1 PIM-SMv6 Commands

Command	Function
clear ipv6 mroute	Clear IPv6 multicast routing entries.
clear ipv6 mroute statistics	Clear statistics about IPv6 multicast routing entries.
clear ipv6 pim sparse-mode bsr rp-set	Clear all dynamic rendezvous point (RP) information.
clear ipv6 pim sparse-mode track	Set the statistics start time and clear statistics of the PIMv6 packets.
ipv6 pim accept-bsr list	Limit the address range of BSRs.
ipv6 pim accept-crp-with-null-group	Enable the BSR to receive advertisement packets with the prefix of a multicast address being 0.
ipv6 pim accept-crp list	Limit the C-RP address range and the address range of the groups served by the C-RPs.
ipv6 pim accept-register	Limit the (S, G) address range in the register messages received by an RP.
Ipv6 pim bsr-border	Configure a BSR border.
ipv6 pim bsr-candidate	Configure C-BSRs.
ipv6 pim bfd	Configure the BFD Support for PIMv6 feature on an interface, also known as PIMv6 BFD.
ipv6 pim dr-priority	Configure the DR priority.
Ipv6 pim ignore-rp-set-priority	Ignore RP priority for RP election.
ipv6 pim jp-timer	Configure the join/prune packet sending interval.
ipv6 pim neighbor-filter	Enable the neighbor filtering function.
ipv6 pim neighbor-tracking	Enable the neighbor tracking function.
ipv6 pim override-interval	Configure the prune override interval of an interface.
ipv6 pim probe-interval	Configure the register-probe time.
ipv6 pim propagation-delay	Configure the propagation delay of an interface.
ipv6 pim query-interval	Configure the hello message sending interval.
ipv6 pim register-checksum-wholepkt	Calculate the checksum of entire register messages.
ipv6 pim register-rate-limit	Limit the sending rate of register messages.

ipv6 pim register-rp-reachability	Enable the RP reachability checking function before a register message is sent.
ipv6 pim register-source	Specify a source IPv6 address in register messages.
ipv6 pim register-suppression	Configure the register suppression time.
ipv6 pim rp-address	Configure static RPs.
ipv6 pim rp-candidate	Configure C-RPs.
ipv6 pim rp-register-kat	Configure the (S, G) entry timeout period on an RP.
ipv6 pim rp embedded	Enable the RP address embedding function.
ipv6 pim sparse-mode	Enable the PIM-SMv6 function on an interface.
ipv6 pim sparse-mode passive	Enable the PIM-SMv6 passive mode on an interface.
ipv6 pim spt-threshold	Enable the shortest path tree (SPT) switchover function.
ipv6 pim ssm	Enable the SSM function and configure an SSM group address range.
ipv6 pim static-rp-preferred	Configure static DR priority to be higher than dynamic RP priority.
ipv6 pim triggered-hello-delay	Configure the hello message sending delay on an interface.
show ipv6 pim sparse-mode bsr-router	Display BSR information.
show ipv6 pim sparse-mode interface	Display PIM-SMv6 information of an interface.
show ipv6 pim sparse-mode local-members	Display local MLD information of a PIM-SMv6 interface.
show ipv6 pim sparse-mode mroute	Display PIM-SMv6 routing information.
show ipv6 pim sparse-mode neighbor	Display neighbor information.
show ipv6 pim sparse-mode nexthop	Display next hop information, including interface, address, and metric value of a next hop.
show ipv6 pim sparse-mode rp mapping	Display all RPs and the groups served by the RPs on the local device.
show ipv6 pim sparse-mode rp-hash	Display RP information corresponding to a multicast group address.
show ipv6 pim sparse-mode track	Display the number of PIM packets sent and received since the statistic start time.

1.1 clear ipv6 mroute

Function

Run the **clear ipv6 mroute** command to clear IPv6 multicast routing entries.

Syntax

clear ipv6 mroute { ***** | *ipv6-group-address* [*ipv6-source-address*] }

Parameter Description

*****: Clears all IPv6 multicast routing entries.

ipv6-group-address: Address of an IPv6 multicast group whose routing entries are to be cleared.

ipv6-source-address: Address of an IPv6 multicast source whose routing entries are to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If the multicast function fails, you can run this command to clear the current multicast routing information to facilitate problem locating and re-learn entries.

Examples

The following example clears all IPv6 multicast routing entries.

```
Hostname> enable
Hostname# clear ipv6 mroute *
```

The following example clears IPv6 multicast routing entries of a specified group.

```
Hostname> enable
Hostname# clear ipv6 mroute ff66::6666
```

The following example clears multicast routing entries of a specified group and source.

```
Hostname> enable
Hostname# clear ipv6 mroute ff66::6666 3333::3333
```

Notifications

N/A

Platform Description

N/A

1.2 clear ipv6 mroute statistics

Function

Run the **clear ipv6 mroute statistics** command to clear statistics about IPv6 multicast routing entries.

Syntax

clear ipv6 pim sparse-mode bsr rp-set *

Parameter Description

*: Clears all dynamic RP information.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to clear dynamic C-RP information, rather than static C-RP information.

Examples

The following example clears all dynamic RP information of PIM-SMv6.

```
Hostname> enable
Hostname# clear ipv6 pim sparse-mode bsr rp-set *
```

Notifications

After the RP-Set information is cleared, the following notification will be displayed:

```
Self RP is changed for group range %R/%u.  Perform Self RP change handler
```

Platform Description

N/A

1.4 clear ipv6 pim sparse-mode track

Function

Run the **clear ipv6 pim sparse-mode track** command to set the statistics start time and clear statistics of the PIMv6 packets.

Syntax

clear ipv6 pim sparse-mode track

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example resets the statistic start time and clears statistics of the PIMv6 packets.

```
Hostname> enable
Hostname# clear ipv6 pim sparse-mode track
```

Notifications

N/A

Platform Description

N/A

1.5 ipv6 pim accept-bsr list

Function

Run the **ipv6 pim accept-bsr list** command to limit the address range of BSRs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

All BSMs are received by default.

