

Table of Contents

Chapter 1 IGMP Snooping Configuration Commands.....	1-1
1.1 IGMP Snooping Configuration Commands	1-1
1.1.1 display igmp-snooping configuration.....	1-1
1.1.2 display igmp-snooping group	1-2
1.1.3 display igmp-snooping statistics.....	1-3
1.1.4 igmp-snooping.....	1-3
1.1.5 igmp-snooping host-aging-time.....	1-4
1.1.6 igmp-snooping max-response-time.....	1-5
1.1.7 igmp-snooping router-aging-time	1-6
1.1.8 reset igmp-snooping statistics.....	1-7
Chapter 2 Multicast Common Configuration Commands	2-1
2.1 Multicast Common Configuration Commands	2-1
2.1.1 debugging multicast forwarding	2-1
2.1.2 debugging multicast kernel-routing	2-1
2.1.3 debugging multicast status-forwarding	2-2
2.1.4 display multicast forwarding-table.....	2-2
2.1.5 display multicast routing-table.....	2-4
2.1.6 multicast route-limit	2-5
2.1.7 multicast routing-enable.....	2-6
2.1.8 reset multicast forwarding-table	2-7
2.1.9 reset multicast routing-table	2-8
Chapter 3 IGMP Configuration Commands	3-1
3.1 IGMP Configuration Commands.....	3-1
3.1.1 debugging igmp.....	3-1
3.1.2 display igmp group	3-1
3.1.3 display igmp interface	3-2
3.1.4 igmp enable.....	3-3
3.1.5 igmp group-limit.....	3-4
3.1.6 igmp group-policy	3-5
3.1.7 igmp group-policy vlan	3-6
3.1.8 igmp host-join	3-7
3.1.9 igmp host-join vlan	3-7
3.1.10 igmp lastmember-queryinterval.....	3-8
3.1.11 igmp max-response-time.....	3-9
3.1.12 igmp proxy	3-10
3.1.13 igmp robust-count	3-11
3.1.14 igmp timer other-querier-present.....	3-12

3.1.15 igmp timer query.....	3-13
3.1.16 igmp version	3-13
3.1.17 reset igmp group	3-14
Chapter 4 PIM Configuration Commands	4-1
4.1 PIM Configuration Commands.....	4-1
4.1.1 bsr-policy	4-1
4.1.2 c-bsr	4-2
4.1.3 c-rp	4-3
4.1.4 crp-policy	4-4
4.1.5 debugging pim common.....	4-5
4.1.6 debugging pim dm.....	4-6
4.1.7 debugging pim sm.....	4-7
4.1.8 display pim bsr-info	4-7
4.1.9 display pim interface	4-8
4.1.10 display pim neighbor	4-9
4.1.11 display pim routing-table	4-10
4.1.12 display pim rp-info	4-11
4.1.13 pim.....	4-12
4.1.14 pim bsr-boundary	4-13
4.1.15 pim dm.....	4-14
4.1.16 pim neighbor-limit.....	4-14
4.1.17 pim neighbor-policy	4-15
4.1.18 pim sm.....	4-16
4.1.19 pim timer hello	4-16
4.1.20 register-policy	4-17
4.1.21 reset pim neighbor	4-18
4.1.22 reset pim routing-table	4-18
4.1.23 source-policy	4-20
4.1.24 static-rp.....	4-21

Chapter 1 IGMP Snooping Configuration Commands

1.1 IGMP Snooping Configuration Commands

1.1.1 display igmp-snooping configuration

Syntax

display igmp-snooping configuration

View

Any view

Parameter

None

Description

Using **display igmp-snooping configuration** command, you can view the IGMP Snooping configuration information.

This command is used to display the IGMP Snooping configuration information of the switch. The information displayed includes whether IGMP Snooping is enabled, router port timeout, maximum response timeout of a query and the member port timeout.

For the related command, see **igmp-snooping**.

Example

Display the IGMP Snooping configuration information of the switch.

```
<Quidway> display igmp-snooping configuration
```

```
Enable IGMP-Snooping.
```

```
The router port timeout is 105 second(s).
```

```
The max response timeout is 15 second(s).
```

```
The host port timeout is 260 second(s).
```

The information above tells us that: IGMP Snooping is enabled; the router port timer is set to be 105 seconds; the max response timer is set to be 15 seconds; the aging timer of multicast group member is set to be 260 seconds.

1.1.2 display igmp-snooping group

Syntax

display igmp-snooping group [**vlan** *vlan_id*]

View

Any view

Parameter

vlan *vlan_id*: Specifies the VLAN where the multicast group to be viewed is located. When the parameter is omitted, the command will display the information about all the multicast groups on the VLAN.

Description

Using **display igmp-snooping group** command, you can view the IP multicast groups and MAC multicast groups under VLAN.

This command displays the IP multicast group and MAC multicast group information of a VLAN or all the VLAN where the Ethernet switch is located. It displays the information such as VLAN ID, router port, IP multicast group address, member ports in the IP multicast group, MAC multicast group, MAC multicast group address, and the member ports in the MAC multicast group.

Example

Display the multicast group information about VLAN2.

```
<Quidway> display igmp-snooping group vlan 2
Total 1 IP Group(s).
Total 1 MAC Group(s).

Vlan(id):2.
Total 1 IP Group(s).
Total 1 MAC Group(s).
Router port(s):Ethernet1/0/1
IP group(s):the following ip group(s) match to one mac group.
    IP group address:225.1.1.1
    Host port(s):Ethernet1/0/2
MAC group(s):
    MAC group address:0100-5e01-0101
    Host port(s):Ethernet1/0/2
```

- There is a multicast group in VLAN 2;
- The router port is Ethernet 1/0/1;
- The address of the multicast group is 225.1.1.1;
- The member of the IP multicast group is Ethernet 1/0/2;

- MAC multicast group is 0100-5e01-0101;
- The member of the MAC multicast group is Ethernet 1/0/2.

1.1.3 display igmp-snooping statistics

Syntax

display igmp-snooping statistics

View

Any view

Parameter

None

Description

Using **display igmp-snooping statistics** command, you can view the statistics information on IGMP Snooping.

This command displays the statistics information about IGMP Snooping of Ethernet switch. It displays the information such as number of received general IGMP query packets, received IGMP specific query packets, received IGMP Version 1 and Version 2 report packets, received IGMP leave packets and error packets, and sent IGMP specific query packets.

For the related command, see **igmp-snooping**.

Example

Display statistics information about IGMP Snooping.

```
<Quidway> display igmp-snooping statistics
Received IGMP general query packet(s) number:0.
Received IGMP specific query packet(s) number:0.
Received IGMP V1 report packet(s) number:0.
Received IGMP V2 report packet(s) number:0.
Received IGMP leave packet(s) number:0.
Received error IGMP packet(s) number:0.
Sent IGMP specific query packet(s) number:0.
```

1.1.4 igmp-snooping

Syntax

igmp-snooping { enable | disable }

View

System view, VLAN view

Parameter

enable: Enables IGMP Snooping.

disable: Disables IGMP Snooping; By default, the switch disables IGMP Snooping feature.

Description

Using **igmp-snooping enable** command, you can enable IGMP Snooping. Using **igmp-snooping disable** command, you can restore the default setting.



