1 PIM-SM Commands

Command	Function
clear ip pim sparse-mode bsr rp-set	Clear dynamic rendezvous point (RP) information.
clear ip pim sparse-mode track	Reset the statistics start time and clear the counter of the PIM packets.
ip pim accept-bsr list	Limit the BSR address range.
ip pim accept-crp-with-null-group	Enable the BSR to receive C-RP-ADV packets with Prefix-Count being 0.
ip pim accept-crp list	Limit the C-RP address range and the address range of the groups served by the C-RPs.
ip pim accept-register	Limit the (S, G) address range in the register messages.
ip pim bsr-border	Configure a BSR border.
ip pim bsr-candidate	Configure C-BSRs.
ip pim bfd	Configure PIM-BFD correlation.
ip pim dr-priority	Configure the DR priority.
ip pim ignore-rp-set-priority	Ignore RP priority for RP election.
ip pim jp-timer	Configure the join/prune packet sending interval.
ip pim neighbor-filter	Enable the neighbor filtering function.
ip pim neighbor-tracking	Enable the neighbor tracking function.
ip pim override-interval	Configure the prune override interval of an interface.
ip pim probe-interval	Configure the register-probe time.
ip pim propagation-delay	Configure the propagation delay of an interface.
ip pim query-interval	Configure the hello message sending interval.
ip pim register-checksum-wholepkt	Calculate the checksum of entire packets.
ip pim register-decapsulate-forward	Enable the function for the RP to decapsulate register messages and forward multicast packets in the messages.
ip pim register-rate-limit	Limit the sending rate of register messages.

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

1.1 clear ip pim sparse-mode bsr rp-set

Function

Run the **clear ip pim sparse-mode bsr rp-set** command to clear dynamic rendezvous point (RP) information.

Syntax

clear ip 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 refresh the RP-Set.

This command cannot clear static RPs.

Examples

The following example clears dynamic RP-Set information.

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

Notifications

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

```
RP is changed for group range 224.0.0.0/4.  Perform RP change handler
```

Platform Description

N/A

1.2 clear ip pim sparse-mode track

Function

Run the **clear ip pim sparse-mode track** command to reset the statistics start time and clear the counter of the PIM packets.

Syntax

clear ip 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 the counter of the PIM packets.

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

Notifications

```
N/A
```

Platform Description

N/A

1.3 ip pim accept-bsr list

Function

Run the **ip pim accept-bsr list** command to limit the BSR address range.

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

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

The BSR address range is not limited by default.

Syntax

ip pim accept-bsr list { *acl-name* | *acl-number* }

no ip pim accept-bsr

default ip pim accept-bsr

Parameter Description

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

list *acl-number*: Uses a standard IP ACL number to limit the BSR address range. The value range is from 1 to 99 or from 1300 to 1999.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is run, the PIM-SM device receives only BSMs sent by legitimate BSRs.

Examples

The following example receives BSMs sent by the legitimate BSRs determined by the access list 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Hostname(config)# ip pim accept-bsr list 1
```

Notifications

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

```
% access-list 1 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ip pim bsr-candidate

1.4 ip pim accept-crp-with-null-group

Function

Run the **ip pim accept-crp-with-null-group** command to enable the BSR to receive C-RP-ADV packets with Prefix-Count 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 C-RP-ADV packets with Prefix-Count being 0 is disabled by default.

Syntax

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

N/A

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 receive C-RP-ADV packets with Prefix-Count being 0. This C-RP can support all groups.

Examples

The following example enables the BSR to receive C-RP-ADV packets with Prefix-Count being 0.

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ip pim accept-crp list

Function

Run the **ip 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

ip pim accept-crp list { *acl-name* | *acl-number* }

no ip pim accept-crp

default ip pim accept-crp

Parameter Description

list *acl-name*: Uses an extended IP 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.

list *acl-number*: Uses an extended IP ACL number to limit the C-RP address range and the address range of the groups served by the C-RPs. The value range is from 100 to 199 or from 2000 to 2699.

