QTECH
МИР ДОСТУПНЕЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Multicast commands

Оглавление

1. IPV4 MULTICAST ROUTING CONFIGURATION COMMANDS

1.1. clear ip mroute

Use this command to remove the forwarding information of the IP multicast routes.

clear ip mroute {* | *group-address* [*source -address*] }

Parameter Description

Parameter	Description
*	Remove all the forwarding information in the IP multicast route table.
group-address	Group IP address of IP multicast routes.
source-address	Source IP address of multicast routess.

Command Mode
Privileged EXEC mode.

Examples

Related Commands

The following example removes the entry whose group IP address is 230.0.0.1 from the multicast routing table:

QTECH# clear ip mroute *230.0.0.1*

1.2. clear ip mroute statistics

this command to remove the statistics of IP multicast routes.

clear ip mroute statistics {***** | *group-address* [*source -address*]}

Command	Description
show ip mroute	Show the forwarding information of multicast routes.

Parameter Description

Parameter	Description
*	Remove all the forwarding entries in the multicast route table.

group-address	Group IP address of IP multicast routes
source-address	Source IP address of multicast route.

Command Mode
Privileged EXEC mode.

Usage Guide

Examples
The following example clears the statistics of entry with the group IP address 230.0.0.1 from the multicast routing table.

```
QTECH# clear ip mroute statistics 230.0.0.1
```

Related Commands

Command	Description
show ip mroute	Show the multicast route forwarding information.
clear ip mroute	Clear the multicast route forwarding information.

1.3. ip mroute

Parameter Description

Use this command to configure static multicast routes. Use the **no** or **default** form of this command to delete the configured routes.

ip mroute *source-address mask*{ [*protocol*] {*rpf-addrress* | *interface-type interface-number*} [*distance*]

no ip mroute *source-address mask* [*protocol*]

default ip mroute *source-address mask* [*protocol*]

Parameter	Description
source-address	Source IP address of the multicast route

mask	Mask of the source IP address
protocol	(Optional) The unicast routing protocol being used.
rpf-address	Incoming interface of the multicast route
interface-type *interface-number*	Interface type and interface ID.
distance	Management distance used to determine whether to use the route for RPF routing, ranging from 1 to 255. The default value is 0.

Default

distance: 0.

Command Mode

Global configuration mode.

Usage Guide

This command is used to configure the route for the purpose of RFF check. Note that the configured route is prior to the route learned in the unicast form.

```
QTECH(config)# ip mroute 172.16.0.0 255.255.0.0
172.30.10.13
```

Examples

The following example allows the multicast routes of all the sources in a

network to pass 172.30.10.13:

1.4. ip multicast-routing

Use this command to enable multicast routing forwarding. The **no** form of this command disables multicast routing forwarding.

ip multicast-routing [**vrf** *vrf-name*]

no ip multicast-routing [**vrf** *vrf-name*]

Parameter Description

Parameter	Description
vrf vrf-name	Specify the VRF instance.

Default
Disabled.

Command Mode

Global configuration mode.
This command allows you to enable IPv4 multicast routing forwarding. The multicast protocol will not be enabled with IPv4 multicast routing forwarding disabled.

Usage Guide
It is not recommended to configure different v4 multicast routing protocols on different interfaces of a device.

Examples
This command enables multicast routing forwarding.

```
QTECH(config)# ip multicast-routing
```

1.5. ip multicast boundary

Use this command to configure the boundary of an IP multicast group. Use the no or default form of this command to remove the configured boundary.

ip multicast boundary *access-list* [in | out]

no ip multicast boundary *access-list* [in | out]

default ip multicast boundary *access-list* [in | out]

Parameter Description

Parameter	Description
access-list	Access list associated with the multicast boundary.
in	Inbound direction.
out	Outbound direction.

Default

The boundary of a specified IP multicast group is defined by default.

Command Mode
Interface configuration mode

Usage Guide

Note that the ACL associated with the multicast boundary is either standard ACL or extended ACL. But the extended ACL only match the destination IP address.

Note:

This command filters IGMP and PIMSM packets of the specified IP address range. Multicast packets will not be received and sent through the interface of the boundary.

The following example configures svi1 as the boundary of all IP multicast groups.

```
QTECH(config)# ip access-list mul-boun
QTECH(config-std-nacl)# permit ip 233.3.3.0 0.0.0.255 QTECH(config-std-nacl)#exit
QTECH(config)# interface vlan 1
QTECH(config-if)# ip multicast boundary mul-boun
```

Examples

1.6. ip multicast route-limit

Use this command to limit the number of the entries that can be added to the multicast routing table. Use the **no** or **default** form of this command to remove the configuration. **ip multicast route-limit** *limit* [*threshold*]

no ip multicast route-limit ***limit***

default ip multicast route-limit

Parameter Description

Parameter	Description
limit	The number of the entries that can be added to the multicast routing table is 1 to 2147483647. The default value is 1024.
threshold	(Optional) Number of multicast routes at which alarms will be triggered. The default value is 2147483647.

Default

The default value of *limit* is 1024.

The default value of *threshold* is 2147483647.

Command Mode
Global configuration mode.

Usage Guide

Note that the hardware resources of different devices are limited. The routes exceeding the hardware resource will be forwarded by software, which leads to lower product performance.

Examples

The following example sets the route limit to 500.

```
QTECH(config)# ip multicast route-limit 500
```

1.7. ip multicast rpf longest-match

Select the multicast static routing, MBGP routing and unicast routing that could be used for the RPF check from the multicast static routing table, MBGP routing table and unicast routing table respectively by following the RPF rules.

Use this command to select the one with the mask longest-matched from the three routings. If the routings are in the same priority, select the routing in order of multicast static routing, MBGP routing, unicast routing.

Use the **no** or **default** form of this command restores it to the default setting. By default, select one routing of the highest priority from the three routings. If the routings are in the same priority, select the routing in order of multicast static routing, MBGP routing, unicast routing.

ip multicast rpf longest-match

no ip multicast rpf longest-match default ip multicast rpf longest-match

Parameter Description

Parameter	Description
N/A	N/A

Default

Use the RPF rule to select the optimal routing for RPF check from the multicast static routing, MBGP routing and unicast routing that are used for the RPF check from the multicast static routing table, MBGP routing table and unicast routing table respectively by following the RPF rules. Then select one routing of the highest priority from the three routings. If the routings are in the same priority, select the routing in order of multicast static routing, MBGP routing, unicast

routing.

Command Mode

Global configuration mode.

Examples

The following example configures to select the routing with the longest-match.

```
QTECH(config)# ip multicast rpf longest-match
```

1.8. ip multicast static

Use this command to enable flow control for multicast packets on the Layer 2 interface. Use the **no** or **default** form of this command removes the setting.

ip multicast static *source-address group-address interface-type interface-number*

no ip multicast static *source-address group-address interface-type interface-number*

default ip multicast static *source-address group-address interface-type interface-number*

Parameter Description

Parameter	Description
source-address	Source IP address
group-address	IP address of the multicast group
interface-type interface number	Layer 2 interface on which multicast packets are allowed to forward

Default

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

You can configure more than one command (or more than one interface) for a multicast flow. With flow control enabled, the multicast flow can only be forwarded through these configured interfaces.

This command controls the forwarding of multicast flows on an interface without

any direct influence on the packet processing of multicast protocols. However, the action of a multicast protocol (for instance, PIM-DM or PIM-SM) may be affected because some features of the multicast protocol are driven by multicast flows.

Examples

The following example configures forwarding multicast flows (192.168.43.4 and 255.1.1.5) through GigabitEthernet 2/6 and FastEthernet 3/2.

```
QTECH(config)# ip multicast static 192.168.43.4 225.1.1.5 G2/6
QTECH(config)# ip multicast static 192.168.43.4 225.1.1.5 F3/2
```

1.9. ip multicast ttl-threshold

Use this command to configure TTL (time-to-live) threshold on the interface. Use the **no** or **default** form of the command to restore it to the default value.

ip multicast ttl-threshold *ttl-value*

ip multicast ttl-threshold default ip multicast ttl-threshold

Parameter Description

Parameter	Description
ttl-value	TTL threshold on the interface, within the range of 0 to 255.

Default

The default *ttl-value* is 0.

Command Mode

Interface configuration mode.

Usage Guide

Use show running-config to display configuration. A device with multicast enabled can maintain one TTL threshold for every interface. If the TTL of the multicast packet received is greater than the threshold of the interface, the packets will be forwarded. Otherwise, the packet is discarded. Note that the TTL threshold is effective only to the multicast frames. In addition, you must configure it on the L3 interface.

Examples

The following example sets the TTL threshold on the interface to 5.

```
QTECH(config-if)# ip multicast ttl-threshold 5
```

1.10. msf force-forwarding

Use this command to enable IPv4 multicast data packets destined for the CPU to be forcedly forwarded by software. Use the **no** or **default** form of this command to restore the default settings.

msf force-forwarding

no msf force-forwarding default msf force-forwarding

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Global configuration mode

Defaults

This function is disabled by default.

Usage Guide

N/A

Examples

The following example enable IPv4 multicast data packets destined for the

CPU to be forcedly forwarded by software.

```
QTECH(config)# msf force-forwarding
```

1.11. msf ipmc-overflow override

Use this command to enable the overflow overriding mechanism. Use the **no** or **default** form of this command to remove the configuration.

msf ipmc-overflow override no msf ipmc-overflow override

default msf ipmc-overflow override

Parameter Description

Parameter	Description

-	-

Default

This function is disabled by default.

Command Mode
Global configuration mode.

Usage Guide

N/A

The following example enables the overflow overriding mechanism.
Examples

```
QTECH (config)# msf ipmc-overflow override
QTECH (config)#
```

1.12. msf nsf

Parameter Description

Default

Use this command to configure the parameter for the continuous multicast forwarding. Use the **no** or **default** form of this command to remove the configuration.

msf nsf {{**convergence-time** *time*} | {**leak** *interval*} }

no msf nsf **{**convergence-time **|**

leak**}** default msf nsf

{convergence-time **|** leak**}**

convergence-time *time* :140s;

leak interval: 150s

Parameter	Description
convergence-time *ttl-value*	Maximum time for the multicast protocol convergence, in the valid range of the 0-3600s.
leak *interval*	Packet multicast leak time, in the valid range of 0-3600s

Command Mode

Global configuration mode.

Usage Guide

N/A

```
QTECH (config)# msf nsf convergence-time 300
QTECH (config)#
```

The following example sets the maximum time for the protocol convergence.

Examples

```
QTECH(config)# msf nsf leak 200
QTECH(config)#
```

The following example sets the packets leak time:

1.13. show ip mrf mfc

Use this command to show the IPv4 multicast routing forwarding table.

show ip mrf mfc [*soure-address group-address*]

Parameter Description

Parameter	Description
source-address	Source address of the multicast routing forwarding entries.
group-address	Group address of the multicast routing forwarding entries.

Default -

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

The three parameters in this command are optional, wherein the source address and group address must be specified at the same time.

- If no source address and group address are specified, all mfc entries are displayed.
- When the source address and group address are specified only, the entries corresponding to the source and group addresses are displayed.

The following example shows all IPv4 layer-3 multicast routing forwarding entries with source address 20.0.1.30.

```
QTECH#show ip mrf mfc 20.0.1.30 233.3.3.3 Multicast Routing and
Forwarding Cache Table (20.0.1.30, 233.3.3.3)
 FAST_SW, SWTCHED, MIN_MTU: 1500, MIN_MTU_IFINDEX: 4099, WRONG IF: 0
 Incoming interface: VLAN 1[4097] Outgoing interface
list:
VLAN 3 (1)
```

The fields in the execution of the **show ip mrf mfc** command are described in the following table.

Examples

Field	Description
20.0.1.30	Source address of the entry.
233.3.3.3	Group address of the entry.
FAST_SW	The Flag shows whether to allow the fast forwarding or not. If the non-Ethernet interface, ppp, hdlc and frame relay exist, no fast forwarding entry generates.
SWTCHED	Indicate whether the entry configuration on the next layer forwarding table has done not not.
MIN_MTU MTU	The minimum MTU of the entry.
MIN_MTU_IFINDEX	The interface index with the minimum MTU value.
WRONG IF	The statistics number of the multicast data packets received on the wrong incoming interface.
Incoming interface	Incoming interface of the entry.
VLAN 3 (1)	The layer-3 outgoing interface of the entry is VLAN3. 1 for the ttl threshold of this layer-3 interface.

1.14. show ip mroute

Use this command to show the multicast forwarding table.

show ip mroute [*group-or-source-address* [*group-or-source-address*]] [**dense** | **sparse**] [**summary** | **count**]

Parameter Description

Parameter	Description
group-or-source-address	Multicast or source IP address
group-or-source-address	Multicast or source IP address. The two addresses must not be the multicast addresses or source addresses at the samet time.
dense	Show PIM-DM multicast routing table.
sparse	Show PIM-SM multicast routing table.
summary	Show the summary of the multicast routing table.
count	Show the count of the multicast routing table.

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuraion mode

Usage Guide

The three parameters in this command are optional, wherein the source address and group address must be specified at the same time.

- If no source address and group address are specified, all mfc entries are displayed.
- When the source address and group address are specified only, the mfc entries corresponding to the source and group addresses are displayed.

The following example shows the information of the multicast routing table:

Examples

```
QTECH# show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed Timers: Uptime/Stat
Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:00:31, stat expires 00:02:59
Owner PIM-SM, Flags: TF
Incoming interface: FastEthernet 2/1 Outgoing interface
list: FastEthernet 1/3
```

```
QTECH# show ip mroute 10.10.1.52 224.0.1.3
IP Multicast Routing Table
```

The following example shows the information of a specific entry:

```
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed Timers:
Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:03:24, stat expires 00:01:28
Owner PIM-SM, Flags: TF
Incoming interface: FastEthernet 2/1 Outgoing interface list: FastEthernet
1/3
```

```
QTECH# show ip mroute count IP Multicast Statistics
Total 1 routes using 132 bytes memory
Route limit/Route threshold: 2147483647/2147483647 Total
NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 1/0/0 Total NOCACHE/WRONGVIF/WHOLEPKT
sent to clients: 1/0/0 Immediate/Timed stat updates sent to clients: 0/0
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0 Next stats poll:
00:01:10
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts Fwd msg counts:
WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent Reg pkt counts: Reg ACK
recv/Reg NACK recv/Reg pkt sent (10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
```

The following example shows the count of the routing table:

```
QTECH# show ip mroute summary IP Multicast Routing
Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed Timers: Uptime/Stat
Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), 00:01:32/00:03:20, PIM-SM, Flags: T
```

The following example shows the summary of the routing table:

Field	Description
Flags	I-Immediate statistic T-Timed statistic F-Already set to the forwarding table
Timers:Uptime/Stat Expiry	Time when the entry is created. Time when it is aged.
Interface State	Interface state.

Owner	Owner of the entry, which may be a multicast routing protocol
Incoming interface	Expected packet incoming interface. If the actual incoming interface does not match it, the packets will be discarded.
Outgoing interface list	Outgoing interface list; the packets will be forwarded on the interfaces in the list.
Forwarding Counts: Pkt count/Byte count,	Forwarding count: packet count/byte count forwarded by the entry
Other Counts: Wrong If pkts	Count of the packets received from the wrong incoming interface.

Related Commands

Command	Description
ip multicast-routing	Enabling the multicast routing forwarding.
ip pim dense-mode	Enable the PIM-DM on the interface.
ip pim sparse-mode	Enable the PIM-SM on the interface.

1.15. show ip mroute static

Use this command to show the v4 static multicast routing information.

show ip mroute static

Parameter Description

Parameter	Description

-	-

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuraion mode

Usage Guide

In the same conditions, the priority of the static multicast routing is higher than the dynamically learned.

Examples

The following example shows the information of the user-configured static multicast routing:

```
QTECH#show ip mroute static
Mroute: 172.16.0.0, RPF neighbor: 172.30.10.13 Protocol: , distance:
 0
```

1.16. show ip mvif

Use this command to show the basic information of the multicast interface.

show ip mvif { *interface-type interface-number* }

Parameter Description

Parameter	Description
interface-type interface-number	Interface Type and number

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuraion mode

The following example shows the basic information of the multicast interface of svil.

Examples

```
QTECH#show ip mvif vlan 1
Interface Vif Owner TTL Local Remote Uptime Idx Module Address
 Address
VLAN 1 1 PIM-DM 2 192.168.1.1 0.0.0.0 00:13:16
```

1.17. show ip rpf

Parameter Description

Use this command to show the RPF information of the specified source IP address.

show ip rpf {*source-address* }

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuraion mode

Parameter	Description
source-address	Specified source IP address

Usage Guide

The three parameters in this command are optional, wherein the source address and group address must be specified at the same time.

- If no source address and group address are specified, all mfc entries are displayed.
- When the source address and group address are specified only, the mfc entries corresponding to the source and group addresses are displayed.

The following example shows the information of the RPF to 192.168.1.54:

Examples

```
QTECH# show ip rpf 192.168.1.54 RPF information for
192.168.1.54 RPF interface: VLAN 1
RPF neighbor: 0.0.0.0
RPF route: 192.168.1.0/24
RPF type: unicast (connected) RPF recursion count:
0
Doing distance-preferred lookups across tables Distance: 0
Metric: 0
```

1.18. show msf msc

Use this command to show IPv4 multi-layer multicast forwarding table.

show msf msc [*soure-address*] [*group-address*]

Parameter Description

Parameter	**Description**
source-address	Specified source IP address of the multi-layer multicast forwarding table.
group-address	Specified group address of the multi-layer multicast forwarding table.

Default -

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuraion mode

Usage Guide

The three parameters in this command are optional.

- If only the source address is specified as s1, all msc entries with source address 1 are displayed.
- If the source address is specified as s1 and the group address as g1, all corresponding msc entries are displayed.
- Each parameter shall be input in order. Only when the parameter in front has been configured, the following one could be set.

The following example shows the IPv4 layer-3 multicast forwarding entries

with source IP address 192.168.195.25:

```
QTECH# show msf msc 192.168.195.25
Multicast Switching Cache Table
(192.168.195.23, 233.3.3.3, 1), SYNC, MTU:0, 1 OIFs
VLAN 1(0): 1 OPORTs, REQ: DONE OPORT 6, IGMP-SNP,
REQ: DONE
```

The fields in the execution of the **show mrf mfc** command are described in the following table.

Examples

Field	Description
192.168.195.23	Source address of the entry.
233.3.3.3	Group address of the entry.
1	Vlan id where the incoming interface of the entry is.
SYNC	The entry has been synchronized to the hardware.
MTU	MTU value
OIFs	Layer-3 outgoing interface number.
VLAN1(0)	The vlan where the layer-3 outgoing

	interface oif is.
1 OPORTs	The number of layer-2 port in the layer-3 outgoing oif.
REQ: DONE	This oif configuration on the hardware has done.
OPORT 6	The layer-2 port in the oif with index 6.
IGMP-SNP	This port is created by the IGMP SNOOPING protocol. This value can also be the PIM-SNP, which means this port is created by the PIM SNOOPING protocol. And the ROUTER means this port is created by the layer-3 protocol.
REQ: DONE	The port configuration on the hardware has done.

1.19. show msf nsf

Use this command to show the configuration of continuous multicast forwarding.

show msf nsf

Parameter Description

Parameter	Description
-	-

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuraion mode

The following example shows the configuration of continuous multicast forwarding.

Examples

```
QTECH# show msf nsf Multicast HA Parameters
++ protocol convergence timeout 120 secs
flow leak interval 20 secs
QTECH#
```

Related Commands

Command	Description
msf nsf	Configure the multicast NSF parameter.

2. IPV6 MULTICAST ROUTING COMMANDS

2.1. clear ipv6 mroute

Use this command to remove the specific or all IPv6 multicast forwarding entries.

clear ipv6 mroute { ***** | *v6group-address* [*v6source -address*]}

Parameter Description

Parameter	Description
*	Removes all the forwarding information in the IPv6 multicast route table.
v6group-address	Group IPv6 address of IPv6 multicast routes
v6source-address	Source IPv6 address of multicast routes

Command Mode

Privileged EXEC mode

Configuration Examples

The following example removes all the multicast routing entries.

```
QTECH# clear ip mroute *
```

Related Commands

Command	Description
show ipv6 mroute	N/A
clear ipv6 mroute statistics	N/A

2.2. clear ipv6 mroute statistics

Use this command to remove the statistics of IPv6 multicast routes.

clear ipv6 mroute statistics {***** | *v6group-address* [*v6source -address*]}

Parameter Description

Parameter	Description
*	Removes all the forwarding entries in the multicast route table.
v6group-address	Group IPv6 address of IPv6 multicast routes
v6source-address	Source IPv6 address of multicast route

Command Mode
Privileged EXEC mode

Usage Guide -

Configuration Examples

The following example clears all the statistical information of the multicast routing entries.

```
QTECH# clear ip mroute statistics *
```

Related Commands

Command	Description
show ipv6 mroute	Displays the multicast route forwarding information.
clear ipv6 mroute	Clears the multicast route forwarding information.

2.3. ipv6 mroute

Use this command to configure static IPv6 multicast routes. Use the **no** or **default** form of this command to restore the default setting.

ipv6 mroute *ipv6-prefix/prefix-length* [*protocol*] { *v6rpf-addrress* | *interface-type interface-number* } [*distance*]

no ipv6 mroute *ipv6-prefix/prefix-length* [*protocol*]

default ipv6 mroute *ipv6-prefix/prefix-length* [*protocol*]

Parameter Description

Parameter	Description
ipv6-prefix/prefix-length	Source IPv6 address of the multicast route

mask	Mask of the source IPv6 address
protocol	(Optional) The unicast routing protocol being used
v6rpf-address	Incoming interface of the multicast route
interface-type *interface-number*	Interface type and interface ID
distance	Management distance used to determine whether to use the route for RPF routing, ranging from 1 to 255. The default value is 0.

Defaults
The static IPv6 multicast routing is not configured by default.

Command Mode
Global configuration mode

Usage Guide
This command is used to configure the route for the purpose of RFF check.
Note that the configured route is prior to the route learned in the unicast form.
If the outgoing direction of static multicast route but not the next-hop IP shall be specified, the outgoing direction must be of the point-to-point type.

Configuration Examples
The following example allows the static multicast route 2233::/64 to pass 3333::3333:

```
QTECH(config)# ipv6 mroute 2233::/64 3333::3333
```

2.4. ipv6 multicast boundary

Use this command to configure the boundary of an IPv6 multicast group. Use the **no** form of this command to restore the default setting.

ipv6 multicast boundary *access-list-name* [**in** | **out**]

no ipv6 multicast boundary *access-list-name* [**in** | **out**]

Parameter Description

Parameter	Description
access-list-name	Access list associated with the multicast boundary
in	Inbound redirection
out	Outbound direction

Defaults

The boundary of a specified IPv6 multicast group is not defined by default.

Command Mode

Interface configuration mode

Note that the ACL associated with the multicast boundary is either standard ACL or extended ACL. But the extended ACL only match the destination IPv6 address.

Usage Guide

This command filters MLD, PIM-SMv6 packets of the specified IPv6 address range. Multicast packets will not be received and sent through the interface of the boundary.

The following example configures svi1 as the boundary of all IPv6 multicast groups.

Configuration Examples

```
QTECH(config)# ip access-list mul-boun
QTECH(config-std-nacl)# permit ip 233.3.3.0 0.0.0.255 QTECH(config-std-
nacl)#exit
QTECH(config)# interface vlan 1
QTECH(config-if)# ip multicast boundary mul-boun
```

2.5. ipv6 multicast route-limit

Use this command to limit the number of the entries that can be added to the IPv6 multicast routing table. Use the **no** or **global** form of this command to restore the default setting. **ipv6 multicast route-limit** *limit* [*threshold*]

no ipv6 multicast route-limit *limit* [*threshold*]

default ipv6 multicast route-limit *limit* [*threshold*]

Parameter Description

Parameter	Description

limit	The number of the entries that can be added to the IPv6 multicast routing table is 1 to 2147483647
threshold	(Optional) Number of IPv6 multicast routes at which alarms will be triggered

Defaults

The default value of *limit* is 1024.

The default value of *threshold* is 2147483647.

Command Mode

Global configuration mode

Usage Guide

The hardware resources of different devices are limited. The routes exceeding the hardware resource will be forwarded by software, which leads to lower product performance.

Configuration Examples

The following example sets the route limit to 500 and the warning value 90.

```
QTECH(config)# ipv6 multicast route-limit 500 90
```

2.6. ipv6 multicast rpf longest-match

Use the RPF rule to select the static multicast route, MBGP route and the unicast route for the purpose of RPF check from the static multicast route list, the MBGP route list and the unicast route list.

Use this command to select one route with the longest-matched mask from the above-mentioned three routes. If the priority values of all three routes are the same, the routes will be selected in order of static multicast route, MBGP route and unicast route.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 multicast rpf longest-match

no ipv6 multicast rpf longest-match default ipv6 multicast rpf longest-match

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Use the RPF rule to select the static multicast route, MBGP route and the

unicast route for the purpose of RPF check from the static multicast route list, the

MBGP route list and the unicast route list.

Use this command to select one route, which is prior to the other two routes, with the longest-matched mask from the above-mentioned three routes. If the priority values of all three routes are the same, the routes will be selected in order of static multicast route, MBGP route and unicast route.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example selects one route with the longest-matched mask from

the above-mentioned three routes.

```
QTECH(config)# ipv6 multicast rpf longest-match
```

2.7. ipv6 multicast static

Parameter Description

Use this command to enable flow control for multicast packets on the Layer 2 interface. Use the

no or **default** form of this command to restore the default setting.

ipv6 multicast static *source-address group-address interface-type interface-number*

no ipv6 multicast static *source-address group-address interface-type interface-number*

default ipv6 multicast static *source-address group-address interface-type interface-number*

Parameter	Description
source-address	Source IPv6 address
group-address	IPv6 address of the multicast group
interface-type interface number	2-layer interface on which multicast packets are allowed to forward

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

You can configure more than one command (or more than one interface) for a multicast flow. With flow control enabled, the multicast flow can only be forwarded through these configured interfaces.

This command controls the forwarding of multicast flows on an interface without any direct influence on the packet processing of multicast protocols. However, the action of a multicast protocol (for instance, PIM-SMv6) may be affected because some features of the multicast protocol are driven by multicast flows.

Configuration Examples

The following example configures forwarding multicast flows (2222::3333, ff66::100) through GigabitEthernet 2/6 and FastEthernet 3/2.

```
QTECH(config)# ipv6 multicast static 2222::3333 ff66::100 G2/6
QTECH(config)# ipv6 multicast static 2222::3333 ff66::100 F3/2
```

2.8. ipv6 multicast-routing

Use this command to enable the IPv6 multicast routing forwarding. Use the **no** or **default** form of this command to restore the default setting.

ipv6 multicast-routing

no ipv6 multicast-routing default ipv6 multicast-routing

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default

Command Mode

Global configuration mode

Use this command to enable the IPv6 multicast routing forwarding. With this function disabled, the multicast protocol cannot be enabled.

Usage Guide

This command must be configured to enable the IPv6 multicast routing forwarding. This function conflicts with IGMP Snooping.

Configuration Examples

The following example enables the IPv6 multicast routing forwarding.

```
QTECH(config)# ipv6 multicast-routing
```

The following example disables the IPv6 multicast routing forwarding.

```
QTECH(config)#no ipv6 multicast-routing
```

2.9. msf6 force-forwarding

Use this command to enable IPv6 multicast data packets destined for the CPU to be forcedly forwarded by software. Use the **no** or **default** form of this command to restore the default settings.

msf6 force-forwarding no msf6 force-forwarding

default msf6 force-forwarding

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Examples

The following example enable IPv6 multicast data packets destined for the

CPU to be forcedly forwarded by software.

```
QTECH(config)# msf6 force-forwarding
```

2.10. msf6 nsf

Use this command to configure parameters for multicast non-stop forwarding. Use the no or default

form of this command to restore the default setting. msf6 nsf { convergence-time *time* | leak *interval* } no msf6 nsf { convergence-time | leak }

default msf6 nsf {convergence-time | leak}

Parameter Description

Parameter	Description
convergence-time *time*	Maximum duration for which the system waits for multicast protocol convergence The unit is second. The value ranges from 0 to 3600.
leak *interval*	Interval at which multicast packets are leaked The unit is second. The value ranges from 0 to 3600.

Defaults

The default convergence-time is 20 seconds and leak interval is 30 seconds.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example sets the maximum duration for which the system waits for multicast protocol convergence.

```
QTECH (config)# msf6 nsf convergence-time 300
```

The following example sets the interval at which multicast packets are leaked.

```
QTECH(config)# msf6 nsf leak 200
```

Command	Description
N/A	N/A

N/A

2.11. show ipv6 mrf6 mfc

Use this command to display the IPv6 multicast forwarding table.

show ipv6 mrf6 mfc [*v6source-address v6group-address*]

Parameter Description

Parameter	Description
v6group-address	IPv6 address of a multicast group
v6source-address	IPv6 address of a multicast source

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

The two parameters are optional. The source address and group address must be specified together.

If the two parameters are not specified, all mrf table entries will be displayed.

If the two parameters are specified, the mrf entries of the specified source address and group address are displayed.

Configuration Examples

The following example displays the 3-layer multicast forwarding table entries of IPv6 (the source address is 2000::1 and the group address is FF55::1).

```
QTECH#show ipv6 mrf6 mfc 2000::1 FF55::1 Multicast Routing
and Forwarding Cache6 Table (2000::1, FF55::1)
 FAST_SW, SWTCHED, MIN_MTU: 1500, MIN_MTU_IFINDEX: 4099, WRONG IF: 0
 Incoming interface: VLAN 1[4097] Outgoing
 interface list:
VLAN 3 (1)
```

Field	Description
2000::1	Source address of entries
FF55::1	Group address of entries
FAST_SW	Indicates whether the entries allow fast forwarding, that is, whether the entries can be forwarded by using hardware or software forwarding. If the entries include an interface that does not support the multicast function (for example, the GRE tunnel interface), fast forwarding is not allowed.
SWTCHED	Indicates whether the entries have been placed in the forwarding table on the next layer.
MIN_MTU MTU	Minimum MTU value of entries
MIN_MTU_IFINDEX	Index of the interface that has the minimum MTU value
WRONG IF	Number of multicast packets sent from the wrong inbound interface
VLAN 1[4097]	Indicates that the rpf inbound interface is VLAN1. 4097 indicates the IFINDEX of the interface.
VLAN 3 (1)	Indicates that the 3-layer outbound interface of the entries is VLAN 3. 1 indicates the ttl threshold of the 3-layer interface.

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

2.12. show ipv6 mroute

Use this command to display the IPv6 multicast forwarding table.

show ipv6 mroute [*group-or-source-address* [*group-or-source-address*]] [**sparse**] [**summary** | **count**]

Parameter Description

Parameter	Description
group-or-source-address	Multicat group IPv6 address
group-or-source-address	Multicast source IPv6 address
sparse	Displays the core entry of the multicast routing table.
summary	Displays the summary of the multicast routing table.
count	Displays the count of the multicast routing table.