Caution:

- Although layer 2 and layer 3 multicast protocols can run together, they cannot run on the same VLAN or its corresponding VLAN interface at the same time. For example, if the layer 2 multicast protocol is enabled on a VLAN, then the layer 3 multicast protocol cannot operate on this VLAN, and vice versa.
 - IGMP Snooping functions only when it is enabled both in system view and in VLAN view. You must first enable IGMP Snooping globally in system view and then the VLAN view before configuring it. Otherwise, the IGMP Snooping fails to operate.
-

Example

Enable IGMP Snooping on VLAN 100.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] igmp-snooping enable
IGMP snooping has already been enabled.
[Quidway] vlan 100
[Quidway-vlan100] igmp-snooping enable
```

1.1.5 igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *seconds*

undo igmp-snooping host-aging-time

View

System view

Parameter

seconds: Specifies the port aging time of the multicast group member, ranging from 200 to 1000 and measured in seconds; By default, 260.

Description

Using **igmp-snooping host-aging-time** command, you can configure the port aging time of the multicast group members. Using **undo igmp-snooping host-aging-time** command, you can restore the default value.

This command is used to set the aging time of the multicast group member so that the refresh frequency can be controlled. When the group members change frequently, the aging time should be comparatively short, and vice versa.

For the related command, see **igmp-snooping**.

Example

Set the aging time to 300 seconds.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] igmp-snooping host-aging-time 300
Set host port timeout 300 second(s).
```

1.1.6 igmp-snooping max-response-time

Syntax

igmp-snooping max-response-time *seconds*
undo igmp-snooping max-response-time

View

System view

Parameter

seconds: Maximum response time for a query ranging from 1 to 25 and measured in seconds; By default, the value is 10.

Description

Using **igmp-snooping max-response-time** command, you can configure the maximum response time for a query. Using **undo igmp-snooping max-response-time** command, you can restore the default value.

The set maximum response time decides the time limit for the switch to respond to IGMP Snooping general query packets.

For the related command, see **igmp-snooping**, **igmp-snooping router-aging-time**.

Example

Configure to respond the IGMP Snooping packet within 20s.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] igmp-snooping max-response-time 20
Set max response timeout 20 second(s).
```

1.1.7 igmp-snooping router-aging-time

Syntax

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

View

System view

Parameter

seconds: Specifies the router port aging time, ranging from 1 to 1000 measured in seconds; By default, 105.

Description

Using **igmp-snooping router-aging-time** command, you can configure the router port aging time of IGMP Snooping. Using **undo igmp-snooping router-aging-time** command, you can restore the default value.

The port here refers to the Ethernet switch port connected to the router. The Layer-2 Ethernet switch receives general query packets from the router via this port. The timer should be set to about 2.5 times of the general query period of the router.

For the related command, see **igmp-snooping**, **igmp-snooping max-response-time**.

Example

Set the aging time of the IGMP Snooping router port to 500 seconds.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] igmp-snooping router-aging-time 500
Set router port timeout 500 second(s)
```


1.1.8 reset igmp-snooping statistics

Syntax

reset igmp-snooping statistics

View

User view

Parameter

None

Description

Using **reset igmp-snooping statistics** command, you can reset the IGMP Snooping statistics information.

For the related command, see **igmp-snooping**.

Example

Clear IGMP Snooping statistics information.

```
<Quidway> reset igmp-snooping statistics
Clear IGMP snooping statistics ok.
```

Chapter 2 Multicast Common Configuration Commands

2.1 Multicast Common Configuration Commands

2.1.1 debugging multicast forwarding

Syntax

```
debugging multicast forwarding
undo debugging multicast forwarding
```

View

User view

Parameter

None

Description

Using **debugging multicast forwarding** command, you can enable multicast packet forwarding debugging functions. Using **undo debugging multicast forwarding** command, you can disable the debugging functions.

By default, the debugging function is disabled.

Example

```
# Enable multicast packet forwarding debugging functions.
<Quidway> debugging multicast forwarding
```

2.1.2 debugging multicast kernel-routing

Syntax

```
debugging multicast kernel-routing
undo debugging multicast kernel-routing
```

View

User view

Parameter

None

Description

Using **debugging multicast kernel-routing** command, you can enable multicast kernel routing debugging functions. Using **undo debugging multicast kernel-routing** command, you can disable the debugging functions.

Example

```
# Enable multicast kernel routing debugging functions.  
<Quidway> debugging multicast kernel-routing
```

2.1.3 debugging multicast status-forwarding

Syntax

```
debugging multicast status-forwarding  
undo debugging multicast status-forwarding
```

View

User view

Parameter

None

Description

Using **debugging multicast status-forwarding** command, you can enable multicast forwarding status debugging functions. Using **undo debugging multicast status-forwarding** command, you can disable the debugging functions.

Example

```
# Enable multicast forwarding status debugging functions.  
<Quidway> debugging multicast status-forwarding
```

2.1.4 display multicast forwarding-table

Syntax

```
display multicast forwarding-table [ group-address [ mask { mask | mask-length } ] ] |  
source-address [ mask { mask | mask-length } ] | incoming-interface { Vlan-interface  
vlan-interface-number | register } ] *
```

View

Any view

Parameter

group-address: Multicast group address, used to specify a multicast group, ranging from 224.0.0.0 to 239.255.255.255.

source-address: Unicast IP address of the multicast source.

incoming-interface: Incoming interface of the multicast forwarding table.

register: Register interface of PIM-SM.

Description

Using **display multicast forwarding-table** command, you can view the information of IP multicast forwarding table.

For the related command, see **display multicast routing-table**.

Example

View the multicast forwarding table information.

```
[Quidway] display multicast forwarding-table
Multicast Forwarding Cache Table
Total 1 entry: 0 entry created by IP, 1 entry created by protocol

00001. (10.0.0.4, 225.1.1.1), iif Vlan-interface2, 0 oifs,
    Protocol Create
    Matched 122 pkts(183000 bytes), Wrong If 0 pkts
    Forwarded 122 pkts(183000 bytes)

Total 1 entry Listed
```

Table 2-1 Description of information generated by the command **display multicast forwarding-table**

Field	Description
Multicast Forwarding Cache Table	Multicast forwarding cache table
Total 1 entries	Total number of entries
00001	Sequence number of entries
(10.0.0.4, 225.1.1.1)	(s,g)
iif Vlan-interface2, 0 oifs	Multicast forwarding cache table has an incoming interface Vlan-interface 2 and no outgoing interface
List of outgoing interface: 01: Vlan-interface2	List of outgoing interface has an outgoing interface Vlan-interface 2

Field	Description
Matched 122 pkts(183000 bytes), Wrong If 0 pkts Forwarded 122 pkts(183000 bytes) Forwarded 233 pkts(3267 bytes)	122 matched packets (183000 bytes); 0 matched packets means wrong; 122 forwarded packets (183000 bytes)

2.1.5 display multicast routing-table

Syntax

display multicast routing-table [*group-address* [**mask** { *mask* | *mask-length* }]] | *source-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { **Vlan-interface** *vlan-interface-number* | **register** }]*

View

Any view

Parameter

group-address: Multicast group address, used to specify a multicast group and display the corresponding routing table information of the group. The value ranges from 224.0.0.0 to 239.255.255.255.

source-address: Unicast IP address of the multicast source.

incoming-interface: Incoming interface of the multicast route entry.

register: Register interface of PIM-SM.

Description

Using **display multicast routing-table** command, you can view the information of IP multicast routing table.

This command displays the multicast routing table information, while the **display multicast forwarding-table** command displays the multicast forwarding table information.