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 sets the C-RP address range and the address range of the groups served by the C-RPs to extended ACL 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list extended 100
Hostname(config-ext-nacl)# permit ip 192.168.195.0 0.0.0.255 225.1.1.1 0.0.0.255
Hostname(config-ext-nacl)# exit
Hostname(config)# ip pim accept-crp list 100
```

Notifications

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

```
% access-list 1 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ip pim rp-candidate

1.6 ip pim accept-register

Function

Run the **ip pim accept-register** command to limit the (S, G) address range in the 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 (S, G) address range of register messages is not limited by default. The RP receives register messages with any (S, G) address.

Syntax

ip pim accept-register { **list** { *acl-name* | *acl-number* } | **route-map** *route-map-name* } *
no ip pim accept-register
default ip pim accept-register

Parameter Description

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

list *acl-number*: Uses an extended IP ACL number to limit the (S, G) address range. The value range is from 100 to 199 or from 2000 to 2699.

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

This command can be run on a static RP or C-RP to limit the (S, G) address range in register messages.

Examples

The following example sets the (S, G) address range in register messages to access list 100, the source address to 192.168.195.0 with reverse mask 0.0.0.255, and the multicast group address to 255.1.1.1 with reverse mask 0.0.0.255.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 100 permit ip 192.168.195.0 0.0.0.255 225.1.1.1
0.0.0.255
Hostname(config)# ip pim accept-register list 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 ip pim bsr-border

Function

Run the **ip 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

ip pim bsr-border
no ip pim bsr-border
default ip pim bsr-border

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

To limit 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 of PIM on GigabitEthernet 0/1.

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip multicast boundary** (IPv4 multicast route management)
- **show ip pim sparse-mode interface**

1.8 ip pim bsr-candidate

Function

Run the **ip 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

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

no ip pim bsr-candidate

default ip pim bsr-candidate

Parameter Description

interface-type interface-number: Specified interface.

hash-mask-length: Length of a hash mask configured for the RP election mechanism. The value range is from 0 to 32, and the default value is **10**.

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-SM 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 with the multicast address 224.0.0.13 in the PIM-SM 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 interface assigned to the 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 a C-BSR to send a BSM through GigabitEthernet 0/1, and sets the hash mask length for the RP election mechanism to **30** and the priority to **192**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip pim bsr-candidate GigabitEthernet 0/1 30 192
```

Notifications

If the current interface is not set to the SM mode, the following notification will be displayed:

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

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 ip pim bfd

Function

Run the **ip pim bfd** command to configure PIM-BFD correlation.

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

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

Syntax

ip pim bfd

no ip pim bfd

default ip 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-SM 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 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 PIM-BFD correlation on GigabitEthernet 0/1.

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

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

1.10 ip pim dr-priority

Function

Run the **ip 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

ip pim dr-priority *priority-value*

no ip pim dr-priority

default ip 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 **10000** on GigabitEthernet 0/1.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim dr-priority 10000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip pim sparse-mode interface**

1.11 ip pim ignore-rp-set-priority

Function

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

Run the **no** form of this command to preferentially select the C-RP with a higher priority.

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

ip pim ignore-rp-set-priority
no ip pim ignore-rp-set-priority
default ip 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 configures to ignore RP priority for RP election.

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 ip pim jp-timer

Function

Run the **ip 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

ip pim jp-timer *interval*

no ip pim jp-timer

default ip 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 50 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip pim jp-timer 50
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 ip pim neighbor-filter

Function

Run the **ip pim neighbor-filter** command to enable the neighbor filtering 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 filtering function is disabled by default.

Syntax

ip pim neighbor-filter { *acl-name* | *acl-number* }

no ip pim neighbor-filter { *acl-name* | *acl-number* }

default ip pim neighbor-filter { *acl-name* | *acl-number* }

Parameter Description

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

acl-number: Standard IP ACL number that is used to limit the address range of neighbors. The value range is from 1 to 99.

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-SM does not create peer relationship with the neighbor or stops the peer relationship with this neighbor.

Examples

The following example uses ACL 14 to filter out a neighbor with the IP address 192.168.1.5 and the mask 0.0.0.255 on GigabitEthernet 0/1. PIM-SM does not create peer relationship with the neighbor (192.168.1.5).

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

