Multicast Configuration Commands

Table of Contents

Chapter 1 Basic Multicast Commands

1.1 Basic Multicast Commands

The basic multicast commands include:

- debug ip mpacket
- debug ip mrouting
- debug ip mroute-cache
- debug ip multicast
- ip mroute
- ip mroute-cache
- ip multicast-routing
- ip multicast route-limit
- ip multicast boundary
- ip multicast helper-map
- ip multicast rate-limit
- ip multicast ttl-threshold
- show ip mflow
- show ip mroute-cache
- show ip mroute mfc
- show ip mroute static

1.1.1 debug ip mpacket

If you want to track the process for the multicast packet, you can use this command "**debug ip mpacket**", and use the"**no**" forma of the command to disable debug information.

debug ip mpacket [**access-list**][*group-address*][**detail**]

no debug ip mpacket

Parameter

Parameter	Description
access-list	Range for tracked multicast packets
group-address	The tracked multicast packet group address
detail	Details for multicast packet processing

Default

Disable debug information output

Command Mode

EXEC

Usage Guidelines

You can use this command to track the main process for igmp-host end protocol.

Example

The following example shows some situations for multicast packet processing.

You have received the (100.168.20.151,224.1.1.1) packet on e0/1 interface, and the packet length is 112 bytes.

You have sent the (192.168.20.99,224.0.0.5) packet on e0/1 interface, and the packet length is 64 bytes.

router#debug ip mpacket

M INPUT : IP Ethernet0/1 (100.168.20.151,224.1.1.1) , len=112

M OUTPUT : IP Ethernet0/1 (192.168.20.99,224.0.0.5) , len=64

Related commands

None

1.1.2 debug ip mrouting

Use this command “debug ip mrouting” to enable “mrouting” tracking function, then you can see the change from the multicast transfer list. In addition, use the”no” forma of the command to close debug information.

Syntas

debug ip mrouting

no debug ip mrouting

Parameter

None

Default

Disable all tracking functions.

Command Mode

EXEC

Usage Guidelines

You can use this command to see the change from the multicast transfer list, such as (S, G)/(*,G) adding/deleting and downstream interface adding/deleting.

Example

The following example shows you some changes from the multicast transfer list. First the (192.168.20.110, 239.0.0.100) item is created, and then Loopback0 is added for downstream interface. Finally, the item is deleted due to timeout.

router#debug ip mrouting

MBR: create (192.168.20.110, 239.0.0.100) MBR: w/ oif Loopback0

MBR: delete (192.168.20.110, 239.0.0.100)

Related Commands

ip multicast-routing

1.1.3 debug ip mroute-cache

Use this command “debug ip mrouting” to enable “mroute-cache” tracking function, then you can see the change from the multicast routing cache. In addition, you can use the “no”format of the command to close the tracking.

Syntas

debug ip mroute-cache *group-address*

no debug ip mroute-cache

Parameter

Parameter	Description
group-address	The tracked multicast routing cache group address

Default

Disable all tracking functions.

Command Mode

EXEC

Usage Guidelines

You can use this command to see the change of the adding/deleting of multicast routing cache.

Example

The following example shows you some changes on the multicast routing cache, and the creating and timeout of (192.168.20.97,230.0.0.1) cache.

router#debug ip mroute-cache

MRC: create (192.168.20.97,230.0.0.1) mroute-cache

MRC: expired (192.168.20.97,230.0.0.1) mroute-cache

1.1.4 debug ip multicast

You can use this command “debug ip multicast” to enable multicast event tracking function, and then see the interaction between the multicast protocol and mrouting. you can use the “no”format of the command to close the function.

Syntas

debug ip multicast [**alert** | **border-router**]

no debug ip multicast [**alert** | **border-router**]

Parameter

Parameter	Description
alert	Track the alert interaction among multicast routing components
border-router	Track related events of multicast border router MBR

default

Disable all tracking functions.

Command Mode

EXEC

Usage Guidelines

Defining some standard events between multicast routing protocol and mrouting indicates “alert”, for example: creation alert/deletion alert which related (S,G). You can use “debug ip multicast alert” to see these alerts.

Multicast routing protocol supinterfaces MBR, and each multicast routing protocol is a “component”. You can use “debug ip multicast border-router” to see the component’s running information.

Example

In the following example, the alert router is turned on for output:

```
router#debug ip multicast alert
    MBR: [(S, G) deletion alert], originated by OLNK, sent to all components
    MBR: [(S, G) creation alert], originated by NONE, sent to all components
    MBR:     src = 192.168.20.110, grp = 239.0.0.100
    MBR:     sent to owner OLNK first
    MBR: [(S, G) join alert], originated by NONE, sent to OLNK
    MBR:         src = 192.168.20.110, grp = 239.0.0.100
    MBR: [(S, G) firstuse alert], originated by NONE, sent to OLNK
    MBR:         src = 192.168.20.110, grp = 239.0.0.100
    MBR: [(S, G) deletion alert], originated by OLNK, sent to all components
    MBR:     src = 192.168.20.110, grp = 239.0.0.100
```

1.1.5 ip mroute

Use the command “ip mroute” to configure the static multicast routing, and use “no ip mroute” to delete the configured static multicast routing.

Syntas

ip mroute *source-address mask* [*rpf-address type-number* [**distance**]]

no ip mroute *source-address mask* [*rpf-address type-number* [**distance**]]

Parameter

Parameter	Description
source-address	Multicast source IP address
mask	Multicast source IP address mask
rpf-address	RPF address of Static multicast routing
type-number	RPF interface of Static multicast routing
distance	Optional management distance

Default

The default management distance is 0.

Command Mode

Gobal configuration

Usage Guidelines

This command allows you to manually configure the location information for the multicast source. It is used when the multicast and unicast topologies are not identical.

Example

The following example will configure a static multicast routing through the specified interface:

router_config#ip mroute 100.1.1.0 255.255.255.0 192.1.1.1 f0/0

Related Commands

show ip mroute static

1.1.6 ip mroute-cache

Use this command “ip mroute-cache” to configure a multicast routing cache on the interface, and “no ip mroute-cache” to disable the multicast routing cache.

Syntas

ip mroute-cache

no ip mroute-cache

Parameter

None

Default

The default is to use the multicast routing cache on the interface.

Command Mode

Interface configuration

Usage Guidelines

Use the command when a interface uses the multicast routing cache to receive/send the packet, ip will search the cache when a multicast packet is received. If there is no routing information in the cache, the interface will ask for multicast routing module.

