timeout	Number of times that the registration suppression has timed out in total.

## Related commands

**reset ipv6 multicast forwarding event**

# display ipv6 multicast forwarding-table

Use **display ipv6 multicast forwarding-table** to display IPv6 multicast forwarding entries.

## Syntax

```

display ipv6 multicast [ vpn-instance vpn-instance-name ] forwarding-table [ ipv6-source-address
[ prefix-length ] | ipv6-group-address [ prefix-length ] | incoming-interface interface-type
interface-number | outgoing-interface { exclude | include | match } interface-type interface-number |
slot slot-number | statistics ] *

```

## Views

Any view

## Predefined user roles

network-admin  
network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays IPv6 multicast forwarding entries on the public network.

*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 numbers from 0 to F.

*prefix-length*: Specifies an address prefix length. The default value is 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. For an IPv6 multicast source address, the value range for this argument is 0 to 128.

**incoming-interface**: Specifies the IPv6 forwarding entries that contain the specified incoming interface.

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

**outgoing-interface**: Specifies the IPv6 forwarding entries that contain the specified outgoing interface.

**exclude**: Specifies the IPv6 forwarding entries that do not contain the specified interface in the outgoing interface list.

**include**: Specifies the IPv6 forwarding entries that contain the specified interface in the outgoing interface list.

**match**: Specifies the IPv6 forwarding entries that contain only the specified interface in the outgoing interface list.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays IPv6 multicast forwarding entries on the master device.

**statistics**: Displays statistics for the IPv6 multicast forwarding entries.

## Examples

# Display IPv6 multicast forwarding entries on the public network.

```
<Sysname> display ipv6 multicast forwarding-table
Total 1 entry, 1 matched

00001. (1::1, ff0e::1)
  Flags: 0x0
  Uptime: 00:08:32, Timeout in: 00:03:26
  Incoming interface: Vlan-interface10
    Incoming sub-VLAN: VLAN 11
    Outgoing sub-VLAN: VLAN 12
                      VLAN 13
  List of 1 outgoing interface:
    1: Vlan-interface20
      Sub-VLAN: VLAN 21
              VLAN 22
  Matched 19648 packets(20512512 bytes), Wrong If 0 packet
  Forwarded 19648 packets(20512512 bytes)
```

**Table 79 Command output**

<b>Field</b>	<b>Description</b>
Total 1 entry, 1 matched	Total number of (S, G) entries, and the total number of matched (S, G) entries.
00001	Sequence number of the (S, G) entry.
(1::1, ff0e::1)	(S, G) entry in the IPv6 multicast forwarding table.
Flags	Current state of the (S, G) entry. Different bits represent different states of the (S, G) entry. For values of this field, see <a href="#">Table 80</a> .
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.
Incoming sub-VLAN	Incoming sub-VLAN of the super VLAN when the incoming interface of the (S, G) entry is the VLAN interface of this super VLAN.
Outgoing sub-VLAN	Outgoing sub-VLAN of the super VLAN when the incoming interface of the (S, G) entry is the VLAN interface of this super VLAN.
List of 1 outgoing interfaces	Outgoing interface list of the (S, G) entry.
Sub-VLAN	Outgoing sub-VLAN of the super VLAN when the outgoing interface of the (S, G) entry is the VLAN interface of this super VLAN.
Matched 19648 packets (20512512 bytes), Wrong If 0 packet	Number of packets (bytes) that match the (S, G) entry, and the number of packets with incoming interface errors.
Forwarded 19648 packets (20512512 bytes)	Number of packets (bytes) that have been forwarded.

**Table 80 Value of the Flags field**

<b>Value</b>	<b>Meaning</b>
0x0	The entry is in correct state.
0x1	The entry is in inactive state.
0x2	The entry is null.
0x4	The entry fails to update.
0x8	The outgoing interface information fails to update for the (S, G) entry.
0x20	A register outgoing interface is available.
0x40	The entry is to be deleted.
0x80	The entry is in registration suppression state.
0x100	The entry is being deleted.
0x200	The entry is in GR state.
0x400	The entry has the VLAN interface of the super VLAN.
0x800	The entry has the associated ND entry of the IPv6 multicast source address.



Value	Meaning
0x20000000	The entry is an IPv6 BIDIR-PIM entry.

## Related commands

**reset ipv6 multicast forwarding-table**

# display ipv6 multicast forwarding-table df-list

Use **display ipv6 multicast forwarding-table df-list** to display information about the DF list in the IPv6 multicast forwarding table.

## Syntax

```
display ipv6 multicast [ vpn-instance vpn-instance-name ] forwarding-table df-list [ ipv6-group-address ]
[ verbose ] [ slot slot-number ]
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays information about the DF list in the IPv6 multicast forwarding table on the public network.

*ipv6-group-address*: Specifies an IPv6 multicast address, in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers from 0 to F.

**verbose**: Displays detailed information. If you do not specify this keyword, the command displays brief information.

**slot** *slot-number*: Specifies an IRF member device by its member ID or a PEX by its virtual slot number. If you do not specify this option, the command displays information about the DF list in the IPv6 multicast forwarding table on the master device.

## Examples

# Display brief information about the DF list in the IPv6 multicast forwarding table on the public network.

```
<Sysname> display ipv6 multicast forwarding-table df-list
Total 1 entry, 1 matched
```

```
00001. (::, FF1E::1)
  List of 1 DF interface:
    1: Vlan-interface1
```

# Display detailed information about the DF list in the IPv6 multicast forwarding table on the public network.

```
<Sysname> display ipv6 multicast forwarding-table df-list verbose
Total 1 entry, 1 matched
```

```

00001. (::, FF1E::1)
  List of 1 DF interface:
    1: Vlan-interfaces
      Product information: 0x347849f6, 0x14bd6837
      Tunnel information: 0xc4857986, 0x128a9c8f

```

**Table 81 Command output**

Field	Description
Total 1 entry, 1 matched	Total number of entries, and the total number of matching entries.
00001	Sequence number of the entry.
(::, FF1E::1)	(*, G) entry.
List of 1 DF interface	DF interface list.

## display ipv6 multicast routing-table

Use **display ipv6 multicast routing-table** to display IPv6 multicast routing entries.

### Syntax

```

display ipv6 multicast [ vpn-instance vpn-instance-name ] routing-table [ ipv6-source-address
[ prefix-length ] | ipv6-group-address [ prefix-length ] | incoming-interface interface-type
interface-number | outgoing-interface { exclude | include | match } interface-type interface-number ] *

```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays IPv6 multicast routing entries on the public network.

*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 numbers from 0 to F.

*prefix-length*: Specifies an address prefix length. The default is 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. For an IPv6 multicast source address, the value range for this argument is 0 to 128.

**incoming-interface**: Displays the IPv6 routing entries that contain the specified incoming interface.

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

**outgoing-interface**: Displays the IPv6 routing entries that contain the specified outgoing interface.

**exclude**: Displays the IPv6 routing entries that do not contain the specified interface in the outgoing interface list.

**include**: Displays the IPv6 routing entries that contain the specified interface in the outgoing interface list.

**match:** Displays the IPv6 routing entries that contain only the specified interface in the outgoing interface list.

## Usage guidelines

IPv6 multicast routing tables are the basis of IPv6 multicast forwarding. You can display the establishment state of an (S, G) entry by examining the IPv6 multicast routing table.

## Examples

```
# Display IPv6 multicast routing entries on the public network.
```

```
<Sysname> display ipv6 multicast routing-table
Total 1 entry

00001. (2001::2, FFE3::101)
  Uptime: 00:00:14
  Upstream Interface: Vlan-interface1
  List of 2 downstream interfaces
    1: Vlan-interface2
    2: Vlan-interface3
```

**Table 82 Command output**

Field	Description
Total 1 entry	Total number of (S, G) entries.
00001	Sequence number of the (S, G) entry.
(2001::2, FFE3::101)	(S, G) entry.
Uptime	Length of time for which the (S, G) entry has been up.
Upstream Interface	Upstream interface at which the (S, G) packets should arrive.
List of 2 downstream interfaces	List of downstream interface lists that need to forward (S, G) packets.

## Related commands

**reset ipv6 multicast routing-table**

# display ipv6 multicast rpf-info

Use **display ipv6 multicast rpf-info** to display RPF information for IPv6 multicast sources.

## Syntax

```
display ipv6 multicast [ vpn-instance vpn-instance-name ] rpf-info ipv6-source-address
[ ipv6-group-address ]
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays RPF information for IPv6 multicast sources on the public network.

*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 numbers from 0 to F.

## Examples

# Display all RPF information of the multicast source with an IPv6 address 2001::101 on the public network.

```
<Sysname> display ipv6 multicast rpf-info 2001::101
RPF information about source 2001::101:
  RPF interface: Vlan-interface1, RPF neighbor: FE80::A01:101:1
  Referenced prefix/prefix length: 2001::/64
  Referenced route type: igp
  Route selection rule: preference-preferred
  Load splitting rule: disable
```

**Table 83 Command output**

Field	Description
RPF information about source 2001::101	RPF information of the IPv6 multicast source 2001::101.
RPF interface	Type and number of the RPF interface.
RPF neighbor	IPv6 address (link-local address) of the RPF neighbor.
Referenced prefix/prefix length	Referenced route and its prefix length.
Referenced route type	Type of the referenced route: <ul style="list-style-type: none"><li>• <b>igp</b>—IPv6 IGP unicast route.</li><li>• <b>egp</b>—IPv6 EGP unicast route.</li><li>• <b>unicast (direct)</b>—IPv6 directly connected unicast route.</li><li>• <b>unicast</b>—Other IPv6 unicast route, such as IPv6 unicast static route.</li></ul>
Route selection rule	RPF route selection rule: <ul style="list-style-type: none"><li>• Route preference.</li><li>• Longest prefix match.</li></ul>
Load splitting rule	Whether the load splitting feature is enabled.

## Related commands

- **display ipv6 multicast forwarding-table**
- **display ipv6 multicast routing-table**

## ipv6 multicast boundary

Use **ipv6 multicast boundary** to configure an IPv6 multicast forwarding boundary.

Use **undo ipv6 multicast boundary** to delete the specified IPv6 multicast forwarding boundary.

## Syntax

```
ipv6 multicast boundary { ipv6-group-address prefix-length | scope { scope-id | admin-local | global | organization-local | site-local } }
```

```
undo ipv6 multicast boundary { ipv6-group-address prefix-length | all | scope { scope-id | admin-local | global | organization-local | site-local } }
```

## Default

No IPv6 multicast forwarding boundary is configured.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*ipv6-group-address*: Specifies an IPv6 multicast group address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers from 0 to F.

*prefix-length*: Specifies an address prefix length in the range of 8 to 128.

**all**: Specifies all IPv6 multicast boundaries configured on the interface.

*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.

## Usage guidelines

You do not need to enable IPv6 multicast routing before executing this command.

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 IPv6 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.

## 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] ipv6 multicast 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] ipv6 multicast boundary scope 4
```

## Related commands

**display ipv6 multicast boundary**

# ipv6 multicast forwarding supervlan community

Use **ipv6 multicast forwarding supervlan community** to configure IPv6 multicast forwarding among sub-VLANs of a super VLAN.

Use **undo ipv6 multicast forwarding supervlan community** to restore the default.

## Syntax

**ipv6 multicast forwarding supervlan community**

**undo ipv6 multicast forwarding supervlan community**

## Default

Multicast data cannot be forwarded among sub-VLANs of the super VLAN.

## Views

VLAN interface view

## Predefined user roles

network-admin

## Usage guidelines

After you execute the **ipv6 multicast forwarding supervlan community** command, you must clear all IPv6 multicast forwarding entries with the super VLAN interface as the incoming interface. Otherwise, this command cannot take effect. To clear the required multicast forwarding entries, use the **reset ipv6 multicast forwarding-table** command.

## Examples

```
# Configure multicast forwarding among sub-VLANs of the super VLAN 2.
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 multicast forwarding supervlan community
```

## Related commands

**reset ipv6 multicast forwarding-table**

# ipv6 multicast routing

Use **ipv6 multicast routing** to enable IPv6 multicast routing and enter IPv6 MRIB view.

Use **undo ipv6 multicast routing** to disable IPv6 multicast routing.

## Syntax

```
ipv6 multicast routing [ vpn-instance vpn-instance-name ]  
undo ipv6 multicast routing [ vpn-instance vpn-instance-name ]
```

## Default

IPv6 multicast routing is disabled.

## Views

System view

## Predefined user roles

network-admin

## parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command enables IPv6 multicast routing on the public network.

## Usage guidelines

Other Layer 3 IPv6 multicast commands take effect only when IPv6 multicast routing is enabled.

The switch does not forward IPv6 multicast packets before IPv6 multicast routing is enabled.

## Examples

```
# Enable IPv6 multicast routing and enter IPv6 MRIB view on the public network.  
<Sysname> system-view  
[Sysname] ipv6 multicast routing  
[Sysname-mrib6]  
  
# Enable IPv6 multicast routing and enter IPv6 MRIB view in the VPN instance mvpn.  
<Sysname> system-view  
[Sysname] ipv6 multicast routing vpn-instance mvpn  
[Sysname-mrib6-mvpn]
```

# load-splitting (IPv6 MRIB view)

Use **load-splitting** to enable load splitting of IPv6 multicast traffic.

Use **multicast load-splitting** to restore the default.

## Syntax

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

## Default

Load splitting of IPv6 multicast traffic is disabled.

## Views

IPv6 MRIB view

## Predefined user roles

network-admin

## Parameters

**source**: Specifies IPv6 multicast load splitting on a per-source basis.

**source-group**: Specifies IPv6 multicast load splitting on a per-source basis and on a per-group basis.

## Usage guidelines

This command does not take effect on IPv6 BIDIR-PIM.

## Examples

```
# Enable load splitting of IPv6 multicast traffic on a per-source basis on the public network.
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib6] load-splitting source
```

# longest-match (IPv6 MRIB view)

Use **longest-match** to specify the longest prefix match principle for RPF route selection.

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

## Syntax

**longest-match**

**undo longest-match**

## Default

Route preference is used for RPF route selection.

## Views

IPv6 MRIB view

## Predefined user roles

network-admin

## Examples

```
# Specify the longest prefix match principle for RPF route selection on the public network.
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib6] longest-match
```

# reset ipv6 multicast forwarding event

Use **reset ipv6 multicast forwarding event** to clear statistics for IPv6 multicast forwarding events.

## Syntax

**reset ipv6 multicast** [ **vpn-instance** *vpn-instance-name* ] **forwarding event**

## Views

User view

## Predefined user roles

network-admin



## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command clears statistics for the IPv6 multicast forwarding events on the public network.

## Examples

```
# Clear statistics for the IPv6 multicast forwarding events on the public network.  
<Sysname> reset ipv6 multicast forwarding event
```

## Related commands

**display ipv6 multicast forwarding event**

# reset ipv6 multicast forwarding-table

Use **reset ipv6 multicast forwarding-table** to clear IPv6 multicast forwarding entries.

## Syntax

```
reset ipv6 multicast [ vpn-instance vpn-instance-name ] forwarding-table { { ipv6-source-address [ prefix-length ] | ipv6-group-address [ prefix-length ] | incoming-interface { interface-type interface-number } } * | all }
```

## Views

User view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command clears IPv6 multicast forwarding entries on the public network.

*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 numbers from 0 to F.

*prefix-length*: Specifies an address prefix length. The default value is 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. For an IPv6 multicast source address, the value range for this argument is 0 to 128.

**incoming-interface**: Specifies the IPv6 multicast forwarding entries that contain the specified incoming interface.

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

**all**: Specifies all forwarding entries in the IPv6 multicast forwarding entries.

## Usage guidelines

When a forwarding entry is deleted from the IPv6 multicast forwarding table, the associated routing entry is also deleted from the IPv6 multicast routing table.

## Examples

```
# On the public network, clear the IPv6 multicast forwarding entry for the IPv6 multicast group FFOE::1 from the IPv6 multicast forwarding table.
```

```
<Sysname> reset ipv6 multicast forwarding-table ff0e::1
```

## Related commands

**display ipv6 multicast forwarding-table**

# reset ipv6 multicast routing-table

Use **reset ipv6 multicast routing-table** to clear IPv6 multicast routing entries.

## Syntax

```
reset ipv6 multicast [ vpn-instance vpn-instance-name ] routing-table { { ipv6-source-address [ prefix-length ] | ipv6-group-address [ prefix-length ] | incoming-interface interface-type interface-number } * | all }
```

## Views

User view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command clears IPv6 multicast routing entries on the public network.

*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 numbers from 0 to F.

*prefix-length*: Specifies an address prefix length. The default is 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. For an IPv6 multicast source address, the value range for this argument is 0 to 128.

**incoming-interface**: Specifies the IPv6 multicast routing entries that contain the specified incoming interface.

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

**all**: Specifies all IPv6 multicast routing entries.

## Usage guidelines

When a routing entry is deleted from the IPv6 multicast routing table, the associated forwarding entry is also deleted from the IPv6 multicast forwarding table.

## Examples

```
# Clear the routing entry for the IPv6 multicast group FF03::101 from the IPv6 multicast routing table on the public network.
```

```
<Sysname> reset ipv6 multicast routing-table ff03::101
```

## Related commands

**display ipv6 multicast routing-table**

---

# MLD commands

The term "interface" in this chapter collectively refers to 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

Use **display mld group** to display MLD information for IPv6 multicast groups.

### Syntax

```
display mld [ vpn-instance vpn-instance-name ] group [ ipv6-group-address | interface interface-type interface-number ] [ static | verbose ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays MLD information for IPv6 multicast groups on the public network.

*ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where "x" and "y" represent any hexadecimal numbers from 0 to F. If you do not specify an IPv6 multicast source, the command displays MLD information for all IPv6 multicast groups.

**interface** *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays MLD information for IPv6 multicast groups on all interfaces.

**static**: Specifies MLD information for IPv6 multicast groups that interfaces joined statically. If you do not specify this keyword, the command displays MLD information for IPv6 multicast groups that interfaces joined dynamically.

**verbose**: Displays detailed MLD information.

### Examples

```
# Display MLD information for all IPv6 multicast groups that interfaces dynamically joined on the public network.
```

```
<Sysname> display mld group
MLD groups in total: 1
Vlan-interface1(FE80::101):
  MLD groups reported in total: 1
  Group address: FF03::101
  Last reporter: FE80::10
  Uptime: 00:02:04
```

Expires: 00:01:15

**Figure 1 Command output**

Field	Description
MLD groups in total	Total number of IPv6 multicast groups.
MLD groups reported in total	Total number of IPv6 multicast groups that the interface has joined dynamically.
Group address	IPv6 multicast group address.
Last reporter	IPv6 address of the receiver host that last reported membership for the group.
Uptime	Length of time since the IPv6 multicast group was joined.
Expires	Remaining lifetime for the IPv6 multicast group. If the timer is disabled, this field displays <b>Off</b> .

# Display detailed MLD information for the IPv6 multicast group FF03::101 that interfaces dynamically joined on the public network. In this example, MLDv2 is running.

```
<Sysname> display mld group ff03::101 verbose
Vlan-interface1(FE80::101):
  MLD groups reported in total: 1
  Group: FF03::101
  Uptime: 00:01:46
  Expires: Off
  Last reporter: FE80::10
  Last-listener-query-counter: 0
  Last-listener-query-timer-expiry: Off
  Group mode: Exclude
  Version1-host-present-timer-expiry: Off
  Source list (sources in total: 1):
    Source: 10::10
      Uptime: 00:00:09
      Expires: 00:04:11
      Last-listener-query-counter: 0
      Last-listener-query-timer-expiry: Off
```

**Table 84 Command output**

Field	Description
MLD groups reported in total	Total number of IPv6 multicast groups that the interface joined dynamically.
Group	IPv6 multicast group address.
Uptime	Length of time since the IPv6 multicast group was joined.
Expires	Remaining time for the IPv6 multicast group. If the timer is disabled, this field displays <b>Off</b> .
Last reporter	IPv6 address of the host that last reported membership for this group.

Field	Description
Last-listener-query-counter	Number of multicast-address-specific queries or multicast-address-and-source-specific queries sent for this group.
Last-listener-query-timer-expiry	Remaining time for the MLD last listener of the multicast group. If the timer is disabled, this field displays <b>Off</b> .
Group mode	Multicast source filtering mode: <ul style="list-style-type: none"> <li>• <b>Include</b>—Include mode.</li> <li>• <b>Exclude</b>—Exclude mode.</li> </ul> This field is displayed only when the switch runs MLDv2.
Version1-host-present-timer-expiry	Remaining time for the MLDv1 host present timer. If the timer is disabled, this field displays <b>Off</b> .
Source list (sources in total )	List of IPv6 multicast sources and total number of IPv6 multicast sources. This field is displayed only when the switch runs MLDv2.
Source	IPv6 multicast source address. This field is displayed only when the switch runs MLDv2.
Uptime	Length of time since the IPv6 multicast source was reported. This field is displayed only when the switch runs MLDv2.
Expires	Remaining time for the IPv6 multicast source. If the timer is disabled, this field displays <b>Off</b> . This field is displayed only when the switch runs MLDv2.
Last-listener-query-counter	Number of multicast-address-specific queries or multicast-address-and-source-specific queries sent for this IPv6 multicast source and group. This field is displayed only when the switch runs MLDv2.
Last-listener-query-timer-expiry	Remaining time for the last listener query timer of the IPv6 multicast source and group. If the timer is disabled, this field displays <b>Off</b> . This field is displayed only when the switch runs MLDv2.

# Display detailed MLD information for the IPv6 multicast groups that interfaces dynamically joined on the public network.

```
<Sysname> display mld group static
Entries in total: 2
(*, FF03::101)
  Interface: Vlan1
  Expires: Never

(2001::101, FF3E::202)
  Interface: Vlan1
  Expires: Never
```

Figure 2 Command output

Field	Description
Entries in total	Total number of IPv6 multicast groups.
(*, FF03::101)	(*, G) entry.
(2001::101, FF3E::202)	(S, G) entry.
Interface	Interface name.
Expires	Remaining time for the IPv6 multicast group. The timer is disabled, and this field displays <b>Never</b> .

## Related commands

**reset mld group**

## display mld interface

Use **display mld interface** to display MLD information for an interface.

## Syntax

```
display mld [ vpn-instance vpn-instance-name ] interface [ interface-type interface-number ] [ verbose ]
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays MLD information for interfaces on the public network.

*interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays MLD information for all MLD-enabled interfaces.

**verbose**: Displays detailed MLD information.

## Examples

```
# Display detailed MLD information for VLAN-interface 1 on the public network.
```

```
<Sysname> display mld interface vlan-interface 1 verbose
```

```
Vlan-interface1(FF80::200:AFF:FE01:101):  
  MLD is enabled.  
  MLD version: 1  
  Query interval for MLD: 125s  
  Other querier present time for MLD: 255s  
  Maximum query response time for MLD: 10s  
  Last listener query interval: 1s  
  Last listener query count: 2  
  Startup query interval: 31s
```

```

Startup query count: 2
General query timer expiry (hh:mm:ss): 00:00:23
Querier for MLD: FE80::200:AFF:FE01:101 (This router)
MLD activity: 1 join(s), 0 done(s)
IPv6 multicast routing on this interface: Enabled
Robustness: 2
Require-router-alert: Disabled
Fast-leave: Disabled
SSM-mapping: Disabled
SSM-mapping: Disabled
Startup-query: Off
Other-querier-present-timer-expiry (hh:mm:ss): --:--:--
MLD groups reported in total: 1

```

**Table 85 Command output**

Field	Description
Vlan-interface1(FE80::200:AFF:FE01:101)	Interface and IPv6 link-local address.
Query interval for MLD	MLD query interval, in seconds.
Other querier present time for MLD	MLD other querier present interval, in seconds.
Maximum query response time for MLD	Maximum response time for general query messages, in seconds.
Last listener query interval	MLD last listener query interval, in seconds.
Last listener query count	Number of MLD multicast-address-specific queries or MLD multicast-address-and-source-specific queries sent for the group.
Startup query interval	MLD startup query interval, in seconds.
Startup query count	Number of MLD general queries sent on startup.
General query timer expiry	Remaining time for the MLD general query timer. If the timer is disabled, this field displays <b>Off</b> .
Querier for MLD	IPv6 link-local address of the MLD querier.
MLD activity: 1 join(s), 0 done(s)	MLD activity statistics: <ul style="list-style-type: none"> <li>• <b>join(s)</b>—Total number of IPv6 multicast groups that the interface has joined.</li> <li>• <b>done(s)</b>—Total number of IPv6 multicast groups that the interface has left.</li> </ul>
IPv6 multicast routing on this interface	Whether IPv6 multicast routing and forwarding is enabled.
Robustness	Robustness variable of the MLD querier.
Require-router-alert	Whether the function of dropping MLD messages without Router-Alert is enabled.
Fast-leave	Whether the MLD fast-leave processing feature is enabled.
SSM-mapping	Whether the MLD SSM mapping feature is enabled.

Field	Description
Startup-query	Whether the MLD querier sends MLD general queries at the startup query interval on startup: <ul style="list-style-type: none"> <li>• <b>On</b>—The MLD querier performs the above action.</li> <li>• <b>Off</b>—The MLD querier does not perform the above action.</li> </ul>
Other-querier-present-timer-expiry	Remaining time for MLD other querier present timer. If the timer is disabled, this field displays <b>Off</b> .
MLD groups reported in total	Total number of IPv6 multicast groups the interface joined dynamically. This field is not displayed if the interface does not join IPv6 multicast groups.

## display mld ssm-mapping

Use **display mld ssm-mapping** to display MLD SSM mappings.

### Syntax

```
display mld [ vpn-instance vpn-instance-name ] ssm-mapping ipv6-group-address
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays MLD SSM mappings on the public network.

*ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where "x" and "y" represent any hexadecimal numbers from 0 to F.

### Examples

# Display MLD SSM mappings for the IPv6 multicast group FF3E::101 on the public network.

```
<Sysname> display mld ssm-mapping ff3e::101
Group: FF3E::101
Source list:
  1::1
  1::2
  10::1
  100::10
```



Table 86 Command output

Fields	Description
Group	IPv6 multicast group address.
Source list	List of IPv6 multicast source addresses.

## last-listener-query-count (MLD view)

Use **last-listener-query-count** to set the MLD global last listener query count.

Use **undo last-listener-query-count** to restore the default.

### Syntax

**mld last-member-query-count** *count*

**undo mld last-member-query-count**

### Default

The MLD last listener query count equals the MLD querier's robustness variable.

### Views

MLD view

### Predefined user roles

network-admin

### Parameters

*count*: Sets an MLD last listener query count in the range of 1 to 255.

### Usage guidelines

This command and the **mld last-listener-query-count** command have the same function but different effective ranges:

- The **last-listener-query-count** command in MLD view takes effect on all interfaces.
- The **mld last-listener-query-count** command takes effect on the current interface.

For an interface, the **mld last-listener-query-count** command takes priority over the **last-listener-query-count** command in MLD view.

### Examples

```
# Set the global MLD last listener query count to 6 on the public network.
<Sysname> system-view
[Sysname] mld
[Sysname-mld] last-listener-query-count 6
```

### Related commands

**mld last-listener-query-count**

## last-listener-query-interval (MLD view)

Use **last-listener-query-interval** to set the MLD last listener query interval globally.

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

## Syntax

**last-listener-query-interval** *interval*

**undo last-listener-query-interval**

## Default

The MLD last listener query interval is 1 second.

## Views

MLD view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an MLD last listener query interval in the range of 1 to 25 seconds.

## Usage guidelines

This command and the **mld last-listener-query-interval** command have the same function but different effective ranges:

- The **last-listener-query-count** command in MLD view takes effect on all interfaces.
- The **mld last-listener-query-count** command takes effect on the current interface.

For an interface, the **mld last-listener-query-count** command takes priority over the **last-listener-query-count** command in MLD view.

## Examples

```
# Set the global MLD last listener query interval to 6 seconds on the public network.
```

```
<Sysname> system-view  
[Sysname] mld  
[Sysname-mld] last-listener-query-interval 6
```

## Related commands

**mld last-listener-query-interval**

# max-response-time (MLD view)

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

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

## Syntax

**max-response-time** *time*

**undo max-response-time**

## Default

The global maximum response time for MLD general queries is 10 seconds.

## Views

MLD view

## Predefined user roles

network-admin

## Parameters

*time*: Sets the maximum response time for MLD general queries in the range of 1 to 3174 seconds.

## Usage guidelines

This command and the **mld max-response-time** command have the same function but different effective ranges:

- The **max-response-time** command in MLD view takes effect on all interfaces.
- The **mld max-response-time** command takes effect on the current interface.

For an interface, the **mld max-response-time** command takes priority over the **max-response-time** command in MLD view.

## Examples

```
# Set the global maximum response time for MLD general queries to 25 seconds on the public network.
<Sysname> system-view
[Sysname] mld
[Sysname-mld] max-response-time 25
```

## Related commands

**mld max-response-time**

# mld

Use **mld** to enter MLD view.

Use **undo mld** to remove the configurations made in MLD view.

## Syntax

```
mld [ vpn-instance vpn-instance-name ]
undo mld [ vpn-instance vpn-instance-name ]
```

## Views

System view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command takes effect on the public network.

## Examples

```
# Enter MLD view of the public network.
<Sysname> system-view
[Sysname] mld
[Sysname-mld]

# Enter MLD view of the VPN instance mvpn.
<Sysname> system-view
[Sysname] mld vpn-instance mvpn
[Sysname-mld-mvpn]
```

## mld enable

Use **mld enable** to enable MLD on an interface.

Use **undo mld enable** to disable MLD on an interface.

### Syntax

**mld enable**

**undo mld enable**

### Default

MLD is disabled on all interfaces.

### Views

Interface view

### Predefined user roles

network-admin

### Usage guidelines

This command takes effect only when IPv6 multicast routing is enabled. If the interface belongs to a VPN instance, make sure IPv6 multicast routing is enabled on the VPN instance.

MLD configurations on an interface take effect only when MLD is enabled on the interface.

### Examples

```
# Enable IPv6 multicast routing, and enable MLD for VLAN-interface 100 on the public network.
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib6] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld enable
```

### Related commands

**ipv6 multicast routing**

## mld fast-leave

Use **mld fast-leave** to enable fast-leave processing on an interface.

Use **undo mld fast-leave** to disable fast-leave processing on an interface.

### Syntax

**mld fast-leave** [ **group-policy** *acl6-number* ]

**undo mld fast-leave**

### Default

Fast-leave processing is disabled. The MLD querier sends MLD multicast-address-specific or multicast-address-and-source-specific queries after receiving MLD done messages.

### Views

Interface view

## Predefined user roles

network-admin

## Parameters

*acl6-number*: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999. If you specify an ACL, the command takes effect only on the IPv6 multicast groups that the ACL permits. The command takes effect on all IPv6 multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not contain valid rules.

## Usage guidelines

This feature enables an MLD querier to send leave notifications to the upstream routers without sending multicast-address-specific or multicast-address-and-source-specific queries after receiving done messages.

In an IPv6 basic ACL, the **source** keyword matches the IPv6 multicast group address in MLD done messages.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

## Examples

```
# Enable MLD fast-leave processing on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld fast-leave
```

# mld group-policy

Use **mld group-policy** to configure an IPv6 multicast group policy on an interface to control the IPv6 multicast groups that the hosts attached to the interface can join.

Use **undo mld group-policy** to remove the configured IPv6 multicast group policy.

## Syntax

```
mld group-policy acl6-number [ version-number ]
```

```
undo mld group-policy
```

## Default

IPv6 multicast group policies are not configured on an interface, and hosts attached to the interface can join IPv6 multicast groups.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*acl6-number*: Specifies an IPv6 basic or advanced ACL by its number in the range of 2000 to 3999. Receiver hosts can join only the IPv6 multicast groups that the ACL permits. If the specified ACL does not exist or the specified ACL does not contain valid rules, receiver hosts cannot join IPv6 multicast groups.

*version-number*: Specifies an MLD version number, 1 or 2. By default, the configured group filter is effective on both MLDv1 reports and MLDv2 reports.