```
Hostname(config)# access-list 14 deny 192.168.1.5 0.0.0.255
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim neighbor-filter 14
Hostname(config-if-GigabitEthernet 0/1)# exit
```

Notifications

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

```
% access-list 14 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip pim sparse-mode interface**

1.14 ip pim neighbor-tracking

Function

Run the **ip 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

ip pim neighbor-tracking

no ip pim neighbor-tracking

default ip 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 a multicast device plans to send a join packet to an uplink multicast device but it receives a join packet sent from the neighbor to the uplink multicast device, this local multicast device 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 to implement neighbor tracking.

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 ip pim override-interval

Function

Run the **ip 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 is **2500** ms.

Syntax

ip pim override-interval *override-interval*

no ip pim override-interval

default ip pim override-interval

Parameter Description

override-interval: Prune override interval, 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 override delay affects the prune override interval.

The network administrator needs to ensure that the prune override interval is smaller than the 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)# ip pim override-interval 3000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ip pim propagation-delay
- show ip pim sparse-mode interface

1.16 ip pim probe-interval

Function

Run the **ip 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

ip pim probe-interval *interval*

no ip pim probe-interval

default ip 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 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)# ip pim probe-interval 6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 ip pim propagation-delay

Function

Run the **ip 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

ip pim propagation-delay *propagation-delay*

no ip pim propagation-delay

default ip pim propagation-delay

Parameter Description

propagation-delay: Propagation delay, 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 override delay affects the prune override interval.

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

Examples

The following example sets the 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)# ip pim propagation-delay 600
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ip pim override-interval
- show ip pim sparse-mode interface

1.18 ip pim query-interval

Function

Run the **ip pim query-interval** command to configure the hello message 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 hello message is sent at an interval of **30** seconds by default.

Syntax

ip pim query-interval *interval*

no ip pim query-interval

default ip 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 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 123 seconds on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim query-interval 123
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip pim sparse-mode interface**

1.19 ip pim register-checksum-wholepkt

Function

Run the **ip pim register-checksum-wholepkt** command to calculate the checksum of entire packets.

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

ip pim register-checksum-wholepkt [**group-list** { *acl-name* | *acl-number* }]

no ip pim register-checksum-wholepkt [**group-list** { *acl-name* | *acl-number* }]

default ip pim register-checksum-wholepkt [**group-list** { *acl-name* | *acl-number* }]

Parameter Description

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

group-list *acl-number*: Uses a standard IP ACL number to limit the addresses of multicast groups that support this configuration. The value range is from 1 to 99 or from 1300 to 1999.

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 calculates the checksum of the entire packets whose multicast group addresses comply with ACL 99, where the multicast group address is 225.1.1.1 and the reverse mask is 0.0.0.255.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 99 permit 225.1.1.1 0.0.0.255
Hostname(config)# ip pim register-checksum-wholepkt group-list 99
```

Notifications

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

```
% access-list 99 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 ip pim register-decapsulate-forward

Function

Run the **ip pim register-decapsulate-forward** command to enable the function for the RP to decapsulate register messages and forward multicast packets in the messages.

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 RP to decapsulate register messages and forward multicast packets in the messages is disabled by default.

Syntax

ip pim register-decapsulate-forward

no ip pim register-decapsulate-forward

default ip pim register-decapsulate-forward

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is run on a static RP or C-RP to decapsulate the received register messages and forward the multicast packets in the received register messages.

The register message decapsulation and multicast packet forwarding function is implemented by this command. If there are too many register messages to be decapsulated and forwarded, the CPU is overloaded. Therefore, you are not advised to enable this function.