Syntax

ipv6 pim accept-bsr list *acl-name*

no ipv6 pim accept-bsr

default ipv6 pim accept-bsr

Parameter Description

list *acl-name*: Uses an ACL name to limit the address range of BSRs. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example uses the ACL bsr-list to limit the address range of BSRs so that only BSMs sent from the BSRs in the bsr-list range are received.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ipv6 access-list bsr-list
Hostname(config-ipv6-acl)# permit ipv6 9000::5/64 any
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim accept-bsr list bsr-list
```

Notifications

If no ACL is configured to limit the BSR address range, the following notification will be displayed:

```
% access-list bsr-list not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 pim bsr-candidate

1.6 ipv6 pim accept-crp-with-null-group

Function

Run the **ipv6 pim accept-crp-with-null-group** command to enable the BSR to receive advertisement packets with the prefix of a multicast address being 0.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The function for the BSR to receive advertisement packets with the prefix of a multicast address being 0 is disabled by default.

Syntax

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

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A C-RP periodically sends advertisement packets to the BSR in unicast mode. The packets include the RP priority, advertisement packet hold time (greater than the interval of sending the advertisement packet), RP address, address of the served group, and prefix of the multicast address. Upon receiving the advertisement packets, the BSR collects the information in the packets as RP-Set in the advertisement packet hold time, encapsulates the information in a BSM, and sends the message to all PIM devices.

After this command is run on a C-BSR and this C-BSR is elected as the BSR, the BSR can receive advertisement packets with the prefix of a multicast address being 0. This C-RP can serve all groups.

Examples

The following example configures the BSR to receive advertisement packets with the prefix of the multicast address being 0 from a C-RP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim accept-crp-with-null-group
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 ipv6 pim accept-crp list

Function

Run the **ipv6 pim accept-crp list** command to limit the C-RP address range and the address range of the groups served by the C-RPs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The C-BSRs receive all external C-RP advertisement packets by default.

Syntax

ipv6 pim accept-crp list *acl-name*

no ipv6 pim accept-crp

default ipv6 pim accept-crp

Parameter Description

list *acl-name*: Uses an ACL name to limit the C-RP address range and the address range of the groups served by the C-RPs. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run on a C-BSR and this C-BSR is elected as the BSR, the BSR can limit the C-RP address range and the address range of the groups served by the C-RPs.

Examples

The following example uses the ACL crp-list to limit the C-RP address range and the address range of the groups served by the C-RPs.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list crp-list
Hostname(config-ipv6-acl)# permit ipv6 9000::5/64 any
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim accept-crp list crp-list
```

Notifications

If no ACL is configured, the following notification will be displayed:

```
% access-list crp-list not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 pim rp-candidate**

1.8 ipv6 pim accept-register

Function

Run the **ipv6 pim accept-register** command to limit the (S, G) address range in the register messages received by an RP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The (S, G) address range of register messages is not limited by default. An RP receives register messages with any (S, G) address.

Syntax

ipv6 pim accept-register { **list** *acl-name* | **route-map** *route-map-name* } *

no ipv6 pim accept-register

default ipv6 pim accept-register

Parameter Description

list *acl-name*: Uses an ACL name to limit the (S, G) group address range. The value is a case-sensitive string of 1 to 99 characters.

route-map *route-map-name*: Uses a route map to limit the (S, G) address range.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run on a static RP or C-RP, the RP replies a register-stop message upon receiving data from an unauthorized source.

Examples

The following example uses an ACL register-access-list to deny register messages from the source FE80::2D0:F8FF:FE22:33AD.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list register-access-list
Hostname(config-ipv6-acl)# deny ipv6 fe80::2d0:f8ff:fe22:33ad/128 any
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim accept-register list register-access-list
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 Ipv6 pim bsr-border

Function

Run the **ipv6 pim bsr-border** command to configure a BSR border.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No BSR border is configured by default.

Syntax

ipv6 pim bsr-border
no ipv6 pim bsr-border
default ipv6 pim bsr-border

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To control BSM flooding, you can configure a BSR border on the interface. Then, this interface discards received BSMs without forwarding them.

Examples

The following example configures a BSR border on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim bsr-border
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 multicast boundary** (IPv6 multicast route management)
- **show ipv6 pim sparse-mode interface**

1.10 ipv6 pim bsr-candidate

Function

Run the **ipv6 pim bsr-candidate** command to configure C-BSRs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No C-BSR is configured by default.

Syntax

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

no ipv6 pim bsr-candidate

Parameter Description

interface-type terface-number: Interface type and interface number. You are advised to use the address of this interface as the address of a C-BSR.

hash-mask-length: Length of a hash mask configured for the RP election mechanism. The value range is from 0 to 128, and the default value is **126**.

priority-value: C-BSR priority. The value range is from 0 to 255, and the default value is **64**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In a PIM SMv6 domain, a unique BSR must be available. The BSR collects and releases RP information. Multiple C-BSRs elect an acknowledged BSR based on BSMs. Before a BSR is elected, each C-BSR considers itself a BSR and periodically sends a BSM in the PIM-SMv6 domain. This message includes the address and priority of the BSR.

This command can be used to send a BSM to all PIM neighbors through the address assigned to a BSR. Each neighbor compares the original BSR address with the address in the received BSM. If the received BSM indicates that the C-BSR of the received BSM boasts a higher priority or a larger IP address, the neighbor saves the address in the BSM as the BSR address and forwards the BSM. Otherwise, the neighbor discards the BSM.

A C-BSR considers itself the BSR until the C-BSR receives a BSM indicating a higher priority from another C-BSR.

Examples

The following example configures the address of GigabitEthernet 0/1 as the address of a C-BSR, and sets the length of the hash mask to 30 and the priority to 100.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# ipv6 pim bsr-candidate gigabitethernet 0/1 30 100
```

Notifications

If the current interface is not configured in SM mode, the following notification will be displayed:

```
Warning: PIMSMv6 not configured on %s, BSR messages not originated.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 ipv6 pim bfd

Function

Run the **ipv6 pim bfd** command to configure the BFD Support for PIMv6 feature on an interface, also known as PIMv6 BFD.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

PIMv6 BFD is not configured on an interface by default.

Syntax

ipv6 pim bfd

no ipv6 pim bfd

default ipv6 pim bfd

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Bidirectional forwarding detection (BFD) is used to quickly detect or monitor links or IP route forwarding connectivity in a network.

Based on the PIM-SMv6 protocol, a designated router (DR) is defined. This DR is the unique role that forwards multicast data in a shared network.

Devices in the shared network exchange PIM hello messages and elect a DR based on the hello messages. When the DR is faulty, a new round of DR election can be started only after the PIM neighbor ages. If this

command is run, when the DR is faulty, this faulty DR can be detected and a new round of election can be started in milliseconds.