## Usage guidelines

In an IPv6 basic ACL, the **source** keyword matches the IPv6 multicast group address in MLD reports. In an IPv6 advanced ACL, the **source** and **destination** keywords match the IPv6 multicast source address and IPv6 multicast group address in MLD report, respectively. The multicast source address is considered to be 0::0 for the following MLD reports:

- MLDv1 reports.
- MLDv2 IS\_EX and MLDv2 TO-EX reports that do not carry IPv6 multicast source addresses.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

This command controls the IPv6 multicast groups that the receiver hosts can join by filtering MLD messages. This command does not take effect on a static member interface, because the static member interface does not send MLD messages.

## Examples

```
# Configure an IPv6 multicast group policy on VLAN-interface 100 so that hosts attached to the interface can join only the IPv6 multicast group FF03::101.
```

```
<Sysname> system-view
[Sysname] acl ipv6 number 2005
[Sysname-acl6-basic-2005] rule permit source ff03::101 128
[Sysname-acl6-basic-2005] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld group-policy 2005
```

# mld last-listener-query-count

Use **mld last-listener-query-count** to set the MLD last member query count on an interface.

Use **undo mld last-listener-query-count** to restore the default.

## Syntax

```
mld last-listener-query-count count
```

```
undo mld last-listener-query-count
```

## Default

The MLD last listener query count equals the MLD querier's robustness variable.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*count*: Sets an MLD last listener query count in the range of 1 to 255.

## Usage guidelines

This command and the **last-listener-query-count** command in MLD view have the same function but different effective ranges:

- The **last-listener-query-count** command in MLD view takes effect on all interfaces.
- The **mld last-listener-query-count** command takes effect on the current interface.

For an interface, the **mld last-listener-query-count** command takes priority over the **last-listener-query-count** command in MLD view.

## Examples

```
# Set the MLD last listener query count to 6 on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld last-listener-query-count 6
```

## Related commands

**last-listener-query-count** (MLD view)

# mld last-listener-query-interval

Use **mld last-listener-query-interval** to set the MLD last listener query interval on an interface.

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

## Syntax

```
mld last-listener-query-interval interval
undo mld last-listener-query-interval
```

## Default

The MLD last listener query interval is 1 second.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an MLD last listener query interval in the range of 1 to 25 seconds.

## Usage guidelines

This command and the **last-listener-query-interval** command in MLD view have the same function but different effective ranges:

- The **last-listener-query-interval** command in MLD view takes effect on all interfaces.
- The **mld last-listener-query-interval** command takes effect on the current interface.

For an interface, the **mld last-listener-query-interval** command takes priority over the **last-listener-query-interval** command in MLD view.

## Examples

```
# Set the MLD last listener query interval to 6 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld last-listener-query-interval 6
```

## Related commands

**last-listener-query-interval** (MLD view)

# mld max-response-time

Use **mld max-response-time** to set the maximum response time for MLD general queries on an interface.

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

## Syntax

**mld max-response-time** *time*

**undo mld max-response-time**

## Default

The maximum response time for MLD general queries is 10 seconds.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*time*: Sets the maximum response time for MLD general queries, in the range of 1 to 3174 seconds.

## Usage guidelines

This command and the **max-response-time** command in MLD view have the same function but different effective ranges:

- The **max-response-time** command in MLD view takes effect on all interfaces.
- The **mld max-response-time** command takes effect on the current interface.

For an interface, the **mld max-response-time** command takes priority over the **max-response-time** command in MLD view.

## Examples

```
# Set the maximum response time for MLD general queries to 25 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld max-response-time 25
```

## Related commands

**max-response-time** (MLD view)



## mld non-stop-routing

Use **mld non-stop-routing** to enable MLD NSR.

Use **undo mld non-stop-routing** to disable MLD NSR.

### Syntax

**mld non-stop-routing**

**undo mld non-stop-routing**

### Default

MLD NSR is disabled.

### Views

System view

### Predefined user roles

network-admin

### Examples

```
# Enable MLD NSR.
<Sysname> system-view
[Sysname] mld non-stop-routing
```

## mld other-querier-present-timeout

Use **mld other-querier-present-timeout** to set the MLD other querier present timer on an interface.

Use **undo mld other-querier-present-timeout** to restore the default.

### Syntax

**mld other-querier-present-timeout** *time*

**undo mld other-querier-present-timeout**

### Default

The MLD other querier present timer is calculated by the following formula:

[ MLD general query interval ] × [ MLD querier's robustness variable ] + [ maximum response time for MLD general queries ] / 2.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

*time*: Sets an MLD other querier present timer in the range of 1 to 31744 seconds.

### Usage guidelines

This command and the **other-querier-present-timer** command have the same function but different effective ranges:

- The **other-querier-present-timer** command takes effect on all interfaces.
- The **mld other-querier-present-timeout** command takes effect on the current interface.

For an interface, the **mld other-querier-present-timeout** command takes priority over the **other-querier-present-timer** command.

## Examples

```
# Set the MLD other querier present timer to 125 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld other-querier-present-timeout 125
```

## Related commands

**other-querier-present-timeout** (MLD view)

# mld query-interval

Use **mld query-interval** to set the MLD general query interval on an interface.

Use **undo mld query-interval** to restore the default.

## Syntax

**mld query-interval** *interval*

**undo mld query-interval**

## Default

The MLD general query interval is 125 seconds.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an MLD general interval in the range of 1 to 31744 seconds.

## Usage guidelines

This command and the **query-interval** command in MLD view have the same function but different effective ranges:

- The **query-interval** command in MLD view takes effect on all interfaces.
- The **mld query-interval** command takes effect on the current interface.

For an interface, the **mld query-interval** command takes priority over the **query-interval** command in MLD view.

## Examples

```
# Set the MLD general query interval to 60 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld query-interval 60
```

## Related commands

**query-interval** (MLD view)

# mld robust-count

Use **mld robust-count** to set the MLD querier's robustness variable on an interface.

Use **undo mld robust-count** to restore the default.

## Syntax

**mld robust-count** *count*

**undo mld robust-count**

## Default

The MLD querier's robustness variable is 2.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*count*: Sets an MLD querier's robustness variable in the range of 1 to 255.

## Usage guidelines

The MLD querier's robustness variable defines the number of times to retransmit MLD queries if packet loss occurs. A higher robustness variable makes the MLD querier more robust, but it increases the timeout time for IPv6 multicast groups.

This command and the **robust-count** command in MLD view have the same function but different effective ranges:

- The **robust-count** command in MLD view takes effect on all interfaces.
- The **mld robust-count** command takes effect on the current interface.

For an interface, the **mld robust-count** command takes priority over the **robust-count** command in MLD view.

## Examples

```
# Set the MLD querier's robustness variable to 5 on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld robust-count 5
```

## Related commands

**robust-count** (MLD view)

# mld startup-query-count

Use **mld startup-query-count** to set the MLD startup query count on an interface.

Use **undo mld startup-query-count** to restore the default.

## Syntax

**mld startup-query-count** *count*

**undo mld startup-query-count**

## Default

The MLD startup query count equals the MLD querier's robustness variable.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*count*: Sets an MLD startup query count in the range of 1 to 255.

## Usage guidelines

This command and the **startup-query-count** command in MLD view have the same function but different effective ranges:

- The **startup-query-count** command in MLD view takes effect on all interfaces.
- The **mld startup-query-count** command takes effect on the current interface.

For an interface, the **mld startup-query-count** command takes priority over the **startup-query-count** command in MLD view.

## Examples

```
# Set the MLD startup query count to 5 on VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] mld startup-query-count 5
```

## Related commands

**startup-query-count** (MLD view)

# mld startup-query-interval

Use **mld startup-query-interval** to set the MLD startup query interval on an interface.

Use **undo mld startup-query-interval** to restore the default.

## Syntax

**mld startup-query-interval** *interval*

**undo mld startup-query-interval**

## Default

The MLD startup query interval equals one quarter of the MLD general query interval.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an MLD startup query interval in the range of 1 to 31744 seconds.

## Usage guidelines

This command and the **startup-query-interval** command in MLD view have the same function but different effective ranges:

- The **startup-query-interval** command in MLD view takes effect on all interfaces.
- The **mld startup-query-interval** command takes effect on the current interface.

For an interface, the **mld startup-query-interval** command takes priority over the **startup-query-interval** command in MLD view.

## Examples

```
# Set the MLD startup query interval to 100 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld startup-query-interval 100
```

## Related commands

**startup-query-interval** (MLD view)

# mld static-group

Use **mld static-group** to configure an interface as a static group member of an IPv6 multicast group.

Use **undo mld static-group** to restore the default.

## Syntax

```
mld static-group ipv6-group-address [ source ipv6-source-address ]
undo mld static-group { all | ipv6-group-address [ source ipv6-source-address ] }
```

## Default

An interface is not a static group member of IPv6 multicast groups.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where "x" and "y" represent any hexadecimal numbers from 0 to F.

*ipv6-source-address*: Specifies an IPv6 multicast source. If you do not specify an IPv6 multicast source, the command configures an interface as a static group member of the multicast groups with all IPv6 multicast source addresses.

**all**: Specifies all IPv6 multicast groups that the interface has statically joined.

## Usage guidelines

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 IPv6 multicast routing entries cannot be established. This restriction does not exist if the specified IPv6 multicast group address is not in the SSM multicast address range.

## Examples

```
# Configure VLAN-interface 100 as a static group 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 as a static group member of the 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 version

Use **mld version** to specify an MLD version for an interface.

Use **undo mld version** to restore the default.

### Syntax

```
mld version version-number
```

```
undo mld version
```

### Default

The MLD version is 1.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

*version-number*: Specifies an MLD version, 1 or 2.

## Examples

```
# Specify MLD version 2 for VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld version 2
```

## other-querier-present-timeout (MLD view)

Use **other-querier-present-timeout** to set the global MLD other querier present timer.

Use **undo other-querier-present-timeout** to restore the default.

## Syntax

**other-querier-present-timeout** *time*  
**undo other-querier-present-timeout**

## Default

The MLD other querier present timer is calculated by the following formula:

[ MLD general query interval ] × [ MLD querier's robustness variable ] + [ maximum response time for MLD general queries ] / 2.

## Views

MLD view

## Predefined user roles

network-admin

## Parameters

*time*: Sets an MLD other querier present timer in the range of 1 to 31744 seconds.

## Usage guidelines

This command and the **mld other-querier-present-timeout** command have the same function but different effective ranges:

- The **other-querier-present-timeout** command takes effect on all interfaces.
- The **mld other-querier-present-timeout** command takes effect on the current interface.

For an interface, the **mld other-querier-present-timeout** command takes priority over the **other-querier-present-timeout** command.

## Examples

```
# Set the global MLD other querier present timer to 125 seconds on the public network.  
<Sysname> system-view  
[Sysname] mld  
[Sysname-mld] other-querier-present-timeout 125
```

## Related commands

**mld other-querier-present-timeout**

# query-interval (MLD view)

Use **query-interval** to set the global MLD general query interval.

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

## Syntax

**query-interval** *interval*  
**undo query-interval**

## Default

The global MLD general query interval is 125 seconds.

## Views

MLD view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an MLD general query interval in the range of 1 to 31744 seconds.

## Usage guidelines

This command and the **mld query-interval** command have the same function but different effective ranges:

- The **query-interval** command in MLD view takes effect on all interfaces.
- The **mld query-interval** command takes effect on the current interface.

For an interface, the **mld query-interval** command takes priority over the **query-interval** command in MLD view.

## Examples

```
# Set the global MLD general query interval to 60 seconds on the public network.
<Sysname> system-view
[Sysname] mld
[Sysname-mld] query-interval 60
```

## Related commands

**mld query-interval**

# reset mld group

Use **reset mld group** to remove dynamic MLD group entries.

## Syntax

```
reset mld [ vpn-instance vpn-instance-name ] group { all | interface interface-type interface-number { all | ipv6-group-address [ prefix-length ] [ ipv6-source-address [ prefix-length ] ] } }
```

## Views

User view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command removes dynamic MLD group entries on the public network.

**all**: The first **all** specifies all interfaces, and the second **all** specifies all MLD groups.

*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 range of FFxy::/16, where "x and "y" represent any hexadecimal numbers from 0 to F.

*ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, the command removes dynamic MLD group entries of all IPv6 multicast source addresses.



*prefix-length*: Specifies an address prefix length. The default is 128. For a multicast source address, the value range for this argument is 0 to 128. For a multicast group address, the value range for this argument is 8 to 128.

## Usage guidelines

This command might interrupt the IPv6 multicast information transmission.

## Examples

```
# Remove the dynamic group entries for all MLD groups on all interfaces on the public network.
```

```
<Sysname> reset mld group all
```

```
# Remove the dynamic group entries for all MLD groups on VLAN-interface 100 on the public network.
```

```
<Sysname> reset mld group interface vlan-interface 100 all
```

```
# Remove the dynamic group entry for the MLD group FF03::101:10 on VLAN-interface 100 on the public network.
```

```
<Sysname> reset mld group interface vlan-interface 100 ff03::101:10
```

## Related commands

**display mld group**

# robust-count (MLD view)

Use **robust-count** to set the global MLD querier's robustness variable.

Use **undo robust-count** to restore the default.

## Syntax

**robust-count** *count*

**undo robust-count**

## Default

The global MLD querier's robustness variable is 2.

## Views

MLD view

## Predefined user roles

network-admin

## Parameters

*count*: Sets an MLD querier's robustness variable in the range of 1 to 255.

## Usage guidelines

The MLD querier's robustness variable defines the number of times to retransmit MLD queries if packet loss occurs. A higher robustness variable makes the MLD querier more robust, but it increases the timeout time for IPv6 multicast groups.

This command and the **mld robust-count** command have the same function but different effective ranges:

- The **robust-count** command in MLD view takes effect on all interfaces.
- The **mld robust-count** command takes effect on the current interface.

For an interface, the **mld robust-count** command takes priority over the **robust-count** command in MLD view.

## Examples

```
# Set the global MLD querier's robustness variable to 5 on the public network.
<Sysname> system-view
[Sysname] mld
[Sysname-mld] robust-count 5
```

## Related commands

**mld robust-count**

# ssm-mapping (MLD view)

Use **ssm-mapping** to configure MLD SSM mappings.

Use **undo ssm-mapping** to remove MLD SSM mappings.

## Syntax

```
ssm-mapping ipv6-source-address acl6-number
undo ssm-mapping { ipv6-source-address | all }
```

## Default

MLD SSM mappings are not configured.

## Views

MLD view

## Predefined user roles

network-admin

## Parameters

*ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address.

*acl6-number*: Specifies an IPv6 basic ACL number in the range of 2000 to 2999. The specified IPv6 multicast source is mapped only to IPv6 multicast groups that the ACL permits. If the ACL does not exist or the ACL does not have valid rules, the specified IPv6 multicast source is not mapped to IPv6 multicast groups.

**all**: Removes all the MLD SSM mappings.

## Usage guidelines

In an IPv6 basic ACL, the **source** keyword matches IPv6 multicast group address in MLD reports.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

## Examples

```
# Map the IPv6 multicast source 1::1 to the IPv6 multicast groups in the range of FF3E::/64 on the public network.
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source ff3e:: 64
[Sysname-acl6-basic-2001] quit
[Sysname] mld
[Sysname-mld] ssm-mapping 1::1 2001
```

## Related commands

`display mld ssm-mapping`

## startup-query-count (MLD view)

Use **startup-query-count** to set the global MLD startup query count.

Use **undo startup-query-count** to restore the default.

### Syntax

**startup-query-count** *count*

**undo startup-query-count**

### Default

The global MLD startup query count equals the MLD querier's robustness variable.

### Views

MLD view

### Predefined user roles

network-admin

### Parameters

*count*: Sets an MLD startup query count in the range of 1 to 255.

### Usage guidelines

This command and the **mld startup-query-count** command have the same function but different effective ranges:

- The **startup-query-count** command in MLD view takes effect on all interfaces.
- The **mld startup-query-count** command takes effect on the current interface.

For an interface, the **mld startup-query-count** command takes priority over the **startup-query-count** command in MLD view.

### Examples