Example

View the route entry information in the multicast routing table.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway]display multicast routing-table
Multicast Routing Table
Total 3 entries
```

```
(4.4.4.4, 224.2.149.17)
    Uptime: 00:15:16, Timeout in 272 sec
    Upstream interface: Vlan-interface1(4.4.4.6)
    Downstream interface list:
        Vlan-interface2(2.2.2.4), Protocol 0x1: IGMP

(4.4.4.4, 224.2.254.84)
    Uptime: 00:15:16, Timeout in 272 sec
    Upstream interface: Vlan-interface1(4.4.4.6)
    Downstream interface list: NULL

(4.4.4.4, 239.255.2.2)
    Uptime: 00:02:57, Timeout in 123 sec
    Upstream interface: Vlan-interface1(4.4.4.6)
    Downstream interface list: NULL
```

Matched 3 entries

Table 2-2 Description of information generated by the command **display multicast routing-table**

Field	Description
Multicast Routing Table	Multicast routing table
Total 3 entries	3 entries in total
(4.4.4.4, 224.2.149.17)	(s, g)
Uptime: 00:15:16, Timeout in 272 sec Upstream interface: Vlan-interface1(4.4.4.6) Downstream interface list: Vlan-interface2(2.2.2.4), Protocol 0x1: IGMP	Multicast routing table lasts 15'16" and times out in 272 seconds. Upstream interface vlan-interface 1 (its IP address is 4.4.4.6). Downstream interface list: has an interface Vlan-interface 2 (its IP address is 2.2.2.4). The downstream interface is configured with IGMP groups.
Matched 3 entries	3 entries in total meeting the requirement

2.1.6 multicast route-limit

Syntax

multicast route-limit *limit*

undo multicast route-limit

View

System view

Parameter

limit: Limits the capacity of multicast routing table, in the range of 0 to 256.

Description

Using **multicast route-limit** command, you can limit the capacity of multicast routing table. When the preset capacity is exceeded, the router will discard new (S, G) protocol and data packets. Using **undo multicast route-limit** command, you can restore the limit to the default value.

By default, the capacity of multicast routing table is set to 256.

If the existing route entries exceed the capacity value you configured during using this command, the system will not delete the existing entries, but prompts the information "Existing route entries exceed the configured capacity value".

The new configuration overwrites the old one if you run the command for a second time.

Example

Limit multicast routing table capacity at 100.

```
[Quidway] multicast route-limit 100
```

2.1.7 multicast routing-enable

Syntax

multicast routing-enable

undo multicast routing-enable

View

System view

Parameter

None

Description

Using **multicast routing-enable** command, you can enable IP multicast routing. Using **undo multicast routing-enable** command, you can disable IP multicast routing.

By default, IP multicast routing is disabled.

The system will not forward any multicast packet when IP multicast routing is disabled.

For the related commands, see **igmp enable**, **pim dm** and **pim sm**.

Example

```
# Enable IP multicast routing.

<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
```

2.1.8 reset multicast forwarding-table

Syntax

```
reset multicast forwarding-table [ statistics ] { all | { group-address [ mask { group-mask | group-mask-length } ] | source-address [ mask { source-mask | source-mask-length } ] | incoming-interface Vlan-interface vlan-interface-number } * }
```

View

User view

Parameter

statistics: If it is selected, the system clears the statistic information of MFC forward entries. Otherwise, the system clears MFC forward entries.

all: All MFC forward entries.

group-address: Specifies group address.

group-mask: Specifies Mask of group address

group-mask-length: Specifies mask length of group address.

source-address: Specifies source address.

source-mask: Specifies mask of source address.

source-mask-length: Specifies mask length of source address.

incoming-interface: Specifies incoming interface for the forward entry.

Vlan-interface *vlan-interface-number*: Interface type and interface number.

Description

Using **reset multicast forwarding-table** command, you can clear MFC forwarding entries or statistic information of MFC forwarding entries.

You can type in source address first and group address after in the command, as long as they both are valid addresses. The system prompts error information if you type in invalid addresses.

For the related commands, see **reset pim routing-table**, **reset multicast routing-table** and **display multicast forwarding-table**.

Example

Clear the forwarding entry with address of 225.5.4.3 from the MFC forwarding table.

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

Clear statistic information of the forwarding entry with address of 225.5.4.3 from the MFC forwarding table.

```
<Quidway> reset multicast forwarding-table statistics 225.5.4.3
```

2.1.9 reset multicast routing-table

Syntax

```
reset multicast routing-table { all | { group-address [ mask { group-mask | group-mask-length } ] | source-address [ mask { source-mask | source-mask-length } ] | incoming-interface Vlan-interface vlan-interface-number } * }
```

View

User view

Parameter

all: All route entries in the core multicast routing table.

group-address: Specifies group address.

group-mask: Specifies Mask of group address

group-mask-length: Specifies mask length of group address.

source-address: Specifies source address.

source-mask: Specifies mask of source address.

source-mask-length: Specifies mask length of source address.

incoming-interface: Specifies incoming interface for the forward entry.

Vlan-interface *vlan-interface-number*: Interface type and interface number.

Description

Using **reset multicast routing-table** command, you can clear route entries from the core multicast routing table, as well as MFC forwarding entries.

You can type in source address first and group address after in the command, as long as they both are valid addresses. The system prompts error information if you type in invalid addresses.

For the related commands, see **reset pim routing-table**, **reset multicast forwarding-table** and **display multicast forwarding-table**.

Example

Clear the route entry with address of 225.5.4.3 from the core multicast routing table.

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

Clear statistic information of the forward entry with address of 225.5.4.3 from the MFC forwarding table.

```
<Quidway> reset multicast forwarding-table statistics 225.5.4.3
```

Chapter 3 IGMP Configuration Commands

3.1 IGMP Configuration Commands

3.1.1 debugging igmp

Syntax

```
debugging igmp { all | event | host | packet | timer }  
undo debugging igmp { all | event | host | packet | timer }
```

View

User view

Parameter

all: All the debugging information of IGMP.
event: Debugging information of IGMP event.
host: Debugging information of IGMP host.
packet: Debugging information of IGMP packets.
timer: Debugging information of IGMP timers.

Description

Using **debugging igmp** command, you can enable IGMP debugging functions. Using **undo debugging igmp** command, you can disable the debugging functions.

By default, IGMP debugging functions are disabled.

Example

```
# Enable all IGMP debugging functions  
<Qidway> debugging igmp all
```

3.1.2 display igmp group

Syntax

```
display igmp group [ group-address | interface Vlan-interface  
vlan-interface-number ]
```

View

Any view

Parameter

group-address: Address of the multicast group.

Vlan-interface *vlan-interface-number*: Interface type and interface number of the router, used to specify the specific interface.

Description

Using **display igmp group** command, you can view the member information of the IGMP multicast group.

You can specify to show the information of a group or the member information of the multicast group on an interface. The information displayed contains the multicast groups which are joined by the downstream hosts through IGMP or through command line.

For the related command, see **igmp host-join**.

Example

View the member information of multicast group in the system.

```
<Quidway> display igmp group
```

```
LoopBack0 (20.20.20.20): Total 3 IGMP Groups reported:
```

Group Address	Last Reporter	Uptime	Expires
225.1.1.1	20.20.20.20	00:02:04	00:01:15
225.1.1.3	20.20.20.20	00:02:04	00:01:15
225.1.1.2	20.20.20.20	00:02:04	00:01:17

Table 3-1 Output description of the **display igmp group** command

Field	Description
Group address	Multicast group address
Last Reporter	The last host reporting to join in the multicast group
Uptime	Time passed since multicast group is discovered (hh: mm: ss).
Expires	Specifies when the member will be removed from the multicast group (hh: mm: ss).

3.1.3 display igmp interface

Syntax

display igmp interface [**Vlan-interface** *vlan-interface-number*]

View

Any view

Parameter

Vlan-interface *vlan-interface-number*: Interface type and interface number of the router, used to specify the interface. If the parameters are omitted, information about all the interfaces running IGMP will be displayed.

Description

Using **display igmp interface** command, you can view the IGMP configuration and running information on an interface.

Example

View the IGMP configuration and running information of all interfaces.