Examples

The following example configures PIMv6 BFD on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname (config-if-GigabitEthernet 0/1)# ipv6 pim bfd
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 pim sparse-mode**
- **show bfd neighbors** (reliability/BFD)

1.12 ipv6 pim dr-priority

Function

Run the **ipv6 pim dr-priority** command to configure the DR priority.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default DR priority is **1**.

Syntax

ipv6 pim dr-priority *priority-value*

no ipv6 pim dr-priority

default ipv6 pim dr-priority

Parameter Description

priority-value: DR priority. A larger value indicates a higher priority. The value range is from 0 to 4294967294.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If multiple devices in a LAN join DR election, the election result is subject to the priorities in hello messages. The device with the highest priority is elected as the DR. If the priorities in the hello messages are the same or the priority parameter is not set in the hello messages, the device with the largest IP address is elected as the DR.

Examples

The following example sets the DR priority to **11234** on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim dr-priority 11234
```

Notifications

If the priority value is smaller than 0, the following notification will be displayed:

```
% Invalid DR priority value.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ipv6 pim sparse-mode interface

1.13 Ipv6 pim ignore-rp-set-priority

Function

Run the **ipv6 pim ignore-rp-set-priority** command to ignore RP priority for RP election.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

A C-RP with the highest priority is selected as the RP by default.

Syntax

Ipv6 pim ignore-rp-set-priority

no ipv6 pim ignore-rp-set-priority

default ipv6 pim ignore-rp-set-priority

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example ignores RP priority for RP election.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim ignore-rp-set-priority
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 ipv6 pim jp-timer

Function

Run the **ipv6 pim jp-timer** command to configure the join/prune packet sending interval.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The join/prune packet is sent at an interval of **60** seconds by default.

Syntax

ipv6 pim jp-timer *interval*

no ipv6 pim jp-timer

default ipv6 pim jp-timer

Parameter Description

interval: Join/prune packet sending interval, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the join/prune packet sending interval to 100 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim jp-timer 100
```

Notifications

If the join/prune packet sending interval is not within the range from 0 to 65535, the following notification will be displayed:

```
% Invalid Join/Prune timer value.
```

If the value of *interval* is greater than the maximum time of adding a prune packet, the following notification will be displayed:

```
WARNING: PIMv2 J/P timer too high, changed %u to %u sec
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 ipv6 pim neighbor-filter

Function

Run the **ipv6 pim neighbor-filter** command to enable the neighbor filtering function.

Run **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The neighbor filtering function is disabled by default.

Syntax

ipv6 pim neighbor-filter *acl-name*

no ipv6 pim neighbor-filter *acl-name*

default ipv6 pim neighbor-filter *acl-name*

Parameter Description

acl-name: ACL name that is used to limit the address range of neighbors. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The neighbor filtering function can strengthen PIM network security and limit the valid address range of neighbors. If a neighbor is filtered out based on an access filtering list, PIM-SMv6 does not create peer relationship with the neighbor or stops the peer relationship with this neighbor.

Examples

The following example uses the ACL to deny requests for establishing peer relationship with the neighbor FE80::2D0:F8FF:FE22:33AD on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl
Hostname(config-ipv6-acl)# deny ipv6 fe80::2d0:f8ff:fe22:33ad/128 any
Hostname(config-ipv6-acl)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim neighbor-filter acl
```

Notifications

If no ACL is configured, the following notification will be displayed:

```
% access-list acl not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 pim sparse-mode interface**

1.16 ipv6 pim neighbor-tracking

Function

Run the **ipv6 pim neighbor-tracking** command to enable the neighbor tracking function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The neighbor tracking function is disabled by default.

Syntax

Ipv6 pim neighbor-tracking

no ipv6 pim neighbor-tracking

default ipv6 pim neighbor-tracking

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After the suppression capability of an interface is enabled, when the local router plans to send a join packet to an uplink neighbor but it receives a join packet sent from the neighbor to the uplink router, this local router suppresses its own join packet. If the suppression capability of the interface is disabled, the join packet can be sent. When the suppression capability of downlink hosts is disabled, an uplink device can determine the number of the downlink hosts based on the quantity of received join packets. This is neighbor tracking.

Examples

The following example disables the suppression function on GigabitEthernet 0/1 and enables neighbor tracking.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim neighbor-tracking
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 ipv6 pim override-interval

Function

Run the **ipv6 pim override-interval** command to configure the prune override interval of an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default prune override interval of an interface is **2500** ms.

Syntax

ipv6 pim override-interval *override-interval*

no ipv6 pim override-interval

default ipv6 pim override-interval

Parameter Description

override-interval: Prune override interval of an interface, in milliseconds. The value range is from 1 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Modifying the propagation delay or prune override delay affects the prune override interval.

The network administrator needs to ensure that the prune override interval is smaller than the join/prune packet hold time. Otherwise, a short interrupt may occur.

Examples

The following example sets the prune override interval to 3000 ms on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim override-interval 3000
```

Notifications

If the configured prune override interval is not within the range from 1 to 65535, the following notification will be displayed:

```
% Invalid Hello option: override-interval value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 pim propagation-delay**
- **show ipv6 pim sparse-mode interface**

1.18 ipv6 pim probe-interval

Function

Run the **ipv6 pim probe-interval** command to configure the register-probe time.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default register-probe time is **5** seconds.

Syntax

ipv6 pim probe-interval *interval*

no ipv6 pim probe-interval

default ipv6 pim probe-interval

Parameter Description

interval: Register-probe interval, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The register-probe time refers to the time when the source DR is allowed to send null register messages to the RP before the register suppression timer times out.

The register-probe time cannot be greater than a half of the register suppression time. Otherwise, the configuration fails and an alarm is generated.

The sum of the three times of register suppression time and the register-probe time does not exceed 65535. Otherwise, the configuration fails and an alarm is generated.

Examples

The following example sets the register-probe time to 6 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim probe-interval 6
```

Notifications

If the configured register-probe time is not within the range from 1 to 65535, the following notification will be displayed:

```
% Invalid probe-interval value
```

If two times of the register-probe time is greater than the register suppression time, the following notification will be displayed:

```
WARNING: Register probe interval MUST be less than half the register suppression
interval. Please set a less one.
```

If the sum of three times of register suppression time and the register-probe time is greater than 65535, the following notification will be displayed:

```
WARNING: Register probe interval is too large. It may cause (3*RST+probe-
interval) > 65535.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 ipv6 pim propagation-delay

Function

Run the **ipv6 pim propagation-delay** command to configure the propagation delay of an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default propagation delay of an interface is **500** ms.