```
# Set the global MLD startup query count to 5 on the public network.  
<Sysname> system-view  
[Sysname] mld  
[Sysname-mld] startup-query-count 5
```

## Related commands

**mld startup-query-count**

## startup-query-interval (MLD view)

Use **startup-query-interval** to set the global MLD startup query interval.

Use **undo startup-query-interval** to restore the default.

### Syntax

**startup-query-interval** *interval*

## **undo startup-query-interval**

### Default

The global MLD startup query interval equals one quarter of the MLD general query interval.

### Views

MLD view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets an MLD startup query interval in the range of 1 to 31744 seconds.

### Usage guidelines

This command and the **mld startup-query-interval** command have the same function but different effective ranges:

- The **startup-query-interval** command in MLD view takes effect on all interfaces.
- The **mld startup-query-interval** command takes effect on the current interface.

For an interface, the **mld startup-query-interval** command takes priority over the **startup-query-interval** command in MLD view.

### Examples

```
# Set the global MLD startup query interval to 100 seconds on the public network.
```

```
<Sysname> system-view  
[Sysname] mld  
[Sysname-mld] startup-query-interval 100
```

### Related commands

**mld startup-query-interval**

---

# IPv6 PIM commands

The term "interface" in this chapter collectively refers to 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*).

## bidir-pim enable (IPv6 PIM view)

Use **bidir-pim enable** to enable IPv6 BIDIR-PIM.

Use **undo bidir-pim enable** to disable IPv6 BIDIR-PIM.

### Syntax

**bidir-pim enable**

**undo bidir-pim enable**

### Default

IPv6 BIDIR-PIM is disabled.

### Views

IPv6 PIM view

### Predefined user roles

network-admin

### Usage guidelines

This command takes effect only when IPv6 multicast routing is enabled.

### Examples

```
# Enable IPv6 multicast routing on the public network, and enable IPv6 BIDIR-PIM.
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib6] quit
[Sysname] ipv6 pim
[Sysname-pim6] bidir-pim enable
```

### Related commands

**ipv6 multicast routing**

## bidir-rp-limit (IPv6 PIM view)

Use **bidir-rp-limit** to configure the maximum number of RPs in BIDIR-PIM.

Use **undo bidir-rp-limit** to restore the default.

### Syntax

**bidir-rp-limit** *limit*

**undo bidir-rp-limit**

## Default

The default setting is 6.

## Views

IPv6 PIM view

## Predefined user roles

network-admin

## Parameters

*limit*: Sets the maximum number of RPs in IPv6 BIDIR-PIM, in the range of 1 to 32.

## Usage guidelines

In an IPv6 BIDIR-PIM domain, one DF election per RP is implemented on all IPv6 PIM-enabled interfaces. To avoid unnecessary DF elections, HP recommends not configuring multiple RPs for BIDIR-PIM.

This configuration sets a limit on the number of IPv6 BIDIR-PIM RPs. If the number of RPs exceeds the limit, excess RPs do not take effect and can be used only for DF election rather than IPv6 multicast data forwarding.

## Examples

```
# Set the maximum number of IPv6 BIDIR RPs to 3 on the public network.
```

```
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] bidir-rp-limit 3
```

# bsm-fragment enable (IPv6 PIM view)

Use **bsm-fragment enable** to enable bootstrap message (BSM) semantic fragmentation.

Use **undo bsm-fragment enable** to disable BSM semantic fragmentation.

## Syntax

**bsm-fragment enable**

**undo bsm-fragment enable**

## Default

BSM semantic fragmentation is enabled.

## Views

IPv6 PIM view

## Predefined user roles

network-admin

## Usage guidelines

Disable BSM semantic fragmentation if the IPv6 PIM-SM domain contains a device that does not support this feature.

## Examples

```
# Disable BSM semantic fragmentation on the public network.
```

```
<Sysname> system-view
[Sysname] ipv6 pim
```

```
[Sysname-pim6] undo bsm-fragment enable
```

## bsr-policy (IPv6 PIM view)

Use **bsr-policy** to configure a BSR policy to define the legal bootstrap router (BSR) address range.

Use **undo bsr-policy** to remove the configuration.

### Syntax

```
bsr-policy acl6-number
```

```
undo bsr-policy
```

### Default

BSR policies are not configured, and bootstrap messages from any IPv6 multicast sources are regarded as valid.

### Views

IPv6 PIM view

### Predefined user roles

network-admin

### Parameters

*acl6-number*: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999.

### Usage guidelines

You can use this command to guard against BSR spoofing.

In an IPv6 basic ACL, the **source** keyword matches the source address in bootstrap messages.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

### Examples

```
# On the public network, configure a BSR policy so that only the devices on the subnet 2001::2/64 can act as 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] ipv6 pim
[Sysname-pim6] bsr-policy 2000
```

### Related commands

**c-bsr** (IPv6 PIM view)

## c-bsr (IPv6 PIM view)

Use **c-bsr** to configure a candidate-BSR (C-BSR).

Use **undo c-bsr** to remove a C-BSR.

## Syntax

```
c-bsr ipv6-address [ scope scope-id ] [ hash-length hash-length | priority priority ] *  
undo c-bsr ipv6-address [ scope scope-id ]
```

## Default

No C-BSR is configured.

## Views

IPv6 PIM view

## Predefined user roles

network-admin

## Parameters

*ipv6-address*: Specifies the IPv6 address of a C-BSR.

**scope** *scope-id*: Specifies the ID of an IPv6 admin-scoped zone, in the range of 3 to 15. If you do not specify an admin-scoped zone, the command designates the C-BSR to the global-scoped zone.

**hash-length** *hash-length*: Specifies a hash mask length in the range of 0 to 128. The default setting is 126.

**priority** *priority*: Sets a C-BSR priority in the range of 0 to 255. The default setting is 64. A larger value represents a higher priority.

## Usage guidelines

The IPv6 address of a C-BSR must be the IPv6 address of a local IPv6 PIM enabled interface on the C-BSR. Otherwise, the configuration does not take effect.

If you execute this command for a zone multiple times, the most recent configuration takes effect.

You can configure the same C-BSR for different zones.

## Examples

```
# On the public network, configure the interface with the IPv6 address of 1101::1 as the C-BSR for the  
global-scoped zone.
```

```
<Sysname> system-view  
[Sysname] ipv6 pim  
[Sysname-pim6] c-bsr 1101::1
```

## c-rp (IPv6 PIM view)

Use **c-rp** to configure a candidate-RP (C-RP).

Use **undo c-rp** to remove the configuration of a C-RP.

## Syntax

```
c-rp ipv6-address [ advertisement-interval adv-interval | { group-policy acl6-number | scope scope-id }  
| holdtime hold-time | priority priority ] * [ bidir ]  
undo c-rp ipv6-address
```

## Default

No C-RPs are configured.



## Views

IPv6 PIM view

## Predefined user roles

network-admin

## Parameters

*ipv6-address*: Specifies the IPv6 address of a C-RP.

**advertisement-interval** *adv-interval*: Specifies an interval between two C-RP-Adv messages, in the range of 1 to 65535 seconds. The default value is 60 seconds.

**group-policy** *acl6-number*: Specifies an IPv6 basic ACL number in the range of 2000 to 2999. The C-RP is designated only to IPv6 multicast groups that the ACL permits. The C-RP is designated to all IPv6 multicast groups FF00::/8 when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

**scope** *scope-id*: Specifies the ID of an IPv6 admin-scoped zone, in the range of 3 to 15.

**holdtime** *hold-time*: Sets a C-RP lifetime in the range of 1 to 65535 seconds. The default value is 150 seconds.

**priority** *priority*: Sets a C-RP priority in the range of 0 to 255. The default setting is 192. A larger value represents a lower priority.

**bidir**: Specifies BIDIR-PIM. If you do not specify this keyword, the C-RP provides services for IPv6 PIM-SM.

## Usage guidelines

The IPv6 address of a C-RP must be the IPv6 address of a local IPv6 PIM enabled interface on the C-RP. Otherwise, the configuration does not take effect.

In an IPv6 basic ACL, the **source** keyword matches the multicast group address in C-RP advertisement messages, and the other parameters are ignored. If the specified IPv6 addresses are not IPv6 multicast group addresses, the ACL rule is not valid. Only groups that the ACL permits are advertised.

To use a C-RP for multiple IPv6 multicast group ranges, specify them by multiple **permit** statements in an ACL and reference the ACL in the **group-policy** keyword.

If you execute this command using the same IPv6 address of a C-RP multiple times, the most recent configuration takes effect.

## Examples

```
# On the public network, configure the interface with the IPv6 address of 2001::1 as the C-RP for IPv6 multicast group range FF0E:0:1391::/96, and set its priority to 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] ipv6 pim
[Sysname-pim6] c-rp 2001::1 group-policy 2000 priority 10
```

## crp-policy (IPv6 PIM view)

Use **crp-policy** to configure a C-RP policy to define the legal C-RP address range and the IPv6 multicast group range to which the C-RP is designated.

Use **undo crp-policy** to remove the configuration.

### Syntax

```
crp-policy acl6-number
```

```
undo crp-policy
```

### Default

C-RP policies are not configured, and all received C-RP messages are regarded as legal.

### Views

IPv6 PIM view

### Predefined user roles

network-admin

### Parameters

*acl6-number*: Specifies an IPv6 advanced ACL number in the range of 3000 to 3999.

### Usage guidelines

You can configure this command to guard against C-RP spoofing.

In an IPv6 advanced ACL, the **source** and **destination** keywords match the RP address and multicast group address in C-RP advertisement messages, respectively. If you do not specify the **source** keyword in rules, all C-RPs are considered to be legal. If you do not specify the **destination** keyword in rules, the C-RPs are designated to all IPv6 multicast groups.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

When the device compares the advertisement message against the destination field in the ACL, it uses only the prefix of the IPv6 multicast group range in the advertisement message. For example, the IPv6 multicast group range specified in a C-RP advertisement message is FFOE:0:1::/96. If the prefix FFOE:0:1:: is in the IPv6 multicast group range specified in the destination field of the ACL, the advertisement message passes the filtering. Otherwise, the advertisement message is discarded.

### Examples

```
# On the public network, configure a C-RP policy so that only devices in the address range of 2001::2/64 can be C-RPs for the IPv6 multicast group range 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] ipv6 pim
[Sysname-pim6] crp-policy 3000
```

### Related commands

**c-rp** (IPv6 PIM view)

# display ipv6 pim bsr-info

Use **display ipv6 pim bsr-info** to display BSR information in the IPv6 PIM-SM domain.

## Syntax

```
display ipv6 pim [ vpn-instance vpn-instance-name ] bsr-info
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays BSR information on the public network.

## Examples

# Display BSR information in the IPv6 PIM-SM domain on the public network.

```
<Sysname> display ipv6 pim bsr-info
Scope: non-scoped
  State: Accept Preferred
  Bootstrap timer: 00:01:44
  Elected BSR address: 12:12::1
  Priority: 64
  Hash mask length: 126
  Uptime: 00:21:56

Scope: 5
  State: Accept Any
  Scope-zone expiry timer: 00:21:12

Scope: 6
  State: Elected
  Bootstrap timer: 00:00:26
  Elected BSR address: 17:11::1
  Priority: 64
  Hash mask length: 126
  Uptime: 02:53:37
  Candidate BSR address: 17:11::1
  Priority: 64
  Hash mask length: 126

Scope: 7
  State: Candidate
  Bootstrap timer: 00:01:56
  Elected BSR address: 61:37::1
```

```

    Priority: 64
    Hash mask length: 126
    Uptime: 02:53:32
Candidate BSR address: 17:12::1
    Priority: 64
    Hash mask length: 126

Scope: 8
    State: Pending
    Bootstrap timer: 00:00:07
Candidate BSR address: 17:13::1
    Priority: 64
    Hash mask length: 126

```

**Table 87 Command output**

Field	Description
Scope-zone expiry timer	Scoped zone aging timer.
Elected BSR address	Address of the elected BSR.
Candidate BSR address	Address of the C-BSR.
Priority	BSR priority.
Uptime	Length of time the BSR has been up.

## display ipv6 pim claimed-route

Use **display ipv6 pim claimed-route** to display information about all routes that IPv6 PIM uses.

### Syntax

```
display ipv6 pim [ vpn-instance vpn-instance-name ] claimed-route [ipv6-source-address ]
```

### Views

Any view

### Predefined user roles

network-admin  
network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays information about all routes that IPv6 PIM uses on the public network.

*ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, the command displays information about all routes that IPv6 PIM uses.

### Examples

# Display information about all routes that IPv6 PIM uses on the public network.

```
<Sysname> display ipv6 pim claimed-route
RPF-route selecting rule: longest-match
```

```

Route/mask: 7:11::/64 (unicast (direct))
  RPF interface: Vlan-interface2, RPF neighbor: 8::2
  Total number of (S,G) or (*,G) dependent on this route entry: 4
  (7:11::10, ff1e::1)
  (7:11::10, ff1e::2)
  (7:11::10, ff1e::3)
  (*, ff1e::4)
Route/mask: 7:12::/64 (unicast)
  RPF interface: Vlan-interface2, RPF neighbor: 8::3,
  Total number of (S,G) or (*,G) dependent on this route entry: 2
  (7:12::10, ff1e::1)
  (7:12::10, ff1e::2)

```

**Table 88 Command output**

Field	Description
Route/mask	Route entry. Route types in parentheses include: <ul style="list-style-type: none"> <li>• <b>igp</b>—IGP unicast route.</li> <li>• <b>egp</b>—EGP unicast route.</li> <li>• <b>unicast (direct)</b>—Directly connected unicast route.</li> <li>• <b>unicast</b>—Other unicast route, such as static unicast route.</li> </ul>
RPF interface	Name of the RPF interface.
RPF neighbor	IPv6 address of the RPF neighbor.
Total number of (S,G) or (*,G) dependent on this route entry	Total number (S, G) or (*, G) entries dependent on the RPF route and their details.

## display ipv6 pim c-rp

Use **display ipv6 pim c-rp** to display C-RP information in the IPv6 PIM-SM domain.

### Syntax

```
display ipv6 pim [ vpn-instance vpn-instance-name ] c-rp [ local ]
```

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays information about learned C-RPs on the public network.

**local**: Specifies local C-RPs. If you do not specify this keyword, the command displays information about all C-RPs.

## Usage guidelines

You can display information about learned C-RPs only on the BSR. On other devices, you can display information about the locally configured C-RPs.

## Examples

# Display information about learned C-RPs on the public network.

```
<Sysname> display ipv6 pim c-rp
Scope: non-scoped
  Group/MaskLen: FF00::/8 [B]
    C-RP address          Priority  HoldTime  Uptime    Expires
    8:12::2 (local)      192     150      00:27:48  00:01:43
  Group/MaskLen: FF23::/92 Expires: 00:02:07
```

# Display information about the locally configured C-RPs.

```
<Sysname> display ipv6 pim c-rp local
Candidate RP: 8:12::2(Loop1)
  Priority: 192
  HoldTime: 150
  Advertisement interval: 60
  Next advertisement scheduled at: 00:00:46
```

**Table 89 Command output**

Field	Description
Group/MaskLen	IPv6 multicast group to which the C-RP is designated.
[B]	The C-RP provides services for IPv6 BIDIR-PIM. If this field is not displayed, the C-RP provides services for IPv6 PIM-SM.
C-RP address	IPv6 address of the C-RP. If the C-RP resides on the device where the command is executed, this field displays <b>(local)</b> after the address.
HoldTime	C-RP lifetime.
Uptime	Length of time the C-RP has been up: <ul style="list-style-type: none"><li>• <b>w</b>—Weeks.</li><li>• <b>d</b>—Days.</li><li>• <b>h</b>—Hours.</li></ul>
Expires	Remaining lifetime for the C-RP and IPv6 multicast group.
Candidate RP	IPv6 address of the locally configured C-RP.
Advertisement interval	Interval between two advertisement messages sent by the locally configured C-RP.
Next advertisement scheduled at	Remaining time for the locally configured C-RP to send the next advertisement message.

## display ipv6 pim df-info

Use **display ipv6 pim df-info** to display the DF information of IPv6 BIDIR-PIM.