Example

The following example will enable multicast routing cache on interface e1/0.

router_config_e1/0#ip mroute-cache

Related Commands

show ip mroute-cache

1.1.7 ip multicast-routing

Use this command “ip multicast-routing” to enable IP multicast packet transferring function, and “no ip multicast-routing” to disable the function.

Syntas

ip multicast-routing

no ip multicast-routing

Parameter

None

Default

The default is not to transfer multicast packets.

Command Mode

Global configuration

Usage Guidelines

If you disable this function, the router will no longer transfer multicast packets, meanwhile, the multicast routing list and the multicast cache will be empty.

Example

The following example will configure the router to transfer multicast packets:

router_config#ip multicast-routing

Related Commands

show ip mroute mfc

1.1.8 ip mfastfw-on

To enable IP multicast packet fast forwarding, run the first one of the following two commands. To disable this feature, use the no form of the command. (Now only Ethernet interfaces are supinterfaceed.)

ip mfastfw-on no
ip mfastfw-on

Parameter

None

Default

The multicast packet is not fast forwarded.

Command Mode

Global configuration

Usage Guidelines

Example
The following example shows how to configure the router forwarding multicast packets: router_config#ip mfastfw-on

1.1.9 ip multicast route-limit

Use this command “ip multicast route-limit” to configure the maximum number of multicast routing item, and “no ip multicast route-limit” to un-limit the number.

Syntas

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

ip multicast route-limit *size*

Parameter

Parameter	Description
size	Maximum number of multicast routing item

Default

The default multicast routing item number is unlimited.

Command Mode

Global configuration

Usage Guidelines

If you have configured this function, the multicast routing item number will be limited.

example

The following example will configure the maximum number of multicast routing list to 2000:

router_config#ip multicast route-limit 2000

Related Commands

show ip mroute mfc

1.1.10 ip multicast boundary

Use this command "**ip multicast boundary**" to manage the range for the interface allowed processing multicast packets; it is valid for input/output packets on the interface. Use "**no ip multicast boundary**" to cancel this command.

Syntas

ip multicast boundary *access-list*

no ip multicast boundary

Parameter

Parameter	Description
access-list	the access-list name used to specify the range for processing multicast packets.

Default

Process all multicast packets.

Command Mode

Interface configuration

Usage Guidelines

If the function is configured, the range for the interface allowed processing multicast packets will be limited.

Example

The following example will configure the range for the interface e1/0 allowed processing multicast packets to the range limited by the access-list testacl:

router_config_e1/0#ip multicast boundary testacl

1.1.11 ip multicast helper-map

Use this command “ip multicast helper-map” to configure the connection of two broadcast networks with the multicast routing on the multicast network, and “**no ip multicast helper-map**” to cancel this command.

ip multicast boundary helper-map {*group-address*|**broadcast**} {*broadcast-address* |*multicast-address* } *access-list*

no ip multicast boundary helper-map {*group-address*|**broadcast**} {*broadcast-address* | *multicast-address* } *access-list*

Parameter

Parameter	Description
group-address	The multicast packet group address which needed to be converted to the broadcast packet. it is used with the broadcast-address keyword.
broadcast	It can convert the broadcast packet to the multicast packet. it is used with the multicast-address keyword.
broadcast-address	The target address of broadcast packet which is sent after converting. it is used with the group-address keyword.
multicast-address	The target address of multicast packet which is sent after converting. It is used with the broadcast keyword.
access-list	IP extended access-list name. You can use it to specify the interface number for packet converting.

Default

Not perform the conversion between any multicast packets and broadcast packets.

Command Mode

Interface configuration

Usage Guidelines

If two broadcast networks are connected with a multicast network, you can convert the broadcast flow to multicast flow on the first hop router connected with the source broadcast network, and then convert the multicast flow to broadcast flow on the last hop router connected with the target broadcast network. Thus, you can utilize the multicast network's multicast characteristic between the two broadcast networks which are required to be connected with each other. Furthermore, it can prevent the packets between two broadcast networks from being sent repeatedly, and utilize the "quick forward" characteristic on the multicast network.

Before using "ip multicast helper-map", you should have configured this command "ip directed-broadcast" on the interface.

Example

Configuration on the router is as follow:

if you configure command"ip directed-broadcast" on interface e0 of the first hop router, it will be allowed to process the link broadcast packets.

If you have configured "ip multicast helper-map broadcast 230.0.0.1 testacl1", you can convert the udp broadcast packet, whose interface number is 4000("ip forward-protocol" command specified) and the source address is 192.168.20.97/24 (testacl1 specified) ,to multicast packet whose target address is 230.0.0.1 ("ip multicast helper-map" command specified).

if you configure command"ip directed-broadcast" on interface e1 of the last hop router, it will be allowed to process the link broadcast packets.

If you have configured "ip multicast helper-map broadcast 230.0.0.1 172.10.255.255 testacl2", you can convert the multicast packet, whose interface number is 4000("ip forward-protocol" command specified), the source address is 192.168.20.97/24 (testacl2 specified) and target address is 230.0.0.1 ,to broadcast packet whose target address is 170.10.255.255 ("ip multicast helper-map" command specified).

On the first hop router which is connected with the source broadcast network:

```
interface ethernet 0
ip directed-broadcast
ip multicast helper-map broadcast 230.0.0.1 testacl
ip pim dense-mode
!
ip access-list extended testacl    permit udp 192.168.20.97 255.255.255.0 any

ip forward-protocol udp 4000
```

On the last hop router which is connected with the target broadcast network:

```
interface ethernet 1
```

ip directed-broadcast

ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2

ip pim dense-mode

!

ip access-list extended testacl2 permit udp 192.168.20.97 255.255.255.0 any

ip forward-protocol udp 4000

Related Commands

ip forward-protocol

ip directed-broadcast

1.1.12 ip multicast rate-limit

Use this command "**ip multicast rate-limit**" to limit the multicast packet flow receiving and sending in the range of a source/group on the interface, and "**no ip multicast rate-limit**" to cancel this flow limitation.

Syntas

ip multicast rate-limit {**in** | **out**} [**group-list** *access-list*] [**source-list** *access-list*] kbps **no**

ip multicast rate-limit {**in** | **out**} [**group-list** *access-list*] [**source-list** *access-list*]

Parameter

Parameter	Description
in	Limit the input packet flow on the interface.
out	Limit the output packet flow on the interface.
group-list *access-list*	(optional) Limit the multicast packet flow for the group address in access-list.
source-list *access-list*	(optional) Limit the multicast packet flow for the source address in access-list.
kbps	(optional) Allowed maximum flow. If its value is 0, no packet will be allowed to pass.

Default

No limitation to the flow.