```
<Quidway> display igmp interface
Vlan-interface1 (10.153.17.99):
  IGMP is enabled
  Current IGMP version is 2
  Value of query interval for IGMP(in seconds): 60
  Value of other querier time out for IGMP(in seconds): 120
  Value of maximum query response time for IGMP(in seconds): 10
  Value of robust count for IGMP: 2
  Value of startup query interval for IGMP(in seconds): 15
  Value of last member query interval for IGMP(in seconds): 1
  Value of query timeout for IGMP version 1(in seconds): 400
  Policy to accept IGMP reports: none
  Querier for IGMP: 10.153.17.99 (this router)
  IGMP group limit is 256
  No IGMP group reported
```

3.1.4 igmp enable

Syntax

igmp enable
undo igmp enable

View

Vlan interface view

Parameter

None

Description

Using **igmp enable** command, you can enable IGMP on an interface. Using **undo igmp enable** command, you can disable IGMP on the interface.

By default, IGMP is not enabled.

Only multicast function is enabled can the **igmp enable** command be executed. After this, you can initiate IGMP feature configuration.

For the related command, see **multicast routing-enable**.

Example

Enable IGMP on Vlan-interface 10.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface10] igmp enable
```

3.1.5 igmp group-limit

Syntax

igmp group-limit *number*

undo igmp group-limit

View

Vlan interface view

Parameter

number: Quantity of multicast groups, in the range of 0 to 256.

Description

Using **igmp group-limit** command, you can limit multicast groups on an interface. Using **undo igmp group-limit** command, you can restore the default setting.

By default, you can add up to 256 IGMP groups on an interface.

If the existing IGMP groups exceed the quantity limit you configured during using this command, the system will not delete the existing entries.

The new configuration overwrites the old one if you run the command for a second time.

Example

Limit the maximum IGMP groups at Vlan-interface10 to 100.

```
<Quidway>system-view
```

```
System View: return to User View with Ctrl+Z.  
[Quidway] interface Vlan-interface 10  
[Quidway-Vlan-interface10] igmp group-limit 100
```

3.1.6 igmp group-policy

Syntax

```
igmp group-policy acl-number [ 1 | 2 | port { interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ] ]  
undo igmp group-policy [ port { interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ] ]
```

View

Vlan interface view

Parameter

acl-number: Number of the basic IP access control list number, defining a multicast group range. The value ranges from 2000 to 2999.

1: IGMP version 1.

2: IGMP version 2. If IGMP version is not specified, version 2 will be used as default.

port: Packets received and sent by the port(s) and applied to the conditions set by the ACL will be filtered. And the port(s) must belong to the VLAN interface being configured by this command.

Description

Using **igmp group-policy** command, you can set the filter of multicast groups on an interface to control the accessing to the IP multicast groups. Using **undo igmp group-policy** command, you can remove the filter configured.

By default, no filter is configured, that is, a host can join any multicast group.

If you do not want the hosts on the network that the interface is on to join some multicast groups and receive the packets from the multicast groups, you can use this command to limit the range of the multicast groups serviced by the interface.

For the related command, see **igmp host-join**.

Example

Configure the access-list 2000.

```
<Quidway>system-view  
System View: return to User View with Ctrl+Z.  
[Quidway] acl number 2000  
[Quidway-acl-basic-2000] rule permit source 225.0.0.0 0.255.255.255.0
```

On the specified interface VLAN-interface10, only the host matching the range of the acl 2000 can be added to multicast group for which the IGMP version is 2.

```
[Quidway-vlan-interface10] igmp group-policy 2000 2
```

3.1.7 igmp group-policy vlan

Syntax

igmp group-policy *acl-number* **vlan** *vlanid*

undo igmp group-policy **vlan** *vlanid*

View

Port view

Parameter

acl-number: Number of the basic IP access control list number, defining a multicast group range. The value ranges from 2000 to 2999.

vlanid: ID of the VLAN to which the port belongs.

Description

Using **igmp group-policy vlan** command, you can set the filter of multicast groups on a port to control the access to the IP multicast groups. Using **undo igmp group-policy vlan** command, you can remove the configured filter.

By default, no filter is configured, that is, a host can join any multicast group.

If you do not want the hosts on the network that the port is on to join some multicast groups nor to receive the packets from the multicast groups, use this command to limit the range of the multicast groups served by the port.

Note that the port configured with this command must belong to the specified VLAN and the IGMP must be enabled on the VLAN interface, otherwise, the configuration takes no effect.

For the related command, see **igmp group-policy**, **igmp host-join port**, **igmp host-join vlan**.

Example

Specify the hosts, which meet the ACL 2000, on the port Ethernet 1/0/1 to join the multicast group.

```
[Quidway-Vlan-interface10] igmp enable
[Quidway-Vlan-interface10] quit
[Quidway] interface Ethernet 1/0/1
[Quidway-Ethernet1/0/1] port access vlan 10
[Quidway-Ethernet1/0/1] igmp group-policy 2000 vlan 10
```


3.1.8 igmp host-join

Syntax

```
igmp host-join group-address port { interface_type interface_num | interface_name }  
[ to { interface_type interface_num | interface_name } ]  
  
undo igmp host-join group-address port { interface_type interface_num |  
interface_name } [ to { interface_type interface_num | interface_name } ]
```

View

VLAN interface view

Parameter

group-address: Multicast address of the multicast group that an interface will join.

port: Specifies the port in the VLAN interface.

Description

Using **igmp host-join** command, you can enable an port in the VLAN interface of an ethernet switch to join a multicast group. Using **undo igmp host-join** command, you can disable the configuration.

By default, an interface does not join any multicast group.

On an ethernet switch, up to 64 interfaces can be configured with **igmp host-join** command at best.

For the related command, see **igmp group-policy**.

Example

Add port Ethernet 1/0/1 in VLAN-interface10 to the multicast group at 225.0.0.1.

```
<Quidway>system-view  
System View: return to User View with Ctrl+Z.  
[Quidway] interface Vlan-interface 10  
[Quidway-Vlan-interface10] igmp host-join 225.0.0.1 port Ethernet 1/0/1
```

3.1.9 igmp host-join vlan

Syntax

```
igmp host-join group-address vlan vlanid  
undo igmp host-join group-address vlan vlanid
```

View

Port view

Parameter

group-address: Multicast address of the multicast group that a port will join.

vlanid: ID of the VLAN to which the port belongs.

Description

Using **igmp host-join vlan** command, you can enable an Ethernet port to join a multicast group. Using **undo igmp host-join vlan** command, you can disable the configuration.

By default, an Ethernet port does not join any multicast group.

For the related command, see **igmp group-policy**.

Example

Specify the Ethernet port Ethernet 1/0/1 to join the multicast group 225.0.0.1.

```
[Quidway-Vlan-interface10] igmp enable
[Quidway-Vlan-interface10] quit
[Quidway] interface Ethernet 1/0/1
[Quidway-Ethernet1/0/1] port access vlan 10
[Quidway-Ethernet1/0/1] igmp host-join 225.0.0.1 vlan 10
```

3.1.10 igmp lastmember-queryinterval

Syntax

igmp lastmember-queryinterval seconds

undo igmp lastmember-queryinterval

View

Vlan interface view

Parameter

seconds: Time interval before IGMP query router sends the IGMP group query message after it receives the IGMP Leave message from the host. It is in the range of 1 to 5 seconds. By default, it is 1 second.

Description

Using **igmp lastmember-queryinterval** command, you can set the time interval before IGMP query router sends the IGMP group query message after it receives the IGMP Leave message from the host. Using **undo igmp lastmember-queryinterval** command, you can restore the default value.

In the shared network, that is, a same network segment including multiple hosts and multicast routers, the query router is responsible for maintaining the IGMP group

membership on the interface. When the IGMP v2 host leaves a group, it sends a IGMP Leave message. When receiving the IGMP Leave message, IGMP query router must send the IGMP group query message for specified times (by the *robust-value* parameter in the **igmp robust-count** command, with default value as 2) in a specified time interval (by the *seconds* parameter in the **igmp lastmember-queryinterval** command, with default value as 1 second). If other hosts which are interested in the specified group receive the IGMP query message from the IGMP query router, they will send back the IGMP Membership Report message within the specified maximum response time interval. If it receives the IGMP Membership Report message within the defined period (equal to *robust-value* × *seconds*), the IGMP query router continues to maintain the membership of this group. When receiving no IGMP Membership Report message from any hosts within the defined period, the IGMP query router considers it as timeout and stops membership maintenance for the group.