Examples

The following example decapsulates the received register messages and forwards the multicast packets in the received register messages on the RP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip pim register-decapsulate-forward
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 ip pim register-rate-limit

Function

Run the **ip 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

ip pim register-rate-limit *rate*

no ip pim register-rate-limit

default ip 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 sets the sending rate of register messages to 3000 per second.

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 ip pim register-rp-reachability

Function

Run the **ip 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 is disabled by default before a register message is sent.

Syntax

ip pim register-rp-reachability

no ip pim register-rp-reachability

default ip 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 message is sent. Otherwise, the 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)# ip pim register-rp-reachability
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 ip pim register-source

Function

Run the **ip pim register-source** command to specify a source IP address in register messages.

Run the **no** form of this command to specify the address of the DR interface connected to the source as the source IP address of register messages.

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

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

Syntax

ip pim register-source { *local-address* | *interface-type interface-number* }
no ip pim register-source
default ip pim register-source

Parameter Description

local-address: Source IP address in register messages.

interface-type interface-number: IP address of local interface, which is specified as source IP address of register messages.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The configured source address in register messages must be reachable so that the source can react properly when the RP sends a correct register-stop message.

It is recommended that the 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.

The status of the PIM function does not affect this configuration.

Examples

The following example specifies the IP address 192.168.195.80 of GigabitEthernet 0/1 as the source IP address in register messages.

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

```
Hostname(config)# ip pim register-source 192.168.195.80
Hostname(config)# ip pim register-source GigabitEthernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 ip pim register-suppression

Function

Run the **ip 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

ip pim register-suppression *suppression-time*

no ip pim register-suppression

default ip 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 suppression time.

If the **ip pim rp-register-kat** command is not run on the DR, configuring the register suppression time on the RP changes the RP keep-alive time.

Examples

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

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ip pim register-suppression 100
```

Notifications

If two times the register-probe time is greater than the register 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 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

1.25 ip pim rp-address

Function

Run the **ip 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

ip pim rp-address *rp-address* [{ *acl-name* | *acl-number* }]

no ip pim rp-address *rp-address* [{ *acl-name* | *acl-number* }]

default ip pim rp-address *rp-address* [{ *acl-name* | *acl-number* }]

Parameter Description

rp-address: IP address of an RP.

acl-name: Standard IP ACL name that is used to limit the address range of groups served by this RP. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Standard IP ACL number that is used to limit the address range of groups served by this RP. The value range is from 1 to 99 or from 1300 to 1999.

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* or *acl-number* parameter is not specified, the static RPs serve all groups.

Examples

The following example sets the IP address of a static RP to 210.34.0.55, the address of the group served by this RP to 255.1.1.1 (defined based on access list 4), and the reverse mask to 0.0.0.255.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 4 permit 225.1.1.1 0.0.0.255
Hostname(config)# ip pim rp-address 210.34.0.55 4
```

Notifications

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

```
Illegal RP address, ignored
```

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

```
Reach PIM-SM static RP configuration limit 65536
```

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

```
% access-list 4 not exist
```

Common Errors

N/A

Platform Description

N/A

Related Commands

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

1.26 ip pim rp-candidate

Function

Run the **ip 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

ip pim rp-candidate *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval*] [**group-list** { *acl-name* | *acl-number* }]

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

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

Parameter Description

interface-type interface-number: Name of an interface whose IP address is used as the C-RP address.

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

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

group-list *acl-name*: Uses a standard IP ACL name to limit the address range of groups served by this C-RP. The value is a case-sensitive string of 1 to 99 characters. By default, a C-RP serves all groups.

group-list *acl-number*: Uses a standard IP ACL number to limit the address range of groups served by this C-RP. The value range is from 1 to 99. By default, the C-RP serves all groups.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In PIM-SM, a rendezvous point tree (RPT) created based on multicast routing data takes the RP as a root and group members as leaves. An RP is elected from C-RPs. 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 sets the address of GigabitEthernet 0/1 to the C-RP address, the RP priority to 200, and the interval of sending C-RP messages to the BSR to 70 seconds, and uses the ACL to limit the address range of groups served by the C-RP to 225.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 3 permit 225.1.1.1 0.0.0.255
Hostname(config)# ip pim rp-candidate GigabitEthernet 0/1 priority 200 group-list
3 interval 70
```

Notifications

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

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

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 ip pim rp-register-kat

Function

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

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

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

By default, the (S, G) entry timeout period is the sum of three times the register suppression time and the register-probe time.