Command Mode

Interface configuration

Usage Guidelines

The packet flow in specified range has exceeded the limit at last second. You have to discard the packet, or the packet will be forwarded.

Example

The maximum output packet flow rate on interface s0 (192.168.20.97 , 230.0.0.1) is limited to 64kbps.

interface serial 0
ip multicast rate-limit out group-list gacl source-list sacl 64 ip access-list standard sacl
permit 192.168.20.97 255.255.255.255 ip access-list standard gacl
permit 230.0.0.1 255.255.255.255

1.1.13 ip multicast ttl-threshold

Use this command “ip multicast ttl-threshold” to configure the maximum threshold value of multicast packet ttl on the interface, and “no ip multicast ttl-threshold” to restore default.

Syntas

ip multicast ttl-threshold *ttl-value*

no ip multicast ttl-threshold

Parameter

Parameter	Description
ttl-value	The multicast packet ttl threshold value on the interface.

Default

The default ttl threshold value on the interface is 1.

Command Mode

Interface configuration

Usage Guidelines

The ttl value of receiving/sending packet should be largerer than the specified threshold value on the interface, you can use this command to configure a router to border router.

Example

The ttl threshold value configured on interface s0 is 200, it means only the multicast packet with ttl value more than 200 is allowed to be received/sent on the interface.

interface serial 0
ip multicast ttl-threshold 200

1.1.14 show ip mflow

You can use this command “show ip mflow” to display global flow information processed by system and multicast flow information processed on the interface.

Syntas

show ip mflow [*group-address*|*source-address*]**interface**

Parameter

Parameter	Description
group-address	The displayed multicast flow information group address.
source-address	The displayed multicast flow information source address.
interface	The displayed interface multicast flow information.

Default

None

Command Mode

EXEC

Usage Guidelines

Display the processed packet number from the multicast flow, wrong incoming interface packet number, and current flow value.

Example

router#show ip mflow IP Multicast Flow (100.168.20.151,224.1.1.1)
total process : 0 wrong_if_count : 0 curr-flux : 0.00 (192.167.20.131,239.1.1.1)
total process : 0 wrong_if_count : 0 curr-flux : 0.00

The following example will display interface multicast flow information:

router#show ip mflow **interface** e0/1

IP Multicast Flow
(192.168.20.97,230.0.0.1)

total recv : 21180 total send : 0 curr-in-flux : 0.00 curr-out-flux :
0.00 (100.168.20.151,224.1.1.1)
total recv : 16822400 total send : 0 curr-in-flux : 0.00 curr-out-flux :
0.00 (192.168.20.97,232.0.0.1)
total recv : 240 total send : 0 curr-in-flux : 0.00 curr-out-flux :
0.00 (192.167.20.131,239.1.1.1)
total recv : 103264 total send : 0 curr-in-flux : 0.90 curr-out-flux : 0.00

1.1.15 show ip mroute-cache

Use this command “show ip mroute-cache” to display the information on the multicast routing cache.

Syntas

show ip mroute-cache [*group-address*]

Parameter

Parameter	Description
group-address	The displayed multicast routing cache group address

Default

None

Command Mode

EXEC

Usage Guidelines

MRC (Multicast Route Cache) is a global multicast routing cache, and every MRC item contains the (S, G)/ (*, G) information, upstream/downstream interface information received from the multicast routing.

Example

The following example will display multicast routing list information:

router#show ip mroute-cache
IP Multicast Route Cache
(192.168.20.97, 230.0.0.1)|(192.168.20.97,230.0.0.1) Incoming interface: Ethernet0/2, Last used : 00:00:34
Outgoing interface list: Loopback0
(192.168.20.97, 230.0.0.2)|(192.168.20.97,230.0.0.2) Incoming interface: Ethernet0/2, Last used : 00:00:12
Outgoing interface list: Loopback1

1.1.16 show ip mroute mfc

You can use this command “show ip mroute mfc” to display the multicast forwarding list information, and then activate the multicast function.

Syntas

show ip mroute mfc

Parameter

none

Default

None

Command Mode

EXEC

Usage Guidelines

MFC (Multicast Forwarding Cache) is a global multicast forwarding list, and the multicast packet is forwarded by it. Every MFC item has (S, G)/ (*, G) information and upstream/downstream interface information.

Example

The following example will display multicast routing list information:

```
router#show ip mroute
mfc


IP Multicast Forwarding Cache
(192.168.20.110/32, 239.0.0.100/32)
  Incoming interface: Ethernet0/2, RPF nbr 0.0.0.0, owned by
  OLNK Outgoing interface list:
    Loopback0, owned by OLNK
(192.168.20.110/32,
239.0.0.101/32)
  Incoming interface: Ethernet0/2, RPF nbr 0.0.0.0, owned by
  OLNK Outgoing interface list:
    Loopback0, owned by
OLNK (192.168.20.138/32,
239.1.1.1/32)
```

Incoming interface: Ethernet0/2, RPF nbr 0.0.0.0, owned by

OLNK Outgoing interface list:

Loopback0, owned by OLNK

Related Commands

show ip mroute olnk

show ip mroute static

1.1.17 show ip mroute static

To show the contents of the IP multicast static routing table, use the show ip mroute command in user EXEC mode.

show ip mroute static

Parameter

None

Default

None

Command Mode

EXEC

Usage Guidelines

Use the show ip mroute command to display information about mroute entries in the mroute table.

Example

The following is sample output from the show ip static mroute command for a router:

```
router#show ip mroute static
Mroute: 200.1.1.1/24, RPF nbr: 192.168.20.1, RPF interface:
    Ethernet0/2 Administrative distance: 0, metric: 0, valid: TRUE
Mroute: 201.1.1.1/24, RPF nbr: 192.168.20.1, RPF interface: Serial0/0
Administrative distance: 0, metric: 0, valid: FALSE
```

Chapter 2 IGMP Configuration Commands

2.1 IGMP Configuration Commands

IGMP configuration commands include:

- clear ip igmp group
- debug ip igmp
- debug ip igmp-host
- ip igmp helper-address
- ip igmp join-group
- ip igmp immediate-leave group-list
- ip igmp last-member-query-interval
- ip igmp querier-timeout
- ip igmp query-interval
- ip igmp query-max-response-time
- ip igmp static-group
- ip igmp version
- show ip igmp groups
- show ip igmp interface
- show ip igmp-host

2.1.1 clear ip igmp group

If you want to clear the multicast group member information saved in multicast router that supinterfaces IGMP, you can use the command "**clear ip igmp group**".

Syntas

clear ip igmp group *type-number group-address*

Parameter

Parameter	Description
type-number	interface type and interface number.
group-address	Multicast group's group address to clear information.