Syntax

ipv6 pim propagation-delay *propagation-delay*

no ipv6 pim propagation-delay

default ipv6 pim propagation-delay

Parameter Description

propagation-delay: Propagation delay of an interface, in milliseconds. The value range is from 1 to 32767.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Modifying the propagation delay or prune override delay affects the prune override interval.

The network administrator needs to ensure that the prune override interval is smaller than the join/prune packet hold time. Otherwise, a short interrupt may occur.

Examples

The following example sets the prune override delay to 600 ms on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim propagation-delay 600
```

Notifications

If the configured prune override delay is not within the range from 1 to 32767, the following notification will be displayed:

```
% Invalid Hello option: propagation-delay value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 pim override-interval**
- **show ipv6 pim sparse-mode interface**

1.20 ipv6 pim query-interval

Function

Run the **ipv6 pim query-interval** command to configure the hello message sending interval.

Run the **no** form of command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The hello message is sent at an interval of **30** seconds by default.

Syntax

ipv6 pim query-interval *interval*

no ipv6 pim query-interval

default ipv6 pim query-interval

Parameter Description

interval: Hello message sending interval, in seconds. The value range is from 1 to 65535.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When the hello message sending interval is updated, the hello message hold time is updated accordingly. The hello message hold time is 3.5 times of the hello message sending interval. If the product of the hello message sending interval and 3.5 is greater than 65535, the hello message sending interval is forcibly reset to 18725.

Examples

The following example sets the hello message sending interval to 60 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim query-interval 60
```

Notifications

If the configured hello message sending interval is not within the range from 1 to 32767, the following notification will be displayed:

```
% Invalid Query interval value
```

If the value of *interval* is greater than the maximum time of a request interval, the following notification will be displayed:

```
WARNING: PIMv2 Query interval too high, changed %u to %d sec.
(corresponding to maximum holdtime 0xFFFF)
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 pim sparse-mode interface**

1.21 ipv6 pim register-checksum-wholepkt

Function

Run the **ipv6 pim register-checksum-wholepkt** command to calculate the checksum of entire register messages.

Run the **no** form of this command to remove this configuration and calculate the checksum of headers of PIM packets and register messages, rather than the entire packets.

Run the **default** form of this command to restore the default configuration.

By default, only the headers of PIM packets and register messages, rather than the entire packets, are specified for calculating the checksum.

Syntax

ipv6 pim register-checksum-wholepkt [**group-list** *acl-name*]

no ipv6 pim register-checksum-wholepkt [**group-list** *acl-name*]

default ipv6 pim register-checksum-wholepkt [**group-list** *acl-name*]

Parameter Description

group-list *acl-name*: Uses an ACL name to limit the address range of multicast groups that support this configuration. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The checksum of the entire PIM protocol packets (including encapsulated multicast packets), rather than the PIM headers of separate register messages, is calculated.

If the **group-list** parameter is not specified, the entire packet checksum calculation method applies to register messages with any group address.

If you run the **no** or **default** form of this command to specify the **group-list** parameter and specify to use the configured ACL, the limits of the ACL associated with the **group-list** parameter are removed. In this case, the entire packet checksum calculation method applies to register messages with any group address.

Examples

The following example uses the ACL checksum-access-list to apply the entire packet checksum calculation method to the register messages with the multicast group address FF66::6666/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list checksum-access-list
Hostname(config-ipv6-acl)# permit ipv6 any ff66::6666/64
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim register-checksum-wholepkt group-list checksum-access-
list
```

Notifications

If no ACL is configured, the following notification will be displayed:

```
% access-list checksum-access-list not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 ipv6 pim register-rate-limit

Function

Run the **ipv6 pim register-rate-limit** command to limit the sending rate of register messages.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The sending rate of register messages is not limited by default.

Syntax

ipv6 pim register-rate-limit *rate*

no ipv6 pim register-rate-limit

default ipv6 pim register-rate-limit

Parameter Description

rate: Maximum number of register messages that can be sent per second. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the sending rate of register messages in (S, G) status, rather than that of the entire system. Running this command can reduce the load of the source DR and RP. Register messages sent at a rate exceeding the limit are discarded.

Examples

The following example limits the sending rate of register messages to 3000 per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim register-rate-limit 3000
```

Notifications

If the configured sending rate of register messages is not within the range from 1 to 65535, the following notification will be displayed:

```
% Invalid Limit value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 ipv6 pim register-rp-reachability

Function

Run the **ipv6 pim register-rp-reachability** command to enable the RP reachability checking function before a register message is sent.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The RP reachability checking function before a register message is sent is disabled by default.

Syntax

ipv6 pim register-rp-reachability

no ipv6 pim register-rp-reachability

default ipv6 pim register-rp-reachability

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run, the RP reachability is checked before a register message is sent. If the RP is reachable, the register message is sent. Otherwise, the register message is not sent.

Examples

The following example enables the RP reachability checking function before a register message is sent.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim register-rp-reachability
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 ipv6 pim register-source

Function

Run the **ipv6 pim register-source** command to specify a source IPv6 address in register messages.

Run the **no** form of this command to remove this configuration and use the address of the DR interface connected to the source as the source IPv6 address in register messages.

Run the **default** form of this command to restore the default configuration.

The source IPv6 address in register messages is the address of the DR interface connected to the source by default.

Syntax

ipv6 pim register-source { *ipv6-local-address* | *interface-type interface-number* }

no ipv6 pim register-source

default ipv6 pim register-source

Parameter Description

ipv6-local-address: Source IPv6 address in register messages.

interface-type interface-number: Interface type and interface number. The IPv6 address of this interface is specified as the source address in register messages.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run, the RP reachability is checked before a register message is sent. If the RP is reachable, the message is sent. Otherwise, the message is not sent.

It is recommended that loopback address be used as the source IP address in register messages. Other physical addresses can be used as the source IP addresses in register messages as well.