This command is only available on the IGMP query router running IGMP v2. For the host running IGMP v1, this command cannot take effect for the host may not send the IGMP Leave message when it leaves a group.

For the related command, see **igmp robust-count** and **display igmp interface**.

Example

Set the query interval at the Vlan-interface10 as 3 seconds.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface10] igmp lastmember-queryinterval 3
```

3.1.11 igmp max-response-time

Syntax

igmp max-response-time *seconds*

undo igmp max-response-time

View

Vlan interface view

Parameter

seconds: Maximum response time in the IGMP query messages in second in the range from 1 to 25. By default, the value is 10 seconds.

Description

Using **igmp max-response-time** command, you can configure the maximum response time contained in the IGMP query messages. Using **undo igmp max-response-time** command, you can restore the default value.

The maximum query response time determines the period for a switch to quickly detect that there are no more directly connected group members in a LAN.

For the related command, see **display igmp group**.

Example

Set the maximum response time carried in host-query message to 8 seconds.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface10] igmp max-response-time 8
```

3.1.12 igmp proxy

Syntax

igmp proxy *Vlan-interface vlan-interface-number*
undo igmp proxy

View

Vlan interface view

Parameter

interface-type: Proxy interface type.

interface-number: Proxy interface number.

Description

Using **igmp proxy** command, you can specify an interface of a leaf network Layer 3 switch as the IGMP proxy of another interface. Using **undo igmp proxy** command, you can remove the configuration.

By default, IGMP proxy function is disabled.

You must enable PIM on the interface before you configure the **igmp proxy** command. An interface cannot act as the IGMP proxy of two or more other interfaces at the same time.

If an interface is configured with IGMP proxy for multiple times, the last one overrides all the previous configurations.

Related command: **pim neighbor-policy**.

Example

Specify VLAN 3 interface as the IGMP proxy of the VLAN 2 interface.

```
[Quidway-Vlan-interface2] igmp proxy Vlan-interface 3
```

3.1.13 igmp robust-count

Syntax

igmp robust-count *robust-value*

undo igmp robust-count

View

Vlan interface view

Parameter

robust-value: IGMP robust value, number of sending the IGMP group query message after the IGMP query router receives the IGMP Leave message from the host. It is in the range of 2 to 5. By default, it is 2.

Description

Using **igmp robust-count** command, you can set the number of sending the IGMP group query message after the IGMP query router receives the IGMP Leave message from the host. Using **undo igmp robust-count** command, you can restore the default value.

In the shared network, that is, a same network segment including multiple hosts and multicast routers, the query router is responsible for maintaining the IGMP group membership on the interface. When the IGMP v2 host leaves a group, it sends a IGMP Leave message. When receiving the IGMP Leave message, IGMP query router must send the IGMP group query message for specified times (by the *robust-value* parameter in the **igmp robust-count** command, with default value as 2) in a specified time interval (by the *seconds* parameter in the **igmp lastmember-queryinterval** command, with default value as 1 second). If other hosts which are interested in the specified group receive the IGMP query message from the IGMP query router, they will send back the IGMP Membership Report message within the specified maximum response time interval. If it receives the IGMP Membership Report message within the defined period (equal to *robust-value* × *seconds*), the IGMP query router continues to maintain the membership of this group. When receiving no IGMP Membership Report message from any hosts within the defined period, the IGMP query router considers it as timeout and stops membership maintenance for the group.

This command is only available on the IGMP query router running IGMP v2. For the host running IGMP v1, this command cannot take effect for the host may not send the IGMP Leave message when it leaves a group.

For the related command, see **igmp lastmember-queryinterval** and **display igmp interface**.

Example

Set the robust value at the Vlan-interface 10 as 3.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface10] igmp robust-count 3
```

3.1.14 igmp timer other-querier-present

Syntax

igmp timer other-querier-present *seconds*
undo igmp timer other-querier-present

View

Vlan interface view

Parameter

seconds: IGMP querier present timer value in second ranging from 1 to 131070. By default, the value is twice the value of IGMP query message interval, i.e., 120 seconds.

Description

Using **igmp timer other-querier-present** command, you can configure the timer of presence of the IGMP querier. Using **undo igmp timer other-querier-present** command, you can restore the default value.

On a shared network, i.e., there are multiple multicast routers on the same network segment, the query router (querier for short) takes charge of sending query messages periodically on the interface. If other non-queriers receive no query messages within the valid period, the router will consider the previous query to be invalid and the router itself becomes a querier.

In IGMP version 1, the selection of a query is determined by the multicast routing protocol. In IGMP version 2, the router with the lowest IP address on the shared network segment acts as the querier.

For the related commands, see **igmp timer query** and **display igmp interface**.

Example

Set querier to expire after 300 seconds.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
```

```
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface10] igmp timer other-querier-present 300
```

3.1.15 igmp timer query

Syntax

```
igmp timer query seconds
undo igmp timer query
```

View

Vlan interface view

Parameter

seconds: Interval at which a router transmits IGMP query messages in second in the range from 1 to 65535. By default, the value is 60 seconds.

Description

Using **igmp timer query** command, you can configure the interval at which a router interface sends IGMP query messages. Using **undo igmp timer query** command, you can restore the default value.

A multicast router periodically sends out IGMP query messages to attached segments to find hosts that belong to different multicast groups. The query interval can be modified according to the practical conditions of the network.

For the related command, see **igmp timer other-querier-present**.

Example

```
# Configure to transmit the host-query message every 60 seconds via
VLAN-interface2.
```

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface2] igmp timer query 60
```

3.1.16 igmp version

Syntax

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

View

Vlan interface view

Parameter

- 1: IGMP Version 1.
- 2: IGMP Version 2. By default, IGMP Version 2 is used.

Description

Using **igmp version** command, you can specify the version of IGMP that a router uses.
Using **undo igmp version** command, you can restore the default value.

All routers on a subnet must support the same version of IGMP. After detecting the presence of IGMP Version 1 system, a router cannot automatically switch to Version 1.

Example

Run IGMP Version 1 on VLAN-interface10.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface10] igmp version 1
```

3.1.17 reset igmp group

Syntax

reset igmp group { all | interface Vlan-interface *vlan-interface-number* { all | *group-address* [*group-mask*] } }

View

User view

Parameter

all: All IGMP groups.

interface Vlan-interface *vlan-interface-number*: Interface type and interface number.

group-address: IGMP group address.

group-mask: Mask of IGMP group address.

Description

Using **reset igmp group** command, you can delete an existing IGMP group from the interface. The deleted group can added again on the interface.

Example

Delete all IGMP groups on all the interfaces.

```
<Quidway> reset igmp group all
```

Delete all IGMP groups on the Vlan-interface10.


```
<Quidway> reset igmp group interface Vlan-interface10 all
```

Delete the group 225.0.0.1 from the Vlan-interface10.

```
<Quidway> reset igmp group interface Vlan-interface10 225.0.0.1
```

Delete the IGMP groups ranging from 225.1.1.0 to 225.1.1.255 on the Vlan-interface10.

```
<Quidway> reset igmp group interface Vlan-interface10 225.1.1.0 255.255.255.0
```

Chapter 4 PIM Configuration Commands

4.1 PIM Configuration Commands

4.1.1 bsr-policy

Syntax

```
bsr-policy acl-number  
undo bsr-policy
```

View

PIM view

Parameter

acl-number: ACL number imported in BSR filtering policy, in the range of 2000 to 2999.

Description

Using **bsr-policy** command, you can limit the range of legal BSRs to prevent BSR proofing. Using **undo bsr-policy** command, you can restore the default setting, that is, no range limit is set and all received messages are taken as legal.