Default

None

Command Mode

EXEC

Usage Guidelines

Using this command, you can clear the multicast group member information saved in router when the saved multicast group information has a problem.

Example

The following example shows you how to clear the information of multicast group 233.33.1.1 on e1/0 interface.

clear ip igmp group e1/0 233.33.1.1

Related Commands

None

2.1.2 debug ip igmp

If you want to track the process for igmp-router end protocol, you can use this command "**debug ip igmp**", and use the"no" forma of the command to close debug information.

Syntas

debug ip igmp no

debug ip igmp

Parameter

None

Default

Disable debug information output

Command Mode

EXEC

Usage Guidelines

You can use this command to track the main process for igmp-router end protocol to find the reason for protocol processing failure.

Example

Igmp-router function module's debug information usually use the natural language to make description. Due to its simplicity, we will not list all of the debug information.

2.1.3 debug ip igmp-host

If you want to track the process for igmp-host end protocol, you can use this command "**debug ip igmph**", and use the"**no**" forma of the command to close debug information.

Syntas

debug ip igmph *group-address*

no debug ip igmph

Parameter

None

Default

Disable debug information output

Command Mode

EXEC

Usage Guidelines

You can use this command to track the main process for igmp-host end protocol to find the reason for protocol processing failure.

Example

Igmp-host function module's debug information usually use the natural language to make description. Due to its simplicity, we will not list all of the debug information.

2.1.4 ip igmp helper-address

If you want an interface to transit IGMP packet, you can use this command to configure the interface. One interface can configure the command only once time, so the next configured command will overwrite the original command.

Syntas

ip igmp helper-address *destination-address*

no ip igmp helper-address *destination-address*

Parameter

Parameter	Description
destination-address	The destination address of transitting IGMP packet。

Default

The interface will not transit IGMP packet

Command Mode

Interface configuration

Usage Guidelines

Use this command “ip igmp helper-address” to transit all received igmp packets.

Example

ip igmp helper-address 192.168.20.10

2.1.5 ip igmp join-group

If you want to add a multicast group on the interface, you can use this command to perform it.

Syntas

ip igmp join-group *group-address* [{**include**|**exclude**} *source-address*]

no ip igmp join-group *group-address* [{include|exclude} *source-address*]

Parameter

Parameter	Description
group-address	The multicast group required to be added to the interface
include	The mode of SSM needed to add a multicast group is “include”.
exclude	The mode of SSM needed to add a multicast group is “exclude”.
source-address	Source filter address whose interface is added to multicast

Default

No multicast group will be added to the interface.

Command Mode

Interface configuration

Usage Guidelines

Use this command “ip igmp join-group” to dynamically add a multicast group to the interface.

Example

ip igmp join-group 230.0.0.1

ip igmp join-group 230.0.0.1 exclude 192.168.20.10

2.1.6 ip igmp immediate-leave group-list

If you want the router interface running IGMP version 2 to run the multicast group function “Exit Now”, you can use this command “**ip igmp immediate-leave group-list**” to perform configuring. In addition, you can use the “**no**”format of the command to forbid the IGMP host to “exit now”.

Syntas

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

no ip igmp immediate-leave *group-list*

Parameter

Parameter	Description
list-name	Pre-configured ip standard access-list name

Default

The IGMP host is not allowed to run “Exit Now” function.

Command Mode

Global configuration/interface configuration

Usage Guidelines

This command is available only for the interface of running IGMP version 2.it can be used when the network connecting with the interface has only one IGMP host. Through configuring this command, the host can immediately exit from a multicast group without the process for packet exchanging and delaying from the router. Besides, you can configure this command in “Global configuration” and “Interface configuration”, but this command configured in “Global configuration” will be prior to the command configured in “Interface configuration”. If you have configured the command in “Global configuration”, the next command configured in “Interface configuration “will be ignored. On the other hand, the command configured in “global configuration mode” will overwrite the original command configured in “interface configurationmode”.

Example

Refer to “Configure multicast routing”.

Related Commands

ip access-list

2.1.7 ip igmp last-member-query-interval

To change the query interval of last group member l on the current interface, use this command “**ip igmp last-member-query-interval”**. You can use the “**no**” format of the command to restore default settings.

Syntas

ip igmp last-member-query-interval *time*

no ip igmp last-member-query-interval

Parameter

Parameter	Description
time	The value of last member query interval configured on the interface. Its unit is millisecond.

Default

The default of the last group member query interval on the interface is 1000ms.

Command Mode

Interface configuration

Usage Guidelines

You can use this command “ip igmp last-member-query-interval” to modify the last group member query interval on the interface.

Example

The following example will modify the last member query interval on the interface to 2 seconds.

interface ethernet 0/0

ip igmp last-member-query-interval 2000

2.1.8 ip igmp querier-timeout

You can use this command “**ip igmp querier-timeout**”to modify other routers for IGMP querier timeout,.use the “**no**” f ormat of this command to restore default.

Syntas

ip igmp querier-timeout *time*

no ip igmp querier-timeout

Parameter

Parameter	Description
time	other querier timeout. Its unit is second.

Default

125 seconds

Command Mode

Interface configuration

Usage Guidelines

You can use this command “ip igmp querier-timeout” to modify other routers for querier timeout. This command is available only for the interface which running IGMP version 2.

Example

The following example shows that the querier-timeout specified on interface Ethernet 0/0 is 100 seconds.

interface ethernet 0/0

ip igmp querier-timeout 100

2.1.9 ip igmp query-interval

To set the interval for IGMP General Query packet sending on the interface, you can use this command "**ip igmp query-interval**". Use the "**no**"format of this command to restore default.

Syntas

ip igmp query-interval *time*

no ip igmp query-interval

Parameter

Parameter	Description
time	Interval of sending general query packet. Its unit is second.

Default

60 seconds

Command Mode

Interface configuration

Usage Guidelines

You can use this command "**ip igmp query-interval**" to set the interval for IGMP General Query packet sending on the interface,

Example

The following example shows that the interval of sending general query packet on Ethernet 0/0 interface is specified to 50 seconds.

interface ethernet 0/0
ip igmp query-interval 50

2.1.10 ip igmp query-max-response-time

To specify the maximum interval for IGMP host to respond General Query packet, you can use this command "**ip igmp query-max-resposne-time**". Use the "**no**"format of this command to restore default.

Syntas

ip igmp query-max-response-time *time*

no ip igmp query-max-response-time

Parameter

Parameter	Description
time	Value of the maximum response time configured on the interface.

Default

10 seconds

Command Mode

Interface configuration

Usage Guidelines

You can use this command "**ip igmp query-max-resposne-time**"to specify the maximum interval for IGMP host to respond General Query packet. This command is available only for the interface which running IGMP version 2 and 3.