Examples

The following example specifies the IPv6 address 3333::3333 as the source address in register messages.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim register-source 3333::3333
```

The following example specifies the IPv6 address of GigabitEthernet 0/1 as the source IP address in register messages.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ipv6 pim register-source gigabitethernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 ipv6 pim register-suppression

Function

Run the **ipv6 pim register-suppression** command to configure the register suppression time.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default register suppression time is **60** seconds.

Syntax

ipv6 pim register-suppression *suppression-time*

no ipv6 pim register-suppression

default ipv6 pim register-suppression

Parameter Description

suppression-time: Register suppression time, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command can be run on the DR to configure the register message suppression time.

If the **ipv6 pim rp-register-kat** command is not run, configuring the register suppression time on the RP changes the (S, G) entry timeout period. The (S, G) entry timeout period on an RP is the sum of three times of the register suppression time and the register-probe time.

Examples

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

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim register-suppression 100
```

Notifications

If the configured register suppression time is not within the range from 1 to 65535, the following notification will be displayed:

```
% Invalid KAT value
```

If two times of the register-probe time is greater than the register message suppression time, the following notification will be displayed:

```
WARNING: Register suppression interval MUST be larger than twice the register
probe interval. Please set a larger one.
```

If the sum of three times of register suppression time and the register-probe time is greater than 65535, the following notification will be displayed:

```
WARNING: Register suppression interval is too large. It may cause (3*RST+probe-
interval) > 65535.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 ipv6 pim rp-address

Function

Run the **ipv6 pim rp-address** command to configure static RPs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No static RP is configured by default.

Syntax

ipv6 pim rp-address *ipv6-rp-address* [*acl-name*]

no ipv6 pim rp-address *ipv6-rp-address*

default ipv6 pim rp-address *ipv6-rp-address*

Parameter Description

ipv6-rp-address: IPv6 address of a static RP.

acl-name: ACL name that is used to limit address range of multicast groups served by static RPs. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If static and dynamic RPs are available at the same time, dynamic RPs are preferred.

If multiple static RPs serve the same multicast group, the static RP with a larger address is preferred.

If the *acl-name* parameter is not specified, the static RPs serve all groups.

Examples

The following example configures the static RP 3333::3333 to serve the multicast group with the address FF66::6666/64 limited by the ACL acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl
Hostname(config-ipv6-acl)# permit ipv6 any ff66::6666/64
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim rp-address 3333::3333 acl
```

Notifications

If the configured RP address is not a valid address, the following notification will be displayed:

```
Illegal RP address, ignored
```

If the number of the RP addresses reaches the upper limit, the following notification will be displayed:

```
Reach PIM-SMv6 static RP configuration limit 65536!
```

If no ACL is configured, the following notification will be displayed:

```
% access-list acl not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 pim sparse-mode rp mapping**
- **show ipv6 pim sparse-mode rp-hash**

1.27 ipv6 pim rp-candidate

Function

Run the **ipv6 pim rp-candidate** command to configure C-RPs.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No C-RP is configured by default.

Syntax

ipv6 pim rp-candidate *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval*] [**group-list** *acl-name*]

no ipv6 pim rp-candidate [*interface-type interface-number*]

default ipv6 pim rp-candidate [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface number. The address of this interface is specified as the address of a C-RP.

priority *priority-value*: Specifies the C-RP priority. The value range is from 0 to 255, and the default value is **192**.

interval *interval*: Specifies the interval of sending C-RP messages to the BSR, in seconds. The value range is from 1 to 16383, and the default value is **60**.

group-list *acl-name*: Uses an ACL name to limit the address range of multicast groups served by a C-RP. The value is a case-sensitive string of 1 to 99 characters. If this parameter is not specified, the C-RP serves all groups.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In PIM-SMv6, an RPT created based on multicast routing takes the RP as a root. After a BSR is elected, all C-RPs periodically send unicast messages to the BSR and then the BSR forwards the messages throughout the PIM domain.

When an ACL is used to specify the address range of groups served by the C-RP, only the permit access control entry (ACE) is calculated, and the deny ACE is not calculated.

Examples

The following example configures the address of GigabitEthernet 0/1 as the C-RP address, sets the RP priority to 200 and the interval of sending C-RP messages to the BSR to 40 seconds, and uses the ACL to limit the address range of groups served by the C-RP to FF66::6666/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl
Hostname(config-ipv6-acl)# permit ipv6 any ff66::6666/64
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim rp-candidate gigabitethernet 0/1 priority 200 group-
list acl interval 40
```

```
Hostname(config)# ipv6 access-list acl
Hostname(config-ipv6-acl)# permit ipv6 any ff66::6666/64
```

Notifications

If the C-RP priority is not within the range from 0 to 255, the following notification will be displayed:

```
% Invalid C-RP Priority value
```

If the interval of sending C-RP messages to the BSR is not within the range from 1 to 16383 seconds, the following notification will be displayed:

```
% Invalid C-RP advertisement intvl value
```

If the multicast function is not enabled on an interface, the following notification will be displayed:

```
Warning: PIMSMv6 not configured on %s, Candidate-RP not advertised
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 ipv6 pim rp-register-kat

Function

Run the **ipv6 pim rp-register-kat** command to configure the (S, G) entry timeout period on an RP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The (S, G) entry timeout period on an RP is the sum of three times of the register suppression time and the register-probe time by default.

Syntax

ipv6 pim rp-register-kat *interval*

no ipv6 pim rp-register-kat

default ipv6 pim rp-register-kat

Parameter Description

Interval: (S, G) entry timeout period on an RP, in seconds. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The value of the (S, G) entry timeout timer on an RP should be greater than the sum of three times of the register suppression time and the register-probe time on the source DR. Otherwise, the (S, G) on the RP may time out before the source DR sends register messages again, causing a short interrupt of multicast streams.

Examples

The following example sets the (S, G) entry timeout period in register messages to 250 seconds on an RP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim rp-register-kat 250
```

Notifications

If the configured (S, G) entry timeout period on an RP is not within the range from 1 to 65535, the following notification will be displayed:

```
% Invalid KAT value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 ipv6 pim rp embedded

Function

Run the **ipv6 pim rp embedded** command to enable the RP address embedding function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

For the IPv6 addresses of multicast groups that support RP address embedding, the RP address embedding function is enabled by default.

Syntax

ipv6 pim rp embedded [**group-list** *acl-name*]

no ipv6 pim rp embedded

default ipv6 pim rp embedded

Parameter Description

group-list *acl-name*: Uses an ACL name to limit the address range of multicast groups. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the **group-list** parameter is not specified, the RP address embedding function is enabled on all IPv6 addresses of multicast groups that support RP address embedding.

Examples

The following example enables the RP address embedding function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim rp embedded
```