### Syntax

```
display ipv6 pim [ vpn-instance vpn-instance-name ] df-info [ ipv6-rp-address ]
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays the DF information of IPv6 BIDIR-PIM on the public network.

*ipv6-rp-address*: Specifies an RP of IPv6 BIDIR-PIM by its IPv6 address.

## Examples

# Display the DF information of IPv6 BIDIR-PIM on the public network.

```
<Sysname> display ipv6 pim df-info
```

```
RP address: 1:1::1
```

Interface	State	DF-Pref	DF-Metric	DF-Uptime	DF-Address
Vlan1	Lose	0	0	00:20:13	FE80:7:11::1
Vlan2	Win	10	1	00:20:12	FE80:10:1::2 (local)

Table 90 Command output

Field	Description
State	DF election state: <ul style="list-style-type: none"><li>• <b>Win</b>—The interface wins the DF election.</li><li>• <b>Lose</b>—The interface loses the DF election.</li><li>• <b>Offer</b>—The interface is in the initial state of the DF election.</li><li>• <b>Backoff</b>—The interface is acting as the DF, but there are more appropriate devices running for the DF.</li><li>• <b>--</b>—The interface does not participate in the DF election.</li></ul>
DF-Pref	Advertised route preference for DF election.
DF-Metric	Advertised route metric for DF election.
DF-Uptime	Length of time the DF has been up.
DF-Address	IP address of DF. If the DF resides on the device where the command is executed, this field displays <b>(local)</b> after the address.

## display ipv6 pim interface

Use **display ipv6 pim interface** to display IPv6 PIM information on an interface.

## Syntax

```
display ipv6 pim [ vpn-instance vpn-instance-name ] interface [ interface-type interface-number ]  
[ verbose ]
```

## Views

Any view

## Predefined user roles

network-admin  
network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays IPv6 PIM information on an interface on the public network.

*interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays IPv6 PIM information on all interfaces.

**verbose**: Displays detailed IPv6 PIM information. If you do not specify this keyword, the command displays brief IPv6 PIM information.

## Examples

# Display IPv6 PIM brief information on all interfaces on the public network.

```
<Sysname> display ipv6 pim interface
Interface          NbrCnt  HelloInt  DR-Pri    DR-Address
Vlan1              1       30       1         FE80::200:5EFF:FE04:8700
```

**Table 91 Command output**

Field	Description
Interface	Name of the interface.
NbrCnt	Number of IPv6 PIM neighbors.
HelloInt	Interval for sending hello messages.
DR-Pri	DR priority.
DR-Address	IPv6 address (link-local address) of the DR.

# Display detailed IPv6 PIM information on VLAN-interface 1 on the public network.

```
<Sysname> display ipv6 pim interface vlan-interface 1 verbose
Interface: Vlan-interface 1, 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
PIM BFD: disabled
PIM passive: 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 92 Command output**

<b>Field</b>	<b>Description</b>
Interface	Interface name and IPv6 address (link-local address).
PIM mode	IPv6 PIM mode: dense or sparse.
PIM DR	IPv6 address (link-local address) of the DR.
PIM DR Priority (configured)	Configured DR priority.
PIM neighbor count	Total number of IPv6 PIM neighbors.
PIM hello interval	Interval between two hello messages.
PIM LAN delay (negotiated)	Negotiated IPv6 message propagation delay.
PIM LAN delay (configured)	Configured IPv6 message propagation delay.
PIM override interval (negotiated)	Negotiated interval for overriding prune messages.
PIM override interval (configured)	Configured interval for overriding prune messages.
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status: enabled or disabled.
PIM neighbor tracking (configured)	Configured neighbor tracking status: enabled or disabled.
PIM require generation ID	Whether the feature of dropping hello messages without Generation_ID is enabled.
PIM hello hold interval	IPv6 PIM neighbor lifetime.
PIM assert hold interval	Assert holdtime timer.
PIM triggered hello delay	Maximum delay for sending hello messages.
PIM J/P interval	Interval between two join/prune messages.
PIM J/P hold interval	Joined/pruned state holdtime timer.
PIM BSR domain border	Whether an IPv6 PIM domain border is configured.
PIM BFD	Whether IPv6 PIM is enabled to work with BFD.
PIM passive	Whether IPv6 PIM passive mode is enabled.
Number of routers on network not using DR priority	Number of routers that do not use the DR priority field on the subnet where the interface resides.
Number of routers on network not using LAN delay	Number of routers that do not use the LAN delay field on the subnet where the interface resides.
Number of routers on network not using neighbor tracking	Number of routers that are not enabled with neighbor tracking on the subnet where the interface resides.

# display ipv6 pim neighbor

Use **display ipv6 pim neighbor** to display IPv6 PIM neighbor information.

## Syntax

```
display ipv6 pim [ vpn-instance vpn-instance-name ] neighbor [ipv6-neighbor-address | interface  
interface-type interface-number | verbose ] *
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays IPv6 PIM neighbor information on the public network.

*ipv6-neighbor-address*: Specifies an IPv6 PIM neighbor by its IPv6 address. If you do not specify an IPv6 PIM neighbor, the command displays information about all IPv6 PIM neighbors.

**interface** *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays information about IPv6 PIM neighbors on all interfaces.

**verbose**: Displays detailed IPv6 PIM neighbor information. If you do not specify this keyword, the command displays brief IPv6 PIM neighbor information.

## Examples

# Display brief information about all IPv6 PIM neighbors on the public network.

```
<Sysname> display ipv6 pim 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	

# Display detailed information about the IPv6 PIM neighbor with the IPv6 address 11.110.0.20 on the public network.

```
<Sysname> display ipv6 pim 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: Enabled
Secondary address(es):
1::1

```

**Table 93 Command output**

Field	Description
Neighbor	Primary IPv6 address (link-local address) of the IPv6 PIM neighbor.
Interface	Interface that connects to the IPv6 PIM neighbor.
Uptime	Length of time the IPv6 PIM neighbor has been up.
Expires/Expiry time	Remaining lifetime for the IPv6 PIM neighbor. If the IPv6 PIM neighbor is always up and reachable, this field displays <b>never</b> .
DR-Priority/DR Priority	Priority of the IPv6 PIM neighbor.
Mode	IPv6 PIM mode. If the IPv6 PIM mode is BIDIR-PIM, this field displays <b>B</b> . If an IPv6 PIM mode other than IPv6 BIDIR-PIM is used, this field is blank.
Generation ID	Generation ID of the IPv6 PIM neighbor. (A random value represents a status change of the IPv6 PIM neighbor.)
Holdtime	Lifetime of the IPv6 PIM neighbor. If the IPv6 PIM neighbor is always up and reachable, this field displays <b>forever</b> .
LAN delay	IPv6 PIM message propagation delay.
Override interval	Interval for overriding prune messages.
State refresh interval	Interval for refreshing state. This field is displayed only when the IPv6 PIM neighbor is operating in IPv6 PIM-DM mode and the state refresh feature is enabled.
Neighbor tracking	Neighbor tracking status: enabled or disabled.
Bidirectional PIM	Whether IPv6 BIDIR-PIM is enabled.
Secondary address(es)	Secondary IPv6 address (non-link-local address) of the IPv6 PIM neighbor.

## display ipv6 pim routing-table

Use **display ipv6 pim routing-table** to display IPv6 PIM routing entries.

### Syntax

```

display ipv6 pim [ vpn-instance vpn-instance-name ] routing-table [ ipv6-group-address [ prefix-length ]
| ipv6-source-address [ prefix-length ] | flags flag-value | fsm | incoming-interface interface-type
interface-number | mode mode-type | outgoing-interface { exclude | include | match } interface-type
interface-number ] *

```

### Views

Any view

### Predefined user roles

network-admin  
network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays IPv6 PIM routing entries on the public network.

*ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers from 0 to F. If you do not specify an IPv6 multicast group, the command displays IPv6 PIM routing entries for all IPv6 multicast groups.

*ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address.

*prefix-length*: Specifies a prefix length of the IPv6 multicast group or IPv6 multicast source address. The default value is 128. For an IPv6 multicast group address, the value for this argument is in the range of 8 to 128. For an IPv6 multicast source address, the value for this argument is in the range of 0 to 128.

**flags** *flag-value*: Specifies a flag. If you do not specify a flag, the command displays IPv6 PIM routing entries that contain all flags.

The following lists the values for the *flag-value* argument and their meanings:

- **act**: Specifies IPv6 PIM routing entries that have been used for routing data.
- **del**: Specifies IPv6 PIM routing entries to be deleted.
- **exprune**: Specifies IPv6 PIM routing entries that contain outgoing interfaces pruned by other IPv6 multicast routing protocols.
- **ext**: Specifies IPv6 PIM routing entries that contain outgoing interfaces provided by other multicast routing protocols.
- **loc**: Specifies IPv6 PIM routing entries on the devices that reside on the same subnet as the IPv6 multicast source.
- **niif**: Specifies IPv6 PIM routing entries that contain unknown incoming interfaces.
- **nonbr**: Specifies IPv6 PIM routing entries with IPv6 PIM neighbor lookup failure.
- **rpt**: Specifies IPv6 PIM routing entries on the RPT branches where (S, G) prunes have been sent to the RP.
- **spt**: Specifies IPv6 PIM routing entries on the SPT.
- **swt**: Specifies IPv6 PIM routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies IPv6 PIM routing entries with wildcards.

**fsm**: Displays detailed information about the finite state machine.

**incoming-interface** *interface-type interface-number*: Specifies an incoming interface. If you do not specify an incoming interface, the command displays IPv6 PIM routing entries that contain all incoming interfaces.

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

**mode** *mode-type*: Specifies an IPv6 PIM mode. If you do not specify an IPv6 PIM mode, the command displays IPv6 PIM routing entries in all modes. The available IPv6 PIM modes include:

- **bidir**: Specifies IPv6 BIDIR-PIM.
- **dm**: Specifies IPv6 PIM-DM.
- **sm**: Specifies IPv6 PIM-SM.
- **ssm**: Specifies IPv6 PIM-SSM.

**outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*: Specifies an outgoing interface. If you do not specify an outgoing interface, the command displays IPv6 PIM routing entries that

contain all outgoing interfaces. Whether the specified outgoing interface is contained in the IPv6 PIM routing table depends on the following conditions:

- If you specify an excluded interface, the command displays IPv6 PIM routing entries that do not contain the specified outgoing interface.
- If you specify an included interface, the command displays IPv6 PIM routing entries that contain the specified outgoing interface.
- If you specify a matching interface, the command displays IPv6 PIM routing entries that contain only the specified outgoing interface.

## Examples

# Display IPv6 PIM routing entries on the public network.

```
<Sysname> display ipv6 pim 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 IPv6 PIM routing entries on the public network.

```
<Sysname> display ipv6 pim 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 94 Command output**

Field	Description
Total 0 (*, G) entry; 1 (S, G) entry	Total number of (S, G) entries and (*, G) entries.
(2001::2, FFE3::101)	(S, G) entry.
Protocol	IPv6 PIM mode: IPv6 PIM-SM or IPv6 PIM-DM.
Flag	Flag of the (S, G) entry or (*, G) entry: <ul style="list-style-type: none"><li>• <b>ACT</b>—The entry has been used for routing data.</li><li>• <b>DEL</b>—The entry will be removed.</li><li>• <b>EXPRUNE</b>—Some outgoing interfaces are pruned by other IPv6 multicast routing protocols.</li><li>• <b>EXT</b>—The entry contains outgoing interfaces provided by other multicast routing protocols.</li><li>• <b>LOC</b>—The entry is on a router directly connected to the same subnet with the IPv6 multicast source.</li><li>• <b>NIIF</b>—The entry contains unknown incoming interfaces.</li><li>• <b>NONBR</b>—The entry has an IPv6 PIM neighbor lookup failure.</li><li>• <b>RPT</b>—The entry is on an RPT branch where (S, G) prunes have been sent to the RP.</li><li>• <b>SPT</b>—The entry is on the SPT.</li><li>• <b>SWT</b>—The entry is in the process of RPT-to-SPT switchover.</li><li>• <b>WC</b>—The entry contains a wildcard.</li></ul>
Uptime	Length of time since the (S, G) entry or (*, G) entry was installed.
Upstream interface	Upstream (incoming) interface of the (S, G) entry or (*, G) entry.
Upstream neighbor	Upstream neighbor of the (S, G) entry or (*, G) entry.
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry: <ul style="list-style-type: none"><li>• For a (*, G) entry, if the RPF neighbor is the RP, the field displays <b>NULL</b>.</li><li>• For an (S, G) entry, if the RPF neighbor is a router that directly connects to the IPv6 multicast source, this field displays <b>NULL</b>.</li></ul>
Downstream interface(s) information	Information about the downstream interfaces: <ul style="list-style-type: none"><li>• Total number of downstream interfaces.</li><li>• Names of the downstream interfaces.</li><li>• Protocol type on the downstream interfaces.</li><li>• Uptime of the downstream interfaces.</li><li>• Expiration time of the downstream interfaces.</li></ul>

## display ipv6 pim rp-info

Use **display ipv6 pim rp-info** to display RP information in the IPv6 PIM-SM domain.

## Syntax

```
display ipv6 pim [ vpn-instance vpn-instance-name ] rp-info [ ipv6-group-address ]
```

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays RP information on the public network.

*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 numbers from 0 to F. If you do not specify an IPv6 multicast group, the command displays RP information for all IPv6 multicast groups.

## Examples

# Display information about the RP for the IPv6 multicast group FF0E::101 on the public network.

```
<Sysname> display ipv6 pim rp-info ff0e::101
```

```
BSR RP address is: 7:12::1
```

```
Priority: 192
```

```
HoldTime: 180
```

```
Uptime: 03:01:10
```

```
Expires: 00:02:30
```

```
Static RP address is: 7:12::1
```

```
Preferred: No
```

```
Configured ACL: 2003
```

```
RP mapping for this group is: 7:12::1 (local host)
```

# Display information about all RPs for all IPv6 multicast groups.

```
<Sysname> display ipv6 pim rp-info
```

```
BSR RP information:
```

```
Scope: non-scoped
```

```
Group/MaskLen: FF00::/8
```

RP address	Priority	HoldTime	Uptime	Expires
8:12::2 (local)	192	180	03:01:36	00:02:29

```
Group/MaskLen: FF23::/92 [B]
```

RP address	Priority	HoldTime	Uptime	Expires
7:12::1 (local)	192	180	00:00:39	00:02:57

```
Static RP information:
```

RP address	ACL	Mode	Preferred
3:3::1	2000	pim-sm	No
3:3::2	2001	bidir	Yes
3:3::3	2002	pim-sm	No

```

3:3::4                pim-sm No
3:3::5                2002 pim-sm Yes

```

**Table 95 Command output**

Field	Description
Group/MaskLen	IPv6 multicast group to which the RP is designated.
[B]	The RP provides services for IPv6 multicast groups in the BIDIR-PIM domain. If this field is not displayed, the RP provides services for groups in the IPv6 PIM-SM domain.
RP address	IPv6 address of the RP. If the RP resides on the device where the command is executed, this field displays <b>(local)</b> after the address.
Priority	Priority of the RP.
HoldTime	RP lifetime.
Uptime	Length of time the RP has been up.
Expires	Remaining lifetime for the RP.
Preferred	Whether the static RP is preferred.
Configured ACL/ACL	ACL defining the IPv6 multicast groups to which the static RP is designated.
Mode	RP service mode: IPv6 PIM-SM or IPv6 BIDIR-PIM.
RP mapping for this group	IPv6 address of the RP that provides services for the IPv6 multicast group.

## display ipv6 pim statistics

Use **display ipv6 pim statistics** to display statistics for IPv6 PIM packets.