Example

The following example will set the IGMP maximum response time on Ethernet 0/0 interface as 15 seconds.

interface ethernet 0/0
ip igmp query-max-response-time 15

2.1.11 ip igmp static-group

If you want to configure a static multicast group on the interface, you can use this command "**ip igmp static-group**" to perform it. Use the "**no**" format of this command to restore default.

Syntas

ip igmp static-group { ***** | ***group-address*** } {**include** *source-address* }

no ip igmp static-group { * | *group-address* } {**include** *source-address*}

Parameter

Parameter	Description
*	All multicast groups.

group-address	Specified multicast group address.
source-address	Specified host source address.

Default

In default, no multicast group is static configured on the interface.

Command Mode

Interface configuration

Usage Guidelines

Configure the static IGMP multicast group information on the current interface.

Notes:

For the same group-address, you can configure several “include source-address” commands for the corresponding static multicast group to have several source-addresses existing. However, for the same group-address, you can’t configure both commands with/without “include source-address”.

Example

Refer to “Configure multicast routing”

2.1.12 ip igmp version

To set the IGMP version number running on the interface, you can use this command “**ip igmp version**”. use the “**no**”format of the command to restore default.

Syntas

ip igmp version *version-*

number **no ip igmp version**

Parameter

Parameter	Description
version-number	The value 1.2 or 3 indicates separately the IGMP version number 1,2 or3.

Default

If you don't configure this command, the default version number for IGMP-Router end protocol running on the interface is 3.

Command Mode

Interface configuration

Usage Guidelines

Use this command "**ip igmp version**"can set the IGMP version number running on the interface,

Example

The following example will specify the IGMP version number running on Ethernet 0/0 interface as 2.

interface ethernet
0/0 ip igmp version 2

2.1.13 show ip igmp groups

You can use the following command to see the multicast group member information that is saved on the current router.

Syntas

show ip igmp groups {***interface*** | ***group-address*** | ***detail***}

Parameter

Parameter	Description
interface	The interface where you want to see the multicast group information. If you don't add this parameter, all multicast groups information on the interface will be displayed.
group-address	The multicast group address to see. If you don't add this parameter, all multicast groups information on the router will be displayed.
detail	T he router whether you want to see the multicast group information.

Default

None

Command Mode

EXEC/Global configuration/Interface configuration.

Usage Guidelines

You can use this command to see the multicast group member information that is saved on the router.

Example

show ip igmp groups e0/0 detail

Running this command will display the following message:

……

…. Interface:

Ethernet0/0

Group address: 233.33.1.3

Uptime: 00:03:46

Group status: Static

Group filter mode:

INCLUDE Last

reinterfaceer: 0.0.0.0

Group source-list: (Flags: S-Static, R-Remote)

Source address:	Uptime	Timer	Fwd	Flags
192.168.20.5	00:03:46	stopped	Yes	S

Interface: Ethernet0/0

Group address: 233.33.1.1

Uptime: 00:03:46

Group status: Static

Group filter mode:

INCLUDE Last

reinterfaceer: 0.0.0.0

Group source-list: (Flags: S-Static, R-Remote)

Source address:	Uptime	Timer	Fwd	Flags
192.168.20.5	00:03:46	stopped	Yes	S
192.168.20.3	00:03:46	stopped	Yes	S
192.168.20.1	00:03:46	stopped	Yes	S

…….

show ip igmp groups 233.33.1.1 detail

Running this command will display the following

message: Interface: Ethernet0/0

Group address: 233.33.1.1

Uptime: 00:02:42

Group status: Static

Group filter mode:

INCLUDE Last

reinterfaceer: 0.0.0.0

Group source-list: (Flags: S-Static, R-Remote)

```
Source address:  Uptime      Timer      Fwd   Flags
192.168.20.5       00:02:42  stopped    Yes   S
192.168.20.3       00:02:42  stopped    Yes   S
192.168.20.1       00:02:42  stopped    Yes   S
```

show ip igmp groups

Running this command will display the following message:

```
Interface        Group address   Uptime     Expires   Last Reinterfaceer
                                 Flags Ethernet0/0    239.255.255.250
00:01:08   00:02:05   192.168.20.141                   R Ethernet0/0
224.2.127.254  00:01:09    00:02:00    32.1.1.67       R Ethernet0/0
224.1.1.1        00:01:24   stopped          0.0.0.0   S Ethernet0/0
233.33.1.5       00:01:24   stopped          0.0.0.0   S Ethernet0/0
233.33.1.3       00:01:24   stopped          0.0.0.0   S Ethernet0/0
233.33.1.1       00:01:24   stopped          0.0.0.0   S

Interface        Group address   Uptime     Expires   Last Reinterfaceer
                 Flags Loopback10       239.255.255.250  00:01:08
00:02:05   192.168.20.141          R Loopback10        224.2.127.254
                 00:01:09   00:02:00    32.1.1.67       R
```

2.1.14 show ip igmp interface

You can use this command to see information on the current router's interface where IGMP is activated.

Syntas

show ip igmp interface *interface*

Parameter

Parameter	Description
interface	The specified interface to display information. If you don't add this parameter, all information on interfaces where IGMP is activated will be displayed.

Default

None

Command Mode

EXEC/Global configuration/Interface configuration

Usage Guidelines

You can use this command to display information on the interface where IGMP is activated.

Example

show ip igmp interface e0/0

Running this command will display the following information:

Ethernet0/0 is up, line protocol is up
Internet address is 192.168.20.167
Current IGMP router version is 3
Router plays role of querier on the interface now
IGMP is enable on the interface
IGMP query-interval is 60 seconds
IGMP max query response time is 10 seconds
IGMP Last member query response time is 1000 milliseconds
IGMP querier timeout is 125 seconds
Multicast routing is enabled on the interface

2.1.15 show ip igmp-host

You can use this command to see IGMP host information on the interface ofcurrent router.

Syntas

show ip igmph { ***interface*** } **detail**

Parameter

Parameter	Description
interface	The specified interface to display information.
detail	Display igmp host detailed information.

Default

None

Command Mode

EXEC/Global configuration/Interface configuration

Usage Guidelines

You can use this command to display basic IGMP host information on the interface.