Notifications

If the group-list is not in the embedded RP linked list, the following notification will be displayed:

```
RP embedded is configured with the same ACL again
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 pim sparse-mode rp-hash**

1.30 ipv6 pim sparse-mode

Function

Run the **ipv6 pim sparse-mode** command to enable the PIM-SMv6 function on an interface.

Run the **no** form of this command to disable this function on an interface.

Run the **default** form of this command to restore the default configuration.

The PIM-SMv6 function on an interface is disabled by default.

Syntax

ipv6 pim sparse-mode

no ipv6 pim sparse-mode

default ipv6 pim sparse-mode

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Before PIM-SMv6 is enabled, you must enable the multicast routing and forwarding function in global configuration mode. Otherwise, multicast packets cannot be sent even if PIM-SMv6 is enabled.

When PIM-SMv6 is enabled, MLD is automatically enabled on different interfaces.

The multicast function can be enabled on a tunnel interface that does not support multicast. In this case, no notification will be displayed and multicast packets will not be sent or received.

A multicast tunnel cannot be nested and does not support multicast data QoS/ACL.

IPv6 multicast forwarding is not supported on a super VLAN.

Examples

The following example enables the PIM-SMv6 function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim sparse-mode
```

Notifications

If the specified interface does not exist, the following notification will be displayed:

```
ipv6 pim sparse-mode (vif == NULL)
```

If the multicast function is not enabled, the following notification will be displayed:

```
WARNING:  \"ip multicast-routing\"  is not configured
```

If the number of configured multicast interfaces exceeds the upper limit, the following notification will be displayed:

```
PIM-SMv6 Configure failed! VIF limit exceeded in NSM!!!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 multicast-routing** (IPv6 multicast routing management)

1.31 ipv6 pim sparse-mode passive

Function

Run the **ipv6 pim sparse-mode passive** command to enable the PIM-SMv6 passive mode on an interface.

Run the **no** form of this command to disable this mode.

Run the **default** form of this command to restore the default configuration.

The PIM-SMv6 mode is disabled on an interface by default.

Syntax

ipv6 pim sparse-mode passive

no ipv6 pim sparse-mode passive

default ipv6 pim sparse-mode passive

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Before the PIM-SMv6 passive mode is enabled, you must enable the multicast routing and forwarding function in global configuration mode. Otherwise, multicast packets cannot be sent even if the PIM-SMv6 passive mode is enabled.

When the PIM-SMv6 mode is enabled, MLD is automatically enabled on different interfaces.

After the PIM-SMv6 passive mode is enabled on an interface, the interface does not receive or send PIM packets, but it can forward multicast packets. It is recommended that the PIM-SMv6 passive mode be enabled on an interface of a stub routing device connected to hosts. This avoids L2 flooding of the PIM hello messages.

Examples

The following example enables the PIM-SMv6 passive mode on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim sparse-mode passive
```

Notifications

N/A

Common Errors

If the PIM-SMv6 passive mode is enabled on an interface connected to a source, the source interface does not send or receive PIM packets. Consequently, the source loses the DR election capability. It is not recommended that the PIM-SMv6 passive mode be enabled on an interface connected to a source.

After the PIM-SMv6 passive mode is enabled on an interface, if two devices in the same network segment forward multicast data, assertion election cannot proceed. As a result, two identical multicast packets are sent to this network segment.

If the PIM-SMv6 passive mode is enabled on an interface of an intermediate device deployed on an L3 multicast network, the networking fails because the interface does not receive or send PIM packets.

Platform Description

N/A

Related Commands

- **ipv6 multicast-routing** (IPv6 multicast routing management)

1.32 ipv6 pim spt-threshold

Function

Run the **ipv6 pim spt-threshold** command to enable the shortest path tree (SPT) switchover function.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The SPT switchover function is disabled by default.

Syntax

ipv6 pim spt-threshold [**group-list** *acl-name*]

no ipv6 pim spt-threshold [**group-list** *acl-name*]

default ipv6 pim spt-threshold [**group-list** *acl-name*]

Parameter Description

group-list *acl-name*: Uses an ACL name to limit the address range of groups that support SPT switchover. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the **group-list** *acl-name* parameter is not specified, all multicast groups support SPT switchover.

If you run the **no** or **default** form of this command to specify the **group-list** parameter and specify to use the configured ACL, the limits on the ACL associated with the **group-list** parameter are removed. In this case, all groups are allowed to switch over from an RPT to an SPT.

Examples

The following example uses the ACL acl to set the address range of the multicast source that supports SPT switchover to FE80::2D0:F8FF:FE22:33AD and the address range of the multicast group to FF66::6666/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl
```

```
Hostname(config-ipv6-acl)# permit ipv6 fe80::2d0:f8ff:fe22:33ad/128 ff66::6666/64
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim spt-threshold group-list acl
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.33 ipv6 pim ssm

Function

Run the **ipv6 pim ssm** command to enable the SSM function and configure an SSM group address range.

Run the **no** form of this command to disable this function.

Run the **default** form of this command to restore the default configuration.

The SSM function is disabled by default.

Syntax

ipv6 pim ssm { **default** | **range** *acl-name* }

no ipv6 pim ssm

default ipv6 pim ssm

Parameter Description

default: Specifies the default SSM group address range to FF3X::/32.

range *acl-name*: Uses an ACL name to limit the SSM group address range. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If SSM needs to be applied in a PIM-SMv6 network, this command must be run.

Examples

The following example enables the SSM function and sets the multicast source address range to FE80::2D0:F8FF:FE22:33AD/128 and the multicast group address range to FF32::3333/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list acl
Hostname(config-ipv6-acl)# permit ipv6 fe80::2d0:f8ff:fe22:33ad/128 ff32::3333/64
Hostname(config-ipv6-acl)# exit
Hostname(config)# ipv6 pim ssm range acl
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ipv6 mld ssm-map enable** (MLD)
- **ipv6 mld ssm-map static** (MLD)
- **show ipv6 mld ssm-mapping** (MLD)

1.34 ipv6 pim static-rp-preferred

Function

Run the **ipv6 pim static-rp-preferred** command to configure static DR priority to be higher than dynamic RP priority.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Dynamic RP priority is higher than static DR priority by default.

Syntax

ipv6 pim static-rp-preferred

no ipv6 pim static-rp-preferred

default ipv6 pim static-rp-preferred

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run, the static RP priority is higher than the dynamic DR priority.