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

The following example displays all information of the IPv6 multicast routing table.

```
QTECH# show ipv6 mroute IPv6 Multicast
Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed Timers:
Uptime/Stat Expiry
Interface State: Interface (TTL)
(2222::1234, ff56::1234), uptime 00:00:31, stat expires 00:02:59 Owner PIM-
SMv6, Flags: TF
Incoming interface: FastEthernet 2/1 Outgoing
interface list:
FastEthernet 1/3
```

The following example displays the count of the routing table.

```
QTECH# show ipv6 mroute count IPv6 Multicast
Statistics
Total 1 routes using 168 bytes memory
```

```
Route limit/Route threshold: 1024/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 77/147/0 Total
NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 77/147/0 Immediate/Timed
stat updates sent to clients: 0/29
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0 Next stats
poll: 00:00:09
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts Fwd msg counts:
WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent Reg pkt counts:
Reg ACK recv/Reg NACK recv/Reg pkt sent (2222::1234, ff56::1234), Forwarding:
1/0, Other: 0
 Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
```

Configurati on Examples

The following example displays the summary of the routing table.

```
QTECH# show ipv6 mroute summary IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed Timers:
Uptime/Stat Expiry
Interface State: Interface (TTL)
(2222::1234, ff56::1234), 00:00:28/00:03:25, PIM-SMv6, Flags: TF
```

Field	Description
Flags	I-Immediate statistic T-Timed statistic F-Already set to the forwarding table
Timers:Uptime/Stat Expiry	Time when the entry is created. Time when it is aged.
Interface State	Interface state.
Owner	Owner of the entry, which may be a multicast routing protocol
Incoming interface	Expected packet incoming interface. If the actual incoming interface does not match it, the packets will be discarded.
Outgoing interface list	Outgoing interface list; the packets will be forwarded on the interfaces in the list.

Forwarding Counts: count/Byte count,	Pkt	Forwarding count: forwarded by the entry	pac ket	count/ byte	
Other Counts: Wrong If pkts	Count of the packets received from the wrong incoming interface.				

Related Commands

Command	Description
clear ipv6 mroute	N/A
clear ipv6 mroute statistics	N/A

2.13. show ipv6 mroute static

Use this command to display the static IPv6 multicast routing information.

show ipv6 mroute static

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

The following example displays the static IPv6 multicast routing information.

Configuration Examples

```
QTECH#show ipv6 mroute static
Mroute: 2233::/64, RPF neighbor: 3333::3333 Protocol: ,
distance: 0
```

2.14. show ipv6 mvif

Use this command to display the basic information of the multicast interface.

show ipv6 mvif { *interface-type interface-number* }

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and number

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

The following example displays the basic information of the multicast interface of svil.

```
QTECH#show ipv6 mvif Interface   Mif Owner    Uptime
Idx Module
Register     0      03d03h09m
VLAN 1 1  PIMSMV6    03d03h09m
```

Configuration Examples

2.15. show ipv6 rpf

Use this command to display the RPF information of the specified source IPv6 address.

show ipv6 rpf *v6source-address*

Parameter Description

Parameter	Description
v6source-address	Specified source IPv6 address

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

The following example displays the information of the RPF to 2222::3333:

```
QTECH# show ipv6 rpf 2222::3333 RPF interface:
 GigabitEthernet 0/1 RPF neighbor: ::
 RPF route: 2222::/64
 RPF type: unicast (connected) RPF recursion
 count: 0
 Doing distance-preferred lookups across tables Distance: 0
 Metric: 0
```

Configuration Examples

2.16. show msf6 msc

Use this command to display entries of the IPv6 routing multicast data stream exchange table.

show msf6 msc [*v6source-address*] [*v6group-address*] [*vlan-id*]

Parameter Description

Parameter	Description
v6group-address	IPv6 address of a multicast group
v6source-address	IPv6 address of a multicast source
vlan-id	VLAN ID of the inbound interface of the entries If the value is greater than 4096, the interface is a routing interface.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

This command is used to display entries of the IPv6 routing multicast data stream exchange table.

The three parameters are all optional.

If only the source address is specified and set to s1, msc entries of this source address will be displayed.

If the source address is set to s1 and the group address is set to g1, msc entries of this source address and group address will be displayed.

If the source address is set to s1, the group address is set to g1, and the VLAN ID is set to v1, then msc entries that meet these three conditions will be displayed.

You must specify these three parameters in sequence. That is, you must specify the current parameter before specifying the next.

Configuration Examples

The following example displays entries of the IPv6 routing multicast data

exchange table of source address 2000::1:

```
QTECH# show msf6 msc 2000::1 Multicast
Switching Cache Table
(2000::1, FF55::1, 1), SYNC, MTU:0, 1 OIFs
 VLAN 4094(8190): 1 OPORTs, REQ: DONE OPORT 6, MLD-
SNP, REQ: DONE
```

Field	Description
2000::1	Source address of entries
FF55::1	Group address of entries
1	VLAN ID of the inbound interface of the entries
SYNC	Indicates that the entries have been synchronized to the bottom-layer hardware.
MTU	MTU value of the entries
OIFs	Number of 3-layer interfaces of the entries
VLAN	Indicates a 3-layer outbound interface VLAN xxx (yyy). If the 3-layer interface is an
4094(8190)	SVI interface, the value of xxx is the VLAN VID of the SVI, and the value of yyy is the VLAN vid+4096. If the 3-layer interface is a routing interface, the value of xxx is the IFINDEX of the interface+4096, and the value of yyy is the IFINDEX. This facilitates the index management of all 3-layer interfaces.
1 OPORTs	Number of 2-layer interfaces owned by this 3-layer exit oif
REQ: DONE	Indicates that the oif has been set to the bottom-layer hardware. The value may be: Waiting to be added. Usually it is waiting for a data stream to be triggered. DEL: Being deleted. DONE: Synchronized to the hardware.
OPORT 6	Indicates that the oif has a 2-layer interface with the interface number of 6.
MLD-SNP	Indicates that the interface is created based on MLD SNOOPING. Alternatively, the value may be one of the following options: ROUTER: Indicates that the interface is created based on the 3-layer protocol. INHERIT_FM_MLD_SNP: Indicates that the interface is created based on the MLD SNOOPING protocol inherited from other entries.

REQ: DONE	Indicates that the interface has been set to the bottom-layer hardware. The value may be: ADD: Waiting to be added. Usually it is waiting for a data stream to be triggered. DEL: Being deleted. DONE: Synchronized to the hardware.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.17. show msf6 nsf

Use this command to display the multicast non-stop forwarding configuration.

show msf6 nsf

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the multicast non-stop forwarding configuration.

```
QTECH# show msf6 nsf Multicast HA
Parameters
++ protocol convergence timeout  120 secs
flow leak interval       20 secs
```

Related Commands

Platform Description

Command	Description
msf6 nsf	Multicast non-stop forwarding

N/A

3.1. clear ip igmp group

Use this command to clear dynamic group member information obtained from the response messages in the IGMP buffer.

clear ip igmp group [*group-address* [*interface-type interface-number*]]

Parameter Description

Parameter	Description
group-address	32-bit multicast group IP address
interface-type	Interface type
interface-number	Interface number

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

The IGMP buffer includes a list that contains the multicast groups that the hosts in the direct subnet join. If the device joins a group, this group will be included in this list. To delete all the entries from the IGMP buffer, use the **clear ip igmp group** command without parameters.

Configuration Examples

Related Commands

Platform Description

The following example clears all group entries.

```
QTECH# clear ip igmp group
```

Command	

	Description
show ip igmp groups	N/A
show ip igmp interface	N/A

N/A

3.2. clear ip igmp interface

Use this command to clear the IGMP entry for the interface.

clear ip igmp interface *interface-type interface-number*

Parameter Description

Parameter	Description
interface-type	Interface type
interface-number	Interface number

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to clear the information on the interface that is generated when IGMP is configured. The information includes the number of report/leave packets, and group members on interfaces.

Configuration Examples

Command	Description
N/A	N/A

Related Commands

The following example clears the IGMP entry for the interface.

```
QTECH# clear ip igmp interface gi 0/1
```

Platform Description

N/

3.3. ip igmp access-group

Use this command to control a multicast group on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp access-group ***access-list*** no ip igmp access-group default ip igmp access-group

Parameter Description

Parameter	Description
access-list	Name of access control list in the range from 1 to 199, 1,300 to 2,699, or characters.

Defaults

This command is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

You can add several multicast groups into the specific interfaces of the host in a subnet. These multicast groups can be controlled using **ip igmp access-group**.

extended ACL is associated. If the IGMP report information received is (S1, S2, S3…Sn, G), the corresponding ACL will be used by this command to the (0, G) for the matching check. In order to use this command normally, the (0, G) must be configured explicitly for the extended ACL so as to implement the normal filtering of (S1, S2, S3…Sn, G).

Configuration Examples

The following example adds the interface Ethernet 0/1 to the group 225.2.2.2.

```
QTECH# configure terminal
QTECH(config)# access-list 1 permit 225.2.2.2 0.0.0.0 QTECH(config)#
interface ethernet 0/1
```

QTECH(config-if-Ethernet 0/1)# ip igmp access-group 1The following example associates the group control list with the extended ACL on the interface Eth 0/1 which only processes the igmp protocol packets with source address 1.1.1.1 and group address 233.3.3.3.

```
QTECH# configure terminal
QTECH(config)# ip access-list extended ext_acl
QTECH(config-ext-nacl)# permit ip host 1.1.1.1 host 233.3.3.3 QTECH(config)# interface
ethernet 0/1
QTECH(config-if-Ethernet 0/1)# ip igmp access-group ext_acl
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.4. ip igmp enforce-router-alert

Use this command to receive IGMP packets with **router-alert** option , and discard those without the option.

ip igmp enforce-router-alert

Use the **no** form of this command to receive all IGMP packets.

no ip igmp enforce-router-alert

Use the **default** form of this command to restore the default setting.

default ip igmp enforce-router-alert

Parameter Description

Parameter	Description
-	-

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuratio n Examples

The following example receives IGMP packets with **router-alert** option.

```
QTECH# configure terminal
QTECH(config)#ip igmp enforce-router-alert
```

Platform Description

N/A

3.5. ip igmp enforce-source-subnet

Use this command to receive only the IGMP report packet containing the source address in the same network segment as the port.

ip igmp enforce-source-subnet

Use the **no** form of this command to restore the default setting.

no ip igmp enforce-source-subnet

Use the **default** form of this command to restore the default setting.

default ip igmp enforce-source-subnet

Parameter Description

Parameter	Description
-	-

Defaults

The source IP address is not checked by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuratio n Examples

The following example receives only the IGMP report packet containing the source address in the same network segment as the port.

```
QTECH# configure terminal
QTECH(config)# ip igmp enforce-source-subnet
```

Platform Description

N/A

3.6. ip igmp immediate-leave group-list

In the IGMPversion2 and IGMPversion3 versions, use this command to shorten the delay of leaving a group. This command is used when a single receiving host is connected to a single interface.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp immediate-leave group-list *access-list*

no ip igmp immediate-leave default ip igmp immediate-leave

Parameter Description

Parameter	Description
access-list	Name of access control list in the range from 1 to 199, 1,300 to 2,699, or characters.

Defaults
This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

If this command is not configured, the device will send a particular group query message upon receiving the leaving message from the interface. When the host response is timeout, the device stops forwarding packets to this interface. The length of timeout depends on the query interval of the last member and IGMP robustness variable. The default value is 2s.

If this command is configured, the device does not send a particular group query message upon receiving the leaving message from the interface. Instead, it directly removes this interface from the IGMP buffer and notifies the IGMP protocol. This will shorten the time significantly.

Configuration Examples

The following example provides the immediate leaving function for some multicast groups. Certainly, you must make sure each interface of these multicast groups have one group member only.

```
QTECH# configure terminal
QTECH(config)# access-list 1 permit 225.192.20.0 0.0.0.255 QTECH(config)#
interface ethernet 0/1
QTECH(config-if-Ethernet 0/1)# ip igmp immediate-leave group-list 1
```

```
QTECH(config-if-Ethernet 0/1)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform
N/A

Description

3.7. ip igmp join-group

Use this command to configure the interface of the switch with host activities and adds it to a multicast group, so that the sub-switch can learn the corresponding group information. You can use this command to add an interface to a group.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp join-group *group-address*

no ip igmp join-group *group-address*

default ip igmp join-group *group-address*

Parameter Description

Parameter	Description
group-address	Multicast group IP address

Defaults
This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

This command enables the host activities for the IGMP interface. When the host function is enabled, the interface can initiate the report message and respond to the query message.

If the IGMP function is enabled on the interface, the interface can initiate the report message, so that the interface can learn the configured group members.

You can use this command to add an interface to a group.

Configuration Examples

The following example adds a host group member manually.

```
QTECH# configure terminal QTECH(config)#
interface fast 0/1
QTECH(config-if-Ethernet 0/1)# ip igmp join-group 233.3.3.3
QTECH(config-if-Ethernet 0/1)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.8. ip igmp last-member-query-count

Use this command to configure the value of **last-member-query-count**.

Parameter Description

Use the **no** or **default** form of this command to restore the default setting.

ip igmp last-member-query-count number no ip igmp last-member-query-count default ip igmp last-member-query-count

Parameter	Description
number	Value of the last member query count in the range from 2 to 7.

Defaults

The default is 2.

Command Mode

Interface configuration mode

Usage Guide

This command only supports IGMPv2 and IGMPv3.

When the interface of the device receives an IGMPv2 group leaving message, the device waits for duration of query interval multiplying **last-member-query-count** time. The device will delete information about this group member if no group member report is received within the waiting time.

The waiting time = last-member-query-interval * last-member-query-count + 1/2 * query-max-response-time

Configuration Examples

The following example sets the value of last member query count to 3.

```
QTECH# configure terminal QTECH(config)# interface
ethernet 0
QTECH(config-if-Ethernet 0/1)# ip igmp last-member-query-count 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.9. ip igmp last-member-query-interval

Use this command to set the time interval of sending the group query message. Use the **no** or **default** form of this command to restore the default setting.

ip igmp last-member-query-interval ***interval*** no ip igmp last-member-query-interval default ip igmp last-member-query-interval

Parameter Description

Parameter	**Description**
interval	The interval sending the group query message in the range from1 to
	255 in the unit of 0.1 second.

Defaults

The default is 10 (1 second).

Command Mode

Interface configuration mode

Usage Guide

This command only supports IGMPv2 and IGMPv3.

When the interface of the device receives an IGMPv2 group leaving message, the device waits for duration of query interval multiplying **last-member-query-count** time. The device will delete information about this group member if no group member report is received within the waiting time.

The waiting time = last-member-query-interval * last-member-query-count + 1/2 * query-max-response-time

Configuration Examples

The following example sets the interval of sending the group query message to 20 seconds.

```
QTECH# configure terminal QTECH(config)#
interface eth 0
QTECH(config-if-Ethernet 0/1)# ip igmp last-member-query-interval 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.10. ip igmp limit

Use this command to globally set the maximum number of IGMP group records. Use the **no** or **default** form of this command to restore the default setting.

ip igmp limit *number* [**except** *access-list*]

no ip igmp limit default ip igmp limit

Parameter Description

Parameter	Description
number	Maximum number of IGMP states, depending on devices
except *access-list*	Name of access control list in the range from 1 to 199, 1,300 to 2,699, or characters.

Defaults

Global: 65,536 Interface:1,0124

Command Mode

Global configuration mode/Interface configuration mode

Usage Guide

Use this command to configure the maximum number of IGMP group records globally or on interfaces. The messages of the members exceeding the threshold will not be saved in the IGMP buffer and will not be forwarded. The messages of the members will be ignored if they exceed the interface or global configuration. If the configured value in global configuration mode is less than that in interface configuration mode, take the former.

Configuration Examples

The following example sets the maximum number to 400 globally and to 300

on interfaces except ACL 1.

```
QTECH# configure terminal
QTECH(config)# ip igmp limit 400 except acl1 QTECH(config)#
interface eth 0/1
QTECH(config-if-Ethernet 0/1)# ip igmp limit 300 except acl1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.11. ip igmp mroute-proxy

Use this command to configure an interface as an mroute-proxy interface that can transmit messages to its uplink ports.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp mroute-proxy *interface-type interface-number*

no ip igmp mroute-proxy default ip igmp mroute-proxy

Parameter Description

Parameter	Description
interface-type *interface-number*	Name of the relevant uplink interface

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Use the **ip igmp proxy-service** command to set the uplink interface as the **proxy-service** interface.

Use the **ip igmp mroute-proxy** command to set the downlink interface as the **mroute-proxy**

interface.

IGMP query packets are forwarded from the **proxy-service** interface to the **mroute-proxy** interface. IGMP report packets are forward reversely.

Configuration Examples

The following example configures E0/1 as **proxy-service** E0/2 as **mroute-proxy**.

```
QTECH(config)# interface eth 0/1
QTECH(config-if-Ethernet 0/1)# ip igmp proxy-service QTECH(config-
if-Ethernet 0/1)# exit
QTECH(config)# interface eth 0/2
QTECH(config-if-Ethernet 0/2)# ip igmp mroute-proxy
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.12. ip igmp proxy-service

Use this command to enable the service function of all downlink **mroute-proxy** ports.

If you run this command on an interface, the interface becomes the uplink port of the corresponding **mroute-proxy** that associates its downlink ports and maintains the group information reported by the downlink ports.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp proxy-service

no ip igmp proxy-service default ip igmp proxy-service

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Interface configuration mode

Usage Guide

Use the **ip igmp proxy-service** command to set the uplink interface as the **proxy-service** interface.

Use the **ip igmp mroute-proxy** command to set the downlink interface as the **mroute-proxy**

interface.

The command can configure at most 32 proxy-service ports. The number of interface with IGMP Proxy enabled is limited by the supported multicast interface number. When receiving a query message, the **proxy-service** port responds according to the IGMP group member information maintained by the port itself. The member information maintained by the **proxy-service** port is

collected from the interface configured with **mroute-proxy**. Therefore, if a port is configured with proxy-service, the port performs the host activities, but not the device activities.

If **switch port** operation is performed on an interface with proxy-service command configured, the **ip igmp mroute-proxy interface** command configured on the associated downlink ports is automatically deleted.

Configuration Examples

The following example configures E0/1 as **proxy-service** and E0/2 as **mroute-prox**

```
QTECH(config)# interface eth 0/1
QTECH(config-if-Ethernet 0/1)# ip igmp proxy-service QTECH(config-
if-Ethernet 0/1)# exit
QTECH(config)# interface eth 0/2
QTECH(config-if-Ethernet 0/2)# ip igmp mroute-proxy
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.13. ip igmp query-interval

Use this command to configure the query interval of an ordinary member. Use the **no** or **default** form of this command to restore the default setting. **ip igmp query-interval** *seconds*

no ip igmp query-interval default ip igmp query-interval

Parameter Description

Parameter	Description
seconds	Query interval of ordinary member, in the range is from 1 to 18,000 in the unit of seconds.

Defaults
The default is 125 seconds.

Command Mode

Interface configuration mode

Usage Guide

Configuration Examples

The following example configures the query interval of ordinary member to

120 seconds on the interface Ethernet 0.

```
QTECH(config-if)# ip igmp query-interval 120
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.14. ip igmp query-max-response-time

Use this command to configure the maximum response interval.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp query-max-response-time ***seconds*** no ip igmp query-max-response-time default ip igmp query-max-response-time

Parameter Description

Parameter	Description
seconds	The maximum response interval, in the range from 1 to 25 seconds

Defaults

The default is 10 seconds.

Command Mode

Interface configuration mode

Usage Guide

This command controls the interval for the respondent to respond the query message before the device deletes the group information.

Configuration Examples

The following example configures the maximum response interval to 20 seconds on the interface Ethernet 0.

```
QTECH(config-if-Ethernet 0/1)# ip igmp query-max-response-time 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.15. ip igmp query-timeout

Use this command to configure the time the device waits before it takes over as the querier. Use the **no** or **default** form of this command to restore the default setting.

Parameter Description

ip igmp query-timeout *seconds* no ip igmp query-timeout default

ip igmp query-timeout

Parameter	Description
seconds	Time the device waits before it takes over as the querier, in the range from 60 to 300 in the unit of seconds.

Defaults

The default is 255 seconds.

Command Mode

Interface configuration mode

Usage Guide

This device becomes the querier if no query packet is received in this duration.

Configuration Examples

The following example configures the time the device waits before it takes over

as the querier to 200 s seconds on the interface Ethernet 0/1.

```
QTECH(config)# interface ethernet 0/1
QTECH(config-if-Ethernet 0/1)# ip igmp query-timeout 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.16. ip igmp robustness-variable

Use this command to change the value of the robustness variable.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp robustness-variable ***number*** no ip igmp robustness-variable default ip igmp robustness-variable

Parameter Description

Parameter	Description
number	The value of robustness variable, in the range from 2 to 7

Defaults
The default is 2.

Command Mode

Interface configuration mode

Usage Guide
N/A

Configuration Examples

The following example sets the value of robustness variable to 3.

```
QTECH(config)# interface ethernet 0/1
QTECH(config-if-Ethernet 0/1)# ip igmp robustness-variable 3
```

Related Commands

Command	Description

N/A	N/A

Platform Description

N/A

3.17. ip igmp send-router-alert

Use this command to send IGMP report packets with the Router Alert option. Use the **no** or **default** form of this command to restore the default setting.

ip igmp send-router-alert

no ip igmp send -router-alert default ip igmp send -router-alert

Parameter Description

Parameter	Description
-	-

Defaults
The Router Alert option is not carried in IGMP packets by default.

Command Mode

Global configuration mode

Usage Guide

N.A

Configuration Examples

The following example sends IGMP report packets with the Router Alert option.

```
QTECH# configure terminal
QTECH(config)# ip igmp send-router-alert
```

Platform Description

N/A

3.18. ip igmp ssm-map enable

Use this command to enable the **igmp ssm-map** function in the global configuration mode. Use the **no** form of this command to restore the default setting.

ip igmp ssm-map enable

no ip igmp ssm-map enable default ip igmp ssm-map enable

Parameter Description

Parameter	Description
-	-

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

If this command is configured, the dynamically learned group information is added forcibly to the associated source record. This command is usually used together with the **ip igmp ssm-map static** command.

Configuration Examples

The following example enables the **igmp ssm-map** function in the global configuration mode.

```
QTECH(config)# ip igmp ssm-map enable
QTECH(config)# ip igmp ssm-map static 11 192.168.2.2.
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.19. ip igmp ssm-map static

Use this command to map the static **ssm-map** source IP address to the group records. Use the **no** or **default** form of this command to restore the default setting.

ip igmp ssm-map static *access-list source-address*

no ip igmp ssm-map static *access-list source-address*

default ip igmp ssm-map enable *access-list source-address*

Parameter Description

Parameter	Description
access-list	ACL name in the range 1 to 99, 1,300 to 1,999 or characters.
source-address	Unicast address mapped to the group record.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is used together with the **ip igmp ssm-map enable** and **ip igmp ssm-map static** command. After configuration, the port maps the corresponding source IP address to all received messages below **v3**.

Configuration Examples

The following example maps the source address 192.168.2.2 to all group records permitted by ACL 11.

```
QTECH(config)# ip igmp ssm-map enable
QTECH(config)# ip igmp ssm-map static 11 192.168.2.2.
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.20. ip igmp static-group

Use this command to directly add an interface to a group.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp static-group *group-address*

no ip igmp static-group *group-address*

default ip igmp static-group *group-address*

Parameter Description

Parameter	Description
group-address	Multicast group IP address

Defaults

The switch is not added to a multicast group by default.

Command Mode

Interface configuration mode

Usage Guide

This command directly adds an interface to a multicast group. The difference from **join-group** is that it directly adds an interface to the group without interacting with a report message.

You can use this command to add an interface to a group.

The added interfaces by this command can only be deleted by using the **no ip igmp static-group** command.

Configuration Examples

The following example adds a host group member.

```
QTECH# configure terminal QTECH(config)# interface
ethernet 0/1
QTECH(config-if-Ethernet 0/1)# ip igmp static-group 236.6.6.6
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.21. ip igmp version

Use this command to set the version number of IGMP to be used on the interface. Use the **no** or **default** form of this command to restore the default setting.

ip igmp version **{** 1 **|** 2 **|** 3 **}** no ip igmp version default ip igmp version

Parameter Description

Parameter	Description
1	IGMP v1
2	IGMP v2
3	IGMP v3

Defaults

The default is IGMPv2.

Command Mode

Interface configuration mode

Usage Guide

Use this command to globally configure the IGMP version. It should be noted that IGMP will reset after configuration.

Configuration Examples

The following example sets the version number to 3.

```
QTECH# configure terminal QTECH(config)# interface
ethernet 0/1
QTECH(config-if-Ethernet 0/1)# ip igmp version 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.22. show ip igmp groups

Use this command to display the groups directly connected to the device and the group information learnt from IGMP.

show ip igmp groups [*interface-type interface-number*] [*group-address*] [**detail**]

Parameter Description

Parameter	Description
group-address	32-bit multicast group IP address, namely Category D address. 8 bits are in one group in decimal form. Groups are separated with dots.
interface-type	Interface type
interface-number	Interface number
detail	Displays the detailed information

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command without any parameters to display group address, interface type, and information about all the multicast groups directly connected to the interface. Information about a specific group is displayed if a group address is added to the command.

Configuration Examples

The following example displays information about all the groups.

```
QTECH# show ip igmp groups
IGMP Connected Group Membership
Group Address Interface    Uptime Expires    Last Reporter


224.0.1.1      eth2    00:00:09     00:04:17     10.10.0.82
224.0.1.24     eth2    00:00:06     00:04:14     10.10.0.84
224.0.1.40     eth2    00:00:09     00:04:15     10.10.0.91
224.0.1.60     eth2    00:00:05     00:04:15     10.10.0.7
239.255.255.250 eth2   00:00:12    00:04:15    10.10.0.228
```

```
239.255.255.254 eth2   00:00:08    00:04:13    10.10.0.84
```

```
QTECH# show ip igmp groups 224.1.1.1 detail Interface
                 : eth1
Group: 224.1.1.1
Uptime: 00:00:42 Group mode:
Include
Last reporter: 192.168.50.111
```

The following example displays detailed information about a specific group.

```
TIB-A Count: 2
TIB-B Count: 0
Group source list: (R - Remote, M - SSM Mapping) Source Address
Uptime v3 Exp Fwd Flags 192.168.55.55 00:00:42 00:03:38 Yes R
192.168.55.66 00:00:42 00:03:38 Yes R
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.23. show ip igmp interface

Use this command to display the information of this interface.

show ip igmp interface [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type	Interface type.
interface-number	Interface number.

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

Run this command without any parameter, and all interface information is displayed by default.

Configuration Examples

The following example displays the information of all the interfaces.

```
QTECH# show ip igmp interface Interface vlan
1(Index 4294967295)
IGMP Active, Non-Querier, Version 3 (default) IGMP querying
router is 0.0.0.0
IGMP query interval is 125 seconds
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.24. show ip igmp ssm-mapping

Use this command to display the **ssm-map** information of the IGMP configuration.

show ip igmp ssm-mapping [*group-address*]

Parameter Description

Parameter	Description
group-address	Source address to be mapped

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Run this command without any parameter, and all SSM-MAP information is displayed.

Configuration Examples

The following example displays the **ssm-map** configuration information.

```
QTECH#show ip igmp ssm-mapping 233.3.3.3 Group address:
233.3.3.3
Database    : Static Source list  :
192.3.3.3
            : 3.3.3.3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.1. clear ipv6 mld group

Use this command to clear the dynamic group member learned by MLD protocol.

clear ipv6 mld group [*group-address*] [*interface-type interface-number*]

Parameter Description

Parameter	Description
group-address	IPv6 multicast group address with 128 bits
interface-type	The associated interface type
interface-number	The associated interface number

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

MLD maintains a list of the multicast groups to be added to the host in the directly-connected sub-net. Use the **clear ipv6 mld group** command to remove all dynamic group member record from the MLD group member list.

Configuration Examples

Related Commands

Platform Description

The following example clears all group records.

```
QTECH# clear ipv6 mld group
```

The following example clears one group record.

```
QTECH# clear ipv6 mld group ff1e::100
```

The following example s clears the record on a specified interface.

```
QTECH# clear ipv6 mld group ff1e::100 interfa fa0/1
```

Command	Description
show ipv6 mld groups	N/A
show ipv6 mld interface	N/A

N/A

4.2. clear ipv6 mld interface

Use this command to clear all MLD statistical information and the group member records on the interface.

clear ipv6 mld interface *interface-type interface-number*

Parameter Description

Parameter	Description
interface-type	The interface type
interface-number	The interface ID

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to clear all group information and some packet statistical information learned by LDP on the interface. Those packet statistical information include the number of the received report packets, the number of the done packets and the the number of the group members on the interface.

Configuration Examples

Related Commands

Platform Description

The following example clears all MLD statistical information and the group member records on the interface.

```
QTECH# clear ipv6 mld interface fa 1/1
```

Command	Description
N/A	N/A

N/A

4.3. ipv6 mld access-group

Use this command to filter the specific requested group on the interface. Only the report packets in accordance with the corresponding ACL are allowed to be processed.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld access-group ***access-list*** no ipv6 mld access-group default ipv6 mld access-group

Parameter Description

Parameter	Description
access-list	The IPv6 ACL name

Defaults
This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Use this command to filter some groups on the interface and associate with the corresponding ACLs. The correspondent ACL deny report packets will be discarded. This command supports the extended ACL and the source record information of the MLDv2 packets can be filtered.

The multicast group access control command is associated with the extended ACL. When the received MLD report mesage is (S1,S2,S3…Sn,G), use this command to match and check the (0,G) message using the corresponding ACL. To this end, a (0,G) must be configured for the extended ACL to filter the (S1,S2,S3…Sn,G).

Configuration Examples

The following example enables the group information carried in the report packets to be in accordance with acl for the normal handling on the interface Eth0/1.

```
QTECH(config)#ipv6 access-list acl
QTECH(config-ipv6-acl)#permit ipv6 ::/64 ff66::100/64 QTECH(config-ipv6-
acl)#permit ipv6 2222::3333/64 ff66::100/64 QTECH(config)# interface ethernet
0/1
QTECH(config-if-Ethernet 0/1-Ethernet 0/1)# ipv6 mld access-group acl
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.4. ipv6 mld immediate-leave group-list

Use this command to set the immediate-leave mechanism. With this command configured, the group within the range of group-list, will not send the query packet for the specific group and will remove this group from the group member list immediately after receiving the corresponding done packets. This function is used in the condition that there is only one multicast source that receives the host request on an interface. Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld immediate-leave group-list ***access-list*** no ipv6 mld immediate-leave group-list default ipv6 mld immediate-leave group-list

Parameter Description

Parameter	Description
access-list	The IPv6 ACL name

Defaults
This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Without this command configured, when the device receives the MLD leave packets, the request packets for the specific groups will be sent. If there is still no host reply within the response time, the device will remove the corresponding group record from the group member list. The timeout interval is determined by the last member query interval and the MLD robustness variable, and the default value is 2 seconds.

With this command configured, when the device receives the MLD leave packets, it will not send the request packets for the specific groups, but remove the group information immediately, which reduces the leave delay greatly in the condion that there is only one host connecting to the interface.

Configuration Examples

The following example configures the immediate-leave function.

```
QTECH# configure terminal QTECH(config)#ipv6
access-list acl
QTECH(config-ipv6-acl)#permit ipv6 2222::3333/64 ff66::100/64 QTECH(config)#
interface ethernet 0/1
QTECH(config-if-Ethernet 0/1-Ethernet 0/1)# ipv6 mld immediate-leave
group-list acl
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.5. ipv6 mld join-group

Use this command to configure the host action for the switch interface and add the related multicast group to the interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld join-group *group-address*

no ipv6 mld join-group *group-address*

default ipv6 mld join-group group-address

Parameter Description

Parameter	Description

group-address	The IPv6 non-management multicast group address, which cannot start with 0xFF*1, 0xFF*2, and 0xFF3*

Defaults

The interface is not added to any group by default.