Syntax

ip pim rp-register-kat *interval*

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

Parameter Description

Interval: (S, G) entry timeout period on the RP, 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 (S, G) entry timeout period to 250 seconds on the RP.

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 ip pim sparse-mode

Function

Run the **ip pim sparse-mode** command to enable the PIM-SM 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-SM function is disabled on an interface by default.

Syntax

ip pim sparse-mode

no ip pim sparse-mode

default ip pim sparse-mode

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

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

It is not recommended that different IPv4 multicast routing protocols be configured on interfaces of a device.

When PIM-SM is enabled, IGMP 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.

Examples

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

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

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
```

Notifications

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

```
ip 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, PIM Sparse-mode
```

If the interfaces exceed the upper limit, the following notification will be displayed:

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

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip multicast-routing** (IPv4 multicast routing management)

1.29 ip pim sparse-mode passive

Function

Run the **ip pim sparse-mode passive** command to enable the PIM-SM 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-SM passive mode is disabled on an interface by default.

Syntax

ip pim sparse-mode passive

no ip pim sparse-mode passive

default ip pim sparse-mode passive

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Before the PIM-SM 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-SM passive mode is enabled.

When the PIM-SM passive mode is enabled, IGMP is automatically enabled on different interfaces.

After the PIM-SM 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-SM passive mode be enabled on an interface of a stub network device connected to hosts. This avoids L2 flooding of the PIM hello messages.

Examples

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

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

Notifications

N/A

Common Errors

The PIM-SM passive mode is enabled on an interface connected to a source. The source interface does not send or receive PIM packets; therefore, it loses the DR election capability. It is not recommended that the PIM-SM passive mode be enabled on an interface connected to a source.

After the PIM-SM 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-SM 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

- **ip multicast-routing** (IPv4 multicast routing management)

1.30 ip pim sparse-mode subvlan

Function

Run the **ip pim sparse-mode subvlan** command to enable the PIM-SM function for sub VLANs of a super VLAN interface.

Run the **no** form of this command to disable this function for sub VLANs of a super VLAN interface.

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

The PIM-SM function is disabled on a super VLAN interface by default.

Syntax

ip pim sparse-mode subvlan { **all** | *vlan-id* }

no ip pim sparse-mode subvlan

default ip pim sparse-mode subvlan

Parameter Description

all: Sends PIM-SM protocol packets to all sub VLANs.

vlan-id: ID of a sub VLAN to which PIM-SM protocol packets are sent.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

Generally, a super VLAN contains many sub VLANs. If PIM-SM is enabled on a super VLAN interface, the super VLAN interface duplicates the protocol packets and sends them to all sub VLANs. If the number of sub VLANs is too many, exceeding the processing capability of the device, packets are discarded, resulting in protocol flapping.

In most scenarios, the PIM-SM protocol is disabled by default and not needed on a super VLAN interface. This interface does not send or receive PIM packets. If the PIM-SM protocol is needed on a super VLAN interface in some scenarios, you can run this command to enable the protocol.

Examples

The following example enables PIM-SM packets to be sent to sub VLAN 200 on super VLAN 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 100
Hostname(config-vlan)# supervlan
Hostname(config-vlan)# interface vlan 100
Hostname(config-if-vlan 100)# ip pim sparse-mode subvlan 200
```

Notifications

If this command is run on a non-super VLAN interface, the following notification will be displayed:

```
%% this command can apply to supervlan switch virtual interface only.
```

If the specified sub VLAN ID is consistent with the VLAN ID of an SVI, the following notification will be displayed:

```
%% subvlan vid(%d) is equal to SVI vlan id, not support
```

Common Errors

- This command is run on a non-super VLAN interface.
- The sub VLAN specified on a super VLAN interface cannot communicate with neighbors.