Examples

The following example configures static DR priority to be higher than dynamic RP priority.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 pim static-rp-preferred
```

Notifications

After static DR priority is configured to be higher than dynamic RP priority and RP switchover is performed, the following notification will be displayed.

```
RP is changed for group range %R/%u.  Perform RP change handler
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 pim rp-address

1.35 ipv6 pim triggered-hello-delay

Function

Run the **ipv6 pim triggered-hello-delay** command to configure the hello message sending delay on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default hello message sending delay is **5** seconds.

Syntax

ipv6 pim triggered-hello-delay *delay*

no ipv6 pim triggered-hello-delay

default ipv6 pim triggered-hello-delay

Parameter Description

delay: Hello message sending delay, in seconds. The value range is from 1 to 5.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When an interface is enabled or detects a new neighbor, a random time is generated. Within this time, the interface sends hello messages out.

Examples

The following example sets the hello message sending delay to 3 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 pim triggered-hello-delay 3
```

Notifications

If the hello message sending delay is not within the range from 1 to 5, the following notification will be displayed:

```
% Invalid Hello option: triggered-hello-delay value
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ipv6 pim sparse-mode interface**

1.36 show ipv6 pim sparse-mode bsr-router

Function

Run the **show ipv6 pim sparse-mode bsr-router** command to display BSR information.

Syntax

show ipv6 pim sparse-mode bsr-router

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays BSR information.

```
Hostname> enable
Hostname# 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
```

Table 1-1Output Fields of the show ipv6 pim sparse-mode bsr-router Command

Field	Description
BSR address	BSR address
Uptime	Update time
BSR Priority	BSR priority
Hash mask length	Hash mask length
Next bootstrap message in *time*	Next bootstrap time
Role	BSR role
Priority	Priority
Hash mask length	Hash mask length
State	BSR status
Candidate RP	C-RP address
Advertisement interval *advertisement-interval* seconds	C-RP advertisement interval
Next Cand_RP_advertisement in *time*	Next C-RP advertisement time

Notifications

N/A

Platform Description

N/A

1.37 show ipv6 pim sparse-mode interface

Function

Run the **show ipv6 pim sparse-mode interface** command to display PIM-SMv6 information of an interface.

Syntax

show ipv6 pim sparse-mode interface [*interface-type interface-number*] [**detail**]

Parameter Description

interface-type interface-number: Interface type and interface number. If this parameter is not specified, the PIM-SMv6 information of all interfaces is displayed.

detail: Displays the detailed PIM-SMv6 information of an interface. If this parameter is not specified, the summary information of an interface is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays PIM-SMv6 information of an interface.

```
Hostname> enable
Hostname# 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
```

Table 1-1 Output Fields of the show ipv6 pim sparse-mode interface detail Command

Field	Description
Address	Interface address
DR	Address of a DR in the same shared network segment as the interface
Hello period *hello-interval* seconds	Hello message sending interval: *hello-interval* seconds
Next Hello in *next-hello-time* seconds	Next hello message *next-hello-time* seconds later
Triggered Hello period *triggered-hello-time* seconds	Triggered-Hello-Delay of an interface: *triggered-hello-time* seconds
Secondary addresses	Secondary address
Neighbors	Neighbors on an interface

Notifications

N/A

Platform Description

N/A

1.38 show ipv6 pim sparse-mode local-members

Function

Run the **show ipv6 pim sparse-mode local-members** command to display local MLD information of a PIM-SMv6 interface.

Syntax

show ipv6 pim sparse-mode local-members [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface number. If this parameter is not specified, the local MLD information of all PIM-SMv6 interfaces is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays local MLD information of a PIM-SMv6 interface.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode local-members
PIM Local membership information
GigabitEthernet 0/5:
  (*, ff66::6666) : Include
```

Table 1-1 Output Fields of the show ipv6 pim sparse-mode local-members Command

Field	Description
PIM Local membership information	Local member information
interface-type interface-number	Interface type and interface number
(*source*, *ipv6-group-address*): mode	(Multicast source, IPv6 multicast group): source filtering mode

Notifications

N/A

Platform Description

N/A

1.39 show ipv6 pim sparse-mode mroute

Function

Run the **show ipv6 pim sparse-mode mroute** command to display PIM-SMv6 routing information.

Syntax

show ipv6 pim sparse-mode mroute [*ipv6-group-or-source-address* [*ipv6-group-or-source-address*]]

Parameter Description

ipv6-group-or-source-address: Address of an IPv6 multicast group or source (the two addresses cannot be both multicast group addresses or both source addresses).

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

Either a source address or a group address can be specified.

A source address and a group address can be specified together.

If you want to configure two addresses, they cannot be both multicast group addresses or both source addresses

If no parameter is specified, all PIM-SMv6 routing information is displayed.

Examples

The following example displays PIM-SMv6 routing information.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
REG Entries: 0

(*, ff16::1)
RP: 3000::5
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .
i  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
Joined
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
FCR:

(1100::2, ff16::1)
RPF nbr: fe80::21a:a9ff:fe3a:6355
RPF idx: GigabitEthernet 0/2
SPT bit: 1
```

```
Upstream State: JOINED
jt_timer expires in 44 seconds
kat expires in 194 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
Joined
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
Outgoing
0  .  .
o  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .

(1100::2, ff16::1, rpt)
RP: 3000::5
RPF nbr: ::
RPF idx: None
Upstream State: PRUNED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
Pruned
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
Outgoing
```

```
0 . .
o . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . .
```

Table 1-1Output Fields of the show ipv6 pim sparse-mode mroute Command

Field	Description
IPv6 Multicast Routing Table	IPv6 multicast routing table
(*,*,RP) Entries	Number of (*, *, RP) entries
(*,G) Entries	Number of (*, G) entries
(S,G) Entries	Number of (S, G) entries
(S,G,rpt) Entries	Number of (S, G, RPT) entries
FCR Entries	Number of FCR entries
REG Entries	Number of register entries
RPF nbr	RPF neighbor
RPF idx	RPF interface index
SPT bit	SPT flag bit: 0 or 1 ● **0**: No multicast data is received. ● **1**: Multicast data is received.
Upstream State	Uplink neighbor status includes PRUNED, NOT PRUNED, JOINED, NOT JOINED, PRUNE_PENDING, and RPT NOT JOINED.
jt_timer expires in *jt-expire-time* seconds	Prune expires *jt-expire-time* seconds later.
kat expires in *kat-expire-time* seconds	(S, G) entry expires *kat-expire-time* seconds later.
Local	Inbound interface of a local multicast group
Pruned	Inbound interface for receiving prune packets
Joined	Inbound interface for receiving join packets
Asserted	Inbound interface for receiving assert packets
Outgoing	Outbound interface for forwarding entries

Notifications

N/A

Platform Description

N/A

1.40 show ipv6 pim sparse-mode neighbor

Function

Run the **show ipv6 pim sparse-mode neighbor** command to display neighbor information.