Example

show ip igmph interface e0/0

Running this command will display the following information:

IGMP host Mode is IGMP_V3_ROUTER
IGMP host Query Interval is 23 second
IGMP host Query Response Interval is
125
IGMP host Query Robustness Variable is
2 IGMP host Last Query Interval is 0
IGMP interface timer is 0
IGMP host group joined(number of users):
230.0.0.1(1)

Chapter 3 PIM-DM Configuration Commands

3.1 PIM-DM Configuration Commands

PIM-DM Configuration Commands include:

- clear ip mroute pim-dm
- clear ip pim-dm interface
- debug ip pim-dm
- ip pim-dm
- ip pim-dm dr-priority
- ip pim-dm hello-interval
- ip pim-dm state-refresh origination-interval
- ip pim-dm neighor-filter
- ip pim-dm state-refresh disable
- ip pim version
- show ip pim-dm neighbor
- show ip pim-dm interface
- show ip rpf pim-dm
- show ip mroute pim-dm

3.1.1 clear ip mroute pim-dm

Use the following command in EXEC to clear the (S,G) routing list items submitted by PIM-DM to mrouting:

Syntas

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

Parameter

Parameter	Description
*****	Delete all multicast routing list items submitted by pim-dm.
group	Delete all list items submitted by pim-dm and satisfied in the specified group.
source	(optional) Delete all list items submitted by pim-dm and satisfied in the specified group's *source*.

Default

None

Command Mode

EXEC

Usage Guidelines

The command will delete all or part of table lists of local multicast router table,and it is possible to affect the normal multicast packet forwarding. This command can only delete the (S,G) items, whose upstream interface is created by PIM-DM multicast routing protocol, and inform mrouting, then mrouting will determine if it should re-establish the corresponding (S,G).

Example

Example1:

Router#clear ip mroute pim-dm *

All (S,G) items, whose middlestream/upstream interface is created by PIM-DM, on local
MRT will be cleared.

Example2:

Router#clear ip mroute pim-dm 239.1.1.1

All (S,G) items with the group address 239.1.1.1, whose middlestream/upstream interface is created by PIM-DM, on local MRT will be cleared.

Example3:

Router#clear ip mroute pim-dm 239.1.1.1 192.168.20.131

All (S,G) items with the address (192.168.20.138, 239.1.1.1), whose middlestream/upstream interface is created by PIM-DM, on local MRT will be cleared.

3.1.2 clear ip pim-dm interface

Reset the multicast packet statistic value forwarded through (S,G) on PIM-DM interface. You can use the command in EXEC:

Syntas

clear ip pim-dm interface {**count** | *type number{**count**}*}

Parameter

Parameter	Description
count	(optional) Delete all multicast packet statistic values on PIM-DM interface.
type number	(optional) Delete multicast packet statistic values on the specified interface.

Default

None

Command Mode

EXEC

Usage Guidelines

This operation will reset the multicast packet number statistic values forwarded through PIM-DM interface in local multicast routing list. This command can only reset the (S,G) items, whose upstream interface is created by PIM-DM multicast routing protocol.

Example

Example1:

Router#clear ip pim-dm interface count

It will reset all multicast packet number statistic values forwarded by (S,G) items, whose upstream interface is created by PIM-DM, on local MRT.

Example2:

Router#clear ip pim-dm interface Ethernet1/1 count

It will reset all multicast packet number statistic values forwarded by (S,G) items, whose upstream interface is Ethernet1/1 and created by PIM-DM, on local MRT.

3.1.3 debug ip pim-dm

Use this command to track input/output PIM packets and caused events. Set this command to “no” to stop tracking.

Syntas

debug ip pim-dm [**group**|**alert**]

Parameter

Parameter	Description
group	(optional) Track the specified group status.
alert	(optional) Track the alert status received from mrouting.

Default

None

Command Mode

EXEC

Usage Guidelines

Receive Alert from mrouting.

Send alert to other components.

Example

Example 1, the output information is as follows: Hello packet prompt sent to each interface. Hello packet prompt received from each interface.

A new neighbor is found.

Delete neighbor.

Interface sending status refresh packet. Interface receiving status refresh packet. Interface is sending Assert packet.
Interface is receiving Assert packet. Interface is sending prune packet. Interface is receiving prune packet. Interface is sending graft ack packet.
Interface is receiving graft ack packet. Interface is sending graft packet. Interface is receiving graft packet.

Interface is sending join/prune packet. Interface is receiving join/prune packet. When a new (S,G) is created
When deleting (S,G)

Router#debug ip pim-dm

2003-3-26 11:45:17 received V2 hello packet on Ethernet2/1 from 192.168.20.133(GenID = 3539)

2003-3-26 11:45:17 Ethernet2/1 create new nbr 192.168.20.133 2003-

3-26 11:45:25 send hello packet to 224.0.0.13 on Loopback1

2003-3-26 11:50:29 Ethernet2/1 delete nbr 192.168.20.133

2003-3-26 11:50:51 received V2 hello packet on Ethernet2/1 from 192.168.20.152

2003-3-26 11:50:51 send hello packet to 224.0.0.13 on Ethernet2/1

2003-3-26 12:04:37 PIM-DM: delete (192.168.20.138, 239.1.1.1) in MRT success

2003-3-26 12:04:37 PIM-DM: clear (192.168.20.138, 239.1.1.1) from MRT successful

2003-3-26 12:04:39 PIM-DM: ignored V2 packet on Ethernet2/1 from 192.168.10.204 (validate source address failed)

2003-3-26 12:04:39 PIM-DM: (192.168.20.138, 239.1.1.1)'s upstream:192.168.20.132 Adding in MRT success

2003-3-26 12:04:39 PIM-DM: (192.168.20.138, 239.1.1.1) Adding in MRT

Example 2, output received alert message:

Router#debug ip pim-dm alert

2003-3-26 12:09:51 receive alert_rt_change alert from mroute

2003-3-26 12:09:54 receive alert_rt_change alert from mroute

2003-3-26 12:11:08 PIM-DM: send sg_deletion alert

2003-3-26 12:11:19 receive alert_sg_creation alert from mroute

2003-3-26 12:11:20 receive alert_sg_prune alert from mroute 2003-

3-26 12:11:56 receive alert_group_reinterface alert from mroute

2003-3-26 12:11:56 receive alert_sg_join alert from mroute

Example 3, track the specified group status:

Router#deb ip pim-dm 239.1.1.1

Router#2003-3-26 12:35:27 PIM-DM: clear (192.168.20.138, 239.1.1.1) forwd pkt count success

2003-3-26 12:35:37 PIM-DM: delete (192.168.20.138, 239.1.1.1) in MRT success

2003-3-26 12:35:37 PIM-DM: clear (192.168.20.138, 239.1.1.1) from MRT successful

2003-3-26 12:35:37 PIM-DM: (192.168.20.138, 239.1.1.1)'s upstream: 192.168.20.132 Adding in MRT success

2003-3-26 12:35:37 PIM-DM: (192.168.20.138, 239.1.1.1)'s downstream: 1.1.1.1 create success

2003-3-26 12:35:37 PIM-DM: (192.168.20.138, 239.1.1.1)'s downstream: 192.167.20.132 create success

2003-3-26 12:35:42 PIM-DM: (192.168.20.138, 239.1.1.1) Adding in MRT

3.1.4 ip pim-dm

This command is used to run PIM-DM on the interface. To disable this feature, use the no form of this command.