Platform Description

N/A

Related Commands

N/A

1.31 ip pim spt-threshold

Function

Run the **ip 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

ip pim spt-threshold [**group-list** { *acl-name* | *acl-number* }]

no ip pim spt-threshold [**group-list** { *acl-name* | *acl-number* }]

default ip pim spt-threshold [**group-list** { *acl-name* | *acl-number* }]

Parameter Description

group-list *acl-name*: Uses a standard IP 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.

group-list *acl-number*: Uses a standard IP ACL number to limit the address range of groups that support SPT switchover. The value range is from 1 to 99 or from 1300 to 1999.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the **group-list** parameter is not specified, all 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 ACL 12 to specify the multicast group with the address 225.1.1.1 and reverse mask 0.0.0.255 to support SPT switchover.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 12 permit 225.1.1.1 0.0.0.255
Hostname(config)# ip pim spt-threshold group-list 12
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 ip pim ssm

Function

Run the **ip 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

ip pim ssm { **default** | **range** { *acl-name* | *acl-number* } }

no ip pim ssm

default ip pim ssm

Parameter Description

default: Specifies the default SSM group address range. The value range is from 232.0.0.0 to 232.0.0.8.

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

range *acl-number*: Uses a standard IP ACL number to limit the SSM group address range. The value range is from 1 to 99.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If SSM applications must be implemented in the PIM-SM network, this command must be run.

Examples

The following example enables the SSM function and sets the SSM group address range to 232/8.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ip pim ssm default
```

The following example enables the SSM function and sets the SSM group address range to 226/8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 10 permit 226.0.0.1 0.0.0.255
Hostname(config)# ip pim ssm range 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip igmp ssm-map enable** (IGMP)
- **ip igmp ssm-map static** (IGMP)
- **show ip igmp ssm-mapping** (IGMP)

1.33 ip pim triggered-hello-delay

Function

Run the **ip 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

ip pim triggered-hello-delay *delay*
no ip pim triggered-hello-delay
default ip 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 a PIM interface is enabled or detects a new neighbor, a random time is generated. Within the time, the interface sends hello messages.

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)# ip pim triggered-hello-delay 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip pim sparse-mode interface**

1.34 show ip pim sparse-mode bsr-router

Function

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

Syntax

show ip 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 PIM-SM BSR information.

```
Hostname> enable
```

```
Hostname# 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
```

Table 1-1Output Fields of the show ip 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 *interval* seconds	C-RP advertisement interval
Next Cand_RP_advertisement in *time*	Next C-RP advertisement time

Notifications

N/A

Platform Description

N/A

1.35 show ip pim sparse-mode interface

Function

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

Syntax

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

Parameter Description

interface-type interface-number: Specified interface. If this parameter is not specified in the command, information of all interfaces is displayed.

detail: Displays details of interfaces.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

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

```
Hostname> enable
Hostname# 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
```

Table 1-1Output Fields of the show ip 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
Neighbors	Neighbors on an interface

Notifications

N/A

Platform Description

N/A

1.36 show ip pim sparse-mode local-members

Function

Run the **show ip pim sparse-mode local-members** command to display local IGMP information of a PIM-SM interface.

Syntax

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

Parameter Description

interface-type interface-number: Interface name.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays local IGMP information of a PIM-SM interface.

```
Hostname> enable
Hostname# show ip pim sparse-mode local-members
PIM Local membership information
GigabitEthernet 0/3:
(*, 225.1.1.1) : Include
```

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

Field	Description
PIM Local membership information	Local member information
interface-type interface-number	Interface name
(*source*, *ip-group-address*): mode	(S, G): source filtering mode

Notifications

N/A

Platform Description

N/A

1.37 show ip pim sparse-mode mroute

Function

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

Syntax

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

Parameter Description

***group-or-source-address*: Group address or source address. The two addresses must be one group address and one source address. 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.

The two addresses must be one group address and one source address.

Examples

The following example displays the PIM-SM routing information.