In the PIM SM network using BSR (bootstrap router) mechanism, every router can set itself as C-BSR (candidate BSR) and take the authority to advertise RP information in the network once it wins in the contention. To prevent malicious BSR proofing in the network, the following two measures need to be taken:

- Prevent the router from being spoofed by hosts though faking legal BSR messages to modify RP mapping. BSR messages are of multicast type and their TTL is 1, so this type of attacks often hit edge routers. Fortunately, BSRs are inside the network, while assaulting hosts are outside, therefore neighbor and RPF checks can be used to stop this type of attacks.
- If a router in the network is manipulated by an attacker, or an illegal router is accessed into the network, the attacker may set itself as C-BSR and try to win the contention and gain authority to advertise RP information among the network. Since the router configured as C-BSR shall propagate BSR messages, which are multicast messages sent hop by hop with TTL as 1, among the network, then the network cannot be affected as long as the peer routers do not receive these BSR messages. One way is to configure **bsr-policy** on each router to limit legal BSR range, for example, only 1.1.1.1/32 and 1.1.1.2/32 can be BSR, thus the routers cannot receive or forward BSR messages other than these two. Even legal BSRs cannot contest with them.

Problems may still exist if a legal BSR is attacked, though these two measures can effectively guarantee high BSR security.

The **source** parameter in the **rule** command is translated as BSR address in the **bsr-policy** command.

For the related commands, see **acl** and **rule**.

Example

Configure BSR filtering policy on routers, only 1.1.1.1/32 can be BSR.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
[Quidway]pim
[Quidway-pim] bsr-policy 2000
[Quidway-pim] quit
[Quidway] acl number 2000
[Quidway-acl-basic-2000] rule 0 permit source 1.1.1.1 0
```

4.1.2 c-bsr

Syntax

c-bsr **Vlan-interface** *vlan-interface-number* *hash-mask-len* [*priority*]

undo c-bsr

View

PIM view

Parameter

Vlan-interface *vlan-interface-number*: Specifies the interface. The candidate BSR is configured on the interface. PIM-SM must be enabled on the interface first.

hash-mask-len: Length of the mask. The value ranges from 0 to 32.

priority: Priority of the candidate BSR. The larger the value of the priority, the higher the priority of the BSR. The value ranges from 0 to 255. By default, the priority is 0.

Description

Using **c-bsr** command, you can configure a candidate BSR. Using **undo c-bsr** command, you can remove the candidate BSR configured.

By default, no candidate BSR is set.

When configure the candidate BSR, the larger bandwidth should be guaranteed since a great amount of information will be exchanged between BSR and other devices in the PIM domain.

For the related command, see **pim sm**.

Example

Configure the Ethernet switch as C-BSR with priority 2 (and the C-BSR address is designated as the IP address of VLAN-interface10).

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
[Quidway]pim
[Quidway-pim] c-bsr vlan-interface 10 24 2
```

4.1.3 c-rp

Syntax

c-rp **Vlan-interface** *vlan-interface-number* [**group-policy** *acl-number* | **priority** *priority-value*]*

undo c-rp { **Vlan-interface** *vlan-interface-number* | **all** }

View

PIM view

Parameter

Vlan-interface *vlan-interface-number*: Specifies interface with the IP address advertised as a candidate RP address.

acl-number: Number of the basic ACL that defines a group range, which is the service range of the advertised RP. The value ranges from 2000 to 2999.

priority-value: Priority value of candidate RP, in the range of 0 to 255. By default, it is 0. The greatest value corresponds to the lowest priority level

all: Remove all candidate RP configurations.

Description

Using **c-rp** command, you can configure the router to advertise itself as a candidate RP. Using **undo c-rp** command, you can remove the configuration.

By default, no candidate RP is configured.

When configuring the candidate RP, a relatively large bandwidth should be reserved for the router and other devices in the PIM domain.

For the related command, see **c-bsr**.

Example

Configure the Ethernet switch to advertise the BSR that he is the C-RP in the PIM. The standard access list 2000 defines the groups related to the RP. The address of C-RP is designated as the IP address of VLAN-interface10.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
[Quidway] acl number 2000
[Quidway-acl-basic-2000] rule permit source 225.0.0.0 0.255.255.255
[Quidway-acl-basic-2000] quit
[Quidway] pim
[Quidway-pim] c-rp vlan-interface 10 group-policy 2000
```

4.1.4 crp-policy

Syntax

crp-policy *acl-number*
undo crp-policy

View

PIM view

Parameter

acl-number: ACL number imported in C-RP filtering policy, ranging from 3000 to 3999.

Description

Using **crp-policy** command, you can limit the range of legal C-RP, as well as target service group range of each C-RP, prevent C-RP proofing. Using **undo crp-policy** command, you can restore the default setting, that is, no range limit is set and all received messages are taken as legal.

In the PIM SM network using BSR mechanism, every router can set itself as C-RP (candidate rendezvous point) servicing particular groups. If elected, a C-RP becomes the RP servicing the current group.

In BSR mechanism, a C-RP router unicasts C-RP messages to the BSR, which then propagates the C-RP messages among the network by BSR message. To prevent C-RP spoofing, you need to configure **crp-policy** on the BSR to limit legal C-RP range and their service group range. Since each C-BSR has the chance to become BSR, you must configure the same filtering policy on each C-BSR router.

This command uses the ACLs numbered between 3000 and 3999. The **source** parameter in the **rule** command is translated as C-RP address in the **crp-policy** command, and the **destination** parameter as the service group range of this C-RP

address. For the C-RP messages received, only when their C-RP addresses match the **source** address and their server group addresses are subset of those in ACL, can the be considered as matched.

For the related commands, see **acl** and **rule**.

Example

Configure C-RP filtering policy on the C-BSR routers, allowing only 1.1.1.1/32 as C-RP and to serve only for the groups 225.1.0.0/16.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
[Quidway] pim
[Quidway-pim] crp-policy 3000
[Quidway-pim] quit
[Quidway] acl number 3000
[Quidway-acl-adv-3000] rule 0 permit source 1.1.1.1 0 destination 225.1.0.0
0.0.255.255
```

4.1.5 debugging pim common

Syntax

```
debugging pim common { all | event | packet | timer }
undo debugging pim common { all | event | packet | timer }
```

View

User view

Parameter

all: All the common debugging information of PIM.

event: Debugging information of common PIM event.

packet: Debugging information of PIM hello packet.

timer: Debugging information of common PIM timer.

Description

Using **debugging pim common** command, you can enable common PIM debugging functions. Using **undo debugging pim common** command, you can disable the debugging functions.

By default, common PIM debugging functions are disabled.

Example

```
# Enable all common PIM debugging functions
```

```
<Quidway> debugging pim common all
```

4.1.6 debugging pim dm

Syntax

```
debugging pim dm { alert | all | mrt | timer | warning | { recv | send } { all | assert |  
graft | graft-ack | join | prune } }
```

```
undo debugging pim dm { alert | all | mrt | timer | warning | { recv | send } { all |  
assert | graft | graft-ack | join | prune } }
```

View

User view

Parameter

alert: Interoperation event debugging information of PIM-DM

all: All the debugging information of PIM-DM.

mrt: Debugging information of PIM-DM multicast routing table.

timer: Debugging information of PIM-DM timer.

warning: Debugging information of PIM-DM warning message.

recv: Debugging information of PIM-DM receiving packets.

send: Debugging information of PIM-DM sending packets.

assert | graft | graft-ack | join | prune: Packets type.

Description

Using **debugging pim dm** command, you can enable PIM-DM debugging functions.

Using **undo debugging pim dm** command, you can disable the debugging functions.

By default, PIM-DM debugging functions are disabled.