PIM-DM on the interface.

Syntas

ip pim-dm

no ip pim-dm

Parameter

None

Default

None

Command Mode

Interface configuration

Usage Guidelines

1. If the “ip multicast-routing” is not configured before configuring this command, it will display the following warning: WARNING: "ip multicast-routing" is not configured, IP Multicast packets will not be forwarded.
2.
2. Once this function is disabled, PIMDM will no longer run on the interface.but it will not affect other PIM-DM configurations. After rerun PIM-DM on the interface, all PIM-DM configurations are still valid.

3. Enabling this function means it is available for forwarding multicast packet on the interface, however, you have to enable the global multicast packet forwarding function first.

Example

Router_config#ip multicast-routing
Router_config#interface Ethernet1/1
Router_config_e1/1#ip pim-dm

Related Commands

ip multicast-routing

show ip pim-dm interface

3.1.5 ip pim-dm dr-priority

Set a router as the priority to specified router (DR). You can set this command to “no” to restore default DR priority on the interface.

Syntas

ip pim-dm dr-prioirty *priority*

no pim-dm dr-prioirty

Parameter

Parameter	Description
priority	Interface DR priority. The larger the value is, the higher the priority is. Its range is from 0 to 4294967294, and the default is 1.

Default

default DR priority on PIM interface is 1.

Command Mode

Interface configuration

Usage Guidelines

1. If all PIM neighbors supinterface DR Priority on the interface, select the one with the highest priority as DR. If all have the same priority, just select the one with the highest interface IP value as DR.

2. If router didn't advertise its priority in Hello packet and there are several routers have the same situation, just select the router with the highest interface IP value as DR.

3.1.6 ip pim-dm hello-interval

This command is used to configure the interval of regularly sent PIM-Hello packets on the interface. You can set this command to "no" to restore default interval.

Syntas

ip pim-dm hello-interval *interval*

no **ip pim-dm hello-interval**

Parameter

Parameter	Description
interval	The interval of regularly sent PIM-Hello packets. Its range is from 0 to 65535, and the default is 30 seconds.

Default

30 seconds

Command Mode

Interface configuration

Usage Guidelines

Regularly sending Hello packets can check if the neighbor exists. Generally, if Hello packets is not received after the 3.5 times hello-interval timeout configured by neighbor, the neighbor will be considered disappeared.

For IGMP v1, you can select the specified router (DR) through PIM-DM Hello packet.

Example

Router_config#interface Ethernet1/1

Router_config_e1/1#ip pim-dm hello-interval 30

Related Commands

ip igmp query-interval

The command can be used to configure the frequency at which the IGMP querier sends IGMP host-query messages from an interface. The IGMP querier sends query-host messages to discover which multicast groups have members on the attached networks of the router.

3.1.7 ip pim version

To configure the Protocol Independent Multicast (PIM) version of the interface, use the ip pim version command in Interface configuration.
ip pim version [*version*]

Parameter

Parameter	Description
version	PIM-DM

Default

Version: 2

Command Mode

Interface Configuration

Usage Guidelines

Version 2 is run by default. The router will not change the interface PIM-DM version if an interface has configured version 2 and the interface has a non PIM-DM version 2 neighbor. (That is, the device only supinterfaces version 2.)

Example

```
Router_config_e1/1#ip pim version 2
```

3.1.8 ip pim-dm state-refresh origination-interval

It allows the router to generate original PIM-DM state refresh packet and configure the state refresh interval. To cancel the generation for original PIM-DM state refresh packet, set this command to “no”.

Syntas

ip pim state-refresh origination-interval [*interval*]

no ip pim state-refresh origination-interval

Parameter

Parameter	Description
interval	For the first interface router connected with the source directly, it is the interval of regularly sending state refresh packet. For the following router, it is interval of allowed receiving and processing state refresh packet for the interface. This parameter is configured optionally, and its range is from 4 to 100 seconds. The default is 60 seconds.

Default

Refer to the command usage.

Command Mode

Interface configuration

Usage Guidelines

Configure this command on the first router's, neighboring directly on the multicast source, incoming interface. By default, it will generate original state refresh packet. During configuring this command on the following router's interface, you can use *interval* to limit the process for received state refresh packet interval. By default, all routers where is running PIM-DM can process and forward state refresh packet.

Example

Router_config_e1/1#ip pim-dm state-refresh origination-interval 80

Related Commands

ip pim-dm state-refresh disable

3.1.9 ip pim-dm neighor-filter

This command is used to prevent some routers from participating PIM-DM operation. Set this command to "no" to cancel the limit.

Syntas

ip pim-dm neighor-filter *acess-list-name*

no ip pim-dm neighor-filter *acess-list-name*

Parameter

Parameter	Description
access-list-name	Standard access-list, whose definition is to deny PIM packets from the specified source.

Default

No filter function.

Command Mode

Interface configuration

Usage Guidelines

You can use multiple filter lists. The router denied by anyone of the lists can't be a neighbor of local PIM-DM.

Example

```
router_config_e1/1#ip pim-dm neighbor-filter nbr_filter
router_config#ip access-list standard nbr_filter
router_config_std_nacl#deny 192.167.20.132 255.255.255.255
router_config_std_nacl#permit 192.168.20.0 255.255.255.0
```

Related Commands

access-list

3.1.10 ip pim-dm state-refresh disable

It will not allow running router process for PIM-DM multicast protocol or forward PIM-DM state refresh control message. You can set this command to "no" to restore the forwarding function.

Syntas

ip pim-dm state-refresh disable

no ip pim-dm state-refresh disable

Parameter

None

Default

By default, it is allowed to run forwarding PIM dense mode state refresh control message.

Command Mode

EXEC

Usage Guidelines

After configuring this command to forbid processing and forwarding PIM-DM state refresh control message, the Hello message in PIM-DM will no longer contain state refresh control options and receive/send state refresh control packet.

Example

The following command forbids forwarding state refresh control message to downstream neighbors of PIM dense mode.

ip pim-dm state-refresh disable

Related Commands

ip pim-dm state-refresh origination-interval

3.1.11 show ip mroute pim-dm

Display PIM-DM multicast routing list information.