### Syntax

**display ipv6 pim statistics**

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Examples

# Display statistics for IPv6 PIM packets.

```
<Sysname> display ipv6 pim statistics
```

```
Received PIM packets: 3295
```

```
Sent PIM packets      : 5975
```

	Valid	Invalid	Succeeded	Failed
Hello	: 3128	0	4333	0
Reg	: 14	0	0	0
Reg-stop	: 0	0	0	0
JP	: 151	0	561	0
BSM	: 0	0	1081	0



```

Assert      : 0          0          0          0
Graft       : 0          0          0          0
Graft-ACK   : 0          0          0          0
C-RP        : 0          0          0          0
SRM         : 0          0          0          0
DF          : 0          0          0          0

```

**Table 96 Command output**

Field	Description
Received PIM packets	Total number of received IPv6 PIM packets.
Sent PIM packets	Total number of sent IPv6 PIM packets.
Valid	Number of received valid IPv6 PIM packets.
Invalid	Number of received invalid IPv6 PIM packets.
Succeeded	Number of valid IPv6 PIM packets that were sent successfully.
Failed	Number of valid IPv6 PIM packets that failed to be sent.
Hello	Hello message statistics.
Reg	Register message statistics.
Reg-stop	Register-stop message statistics.
JP	Join/prune message statistics.
BSM	Bootstrap message statistics.
Assert	Assert message statistics.
Graft	Graft message statistics.
Graft-ACK	Graft-ACK message statistics.
C-RP	C-RP message statistics.
SRM	State refresh message statistics.
DF	Designated forwarder message statistics

## hello-option dr-priority (IPv6 PIM view)

Use **hello-option dr-priority** to set the global DR priority.

Use **undo hello-option dr-priority** to restore the default.

### Syntax

**hello-option dr-priority** *priority*

**undo hello-option dr-priority**

### Default

The global DR priority is 1.

### Views

IPv6 PIM view

## Predefined user roles

network-admin

## Parameters

*priority*: Sets a DR priority in the range of 0 to 4294967295. A larger value represents a higher priority.

## Usage guidelines

You can set the DR priority for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

## Examples

```
# Set the global DR priority to 3 on the public network.
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] hello-option dr-priority 3
```

## Related commands

**ipv6 pim hello-option dr-priority**

# hello-option holdtime (IPv6 PIM view)

Use **hello-option holdtime** to set the global IPv6 PIM neighbor lifetime.

Use **undo hello-option holdtime** to restore the default.

## Syntax

```
hello-option holdtime time
undo hello-option holdtime
```

## Default

The global IPv6 PIM neighbor lifetime is 105 seconds.

## Views

IPv6 PIM view

## Predefined user roles

network-admin

## Parameters

*time*: Sets an IPv6 PIM neighbor lifetime in the range of 1 to 65535 seconds. If you set the value to 65535 seconds, the IPv6 PIM neighbors are always reachable.

## Usage guidelines

You can set the IPv6 PIM neighbor lifetime for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

## Examples

```
# Set the global IPv6 PIM neighbor lifetime to 120 seconds on the public network.
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] hello-option holdtime 120
```

## Related commands

**ipv6 pim hello-option holdtime**

# hello-option lan-delay (IPv6 PIM view)

Use **hello-option lan-delay** to set the global IPv6 PIM message propagation delay on a shared-media LAN.

Use **undo hello-option lan-delay** to restore the default.

## Syntax

**hello-option lan-delay** *delay*

**undo hello-option lan-delay**

## Default

The global IPv6 PIM message propagation delay on a shared-media LAN is 500 milliseconds.

## Views

IPv6 PIM view

## Predefined user roles

network-admin

## Parameters

*delay*: Sets an IPv6 PIM message propagation delay on a shared-media LAN in the range of 1 to 32767 milliseconds.

## Usage guidelines

You can set the IPv6 PIM message propagation delay on a shared-media LAN for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

## Examples

```
# Set the global IPv6 PIM message propagation delay on a shared-media LAN to 200 milliseconds on the public network.
```

```
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] hello-option lan-delay 200
```

## Related commands

- **hello-option override-interval** (IPv6 PIM view)
- **ipv6 pim hello-option lan-delay**
- **ipv6 pim hello-option override-interval**

# hello-option neighbor-tracking (IPv6 PIM view)

Use **hello-option neighbor-tracking** to enable neighbor tracking globally and disable join message suppression.

Use **undo hello-option neighbor-tracking** to restore the default.

## Syntax

```
hello-option neighbor-tracking  
undo hello-option neighbor-tracking
```

## Default

Neighbor tracking is disabled, and join message suppression is enabled.

## Views

IPv6 PIM view

## Predefined user roles

network-admin

## Usage guidelines

You can enable neighbor tracking for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

## Examples

```
# Enable neighbor tracking globally on the public network.  
<Sysname> system-view  
[Sysname] ipv6 pim  
[Sysname-pim6] hello-option neighbor-tracking
```

## Related commands

```
ipv6 pim hello-option neighbor-tracking
```

# ipv6 pim passive

Use **ipv6 pim passive** to enable IPv6 PIM passive mode on an interface.

Use **undo ipv6 pim passive** to restore the default.

## Syntax

```
ipv6 pim passive  
undo ipv6 pim passive
```

## Default

The IPv6 PIM passive mode is disabled for an interface.

## Views

Interface view

## Predefined user roles

network-admin

## Usage guidelines

This command takes effect only when IPv6 PIM-DM or IPv6 PIM-SM is enabled on the interface.

## Examples

```
# On the public network, enable IPv6 multicast routing. Then, enable IPv6 PIM-DM and IPv6 PIM passive mode on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim dm
[Sysname-Vlan-interface100] ipv6 pim passive
```

## hello-option override-interval (IPv6 PIM view)

Use **hello-option override-interval** to set the global override interval.

Use **undo hello-option override-interval** to restore the default.

### Syntax

**hello-option override-interval** *interval*

**undo hello-option override-interval**

### Default

The global override interval is 2500 milliseconds.

### Views

IPv6 PIM view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets an override interval in the range of 1 to 65535 milliseconds.

### Usage guidelines

You can set the override interval for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

### Examples

```
# Set the global override interval to 2000 milliseconds on the public network.
```

```
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] hello-option override-interval 2000
```

### Related commands

- **hello-option lan-delay** (IPv6 PIM view)
- **ipv6 pim hello-option lan-delay**
- **ipv6 pim hello-option override-interval**

## holdtime join-prune (IPv6 PIM view)

Use **holdtime join-prune** to set the global joined/pruned state holdtime timer.

Use **undo holdtime join-prune** to restore the default.

## Syntax

```
holdtime join-prune time  
undo holdtime join-prune
```

## Default

The global joined/pruned state holdtime timer is 210 seconds.

## Views

IPv6 PIM view

## Predefined user roles

network-admin

## Parameters

*time*: Sets a joined/pruned state holdtime timer in the range of 1 to 65535 seconds.

## Usage guidelines

You can set the joined/pruned state holdtime timer for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

To prevent the upstream neighbors from aging out, you must configure the join/prune interval to be less than the joined/pruned state holdtime timer.

## Examples

```
# Set the global joined/pruned state holdtime timer to 280 seconds on the public network.  
<Sysname> system-view  
[Sysname] ipv6 pim  
[Sysname-pim6] holdtime join-prune 280
```

## Related commands

- **ipv6 pim holdtime join-prune**
- **timer join-prune** (IPv6 PIM view)

# ipv6 pim

Use **ipv6 pim** to enter IPv6 PIM view.

Use **undo ipv6 pim** to remove all configurations in IPv6 PIM view.

## Syntax

```
ipv6 pim [ vpn-instance vpn-instance-name ]  
undo ipv6 pim [ vpn-instance vpn-instance-name ]
```

## Views

System view

## Predefined user roles

network-admin

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, you enter public network IPv6 PIM view.

## Examples

# Enable IPv6 multicast routing on the public network and enter public network IPv6 PIM view.

```
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib6] quit
[Sysname] ipv6 pim
[Sysname-pim6]
```

# Enable IPv6 multicast routing in VPN instance **mvpn** and enter IPv6 PIM view of VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] ipv6 multicast routing vpn-instance mvpn
[Sysname-mrib6-mvpn] quit
[Sysname] ipv6 pim vpn-instance mvpn
[Sysname-pim6-mvpn]
```

## ipv6 pim bfd enable

Use **ipv6 pim bfd enable** to enable BFD for IPv6 PIM.

Use **undo ipv6 pim bfd enable** to disable BFD for IPv6 PIM.

## Syntax

**ipv6 pim bfd enable**

**undo ipv6 pim bfd enable**

## Default

BFD is disabled for IPv6 PIM.

## Views

Interface view

## Predefined user roles

network-admin

## Usage guidelines

This command takes effect only when IPv6 PIM-DM or IPv6 PIM-SM is enabled on the interface.

## Examples

# On the public network, enable IPv6 multicast routing, enable IPv6 PIM-DM on interface VLAN-interface 100, and enable BFD for IPv6 PIM on the interface.

```
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib6] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim dm
[Sysname-Vlan-interface100] ipv6 pim bfd enable
```

## Related commands

- **ipv6 pim dm**
- **ipv6 pim sm**

# ipv6 pim bsr-boundary

Use **ipv6 pim bsr-boundary** to configure an IPv6 PIM domain border (a bootstrap message boundary).

Use **ipv6 pim bsr-boundary** to remove the configured IPv6 PIM-SM domain border.

## Syntax

**ipv6 pim bsr-boundary**

**undo ipv6 pim bsr-boundary**

## Default

No IPv6 PIM-SM domain border is configured.

## Views

Interface view

## Predefined user roles

network-admin

## Examples

```
# Configure VLAN-interface 100 as an IPv6 PIM-SM domain border.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] ipv6 pim bsr-boundary
```

## Related commands

- **c-bsr** (IPv6 PIM view)
- **ipv6 multicast boundary**

# ipv6 pim dm

Use **ipv6 pim dm** to enable IPv6 PIM-DM.

Use **undo ipv6 pim dm** to disable IPv6 PIM-DM.

## Syntax

**ipv6 pim dm**

**undo ipv6 pim dm**

## Default

IPv6 PIM-DM is disabled.

## Views

Interface view

## Predefined user roles

network-admin



## Usage guidelines

This command takes effect only when IPv6 multicast routing is enabled. If the interface belongs to a VPN instance, make sure IPv6 multicast routing is enabled on the VPN instance.

## Examples

```
# Enable IPv6 multicast routing, and enable IPv6 PIM-DM on VLAN-interface 100 on the public network.
```

```
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib6] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim dm
```

## Related commands

**ipv6 multicast routing**

# ipv6 pim hello-option dr-priority

Use **ipv6 pim hello-option dr-priority** to set the DR priority on an interface.

Use **undo ipv6 pim hello-option dr-priority** to restore the default.

## Syntax

**ipv6 pim hello-option dr-priority** *priority*

**undo ipv6 pim hello-option dr-priority**

## Default

The DR priority on an interface is 1.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*priority*: Sets a DR priority in the range of 0 to 4294967295. A larger value represents a higher priority.

## Usage guidelines

You can set the DR priority for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

## Examples

```
# Set the DR priority to 3 on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim hello-option dr-priority 3
```

## Related commands

**hello-option dr-priority** (IPv6 PIM view)

## ipv6 pim hello-option holdtime

Use **ipv6 pim hello-option holdtime** to set the IPv6 PIM neighbor lifetime on an interface.

Use **undo ipv6 pim hello-option holdtime** to restore the default.

### Syntax

**ipv6 pim hello-option holdtime** *time*

**undo ipv6 pim hello-option holdtime**

### Default

The IPv6 PIM neighbor lifetime is 105 seconds.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

*time*: Sets an IPv6 PIM neighbor lifetime in the range of 1 to 65535 seconds. If you set the value to 65535 seconds, the IPv6 PIM neighbor is always reachable.

### Usage guidelines

You can set the IPv6 PIM neighbor lifetime for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

### Examples

```
# Sets the IPv6 PIM neighbor lifetime to 120 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim hello-option holdtime 120
```

### Related commands

**hello-option holdtime** (IPv6 PIM view)

## ipv6 pim hello-option lan-delay

Use **ipv6 pim hello-option lan-delay** to set the IPv6 PIM message propagation delay on a shared-media LAN for an interface.

Use **undo ipv6 pim hello-option lan-delay** to restore the default.

### Syntax

**ipv6 pim hello-option lan-delay** *delay*

**undo ipv6 pim hello-option lan-delay**

### Default

The IPv6 PIM message propagation delay on a shared-media LAN is 500 milliseconds.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*delay*: Sets an IPv6 PIM message propagation delay on a shared-media LAN in the range of 1 to 32767 milliseconds.

## Usage guidelines

You can set the IPv6 PIM message propagation delay on a shared-media LAN for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

## Examples

```
# Set the IPv6 PIM message propagation delay on a shared-media LAN to 200 milliseconds on
VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim hello-option lan-delay 200
```

## Related commands

- **hello-option lan-delay** (IPv6 PIM view)
- **hello-option override-interval** (IPv6 PIM view)
- **ipv6 pim hello-option override-interval**

# ipv6 pim hello-option neighbor-tracking

Use **ipv6 pim hello-option neighbor-tracking** to enable neighbor tracking and disable join message suppression on an interface.

Use **ipv6 pim hello-option neighbor-tracking disable** to disable neighbor tracking on an interface when join message suppression is disabled globally.

Use **undo ipv6 pim hello-option neighbor-tracking** to restore neighbor tracking on an interface to be consistent with the global setting.

## Syntax

**ipv6 pim hello-option neighbor-tracking**

**ipv6 pim hello-option neighbor-tracking disable**

**undo ipv6 pim hello-option neighbor-tracking**

## Default

Neighbor tracking is disabled, and join message suppression is enabled.

## Views

Interface view

## Predefined user roles

network-admin

## Usage guidelines

You can enable neighbor tracking for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

## Examples

```
# Enable neighbor tracking on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim hello-option neighbor-tracking
```

```
# On the public network, disable neighbor tracking on VLAN-interface 100 when neighbor tracking is enabled globally.
```

```
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] hello-option neighbor-tracking
[Sysname-pim6] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim hello-option neighbor-tracking disable
```

## Related commands

**hello-option neighbor-tracking** (IPv6 PIM view)

# ipv6 pim hello-option override-interval

Use **ipv6 pim hello-option override-interval** to set the override interval on an interface.

Use **undo ipv6 pim hello-option override-interval** to restore the default.

## Syntax

```
ipv6 pim hello-option override-interval interval
```

```
undo ipv6 pim hello-option override-interval
```

## Default

The override interval is 2500 milliseconds.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets an override interval in the range of 1 to 65535 milliseconds.

## Usage guidelines

You can set the override interval for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

## Examples

```
# Set the override interval to 2000 milliseconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim hello-option override-interval 2000
```

### Related commands

- **hello-option lan-delay** (IPv6 PIM view)
- **hello-option override-interval** (IPv6 PIM view)
- **ipv6 pim hello-option lan-delay**

## ipv6 pim holdtime join-prune

Use **ipv6 pim holdtime join-prune** to set the joined/pruned state holdtime timer on an interface.

Use **undo ipv6 pim holdtime join-prune** to restore the default.

### Syntax

```
ipv6 pim holdtime join-prune time
```

```
undo ipv6 pim holdtime join-prune
```

### Default

The joined/pruned state holdtime timer is 210 seconds.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

*time*: Sets a joined/pruned state holdtime timer in the range of 1 to 65535 seconds.

### Usage guidelines

You can set the joined/pruned state holdtime timer for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

To prevent the upstream neighbors from aging out, you must configure the join/prune interval to be less than the joined/pruned state holdtime timer.

### Examples

```
# Set the joined/pruned state holdtime timer to 280 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim holdtime join-prune 280
```

### Related commands

- **holdtime join-prune** (IPv6 PIM view)
- **ipv6 pim timer join-prune**

## ipv6 pim neighbor-policy

Use **ipv6 pim neighbor-policy** to configure an IPv6 PIM hello policy to define the legal source address range for hello messages.

Use **undo ipv6 pim neighbor-policy** to restore the default.

### Syntax

```
ipv6 pim neighbor-policy acl6-number
```

```
undo ipv6 pim neighbor-policy
```

### Default

IPv6 PIM hello policies are not configured, and all the received hello messages are considered legal.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

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

### Usage guidelines

You can configure this command to guard against hello message spoofing.

In an IPv6 basic ACL, the **source** keyword matches the source address in hello messages.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

### Examples