Command Mode

Interface configuration mode

Usage Guide

Use this command to enable the MLD host action on the interface. The interface can not only send the packets initiatively, but also reply to the query packets.

Use this command if it is necessary to join a group member to the interface.

Configuration Examples

The following example adds the host group member:

```
QTECH# configure terminal QTECH(config)# interface
ethernet 0/1
QTECH(config-if-Ethernet 0/1-Ethernet 0/1)# ipv6 mld join-group ff55::100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.6. ipv6 mld last-member-query-count

Use this command to set the last-member-query-count number.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld last-member-query-count ***number*** no ipv6 mld last-member-query-count default ipv6 mld last-member-query-count

Parameter Description

Parameter	Description

number	The last member query count number. The valid range is 2 to 7.

Defaults
The default is 2.

Command Mode

Interface configuration mode

Usage Guide

With the MLD leave packets received on the interface, if there is no group reply within the timeout interval, this group will be removed from the MLD group member list on the interface. The timeout interval is the query interval for the specific group (multiplied by the value of **mld**

last-member-query-count) plus half the reply time.

Configuration Examples

The following example sets the last-member-query-count number to 3.

```
QTECH# configure terminal QTECH(config)# interface
ethernet 0/1
QTECH(config-if-Ethernet 0/1)# ipv6 mld last-member-query-count 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.7. ipv6 mld last-member-query-interval

Use this command to set the time interval of sending the query packets to the specific group. Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld last-member-query-interval ***interval*** no ipv6 mld ast-member-query-interval default ipv6 mld last-member-query-interval

Parameter Description

Parameter	**Description**

interval	The valid range is 1-255 in the unit of 0.1 seconds.

Defaults
The default is 10 seconds.

Command Mode

Interface configuration mode

Usage Guide

With the MLD leave packets received on the interface, if there is no group reply within the timeout interval, this group will be removed from the MLD group member list on the interface. The timeout interval is the query interval for the specific group(multiplied by the value of **mld**

last-member-query-count) plus half the reply time.

Configuration Examples

The following example sets the mld last-member-query-interval to 2 seconds.

```
QTECH# configure terminal QTECH(config)# interface
ethernet 0/1
QTECH(config-if-Ethernet 0/1)# ipv6 mld last-member-query-interval 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.8. ipv6 mld limit

Use this command to enable to learn the max-number of the group member through the MLD

protocol.

Parameter Description

Parameter	Description

number	The maximum number of the group member learned by the MLD
except *access-list*	(Optional) The ACL beyond the configured mld limit

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld limit *number* [**except** *access-list*]

no ipv6 mld limit *number* [**except** *access-list*]

default ipv6 mld limit *number* [**except** *access-list*]

Defaults

Interface: 1,024

Global: 65,536

Command Mode

Interface configuration mode/Global configuration mode

Usage Guide

Use this command to set the max-number of the group members learned through the MLD in the global configuration mode. If the group member number has exceeded the limit, the received report packets later will be discarded and fail to form the group record.

If the except list has also been set at the same time, the group member packets, including the packets in the access-list, will be free from the member number limit.

This command can also be used in the interface configuration mode. The configurations in two different configuration modes are independent. If the number limit in the global configuration mode is lower than the one in the interface configuration mode, the former configuration takes precedence.

Configuration Examples

The following example sets the MLD limit to 400, but the configured ACL can still learn.

```
QTECH(config-if)# ipv6 mld limit 300 except acl
QTECH# configure terminal
QTECH(config)# ipv6 mld limit 400 except acl1 QTECH(config)#
interface eth 0/1
QTECH(config-if-Ethernet 0/1)# ipv6 mld limit 300 except acl1
```

Related Commands

Command	Description

N/A	N/A

Platform Description

N/A

4.9. ipv6 mld mroute-proxy

Use this command to enable the interface to forward the packets to the correspondent connected interface.

Parameter Description

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld mroute-proxy *interface-type interface-number*

no ipv6 mld mroute-proxy default ipv6 mld mroute-proxy

Parameter	Description
interface-type interface-number	The correspondent connected interface

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Use the **ipv6 mld proxy-service** command to configure the uplink interface as **proxyservice** one. Use the **ipv6 mld mroute-proxy** command to configure the downlink interface as **mroute-proxy** one. After the connected interface has been configured as the proxy-service interface, it can forward the MLD packets sent from other members.

Configuration Examples

The following example sets the interface as the mroute-proxy interface and enables multicast proxy.

```
QTECH(config)# interface eth 0/1
QTECH(config-if-Ethernet 0/1)# ipv6 mld proxy-service QTECH(config-
if-Ethernet 0/1)# exit
QTECH(config)# interface eth 0/2
QTECH(config-if-Ethernet 0/2)# ipv6 mld mroute-proxy eth 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.10. ipv6 mld proxy-service

Use this command to enable the proxy-service function for the interface connected with the mroute-proxy interface in the downward direction. After configuring this command, the interface

becomes the one connected with the mroute-proxy in the upward direction, and associates with and maintains the group information from the interfaces in the downward direction. Use the **no** or **default** form of this command to disable the default setting.

ipv6 mld proxy-service no ipv6 mld proxy-service

default ipv6 mld proxy-service

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Interface configuration mode

Usage Guide

Use the **ipv6 mld proxy-service** command to configure the uplink interface as **proxy-service** one. Use the **ipv6 mld mroute-proxy** command to configure the downlink interface as **mroute-proxy** one. The configurable max-number limit is 32. The number of the interfaces with MLD Proxy enabled is limited by the number multicast interfaces supported device. After receiving the query packet, the proxy-service interface replies according to the member information, which are collected from the mroute-proxy interface and maintained by the proxy-service interface itself. With proxy-service configured, this interface owns the host action rather than the router action.

The **ipv6 mld mroute-proxy interface** command configuration on the associated interface in the downward direction is removed automatically if the switchport operation is performed on the interfaces.

Configuration Examples

The following example sets the interface proxy-service and enables multicast proxy.

```
QTECH(config)# interface eth 0/1
QTECH(config-if-Ethernet 0/1)# ipv6 mld proxy-service QTECH(config-
if-Ethernet 0/1)# exit
QTECH(config)# interface eth 0/2
QTECH(config-if-Ethernet 0/1-Ethernet 0/2)# ipv6 mld mroute-proxy eth 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.11. ipv6 mld querier-timeout

Use this command to set the querier alive period.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld querier-timeout ***seconds*** no ipv6 mld querier-timeout default ipv6 mld querier-timeout

Parameter

Parameter	Description
seconds	The querier alive period, in the range from 60 to 300 in the unit of seconds.

Description

Defaults

The default is 255 seconds.

Command Mode

Interface configuration mode

Usage Guide

After the querier sends the query packet, the querier will wait to receive the query packet sent by another querier within the alive period. If no packet is received by the first querier within the alive period, then the first querier takes itself as the only querier on the network segment.

Configuration Examples

Related Commands

Platform Description

The following example sets the querier alive period to 200 seconds.

```
QTECH(config-if-Ethernet 0/1)# ipv6 mld querier-timeout200
```

Command	Description
N/A	N/A

N/A

4.12. ipv6 mld query-interval

Use this command to set the query interval for the general member.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld query-interval ***seconds*** no ipv6 mld query-interval default ipv6 mld query-interval

Parameter Description

Parameter	Description
seconds	The query interval for the general member, in the range from 1 to 18,000 in the unit of seconds.

Defaults

The default is 125 seconds.

Command Mode

Interface configuration mode

Usage Guide

Configuration

The following example sets the query-interval for the general member on the interface Ethernet 0/1.

Examples

```
QTECH(config-if-Ethernet 0/1)# ipv6 mld query-interval120
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.13. ipv6 mld query-max-response-time

Use this command to set the maximum response time.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld query-max-response-time ***seconds*** no

ipv6 mld query-max-response-time default ipv6 mld query-max-response-time

Parameter Description

Parameter	Description
seconds	The maximum response time, in the range from 1 to 25 in the unit of seconds

Defaults

The default is 10 seconds.

Command Mode

Interface configuration mode

Usage Guide

Use this command to control the maximum response time of the host after the device sends the query packets. If there is no response within the maximum response time, MLD will remove the corresponding group from the group member list.

Configuration Examples

The following example sets the maximum query response time on the interface Ethernet 0/1.

```
QTECH(config-if-Ethernet 0/1)# ipv6 mld query-max-response-time 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.14. ipv6 mld robustness-variable

Use this command to set querier robustness value.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld robustness-variable ***number*** no ipv6 mld robustness-variable default ipv6 mld robustness-variable

Parameter Description

Parameter	Description
number	Sets the querier robustness value, in the range from 2 to 7.

Defaults

The default is 2.

Command Mode

Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the querier robustness value to 3.

```
QTECH# configure terminal QTECH(config)# interface
ethernet 0/1
QTECH(config-if-Ethernet 0/1)# ipv6 mld robustness
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.15. ipv6 mld ssm-map enable

Use this command to enable the mld ssm-map function.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld ssm-map enable no ipv6 mld ssm-map enable

default ipv6 mld ssm-map enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

With this command configured, the group information dynamically learned will be added to the related source record forcibly. Usually, this command is set with the **ipv6 mld ssm-map static** command.

Configuration Examples

The following example enables the mld ssm-map function in the global configuration mode.

```
QTECH(config)# ipv6 mld ssm-map enable
QTECH(config)# ipv6 mld ssm-map static 11 4444::1234
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.16. ipv6 mld ssm-map static

Use this command to set the mld ssm-map static mapping source record in the global configuration mode.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld ssm-map static *access-list source-address*

no ipv6 mld ssm-map static *access-list source-address*

default ipv6 mld ssm-map static *access-list source-address*

Parameter Description

Parameter	Description
access-list	Sets the IPv6 ACL name.
source-address	Sets the unicast address for the group record mapping.

Defaults

There is no mapping source address by default.

Command Mode

Global configuration mode

Usage Guide

This command is used with the **ipv6 mld ssm-map enable** command.

With this command configured, the received mldv1 packets are mapped to the correspondent source record.

Configuration Examples

The following example maps all group record of the ACL name to the source address 4444::1234.

```
QTECH(config)# ipv6 mld ssm-map enable
QTECH(config)# ipv6 mld ssm-map static te 4444::1234
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.17. ipv6 mld static-group

Use this command to add an interface to a group statically.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld static-group *group-address*

no ipv6 mld static-group *group-address*

default ipv6 mld static-group *group-address*

Parameter Description

Parameter	Description
group-address	Sets the IPv6 non-management multicast group address.

Defaults

The interface is not added to any group statically.

Command Mode

Interface configuration mode

Usage Guide

Use this command to add a multicast group to the interface directly. The difference from the join-group is that the packet interaction is not necessary.

Use this command when it is necessary to add a group member to the interface. It is worth mentioning that only the **no ipv6 mld static-group** command can be used to delete the group, but not the **clear** command.

Configuration Examples

The following example adds interface Eth0/1 to group ff55::3 statically.

```
QTECH# configure terminal QTECH(config)# interface
ethernet 0/1
QTECH(config-if-Ethernet 0/1)# ipv6 mld static-group ff55::3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.18. ipv6 mld version

Use this command to set the MLD version number on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld version **{** 1 **|** 2 **}** no ipv6 mld version default ipv6 mld version

Parameter Description

Parameter	Description

{ 1 | 2 }	Sets the MLD version number.

Defaults
The default is 2.

Command Mode
Interface configuration mode

Usage Guide
Use this command to control the MLD version number.

Configuration Examples
The following example sets the MLD version 1.

```
QTECH# configure terminal QTECH(config)# interface
ethernet 0/1
QTECH(config-if-Ethernet 0/1)# ipv6 mld version 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.19. show ipv6 mld groups

Use this command to display the group connected with the switch and the group information learned from the MLD.

show ipv6 mld groups [*group-address* | *interface-type interface-number*] [**detail**]
Displays all the group information.

Defaults
N/A

Command Mode
Privileged EXEC mode/Interface configuration mode

Usage Guide

Use this command without the parameters to display the information including the group address, the interface type and the multicast group information. Use this command with a parameter to display the information on a specific group.

Configuration Examples

The following example displays all group information.

```
QTECH# show ipv6 mld groups MLD Connected
Group Membership
Group Address Interface Uptime Expires Last Reporter
ff66::1 VLAN1 00:10:57 00:02:16 fe80::2d0:f8ff:fe22:3378

QTECH# show ipv6 mld groups detail Interface: VLAN
1
Group:         ff66::1
Uptime:        00:10:26
Group mode:     Exclude (Expires: 00:02:47) Last reporter:
fe80::2d0:f8ff:fe22:3378 Source list is empty
```

The following example displays the detailed information.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.20. show ipv6 mld interface

Use this command to display the configurations on the interface.

show ipv6 mld interface [interface-type interface-number]

Parameter Description

Parameter	Description
interface-type	Sets the interface type.

interface-number	Sets the interface number.

Defaults
N/A

Command Mode
User EXEC mode/Privileged EXEC mode

Usage Guide
N/A

Configuration Examples

The following example displays the state information of all interfaces.

```
QTECH# show ipv6 mld interface Interface VLAN
2 (Index 4098)
 MLD Enabled, Inactive, Version 2 (default) MLD interface
 limit is 1024
 MLD interface has 0 group-record states MLD interface
 has 1 join-group records MLD interface has 0 static-
 group records MLD activity: 0 joins, 0 leaves
 MLD query interval is 125 seconds MLD querier
 timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 10 (1/10s) Last member
 query count is 2
 Group Membership interval is 260
 Robustness Variable is 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.21. show ipv6 mld ssm-mapping

Use this command to display the mapping information of the source address for the group record.

show ipv6 mld ssm-mapping [*group-address*]

Parameter Description

Parameter	Description
group-address	Displays the group address.

Defaults
N/A

Command Mode
User EXEC mode/Privileged EXEC mode

Usage Guide
N/A

Configuration Examples

The following example displays the state information of all interfaces.

```
QTECH# show ipv6 mld interface Interface VLAN
2 (Index 4098)
 MLD Enabled, Inactive, Version 2 (default) MLD interface
 limit is 1024
 MLD interface has 0 group-record states MLD interface
 has 1 join-group records MLD interface has 0 static-
 group records MLD activity: 0 joins, 0 leaves
 MLD query interval is 125 seconds MLD querier
 timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 10 (1/10s) Last member
 query count is 2
 Group Membership interval is 260
 Robustness Variable is 2
```

Related Commands

Command	Description
N/A	N/A

5.1. clear ip pim dense-mode track

Use this command to clear the statistics of PIM-DM packets.

clear ip pim dense-mode track

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to reconfigure the start time of the statistics and clear the PIM packet counter.

Configuration Examples

Related Commands

Platform Description

The following example clears the statistics of PIM-DM packets.

```
QTECH# clear ip pim dense-mode track
```

Command	Description
show ip pim dense-mode track	Displays the statistics of the PIM packets.

N/A

5.2. ip pim dense-mode

Use this command to enable PIM-DM on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip pim dense-mode

no ip pim dense-mode default ip pim dense-mode

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

- Before enabling the PIM-DM, enable the multicast forwarding function in the global configuration mode. Otherwise, the multicast data packet cannot be forwarded even the PIM-DM is enabled.
- Once the PIM-DM is enabled, the IGMP is enabled automatically on the interface without manual configuration.
- During the execution of this command, if the prompt "Failed to enable PIM-DM on <Interface Name>, resource temporarily unavailable, please try again" appears, re-execute this command.
- During the execution of this command, if the prompt "PIM-DM Configure failed! VIF limit exceeded in NSM!!!" appears; it indicates the allowed configured multicast interface number
- exceeds the upper limit of the multicast interfaces. In this case, if it's still necessary to enable the PIM-DM on the interface, delete the unnecessary PIM-DM, PIM-SM or DVMRP interfaces.
- It is not recommended to configure different IPv4 multicast routing protocols on different interfaces of a device.

Configuration Examples

The following example enables PIM-DM on the interface.

```
QTECH# configure terminal
QTECH(config)# interface fastethernet 0/1 QTECH(config-
if)# ip pim dense-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.3. ip pim dense-mode passive

Use this command to enable PIM-DM PASSIVE.

Use the **no** or **default** form of this command to restore the default setting.

ip pim dense-mode passive no ip pim dense-mode passive

default ip pim dense-mode passive

Parameter Description

Parameter	Description
N/A	N/A

Defaults

PIM-DM PASSIVE is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Please configure multicast route forwarding in global configuration mode before enabling PIM-DM PASSIVE.

When PIM-DM PASSIVE is enabled, IGMP is enabled on each interface automatically. Enabled with PIM-DM PASSIVE, the interface neither receives nor sends PIM packets. Instead, it forwards multicast packets. PIM-DM PASSIVE is generally configured on the device of the stub area, so as to avoid floods of PIM hello packets.

Configuration Examples

The following example enables PIM-DM PASSIVE on interface fastethernet 0/1.

```
QTECH# configure  terminal QTECH(config)# interface
fastethernet 0/1
QTECH(config-if)# ip pim dense-mode passive
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.4. ip pim dense-mode subvlan

Use this command to enable PIM-DM on the Super VLAN interface. Use the no or default form of this command is to restore the default setting.

ip pim dense-mode subvlan [all | *vid*] no ip pim dense-mode subvlan default ip pim dense-mode subvlan

Parameter Description

Parameter	Description
all	Sends PIM packets to all sub VLANs.
vid	Sends PIM packets to the specified VLAN.

Defaults

PIM-DM is disabled on the Super VLAN interface by default.

Command Mode

Interface configuration mode

Usage Guide

In general, a super VLAN includes many sub VLANs. If the PIM-DM protocol is enabled on the interfaces of the super VLAN, PIM-DM multicast packets will be replicated and sent to all sub VLANs. As a result, the traffic may exceed the device capability, causing protocol flapping. The Super VLAN

interface is disabled with PIM-DM generally. Use this command to enable PIM-DM on the Super VLAN interface to send PIM packets to all sub VLANs or the specified sub VLAN.

Configuration Examples

The following example enables PIM-DM on the Super VLAN interface and

sends PIM packets to sub VLAN 200.

```
QTECH# configure terminal QTECH(config)# interface vlan
100
QTECH(config-if-vlan 100)# ip pim dense-mode subvlan 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.5. ip pim neighbor-filter

Use this command to enable the neighbor filtering on the interface. Use the **no** or **default** form of this command is to restore the default setting.

ip pim neighbor-filter *access-list*

no ip pim neighbor-filter *access-list*

default ip pim neighbor-filter *access-list*

Parameter Description

Parameter	Description
access-list	Access control list supporting numerical ACL in the range from 1 to 99 and name ACL

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

If the neighbor filtering is set, PIM-DM will not establish the peering relationship with this neighbor or will terminate the established peering relationship with this neighbor once the neighbor is denied by the filtering access list.

Configuration Examples

The following example enables the neighbor filtering on the interface.

```
QTECH# configure terminal
QTECH(config)# interface fastethernet 0/1 QTECH(config-if)#
ip pim neighbor-filter 14
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.6. ip pim override-interval

Use this command to reconfigure the override-interval of the hello message. Use the **no** or **default** form of this command to restore the default setting. **ip pim override-interval** *interval-milliseconds*

no ip pim override-interval default ip pim override-interval

Parameter Description

Parameter	Description
interval-milliseconds	In the range from 1 to 65,535 in the unit of milliseconds

Defaults

The default is 2,500 milliseconds.

Command Mode

Interface configuration mode

Usage Guide

Configuring the override-interval is to set the pruning veto time for the interface.

Configuration Examples

The following example sets the override-interval to 3,000 milliseconds.

```
QTECH# configure terminal
QTECH(config)# interface fastethernet 0/1 QTECH(config-if)# ip
pim override-interval 3000
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.7. ip pim propagation-delay

Use this command to reconfigure the propagation-interval of the hello message. Use the **no** or **default** form of this command to restore the default setting.

ip pim propagation-delay *interval-milliseconds*

no ip pim propagation-delay

default ip pim propagation-delay

Parameter Description

Parameter	Description
interval-milliseconds	Propagation-interval of the hello message in the range from 1 to 32,767 in the unit of milliseconds

Defaults

The default is 500 milliseconds.

Command Mode

Interface configuration mode

Usage Guide

Configuring the propagation-delay is to set the transmission delay time for the interface.

Configuration Examples

The following example sets the propagation-delay to 600 milliseconds.

```
QTECH# configure  terminal QTECH(config)# interface
fastethernet 0/1
QTECH(config-if)# ip pim propagation-delay 600
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.8. ip pim query-interval

Use this command to reconfigure the interval of sending the hello message. Use the **no** or **default** form of this command to restore the default setting. **ip pim query-interval** *interval-seconds*

no ip pim query-interval default ip pim query-interval

Parameter Description

Parameter	Description
interval-seconds	Interval of sending the hello message in the range from 1 to 65,535 in the unit of seconds

Defaults

The default is 30 seconds.

Command Mode

Interface configuration mode

Usage Guide

If hello interval is set, the hello holdtime value will be updated to 3.5 times of hello interval.

Configuration Examples

The following example sets the interval of sending the hello message to 123 seconds.

```
QTECH# configure  terminal QTECH(config)# interface
fastethernet 0/1
QTECH(config-if)# ip pim query-interval 123
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.9. ip pim state-refresh disable

Use this command to prohibit the interface from processing and forwarding the PIM-DM state refresh messages.

Use the **no** or **default** form of this command to restore the default setting.

ip pim state-refresh disable no ip pim state-refresh disable

default ip pim state-refresh disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, the PIM-DM state refresh messages can be processed and forwarded.

Command Mode

Global configuration mode

Usage Guide

When the state refresh function is disabled, the PIM-DM state refresh message is not processed and forwarded. The sent Hello message does not contain the status refresh option. Consequently, the SR Cap field will not be processed when the Hello message is received.

Generally, it is not recommended to disable the status refresh function because disabling this function may converge the PIM-DM multicast forwarding tree again that has been converged, resulting in unnecessary waste of bandwidth and oscillation of multicast routing table.

Configuration Examples

The following example disables the processing of the PIM-DM state refresh message.

```
QTECH# configure terminal
QTECH(config)# ip pim state-refresh disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.10. ip pim state-refresh origination-interval

Use this command to set the interval of sending the PIM-DM state refresh message. The interval is the seconds elapsed between two state refresh messages.

Use the **no** or **default** form of this command to restore the default setting.

ip pim state-refresh origination-interval *interval-seconds*

no ip pim state-refresh origination-interval default ip pim state-refresh origination-interval

Parameter Description

Parameter	Description
interval-seconds	Interval of sending the PIM-DM update message in the range from 1 to 100 in unit of seconds

Defaults

The default is 60 seconds.

Command Mode

Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the interval of sending the PIM-DM state refresh message to 65 seconds.

```
QTECH# configure  terminal QTECH(config)# interface
fastethernet 0/1
QTECH(config-if)# ip pim state-refresh origination-interval 65
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.11. ip pim mib dense-mode

Use this command to switch the device from the PIM MIB sparse mode to the PIM MIB dense mode. Use the **no** form or **default** form of this command to switch back to the PIM MIB sparse mode.

Parameter Description

ip pim mib dense-mode no ip pim mib dense-mode

default ip pim mib dense-mode

Parameter	Description
N/A	N/A

Defaults

The device is in the PIM MIB sparse mode by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example switches the device from the PIM MIB sparse mode to the PIM MIB dense mode.

```
QTECH# configure terminal
QTECH(config)# ip pim mib dense-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.12. show ip pim dense-mode interface

Use this command to display the information about the PIM-DM interface.

show ip pim dense-mode interface [*interface-type interface-number*] [**detail**]

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and interface ID
detail	Displays details of the interface.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the information about the PIM-DM interface.

```
QTECH# show ip pim dense-mode interface Address
```

```
          Interface  VIFIndex  Ver/Mode    Nbr Mode Count
10.10.10.10 FastEthernet 0/45 3   v2/D         1
50.50.50.50 VLAN4          2      v2/D          1
```

Field	Description
Address	Primary IP address of the PIM-DM interface
Interface	Name of the PIM-DM interface
VIF Index	VIF ID (ID)
Ver/Mode	PIM version/mode
Nbr Count	Number of neighbors of the PIM-DM interface.

Related Commands

Platform Description

Command	Description
show ip pim dense-mode neighbor	Displays the information about the neighbors of the PIM-DM interface.

N/A

5.13. show ip pim dense-mode mroute

Use this command to display the information about the PIM-DM routing table.

show ip pim dense-mode mroute [*group-or-source-address* [*group-or-source-address*]] [**summary**]

Parameter Description

Parameter	Description
group-or-source-address	Group address or source address

group-or-source-address	Group address or source address. Two addresses cannot both be the group addresses or the source addresses.
summary	Displays the brief information of routing entries.

Defaults
N/A

Command Mode
Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide
N/A

Configuration Examples

The following example displays the information about the PIM-Dm routing table.

```
QTECH# show ip pim dense-mode mroute PIM-DM
Multicast Routing Table (1.1.1.111, 229.1.1.1)
  MRT lifetime expires in 205 seconds
  RPF Neighbor: 50.50.50.1, Nexthop:50.50.50.1,VLAN 4
  Upstream IF: VLAN 4
    Upstream State: Pruned, PLT:200 Assert State:
    NoInfo
  Downstream IF List: FastEthernet
    0/45:
      Downstream State: NoInfo
      Assert State: Loser, AT:170
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.14. show ip pim dense-mode neighbor

Use this command to display the information about the PIM-DM neighbors.

show ip pim dense-mode neighbor [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type *interface-number*	Interface type and interface ID

Defaults
N/A

Command Mode
Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide
N/A

Configuration Examples

The following example displays the information about the PIM-DM neighbors.

```
QTECH# show ip pim dense-mode neighbor
Neighbor-Address Interface Uptime/Expires  Ver
10.10.10.1   FastEthernet 0/45 00:19:29/00:01:21 v2
50.50.50.1    VLAN 4      00:22:09/00:01:39  v2
```

Description of fields in the results:

Field	Description
Neighbor-Address	IP address of the neighbor
Interface	Name of the interface connecting the neighbor
Uptime/Expires	Valid time and aging time of the entry
Ver	PIM version

Related Commands

Command	Description

N/A	N/A

Platform Description

N/A

5.15. show ip pim dense-mode nexthop

Use this command to display the information about the PIM-DM next hop.

show ip pim dense-mode nexthop

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the information about the PIM-Dm next hop:

```
QTECH# show ip pim dense-mode nexthop
Destination  NexthopNexthop  Nexthop   Metric Pref

           Num       Addr      Interface
1.1.1.111     1       50.50.50.1  VLAN 4     0     1
```

Field	Description
Destination	Multicast source IP address
Nexthop Num	Number of next hop
Nexthop Addr	IP address of next hop
Nexthop	Interface connecting to the of next hop

interface	
Metric	Route metric
Pref	Route priority

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.16. show ip pim dense-mode track

Use this command to display the statistics of the PIM-DM packets.

show ip pim dense-mode track

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

This command is used to display the number of sent and received PIM packets during the period from the beginning of the statistics till now. When the system starts up, it sets the start time of the statistics. The start time of the statistics is reconfigured and the PIM packet counter is cleared on calling the clear ip pim dense-mode track every time.

Configuration Examples

The following example displays the statistics of the PIM-DM packets.

```
QTECH# show ip pim dense-mode track
             PIM packet counters
Elapsed time since counters cleared: 00:04:03
                       received    sent
Valid PIMDM packets:         1           8
Hello:                       1           8
Join/Prune:                0           0
Graft:                       0           0
Graft-Ack:                   0           0
Assert:                    0           0
State-Refresh:             0           0
PIM-SM-Register:           0           0
PIM-SM-Register-Stop:      0           0
PIM-SM-BSM:                0           0
PIM-SM-C-RP-ADV:           0           0
Unknown Type:              0
Errors:
Malformed packets:         0
Bad checksums:             0
Unknown PIM version:       0
Send errors:               0
```

Related Commands

Command	Description
clear ip pim dense-mode track	Clears the statistics of the PIM packets.

Platform Description

N/A

6.1. clear ip pim sparse-mode bsr rp-set *

Use this command to clear all the RP information learnt dynamically.

clear ip pim sparse-mode bsr rp-set *

Parameter Description

Parameter	Description
-	-

Defaults
N/A

Command Mode
Privileged EXEC mode

Usage Guide
All the RP information learnt dynamically can be cleared manually.

Configuration Examples

Related Commands

Platform Description
The following example clears all the RP information learnt dynamically.

```
QTECH# clear ip pim sparse-mode bsr rp-set*
```

Command	Description
N/A	N/A

N/A

6.2. clear ip pim sparse-mode track

Use this command to reconfigure the start time of the statistics and clear the PIMv6 packet counter.

clear ip pim sparse-mode track

Parameter Description

Parameter	Description
-	-

Defaults
N/A

Command Mode
Privileged EXEC mode

Usage Guide

Configuration Examples

Related Commands

Platform Description

The following example clears the PIM packet counter.

```
QTECH# clear ip pim sparse-mode track
```

Command	Description
show ip pim sparse-mode track	Displays the PIM packet statistics.

N/A

6.3. ip pim accept-bsr list

Use this command to confine the BSR address range.

Use the **no** or **default** form this command to restore the default setting.

ip pim accept-bsr list *access-list*

no ip pim accept-bsr default ip pim accept-bsr

Parameter Description

Parameter	Description
list *access-list*	IP standard number ACL in the range of 1 to 99, 1300 to 1999 and characters

Defaults
By default, the PIMSM router receives all external BSM packets.

Command Mode
Global configuration mode

Usage Guide
Use this command to limit the range of the legal BSR.

Configuration Examples

Related Commands

Platform Description

The following example confines the BSR address range.

```
QTECH(config)# ip pim accept-bsr list 1
```

Command	Description
N/A	N/A

N/A

6.4. ip pim accept-crp list

Use this command to confine the C-RP address range and the multicast group address range it serves.

Use the **no** or **default** form of this command to restore the default setting,

ip pim accept-crp list *access-list*

no ip pim accept-crp default ip pim accept-crp

Parameter Description

Parameter	Description
list *access-list*	IP extension number ACL in the range of 1 to 99, 1300 to 1999 and characters

Defaults
By default, the elected BSR receives all external advertisements of candidate RPs.

Command Mode
Global configuration mode

Usage Guide

With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to limit the address range of the legal C-RP and the multicast group range it serves.

Configuration Examples

Related Commands

Platform Description

The following example confines the C-RP address range and the multicast group address range it serves.

```
QTECH (config)# ip pim accept-crp list 100
```

Command	Description
N/A	N/A

N/A

6.5. ip pim accept-crp-with-null-group

Use this command to receive the C-RP-ADV packets whose prefix-count is 0. Use the **no** or **default** form of this command to restore the default setting.

ip pim accept-crp-with-null-group

no ip pim accept-crp-with-null-group default ip pim accept-crp-with-null-group

Parameter Description

Parameter	Description
-	-

Defaults

By default, the BSR does not receive the C-RP-ADV packets whose prefix-count is 0.

Command Mode

Global configuration mode

Usage Guide

With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to receive the C-RP-ADV packets whose prefix-count is 0, and considers this C-RP supports all groups.