Example

```
# Enable all PIM-DM debugging functions
```

```
<Quidway> debugging pim dm all
```

4.1.7 debugging pim sm

Syntax

```
debugging pim sm { all | verbose | mrt | warning | mbr { alert | fresh } | timer { assert  
| bsr | crpadv | jp | jpdelay | mrt | probe | spt } | { recv | send } { assert | bootstrap |  
crpadv | reg | regstop | jp } }  
undo debugging pim sm { all | verbose | mrt | warning | mbr { alert | fresh } | timer  
{ assert | bsr | crpadv | jp | jpdelay | mrt | probe | spt } | { recv | send } { assert |  
bootstrap | crpadv | reg | regstop | jp } }
```

View

User view

Parameter

mbr: Debugging information of PIM-SM multicast border router event.

verbose: Debugging detail information of PIM-SM.

mrt: Debugging information of PIM-SM multicast routing table.

timer: Debugging information of PIM-SM timer.

warning: Debugging information of PIM-SM warning message.

recv: Debugging information of PIM-SM receiving packets.

send: Debugging information of PIM-SM sending packets.

alert | **fresh**: Type of debugging information of PIM-SM multicast border router event.

assert | **bootstrap** | **crpadv** | **jp** | **reg** | **regstop**: Packets type.

assert | **bsr** | **crpadv** | **jp** | **jpdelay** | **mrt** | **probe** | **spt**: Type of debugging information of PIM-SM timer.

Description

Using **debugging pim sm** command, you can enable PIM-SM debugging functions.

Using **undo debugging pim sm** command, you can disable the debugging functions.

By default, PIM-SM debugging functions are disabled.

Example

```
# Enable all PIM-SM debugging functions
```

```
<Quidway> debugging pim sm all
```

4.1.8 display pim bsr-info

Syntax

```
display pim bsr-info
```


View

Any view

Parameter

None

Description

Using **display pim bsr-info** command, you can view the BSR information.

For the related commands, see **c-bsr** and **c-rp**.

Example

```
<Quidway> display pim bsr-info
Current BSR Address: 20.20.20.30
Priority: 0
Mask Length: 30
Expires: 00:01:55
Local host is BSR
```

Table 4-1 Output description of the **display pim bsr-info** command

Field	Description
BSR	Boot trap router
Priority	Priority of BSR
Mask Length: 30	Length of mask
Expires: 00:01:55	Expire time

4.1.9 display pim interface

Syntax

display pim interface [**Vlan-interface** *vlan-interface-number*]

View

Any view

Parameter

Vlan-interface *vlan-interface-number* Interface type and interface number, used to specify the interface.

Description

Using **display pim interface** command, you can view the PIM interface configuration information.

Example

```
<Quidway> display pim interface
PIM information of VLAN-interface 2:
  IP address of the interface is 10.10.1.20
  PIM is enabled
  PIM version is 2
  PIM mode is Sparse
  PIM query interval is 30 seconds
PIM neighbor limit is 128
  PIM neighbor policy is none
  Total 1 PIM neighbor on interface
  PIM DR(designated router) is 10.10.1.20
```

Table 4-2 Output description of the **display pim interface** command

Field	Description
PIM version	Version of PIM
PIM mode	PIM mode enabled on the interface (DM or SM)
PIM query interval	Hello packet interval
PIM neighbor limit	Limit of the PIM neighbors on an interface. No neighbor can be added any more when the limit is reached
PIM neighbor policy	Filtering policy of the PIM neighbors on the current interface
PIM DR	Designated router

4.1.10 display pim neighbor

Syntax

display pim neighbor [interface Vlan-interface *vlan-interface-number*]

View

Any view

Parameter

Vlan-interface *vlan-interface-number*: Interface type and interface number, used to specify the interface.

Description

Using **display pim neighbor** command, you can view the PIM neighbor information.

Example

```
<Quidway> display pim neighbor
Neighbor Address   Interface Name      Uptime      Expires
8.8.8.6            VLAN-interface10    1637        89
```

Table 4-3 Output description about PIM neighbors

Field	Description
Neighbor Address	Neighbor address
Interface	Interface where the neighbor has been discovered
Uptime	Time passed since the multicast group has been discovered
Expires	Specifies when the member will be removed from the group

4.1.11 display pim routing-table

Syntax

```
display pim routing-table [ { { *g [ group-address [ mask { mask-length | mask } ] ] |  

**rp [ rp-address [ mask { mask-length | mask } ] ] } | { group-address [ mask  

{ mask-length | mask } ] | source-address [ mask { mask-length | mask } ] } * } |  

incoming-interface { Vlan-interface vlan-interface-number | null } | { dense-mode |  

sparse-mode } ] *
```

View

Any view

Parameter

****rp**: (*, *, RP) route entry.

***g**: (*, G) route entry.

group-address: Address of the multicast group.

source-address: IP address of the multicast source.

incoming-interface Vlan-interface *vlan-interface-number*: Route entry with the specified incoming interface.

null: Specifies the incoming interface type as Null.

dense-mode: Specifies the multicast routing protocol as PIM-DM.

sparse-mode: Specifies the multicast routing protocol as PIM-SM.

Description

Using **display pim routing-table** command, you can view the contents of the PIM multicast routing table.

For the related command, see display multicast routing-table.

Example

View the contents of the PIM multicast routing table on the router.

```
<Quidway> display pim routing-table
PIM-SM Routing Table
Total 0 (*,*,RP)entry, 0 (*,G)entry, 2 (S,G)entries

(192.168.1.2, 224.2.178.130),
Protocol 0x20: PIMSM, Flag 0x4: SPT
UpTime: 23:59, Timeout after 196 seconds
Upstream interface: VLAN-interface2, RPF neighbor: NULL
Downstream interface list: NULL

(192.168.1.2, 224.2.181.90),
Protocol 0x20: PIMSM, Flag 0x4: SPT
UpTime: 23:59, Timeout after 196 seconds
Upstream interface: VLAN-interface2, RPF neighbor: NULL
Downstream interface list: NULL

Total 2 entries listed
```

Table 4-4 Output description about PIM routing table

Field	Description
RP	Rendezvous Point
(S,G)	(source address, multicast group)
PIM-SM	PIM Sparse Mode
SPT	Shortest Path Tree
RPF	Reverse Path Forwarding

4.1.12 display pim rp-info

Syntax

display pim rp-info [*group-address*]

View

Any view

Parameter

group-address: Specifies the group address to display. If no multicast group is specified, the RP information about all multicast groups will be displayed.

Description

Using **display pim rp-info** command, you can view the RP information of multicast group.

In addition, this command can also display the BSR and static RP information.

Example

View the RP information of multicast group

```
<Quidway> display pim rp-info
PIM-SM RP-SET information:
  BSR is: 20.20.20.20

  Group/MaskLen: 224.0.0.0/4
    RP 20.20.20.20
      Version: 2
      Priority: 0
      Uptime: 00:00:05
      Expires: 00:02:25
```

4.1.13 pim

Syntax

pim
undo pim

View

System view

Parameter

None

Description

Using **pim** command, you can enter the PIM view. Using **undo pim** command, you can clear the configurations in PIM view.

Example

Enable multicast and enter the PIM view.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
[Quidway] pim
[Quidway-pim]
```

4.1.14 pim bsr-boundary

Syntax

pim bsr-boundary
undo pim bsr-boundary

View

Vlan interface view

Parameter

None

Description

Using **pim bsr-boundary** command, you can configure an interface to be the PIM domain border. Using **undo pim bsr-boundary** command, you can remove the border.

You can use this command to set border of bootstraps messages, that is to say, bootstrap messages cannot pass interfaces that are configured with **pim bsr-boundary** command while other PIM messages can. In this way, the network is divided into different BSR domains.

By default, no domain border is set.

For the related command, see **c-bsr**.

Example

Configure domain border on VLAN-interface10.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface10] pim bsr-boundary
```

4.1.15 pim dm

Syntax

pim dm
undo pim dm

View

Vlan interface view

Parameter

None

Description

Using **pim dm** command, you can enable PIM-DM. Using **undo pim dm** command, you can disable PIM-DM.

By default, PIM-DM is disabled.

Once enabled PIM-DM on an interface, PIM-SM cannot be enabled on the same interface and vice versa.