```
# Configure an IPv6 PIM hello policy 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] ipv6 pim neighbor-policy 2000
```

## ipv6 pim require-genid

Use **ipv6 pim require-genid** to enable dropping hello messages without the generation ID options.

Use **undo ipv6 pim require-genid** to restore the default.

### Syntax

```
ipv6 pim require-genid
```

```
undo ipv6 pim require-genid
```

### Default

Hello messages without the generation ID options are accepted.

## Views

Interface view

## Predefined user roles

network-admin

## Examples

```
# Enable VLAN-interface 100 to drop hello messages without the generation ID options.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim require-genid
```

# ipv6 pim sm

Use **ipv6 pim sm** to enable IPv6 PIM-SM.

Use **undo ipv6 pim sm** to disable IPv6 PIM-SM.

## Syntax

**ipv6 pim sm**

**undo ipv6 pim sm**

## Default

IPv6 PIM-SM is disabled.

## Views

Interface view

## Predefined user roles

network-admin

## Usage guidelines

This command takes effect only when IPv6 multicast routing is enabled. If the interface belongs to a VPN instance, make sure IPv6 multicast routing is enabled on the VPN instance.

## Examples

```
# On the public network, enable IPv6 multicast routing, and enable IPv6 PIM-SM on VLAN-interface 100.
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib6] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim sm
```

## Related commands

**ipv6 multicast routing**

# ipv6 pim state-refresh-capable

Use **ipv6 pim state-refresh-capable** to enable the state refresh feature on an interface.

Use **undo ipv6 pim state-refresh-capable** to disable the state refresh feature.

## Syntax

```
ipv6 pim state-refresh-capable
undo ipv6 pim state-refresh-capable
```

## Default

The state refresh feature is enabled.

## Views

Interface view

## Predefined user roles

network-admin

## Examples

```
# Disable state refresh on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo ipv6 pim state-refresh-capable
```

## Related commands

- **state-refresh-hoplimit** (IPv6 PIM view)
- **state-refresh-interval** (IPv6 PIM view)
- **state-refresh-rate-limit** (IPv6 PIM view)

# ipv6 pim timer graft-retry

Use **ipv6 pim timer graft-retry** to set a graft retry timer.

Use **undo ipv6 pim timer graft-retry** to restore the default.

## Syntax

```
ipv6 pim timer graft-retry interval
undo ipv6 pim timer graft-retry
```

## Default

The graft retry timer is 3 seconds.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets a graft retry timer in the range of 1 to 65535 seconds.

## Examples

```
# Set the graft retry timer to 80 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim timer graft-retry 80
```



## ipv6 pim timer hello

Use **ipv6 pim timer hello** to set the hello interval on an interface.

Use **undo ipv6 pim timer hello** to restore the default.

### Syntax

**ipv6 pim timer hello** *interval*

**undo ipv6 pim timer hello**

### Default

The hello interval is 30 seconds.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets a hello interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send hello messages.

### Usage guidelines

You can set the hello interval for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

### Examples

```
# Set the hello interval to 40 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim timer hello 40
```

### Related commands

**timer hello** (IPv6 PIM view)

## ipv6 pim timer join-prune

Use **ipv6 pim timer join-prune** to set the join/prune interval on an interface.

Use **undo ipv6 pim timer join-prune** to restore the default.

### Syntax

**ipv6 pim timer join-prune** *interval*

**undo ipv6 pim timer join-prune**

### Default

The join/prune interval is 60 seconds.

### Views

Interface view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets a join/prune interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send join or prune messages.

## Usage guidelines

You can set the join/prune interval for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

The configuration takes effect after the current interval ends.

To prevent the upstream neighbors from aging out, you must configure the interval for sending join/prune messages to be less than the joined/pruned state holdtime timer.

## Examples

```
# Set the join/prune interval to 80 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim timer join-prune 80
```

## Related commands

- **ipv6 pim holdtime join-prune**
- **timer join-prune** (IPv6 PIM view)

# ipv6 pim triggered-hello-delay

Use **ipv6 pim triggered-hello-delay** to set the triggered hello delay.

Use **undo ipv6 pim triggered-hello-delay** to restore the default.

## Syntax

```
ipv6 pim triggered-hello-delay delay
undo ipv6 pim triggered-hello-delay
```

## Default

The triggered hello delay is 5 seconds.

## Views

Interface view

## Predefined user roles

network-admin

## Parameters

*delay*: Sets a triggered hello delay in the range of 1 to 60 seconds.

## Usage guidelines

The triggered hello delay defines the maximum delay for sending a hello message.

## Examples

```
# Set the triggered hello delay to 3 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 pim triggered-hello-delay 3
```

## jp-pkt-size (IPv6 PIM view)

Use **jp-pkt-size** to set the maximum size of each join/prune message.

Use **undo jp-pkt-size** to restore the default.

### Syntax

```
jp-pkt-size size
undo jp-pkt-size
```

### Default

The maximum size of a join/prune message is 8100 bytes.

### Views

IPv6 PIM view

### Predefined user roles

network-admin

### Parameters

*size*: Sets the maximum size of each join/prune message, in the range of 100 to 64000 bytes.

## Examples

```
# Set the maximum size of each join/prune message to 1500 bytes on the public network.
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] jp-pkt-size 1500
```

## register-policy (IPv6 PIM view)

Use **register-policy** to configure an IPv6 PIM register policy.

Use **undo register-policy** to remove the configured IPv6 PIM register policy.

### Syntax

```
register-policy acl6-number
undo register-policy
```

### Default

IPv6 PIM register policies are not configured.

### Views

IPv6 PIM view

## Predefined user roles

network-admin

## Parameters

*acl6-number*: Specifies an IPv6 advanced ACL number in the range of 3000 to 3999.

## Usage guidelines

In an IPv6 advanced ACL, the **source** and **destination** keywords match the source address and multicast group address in register messages, respectively.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

## Examples

# On the public network, configure an IPv6 PIM register policy to accept the register messages from the sources on the subnet of **3:1::/64** to the groups on the subnet of **FF0E:13::/64**.

```
<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] ipv6 pim
[Sysname-pim6] register-policy 3000
```

# register-whole-checksum (IPv6 PIM view)

Use **register-whole-checksum** to configure the switch to calculate the checksum based on an entire register message.

Use **undo register-whole-checksum** to restore the default.

## Syntax

**register-whole-checksum**

**undo register-whole-checksum**

## Default

The switch calculates the checksum based on the register message header.

## Views

IPv6 PIM view

## Predefined user roles

network-admin

## Examples

# On the public network, configure the switch to calculate the checksum based on an entire register message.

```
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] register-whole-checksum
```

## source-lifetime (IPv6 PIM view)

Use **source-lifetime** to set the IPv6 multicast source lifetime.

Use **undo source-lifetime** to restore the default.

### Syntax

**source-lifetime** *time*

**undo source-lifetime**

### Default

The IPv6 multicast source lifetime is 210 seconds.

### Views

IPv6 PIM view

### Predefined user roles

network-admin

### Parameters

*time*: Sets an IPv6 multicast source lifetime in the range of 0 to 31536000 seconds. If you set the value to 0 seconds, IPv6 multicast sources are never aged out.

### Examples

# Set the IPv6 multicast source lifetime to 200 seconds on the public network.

```
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] source-lifetime 200
```

## source-policy (IPv6 PIM view)

Use **source-policy** to configure an IPv6 multicast source policy.

Use **undo source-policy** to remove the configured IPv6 multicast source policy.

### Syntax

**source-policy** *acl6-number*

**undo source-policy**

### Default

IPv6 multicast source policies are not configured.

### Views

IPv6 PIM view

### Predefined user roles

network-admin

### Parameters

*acl6-number*: Specifies an IPv6 basic or advanced ACL number in the range of 2000 to 3999.

## Usage guidelines

In an IPv6 basic ACL, the **source** keyword matches the source address in IPv6 multicast data packets. In an IPv6 advanced ACL, the **source** and **destination** keywords match the source address and multicast group address in IPv6 multicast data packets, respectively.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

If you execute this command multiple times, the most recent configuration takes effect.

## Examples

# On the public network, configure an IPv6 multicast source policy to permit IPv6 multicast data from the source **3121::1** and deny data from the source **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] ipv6 pim
[Sysname-pim6] source-policy 2000
[Sysname-pim6] quit
```

## spt-switch-threshold (IPv6 PIM view)

Use **spt-switch-threshold** to configure the switchover to SPT.

Use **undo spt-switch-threshold** to restore the default.

### Syntax

```
spt-switch-threshold { immediacy | infinity } [ group-policy acl6-number ]
undo spt-switch-threshold [ immediacy | infinity ] [ group-policy acl6-number ]
```

### Default

The switch immediately triggers the switchover to SPT after receiving the first IPv6 multicast packet.

### Views

IPv6 PIM view

### Predefined user roles

network-admin

### Parameters

**immediacy**: Triggers the switchover to SPT immediately.

**infinity**: Disables the switchover to SPT.

**group-policy** *acl6-number*: Specifies an IPv6 basic ACL number in the range of 2000 to 2999. If you specify an ACL, the configuration applies to the IPv6 multicast groups that the ACL permits. The configuration applies to all IPv6 multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

## Usage guidelines

---

### CAUTION:

If the device is an RP, disabling the switchover to SPT might cause multicast traffic forwarding failures on the source-side DR. When disabling the switchover to SPT, be sure you fully understand its impact on your network.

---

In an IPv6 basic ACL, the **source** keyword matches the multicast group address in IPv6 multicast packets. If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

## Examples

```
# Disable the switchover to SPT on receiver-side DR on the public network.
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] spt-switch-threshold infinity
```

## ssm-policy (IPv6 PIM view)

Use **ssm-policy** to configure the IPv6 SSM group range.

Use **undo ssm-policy** to restore the default.

## Syntax

```
ssm-policy acl6-number
undo ssm-policy
```

## Default

The IPv6 SSM group range is FF3x::/32, where x can be any valid scope.

## Views

IPv6 PIM view

## Predefined user roles

network-admin

## Parameters

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

## Usage guidelines

In an IPv6 basic ACL, the **source** keyword matches the multicast group address in MLD reports.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

You can use this command to define an IPv6 multicast group address range. If a packet to an IPv6 multicast group is permitted by the used ACL, the multicast mode for the packet 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] ipv6 pim
[Sysname-pim6] ssm-policy 2000
```

## state-refresh-hoplimit (IPv6 PIM view)

Use **state-refresh-hoplimit** to set the hop limit for state refresh messages.

Use **undo state-refresh-hoplimit** to restore the default.

### Syntax

```
state-refresh-hoplimit hoplimit-value
```

```
undo state-refresh-hoplimit
```

### Default

The hop limit for state refresh messages is 255.

### Views

IPv6 PIM view

### Predefined user roles

network-admin

### Parameters

*hoplimit-value*: Sets a hop limit for state refresh messages, in the range of 1 to 255.

### Examples

```
# Set the hop limit for state refresh messages to 45 on the public network.
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] state-refresh-hoplimit 45
```

### Related commands

- **ipv6 pim state-refresh-capable**
- **state-refresh-interval** (IPv6 PIM view)
- **state-refresh-rate-limit** (IPv6 PIM view)

## state-refresh-interval (IPv6 PIM view)

Use **state-refresh-interval** to set the state refresh interval.

Use **undo state-refresh-interval** to restore the default.

### Syntax

```
state-refresh-interval interval
```

```
undo state-refresh-interval
```

### Default

The state refresh interval is 60 seconds.



## Views

IPv6 PIM view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets a state refresh interval in the range of 1 to 255 seconds.

## Examples

# Set the state refresh interval to 70 seconds on the public network.

```
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] state-refresh-interval 70
```

## Related commands

- **ipv6 pim state-refresh-capable**
- **state-refresh-hoplimit** (IPv6 PIM view)
- **state-refresh-rate-limit** (IPv6 PIM view)

# state-refresh-rate-limit (IPv6 PIM view)

Use **state-refresh-rate-limit** to set the amount of time that the switch waits before accepting a new state refresh message.

Use **undo state-refresh-rate-limit** to restore the default.

## Syntax

**state-refresh-rate-limit** *time*

**undo state-refresh-rate-limit**

## Default

The switch waits 30 seconds before it accepts a new state refresh message.

## Views

IPv6 PIM view

## Predefined user roles

network-admin

## Parameters

*time*: Sets an amount of time that the switch waits before accepting a new refresh message, in the range of 1 to 65535 seconds.

## Examples

# On the public network, set the switch to wait 45 seconds before it accepts a new state refresh message.

```
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] state-refresh-rate-limit 45
```

## Related commands

- **ipv6 pim state-refresh-capable**
- **state-refresh-hoplimit** (IPv6 PIM view)
- **state-refresh-interval** (IPv6 PIM view)

## static-rp (IPv6 PIM view)

Use **static-rp** to configure a static RP.

Use **undo static-rp** to remove a static RP.

### Syntax

```
static-rp ipv6-rp-address [ acl6-number | bidir | preferred ] *
```

```
undo static-rp ipv6-rp-address
```

### Default

No static RP is configured.

### Views

IPv6 PIM view

### Predefined user roles

network-admin

### Parameters

*ipv6-rp-address*: Specifies the IPv6 address of the static RP. This address must be a valid IPv6 global unicast address.

*acl6-number*: Specifies an IPv6 basic ACL number in the range of 2000 to 2999 to filter IPv6 multicast groups. The C-RP is designated only to IPv6 multicast groups that the ACL permits. The static RP is designated to all IPv6 multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not contain valid rules.

**bidir**: Specifies IPv6 BIDIR-PIM to which the static RP is designated. If you do not specify this keyword, the PIM mode is IPv6 PIM-SM.

**preferred**: Gives priority to the static RP if the static RP and the dynamic RP exist at the same time in the network. The dynamic RP takes effect only if no static RP exists in the network. If you do not specify this keyword, the dynamic RP has priority. The static RP takes effect only if no dynamic RP exists in the network or when the dynamic RP fails.

### Usage guidelines

You do not need to enable IPv6 PIM on an interface that acts as a static RP.

In an IPv6 basic ACL, the **source** keyword matches the multicast group address in IPv6 multicast packets.

If you specify the **vpn-instance** keyword in an ACL rule, the rule does not take effect. The other optional parameters except the **time-range** keyword and the **fragment** keyword in the ACL rules are ignored.

When the ACL rules used by a static RP change, new RPs must be elected for all IPv6 multicast groups.

You can configure multiple static RPs by using this command multiple times. However, if you specify the same static RP address or reference the same ACL in the commands, the most recent configuration takes effect. If you configure multiple static RPs for the same IPv6 multicast group, the static RP with the highest IPv6 address is used.

## Examples

```
# On the public network, configure the interface with the IPv6 address of 2001::2 as a static RP for the IPv6 multicast groups FF03::101/64, and give priority to this static RP.
```

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source ff03::101 64
[Sysname-acl6-basic-2001] quit
[Sysname] ipv6 pim
[Sysname-pim6] static-rp 2001::2 2001 preferred
```

## Related commands

**display ipv6 pim rp-info**

## timer hello (IPv6 PIM view)

Use **timer hello** to set the global hello interval.

Use **undo timer hello** to restore the default.

## Syntax

**timer hello** *interval*

**undo timer hello**

## Default

The global hello interval is 30 seconds.

## Views

IPv6 PIM view

## Predefined user roles

network-admin

## Parameters

*interval*: Sets a hello interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send hello messages.

## Usage guidelines

You can set the hello interval for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

## Examples

```
# Set the global hello interval to 40 seconds on the public network.
```

```
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] timer hello 40
```

## Related commands

**ipv6 pim timer hello**

## timer join-prune (IPv6 PIM view)

Use **timer join-prune** to set the global join/prune interval.

Use **undo timer join-prune** to restore the default.

### Syntax

**timer join-prune** *interval*

**undo timer join-prune**

### Default

The global join/prune interval is 60 seconds.

### Views

IPv6 PIM view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets a join/prune interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send join or prune messages.

### Usage guidelines

You can set the join/prune interval for all interfaces in IPv6 PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in IPv6 PIM view.

The configuration takes effect after the current interval ends.

To prevent the upstream neighbors from aging out, you must configure the interval for sending join/prune messages to be less than the joined/pruned state holdtime timer.