Configuration Examples

Related Commands

Platform Description

The following example receives the C-RP-ADV packets whose prefix-count is 0.

```
QTECH (config)# ip pim accept-crp-with-null-group
```

Command	Description
N/A	N/A

N/A

6.6. ip pim accept-register list

Use this command to confine the address range of the (S,G) entry of the register packets. Use the **no** or **default** form of this command to restore the default setting.

ip pim accept-register { **list** *access-list* [**route-map** *map-name*] | **route-map** *map-name* [**list**

access-list] }

no ip pim accept-register default ip pim accept-register

Parameter Description

Parameter	Description
list *access-list*	Uses an extended IP access list to define the (S, G) address range. Access control list supporting numerical ACL in the range of 100 to 199 and 2000 to 2699 and name ACL.
route-map *map-name*	Uses a route map to define the (S, G) address range.

Defaults

The (S, G) address range is not confined by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to confine the source IP address of register messages on RP.

Configuration Examples

The following example confines the source address of register packets on the RP.

```
QTECH (config)# ip pim accept-register list 100
QTECH (config)# access-list 100 permit ip 192.168.195.0 0.0.0.255 225.1.1.1
0.0.0.255
```

Related Commands

Command	Description
access-list	N/A

Platform Description

N/A

6.7. ip pim bsr-border

Use this command to configure the BSR border.

Use the **no** or **default** form of this command to restore the default setting.

ip pim bsr-border no ip pim bsr-border

default ip pim bsr-border

Parameter Description

Parameter	Description
N/A	N/A

Defaults
No BSR border is configured by default.

Command Mode

Interface configuration mode

Usage Guide

To restrain BSM flooding, configure BSR border on the interface so that the interface drops BSM packets upon receiving them and the BSM packets are not forwarded from this interface.

Configuration Examples

The following example sets the BSR border on the interface *g 0/3*

```
QTECH(config)# interface gi 0/3
QTECH(config-if- GigabitEthernet 0/3)# ip pim bsr-border
```

Related Commands

Commnd	Description
N/A	N/A

Platform Description

N/A

6.8. ip pim bsr-candidate

Use this command to configure the C-BSR.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim bsr-candidate *interface-type interface-number* [*hash-mask-length* [*priority-value*]]

no ipv6 pim bsr-candidate default ip pim bsr-candidate

Parameter Description

Parameter	Description
interface-type *interface-number*	Interface type and number
hash-mask-length	(Optional) HASK mask length configured for electing the RP in the range from 0 to 32, The default is 10.
priority-value	(Optional) Priority configured for the candidate BSR in the range from 0 to 255. The default is 64.

Defaults

No C-BSR is configured by default.

Command Mode

Global configuration mode

Usage Guide

A PIM-SM domain must contain a unique BootStrap Router (BSR). BSR is responsible for collect and issue RP information. A unique recognized BSR is elected among multiple candidate BSRs through the bootstrap packet. Before BSR information is available, C-BSRs consider them to be the BSR, and regularly send bootstrap packets using the multicast address 224.0.0.13 in the PIM-SM domain. This packet contains the address and priority of the BSR.

This command allows the device to send a bootstrap message to all the PIM neighbors using the assigned BSR address. Each neighbor compares the original BSR address with the address in the received bootstrap message. If the IP address of the received address is equal to or larger than the original address, each neighbor saves this received address as the BSR address. Otherwise, they will discard this message.

The current device considers itself to be BSR until it receives a bootstrap message from another candidate BSR and is notified that it has a higher priority value (or the same priority value, but with a larger IP address).

Configuration Examples

Related Commands

The following example configures the C-BSR.

```
QTECH(config)# ip pim bsr-candidate gi 0/3 30 192
```

Command	Description
access-list	N/A

Platform

N/A

Description

6.9. ip pim dr-priority

Use this command to set the DR priority.

Use the **no** or **default** form of this command to restore the default setting.

ip pim dr-priority *priority-value*

no ip pim dr-priority default ip pim dr-priority

Parameter Description

Parameter	Description
priority-value	The larger the value, the higher the priority is. The range is from 0 to 4,294,967,294.

Defaults

The default is 1.

Command Mode

Interface configuration mode

Usage Guide

To select a DR:

If the priority parameter of the Hello message is set for the devices in a LAN, the one of the highest priority is elected to be the DR. If several devices have the same priority, the one of the largest IP address is elected to be the DR.

If the priority parameter of the Hello message is not set for the devices in a LAN, the one of the largest IP address is elected to be the DR.

Configuration Examples

The following example sets the DR priority.

```
QTECH(config)# interface gi 0/3
QTECH(config-if-GigabitEthernet 0/3)# ip pim dr-priority 10000
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.10. ip pim ignore-rp-set-priority

Use this command to ignore the RP priority.

Use the **no** or **default** form of this command to restore the default setting.

ip pim ignore-rp-set-priority

Parameter Description

no ip pim ignore-rp-set-priority default ip pim ignore-rp-set-priority

Parameter	Description
-	-

Defaults

By default, the C-RP with higher priority is selected.

Command Mode

Global configuration mode

Usage Guide

Configuration Examples

Related Commands

Platform Description

The following example ignores the RP priority.

```
QTECH(config)# ip pim ignore-rp-set-priority
```

Command	Description
N/A	N/A

N/A

6.11. ip pim jp-timer

Use this command to set the interval to send the join/prune message. Use the **no** or **default** form of this command to restore the default setting. **ip pim jp-timer** *seconds*

no ip pim jp-timer default ip pim jp-timer

Parameter Description

Parameter	Description
seconds	Interval to send the join/prune message in the range from 1 to 65535 in the unit of seconds

Defaults

The default is 60 seconds.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example sets the interval to send the Join/Prune message to 50 seconds.

```
QTECH(config)# ip pim jp-timer 50
```

Command	Description
N/A	N/A

N/A

6.12. ip pim neighbor-filter

Use this command to confine the neighbor address range.

Use the **no** or **default** form of this command to restore the default setting.

ip pim neighbor-filter *access_list*

no ip pim neighbor-filter *access_list*

default ip pim neighbor-filter *access_list*

Parameter Description

Parameter	Description
access_list	Access control list supporting numerical ACL in the range 1 to 99 and name ACL

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Neighbor filtering can enhance the security of a PIM-enabled network and provide neighbor restriction. As long as a neighbor is denied by the access list, PIM-SM will not establish the peering relationship with this neighbor or terminate the established peering relationship with this neighbor.

Configuration Examples

The following example blocks the neighbor address 192.168.1.5.

```
QTECH(config)# interface gi 0/3
QTECH(config-if- GigabitEthernet 0/3)# ip pim neighbor-filter 14 QTECH(config-
if- GigabitEthernet 0/3)# exit
QTECH(config)# access-list 14 deny 192.168.1.5 0.0.0.255
```

Related Commands

Command	Description
access-list	N/A

Platform Description

N/A

6.13. ip pim neighbor-tracking

Use this command to disable join restraint on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip pim neighbor-tracking

no ip pim neighbor-tracking default ip pim neighbor-tracking

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Interface configuration mode

Usage Guide

Use this command to disable join restraint on the interface. With join constraint enabled, the interface is constrained not to send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. On the other hand, with join constrain disabled, the interface will send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. This function allows upstream routers to track how many receivers in downstream in accord with all received Join messages.

Configuration Examples

The following example disables join restraint on the interface.

```
QTECH(config)# interface gi 0/3
QTECH(config-if-GigabitEthernet 0/3)# ip pim neighbor-tracking
```

Related Commands

Command	Description
ip pim propagation-delay	N/A

Platform Description

N/A

6.14. ip pim override-interval

Use this command to set the override-interval on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip pim override-interval *milliseconds*

no ip pim override-interval default ip pim override-interval

Parameter Description

Parameter	Description
interval-milliseconds	In the range from 1 to 65,535 in the unit of milliseconds

Defaults

The default is 2,500 milliseconds.

Command Mode

Interface configuration mode

Usage Guide

Use this command to set the override-interval for the interface.

Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Configuration Examples

The following example sets the override-interval as 3000 milliseconds.

```
QTECH(config)# interface gi 0/3
QTECH(config-if-GigabitEthernet 0/3)# ip pim override-interval 3000
```

Related Commands

Command	Description
ip pim propagation-delay	N/A

Platform Description

N/A

6.15. ip pim probe-interval

Use this command to set the register probe interval.

Use the **no** or **default** form of this command to restore the default setting.

ip pim probe-interval ***seconds*** no ip pim probe-interval default ip pim probe-interval

Parameter Description

Parameter	Description
interval-seconds	In the range from 1 to 65535 seconds

Defaults

The default is 5 seconds.

Command Mode

Global configuration mode

Usage Guide

Use this command to set the registration probe time. The DR can send the null registration message

to the RP in a period before the registration suppression time expires. This period is called probe time of null registration packet.

The probe time must be less than half of registration suppression time. Furthermore, 3* registration suppression time plus registration probe time should be no more than 65535s or

otherwise the system triggers an alarm.

Configuration Examples

Related Commands

Platform Description

The following example sets the probe time to 6 seconds.

```
QTECH(config)# ip pim probe-interval 6
```

Command	Description
N/A	N/A

N/A

6.16. ip pim propagation-delay

Use this command to set the propagation-delay on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip pim propagation-delay *milliseconds*

no ip pim propagation-delay default ip pim propagation-delay

Parameter Description

Parameter	Description
interval-milliseconds	In the range from 1 to 32,765 milliseconds

Defaults

The default is 500 milliseconds.

Command Mode

Interface configuration mode

Usage Guide

Use this command to set the propagation-delay for the interface.

Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Configuration Examples

The following example sets the propagation delay to 600 milliseconds.

```
QTECH(config)# interface gi 0/3
QTECH(config)# ip pim propagation-delay 600
```

Related Commands

Platform Description

Command	Description
ip pim override-interval	N/A
Ip pim neighbor-tracking	N/A

N/A

6.17. ip pim query-interval

Use this command to set the interval to send the hello packets.

Use the **no** or **default** form of this command to restore the default setting.

ip pim query-interval ***seconds*** no ip pim query-interval default ip pim query-interval

Parameter Description

Parameter	Description
interval-seconds	Interval to send the Hello message, in the range from 1 to 65,535 in the unit of seconds.

Defaults

The default is 30 seconds.

Command Mode

Interface configuration mode

Usage Guide

Upon updating the interval to send the Hello message, the time of holding the Hello message is updated by the following principle: The hold time is updated to be 3.5 times the transmission interval. If the transmission interval*3.5 is more than 65535, the hold time is updated to 18752.

Configuration Examples

The following example sets the interval to send the hello packets to 123 seconds.

```
QTECH(config)# interface gi 0/3
QTECH(config)# ip pim query-interval 123
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.18. ip pim register-checksum-wholepkt

Use this command to calculate the checksum of the whole register packet. Use the **no** or **default** form of this command to restore the default setting. **ip pim register-checksum-wholepkt** [**group-list** *access-list*]

no ip pim register-checksum-wholepkt [**group-list** *access-list*]

default ip pim register-checksum-wholepkt [**group-list** *access-list*]

Parameter Description

Parameter	Description
access-list	Access-list: access control list supporting numerical ACL in the range from100 to 199 and from1300 to 1999 and name ACL. Group-list access-list :all multicast packets use this configuration by default

Defaults

By default, the checksum of register messages calculates the head of PIM

message and register message rather than the whole PIM message

Command Mode

Global configuration mode

Usage Guide

Some vendors calculate checksum based on the overall registration packets. QTECH Networks introduces this function for the compatibility with devices of other vendors.

Configuration Examples

The following example calculates the checksum of the whole register packet.

```
QTECH(config)#ip pim register-checksum-wholepkt group-list 99
QTECH(config)# access-list 99 permit 225.1.1.1 0.0.0.255
```

Related Commands

Command	Description
access-list	N/A

Platform Description

N/A

6.19. ip pim register-decapsulate-forward

Use this command to enable the RP to decapsulate the register packets and forward the multicast packets.

Use the **no** or **default** form of this command to restore the default setting.

ip pim register-decapsulate-forward

no ip pim register-decapsulate-forward default ip pim register-decapsulate-forward

Parameter Description

Parameter	Description
-	-

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to implement the decapsulate of the PIM-SM registration packets with the multicast data packets received on the candidate RP and forward the multicast data packets.

As the decapsulating and forwarding are performed by the software, it is not recommended to configure this command in the case that many registration packets need to be decapsulated and forwarded, which may cause the CPU busy with this function configured.

Configuration Examples

Related Commands

Platform Description

The following example enables the RP to decapsulate the register packets and forwards the multicast packets.

```
QTECH(config)# ip pim register-decapsulate-forward
```

Command	Description
N/A	N/A

N/A

6.20. ip pim register-rate-limit

Use this command to limit the rate of register packets.

Use the **no** form of this command to restore the default setting.

ip pim register-rate-limit ***rate***

no ip pim register-rate-limit default ip pim register-rate-limit

Parameter Description

Parameter	Description
-	-
rate	Maximum number of register packets that can be sent per second, in the range from 1 to 65,535

Defaults

By default, there is no rate limitation on register messages.

Command Mode

Global configuration mode

Usage Guide

This command is used to configure speed of transmitting register packet in each (S, G) status, not the speed of transmitting register packets in the system. Using this command will decrease the load of source DR and RP. The register packets can be transmitted at the speed within the limit.

Configuration Examples

Related Commands

Platform Description

The following example limits the rate of register packets.

```
QTECH(config)# ip pim register-rate-limit 3000
```

Command	Description
N/A	N/A

N/A

6.21. ip pim register-rp-reachability

Use this command to check RP reachability before sending register packets**.** Use the **no** or **default** form of this command to restore the default setting.

ip pim register-rp-reachability

no ip pim register-rp-reachability default ip pim register-rp-reachability

Parameter Description

Parameter	Description
-	-

Defaults

By default, the RP reachability is not checked before sending register packets.

Command Mode

Global configuration mode

Usage Guide

This command is used to check the RP reachability before sending register packets. If not, register packets are not transmitted.

Configuration Examples

Related Commands

The following example checks the RP reachability before sending register packets.

```
QTECH(config)# ipv6 pim register-rp-reachability
```

Command	Description
N/A	N/A

Platform

N/A

Description

6.22. ip pim register-source

Use this command to specify the source IP address of the register packets. Use the no or default form of this command to restore the default setting. ip pim register-source { *local_address* | *interface-type interface-number* } no ip pim register-source

default ip pim register-source

Parameter Description

Parameter	Description
-	-
interface-type interface-number	Interface whose IP address is used as the source IP address of

	register packets
local_address	Specifies the source IP address of the register packet.

Defaults

By default, the source IP address of register packets is the IP address of the DR interface connecting the multicast source.

Command Mode

Global configuration mode

Usage Guide

This command is used to configure the source IP address of register messages.

The source IP address must be reachable. When RP receives the register packet, it transmits Register-Stop packet, using its source IP address as the destination IP address of the Register-Stop packet. It is not necessary to enable the PIM.

Configuration Examples

The following example specifies the source IP address of the register packets.

```
QTECH(config)# ip pim register-source 192.168.195.80
QTECH(config)# ip pim register-source gi 0/3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.23. ip pim register-suppression

Use this command to set the register suppression time.

Use the **no** or **default** form of this command to restore the default setting.

Parameter Description

Parameter	Description
suppression	Suppression time in the range from 1 to 65,535 in the unit of seconds.

ip pim register-suppression

seconds **no ip pim register-**

suppression default ip pim

register-suppression

Defaults

The default is 60 seconds.

Command Mode

Global configuration mode

Usage Guide

Executing this command on the DR will change the register packet suppression time configured. if the **ip pim rp-register-kat** command is not configured, executing this command on RP will modify the period of RP keepalive.

Configuration Examples

Related Commands

Platform Description

The following example sets the register suppression time to 100 seconds.

```
QTECH(config)# ip pim register-suppression 100
```

Command	Description
N/A	N/A

N/A

6.24. ip pim rp-address

Use this command to configure the static RP.

Use the **no** or **default** form of this command to restore the default setting.

ip pim rp-address *rp-address* [*access_list*]

no ip pim rp-address *rp-address* [*access_list*]

default ip pim rp-address *rp-address* [*access_list*]

Parameter Description

Parameter	Description
rp-address	IP address of RP
access_list	Access control list supporting numerical ACL in the range 1 to 99 and 1300 to 1999 and name ACL. All multicast groups are supported by default.

Defaults

No IP address is configured for the static RP by default.

Command Mode

Global configuration mode

Usage Guide

This system supports the configuration of multicast static RP, as well as the configuration of static RP and BSR mechanisms at the same time. When you use this command, note that:

If both the BSR mechanism and the static RP configuration take effect, the dynamic configuration takes precedence.

You can configure multiple multicast groups (using ACL) or all multicast groups (not using ACL) for the static RP. But a static RP can be configured only once.

If there are more than one static RP in a multicast group, the one of the highest IP address is used. Only the addresses permitted by ACL are valid multicast groups. By default, all the multicast groups 224/4 are permitted.

After configuration is performed, the static RP's source IP address is inserted to the group

range-based static RP group tree structure. Each group range-based static multicast group maintains the chain list structure of a static RP group. This chain list is sorted in descending order of IP address. When you select a RP from a static RP group, the first entry, namely the one with the largest IP address, will be selected first.

Deleting a static IP address also deletes this address from all the existing static RP groups and selects one from in the existing RP group tree structure as the RP address.

Configuration Examples

The following example specifies the source IPv6 address of the register packet.

```
QTECH(config)# ip pim rp-address 210.34.0.55 4
QTECH(config)# access-list 4 permit 255.1.1.1 0.0.0.255
```

Related Commands

Command	Description
access-list	N/A

Platform Description

N/A

6.25. ip pim rp-candidate

Use this command to configure the C-RP.

Use the **no** or **default** form of this command to restore the default setting.

ip pim rp-candidate *interface-type interface-number* [**priority** *priority-value*] [**interval** *seconds*] [**group-list** *access_list*]

no ip pim rp-candidate [*interface-type interface-number*]

default ip pim rp-candidate [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and interface number
priority-value	(Optional) Priority in the range 0 to 255, 192 by default
seconds	(Optional) Interval in the range 0 to 16,383 seconds, 60s by default
access_list	(Optional) Numerical ACL in the range 1 to 99 or name ACL. By default, all multicast groups are permitted.

Defaults

No C-RP is configured by default.

Command Mode

Global configuration mode

Usage Guide

In the PIM-SM protocol, the shared tree RPT created by the multicast routing uses the Rendezvous Point (RP) as the root node. RP is elected by the candidate RPs. After BSR is elected, all C-RPs sends C-RP messages in the unicast form to BSR regularly, and BSR spreads the messages throughout the PIM domain.

To specify an interface as the candidate RP of a specific group, execute this command with ACL. Note that the group range is calculated only based on the permit rule, not the deny rule.

Configuration Examples

The following example configures the C-RP.

```
QTECH(config)# ip pim rp-candidate gi 0/3 priority 200 group-list 3 interval 70
QTECH(config)# access-list 3 permit 255.1.1.1 0.0.0.255
```

Related Commands

Command	Description
access-list	N/A

Platform Description

N/A

6.26. ip pim rp-register-kat

Use this command to set the KAT interval on the RP.

Use the **no** or **default** form of this command to restore the default setting.

ip pim rp-register-kat ***seconds*** no ip pim rp-register-kat default ip pim rp-register-kat

Parameter Description

Parameter	Description
seconds	KAT timer time in the range from 1 to 65,525 in the unit of seconds

Defaults

The default is 210 seconds.

Command Mode

Global configuration mode

Usage Guide

Configuration Examples

Related Commands

Platform Description

The following example sets the KAT interval on the RP to 250 seconds.

```
ruijie(config)# ip pim rp-register-kat 250
```

Command	Description
N/A	N/A

N/A

6.27. ip pim sparse-mode

Use this command to enable PIM-SM on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip pim sparse-mode no ip pim sparse-mode

default ip pim sparse-mode

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

This command is used to enable PIM-SM on the interface.

You need to enable multicast routing forwarding in the global configuration mode before enabling PIM-SM. Otherwise, multicast packets cannot be forwarded even though you enable

PIM-SM.

During the execution of this command, if the prompt "Failed to enable PIM-SM on <Interface Name>, resource temporarily unavailable, please try again" appears, re-execute this command.

During the execution of this command, if the prompt "PIM-SM Configure failed! VIF limit exceeded in NSM!!!" appears; it indicates the allowed configured interface number exceeds the

upper limit of the multicast interfaces. In this case, if you still need to enable PIM-SM on the interface, delete the unnecessary PIM-SM, PIM-DM or DVMRP interfaces.

It is not recommended to configure different IPv4 multicast routing protocols on different

interfaces of a device.

Configuration Examples

The following example enables PIM-SM on the interface.

```
QTECH(config)# interface gi 0/3
QTECH(config-if-GigabitEthernet 0/3)# ip pim sparse-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.28. ip pim sparse-mode passive

Use this command to enable PIM-SM PASSIVE.

Use the **no** or **default** form of this command to restore the default setting.

ip pim sparse-mode passive

no ip pim sparse -mode passive default ip pim sparse-mode passive

Parameter Description

Parameter	Description
N/A	N/A

Defaults

PIM-SM PASSIVE is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Please configure multicast route forwarding in global configuration mode before enabling PIM-SM PASSIVE.

When PIM-SM PASSIVE is enabled, IGMP is enabled on each interface automatically.

Enabled with PIM-SM PASSIVE, the interface neither receives nor sends PIM packets. Instead, it forwards multicast packets. PIM-SM PASSIVE is generally configured on the device of the stub area, so as to avoid floods of PIM hello packets.

Configuration Examples

The following example enables PIM-SM PASSIVE on interface GigabitEthernet 0/3.

Related Commands

```
QTECH# configure terminal
QTECH(config)# interface gi 0/3
QTECH(config-if-GigabitEthernet 0/3)# ip pim sparse-mode passive
```

Command	Description
N/A	N/A

Platform Description

N/A

6.29. ip pim sparse-mode subvlan

Use this command to enable PIM-SM on the Super VLAN interface. Use the **no** or **default** form of this command is to restore the default setting.

ip pim sparse-mode subvlan **[** all **|** ***vid*** **]** no ip pim sparse-mode subvlan default ip pim sparse-mode subvlan

Parameter Description

Parameter	Description
all	Sends PIM packets to all sub VLANs.
vid	Sends PIM packets to the specified VLAN.

Defaults
PIM-SM is disabled on the Super VLAN interface by default.

Command Mode

Interface configuration mode

Usage Guide

In general, a super VLAN includes many sub VLANs. If the PIM-SM protocol is enabled on the interfaces of the super VLAN, PIM-SM multicast packets will be replicated and sent to all sub VLANs. As a result, the traffic may exceed the device capability, causing protocol flapping. The Super VLAN interface is disabled with PIM-SM generally. Use this command to enable PIM-SM on the Super VLAN interface to send PIM packets to all sub VLANs or the specified sub VLAN.

Configuration Examples

The following example enables PIM-SM on the Super VLAN interface and

sends PIM packets to sub VLAN 200.

```
QTECH# configure terminal QTECH(config)# interface vlan
100
QTECH(config-if-vlan 100)# ip pim sparse-mode subvlan 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.30. ip pim spt-threshold

Use this command to enable the SPT switching function.

Use the **no** or **default** form of this command to restore the default setting.

ip pim spt-threshold [**group-list** *access-list*]

no ip pim spt-threshold [**group-list** *access-list*]

default ip pim spt-threshold [**group-list** *access-list*]

Parameter Description

Parameter	Description
access_list	(Optional) Numerical ACL in the range 1 to 99 and 1300 to 1999 or name ACL. By default, all multicast groups are permitted for SPT switching.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to enable the RP tree-to-SPT tree switching function in a specific multicast group range (using **group-list**) or all multicast groups (not using **group-list**) .

Configuration Examples

The following example enables the SPT switching function.

```
QTECH(config)# ip pim spt-threshold group-list 12
QTECH(config)# access-list 12 permit 225.1.1.1 0.0.0.255
```

Related Commands

Command	Description
access-list	N/A

Platform Description

N/A

6.31. ip pim ssm

Use this command to enable SSM and set the SSM group address range. Use the **no** or **default** form of this command to restore the default setting. **ip pim ssm** { **default** | **range** *access_list* }

no ip pim ssm default ip pim ssm

Parameter Description

Parameter	**Description**
default	Multicast groups of 232/8
range *access_list*	Numerical ACL in the range 1 to 99 and 1300 to 1999 or name ACL.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to enable PIM-SSM (or in some specific multicast groups).

Configuration Examples

The following command enables SSM and sets the SSM group range to 232/8:

```
QTECH(config)# ip pim ssm default
```

The following command sets the source-specific multicast with ACL 10.

```
QTECH(config)# ip pim ssm range 10
QTECH(config)# access-list 10 permit 232.0.0.1 0.0.0.255
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description

N/A

6.32. ip pim triggered-hello-delay

Use this command to configure Triggered-Hello-Delay time on the interface. Use the **no** or **default** form of this command to restore the default setting. **ip pim triggered-hello-delay** *seconds*

no ip pim triggered-hello-delay default ip pim triggered-hello-delay

Parameter Description

Parameter	Description
seconds	In the range from 1 to 5 in the unit of seconds.

Defaults
The default is 5 seconds.

Command Mode

Interface configuration mode

Usage Guide

Use this command to configure the triggered-hello-delay of the interface. When the interface starts or detects a new neighbor, it uses the trigger-hello-delay to generate random time, and then the interface sends the Hello message in random time.

Configuration Examples

The following command sets the triggered-hello-delay to 3 seconds.

```
QTECH(config)# interface gi 0/3
QTECH(config-if-GigabitEthernet 0/3)# ip pim triggered-hello-delay 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.33. show debugging

Use this command to display the debugging status.

show debugging

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode
Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Configuration Examples

The following example displays the debugging status.

```
QTECH#show debugging ip packet
debug:
ip packet debug debugging is on, acl: 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.34. show ip pim sparse-mode bsr-router

Use this command to display the BSR information
show ip pim sparse-mode bsr-router

Parameter Description

Parameter	**Description**
-	-

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Configuration Examples

The following example displays BSR information.

```
QTECH# show ip pim sparse-mode bsr-router PIMv2 Bootstrap
information
This system is the Bootstrap Router (BSR) BSR address:
192.168.127.1
Uptime: 01d23h14m, BSR Priority: 64, Hash mask length: 10 Next bootstrap
message in 00:00:42
Role: Candidate BSR   Priority: 64, Hash mask length: 10 State: Elected
BSR
Candidate RP: 30.30.100.200(GigabitEthernet 0/3) Advertisement
interval 60 seconds
00:00:32
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.35. show ip pim sparse-mode interface

Use this command to display PIM-SM interface information.

show ip pim sparse-mode interface [*interface-type interface-number*] [**detail**]

Parameter Description

Parameter	Description
interface-type interface-number	(Optional) Interface name. This command takes effect for all interfaces by default.

detail	(Optional) Displays the details of an interface.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Configuration Examples

The following example displays the PIM-SM information on the interface.

```
QTECH#show ip pim sparse-mode interface detail GigabitEthernet
0/3 (vif 3):
Address 30.30.100.200, DR 30.30.100.200
Hello period 30 seconds, Next Hello in 11 seconds Triggered
Hello period 5 seconds
Neighbors:
2.2.2.2
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.36. show ip pim sparse-mode local-members

Use this command to display the local IGMP information on the PIM-SM interface.

show ip pim sparse-mode local-members [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	(Optional) Interface name. This command takes effect for all

	interfaces by default.

Defaults
N/A

Command Mode
Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Configuration Examples

The following example displays the local IGMP information on the PIM-SM interface.

```
QTECH (config-if)#sh ip pim sparse-mode local-members PIM Local
membership information
GigabitEthernet 0/3:
(*, 225.1.1.1) : Include
Loopback 1:
GigabitEthernet 0/5:
```

Related Commands

Command	Description
N/A	N/A

Platform Description
N/A

6.37. show ip pim sparse-mode mroute

Use this command to display the PIM-SM routing information.

show ip pim sparse-mode mroute [*group-or-source-address* [*group-or-source-address*]]

Parameter Description

Parameter	Description
group-or-source-address	Group IP address or source IP address. Two addresses cannot both be the group addresses or the source

	addresses.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

This command is used to display routing information. Only one group IP address, one source IP address or one group IP address-source IP address pair can be configured at a time. You can also specify no group IP address or source IP address.

Configuration Examples

Related Commands

Platform Description

The following example displays the PIM-SM routing information.

```
QTECH#show ip pim sparse-mode mroute
```

Command	Description
N/A	N/A

N/A

6.38. show ip pim sparse-mode neighbor

Use this command to display the neighbor information.

show ip pim sparse-mode neighbor **[** detail **]**

Parameter Description

Parameter	Description

detail	(Optional) Displays the details of an interface.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Configuration Examples

The following example displays the neighbor information.

```
QTECH# show ip pim sparse-mode neighbor
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.39. show ip pim sparse-mode nexthop

Use this command to display the next-hop information, including the interface ID, address and metric.

show ip pim sparse-mode nexthop

Parameter Description

Parameter	Description
-	-

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

Related

The following example displays the next-hop information.

```
QTECH# show ip pim sparse-mode nexthop
```

Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.40. show ip pim sparse-mode rp mapping

Use this command to display the information on all RPs and the multicast groups they serve.

show ip pim sparse-mode rp mapping

Parameter Description

Parameter	Description
mapping	All group and RP information

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the information on all RPs and the multicast groups they serve.

```
QTECH# show ip pim sparse-mode rp mapping PIM Group-to-RP
Mappings
Group(s): 224.0.0.0/4 RP:
30.30.200.1
Info source: 30.30.200.1, via bootstrap, priority 192 Uptime:
00:00:51, expires: 00:01:39
RP: 30.30.100.1
Info source: 30.30.200.1, via bootstrap, priority 192 Uptime:
00:19:14, expires: 00:01:38
Group(s): 224.0.0.0/4, Static RP:
100.100.100.100
Uptime: 00:45:35
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.41. show ip pim sparse-mode rp-hash

Use this command to display the RP information corresponding to the group address.

show ip pim sparse-mode rp-hash *group-address*

Parameter Description

Parameter	Description
group-address	Group address to be resolved

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Configuration Examples

The following example displays the RP information corresponding to the group address.

```
QTECH# show ip pim sparse-mode rp-hash 255.1.1.1 RP: 30.30.100.1
Info source: 30.30.100.1, via bootstrap
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.42. show ip pim sparse-mode track

Use this command to display the number of sent and received PIM packets during the period from the beginning of the statistics till now.

show ip pim sparse-mode track

Parameter Description

Parameter	Description
-	-

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

This command is used to display the number of sent and received PIM packets during the period from the beginning of the statistics till now. When the system starts up, it sets the start time of the statistics. The start time of the statistics is reconfigured and the PIM packet counter is cleared on calling the **clear ip pim sparse-mode track** every time.

Configuration Examples

The following example displays the number of sent and received PIM packets during the period from the beginning of the statistics till now.