```
Hostname> enable
Hostname# show ip pim sparse-mode mroute
IP Multicast Routing Table

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

(192.168.1.100, 233.3.3.3)
RPF nbr: 192.168.36.90
RPF idx: VLAN 1
SPT bit: 0
Upstream State: NOT JOINED
kat expires in 49 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  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
Joined
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
Outgoing
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .

(192.168.1.100, 233.3.3.3, rpt)
RP: 192.168.8.8
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: RPT NOT 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  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
Pruned
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
Outgoing
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .  .  .  .
```

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

Field	Description
IP Multicast Routing Table	IP 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

Field	Description
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

1.38 show ip pim sparse-mode neighbor

Function

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

Syntax

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

Parameter Description

detail: Displays details. If this parameter is not specified, the summary information of neighbors is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays PIM-SM neighbor information.

```
Hostname> enable
Hostname# show ip pim sparse-mode neighbor
Neighbor          Interface                     Uptime/Expires      Ver   DR
Address
Priority/Mode
10.0.0.2          GigabitEthernet 0/23          02:01:23/00:01:21   v2    1 / DR
```

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

Field	Description
Neighbor	Neighbor
Interface	Interface
Uptime/Expires	Update time/expiry time
Ver	Version
DR Address	DR address
Priority/Mode	Priority/Mode

Notifications

N/A

Platform Description

N/A

1.39 show ip pim sparse-mode nexthop

Function

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

Syntax

show ip 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-SM next hop information.

```
Hostname> enable
Hostname# show ip pim sparse-mode nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination     Type  Nexthop   Nexthop         Nexthop                Metric
Pref  Refcnt
                        Num     Addr            Name
__________________________________________________________________________________
___________
20.0.0.1        R  1         0.0.0.0         GigabitEthernet 0/24      0      0
2
30.0.0.2        S  1         20.0.0.1        GigabitEthernet 0/24      2      110
2
```

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

Field	Description
Destination	Destination address
Type	Type
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

1.40 show ip pim sparse-mode rp-hash

Function

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

Syntax

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

Parameter Description

group-address: Address of a multicast group resolved.

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 225.1.1.1.

```
Hostname> enable
Hostname# show ip pim sparse-mode rp-hash 225.1.1.1
RP: 30.30.100.1
Info source: 30.30.100.1, via bootstrap
```

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

Field	Description
RP	RP address
Info source	Address of a source that sends information
via bootstrap	Messages from a BSR

Notifications

N/A

Platform Description

N/A

1.41 show ip pim sparse-mode rp mapping

Function

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

Syntax

show ip 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 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
```

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

Field	Description
Group(s)	Address/Mask of a group
RP	RP address
Info source	Address of a source that sends information
via bootstrap	Messages from a BSR

Field	Description
priority	Priority
Uptime	Update time
expires	Expiry time

Notifications

N/A

Platform Description

N/A

1.42 show ip pim sparse-mode track

Function

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

Syntax

show ip 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 ip 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 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-Refresh:    0
Unknown PIM Type:       0
Errors:
Malformed packets:      0
Bad checksums:          0
Send errors:            0
Packets received with unknown PIM version:  0
```

Figure 1-1Output Fields of the show ip 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 PIMSM 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
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
PIMDM-Graft	Statistical value of PIM-DM graft packets
PIMDM-Graft-Ack	Statistical value of PIM-DM graft acknowledgment packets
PIMDM-State-Refresh	Statistical value of PIM-DM SRMs
Unknown PIM Type	Unknown PIM packets
Errors	Statistical value of error packets
Malformed packets	Number of malformed packets

Field	Description
Bad checksums	Number of packets with incorrect checksums
Send errors	Number of sent error packets
Packets received with unknown PIM version	Number of PIM packets with unknown version

Notifications

N/A

Platform Description

N/A