### Examples

```
# Set the global join/prune interval to 80 seconds on the public network.
```

```
<Sysname> system-view
[Sysname] ipv6 pim
[Sysname-pim6] timer join-prune 80
```

### Related commands

- **holdtime join-prune** (IPv6 PIM view)
- **ipv6 pim timer join-prune**

---

# 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
<b>Boldface</b>	<b>Bold</b> 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
<b>Boldface</b>	Window names, button names, field names, and menu items are in bold text. For example, the <b>New User</b> window appears; click <b>OK</b> .
>	Multi-level menus are separated by angle brackets. For example, <b>File &gt; Create &gt; Folder</b> .

## Symbols

Convention	Description
 <b>WARNING</b>	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 <b>CAUTION</b>	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.
 <b>IMPORTANT</b>	An alert that calls attention to essential information.
<b>NOTE</b>	An alert that contains additional or supplementary information.
 <b>TIP</b>	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 mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load-balancing device.
	Represents a security card, such as a firewall, load-balancing, NetStream, SSL VPN, IPS, or ACG 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](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [V](#)

### A

auto-rp enable, [112](#)

### B

bidir-pim enable (IPv6 PIM view), [299](#)

bidir-pim enable (PIM view), [112](#)

bidir-rp-limit (IPv6 PIM view), [299](#)

bidir-rp-limit (PIM view), [113](#)

bsm-fragment enable (IPv6 PIM view), [300](#)

bsm-fragment enable (PIM view), [114](#)

bsr-policy (IPv6 PIM view), [301](#)

bsr-policy (PIM view), [114](#)

### C

cache-sa-enable, [163](#)

c-bsr (IPv6 PIM view), [301](#)

c-bsr (PIM view), [115](#)

c-rp (IPv6 PIM view), [302](#)

c-rp (PIM view), [116](#)

crp-policy (IPv6 PIM view), [304](#)

crp-policy (PIM view), [117](#)

### D

data-delay, [185](#)

data-group, [185](#)

default-group, [186](#)

delete ip rpf-route-static, [63](#)

display igmp group, [86](#)

display igmp interface, [89](#)

display igmp ssm-mapping, [91](#)

display igmp-snooping, [1](#)

display igmp-snooping group, [3](#)

display igmp-snooping router-port, [4](#)

display igmp-snooping static-group, [5](#)

display igmp-snooping static-router-port, [6](#)

display igmp-snooping statistics, [7](#)

display interface register-tunnel, [118](#)

display ipv6 l2-multicast ip, [193](#)

display ipv6 l2-multicast ip forwarding, [194](#)

display ipv6 l2-multicast mac, [195](#)

display ipv6 l2-multicast mac forwarding, [196](#)

display ipv6 mrib interface, [255](#)

display ipv6 multicast boundary, [256](#)

display ipv6 multicast forwarding df-info, [257](#)

display ipv6 multicast forwarding event, [259](#)

display ipv6 multicast forwarding-table, [260](#)

display ipv6 multicast forwarding-table df-list, [263](#)

display ipv6 multicast routing-table, [264](#)

display ipv6 multicast rpf-info, [265](#)

display ipv6 multicast-vlan, [246](#)

display ipv6 multicast-vlan forwarding-table, [248](#)

display ipv6 multicast-vlan group, [247](#)

display ipv6 pim bsr-info, [305](#)

display ipv6 pim claimed-route, [306](#)

display ipv6 pim c-rp, [307](#)

display ipv6 pim df-info, [308](#)

display ipv6 pim interface, [309](#)

display ipv6 pim neighbor, [312](#)

display ipv6 pim routing-table, [313](#)

display ipv6 pim rp-info, [316](#)

display ipv6 pim statistics, [318](#)

display ipv6 pim-snooping neighbor, [238](#)

display ipv6 pim-snooping router-port, [239](#)

display ipv6 pim-snooping routing-table, [240](#)

display ipv6 pim-snooping statistics, [241](#)

display l2-multicast ip, [8](#)

display l2-multicast ip forwarding, [10](#)

display l2-multicast mac, [11](#)

display l2-multicast mac forwarding, [12](#)

display mac-address multicast, [63](#)

display mld group, [273](#)

display mld interface, [276](#)

display mld ssm-mapping, [278](#)

display mld-snooping, [197](#)

display mld-snooping group, [199](#)

display mld-snooping router-port, [201](#)

display mld-snooping static-group, [202](#)



- display mld-snooping static-router-port,203
- display mld-snooping statistics,204
- display mrib interface,65
- display msdp brief,163
- display msdp peer-status,165
- display msdp sa-cache,168
- display msdp sa-count,169
- display multicast boundary,66
- display multicast forwarding df-info,67
- display multicast forwarding event,69
- display multicast forwarding-table,70
- display multicast forwarding-table df-list,72
- display multicast routing-table,73
- display multicast routing-table static,75
- display multicast rpf-info,76
- display multicast-domain data-group receive,187
- display multicast-domain data-group send,189
- display multicast-domain default-group,190
- display multicast-vlan,54
- display multicast-vlan forwarding-table,56
- display multicast-vlan group,55
- display pim bsr-info,121
- display pim claimed-route,122
- display pim c-rp,123
- display pim df-info,125
- display pim interface,126
- display pim neighbor,128
- display pim routing-table,130
- display pim rp-info,132
- display pim statistics,134
- display pim-snooping neighbor,46
- display pim-snooping router-port,47
- display pim-snooping routing-table,48
- display pim-snooping statistics,49
- dot1 p-priority (IGMP-snooping view),13
- dot1 p-priority (MLD-snooping view),205

## E

- enable (IGMP-snooping view),14
- enable (MLD-snooping view),206
- encap-data-enable,170
- entry-limit (IGMP-snooping view),14
- entry-limit (MLD-snooping view),207

## F

- fast-leave (IGMP-snooping view),15

- fast-leave (MLD-snooping view),207

## G

- group-policy (IGMP-snooping view),16
- group-policy (MLD-snooping view),208

## H

- hello-option dr-priority (IPv6 PIM view),319
- hello-option dr-priority (PIM view),135
- hello-option holdtime (IPv6 PIM view),320
- hello-option holdtime (PIM view),136
- hello-option lan-delay (IPv6 PIM view),321
- hello-option lan-delay (PIM view),137
- hello-option neighbor-tracking (IPv6 PIM view),321
- hello-option neighbor-tracking (PIM view),138
- hello-option override-interval (IPv6 PIM view),323
- hello-option override-interval (PIM view),138
- holdtime join-prune (IPv6 PIM view),323
- holdtime join-prune (PIM view),139
- host-aging-time (IGMP-snooping view),17
- host-aging-time (MLD-snooping view),209

## I

- igmp,92
- igmp enable,92
- igmp fast-leave,93
- igmp group-policy,94
- igmp last-member-query-count,95
- igmp last-member-query-interval,96
- igmp max-response-time,96
- igmp non-stop-routing,97
- igmp other-querier-present-interval,98
- igmp query-interval,98
- igmp robust-count,99
- igmp startup-query-count,100
- igmp startup-query-interval,101
- igmp static-group,102
- igmp version,102
- igmp-snooping,18
- igmp-snooping dot1 p-priority,19
- igmp-snooping drop-unknown,20
- igmp-snooping enable,20
- igmp-snooping fast-leave,21
- igmp-snooping general-query source-ip,22
- igmp-snooping group-limit,23
- igmp-snooping group-policy,23

- igmp-snooping host-aging-time,25
- igmp-snooping host-join,26
- igmp-snooping last-member-query-interval,27
- igmp-snooping leave source-ip,28
- igmp-snooping max-response-time,28
- igmp-snooping overflow-replace,29
- igmp-snooping querier,30
- igmp-snooping query-interval,31
- igmp-snooping report source-ip,32
- igmp-snooping router-aging-time,33
- igmp-snooping router-port-deny,34
- igmp-snooping source-deny,34
- igmp-snooping special-query source-ip,35
- igmp-snooping static-group,36
- igmp-snooping static-router-port,37
- igmp-snooping version,37
- import-source,171
- ip rpf-route-static,77
- ipv6 multicast boundary,266
- ipv6 multicast forwarding supervlan community,268
- ipv6 multicast routing,268
- ipv6 multicast-vlan,250
- ipv6 multicast-vlan entry-limit,251
- ipv6 pim,324
- ipv6 pim bfd enable,325
- ipv6 pim bsr-boundary,326
- ipv6 pim dm,326
- ipv6 pim hello-option dr-priority,327
- ipv6 pim hello-option holdtime,328
- ipv6 pim hello-option lan-delay,328
- ipv6 pim hello-option neighbor-tracking,329
- ipv6 pim hello-option override-interval,330
- ipv6 pim holdtime join-prune,331
- ipv6 pim neighbor-policy,332
- ipv6 pim passive,322
- ipv6 pim require-genid,332
- ipv6 pim sm,333
- ipv6 pim state-refresh-capable,333
- ipv6 pim timer graft-retry,334
- ipv6 pim timer hello,335
- ipv6 pim timer join-prune,335
- ipv6 pim triggered-hello-delay,336
- ipv6 pim-snooping enable,242
- ipv6 pim-snooping graceful-restart join-aging-time,243

- ipv6 pim-snooping graceful-restart
- neighbor-aging-time,244
- ipv6 port multicast-vlan,252

## J

- jp-pkt-size (IPv6 PIM view),337
- jp-pkt-size (PIM view),140

## L

- last-listener-query-count (MLD view),279
- last-listener-query-interval (MLD view),279
- last-listener-query-interval (MLD-snooping view),210
- last-member-query-count (IGMP view),103
- last-member-query-interval (IGMP view),104
- last-member-query-interval (IGMP-snooping view),38
- load-splitting (IPv6 MRIB view),269
- load-splitting (MRIB view),78
- log data-group-reuse,191
- longest-match (IPv6 MRIB view),270
- longest-match (MRIB view),79

## M

- mac-address multicast,79
- max-response-time (IGMP view),105
- max-response-time (IGMP-snooping view),39
- max-response-time (MLD view),280
- max-response-time (MLD-snooping view),211
- mld,281
- mld enable,282
- mld fast-leave,282
- mld group-policy,283
- mld last-listener-query-count,284
- mld last-listener-query-interval,285
- mld max-response-time,286
- mld non-stop-routing,287
- mld other-querier-present-timeout,287
- mld query-interval,288
- mld robust-count,289
- mld startup-query-count,289
- mld startup-query-interval,290
- mld static-group,291
- mld version,292
- mld-snooping,212
- mld-snooping done source-ip,212
- mld-snooping dot1p-priority,213
- mld-snooping drop-unknown,214

- mld-snooping enable, 215
- mld-snooping fast-leave, 216
- mld-snooping general-query source-ip, 217
- mld-snooping group-limit, 217
- mld-snooping group-policy, 218
- mld-snooping host-aging-time, 219
- mld-snooping host-join, 220
- mld-snooping last-listener-query-interval, 221
- mld-snooping max-response-time, 222
- mld-snooping overflow-replace, 223
- mld-snooping querier, 224
- mld-snooping query-interval, 226
- mld-snooping report source-ip, 225
- mld-snooping router-aging-time, 227
- mld-snooping router-port-deny, 228
- mld-snooping source-deny, 228
- mld-snooping special-query source-ip, 229
- mld-snooping static-group, 230
- mld-snooping static-router-port, 231
- mld-snooping version, 231
- msdp, 172
- multicast boundary, 81
- multicast forwarding supervlan community, 81
- multicast routing, 82
- multicast-domain, 191
- multicast-vlan, 58
- multicast-vlan entry-limit, 59

## O

- originating-rp, 173
- other-querier-present-interval (IGMP view), 105
- other-querier-present-timeout (MLD view), 292
- overflow-replace (IGMP-snooping view), 40
- overflow-replace (MLD-snooping view), 232

## P

- peer connect-interface, 173
- peer description, 174
- peer mesh-group, 175
- peer minimum-ttl, 175
- peer password, 176
- peer request-sa-enable, 177
- peer sa-cache-maximum, 178
- peer sa-policy, 178
- peer sa-request-policy, 179
- pim, 140

- pim bfd enable, 141
- pim bsr-boundary, 142
- pim dm, 142
- pim hello-option dr-priority, 143
- pim hello-option holdtime, 144
- pim hello-option lan-delay, 144
- pim hello-option neighbor-tracking, 145
- pim hello-option override-interval, 146
- pim holdtime join-prune, 147
- pim neighbor-policy, 147
- pim passive, 148
- pim require-genid, 149
- pim sm, 149
- pim state-refresh-capable, 150
- pim timer graft-retry, 151
- pim timer hello, 151
- pim timer join-prune, 152
- pim triggered-hello-delay, 153
- pim-snooping enable, 50
- pim-snooping graceful-restart join-aging-time, 51
- pim-snooping graceful-restart neighbor-aging-time, 52
- port (IPv6 multicast VLAN view), 252
- port (multicast-VLAN view), 60
- port multicast-vlan, 60

## Q

- query-interval (IGMP view), 106
- query-interval (MLD view), 293

## R

- register-policy (IPv6 PIM view), 337
- register-policy (PIM view), 153
- register-whole-checksum (IPv6 PIM view), 338
- register-whole-checksum (PIM view), 154
- report-aggregation (IGMP-snooping view), 41
- report-aggregation (MLD-snooping view), 233
- reset igmp group, 107
- reset igmp-snooping group, 41
- reset igmp-snooping router-port, 42
- reset igmp-snooping statistics, 42
- reset ipv6 multicast forwarding event, 270
- reset ipv6 multicast forwarding-table, 271
- reset ipv6 multicast routing-table, 272
- reset ipv6 multicast-vlan group, 253
- reset ipv6 pim-snooping statistics, 244
- reset mld group, 294

- reset mld-snooping group, [233](#)
- reset mld-snooping router-port, [234](#)
- reset mld-snooping statistics, [235](#)
- reset msdp peer, [180](#)
- reset msdp sa-cache, [181](#)
- reset msdp statistics, [181](#)
- reset multicast forwarding event, [83](#)
- reset multicast forwarding-table, [83](#)
- reset multicast routing-table, [84](#)
- reset multicast-vlan group, [61](#)
- reset pim-snooping statistics, [52](#)
- robust-count (IGMP view), [108](#)
- robust-count (MLD view), [295](#)
- router-aging-time (IGMP-snooping view), [43](#)
- router-aging-time (MLD-snooping view), [235](#)

## S

- shutdown (MSDP view), [182](#)
- source, [192](#)
- source-deny (IGMP-snooping view), [43](#)
- source-deny (MLD-snooping view), [236](#)
- source-lifetime (IPv6 PIM view), [339](#)
- source-lifetime (PIM view), [154](#)
- source-policy (IPv6 PIM view), [339](#)
- source-policy (PIM view), [155](#)
- spt-switch-threshold (IPv6 PIM view), [340](#)
- spt-switch-threshold (PIM view), [156](#)
- ssm-mapping (IGMP view), [109](#)
- ssm-mapping (MLD view), [296](#)

- ssm-policy (IPv6 PIM view), [341](#)
- ssm-policy (PIM view), [157](#)
- startup-query-count (IGMP view), [110](#)
- startup-query-count (MLD view), [297](#)
- startup-query-interval (IGMP view), [110](#)
- startup-query-interval (MLD view), [297](#)
- state-refresh-hoplimit (IPv6 PIM view), [342](#)
- state-refresh-interval (IPv6 PIM view), [342](#)
- state-refresh-interval (PIM view), [158](#)
- state-refresh-rate-limit (IPv6 PIM view), [343](#)
- state-refresh-rate-limit (PIM view), [158](#)
- state-refresh-ttl (PIM view), [159](#)
- static-rp (IPv6 PIM view), [344](#)
- static-rp (PIM view), [160](#)
- static-rpf-peer, [183](#)
- subvlan (IPv6 multicast VLAN view), [254](#)
- subvlan (multicast-VLAN view), [62](#)

## T

- timer hello (IPv6 PIM view), [345](#)
- timer hello (PIM view), [161](#)
- timer join-prune (IPv6 PIM view), [346](#)
- timer join-prune (PIM view), [162](#)
- timer retry, [183](#)

## V

- version (IGMP-snooping view), [44](#)
- version (MLD-snooping view), [237](#)