```
QTECH # show ip pim sparse-mode track PIM packet counters track
Elapsed time since counters cleared: 00:04:03 received     sent
Valid PIMSM packets:    0           8
Hello:                      0         8
Join-Prune:         0           0
Register:           0           0
Register-Stop:      0           0
Assert:             0           0
BSM:                0           0
C-RP-ADV:                   0         0
PIMDM-Graft:            0
PIMDM-Graft-Ack     0
:
PIMDM-State-        0
Refresh:
Unknown       PIM   0
Type:
Errors:
Malformed                       0
packets:
Bad checksums:                  0
Send errors:                    0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.1. clear ipv6 mroute

Use this command to clear multicast routing entries.

clear ipv6 mroute {* | *ipv6_group_address* [*ipv6_source_address*] }

Parameter Description

Parameter	Description
*	Deletes all the multicast routing entries.
ipv6_group_address	Deletes the multicast routing entries of the specific group.
ipv6_source_address	Deletes the multicast routing entries of the specific group and source IPv6 address.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example clears all the multicast routing entries.

```
QTECH# clear ipv6 mroute *
```

The following example clears the multicast routing entries of the specified group.

```
QTECH# clear ipv6 mroute ff66::6666
```

The following example clears the multicast routing entries of the specified group

and source address. QTECH# clear ipv6 mroute ff66::6666 3333::3333

Command	Description
N/A	N/A

N/A

7.2. clear ipv6 mroute statistics

Use this command to delete the statistics of the multicast routing entries.

clear ipv6 mroute statistics {* | *ipv6_group_address* [*ipv6_source_address*] }

Parameter **Description**

Parameter	Description
*	Deletes the statistics of all multicast routing entries.
ipv6_group_address	Deletes the statistics of the multicast routing entries of the specific group.
ipv6_source_address	Deletes the statistics of the multicast routing entries of the specific group and source IPv6 address.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example deletes the statistics of the multicast routing entries.

```
QTECH# clear ipv6 mroute statistics *
```

The following example clears the statistics of the multicast routing entries of the specified group.

```
QTECH# clear ipv6 mroute statistics ff66::6666
```

The following example clears the statistics of the multicast routing entries of the specified group and source address.

```
QTECH# clear ipv6 mroute statistics ff66::6666 3333::3333
```

Command	Description
N/A	N/A

N/A

7.3. clear ipv6 pim sparse-mode bsr rp-set *

Use this command to clears the RP information learnt dynamically.

clear ipv6 pim sparse-mode bsr rp-set *

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Only the RP information learnt dynamically can be cleared manually.

Configuration Examples

Related Commands

Platform Description

The following example clears the RP information learnt dynamically.

```
QTECH# clear ipv6 pim sparse-mode bsr rp-set *
```

Command	Description
N/A	N/A

N/A

7.4. clear ipv6 pim sparse-mode track

Use this command to reconfigure the start time of the statistics and clear the PIMv6 packet counter.

clear ipv6 pim sparse-mode track

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example clears the PIMv6 packet counter.

```
QTECH# clear ipv6 pim sparse-mode track
```

Command	Description
show ipv6 pim sparse-mode track	N/A

N/A

7.5. ipv6 pim accept-bsr list

Use this command to confine the BSR address range.

Use the **no** or **default** form this command to restore the default setting.

ipv6 pim accept-bsrr list *ipv6_access-list*

no ipv6 pim accept-bsr

default ipv6 pim accept-bsr

Parameter Description

Parameter	Description
list *ipv6_access-list*	IPv6 ACL supporting named ACL

Defaults

By default, the PIM-SMv6 router receives all external BSM packets.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example confines the BSR address range.

QTECH(config)# ipv6 pim accept-bsr list bsr-list

Command	Description
N/A	N/A

N/A

7.6. ipv6 pim accept-crp list

Use this command to confine the C-RP address range and the multicast group address range it serves.

Use the no or default form of this command to restore the default setting, ipv6 pim accept-crp list *ipv6_access-list*

no ipv6 pim accept-crp

default ipv6 pim accept-crp-with-null-group

Parameter Description

Parameter	Description
list *ipv6_access-list*	IPv6 ACL supporting named ACL

Defaults
No address is filtered by default.

Command Mode
Global configuration mode

Usage Guide

With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to limit the address range of the legal C-RP and the multicast group range it serves.

Configuration Examples

Related Commands

Platform Description

The following example confines the C-RP address range and the multicast group address range it serves.

```
QTECH (config)# ipv6 pim accept-crp list crp-list
```

Command	Description
N/A	N/A

N/A

7.7. ipv6 pim accept-crp-with-null-group

Use this command to receive the C-RP-ADV packets whose prefix-count is 0. Use the **no** or **default** form of this command to restore the default setting. **ipv6 pim accept-crp-with-null-group**

no ipv6 pim accept-crp-with-null-group default ipv6 pim accept-crp-with-null-group

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to receive the C-RP-ADV packets whose prefix-count is 0, and considers this C-RP supports all groups.

Configuration Examples

Related Commands

Platform Description

The following example receives the C-RP-ADV packets whose prefix-count is 0.

```
QTECH (config)# ipv6 pim accept-crp-with-null-group
```

Command	Description
N/A	N/A

N/A

7.8. ipv6 pim accept-register

Use this command to accept specific register packets at the RP.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim accept-register { **list** *ipv6_access-list* [**route-map** *map-name*] | **route-map** *map-name*

[**list** *ipv6_access-list*] }

no ipv6 pim accept-register default ipv6 pim accept-register

Parameter Description

Parameter	Description
list *ipv6_access-list*	IPv6 ACL supporting named ACL
route-map *map-name*	Defines the routing map rule

Defaults

All register packets are received by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to confine the source IPv6 address of register messages on RP. If the unauthorized register source is received, the RP will return the Register-Stop message immediately.

Configuration Examples

The following example denies register packets of the specified source address at the RP.

```
QTECH(config)# ipv6 pim accept-register list register-access-list QTECH(config)#
ipv6 access-list register-access-list
QTECH(config-ipv6-acl)# deny ipv6 fe80::2d0:f8ff:fe22:33ad/128 any
```

Platform Description

N/A

7.9. ipv6 pim bsr-border

Use this command to configure the BSR border.

Use the no or default form of this command to restore the default setting.

ipv6 pim bsr-border

no ipv6 pim bsr-border default ipv6 pim bsr-border

Parameter Description

Parameter	Description
N/A	N/A

Defaults

No BSR border is configured by default.

Command Mode

Interface configuration mode

Usage Guide

To restrain BSM flooding, configure BSR border on the interface so that the interface drops BSM packets upon receiving them and the BSM packets are not forwarded from this interface.

Configuration Examples

The following example sets the BSR border on the interface *gi 0/3*.

```
QTECH(config)# interface gi 0/3
QTECH(config-if-GigabitEthernet)# ipv6 pim bsr-border
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.10. ipv6 pim bsr-candidate

Use this command to configure the candidate bootstrap router (C-BSR). Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim bsr-candidate *interface-type interface-number* [*hash-mask-length* [*priority-value*]]

no ipv6 pim bsr-candidate default ipv6 pim bsr-candidate

Parameter Description

Parameter	Description
interface-type *interface-number*	Interface type and number.
hash-mask-length	(Optional) HASK mask length configured for electing the RP in the range from 0 to 128. The default is 126.
priority-value	(Optional) Priority configured for the C-BSR in the range from 0 to 255. The default is 64.

Defaults

No C-BSR is configured by default.

Command Mode

Global configuration mode

Usage Guide

A PIM-SMv6 domain must contain a unique BootStrap Router (BSR). BSR is responsible for collect and issue RP information. A unique recognized BSR is elected among multiple candidate BSRs through the bootstrap packet. Before BSR information is available, C-BSRs consider them to be the BSR, and regularly send bootstrap packets using the multicast address 224.0.0.13 in the PIM-SM

domain. This packet contains the address and priority of the BSR.

This command allows the device to send a bootstrap message to all the PIM neighbors using the assigned BSR address. Each neighbor compares the original BSR address with

the address in the received bootstrap message. If the IPv6 address of the received address is equal to or larger than the original address, each neighbor saves this received address as the BSR address. Otherwise, they will discard this message.

The current device considers itself to be BSR until it receives a bootstrap message from another candidate BSR and is notified that it has a higher priority value (or the same priority value, but with a larger IPv6 address).

Configuration Examples

Related Commands

Platform Description

The following example s configures the C-BSR.

QTECH(config)# ipv6 pim bsr-candidate gi 0/3 30 100

Command	Description
N/A	N/A

N/A

7.11. ipv6 pim dr-priority

Use this command to configure the DR priority.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim dr-priority *priority-value*

no ipv6 pim dr-priority default ipv6 pim dr-priority

Parameter Description

Parameter	Description
priority-value	The larger the value, the higher the priority is. The range is from 0 to 4,294,967,294. The default is 1.

Defaults
The default is 1.

Command Mode

Interface configuration mode

Usage Guide

To select a DR:

- If the priority parameter of the Hello message is set for the devices in a LAN, the one of the highest priority is elected to be the DR. If several devices have the same priority, the one of the largest IP address is elected to be the DR.
- If the priority parameter of the Hello message is not set for the devices in a LAN, the one of the largest IP address is elected to be the DR.

Configuration Examples

The following example configures the DR priority.

```
QTECH(config)# interface gi 0/3
QTECH(config-if)# ipv6 pim dr-priority 11234
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.12. ipv6 pim ignore-rp-set-priority

Use this command to ignore the RP priority.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim ignore-rp-set-priority

no ipv6 pim ignore-rp-set-priority default ipv6 pim ignore-rp-set-priority

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, the C-RP with a higher priority is selected.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example ignores the RP priority.

```
QTECH(config-if)# ipv6 pim ignore-rp-set-priority
```

Command	Description
N/A	N/A

N/A

7.13. ipv6 pim jp-timer

Use this command to set the interval to send the join/prune message. Use the **no** or **default** form of this command to restore the default setting. **ipv6 pim jp-timer** *seconds*

no ipv6 pim jp-timer default ipv6 pim jp-timer

Parameter Description

Parameter	Description
seconds	Interval to send the join/prune message in the range from 1 to 65,535 in the unit of seconds

Defaults

The default is 60 seconds.

Command Mode

Global configuration mode

Usage Guide

Configuration Examples

The following example sets the interval to send the Join/Prune message to 100 seconds.

```
QTECH# configure terminal
QTECH(config)# ipv6 pim jp-timer 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.14. ipv6 pim neighbor-filter

Use this command to confine the neighbor address range.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim neighbor-filter *ipv6_access-list*

no ipv6 pim neighbor-filter *ipv6_access-list*

default ipv6 pim neighbor-filter *ipv6_access-list*

Parameter Description

Parameter	Description
ipv6_access_list	IPv6 ACL supporting named ACL

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Neighbor filtering can enhance the security of a PIM-enabled network and provide neighbor restriction. As long as a neighbor is denied by the access list, PIM-SM will not establish the peering relationship with this neighbor or terminate the established peering relationship with this neighbor.

Configuration Examples

The following example blocks the neighbor address fe80::2d0:f8ff:fe22:33ad.

```
QTECH(config)# interface gi 0/3
QTECH(config-if- GigabitEthernet 0/3)# ipv6 pim neighbor-filter acl QTECH(config-
if- GigabitEthernet 0/3)# exit
QTECH(config)# ipv6 access-list acl
QTECH(config-ipv6-acl)# deny ipv6 fe80::2d0:f8ff:fe22:33ad/128 any
```

Related Commands

Command	Description
ipv6_access-list	N/A

Platform Description

N/A

7.15. ipv6 pim neighbor-tracking

Use this command to disable join restraint on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim neighbor-tracking no ipv6 pim neighbor-tracking

default ipv6 pim neighbor-tracking

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Interface configuration mode

Usage Guide

Use this command to disable join restraint on the interface. With join constraint enabled, the interface is constrained not to send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. On the other hand, with join constrain disabled, the interface will send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream

neighbor. This function allows upstream routers to track how many receivers in downstream in accord with all received Join messages.

Configuration Examples

The following example disables join restraint on the interface.

```
QTECH(config)# interface gi 0/3
QTECH(config-if-GigabitEthernet)# ipv6 pim neighbor-tracking
```

Related Commands

Command	Description
ipv6 pim propagation-delay	N/A

Platform Description

N/A

7.16. ipv6 pim override-interval

Use this command to set the override-interval on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim override-interval *milliseconds*

no ipv6 pim override-interval default ipv6 pim override-interval

Parameter Description

Parameter	Description
milliseconds	In the range 1 to 65,535 in the unit of milliseconds

Defaults

The default is 2,500 milliseconds.

Command Mode

Interface configuration mode

Usage Guide

Use this command to set the override-interval for the interface.

Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Configuration Examples

The following example sets the override-interval to 3,000 milliseconds.

```
QTECH(config)# interface gi 0/3
QTECH(config-if-GigabitEthernet)# ipv6 pim override-interval 3000
```

Related Commands

Command	Description
ipv6 pim propagation-delay	N/A

Platform Description

N/A

7.17. ipv6 pim probe-interval

Use this command to set the register probe interval.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim probe-interval ***seconds*** no ipv6 pim probe-interval default ipv6 pim probe-interval

Parameter Description

Parameter	Description
seconds	In the range from 1 to 65,535 in the unit of seconds

Defaults

The default is 5 seconds.

Command Mode

Global configuration mode

Usage Guide

Use this command to set the registration probe time. The DR can send the null registration message to the RP in a period before the registration suppression time expires. This period is called probe time of null registration packet.

The probe time must be less than half of registration suppression time. Furthermore, 3* registration suppression time plus registration probe time should be no more than 65535s or

otherwise the system triggers an alarm.

Configuration Examples

Related Commands

Platform Description

The following example sets the probe time as 6 seconds.

```
QTECH(config)# ipv6 pim probe-interval 6
```

Command	Description
ipv6 pim register-suppression	N/A

N/A

7.18. ipv6 pim propagation-delay

Use this command to set the propagation-delay on the interface.

Use the **no** or **default** form of this command to restore the default setting.

Parameter Description

ipv6 pim propagation-delay *milliseconds*

no ipv6 pim propagation-delay default ipv6 pim propagation-delay

Parameter	Description
milliseconds	In the range from 1 to 32,765 in the unit of milliseconds

Defaults

The default is 500 milliseconds.

Command Mode

Interface configuration mode

Usage Guide

Use this command to set the propagation-delay for the interface.

- ❖ Change of propagation delay or prune delay will influence the override interval of Join/prune message.

As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Configuration Examples

The following example sets the propagation delay to 600 milliseconds.

```
QTECH(config)# interface gi 0/3
QTECH(config-if-GigabitEthernet 0/3)# ipv6 pim propagation-delay 600
```

Related Commands

Command	Description
ipv6 pim override-interval	N/A
ipv6 pim neighbor-tracking	N/A

Platform Description

N/A

7.19. ipv6 pim query-interval

Use this command to set the interval to send the hellp packets.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim query-interval ***seconds*** no ipv6 pim query-interval default ipv6 pim query-interval

Parameter Description

Parameter	Description
seconds	Interval to send the Hello message in the range from 1 to 65,535 in the unit of seconds

Defaults

The default is 30.

Command Mode

Interface configuration mode

Usage Guide

Upon updating the interval to send the Hello message, the time of holding the Hello message is updated by the following principle: The hold time is updated to be 3.5 times the transmission interval. If the transmission interval*3.5 is more than 65535, the hold time is updated to 18725.

Configuration Examples

The following example sets the interval to send the hello packets.

```
QTECH(config)# interface gi 0/3
QTECH(config-if-GigabitEthernet 0/3)# ipv6 pim query-interval 60
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.20. ipv6 pim register-checksum-wholepkt

Use this command to calculate the checksum of the whole register packet. Use the **no** or **default** form of this command to restore the default setting. **ipv6 pim register-checksum-wholepkt** [**group-list** *ipv6_access-list*]

no ipv6 pim register-checksum-wholepkt [**group-list** *ipv6_access-list*]

default ipv6 pim register-checksum-wholepkt [**group-list** *ipv6_access-list*]

Parameter Description

Parameter	Description
group-list *ipv6_access-list*	IPv6 ACL supporting named ACL. *ipv6_access-list*:all multicast packets use this configuration by default

Defaults

By default, the checksum of register messages calculates the head of PIM message and register message rather than the whole PIM message.

Command Mode

Global configuration mode

Usage Guide

Some vendors calculate checksum based on the overall registration packets. QTECH Networks introduces this function for the compatibility with these vendors.

Configuration Examples

The following example calculates the checksum of the whole register packet.

```
QTECH(config)#ipv6 pim register-checksum-wholepktgroup-list
```

Related Commands

Command	Description
ipv6 access-list	N/A

Platform Description

N/A

7.21. ipv6 pim register-rate-limit

Use this command to limit the rate of register packets.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim register-rate-limit ***rate***

no ipv6 pim register-rate-limit default ipv6 pim register-rate-limit

Parameter Description

Parameter	Description
rate	Maximum number of register packets that can be sent per second, in the range from 1 to 65,535.

Defaults

By default, there is no rate limitation on register messages.

Command Mode

Global configuration mode

Usage Guide

This command is used to configure speed of transmitting register packet in each (S, G) status, not the speed of transmitting register packets in the system. Using this command will decrease the load of source DR and RP. The register packets can be transmitted at the speed within the limit.

Configuration Examples

Related Commands

Platform Description

The following example limits the rate of register packets.

```
QTECH(config)# ipv6 pim register-rate-limit 3000
```

Command	Description
N/A	N/A

N/A

7.22. ipv6 pim register-rp-reachability

Use this command to check RP reachability before sending register packets**.** Use the **no** or **default** form of this command to restore the default setting. **ipv6 pim register-rp-reachability**

no ipv6 pim register-rp-reachability default ipv6 pim register-rp-reachability

Parameter Description

Parameter	Description
N/A	N/A

Defaults
By default, the RP reachability is not checked before sending register packets.

Command Mode

Global configuration mode

Usage Guide

This command is used to check the RP reachability before transmission. If not, register packets are not transmitted.

Configuration Examples

Related Commands

Platform Description

The following example checks the RP reachability before sending register packets.

```
QTECH(config)# ipv6 pim register-rp-reachability
```

Command	Description
N/A	N/A

N/A

7.23. ipv6 pim register-source

Use this command to specify the source IPv6 address in the register packets. Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim register-source { *ipv6_local_address* | *interface-type interface-number* }

no ipv6 pim register-source default ipv6 pim register-source

Parameter Description

Parameter	Description
ipv6_local_address	Source IPv6 address of register packets
interface-type *interface-number*	Interface whose IPv6 address is used as the source IPv6 address of register packets

Defaults

By default, the source IPv6 address of register packets is the IPv6 address of the DR interface connecting the multicast source.

Command Mode

Global configuration mode

Usage Guide

The source IPv6 address must be reachable. When RP receives the register packet, it transmits Register-Stop packet, using its source IPv6 address as the destination IPv6 address of the Register-Stop packet.

- It is not necessary to enable the PIM-SMv6 on the associated interfaces

Configuration Examples

The following example configures the source IPv6 address of register messages.

```
QTECH(config)# ipv6 pim register-source 3333::3333
QTECH(config)# ipv6 pim register-source gi 0/3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.24. ipv6 pim register-suppression

Use this command to set the register suppression time.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim register-suppression ***seconds*** no ipv6 pim register-suppression default ipv6 pim register-suppression

Parameter Description

Parameter	Description
seconds	Suppression time in the range from 1 to 65,535 in the unit of seconds

Defaults
The default is 60 seconds.

Command Mode

Global configuration mode

Usage Guide

Executing this command on the DR will change the register packet suppression time configured. if the ipv6 pim rp-register-kat command is not configured, executing this command on RP will modify the period of RP keepalive.

Configuration Examples

Related Commands

Platform Description

The following example sets the register packet suppression time.

```
QTECH(config)# ipv6 pim register-suppression 100
```

Command	Description
N/A	N/A

N/A

7.25. ipv6 pim rp embedded

Use this command to enable the embedded RP function.

Use the **no** or **default** form of this command to disable this function.

ipv6 pim rp embedded [**group-list** *ipv6_acl_name*]

no ipv6 pim rp embedded default ipv6 pim rp embedded

Parameter Description

Parameter	Description
group-list *ipv6_acl_name*	IPv6 ACL

Defaults

This function is enabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to enable the embedded RP function explicitly and to enable the embedded RP for the IPv6 multicast address of specified embedded RP address.

Configuration Examples

Related Commands

Platform Description

The following example enables the embedded RP for the IPv6 multicast addresses of all embedded RP addresses.

```
QTECH(config)# ipv6 pim rp embedded
```

Command	Description
ipv6 access-list	N/A

N/A

7.26. ipv6 pim rp-address

Use this command to configure the static RP.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim rp-address *ipv6_rp-address* [*ipv6_access_list*]

no ipv6 pim rp-address *ipv6_rp-address* [*ipv6_access-list*]

default ipv6 pim rp-address *ipv6_rp-address* [*ipv6_access-list*]

Parameter Description

Parameter	Description
ipv6_rp-address	IPv6 address of RP
ipv6_access_list	IPv6 ACL supporting named ACL

Defaults

No IPv6 address is configured for the static RP by default.

Command Mode

Global configuration mode

Usage Guide

This system supports the configuration of multicast static RP, as well as the configuration of static RP and BSR mechanisms at the same time. When you use this command, note that:

- If both the BSR mechanism and the static RP configuration take effect, the dynamic configuration takes precedence.
- You can configure multiple multicast groups (using ACL) or all multicast groups (not using ACL) for the static RP. But a static RP can be configured only once.
- If there are more than one static RP in a multicast group, the one of the highest IPv6 address is used.
- Only the addresses permitted by ACL are valid multicast groups. By default, all the multicast groups 224/4 are permitted.
- After configuration is performed, the static RP's source IPv6 address is inserted to the group range-based static RP group tree structure. Each group range-based static multicast group maintains the chain list structure of a static RP group. This chain list is sorted in descending order of IPv6 address. When you select a RP from a static RP group, the first entry, namely the one with the largest IPv6 address, will be selected first.

Deleting a static IPv6 address also deletes this address from all the existing static RP groups and selects one from in the existing RP group tree structure as the RP address.

Configuration Examples

The following example configures the RP static address.

```
QTECH(config)# ipv6 pim rp-address 3333::3333 acl QTECH(config)#
ipv6 access-list acl
QTECH(config)# permit ipv6 any ff66::6666/64
```

Related Commands

Command	Description
ipv6 access-list	N/A

Platform Description

N/A

7.27. ipv6 pim rp-candidate

Use this command to configure the candidate RP (C-RP).

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim rp-candidate *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *ipv6_access-list*]

no ipv6 pim rp-candidate [*interface-type interface-number*]

default ipv6 pim rp-candidate [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type *interface-number*	Interface type and interface number
priority-value	(Optional) Priority in the range from 0 to 255, 192 by default
interval-seconds	(Optional) Interval in the range from 0 to 16383 in the unit of seconds, 60 by default
ipv6_access_list	(Optional) IPv6 ACL supporting named ACL

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

In the PIM-SMv6 protocol, the shared tree RPT created by the multicast routing uses the Rendezvous Point (RP) as the root node. RP is elected by the candidate RPs. After BSR is elected, all C-RPs sends C-RP messages in the unicast form to BSR regularly, and BSR spreads the messages throughout the PIM domain.

To specify an interface as the candidate RP of a specific group, execute this command with ACL. Note that the group range is calculated only based on the permit rule, not the deny rule.

Configuration Examples

The following example configures the RP candidate.

```
QTECH(config)# ipv6 pim rp-candidate gi 0/3 priority 200 group-list acl interval 40
QTECH(config)# ipv6 access-list acl
QTECH(config-ipv6-acl)# permit ipv6 any ff66::6666/64
```

Command	Description
N/A	N/A

Platform Description

N/A

7.28. ipv6 pim rp-register-kat

Use this command to set the Keepalive Timer (KAT) of a (S, G) entry created by the register packet at the RP.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim rp-register-kat ***seconds*** no ipv6 pim rp-register-kat default ipv6 pim rp-register-kat

Parameter Description

Parameter	Description
seconds	KAT value in the range from1 to 65,525 in the unit of seconds.

Defaults
The default is equal to the sum of register probe time and three times register suppression time.

Command Mode

Global configuration mode

Usage Guide

The KAT value at the RP should be greater than three times the register suppression time at the source DR. Otherwise, the KAT will end and the entry (S,G) will time out before another register packet is sent, so that multicast stream will break down in a short while.

Configuration Examples

Related Commands

Platform Description

The following example configures the KAT interval of RP.

QTECH(config)# ipv6 pim rp-register-kat 250

Command	Description
N/A	N/A

N/A

7.29. ipv6 pim sparse-mode

Use this command to enable PIM-SMv6 on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim sparse-mode no ipv6 pim sparse-mode

default ipv6 pim sparse-mode

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

This command is used to enable PIM-SMv6 on the interface.

- You need to enable multicast routing forwarding in the global configuration mode before enabling PIM-SMv6. Otherwise, multicast packets cannot be forwarded even though you enable PIM-SM.

- During the execution of this command, if the prompt "Failed to enable PIM-SMv6 on <Interface Name>, resource temporarily unavailable, please try again" appears, re-execute this command.

- IPv6 multicast packets cannot be forwarded through SuperVLAN.

- During the execution of this command, if the prompt "PIM-SMv6 Configure failed! VIF limit exceeded in NSM!!!" appears; it indicates the allowed configured interface number exceeds the upper limit of the multicast interfaces. In this case, if you still need to enable PIM-SMv6 on the interface, delete the unnecessary PIM-SMv6,or PIM-DMv6 interfaces.

Configuration Examples

The following example enables PIM-SMv6 on the interface.

```
QTECH(config)# interface gi 0/3
QTECH(config-if-GigabitEthernet 0/3)# ipv6 pim sparse-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.30. ipv6 pim sparse-mode passive

Use this command to enable PIM-SMv6 PASSIVE.

Use the no or default form of this command to restore the default setting.

ipv6 pim sparse-mode passive

no ipv6 pim sparse -mode passive default ipv6 pim sparse-mode passive

Parameter Description

Parameter	Description
N/A	N/A

Defaults

PIM-SMv6 PASSIVE is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Please configure multicast route forwarding in global configuration mode before enabling PIM-SMv6 PASSIVE.

When PIM-SMv6 PASSIVE is enabled, IGMP is enabled on each interface automatically.

Enabled with PIM-SMv6 PASSIVE, the interface neither receives nor sends PIM packets. Instead, it forwards multicast packets. PIM-SMv6 PASSIVE is generally configured on the device of the stub area, so as to avoid floods of PIM hello packets.

Configuration Examples

The following example enables PIM-SMv6 PASSIVE on interface GigabitEthernet 0/3.

```
QTECH# configure terminal QTECH(config)#
interface gi 0/3
QTECH(config-if-GigabitEthernet 0/3)# ipv6 pim sparse-mode passive
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.31. ipv6 pim sparse-mode subvlan

Use this command to enable PIM-SMv6 on the Super VLAN interface. Use the **no** or **default** form of this command is to restore the default setting.

ipv6 pim sparse-mode subvlan **[** all **|** ***vid*** **]** no ipv6 pim sparse-mode subvlan default ipv6 pim sparse-mode subvlan

Parameter Description

Parameter	Description
all	Sends PIM packets to all sub VLANs.
vid	Sends PIM packets to the specified VLAN.

Defaults

PIM-SMv6 is disabled on the Super VLAN interface by default.

Command Mode

Interface configuration mode

Usage Guide

In general, a super VLAN includes many sub VLANs. If the PIM-SMv6 protocol is enabled on the interfaces of the super VLAN, PIM-SMv6 multicast packets will be replicated and sent to all sub VLANs. As a result, the traffic may exceed the device capability, causing protocol flapping. The Super VLAN interface is disabled with PIM-SMv6 generally. Use this command to enable PIM-SMv6 on the Super VLAN interface to send PIM packets to all sub VLANs or the specified sub VLAN.

Configuration Examples

The following example enables PIM-SMv6 on the Super VLAN interface and sends PIM packets to sub VLAN 200.

```
QTECH# configure terminal QTECH(config)# interface vlan
100
QTECH(config-if-vlan 100)# ipv6 pim sparse-mode subvlan 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.32. ipv6 pim spt-threshold

Use this command to enable SPT switch.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim spt-threshold [**group-list** *ipv6_access-list*]

no ipv6 pim spt-threshold [**group-list** *ipv6_access-list*]

default ipv6 pim spt-threshold [**group-list** *ipv6_access-list*]

Parameter Description

Parameter	Description
ipv6_access_list	(Optional) IPv6 ACL supporting named ACL

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to enable the RP tree-to-SPT tree switching function in a specific multicast group range (using group-list) or all multicast groups (not using group-list) .

Configuration Examples

The following example enables the SPT switch.

```
QTECH(config)# ipv6 pim spt-threshold acl QTECH(config)#
ipv6 access-list acl
QTECH(config-ipv6-acl)# permit ipv6 fe80::2d0:f8ff:fe22:33ad /128
ff66::6666/64
```

Related Commans

Command	Description
ipv6 access-list	N/A

Platform Description

N/A

7.33. ipv6 pim ssm

Use this command to enable SSM and set the SSM group address range. Use the **no** or **default** form of this command to restore the default setting. **ipv6 pim ssm** { **default** | **range** *ipv6_access-list* }

no ipv6 pim ssm default ipv6 pim ssm

Parameter Description

Parameter	Description
default	Group in the range of FF3x::/32
range *ipv6_access_list*	IPv6 ACL supporting named ACL

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to enable PIM-SSMv6 (or in some specific multicast groups).

Configuration Examples

The following example sets the source-specific multicast of the multicast group range ACL.

```
QTECH# configure terminal
QTECH(config)# ipv6 pim ssm range aclQTECH(config-ipv6-acl)# permit ipv6
fe80::2d0:f8ff:fe22:33ad /128  ff32::3333/64
```

Related Commands

Command	Description
ipv6 access-list	N/A

Platform Description

N/A

7.34. ipv6 pim static-rp-preferred

Use this command to configure a higher priority for static RP over the C-RP. Use the **no** or **default** form of this command to restore the default setting.

Parameter Description

ipv6 pim static-rp-

preferred no ipv6 pim

static-rp-preferred

default ipv6 pim static-rp-preferred

Parameter	Description
N/A	N/A

Defaults

By default, the priority of the RP elected through BSR mechanism is high than the one configured statically.

Command Mode

Global configuration mode

Usage Guide

With this command configured, the priority of the static RP is higher than the one elected through the BSR mechanism.

Configuration Examples

Related Commands

Platform Description

The following example configures the priority of the static RP is higher than the one elected through the BSR mechanism.

```
QTECH(config-if)# ipv6 pim static-rp-preferred
```

Command	Description
N/A	N/A

N/A

7.35. ipv6 pim triggered-hello-delay

Use this command to configure Triggered-Hello-Delay time on the interface. Use the **no** or **default** form of this command to restore the default setting. **ipv6 pim triggered-hello-delay** *seconds*

no ipv6 pim triggered-hello-delay default ipv6 pim triggered-hello-delay

Parameter Description

Parameter	Description
seconds	In the range from1 to 5 in the unit of seconds.

Defaults
The default is 5 seconds.

Command Mode

Interface configuration mode

Usage Guide

Use this command to configure the triggered-hello-delay of the interface. When the interface starts or detects a new neighbor, it uses the trigger-hello-delay to generate random time, and then the interface sends the Hello message at the random time.

Configuration Examples

The following example sets the triggered-hello-delay to 3 seconds.

```
QTECH(config)# interface gi 0/3
QTECH(config-if-GigabitEthernet 0/3)# ipv6 pim triggered-hello-delay 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.36. show debugging

Use this command to display the debugging status.

show debugging

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the debugging status.