Example

Enable PIM-DM on VLAN-interface10 of the Ethernet switch.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface10] pim dm
```

4.1.16 pim neighbor-limit

Syntax

pim neighbor-limit *limit*
undo pim neighbor-limit

View

Vlan interface view

Parameter

limit: Limits of PIM neighbors on the interface, in the range of 0~128.

Description

Using **pim neighbor-limit** command, you can limit the PIM neighbors on an interface. No neighbor can be added any more when the limit is reached. Using **undo pim neighbor-limit** command, you can restore the default setting.

By default, the PIM neighbors on the interface are limited to 128.

If the existing PIM neighbors exceed the configured value during configuration, they will not be deleted.

Example

Limit the PIM neighbors on the Vlan-interface10 to 50.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface10] pim neighbor-limit 50
```

4.1.17 pim neighbor-policy

Syntax

pim neighbor-policy *acl-number*
undo pim neighbor-policy

View

Vlan interface view

Parameter

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

Description

Using **pim neighbor-policy** command, you can set to filter the PIM neighbors on the current interface. Using **undo pim neighbor-policy** command, you can remove the setting.

Only the routers that match the filtering rule in the ACL can serve as a PIM neighbor of the current interface.

The new configuration overwrites the old one if you run the command for a second time.

Example

Configure that 10.10.1.2 can serve as a PIM neighbor of the Vlan-interface10, but not 10.10.1.1.


```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface10] pim neighbor-policy 2000
[Quidway-Vlan-interface10] quit
[Quidway] acl number 2000
[Quidway-acl-basic-2000] rule permit source 10.10.1.2 0
[Quidway-acl-basic-2000] rule deny source 10.10.1.1 0
```

4.1.18 pim sm

Syntax

pim sm
undo pim sm

View

Vlan interface view

Parameter

None

Description

Using **pim sm** command, you can enable the PIM-SM protocol on an interface. Using **undo pim sm** command, you can disable the PIM-SM protocol.

By default, PIM-SM is disabled.

Once enabled PIM-SM on an interface, PIM-DM cannot be enabled on the same interface and vice versa.

Example

Enable PIM-SM on VLAN-interface10.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface10] pim sm
```

4.1.19 pim timer hello

Syntax

pim timer hello seconds

undo pim timer hello

View

Vlan interface view

Parameter

seconds: Interval of sending Hello messages in second ranging from 1 to 18000. By default, the interval value is 30 seconds.

Description

Using **pim timer hello** command, you can configure the interval of sending PIM router Hello messages. Using **undo pim timer hello** command, you can restore the default value.

Example

Configure to transmit Hello packet via VLAN-interface10 every 40 seconds.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
[Quidway] interface Vlan-interface 10
[Quidway-Vlan-interface10] pim timer hello 40
```

4.1.20 register-policy

Syntax

register-policy *acl-number*

undo register-policy

View

PIM view

Parameter

acl-number: Number of IP advanced ACL, defining the rule of filtering the source and group addresses. The value ranges from 3000 to 3999.

Description

Using **register-policy** command, you can configure a RP to filter the register messages sent by the DR in the PIM-SM network and to accept the specified messages only. Using **undo register-policy** command, you can remove the configured message filtering.

Example

If the local device is the RP in the network, using the following command can only accept multicast message register of the source sending multicast address in the range of 225.1.0.0/16 on network segment 10.10.0.0/16.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
[Quidway] acl number 3010
[Quidway-acl-adv-3010] rule permit ip source 10.10.0.0 0.0.255.255
destination 225.1.0.0 0.0.255.255
[Quidway-acl-adv-3010] quit
[Quidway] pim
[Quidway-pim] register-policy 3010
```

4.1.21 reset pim neighbor

Syntax

```
reset pim neighbor { all | { neighbor-address | interface Vlan-interface
vlan-interface-number } * }
```

View

User view

Parameter

all: All PIM neighbors

neighbor-address: Specifies neighbor address.

Vlan-interface *vlan-interface-number*: Specifies interface.

Description

Using **reset pim neighbor** command, you can clear a PIM neighbor.

For the related command, see **display pim neighbor**.

Example

Clear the PIM neighbor 25.5.4.3.

```
<Quidway> reset pim neighbor 25.5.4.3
```

4.1.22 reset pim routing-table

Syntax

```
reset pim routing-table { all | { group-address [ mask { group-mask |  
group-mask-length } ] | source-address [ mask { source-mask | source-mask-length } ]  
| { incoming-interface { Vlan-interface vlan-interface-number | null } } * }
```

View

User view

Parameter

all: All PIM neighbors

group-address: Specifies group address.

mask *group-mask*: Specifies group mask.

group-mask-length: Specifies mask length of the group address.

source-address: Specifies source address.

mask *source-mask*: Specifies source mask.

source-mask-length: Specifies mask length of the group address.

incoming-interface: Specifies incoming interface for the route entry in PIM routing table.

Vlan-interface *vlan-interface-number*: Specifies the interface.

null: Specifies the incoming interface of the route entry as null.

Description

Using **reset pim routing-table** command, you can clear a PIM route entry.

You can type in source address first and group address after in the command, as long as they are valid. Error information will be given if you type in invalid addresses.

If in this command, the *group-address* is 224.0.0.0/24 and *source-address* is the RP address (where group address can have a mask, but the resulted IP address must be 224.0.0.0, and source address has no mask), then it means only the (*, *, RP) item will be cleared.

If in this command, the *group-address* is any a group address, and *source-address* is 0 (where group address can have a mask, and source address has no mask), then only the (*, G) item will be cleared.

This command shall clear not only multicast route entries from PIM routing table, but also the corresponding route entries and forward entries in the multicast core routing table and MFC.

For the related commands, see **reset multicast routing-table**, **reset multicast forwarding-table** and **display pim routing-table**.

Example

```
# Clear the route entries with group address 225.5.4.3 from the PIM routing table.
```

```
<Quidway> reset pim neighbor 25.5.4.3
```

4.1.23 source-policy

Syntax

source-policy *acl-number*

undo source-policy

View

PIM view

Parameter

acl-number: Basic or advanced ACL, in the range of 2000 to 3999.

Description

Using **source-policy** command, you can set to filter the source (and group) address of multicast data packets. Using **undo source-policy** command, you can remove the configuration.

If source address filtering is configured, as well as basic ACLs, then the router filters the source addresses of all multicast data packets received. Those not matched will be discarded.

If source address filtering is configured, as well as advanced ACLs, then the router filters the source and group addresses of all multicast data packets received. Those not matched will be discarded.

When this feature is configured, the router filters not only multicast data, but the multicast data encapsulated in the registration packets.

The new configuration overwrites the former one if you run the command for a second time.

Example

Set to receive the multicast data packets from source address 10.10.1.2, but discard those from 10.10.1.1.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
[Quidway] pim
[Quidway-pim] source-policy 2000
[Quidway-pim] quit
[Quidway] acl number 2000
[Quidway-acl-basic-2000] rule permit source 10.10.1.2 0
[Quidway-acl-basic-2000] rule deny source 10.10.1.1 0
```

4.1.24 static-rp

Syntax

static-rp *rp-address* [*acl-number*]

undo static-rp

View

PIM view

Parameter

rp-address: Static RP address, only being legal unicast IP address.

acl-number: Basic ACL, used to control the range of multicast group served by static RP, which ranges from 2000 to 2999. If an ACL is not specified upon configuration, static RP will serve all multicast groups; if an ACL is specified, static RP will only serve the multicast group passing the ACL.

Description

Using **static-rp** command, you can configure static RP. Using **undo static-rp** command, you can remove the configuration.

Static RP functions as the backup of dynamic RP so as to improve the network robusticity. If the RP elected by BSR mechanism is valid, static RP will not work.

All routers in the PIM domain should be configured with this command and be specified with the same RP address.

The new configuration overwrites the old one if you run the command for a second time.

For related command, see **display pim rp-info**.

Example

Configure 10.110.0.6 as a static RP.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] multicast routing-enable
[Quidway] pim
[Quidway-pim] static-rp 10.110.0.6
```