Syntax

show ipv6 pim sparse-mode neighbor [**detail**]

Parameter Description

detail: Displays detailed neighbor information. If this parameter is not specified, the summary information of a neighbor is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays neighbor information.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode neighbor detail
Nbr fe80::2d0:f8ff:fe22:34b3 (GigabitEthernet 0/5)
 Expires in 86 seconds
  Secondary addresses:
   6666::6666
```

Table 1-1 Output Fields of the show ipv6 pim sparse-mode neighbor detail Command

Field	Description
Nbr	Neighbor information
Expires in *expire-time* seconds	Expiry in *expire-time* seconds
Secondary addresses	Secondary address

Notifications

N/A

Platform Description

N/A

1.41 show ipv6 pim sparse-mode nexthop

Function

Run the **show ipv6 pim sparse-mode nexthop** command to display next hop information, including interface, address, and metric value of a next hop.

Syntax

show ipv6 pim sparse-mode nexthop

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the PIM-SMv6 next hop information.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination   Type Nxhp Nexthop                    Nexthop
Metrc Pref Rcnt
                     Num   Addr                        Name
_____________________________________________________________________________
_
100::2        .RS.  1    fe80::21a:a9ff:fe51:2d17 AggregatePort 64.3014   1
110  1
```

Table 1-1 Output Fields of the show ipv6 pim sparse-mode nexthop Command

Field	Description
Destination	Destination address
Type	Type

Field	Description
Nexthop Num	Number of next hops
Nexthop Addr	Next hop address
Nexthop Name	Outbound interface of next hop
Metric	Number of hops to reach the destination address
Pref	Priority of unicast route to reach the destination address
Refcnt	Reference count

Notifications

N/A

Platform Description

N/A

1.42 show ipv6 pim sparse-mode rp mapping

Function

Run the **show ipv6 pim sparse-mode rp mapping** command to display all RPs and the groups served by the RPs on the local device.

Syntax

show ipv6 pim sparse-mode rp mapping

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all RPs and the groups served by the RPs on the local device.

```
Hostname> enable
Hostname# 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
```

Table 1-1 Output Fields of the show ipv6 pim sparse-mode rp mapping Command

Field	Description
PIM Group-to-RP Mappings	Mapping of PIM RPs to the groups served by the RPs
Group(s)	Address/Mask of a group
RP: *ipv6-rp-address*	RP address: *ipv6-rp-address*
Info source: *ipv6-rp-address*, via bootstrap, priority *priority*	RP address *ipv6-rp-address* is obtained from a BSM, with the priority *priority*.
Uptime	Update time
expires	Expiry time

Notifications

N/A

Platform Description

N/A

1.43 show ipv6 pim sparse-mode rp-hash

Function

Run the **show ipv6 pim sparse-mode rp-hash** command to display RP information corresponding to a multicast group address.

Syntax

show ipv6 pim sparse-mode rp-hash *ipv6-group-address*

Parameter Description

ipv6-group-address: Address of an IPv6 multicast group.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays RP information corresponding to a group address FF66::6666.

```
Hostname> enable
Hostname# show ipv6 pim sparse-mode rp-hash ff66::6666
 RP: 20::2
Info source: 20::2, via bootstrap

PIMv2 Hash Value 126
RP 20::2, via bootstrap, priority 200, hash value 2007554652
RP 20::1, via bootstrap, priority 200, hash value 844492565
```

Table 1-1 Output Fields of the show ipv6 pim sparse-mode rp-hash Command

Field	Description
RP: *ipv6-rp-address*	Address of the RP serving this multicast group: *ipv6-rp-address*
Info source: *ipv6-rp-address*,via bootstrap	RP address *ipv6-rp-address* is obtained from a BSM.
PIMv2 Hash Value *hash-value*	PIMv2 hash value: *hash-value*
RP *ipv6-rp-address*, via bootstrap, priority *priority* hash value *hash-value*	RP address *ipv6-rp-address* is obtained from a BSM, with the priority *priority* and hash value *hash-value*.

Notifications

N/A

Platform Description

N/A

1.44 show ipv6 pim sparse-mode track

Function

Run the **show ipv6 pim sparse-mode track** command to display the number of PIM packets sent and received since the statistic start time.

Syntax

show ipv6 pim sparse-mode track

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

When the system is started for the first time, the statistic start time is set. If you run the **clear ipv6 pim sparse-mode track** command, the statistic start time and the PIM packet counter are reset.

Examples

The following example displays the number of PIM packets sent and received since the statistic start time.

```
Hostname> enable
Hostname# 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
```

Table 1-1Output Fields of the show ipv6 pim sparse-mode track Command

Field	Description
Elapsed time since counters cleared	Duration since the statistic start time till now
Received	Number of received PIM packets
sent	Number of sent PIM packets
Valid PIMSMv6 packets	Valid PIM-SM packets
Hello	Statistical value of hello messages
Join-Prune	Statistical value of join-prune packets
Register	Statistical value of register messages

Field	Description
Register-Stop	Statistical value of register-stop packets
Assert	Statistical value of assert packets
BSM	Statistical value of BSMs
C-RP-ADV	Statistical value of C-RP advertisement packets
PIMDMv6-Graft	Statistical value of PIM-DMv6 graft packets
PIMDMv6-Graft-Ack	Statistical value of PIM-DMv6 graft acknowledgment packets
PIMDMv6-State-Refresh	Statistical value of PIM-DM SRMs
Unknown PIMv6 Type	Unknown PIM packets
Errors	Statistical value of error packets
Malformed packets	Number of malformed packets
Bad checksums	Number of packets with incorrect checksums
Send errors	Number of sent error packets
Packets received with unknown PIMv6 version	Number of PIM packets with unknown version

Notifications

N/A

Platform Description

N/A