```
QTECH # show debugging
PIM-SM Debugging status: PIM packet
debugging is on.
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.37. show ipv6 pim sparse-mode bsr-router

Use this command to display the BSR information.

show ipv6 pim sparse-mode bsr-router

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Command Mode

Privileged EXEC mode/ global configuration mode / interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays BSR information.

```
QTECH# show ipv6 pim sparse-mode bsr-router PIMv2 Bootstrap
information
This system is the Bootstrap Router (BSR) BSR address:
3333::8888
Uptime:00:03:31, BSR Priority: 64, Hash mask length: 126 Next bootstrap
message in 00:00:47
```

```
Role: Candidate BSR Priority: 64, Hash mask length: 126 State: Elected BSR
Candidate RP: 3333::8888(GigabitEthernet 0/5) Advertisement
interval 60 seconds
Next Cand_RP_advertisement in 00:00:37
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.38. show ipv6 pim sparse-mode interface

Use this command to display PIM-SMv6 interface information.

show ipv6 pim sparse-mode interface [*interface-type interface-number*] [**detail**]

Parameter Description

Parameter	Description
interface-type interface-number	(Optional) Interface name. This command takes effect for all interfaces by default.
detail	(Optional) Displays the details of an interface.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the PIM-SMv6 interface information.

```
QTECH #show ipv6 pim sparse-mode interface detail
GigabitEthernet 0/5 (vif 1):
```

```
Address fe80::2d0:f8ff:fe22:33ad, DR fe80::2d0:f8ff:fe22:34b3 Hello
period 30 seconds, Next Hello in 6 seconds
Triggered Hello period 5 seconds Secondary
addresses:
   3333::8888
   4444::4444
  Neighbors: fe80::2d0:f8ff:fe22:34b3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.39. show ipv6 pim sparse-mode local-members

Use this command to display the local MLD information on the PIM-SMv6 interface.

show ipv6 pim sparse-mode local-members [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	(Optional) Interface name. This command takes effect for all interfaces by default.

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the local MLD information on the PIM-SMv6 interface.

```
QTECH (config-if)#show ipv6 pim sparse-mode local-members PIM Local
```

```
membership information

GigabitEthernet 0/5:

  (*, ff66::6666) : Include
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.40. show ipv6 pim sparse-mode mroute

Use this command to display the PIM-SMv6 routing information.

show ipv6 pim sparse-mode mroute [*group-or-source-address* [*group-or-source-address*]]

Parameter Description

Parameter	Description
group-or-source-address	Group address or source address. Two addresses cannot both be the group addresses or the source addresses.

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

This command is used to display route information. Only one group IPv6 address, one source IPv6 address or one group IPv6 address-source IPv6 address pair can be configured at a time. You can also specify no group IP address or source IPv6 address.

Configuration Examples

Related Commands

Platform Description

N/A

Command	Description
N/A	N/A

N/A

7.41. show ipv6 pim sparse-mode neighbor

Use this command to display the neighbor information.

show ipv6 pim sparse-mode neighbor **[** detail **]**

Parameter Description

Parameter	Description
detail	(Optional) Displays the details of an interface.

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Configuration Examples

The following example displays the neighbor information..

```
QTECH# show ipv6 pim sparse-mode neighbor detail Nbr
fe80::2d0:f8ff:fe22:34b3 (GigabitEthernet 0/5) Expires in 86
seconds
  Secondary addresses:
   6666::6666
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.42. show ipv6 pim sparse-mode nexthop

Use this command to display the next hop information, including the interface ID, address and metric.

show ipv6 pim sparse-mode nexthop

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

N/A

Command	Description
N/A	N/A

N/A

7.43. show ipv6 pim sparse-mode rp mapping

Use this command to display the information on all RPs and the multicast groups they serve.

show ipv6 pim sparse-mode rp mapping

Parameter Description

Parameter	Description
mapping	All groups and RP information.

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the information on all RPs and the multicast groups they serve.

```
QTECH# show ipv6 pim sparse-mode rp mapping PIM Group-
to-RP Mappings
This system is the Bootstrap Router (v2) Group(s):
ff00::/8
  RP: 3333::1
    Info source: 3333::1, via bootstrap, priority 192 Uptime:
        00:12:40, expires: 00:01:50
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.44. show ipv6 pim sparse-mode rp-hash

Use this command to display the RP information corresponding to the group address.

show ipv6 pim sparse-mode rp-hash *ipv6-group-address*

Parameter Description

Parameter	Description
ipv6_group-address	IPv6 group address

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the RP information corresponding to the group address..

```
QTECH# show ipv6 pim sparse-mode rp-hash ff66::6666 RP:
3333::8888
Info source: 3333::8888, via bootstrap PIMv2 Hash
Value 126
RP 3333::8888, via bootstrap, priority 192, hash value 1468234650
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.45. show ipv6 pim sparse-mode track

Use this command to display the number of sent and received PIM packets during the period from the beginning of the statistics till now.

show ipv6 pim sparse-mode track

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

This command is used to display the number of sent and received PIM packets during the period from the beginning of the statistics till now.. When the system starts up, it sets the start time of the statistics. The start time of the statistics is reconfigured and the PIMv6 packet counter is cleared on calling the clear ipv6 pim sparse-mode track every time.

Configuration Examples

The following example displays the number of sent and received PIM packets during the period from the beginning of the statistics till now.

```
QTECH# show ipv6 pim sparse-mode track
PIMv6 packet counters track
Elapsed time since counters cleared: 00:04:03
                           received        sent
Valid PIMSMv6 packets:     0               8
Hello:                     0               8
Join-Prune:                0               0
Register:                  0               0
Register-Stop:             0               0
Assert:                    0               0
BSM:                       0               0
C-RP-ADV:                  0               0
PIMDMv6-Graft:             0
PIMDMv6-Graft-Ack:         0
PIMDMv6-State-Refresh:     0
Unknown PIMv6 Type:        0
Errors:
Malformed packets:                         0
Bad checksums:                                   0
Send errors:                                         0
Packets received with unknown PIMv6 version:   0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

8.1. clear ip igmp snooping gda-table

Use this command to clear the Group Destination Address (GDA) table.

clear ip igmp snooping gda-table

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

The IGMP Snooping GDA table contains VLAN IDs (VIDs), group addresses, routing interface (static or dynamic) ID, and member interface ID. Among them, the VID and group address identify a forwarding entry; the static routing interfaces will not age and cannot be deleted by using the **clear ip igmp snooping gda-table** command.

Configuration Examples

The following example clears the Group Destination Address (GDA) table.

```
QTECH# clear ip igmp snooping gda-table
```

Platform Description

N/A

8.2. clear ip igmp snooping statistics

Use this command to clear IGMP Snooping statistics.

clear ip igmp snooping statistics

Parameter Description

Parameter	Description

N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide
This command is used to clear the IGMP Snooping statistics, which can be displayed by using the **show**

ip igmp snooping statistics command.

Configuration Examples
The following example clears the IGMP Snooping statistics.

```
QTECH# clear ip igmp snooping statistics
```

Platform Description
N/A

8.3. deny

Parameter Description
Use this command to deny the forwarding of the multicast streams in the range specified by the profile.

deny

Parameter	Description
N/A	N/A

Defaults
The forwarding of the multicast streams in the range specified by the profile is denied.

Command Mode

Profile configuration mode

Usage Guide

First, configure the multicast range using the range command in the profile configuration mode. In addition, the profile must be applied to the interface in order to make the profile configuration take effect.

Configuration Examples

The following is an example of deny the forwarding of the multicast stream 224.2.2.2 to 224.2.2.244.

```
QTECH(config)# ip igmp profile 1
QTECH(config-profile)# range 224.2.2.2 224.2.2.244
QTECH(config-profile)# deny
```

Platform Description

N/A

8.4. ip igmp profile

Use this command to create a profile and enter the IGMP profile configuration mode. Use the **no** or **default** form of this command to restore the default setting.

ip igmp profile *profile-number*

no ip igmp profile *profile-number*

default ip igmp profile *profile-number*

Parameter Description

Parameter	Description
profile-number	Profile number, in the range from 1 to 1024

Defaults

No profile is created by default.

Command Mode

Global configuration mode

Usage Guide

The profile is a filter to permit/deny specified groups in the following steps:

- Use the **ip igmp profile** command to create a profile and enter profile configuration mode.
- Use the **range** command to define a profile range.
- Use the **permit** command to permit this profile in the filtering, or use the **deny** command to deny this profile in the filtering.
- If the **deny** command is used without any profile specified, all profiles in the profile are permitted.

- If the **permit** command is used without any profile specified, all profiles in the profile are denied.

Configuration Examples

The following example creates and permits profile 1 with addresses from 224.2.2.2 to 224.2.2.244.

```
QTECH(config)# ip igmp profile 1
QTECH(config-profile)# range 224.2.2.2 224.2.2.244
QTECH(config-profile)# permit
```

Platform Description

N/A

8.5. ip igmp snooping

Use this command to enable IGMP snooping and enter the IVGL mode.

ip igmp snooping ivgl

Use this command to enable IGMP snooping and enter the SVGL mode.

ip igmp snooping svgl

Use this command to enable IGMP snooping and enter the IVGL-SVGL mode.

ip igmp snooping ivgl-svgl

Use the **no** or **default** command to restore the default setting.

no ip igmp snooping default ip igmp snooping

Parameter Description

Parameter	Description
N/A	N/A

Defaults

IGMP Snooping is disabled by default.

Command Mode

Global configuration mode

Usage Guide

- **IVGL (Independent VLAN Group Learning):** In this mode, the multicast flows in different VLANs are independent. A host can only request multicast flows to the router interface in the same VLAN. Upon receiving the multicast flow in any VLAN, the switch forwards the flow to the member port in

the same VLAN.

- **SVGL (Shared VLAN Group Learning):** In this mode, the hosts in different VLANs share the

  same multicast flow. A host can request multicast flows across VLANs. By designating a Shared

  VLAN, you can only forward the multicast flows received in this Shared VLAN to other member

  ports in different VLANs. In the SVGL mode, IGMP Profile must be used to divide the multicast

  address range, within which the multicast flow can be forwarded across VLANs. By default, all

  group range is not within the SVGL range and all multicast flows are dropped. As shown in

  Figure-3:

- **IVGL-SVGL mode:** also known as promiscuous mode. In this mode, the IVGL mode and the SVGL

  mode can co-exist. Use IGMP Profile to divide a set of multicast address range to the SVGL, within

  which the member port of the multicast forwarding entry can be forwarded across VLANs and

  without which the member ports are forwarded in the same VLAN.

- For wireless products, only IVGL mode is supported. Use the **ip igmp snooping** command to

  enable IGMP Snooping in global configuration mode, and use the **igmp snooping** command in AP

  configuration mode.

SVGL mode and IVGL-SVGL mode conflict with the IP multicast function.

PIM Snooping must depend on either IVGL or IVGL-SVGL mode of IGMP Snooping. Use **no ip igmp snooping** command to disable IGMP Snooping after PIM Snooping is disabled.

Configuration Examples

```
QTECH(config)# ip igmp snooping ivgl
```

The following example enables IGMP Snooping and enters the IVGL mode.

```
QTECH(config)# ip igmp snooping svgl
QTECH(config)# ip igmp snooping svgl profile 1
```

The following example enables IGMP Snooping and enters the SVGL mode.

```
QTECH(config)# ip igmp snooping ivgl-svgl
QTECH(config)# ip igmp snooping svgl profile 1
```

The following example enables IGMP Snooping and enters the IVGL-SVGL mode.

```
QTECH(config)# ip igmp snooping
QTECH(ap-config)# igmp snooping
```

The following example enables IGMP Snooping on APs.

Platform Description

N/A

8.6. ip igmp snooping dyn-mr-aging-time

Use this command to set the aging time of a dynamic routing interface. Use the **no** or **default** form of this command to restore the default setting. **ip igmp snooping dyn-mr-aging-time** *seconds*

no ip igmp snooping dyn-mr-aging-time default ip igmp snooping dyn-mr-aging-time

Parameter Description

Parameter	Description
seconds	Aging time from 1 to 3,600 in the unit of seconds

Defaults

The default is 300 seconds.

Command Mode

Global configuration mode

Usage Guide

If a dynamic routing interface does not receive IGMP query packets or PIM hello packets before aged, this interface will be deleted.

When the dynamic routing interface learning function is enabled, this command sets the aging time of the routing interface. If the aging time is set too short, the routes may be added and deleted frequently.

Configuration Examples

The following example sets the aging time of the routing interface that the switch

learns dynamically to 100 seconds.

```
QTECH(config)# ip igmp snooping dyn-mr-aging-time 100
```

Platform Description

N/A

8.7. ip igmp snooping fast-leave enable

Use this command to enable the fast leave function.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping fast-leave enable no ip igmp snooping fast-leave enable

default ip igmp snooping fast-leave enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

After you execute this command to enable the fast-leave function, the system will remove the corresponding multicast group on the corresponding interface upon the receipt of the IGMP leave message.

Subsequently, when the system receives a specific group query packet, the system does not forward it to the corresponding interface. Leave packets refer to the IGMPv2 leave packets. The fast leave function applies to scenarios in which one interface is connected to only one host. This function saves bandwidth and resources.

Configuration Examples

The following example enables the fast leave function.

```
QTECH(config)# ip igmp snooping fast-leave
```

Platform Description

N/A

8.8. ip igmp snooping filter

Use this command to specify the profile for ports.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping filter *profile-number* **no ip igmp snooping filter** *profile-number* **default ip igmp snooping filter**

Use this command to specify the profile for VLANs.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping vlan *vlan-id* **filter** *profile-number*

no ip igmp snooping vlan ***vlan-id*** filter default ip igmp snooping vlan ***vlan-id*** filter

Parameter Description

Parameter	Description
profile-number	Profile number from 1 to 1024

Defaults

This function is disabled by default.

Command Mode

Global configuration mode/Interface configuration mode

Usage Guide

A specific profile must be created before association.

Configuration Examples

The following example specifies profile 1 for interface fastEthernet 0/1.

```
QTECH(config)# interface fastEthernet 0/1
```

```
QTECH(config-if)# ip igmp snooping filter 1
```

Platform Description

N/A

8.9. ip igmp snooping host-aging-time

Use this command to configure the aging time of IGMP dynamic ports. Use the **no** or **default** form of this command to restore the default setting. **ip igmp snooping host-aging-time** *seconds*

no ip igmp snooping host-aging-time default ip igmp snooping host-aging-time

Parameter Description

Parameter	Description
seconds	Aging time. The unit is second. The value ranges from 1 to 65,535.

Defaults
The default is 260 seconds.

Command Mode

Global configuration mode

Usage Guide

The aging time of a dynamic port is set by the system when the port receives an IGMP packet from the host for joining a certain IP multicast group.

When such an IGMP packet is received, the system resets the aging timer for the port. The duration of this timer is determined by **host-aging-time**. If the timer expires, the system determines that there is no host in this port for receiving multicast packets. The multicast device removes the port from the IGMP Snooping group. After the **ip igmp snooping host-aging-time** command is executed, the aging time will be determined by **host-aging-time**. This command takes effect only after the system receives the next IGMP packet. This command does not change the current aging time.

Configuration Examples

Related Commands

Platform Description

The following example sets the aging time to 30 seconds.

```
QTECH(config)# ip igmp snooping host-aging-time 30
```

Command	Description
N/A	N/A

N/A

8.10. ip igmp snooping l2-entry-limit

Use this command to set the maximum number of multicast groups.

Use the **no** or **default** form of this command to restore the default setting.

Parameter Description

ip igmp snooping l2-entry-limit *number*

no ip igmp snooping l2-entry-limit

default ip igmp snooping l2-entry-limit

Parameter	Description
number	Number of multicast groups. The value ranges from 0 to 65,536.

Defaults

The default is 65,536.

Command Mode

Global configuration mode

Usage Guide

The maximum number of multicast groups includes the multicast groups in all ports of all VLANs (including dynamic and static multicast groups). When the number of multicast groups reaches the limit, learning new group records and configuring new static multicast group ports are not allowed.

Configuration Examples

Related Commands

The following example sets the maximum number of multicast groups to 2000.

```
QTECH(config)# ip igmp snooping l2-entry-limit2000
```

Command	Description
show ip igmp snooping	Displays the maximum number of multicast groups.

Platform Description

N/A

8.11. ip igmp snooping limit-ipmc

Use this command to add a multicast source IP address check entry.

Use the **no** or **default** form of this command is used to delete a source IP checklist entry.

ip igmp snooping limit-ipmc vlan *vid* **address** *gaddress* **server** *saddress*

no ip igmp snooping limit-ipmc vlan *vid* **address** *gaddress*

default ip igmp snooping limit-ipmc vlan ***vid*** address ***gaddress***

Parameter Description

Parameter	Description
vid	VLAN ID
group-address	Multicast group address
source-address	Multicast source IP address

Defaults

Only source IP address check is enabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to filter the multicast packets. With it enabled, all multicast packets from illegal IP addresses will be discarded.

Source IP address check and multicast routing function cannot be enabled meanwhile.

Configuration steps:

1. Enable source IP address check and specify the source IP address.
2. (Optional) Specify the multicast group address and source IP address for a specific VLAN.

Configuration Examples

The following example enables source address check to receive multicast

packets only from 192.168.1.10 and allows packets into VLAN 2013 and VLAN 104 from (192.168.1.10 , 229.1.1.1).

```
QTECH# configure terminal
QTECH(config)# ip igmp snooping source-check default-server 192.168.1.10
QTECH(config)# ip igmp snooping limit-ipmc vlan 203 address 229.1.1.1 server
192.168.1.10
QTECH(config)# ip igmp snooping limit-ipmc vlan 204 address 229.1.1.1 server
192.168.1.10
QTECH(config)# end
```

Platform Description

N/A

8.12. ip igmp snooping max-groups

Use this command to configure the maximum number of groups that can be added dynamically to this interface.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping max-groups ***number*** no ip igmp snooping max-groups default ip igmp snooping max-groups

Parameter Description

Parameter	Description
number	The maximum group number from 0 to 1,024

Defaults

No maximum group number is configured by default.

Command Mode

Interface configuration mode

Usage Guide

If a maximum number of multicast groups are configured, the device will no longer receive and process IGMP Report messages when the number of multicast groups on this interface is beyond the range.

Configuration Examples

The following example configures the maximum number of multicast groups

to 100 on the megabit interface 0/1:

```
QTECH(config)# interface Ethernet 0/1
QTECH(config-if)# ip igmp snooping max-group 100
```

Platform Description

N/A

8.13. ip igmp snooping mrouter learn pim-dvmrp

Use this command to configure a device to listen to the IGMP Query/Dvmrp or PIM Help packets dynamically in order to automatically identify a routing interface

Use the **no** form of this command to disable the dynamic learning. Use the **default** form of this command to restore the default setting. **ip igmp snooping** [**vlan** *vid*] **mrouter learn pim-dvmrp**

no ip igmp snooping **[** vlan ***vid*** **]** mrouter learn pim-dvmrp default ip igmp snooping **[** vlan ***vid*** **]** mrouter learn pim-dvmrp

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults

This function is enabled by default.

Command Mode

Global configuration mode

Usage Guide

Routing interface is a port through which a multicast device (with IGMP Snooping enabled) is directly connected to a multicast neighbouring device (with multicast routing protocols enabled).

By default, the dynamic routing interface learning function is enabled. You can use the no form of this command to disable this function and clear all routing interfaces learnt dynamically. With dynamic routing interface learning function disabled globally, the function of all vlans will be disabled. Beside, with this function enabled globally, if the function of specified vlan is disabled, the dynamic routing interface learning function of the corresponding vlan is disabled. When the source port check function is enabled, only the multicast flow enters from the routing interface is legal and it is forwarded to the registered interface by the multicast equipment, the multicast flow from the non routing interface is considered to be the illegal and is discarded. With the source port check function enabled, the dynamic routing interface learning function will improve the application flexibility of IGMP snooping.

Configuration Examples

The following example enables the dynamic routing interface learning function on VLAN 1.

```
QTECH(config)# no ip igmp snooping mrouter learn pim-dvmrp
QTECH(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

Platform Description

N/A

8.14. ip igmp snooping preview

Use this command to allow the user to preview the specific multicast streams when the user doesn't have access to such multicast streams.

Use **no** or **default** form of this command to disable multicast preview.

ip igmp snooping preview *profile-number*

no ip igmp snooping preview default ip igmp snooping preview

Parameter Description

Parameter	Description
profile-number	Profile number (1-1024)

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Apply the IGMP Profile to a multicast preview function. When the user doesn't have access to the multicast streams (namely the user might be filtered by IGMP Snooping filter), it can allow the user to preview partial contents. This function shall be used in conjunction with IGMP Snooping filter or multicast control in order to realize effective multicast preview.

Configuration Examples

The following example associates the profile 2 to the Ethernet 0/1 and associates multicast preview with profile 1.

Platform Description

N/A

8.15. ip igmp snooping preview interval

Use this command to configure the interval that allows the user to preview the specific multicast streams when the user doesn't have access to such multicast streams.

Use **no** or **default** form of this command to restore the default setting.

ip igmp snooping preview interval ***seconds*** no ip igmp snooping preview interval defaut ip igmp snooping preview interval

Parameter Description

Parameter	Description
seconds	Preview interval from 1 to 300 in the unit of seconds

Defaults

The default is 60 seconds.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the multicast preview interval as 100 seconds on the 100M port of 0/1:

```
QTECH(config)# ip igmp snooping preview 1
QTECH(config)# ip igmp snooping preview interval 100
```

Platform Description

N/A

8.16. ip igmp snooping querier

Use this command to enable the IGMP querier.

Use no or default form of this command to restore the default setting.

ip igmp snooping [vlan *vid*] querier no ip igmp snooping [vlan *vid*] querier

default ip igmp snooping [vlan *vid*] querier

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults
This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

After globally enabling the IGMP querier, you must enable the IGMP querier function in VLAN to activate this function.

If the IGMP querier function is disabled globally, the IGMP querier will be disabled in all VLANs.

Configuration Examples

The following example enables the IGMP querier function in VLAN 2.

```
QTECH(config)# ip igmp snooping querier
QTECH(config)# ip igmp snooping vlan 2 querier
```

Platform Description

N/A

8.17. ip igmp snooping querier address

Use this command to specify a source IP address for IGMP querier.

Use **no** or **default** form of this command to remove the source IP address configured.

ip igmp snooping [**vlan** *vid*] **querier address** *a.b.c.d* **no ip igmp snooping** [**vlan** *vid*] **querier address default ip igmp snooping** [**vlan** *vid*] **querier address**

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.
a.b.c.d	Source IP address of the IGMP querier

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

After enabling IGMP querier, you msut configure a source IP address for the IGMP querier to activate this function..

If the IGMP querier source IP has been specified in VLAN, the source IP configured in the relevant VLAN will be used first.

Configuration Examples

The following example specifies the source IP of the IGMP querier as 1.1.1.1 on the device. QTECH(config)# ip igmp snooping querier address 1.1.1.1 The following example specifies the source IP of the IGMP querier as 1.1.1.1 in VLAN 3.

QTECH(config)# ip igmp snooping vlan 3 querier address 1.1.1.1

Platform Description

8.18. ip igmp snooping querier max-response-time

Use this command to configure the maximum response time of the IGMP querier. Use **no** or **default** form of this command to restore to the default setting.

ip igmp snooping **[** vlan ***vid*** **]** querier max-response-time ***seconds*** no ip igmp snooping **[** vlan ***vid*** **]** querier max-response-time default ip igmp snooping **[** vlan ***vid*** **]** querier max-response-time

Parameter Description

Parameter	Description
seconds	Maximum response time from 1 to 25 in the unit of seconds
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults

The default is 10 seconds.

Command Mode

Global configuration mode

Usage Guide

By default, the maximum response time is 10 seconds. If the maximum response time has been specified in the corresponding VLAN, the value specified in VLAN will be used first.

Configuration Examples

The following example specifies the maximum response time of the IGMP querier on the device.

```
QTECH(config)# ip igmp snooping querier max-response-time 15
```

The following example specifies the maximum response time of the IGMP querier in VLAN 3.

```
QTECH(config)# ip igmp snooping vlan 3 querier max-response-time15
```

Platform Description

N/A

8.19. ip igmp snooping querier query-interval

Use this command to specify the interval for IGMP querier to send query packets. Use **no** or **default** form of this command to restore the default setting.

ip igmp snooping **[** vlan ***vid*** **]** querier query-interval ***seconds*** no ip igmp snooping **[** vlan ***vid*** **]** querier query-interval default ip igmp snooping **[** vlan ***vid*** **]** querier query-interval

Parameter Description

Parameter	Description
seconds	Query interval from 1 to 18,000 in the unit of seconds
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults

The default is 60 seconds.

Command Mode

Global configuration mode

Usage Guide

If the query interval has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

Configuration Examples

The following example configures the query interval on the device.

```
QTECH(config)# ip igmp snooping querier query-interval100
```

The following example configures the query interval in VLAN 3.

```
QTECH(config)# ip igmp snooping vlan 3 querier query-interval100
```

Platform

N/A

Description

8.20. ip igmp snooping querier timer expiry

Use this command to specify the expiration timer for non-querier. Use **no** form of this command to restore the default setting.

ip igmp snooping [**vlan** *vid*] **querier timer expiry** *seconds* **ip igmp snooping** [**vlan** *vid*] **querier timer expiry** *seconds* **default ip igmp snooping** [**vlan** *vid*] **querier timer expiry**

Parameter Description

Parameter	Description
seconds	Theexpiration timer from 60 to 300 in the unit of seconds
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults
The default is 125 seconds.
Command Mode

Global configuration mode

Usage Guide

After globally enabling IGMP querier, if the device is elected as a non-querier, execute this command to change the expiration timer for non-querier.

If expiration timer has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

Configuration Examples

The following example configures the non-querier expiration timer on the device.

```
QTECH(config)# ip igmp snooping querier timer expiry 60
```

The following example configures the non-querier expiration timer in VLAN 3.

```
QTECH(config)# ip igmp snooping vlan 3 querier timer expiry 60
```

Platform Description

N/A

8.21. ip igmp snooping querier version

Use the following commands to specify IGMP Snooping querier version.

ip igmp snooping **[** vlan ***vid*** **]** querier version 1 ip igmp snooping **[** vlan ***vid*** **]** querier version 2 ip igmp snooping **[** vlan ***vid*** **]** querier version 3

Use **no** or **default** form of this command to restore to the default setting.

no ip igmp snooping **[** vlan ***vid*** **]** querier version default ip igmp snooping **[** vlan ***vid*** **]** querier version

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults

The default version is IGMPv2.

Command Mode

Global configuration mode

Usage Guide

If an IGMP querier version has been configured in a VLAN, the version specified in the VLAN will be used first.

Configuration Examples

The following example configures IGMP querier version on the device.

```
QTECH(config)# ip igmp snooping querier version 1
```

Platform Description

N/A

8.22. ip igmp snooping query-max-response-time

Use this command to specify the time for the switch to wait for the member join message after receiving the **query** message.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping query-max-response-time ***seconds*** no ip igmp snooping query-max-resposne-time default ip igmp snooping query-max-response-time

Parameter Description

Parameter	Description
seconds	The aging time of the routing inerface that the switch learns dynamically, in the range from 1 to 65.535

Defaults

The default is 10 seconds.

Command Mode

Global configuration mode

Usage Guide

You can specify the time for the switch to wait for the member join message after receiving the query message. If the switch does not receive the member join message in the specified time, it considers that the member has left and then deletes the member.

This command lets you adjust the waiting time after receiving the query message. This command takes effect only after the switch receives the next member join message. This command does not change the current wait time.

Configuration Examples

The following examples sets the aging time of the routing interface that the switch

learns dynamically to 100 seconds.

QTECH(config)# ip igmp snooping query-max-response-time*100*

Platform Description

N/A

8.23. ip igmp snooping source-check default-server

Use this command to enable the source IP address check to permit one or several IPMC flows from the server of the specified IP address.

Use the **no** or **default** form of this command is used to restore the default setting.

ip igmp snooping source-check default-server *source-address*

no ip igmp snooping source-check default ip igmp snooping source-check

Parameter Description

Parameter	Description
source-address	Default multicast source IP address

Defaults
This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

The source IP address check function takes effect globally. Once it is enabled, only the IPMC streams from the specified IP address are permitted.

Source IP address check and IP multicast function cannot work meanwhile.

The device allows users to configure the source IP address of all IPMC streams, called default multicast server. The default server must be set as long as the source IP address check function is enabled.

Configuration Examples

The following example enables the multicast source IP address check function.

```
QTECH# configure terminal
QTECH(config)# ip igmp snooping source-check default-server 192.168.1.10
QTECH(config)# ip igmp snooping limit-ipmc vlan 203 address 229.1.1.1 server
```

```
192.168.1.10
QTECH(config)# ip igmp snooping limit-ipmc vlan 204 address 229.1.1.1 server
192.168.1.10
QTECH(config)# end
```

Platform Description

N/A

8.24. ip igmp snooping source-check port

Use this command to enable the source port check function of IGMP Snooping. Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping source-check port no ip igmp snooping source-check port

default ip igmp snooping source-check port

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

The source port check function is used to permit one or several IPMC flows from the mroute port. When it is enabled, only the IPMC streams from the specified port are permitted. When it is disabled, all the IPMC streams are permitted and forwarded.

Configuration Examples

The following example enables the source port check function of IGMP Snooping.

```
QTECH(config)# ip igmp snooping source-check port
```

Platform Description

N/A

8.25. ip igmp snooping suppression enable

Use this command to enable IGMP snooping suppression.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping suppression enable

no ip igmp snooping suppression enable default ip igmp snooping suppression enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

When this function is enabled, IGMP Snooping only forwards the first report from a specific VLAN or group, and suppresses the following reports to constrain traffic in the networks.

This function is only supported on IGMPv1 and IGMPv2 reports.

Configuration Examples

The following example enables IGMP snooping suppression on the device.

```
QTECH(config)# ip igmp snooping suppression enable
```

Platform Description

N/A

8.26. ip igmp snooping svgl profile

Use this command to specify the multicast group address range applied in the SVGL/IVGL-SVGL mode. Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping svgl profile *profile-number*

no ip igmp snooping svgl profile default ip igmp snooping svgl profile

Parameter Description

Parameter	Description
profile-number	Profile number, in the range of 1-1,024

Defaults
No profile is associated.

Command Mode

Global configuration mode

Usage Guide

When the IGMP Snooping works in the SVGL and IVGL-SVGL mode, a profile shall be associated to specify the multicast group address range applied in the SVGL or IVGL-SVGL mode. That is to say, the member ports of the multicast forwarding entry can be forwarded across the VLANs while the member ports of the multicast forwarding entry in the other multicast address range must belong to the same VLAN.

Configuration Examples

The following example specifies the profile 2 applied in SVGL mode.

```
QTECH(config)# ip igmp snooping svgl profile 2
```

Platform Description

N/A

8.27. ip igmp snooping svgl subvlan

Use this command to specify the subvlan of multicast VLAN.

Parameter Description

Parameter	Description
vid-range	VLAN ID or range of VLAN ID

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping svgl subvlan [*vid-range*]

no ip igmp snooping svgl subvlan [*vid-range*]

default ip igmp snooping svgl subvlan [*vid-range*]

Defaults

By default, all VLANs except shared VLANs serve as its sub VLANs.

Command Mode

Global configuration mode

Usage Guide

This command only takes effect in SVGL and IVGL-SVGL mode.

Configuration Examples

The following example specifies VLAN 3 as the shared VLAN and VLAN 2,

VLAN 5 to 7 as the sub VLANs.

```
QTECH(config)# ip igmp snooping svgl vlan 3
QTECH(config)# ip igmp snooping svgl subvlan 2,5-7
```

Platform Description

N/A

8.28. ip igmp snooping svgl vlan

Use this command to specify the shared VLAN in SVGL mode. Use the no form of this command to restore the default setting. ip igmp snooping svgl vlan *vid*

no ip igmp snooping svgl vlan default ip igmp snooping svgl vlan

Parameter Description

Parameter	Description
vid	VLAN ID

Defaults

By default , the shared VLAN is VLAN 1.

Command Mode

Global configuration mode

Usage Guide

This command only works in the SVGL and IVGL-SVGL mode.

Configuration

The following example specifies VLAN 3 as the shared VLAN and VLAN 2, VLAN 5 to 7 as the sub

Examples

VLANs.

```
QTECH(config)# ip igmp snooping svgl vlan 3
QTECH(config)# ip igmp snooping svgl subvlan 2,5-7
```

Platform Description

N/A

8.29. ip igmp snooping tunnel

Use this command to enable 802.1Q tunneling (QinQ) support for IGMP Snooping. Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping tunnel no ip igmp snooping tunnel

default ip igmp snooping tunnel

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled.

Command Mode

Global configuration mode

Usage Guide

After IGMP Snooping is enabled and dot1q-tunnel port is configured on the device, IGMP packets received from dot1q-tunnel port will be handled in two ways:

- First: QinQ transmits IGMP packets transparently. Create multicast entries in the VLAN to which the IGMP packets belong, and forward IGMP packets in the VLAN.
- For example: It is assumed that IGMP Snooping has been enabled on the device; Port A is a dot1q-tunnel port; the default VLAN of Port A is VLAN 1, and packets from VLAN 1 and VLAN 10 are allowed by Port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 10 and forward the multicast requests to the router port of VLAN 10.
- Second: Create multicast entries in the default VLAN to which the dot1q-tunnel ports belong, and forward multicast packets in the default VLAN of dot1q-tunnel port after inserting the VLAN Tag of the default VLAN of dot1q-tunnel port.

- For example: It is assumed that IGMP Snooping has been enabled on the device; Port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 are allowed Port A. When multicast requests of VLAN 10 are sent to Port A, IGMP Snooping will create the multicast entry of VLAN 1 and insert the VLAN Tag of VLAN 1 into multicast requests before forwarding the multicast requests to the router port of VLAN 1.
- By default, the second way is used.

Configuration
The following example enables QinQ support for IGMP Snooping.

Examples
```
QTECH(config)# ip igmp snooping tunnel
```

Platform Description

N/A

8.30. ip igmp snooping vlan

Use this command to enable the IGMP Snooping in the specified VLAN and enter IVGL mode. Use the **no** form of this command is used to disable the IGMP Snooping.

Use the **default** form of this command to restore the default setting.

ip igmp snooping vlan ***vid***

no ip igmp snooping vlan *vid*

default ip igmp snooping vlan *vid*

Parameter Description

Parameter	Description
vid	VLAN ID in the range from 1 to 4,094

Defaults
IGMP Snooping is disabled by default.

Command Mode

Global configuration mode

Usage Guide
Use this command to enable or disable the IGMP snooping on the specified vlan.

The PIM Snooping in the specified VLAN works only when IGMP Snooping is configured. To disable PIM Snooping, you must disable IGMP Snooping in the VLAN first, or disabling will fail and be prompted.

Configuration Examples

The following example enters IVGL mode and disables the IGMP Snooping in the VLAN 2.

```
QTECH(config)# ip igmp snooping ivgl
QTECH(config)# no ip igmp snooping vlan 2
```

Platform Description

N/A

8.31. ip igmp snooping vlan mrouter interface

Use this command to configure a static routing interface.

Use the **no** form of this command to delete a static routing interface. Use the **default** form of this command to restore the default setting.

ip igmp snooping vlan *vid* **mrouter interface** *interface-type interface-number*

no ip igmp snooping vlan *vid* **mrouter interface** *interface-type interface-number*

default ip igmp snooping vlan *vid* mrouter interface *interface-type interface-number*

Parameter Description

Parameter	Description
vid	VLAN ID in the range from 1 to 4,094
interface-type interface-number	Interface ID

Defaults

No static routing interface is configured by default.

Command Mode

Global configuration mode

Usage Guide

A dynamic routing interface is learned dynamically through IGMP Snooping. A static routing interface is configured by using this command and cannot age.

When an interface is configured as a static routing interface, all multicast streams received on this interface will be forwarded.

When the source port check function is enabled, only the multicast flows from the routing interface are forwarded, and other flows will be discarded.

Configuration Examples

The following example configures a static routing interface.

```
QTECH(config)# ip igmp snooping vlan 1 mrout erinterface fastEthernet0/1
```

Platform Description

N/A

8.32. ip igmp snooping vlan static interface

Use this command to configure a static member interface of a multicast group.

Use the **no** form of this command to delete a static member interface from a multicast group. Use the **default** form of this command to restore the default setting.

ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*

no ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*

default ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*

Parameter Description

Parameter	Description
vid	VLAN ID in the range from 1 to 4,094
ip-addr	Multicast IP address
interface-id	Interface ID

Defaults

No static member interface of any multicast group is configured by default.

Command Mode

Global configuration mode

Usage Guide

The IGMP Snooping GDA table contains VLAN IDs (VIDs), group addresses, routing interface (static or dynamic) ID, and member interface ID. Among them, the VID and group address identify a forwarding entry; the static routing interfaces will not age and cannot be deleted by using the **clear ip igmp snooping gda-table** command.

Configuration Examples

```
QTECH(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface
GigabitEthernet 0/1
```

The following example configures a static member interface for the multicast group 224.1.1.1.

Platform Description

N/A

8.33. permit

Use this command to permit the multicast forwarding for specified ranges of a specified profile.

permit

Parameter Description

Parameter	Description
N/A	N/A

Defaults
The forwarding of the multicast streams in the range specified by the profile is denied.

Command Mode

Profile configuration mode

Usage Guide

A profile is used to filter a group of multicast packets, so as to assist other features.

Configuration steps:

1. Use the **ip igmp profile** command to create a profile and enter profile configuration mode.
2. Use the **range** command to define a range for the profile.
3. Use the **permit** command to permit the multicast forwarding for the profile.

Configuration Examples

The following example permits the forwarding of the multicast streams from 224.2.2.2 to 224.2.2.244 of profile 1.

```
QTECH(config)# ip igmp profile 1
QTECH(config-profile)# range 224.2.2.2 224.2.2.244
QTECH(config-profile)# permit
```

Platform Description

N/A

8.34. range

Parameter Description

Use this command to define a range for a specific profile.

Use the **no** form of the command to remove the range from the profile.

range *low-ip-address* [*high-ip-address*]

no range *low-ip-address* [*high-ip-address*]

Parameter	Description
low-ip-address	Start address of a range
high-ip-address	End address of a range

Defaults

No range is defined for a profile by default.

Command Mode

Profile configuration mode

Usage Guide

A profile is used to filter a group of multicast packets, so as to assist other features.

Configuration steps:

3. Use the **ip igmp profile** command to create a profile and enter profile configuration mode.
4. Use the **range** command to define a range for the profile.
5. Use the **permit** command to permit the multicast forwarding for the profile.

Configuration Examples

The following is an example of allowingpermits the forwarding of the multicast streams from 224.2.2.2 to 224.2.2.244: of profile 1.

```
QTECH(config)# ip igmp profile 1
QTECH(config-profile)# range 224.2.2.2 224.2.2.244224.2.2.2
QTECH(config-profile)# permit
```

Platform Description

N/A

8.35. show ip igmp profile

Use this command to display the profile information.

show ip igmp profile *profile-number*

Parameter Description

Parameter	Description
profile-number	Displays configuration information of the designated profile.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the profile information.

Configuration Examples

The following example displays the profile information.

```
QTECH(config-if)# show ip igmp profile Profile 1
Permit
range 224.0.1.0, 239.255.255.255
```

8.36. show ip igmp snooping

Use this command to display related information of IGMP Snooping.

show ip igmp snooping [**gda-table** | **interfaces** *interface-type interface-number* | **mdevice**| **statistics**

[**vlan** *vlan-id*] | **querier** [**detail | vlan** *vid*] | **user-info**]

Par ameter Description

Parameter	Description
vlan *vid*	VLAN ID. By defualt, IGMP Snooping information of all VLANs are displayed.
interface-type *interface-number*	Interface type and number

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide
N/A

Configuration Examples

The following example displays global IGMP Snooping information.

```
QTECH#show ip igmp snooping IGMP Snooping
running mode: IVGL
IGMP Snooping L2-entry-limit: 65536 Source
port check: Disable
Source ip check: Disable IGMP
Fast-Leave: Disable
IGMP Report suppress: Disable IGMP
Global Querier: Disable IGMP Preview:
Disable
IGMP Tunnel: Disable IGMP
Snooping version: 2
IGMP Snooping version: 2IGMP Preview group aging time : 60(Seconds)

Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)

QTECH#show ip igmp snooping vlan 1 IGMP Snooping running mode: IVGL IGMP
Snooping L2-entry-limit: 65536 Global IGMPv2 Fast-Leave :Disable
Global multicast router learning mode :Enable Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
```

```
Vlan 1

IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp IGMP Fast-Leave: Disable
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
```

The following example displays VLAN1 IGMP Snooping information.

Platform Description

N/A

9. MLD SNOOPING COMMANDS

9.1. clear ipv6 mld snooping gda-table

Use this command to clear the forwarding table information learned dynamically.

clear ipv6 mld snooping gda-table

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to clear the forwarding table information learned dynamically.

Configuration Examples

Related Commands

Platform Description

The following example clears the forwarding table information learned dynamically:

```
QTECH# clear ipv6 mld snooping gda-table
```

Command	Description
N/A	N/A

N/A

9.2. clear ipv6 mld snooping statistics

Use this command to clear the MLD Snooping statistics, including the entry number, the entry volume, the number of various received packets, the group information and the interface information of the corresponding group.

clear ipv6 mld snooping statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide
Use the **show ipv6 mld snooping statistics** command to verify the configuration.

Configuration Examples

Related Commands

Platform Description

The following example clears the MLD Snooping statistics.

```
QTECH# clear ipv6 mld snooping statistics
```

Command	Description
N/A	N/A

N/A

9.3. deny

Parameter Description

Parameter	Description
N/A	N/A

Use this command to prevent the multicast flow profile within the specified range from being forwarded in the profile configuration mode.

deny

Defaults

The default profile action is **deny**.

Command Mode

Profile configuration mode

Usage Guide

Profile is a kind of group “filter” that can be referred to by other functions.

Configuration Steps:

Use the **ipv6mld profile** command to create a profile and enter the profile mode.

Use the **range** command to define a group.

Use the **permit** command to allow this group to pass the filtering; Use the **deny** command to filter the packets of this group. The default command is **deny**.

Configuration Examples

```
QTECH(config)# ipv6 mld profile 1 QTECH(config-profile)# range FF15::1 FF15::100
QTECH(config-profile)# deny
```

The following example prevents the multicast flow profile within the range from FF15::1 to FF15::100 from being forwarded.

Related Commands

Command	Description
ipv6 mld profile	Creates one profile.
range	Sets the multicast address range.
permit	Sets the profile action permit.

Platform Description

N/A

9.4. ipv6 mld profile

Use the following command to create a profile.

Use the no or default form of this command to delete a profile.

ipv6 mld profile *profile-number*

no ipv6 mld profile *profile-number*

default ipv6 mld profile *profile-number*

Parameter Description

Parameter	Description
profile-number	Profile number, in the range from 1 to 1024.

Defaults
N/A

Command Mode
Global configuration mode

Usage Guide
Profile is a kind of group “filter” that can be referred to by other functions.

Configuration Steps:

1. Use the **ipv6mld profile** command to create a profile and enter the profile mode.
2. Use the **range** command to define a group.
3. Use the **permit** command to allow this group to pass the filtering; Use the **deny** command to filter the packets of this group. The default command is **deny**.

Configuration Examples
The following example creates profile 1 and allows the packets sent by devices with MAC address ranging from FF15::1 to FF15::100 to pass the filtering.

```
QTECH(config)#ipv6 mld profile 1
QTECH(config-profile)#range FF15::1 FF15::100 QTECH(config-profile)#permit
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

9.5. ipv6 mld snooping

Use this command to enable MLD Snooping and specify IVGL/SVGL/IVGL-SVGL mode.

Use the no or default form of this command to restore the default setting.

ipv6 mld snooping {ivgl | svgl | ivgl-svgl} no ipv6 mld snooping [ivgl | svgl | ivgl-svgl]

default ipv6 mld snooping [ivgl | svgl | ivgl-svgl]

Parameter Description

Parameter	Description
ivgl	MLD Snooping is running IVGL mode.
svgl	MLD Snooping is running SVGL mode.
ivgl-svgl	MLD Snooping is running IVGL-SVGL mode.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

In IVGL mode, multicast flow in each VLAN is independent. The host only requests multicast flow from the routing interface within the same VLAN. The device forwards the multicast flow from any VLAN to the member port within the same VLAN.

- In SVGL mode, multicast flow is shared among VLANs. The host can request multicast flow across VLANs. Shared VLAN (VLAN 1 by default) should be specified. Only multicast flow from Shared VLAN can be forwarded to all member ports within the group address range, which may belong to different VLANs. Profile is used to

specify a group range for SVGL. Only multicast flow within this range can be forwarded across VLANs. The other multicast flow is discarded.

- In IVGL-SVGL mode, Profile is used to specify a group range for SVGL. Multicast flow within this range is in SVGL mode and the other multicast flow is in IVGL mode.
- IPv6 multicast packets cannot be forwarded through SuperVLAN.

Configuration Examples

The following example enables MLD Snooping IVGL mode.

QTECH(config)# ipv6 igmp snooping ivgl

The following example enables MLD Snooping SVGL mode and specifies the shared VLAN and SVGL group range as VLAN1 and profile1 respectively.

```
QTECH(config)# ipv6 igmp snooping svgl
QTECH(config)# ipv6 igmp snooping svgl profile 1
```

Related Commands

Command	Description
N/A	N/A

Platform
N/A

Description

9.6. ipv6 mld snooping dyn-mr-aging-time

Use this command to set the aging time of the dynamic multicast route port. Use the **no** or **default** form of this command to restore the default setting. **ipv6 mld snooping dyn-mr-aging-time** *second*

no ipv6 mld snooping dyn-mr-aging-time default ipv6 mld snooping dyn-mr-aging-time

Parameter Description

Parameter	Description
second	Sets the aging time of the dynamic multicast route port, in the range from 1 to 3,600 in the unit of seconds.

Defaults

The default is 300 seconds.

Command Mode

Global configuration mode.

Usage Guide The switch will remove the dynamic multicast router interface from the router interface list if it fails to receive the MLD general group query packets or the ipv6 PIM Hello packets within the aging timeout on this interface. Use this command to change the aging time of the routing ports learned dynamically. If the aging time is too short, routing ports will be added and deleted frequently.

By default, the dynamic learning of routing ports is enabled. If learning fails, use the **show run** command to check whether this function is enabled.

Configuration Examples

Related Commands

Platform Description

The following example sets the aging time of the dynamic multicast routing port to 100 seconds.

```
QTECH(config)# ipv6 mld snooping dyn-mr-aging-time 100
```

Command	Description
N/A	N/A

N/A

9.7. ipv6 mld snooping fast-leave enable

Use this command to enable the MLD Snooping fast-leave function.

Use the **no** or **default** form of this command to restore the default setting.

Parameter Description

ipv6 mld snooping fast-leave enable

no ipv6 mld snooping fast-leave enable default ipv6 mld snooping fast-leave enable

Defaults

This function is disabled by default.

Parameter	Description
N/A	N/A

Command Mode

Global configuration mode.

Usage Guide

The interface fast leave is that when IPv6 MLD Leave packets sent from the host are received on an interface, the interface is removed form the outgoing interface list of the corresponding forwarding entry. Then, the switch will not forward the received IPv6 MLD specific group query packets to the interface.If there is only one receiver connected with the interface, enable the interface fast leave function to save the bandwidth and resources.

Configuration Examples

Related Commands

Platform Description

The following example enables mld snooping fast-leave.

```
QTECH(config)# ipv6 mld snooping fast-leave
```

Command	Description
N/A	N/A

N/A

9.8. ipv6 mld snooping filter

Use this command to filter the specific multicast flows.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping filter *profile-number*

no ipv6 mld snooping filter default ipv6 mld snooping filter

Parameter Description

Parameter	Description
profile-number	Sets the profile number in the range from 1 to 1024.

Defaults
This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

You can configure an MLD Profile on an interface. If the MLD Report packets are received on the interface, the layer-2 device will determine whether the multicast address to be joined the interface is within the allowed range of the MLD Profile. The specified profile must be created before using this command.

Configuration Examples

The following example associates profile1 with the interface GigabitEthernet 0/1.

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if-GigabitEthernet 0/1)# ipv6 mld snooping filter 1
```

Related Commands

Command	Description
ipv6 mld profile	Creates a profile.

Platform Description

N/A

9.9. ipv6 mld snooping host-aging-time

Use this command to set the aging time of the dynamic member port. Use the **no** form of this command to cancel this configuration.

Use the **default** form of this command to restore the default setting.

ipv6 mld snooping host-aging-time ***seconds*** no ipv6 mld snooping host-aging-time default ipv6 mld snooping host-aging-time

Parameter Description

Parameter	Description
seconds	Sets the aging time of the dynamic member port, in seconds, ranging from 1-65,536 in the unit of seconds.

Defaults
The default aging time of the dynamic member port is 260 seconds.

Command Mode
Global configuration mode

Usage Guide

The switch will remove the dynamic multicast router interface from the router interface list if it fails to receive the MLD general group query packets or the IPv6 PIM Hello packets within the aging timeout on this interface.
When the MLD Snooping is enabled, the port that receives the MLD Report packet will learn to be a dynamic member port. The default aging time of such dynamic member port is 260 seconds. You can use this command to adjust the aging time. This configuration takes effect after the port receives the the next Report packet. The aging time of the dynamic member port should be longer than the query interval.

Configuration Examples

Related Commands

Platform Description

The following example sets the aging time of the dynamic member port to 30 seconds:

```
QTECH(config)# ipv6 mld snooping host-aging-time 30
```

Command	Description
N/A	N/A

N/A

9.10. ipv6 mld snooping max-groups

Use this command to set the maximum group allowed to join the interface dynamically. Use the no or default form of this command to restore the default setting.

ipv6 mld snooping max-groups *number* no ipv6 mld snooping max-groups default ipv6 mld snooping max-groups

Parameter Description

Parameter	Description
number	The number of groups, in the range from 0 to 65,536

Defaults
The default is 65,536.

Command Mode

Interface configuration mode

Usage Guide

With this command configured, when the group number exceeds the specified range on the interface, the switch will not receive and deal with the MLD Report packets.

The multicast groups are counted based on VLANs of an interface. If the interface has 3 VLANs, the counting result is 3 instead of 1 when an FF15::100 multicast request is received by all the VLAN.

Configuration Examples

The following example sets the maximum 100 multicast group on the interface GigabitEthernet 0/1.

```
QTECH(config)# interface gigabitEthernet 0/1
QTECH(config-if-GigabitEthernet 0/1)# ipv6 mld snooping max-groups 100
```

Related Commands

Command	Description
ipv6 mld snooping filter	Filters the multicast group on the interface.

Platform Description

N/A

9.11. Ipv6 mld snooping mrouter learn

Use this command to enable the switch to dynamically learn MLD query or PIM packets to identify the mrouter interface automatically.

Use the **no** form of this command to disable this function.

Use the **default** form of this command to restore the default setting.

ipv6 mld snooping **[** vlan ***vid*** **]** mrouter learn no ipv6 mld snooping **[** vlan ***vid*** **]** mrouter learn

default ipv6 mld snooping [**vlan** *vid*] **mrouter learn**

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID, in the range from 1 to 4094

Defaults

This function is enabled by default.

Command Mode

Global configuration mode

Usage Guide

The routing interface is the interface of the multicast device connected with the peer device. By default, the dynamically learned routing interface is enabled on the layer-2 multicast device. Use the **no** option to disable this function and clear all dynamically-learned routing interfaces.

With the source port check enabled, only the multicast flow through the mroute interface are valid and forwarded to the registered interface on the layer-2 multicast device. Those multicast flow

through the non-mroute interface are invalid and will be discarded.

Configuration Examples

The following example enables the dynamic multicast routing port learning function for VLAN1.

```
QTECH(config)# no ipv6 mld snooping mrouter learn
QTECH(config)# ipv6 mld snooping vlan 1 mrouter learn
```

Related Commands

9.12. ipv6 mld snooping query-max-response-time

Use this command to set t the maximum response time of the MLD general query packet. Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping query-max-response-time ***seconds***

no ipv6 mld snooping query-max-response-time

default ipv6 mld snooping query-max-response-time

Parameter Description

Parameter	Description
seconds	Sets the maximum response time of the MLD general query packet in the range from 1 to 65,535 in the unit of seconds.

Defaults
The default is 10 seconds.

Command Mode

Global configuration mode

Usage Guide

Upon receiving the MLD general query packets, the Layer-2 multicast device updates the aging timer of all member ports. The time of the timer is the longest response value. When the timer value decreases to 0, it indicates that there is no member receiving the multicast flow on the interface, and the Layer-2 device removes this interface from the MLD Snooping forwarding list.

Upon receiving the MLD specific group query packets, the Layer-2 multicast device enables the aging timer of all member ports in this specific group. The time of the timer is the longest response value. When the timer value decreases to 0, it indicates that there is no member receiving the multicast flow on the interface, and the Layer-2 device removes this interface from the MLD Snooping forwarding list.

For the source query packets of the MLD specific group, the timer is not updated.

The configured maximum response time is effective after another query packet is received.

Configuration Examples

Related Commands

Platform Description

The following example sets the maximum response time of the MLD general query packet to 100 seconds.

```
QTECH(config)# ipv6 mld snooping query-max-response-time100
```

Command	Description
N/A	N/A

N/A

9.13. ipv6 mld snooping source-check port

Use this command to enable the MLD source-check port.

Use the no or default form of this command to restore the default setting.

ipv6 mld snooping source-check port

no ipv6 mld snooping source-check port default ipv6 mld snooping source-check port

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The source-check port is disabled by default.

Command Mode

Global configuration mode

Usage Guide

The MLD Snooping source port check function is to limit the MLD multicast flow through the interace strictly. With the source port check disabled, all video flow are illegal and forwarded to the registered member port according to the MLD Snooping forwarding list. With the MLD Snooping source port check enabled, only the mulitcast flow through the mroute interface is legal and forwarded to the registered interface by the layer-2 multicast device; and the multicast flow through the non-mroute interface are illegal and discarded.

This command is used to enabled the source port check globally. Once this function is enabld, all multicast flow must come from the mroute interface, or they'll be discarded.

Configuration Examples

Related Commands

Platform Description

The following example enables MLD Snooping source-check port.

```
QTECH(config)# ipv6 mld snooping source-check port
```

Command	Description
N/A	N/A

N/A

9.14. ipv6 mld snooping suppression enable

Use this command to enable the MLD Snooping suppression.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping suppression enable no ipv6 mld snooping suppression enable

default ipv6 mld snooping suppression enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The MLD Snooping suppression function is disabled by default.

Command Mode

Global configuration mode.

Usage Guide

Configuration Examples

Related Commands

Platform Description

The following example enables MLD Snooping suppression.

```
QTECH(config)# ipv6 mld snooping suppression enable
```

Command	Description
N/A	N/A

N/A

9.15. ipv6 mld snooping svgl profile

Use this command to specify the group address range to be in the SVGL mode. Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping svgl profile *profile-number*

no ipv6 mld snooping svgl profile default ipv6 mld snooping svgl profile

Parameter Description

Parameter	Description
profile-number	Sets the profile number, in the range from 1 to 1024.

Defaults
No profiles are associated with SVGL by default.

Command Mode

Global configuration mode

Usage Guide

With the SVGL mode or IVGL-SVGL mode configured for the MLD Snooping working mode, a profile shall be associated with the IVGL for the purpose of specifying the group address range in the SVGL mode. That is to say, the member port of the multicast forwarding entry can be forwarded across the VLANs, while the member ports of the corresponding multicast forwarding entries within other multicast address range must belong to the same VLAN. By default, no profile is associated, which means that apply no multicast group in the SVGL mode.

Configuration Examples

The following example specifies the SVGL mode application range as the profie 2 group address range.

Related Commands

Platform Description

```
QTECH(config)# ipv6 mld snooping svgl profile 2
```

Command	Description
ipv6 mld snooping ivgl	Enables the MLD Snooping and set the ivgl mode.
ipv6 mld snooping ivgl-svgl	Enables the MLD Snooping and set the ivgl-svgl mode.

N/A

9.16. ipv6 mld snooping svgl vlan

Use this command to specify the shared VLAN in MLD Snooping SVGL mode. Use the **no** or **default** form of this command to restore the default setting. **ipv6 mld snooping svgl vlan** *vid*

no ipv6 mld snooping svgl vlan default ipv6 mld snooping svgl vlan

Parameter Description

Parameter	Description
vid	The VLAN ID, in the range from 1 to 4094.

Defaults
The default is 1.

Command Mode

Global configuration mode

Usage Guide

This command is used to specify the SVGL shared VLAN if MLD Snooping is running in SVGL or IVGL-SVGL mode.

Configuration Examples

Related Commands

Platform Description

The following example sets the shared VLAN in MLD Snooping SVGL mode to 5.

```
QTECH(config)# ipv6 mld snooping svgl vlan 5
```

Command	Description
N/A	N/A

N/A

9.17. ipv6 mld snooping vlan

Use this command to enable the MLD Snooping function for the specified VLAN. Use the **no** form of this command to disable this function.

Use the **default** form of this command to restore the default setting.

ipv6 mld snooping vlan ***vid***

no ipv6 mld snooping vlan *vid*

default ipv6 mld snooping vlan *vid*

Parameter Description

Parameter	Description
vid	VLAN ID, in the range from 1 to 4094.

Defaults

The MLD Snooping function is enabled by default.

Command Mode

Global configuration mode

Usage Guide

By default, the MLD Snooping is enabled in all VLANs. You can disable the MLD Snooping for the specified VLAN.

Configuration Examples

The following example disables the MLD Snooping function in VLAN 2 in IVGL mode.

```
QTECH(config)# ipv6 mld snooping ivgl
QTECH(config)# no ipv6 mld snooping vlan 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

9.18. ipv6 mld snooping vlan mrouter interface

Use this command to set the static mrouter interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping vlan *vid* **mrouter interface** *interface-type interface-number*

no ipv6 mld snooping vlan *vid* **mrouter interface** *interface-type interface-number*

default ipv6 mld snooping vlan *vid* **mrouter interface** *interface-type interface-number*

Parameter Description

Parameter	Description
vid	VLAN ID, in the range from 1 to 4094.
interface-type interface-number	The interface number

Defaults

No static mrouter interface is configured by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to set the static mrouter interface for the purpose that all IPv6 multicast data received on the switch can be forwarded. With the source port check function enabled, only the multicast flow through the mroute interface can be forwarded.

Configuration Examples

Related Commands

Platform Description

The following example sets a multicast routing port.

```
QTECH(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitEthernet 0/1
```

Command	Description
ipv6 mld snooping source-check port	Sets the multicast source port check.

N/A

9.19. ipv6 mld snooping vlan static interface

Use this command to set a static member port to receive the multicast flow for the purpose of preventing the port from being influenced by the MLD Report packets with the MLD Snooping enabled.

Uses the no form of this command to restore the default setting.

ipv6 mld snooping vlan *vid* static *group-address* interface *interface-type interface-number*

no ipv6 mld snooping vlan *vid* static *group-address* interface *interface-type interface-number*

Parameter Description

Parameter	Description
vid	VLAN ID, in the range from 1 to 4094. The default is 1.

group-address	The multicast address
interface-type *interface-number*	The interface number

Defaults
No static member port is configured by default.

Command Mode
Global configuration mode

Usage Guide
Use this command to set the interface as the member port of multiple static multicast addresses.

Configuration Examples
The following example sets the interface gigabitEthernet 0/1 as the static member port of the FF88::1 group.

Related Commands

Command	Description
ipv6 mld snooping vlan mrouter interface	Sets the mrouter interface.

Platform Description

N/A

9.20. permit

Use this command to allow the multicast flow profile within the specified range in the profile configuration mode.

permit

Parameter Description

Parameter	Description

N/A	N/A

Defaults
The default profile action is **deny**.

Command Mode
Profile configuration mode

Usage Guide
Before configuring this command, use the **range** command to set the multicast range first.

Configuration Examples
The following example allows the multicast flow profile within the range from FF15::1 to FF15::100 to be forwarded only.

```
QTECH(config)# ipv6 mld snooping profile 1 QTECH(config-profile)# range FF15::1 FF15::100
QTECH(config-profile)# permit
```

Related Commands

Command	Description
ipv6 mld profile	Creates one profile.
range	Sets the multicast address range.
deny	Sets the profile action deny.

Platform Description

N/A

9.21. range

Parameter Description
Use this command to specify the profile multicast flow range, which can be one single multicast address, or can be the multicast address within the specified range when configuring a profile in the profile configuration mode.
range *low-ipv6-address* [*high-ip-address*]

Parameter	Description

low-ip-address	The low address within the specified range
high-ip-address	The high address within the specified range

Defaults
No range is defined by default.

Command Mode

Profile configuration mode

Usage Guide

The value of low-ipv6-address shall be smaller than the one of high-ipv6-address. With the address range configured, an action shall be specified, and the default profile action is deny.

Configuration Examples

he following example creates the multicast flow profile within the range from FF15::1 to FF15::100.

```
QTECH(config)# ipv6 mld snooping profile 1 QTECH(config-profile)# range FF15::1 FF15::100
QTECH(config-profile)# permit
```

Related Commands

Command	Description
ipv6 mld profile	Creates one profile.
deny	Sets the profile action deny.
permit	Sets the profile action permit.

Platform Description

N/A

9.22. show ipv6 mld profile

Use this command to display the related MLD profile configuration.

show ipv6 mld profile *profile-number*

Parameter Description

Parameter	Description
profile-number	Profile number in the range from 1 to 1024

Defaults

N/A

Command Mode

Privileged EXEC

mode/Global configuration mode/Interface configuration mode

Usage Guide

Use this command to display the related MLD profile configuration.

Configuration Examples

The following example displays the MLD profile configuration.

```
QTECH# show ipv6 mld profile ipv6 mld profile  1
permit
range FF15::1 FF15::100
ipv6 mld profile
deny
range FF88::1  FF88::100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

9.23. show ipv6 mld snooping

Use this command to display the related MLD Snooping information.

show ipv6 mld snooping [gda-table | interfaces *interface-type interface-number* | mrouter |statistics [vlan *vid*] | vlan *vid*]

Parameter Description

Parameter	Description
gda-table	Displays the multicast forwarding rule table.
Interfaces *interface-type* *interface-number*	Displays the MLD Snooping filtering configuration.
mrouter	Displays the information about mrouter interface.
statistics	Displays the MLD Snooping statistics.
vlan *vlan-id*	Displays the MLD Snooping information of the specified vlan.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Use this command to display the related MLD Snooping information.

Configuration Examples

The following example displays the MLD Snooping configurations.

In IVGL mode:

```
QTECH#show ipv6 mld snooping MLD-snooping mode: IVGL Source port check: Disable MLD Fast-Leave: Disable
MLD Report suppress: Disable
Query Max Response Time: 10 (Seconds) Dynamic Mroute Aging Time: 300(Seconds) Dynamic Host Aging Time: 260(Seconds)

vlan 1

MLD Snooping state: Enabled
Multicast router learning mode: Enable MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC
```

```
In SVGL mode:
QTECH#show ipv6 mld snooping MLD-snooping mode: SVGL
SVGL vlan: 1
SVGL profile number: 1 Source port check: Disable MLD Fast-Leave: Disable
MLD Report suppress: Disable
Query Max Respone Time: 10 (Seconds) Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)

In IVGL-SVGL mode: QTECH#show ipv6 mld snooping MLD-snooping mode: IVGL-SVGL
SVGL
 vlan: 1
SVGL profile number: 1 Source port check: Disable MLD Fast-Leave: Disable
MLD Report suppress: Disable
Query Max Respone Time: 10 (Seconds) Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)

vlan 1

MLD Snooping state: Enabled
Multicast router learning mode: Enable MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

10.1. clear ip msdp peer

Use this command to clear specific MSDP peer. This will clear the connection to the MSDP peer and then reestablish the connection to MDSP peer. The statistics of MSDP peer will be cleared at the same time.

clear ip msdp peer *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of the MSDP peer

Defaults
N/A

Command Mode
Privileged EXEC mode

Usage Guide

This command is used to clear the TCP connection to the specified MSDP peer and clear all the MSDP peer statistics.

Configuration Examples

Related Commands

Platform Description

The following example clears MDSP peer of 218.14.5.23.

```
QTECH# clear ip msdp peer 218.14.5.23
```

Command	Description
N/A	N/A

This command is supported only on L3 devices.

10.2. clear ip msdp sa-cache

Use this command to clear SA cache entries.

clear ip msdp sa-cache [*group-address*]

Parameter Description

Parameter	Description
group-address	Group address

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to clear the SA cache entries learned from MSDP peer. If no multicast group address is specified, all SA cache entries will be cleared.

After SA cache entries are cleared, the MSDP device will need to relearn SA messages.

Configuration Examples

Related Commands

Platform Description

The following example clears the SA cache entries with the multicast group 224.1.1.1.

```
QTECH# clear ip msdp sa-cache 224.1.1.1
```

Command	Description
N/A	N/A

This command is supported only on L3 devices.

10.3. clear ip msdp statistics

Use this command to clear the statistics of MSDP peers without resetting the TCP sessions.

clear ip msdp statistics [*peer-address*]

Parameter Description

Parameter	Description
peer-address	IP address of MSDP peer whose statistics counters, reset count, and input/output count will be cleared.

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to clear the statistics of MSDP peers and view the new statistics of MSDP peers. This command can clear the statistics of one or more MDSP peers without resetting the MSDP peer.

Configuration Examples

Related Commands

The following example clears the statistics of the MSDP peer with IP address being 61.83.1.52.

```
QTECH# clear ip msdp statistics 61.83.1.52
```

Command	Description
N/A	N/A

Platform

This command is supported only on L3 devices.

Description

10.4. ip msdp default-peer

Use this command to define a default MSDP peer.

Use **no** or **default** form of this command to restore the default setting.

ip msdp default-peer *peer-address* [**prefix-list** *prefix-list-name*]

no ip msdp default-peer *peer-address*

default ip msdp default-peer *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of the MSDP peer
prefix-list *prefix-list-name*	Specifies the BGP prefix list.

Defaults

By default, no default MSDP peer is configured.

Command Mode

Global configuration mode

Usage Guide

The RPF-Peer calculation rule for the specified RP address may leads the loss of RPF-Peer information, which causes that the SA messages are dropped directly without the Peer-RPF check. With a default peer configured, the SA messages are ensured to pass the Peer-RFP check, so that the local host could accept the SA messages to learn the multicast source information carried by the SA messages.

If "prefix-list prefix-list-name" is not specified, all SA messages from the default MSDP peer will be accepted.

If "prefix-list prefix-list-name" is specified, only the SA messages from the RP specified by prefix-list prefix-list-name will be accepted.

If "prefix-list prefix-list-name" is specified but the prefix list is not configured, all SA messages from this default MSDP peer will be accepted.

Configuration Examples

The following example configures 172.16.33.1 as the default peer.

```
QTECH(config)# ip msdp peer 172.16.33.1
QTECH(config)# ip msdp peer 172.16.34.2 QTECH(config)# ip msdp default-peer 172.16.33.1
```

Related Commands

Command	Description

ip msdp peer	Creates MSDP peer.

Platform Description

This command is supported only on layer-3 device.

10.5. ip msdp description

Use this command to add descriptive information for MSDP peer.

Use **no** or **default** form of this command to restore the default setting.

ip msdp description *peer-address text*

no ip msdp description *peer-address*

default ip msdp description *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of the MSDP peer
text	Descriptive information for MSDP peer

Defaults

No descriptive information is configured for MSDP peer.

Command Mode

Global configuration mode

Usage Guide

The administrator can configure descriptive information for MSDP peers in order to identify them conveniently.

If the descriptive information A is specified for an MSDP peer, A is displayed. If no descriptive information is specified, “No description” is displayed.

Configuration Examples

Related Commands

Platform Description

The following example configures the descriptive information for peer 172.17.1.2 as "customer-a".

```
QTECH(config)# ip msdp description 172.171.1.2customer-a
```

Command	Description
show ip msdp peer	Displays the descriptive information for MSDP peer.

This command is supported only on L3 devices.

10.6. ip msdp filter-sa-request

Use this command to filter the SA request messages sent from MSDP peer. Use the **no** or **default** form of this command to restore the default setting. **ip msdp filter-sa-request** *peer-address* [**list** *access-list*]

no ip msdp filter-sa-request *peer-address*

default ip msdp filter-sa-request *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of the MSDP peer
list *access-list*	The standard IP access list number or name for limiting multicast group addresses

Defaults

All SA request messages from MSDP peer will be accepted and replied.

Command Mode

Global configuration mode

Usage Guide

Use this command to control which SA request messages will be accepted and replied.

If no access list is specified, all SA request messages will be ignored.

If a null access list is specified, all SA request messages will be ignored.

If an access list is specified, only the SA request messages from the multicast group permitted by the access list will be accepted, and other messages will be ignored.

Configuration Examples

The following example configures to filter SA request messages from peer 172.16.223.1 and only accept SA request messages with group address falling within 224.0.1.0-224.0.1.255.

```
QTECH(config)# ip msdp filter-sa-request 172.16.223.1 list 1
QTECH(config)# access-list 1 permit 224.0.1.1 0.0.0.255
```

Related Commands

Command	Description
ip msdp peer	Creates MSDP peer.

Platform Description

This command is supported only on L3 devices.

10.7. ip msdp mesh-group

Use this command to configure a MSDP peer to be a member of a mesh group. Use the **no** form of this command to remove the configuration.

Use the **default** form of this command to restore the default settings.

ip msdp mesh-group *mesh-name peer-address*

no ip msdp mesh-group *mesh-name peer-address*

default ip msdp mesh-group *mesh-name peer-address*

Parameter Description

Parameter	Description
mesh-name	Name of mesh group, case sensitive
peer-address	IP address of the MSDP peer to be a member of mesh group.

Defaults

No mesh group will be created, and MSDP peers do not belong to any mesh group.

Command Mode

Global configuration mode

Usage Guide

All MSDP peers in the mesh group shall be fully meshed, namely MSDP peer relationship has been established between every two members in the mesh group.

The SA received by one member of the mesh group won't be forwarded to other members in the same mesh group, thus reducing SA flooding and simplify Peer-RPF forwarding.

Configuration Examples

Related Commands

Platform Description

The following example configures MSDP peer at address 192.168.1.3 to be a member of the mesh group named "msdp-mesh".

QTECH(config)# **ip msdp mesh-group** *msdp-mesh192.168.1.3*

Command	Description
show ip msdp mesh-group	Displays the information of mesh group.

This command is supported only on L3 devices.

10.8. ip msdp originator-id

Use this command to allow a speaker that originates a SA message to use the IP address of the interface as the originator address in the SA message.

Use the **no** form of this command to remove this configuration.

Use the **default** form of this command to restore the default setting.

ip msdp originator-id *interface-type interface-number*

no ip msdp originator-id default ip msdp originator-id

Parameter Description

Parameter	Description

interface-type	Interface type
interface-number	Interface number

Defaults

By default, the originator address in SA messages will be the RP address configured by PIM.

```
QTECH(config)# ipv6 mld snooping vlan 1 static FF88::1 interface
gigabitEthernet 0/1
```

Global configuration mode

Usage Guide

The master IP address of this interface will be used as the originator address in the SA messages. If no IP address is configured for this interface, or the interface is shut down, then the originator address in the SA messages won't use the master IP address of this interface, but use the RP address configured by PIM.

Under certain circumstances, you may expect to change the originator address in SA messages, such as during Anycast-RP deployment. By this time, you can use this command to modify the originator address in SA messages.

```
QTECH(config)# ipv6 mld snooping vlan 1 static FF88::1 interface
gigabitEthernet 0/1
```

Related Commands

Platform Description

The following example uses the IP address of Loopback0 as the RP address in SA messages.

```
QTECH(config)# ip msdp originator-id loopback0
```

Command	Description
N/A	N/A

This command is supported only on L3 devices.

10.9. ip msdp password

Use this command to enable MD5 encryption of the TCP connection between MSDP peers. Use the **no** or **default** form of this command to restore the default setting.

ip msdp password peer *peer-address* [*encryption-type*] *string*

no ip msdp password peer *peer-address*

default ip msdp password peer *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of MSDP peer
encryption-type	Grade of password: 0 (lowest level)-7 (highest level). Currently, only 0 and 7 are supported. The default encryption type is 0.
string	The password used for TCP MD5 authentication. Range: up to 80 characters when the encryption type is 0; up to 160 characters when the encryption type is 7.

Defaults

MD5 encryption of the TCP connection between MSDP peers is disabled.

Command Mode

Global configuration mode

Usage Guide

When it is needed to authenticate the MSDP peers, you can enable MD5 encryption of TCP connection between MSDP peers. In such a case, two interconnected MSDP peers must be configured with MD5 authentication with same password, or else the connection will fail.

If the password is configured or changed, the local MSDP device won't terminate the current session, but will try to use the new password to maintain the current session until timeout.

If you have configure the password locally for the MSDP peer but no password is configured on MSDP, the following warning message will be displayed on the console:

```
%TCP-6-BADAUTH: MD5 digest NOT expected but found (200.200.200.6,
39996)->(200.200.200.16, 639)
```

If different MD5 passwords are configured between MSDP peers, the following warning message will be displayed on the console:

```
%TCP-6-BADAUTH: MD5 digest failed for (200.200.200.6,
12302)->(200.200.200.16, 639)
```

If the encryption type is 0, the encryption key for TCP is the string entered in the console. That is, this type of encryption is supported when QTECH Networks MSDP devices communicates with those from other vendors. Thus, this encryption type is recommended for mutual communication between devices from different vendors.

If the encryption type is 7, the entered encryption key must be even and not less than 4.

Different from type 0, the encryption key is not the string entered in the console. Instead, it is a new string computed by QTECH-defined algorithm. In addition, our algorithm is different from other private vendor-specific algorithms. Therefore, this encryption type is supported only when QTECH Networks devices are mutually connected.

Configuration Examples

Related Commands

Platform Description

The following example configures the MD5 password of "test" for the MSDP peer of 10.32.43.144.

```
Ruijie(config)# ip msdp password peer 10.32.43.144 0 test
```

Command	Description
N/A	N/A

This command is supported only on L3 devices.

10.10. ip msdp peer connect-source

Use this command to create MSDP peer.

Use **no** or **default** form of this command to remove MSDP peer.

ip msdp peer *peer-address* **connect-source** *interface-type interface-number*

no ip msdp peer *peer-address*

default ip msdp peer *peer-address*

Parameter Description

Parameter	Description

peer-address	IP address of MSDP peer The peer MSDP device uses this address to communicate with the local MSDP device for TCP connection.
interface-type interface-number	Interface type and interface number. The local MSDP device uses the main address of this interface as the source IP for the TCP connection to the remote MSDP peer. Loopback interface is recommended. If no IP address is configured for this interface, or the interface is shut down, then MSDP peer relation cannot be established.

Defaults

No MSDP peer is created.

Command Mode

Global configuration mode

Usage Guide

To enable MSDP, MSDP peer must be created.

Configuration Examples

Related Commands

Platform Description

The following example configures the main address of interface loopback 0 as the source address for establishing MSDP peer relation with 192.168.5.1.

```
QTECH(config)# ip msdp peer 192.168.5.1 connect-source loopback0
```

Command	Description
show ip msdp peer	Displays the information about MSDP peer.

This command is supported only on L3 devices.

10.11. ip msdp redistribute

Use this command to configure which (S, G) entries from the multicast routing table can be advertised to MSDP peers.

Use the **no** form of this command to remove this configuration.

Use the **default** form of this command to restore the default settings. **ip msdp redistribute** [**list** *access-list-name*] [**route-map** *route-map*] **no ip msdp redistribute**

default ip msdp redistribute

Parameter Description

Parameter	Description
list *access-list-name*	Number or name of an extended IP access list that controls which multicast routes (S, G) can be advertised.
route-map *route-map*	Defines route-map.

Defaults

All multicast sources (S, G) registered on the local RP will be advertised.

Command Mode

Global configuration mode

Usage Guide

After redistribution filtering is configured, the (S, G) information from the local AS or the other AS can be added to the MSDP only through redistribution filtering.

If "**list** *access-list-name*" is specified, only those matched multicast routes (S, G) will be advertised. If "**route-map** *map-name"* is specified, only multicast routes (S, G) matching the criteria given in "map-name" will be advertised.

If two keywords are specified, then multicast routes (S, G) matching all conditions will be advertised. If the "**ip msdp redistribute**" command is configured with no keywords, no multicast sources will be advertised.

Configuration Examples

The following example configures to only advertise multicast routes with

multicast source being 200.200.200.0/24 and group address being

225.1.1.0/24.

```
Router(config)# ip msdp redistribute list 100
Router(config)# ip access-list extended 100
Router(config-ext-nacl)# permit ip 200.200.200.0 0.0.0.255 225.1.1.0
0.0.0.255
```

Related Commands

Command	Description
ip msdp sa-filter in	Configures the incoming filter for SA messages.
ip msdp sa-filter out	Configures the outgoing filter for SA messages.

Platform Description

This command is supported only on L3 devices.

10.12. ip msdp sa-filter in

Use this command to configure an incoming filter for SA messages.

Use the **no** or **default** form of this command to remove the incoming filter.

ip msdp sa-filter in *peer-address* [**list** *access-list*] [**route–map** *route-map*] [**rp-list** *rp-access-list*] [**rp-route-map** *rp-route-map*]

no ip msdp sa-filter in *peer-address*

default ip msdp sa-filter in *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of MSDP peer
list *access-list*	Number or name of an extended IP access list that controls which multicast routes (S, G) can be received.

route-map *route-map*	Specify the name of route-map; only SA messages matching the criteria given in "map-name" can pass through.
rp-list *rp-access-list*	Number or name of standard access list that controls RPs.
rp-route-map *rp-route-map*	Specify the name of route map for RP; only the SA messages matching rp-map-name can be accepted.

Defaults

All incoming SA messages will be accepted without filtering.

Command Mode

Global configuration mode

Usage Guide

If the command is configured, but no access list or route map is specified, all incoming SA messages will be filtered.

If only the **list** keyword or the **route-map** keyword is used, the multicast source (S, G) in SA messages matching the criteria corresponding to this keyword will be accepted.

If only the **rp-list** keyword or the **rp-route-map** keyword is used, the SA message will be accepted if the RP address carried in SA message matches the criteria corresponding to this keyword.

If two or more keywords of **list, route-map, rp-list** and **rp-route-map** are used, the SA message will be accepted if any multicast source (S, G) in SA message meet the criteria corresponding to all keywords.

Configuration Examples

The following example configures that all SA messages from the peer of 10.234.1.43 will be filtered.

```
QTECH(config)# ip msdp peer 10.234.1.43
QTECH(config)# ip msdp sa-filter in 10.234.1.43
```

Related Commands

Command	Description
ip msdp peer	Configures MSDP peer.

ip msdp sa-filter-out	Configures the outgoing filter for SA messages received from MSDP peers.

Platform Description

This command is supported only on L3 devices.

10.13. ip msdp sa-filter out

Use this command to configure an outgoing filter for SA messages.

Use the **no** or **default** form of this command to remove the outgoing filter.

ip msdp sa-filter out *peer-address* [**list** *access-list*] [**route–map** *route-map*] [**rp-list** *rp-access-list*] [**rp-route-map** *rp-route-map*] **no ip msdp sa-filter out** *peer-address* **default ip msdp sa-filter out** *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of MSDP peer
list access-list	Number or name of an extended IP access list that controls which multicast routes (S, G) can be received.
route-map route-map	Specify the name of route-map; only SA messages matching the criteria given in "map-name" can pass through.
rp-list rp-access-list	Number or name of standard access list that controls RPs.
rp-route-map rp-route-map	Specify the name of route map for RP; only the SA messages
	matching rp-map-name can be accepted.

Defaults

All SA messages received will be forwarded to the MSDP peer.

Command Mode

Global configuration mode

Usage Guide

If the command is configured, but no access list or route map is specified, all SA messages won't be forwarded to this MSDP peer.

If only one keyword of **list, route-map, rp-list** and **rp-route-map** is used, the multicast source pair (S, G) will be forwarded to this MSDP peer if the criteria corresponding to this keyword are met.

If two or more keywords of **list, route-map, rp-list** and **rp-route-map** are used, the (S, G) pair will only be forwarded to this MSDP peer if criteria corresponding to all keywords are met.

Configuration Examples

The following example allows only multicast sources that pass access list 100

to be forwarded to the peer of 10.234.1.43.

```
QTECH(config)# ip msdp peer 10.234.1.43
QTECH(config)# ip msdp sa-filter out 10.234.1.43 list 100
QTECH(config)# access-list 100 permit ip 10.211.0.0 0.0.255.255 224.12.0.0
0.0.255.255
```

Related Commands

Command	Description
ip msdp peer	Configures MSDP peer.
ip msdp sa-filter-in	Configures the incoming filter for SA messages received from MSDP peers.

Platform Description

This command is supported only on L3 devices.

10.14. ip msdp sa-limit

Use this command to configure the allowable maximum number of Source-Active (SA) cache entries from a MSDP peer.

Use the **no** or **default** form of this command to restore the default settings.

ip msdp sa-limit *peer-address sa-limit* **no ip msdp sa-limit** *peer-address* **default ip msdp sa-limit** *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of MSDP peer
sa-limit	Maximum number of SA messages from an MSDP peer allowed in the SA cache

Defaults

The maximum number of SA messages from an MSDP peer allowed in the SA cache is not limited.

Command Mode

Global configuration mode

Usage Guide

It is suggested to configure this command on all MSDP peers to prevent SA flooding attacks from MSDP peers.

When the local device has learned A (quantity) SA entries from an MSDP peer, and A is greater than B (the SA limit), the SA entries from this peer will not be cleared at once. Instead, the aging mechanism (no more than 135 seconds) will lower A to B. That is, this command is not effective immediately. It aims to saving effective multicast information best to raise networking productivity. If you want to clear the SA entries in such case, use the **clear ip msdp sa-cache** command.

Configuration Examples

Related Commands

Platform Description

The following example configures the SA message limit to 100 for the MSDP peer with IP address being 172.16.3.1.

QTECH(config)# **ip msdp sa-limit** *172.16.3.1 100*

Command	Description
N/A	N/A

This command is supported only on L3 devices.

10.15. ip msdp shutdown

Use this command to shut down the connection to MSDP peer.

Use the **no** or **default** form of this command to restore the default settings.

ip msdp shutdown *peer-address*

no ip msdp shutdown *peer-address*

default ip msdp shutdown *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of the MSDP peer

Defaults

The connection to peer is not shut down.

Command Mode

Global configuration mode

Usage Guide

Only the TCP connection to the specified MSDP peer will be shut down.

Neither the MSDP peer nor its configurations will be cleared.

Configuration Examples

Related Commands

Platform Description

The following example shuts down the MSDP peer at IP address 192.168.7.20.

QTECH(config)# **ip msdp shutdown***192.168.7.20*

Command	Description
ip msdp peer	Creates MSDP peer.

This command is supported only on L3 devices.

10.16. ip msdp timer

Use this command to configure the interval for timer re-connection.

Use the **no** or **default** form of this command to restore the default settings.

ip msdp timer ***interval*** no ip msdp time default ip msdp timer

Parameter Description

Parameter	Description
interval	Interval for timer re-connection, within the range from 1 to 60 in the unit of seconds

Defaults

The default interval is 30 seconds.

Command Mode

Global configuration mode

Usage Guide

By default, the interval for timer re-connection is 30 seconds, that is, the peer in active end can initiate only one TCP connection within 30 seconds. In certain applications, the interval is expected to be decreased in order to accelerate convergence of MSDP peering relation.

Configuration Examples

Related Commands

Platform Description

The following example sets the interval for timer re-connection to 20 seconds.

QTECH(config)# **ip msdp timer** *20*

Command	Description

N/A	N/A

This command is supported only on L3 devices.

10.17. ip msdp ttl-threshold

Use this command to limit the TTL value of multicast data packets carried in SA messages in order to limit the transmission of multicast packets.

Use the **no** or **default** form of this command to restore to the default settings.

ip msdp ttl-threshold *peer-address ttl-value* **no ip msdp ttl-threshold** *peer-address* **default ip msdp ttl-threshold** *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of the MSDP peer
ttl-value	TTL value in the range from 0 to 255

Defaults

TTL threshold is 0 by default.

Command Mode

Global configuration mode

Usage Guide

This command limits multicast data packets which are sent in data-encapsulated SA messages. Only multicast packets with an IP-header TTL greater than or equal to the ttl-value will be sent to the MSDP peer. If the TTL value of multicast data is less than the threshold configured, then the multicast data will be separated from SA messages and discarded, and the SA messages without multicast data will be sent to the MSDP peer.

This command only limits the transmission of multicast data in SA messages without compromising the transmission of multicast sources in SA messages

Configuration Examples

Related Commands

Platform Description

The following example configures the TTL threshold for peer at IP address 192.168.10.1 to 8 hops:

QTECH(config)# **ip msdp ttl-threshold** *192.168.10.18*

Command	Description
N/A	N/A

This command is supported only on L3 devices.

10.18. ip msdp peer-limit

Use this command to set the upper limit of MSDP peers.

Use the **no** form of this command to remove the configuration.

Use the **default** form of this command to restore the default settings.

ip msdp peer-limit *peer-limit*

Parameter Description

Parameter	Description
peer-limit	The upper limit of MSDP peers, in the range from 1 to128.

no ip msdp peer-limit

default ip msdp peer-limit

Defaults

The default is 64.

Command Mode

Global configuration mode

Usage Guide

This command is used to set the upper limit of MSDP peers. If the number of

existing MSDP peers exceeds the upper limit to be configured, you should delete some peers, or the configuration will fail.

Configuration Examples

The following example sets the upper limit of MSDP peers to 128.

```
QTECH(config)# ip msdp peer-limit 128
```

Platform Description

This command is supported only on L3 devices.

10.19. ip msdp global-sa-limit

Use this command to configure the maximum SA cache.

Use the **no** form of this command to remove the configuration.

Use the **default** form of this command to restore the default settings.

ip msdp global-sa-limit *sa-limit*

no ip msdp global-sa-limit *sa-limit*

default ip msdp global-sa-limit ***sa-limit***

Parameter Description

Parameter	Description
sa-limit	The maximum SA cache, in the range from1 to 4,096

Defaults

The default SA cache is 1,024.

Command Mode

Global configuration mode

Usage Guide

This command is used to set the maximum SA cache. It's recommended to configure it at the beginning of startup.

When MSDP is running, the increase in maximum SA cache has no influence upon the previously learned entries; the decrease in maximum SA cache will clear all entries learned before and start caching again.

Configuration Examples

The following example sets the maximum SA cache to 4,096.

```
QTECH(config)# ip msdp global-sa-limit 4096
```

Platform Description

This command is supported only on L3 devices.

10.20. show ip msdp count

Use this command to display the number of sources and groups originated in SA messages and the number of SA messages from an MSDP peer in the SA cache.

show ip msdp count [*as-number*]

Parameter Description

Parameter	Description
as-number	Displays the number of sources and groups originated in SA messages from the specified autonomous system number.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

```
QTECH# sh ip msdp count
SA State per Peer Counters, <Peer>: <# SA learned>
1.1.1.2     :  0  100.100.100.14  :  0  100.100.100.15  :  0  100.100.100.200:  0
200.200.200.2  :  2  200.200.200.3  :  0  200.200.200.6  :  0  200.200.200.13  :  0
200.200.200.66 : 0
SA State per ASN Counters, <asn>: <# sources>/<# groups> Total entries: 2
```

Field	Description
200.200.200.200:2	MSDP peer with IP address 200.200.200.200; 2 SA messages in the SA cache.

Total entries	Total number of SA entries in the SA cache.
?:1/2	Unknown autonomous system: 1 source address/2 multicast group addresses

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on L3 devices.

10.21. show ip msdp mesh-group

Use this command to display the information of mesh group.
show ip msdp mesh-group

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

```
QTECH# sh ip msdp mesh-group
MSDP peers in each Mesh-group,<Mesh-group name>:<# peers> msdp-mesh
1.1.1.2
1.1.1.3
```

Field	Description
msdp-mesh	Name of mesh group
1.1.1.2	One MSDP peer under this mesh group.

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on L3 devices.

10.22. show ip msdp peer

Use this command to display detailed information about the MSDP peer.

show ip msdp peer [*peer-address*]

Parameter Description

Parameter	Description
peer-address	IP address of the MSDP peer

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

```
QTECH#show ip msdp peer 20.0.0.1
MSDP PEER 20.0.0.1 (No description), AS unknown Connection status:
State: Listen, Resets: 1, Connection source: GigabitEthernet 0/1 (20.0.0.2)
Uptime(Downtime): 00:00:25, Message sent/received: 13/19
Input messages discarded: 0
Connection and counters cleared 00:13:25 ago Local Address of connection:
```

Field	Description
MSDP Peer	IP address of MSDP peer.
AS	Autonomous system to which the MSDP peer belongs. If it is an unknown AS, “unknown” will be displayed.
State:	State of the MSDP peer.
Connection source:	Interface used to obtain the source address for TCP connection.
Uptime(Downtime):	Up time/down time of MSDP peer.
Messages sent/received:	Number of SA messages received.
SA Filtering:	SA filtering information.
SAs learned from this peer:	Number of SA entries learned from MSDP peer.
SAs limit:	SA message limit for this MSDP peer.

Related Commands

Command	Description

N/A	N/A

Platform Description

This command is supported only on L3 devices.

10.23. show ip msdp rpf-peer

Use this command to display the information about MSDP RPF peer corresponding to the specified originator address.

show ip msdp rpf-peer *ip-address*

Parameter Description

Parameter	Description
ip-address	IP address of the originator of SA messages

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the rpf-peer information of RP at address 1.1.1.1:

```
QTECH# sh ip msdp rpf-peer 1.1.1.1
RPF peer information for 1.1.1.1 RPF peer: 200.200.200.2
RPF rule: Peer is only active peer RPF route/mask: Not-used
RPF type: Not-used
```

Related Commands

Command	Description

N/A	N/A

Platform Description

his command is only supported on L3 devices.

10.24. show ip msdp sa-cache

Use this command to display (S, G) state learned.

show ip msdp sa-cache [*group-address* | *source-address*] [*group-address* | *source-address*] [*as-number*]

Parameter Description

Parameter	Description
group-address	Group address of the group or source about which (S, G) information is displayed
source -address	Source address of the group or source about which (S, G) information is displayed.
as-number	Autonomous system number generated by SA messages.

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays (S, G) state learned.

```
QTECH# sh ip msdp sa-cache
MSDP Source-Active Cache: 2 entries MSDP Source-Active Cache: 2 entries
```

```
(200.200.200.200, 227.1.2.2), RP: 20.20.20.20, (M)BGP/AS 100,
04:17:09/00:02:05, Peer 200.200.200.2
Learned from peer 200.200.200.2, RPF peer 200.200.200.2,
SAs received: 277, Encapsulated data received: 0 (200.200.200.200, 227.1.2.3), RP: 20.20.20.20, (M)BGP/AS 100,
04:17:09/00:02:05, Peer 200.200.200.2
Learned from peer 200.200.200.2, RPF peer 200.200.200.2, SAs received: 277, Encapsulated data received: 0
```

Field	Description
(200.200.200.200, 227.1.2.2)	Source address and group address.
RP 20.20.20.20	RP address generating SA messages.
MBGP/AS	The autonomous system of the RP generating SA messages is unknown.
04:17:09/00:02:05	The route has been cached for 4 hours 17 minutes and 9 seconds. If no SA message is received in 2 minutes and 5 seconds, it will be removed from the SA cache.

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is only supported on L3 devices.

10.25. show ip msdp sa-originated

Use this command to display the (S, G) information to be sent by the local device. The (S, G) information has passed redistribution filtering.

show ip msdp sa-originated

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode
Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

This command can be used to display the (S, G) information sent by the local device that is the RP in PIM-SM with the multicast source (S, G) registered and is configured with MSDP peer.
(S, G) information displayed has passed redistribution filtering, but, whether the information can be sent to the MSDP peer requires the results of egress filtering for the information.

Configuration Examples
The following is sample output of "show ip msdp sa-originated" command.

```
QTECH# sh ip msdp sa-originated
MSDP Source-Active Originated: 5 entries
(192.168.23.78, 225.0.0.1), RP: 192.168.23.249
(192.168.23.79, 225.0.0.2), RP: 192.168.23.249
(192.168.23.80, 225.0.0.3), RP: 192.168.23.249
(192.168.23.81, 225.0.0.4), RP: 192.168.23.249
(192.168.23.82, 225.0.0.5), RP: 192.168.23.249
```

Field	Description
(192.168.23.78, 225.0.0.1)	The source address (the first IP address) and group address (the second IP address) of SA to be sent.
RP 192.168.23.249	RP address of SA sent.

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is only supported on L3 devices.

10.26. show ip msdp summary

Use this command to display the summary information about all MSDP peers.
show ip msdp summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode
Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

If the local device configured with MSDP peers is the PIM-SM Rendezvous Point (RP) and multicast sources (S,G) registers in the RP, the command will display: (S,G) to Send
The displayed (S,G) have gone through redistribution filtering (command: **ip msdp redistribute**). However, whether these (S,G) will be delivered to MSDP peers successfully relies on the outgoing filter (command: **ip msdp sa-filter out**).

Configuration Examples
The following example displays the summary information about all MSDP peers.

```
peer-A
QTECH# sh ip msdp summary

Msdp Peer Status Summary
Peer Address      As      State     Uptime/Downtime    Reset-Count
Sa-Count    Peer-description
200.200.200.2     100     Up        04:22:11           10             6616
No description
200.200.200.3     100     Down      19:17:13           4              0
```

Field	Description
Peer Address	IP address of MSDP peer
AS	Autonomous system to which the MSDP peer belongs
State	State of the MSDP peer
Uptime/Downtime	Up time or down time of MSDP peer

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is only supported on L3 devices.