Syntas

s**how ip mroute pim-dm** *group-address* ***source***

Parameter

Parameter	Description
group-address	(optional) group address
source	(optional) source address

Default

None

Command Mode

All modes except the user mode.

Usage Guidelines

It can display all (S,G) or specified (S,G) only in local MRT.

Example

Example1: Display all (S,G) in local MRT.

```
Router#show ip mroute pim-
dm PIM-DM Multicast
Routing Table Timers:
Uptime/Expires
State: Interface state
RPF nbr: RPF neighbor address
(192.168.20.151, 224.1.1.1), 00:00:03 /00:03:27
  Incoming interface:
    Ethernet2/1   Forwarding        0.0.0.0
  Outgoing interface list:
    Loopback1      NoInfo    00:00:07 /00:00:00

(192.168.20.138, 239.1.1.1), 00:00:03 /00:03:27
  Incoming interface:
    Ethernet2/1 Forwarding 0.0.0.0
  Outgoing interface list:


    Loopback1      NoInfo    00:00:07 /00:00:00
    Ethernet1/1   NoInfo     00:02:43 /00:00:00
```

Example 2: Display the specified (S,G) in local MRT.

```
Router#show ip mroute pim-dm 224.1.1.1
PIM-DM Multicast Routing Table
Timers: Uptime/Expires
State: Interface state
RPF nbr: RPF neighbor address
(192.168.20.151, 224.1.1.1), 00:00:01 /00:03:29
Incoming interface:
Ethernet2/1   Forwarding          0.0.0.0
Outgoing interface list:
Loopback1        NoInfo  00:03:50 /00:00:00
```

Example3: Display the specified (S,G) in local MRT.

Router#show ip mroute pim-dm 224.1.1.1 192.168.20.131

PIM-DM Multicast Routing Table

3.1.12 show ip pim-dm neighbor

To display the PIM-DM neighbor and the selected DR, run the following command:

show ip pim-dm neighbor [***interface-type*** *interface-number*]

Parameter

Parameter	Description
interface-type *interface-number*	Type and ID of the interface, such as Ethernet1/1 and serial 11/0

Default

None

Command Mode

All modes except the user mode

Usage Guidelines

This command is used to check on which LAN routers PIM-DM or PIM-SM is configured.

Example

Example 1:

Router#show ip pim-dm neighbor

PIM-DM Neighbor Table

Neighbor Address	Interface	Uptime/Expires	Ver	DR Prior/Mode	
192.167.20.132	Ethernet1/1	03:13:34 / 00:00:00	v2	4/D	(DR)
1.1.1.1	Loopback1	03:52:30 / 00:00:00	v2	1/D	(DR)
192.168.20.13	Ethernet2/1	19:35:56 /	v2	1/D	
192.168.20.15	Ethernet2/1	00:00:04 /	v2	1/D	
192.168.20.20	Ethernet2/1	00:00:36 /	v2	20/D	(DR)

Example 2:

```
Router# show ip pim-dm neighbor Ethernet2/1
PIM-DM Neighbor Table
Neighbor        Interface       Uptime/Expires   Ver  DR Prior/Mode
Address
192.168.20.13   Ethernet2/1     19:39:22 /       v2   1/D
192.168.20.15   Ethernet2/1     00:00:30 /       v2   1/D
192.168.20.20   Ethernet2/1     00:00:04 /       v2   20/D   (DR)
```

Related command

ip pim-dm

ip pim-dm dr-priority

ip pim-dm hello-interval

ip pim version

ip pim-dm neighor-filter

show ip pim-dm interface

3.1.13 show ip pim-dm interface

To display the state of the PIM-DM interface, run the following command: **show ip pim-dm interface** [***interface-type*** *interface-number*] [***count***][***detail***]

Parameter

Parameter	Description
interface-type *interface-number*	Type and ID of the interface, such as Ethernet1/1 and serial 11/0

Default

None

Command Mode

All modes except the user mode

Usage Guidelines

Only the state of the PIM-DM interface can be displayed after this command is run. If the PIM-DM interface is not designated, the information about all PIM-DM interfaces' state will be displayed.

Example

Example 1:

```
Router#show ip pim interface
address          Interface          Ver/   Nbr    Hello   DR      DR
                                    Mode   Count  intvl   Prior
192.167.20.132   Ethernet1/1        v2/D   0      30      4       192.167.20.132
1.1.1.1          Loopback1          v2/D   0      30      1       1.1.1.1
192.168.20.132   Ethernet2/1        v2/D   2      30      1       192.168.20.204
```

Example 2:

```
Router#show ip pim interface Ethernet2/1
address          Interface          Ver/   Nbr    Hello   DR      DR
                                    Mode   Count  intvl   Prior
192.168.20.132   Ethernet2/1        v2/D   2      30      1       192.168.20.204
```

Related command

ip pim-dm

ip pim-dm dr-priority

ip pim-dm hello-interval

ip pim version

ip pim-dm neighor-filter

show ip pim-dm neighbor

3.1.14 show ip rpf pim-dm

To display how the multicast route conducts the Reverse Path Forwarding (RPF), run the following command:

show ip rpf pim-dm *source-address*

Parameter

Parameter	Description
source-address	Displays the RFP information of the designated source address.

Default

None

Command Mode

All modes except the user mode

Usage Guidelines

The PIM-DM protocol can obtain the RPF information from multiple types of routing tables. This command tells you where the RPF information is obtained.

Example

Router#show ip rpf pim 4.1.1.1
RPF information for (4.1.1.1)
RPF interface: Ethernet2/1
RPF neighbor: 192.168.20.80
RPF route/mask: 192.168.20.0/24
RPF type: unicast
Metric preference: 120
Metric: 1

Related command

None

Chapter 4 PIM-SM Configuration Commands

4.1 PIM-SM Configuration Commands

PIM-SM configuration commands include:

- ip pim-sm
- ip pim-sm admin-scope
- ip pim-sm asrt-hold
- ip pim-sm bsr-border
- ip pim-sm dr-pri
- ip pim-sm hello-intvl
- ip pim-sm holdtime
- ip pim-sm horizon-split
- ip pim-sm jp-hold
- ip pim-sm jp-intvl
- ip pim-sm lan-delay
- ip pim-sm nbma-mode
- ip pim-sm nbr-filter
- ip pim-sm nbr-track
- ip pim-sm override
- router pim-sm
- hello-option
- accept bsm-adv
- accept crp-adv
- accept rp-addr
- accept register
- anycast-rp
- reg-rate-limit
- reg-src
- spt-threshold
- ssm
- c-bsr intf_type intf_name
- c-bsr admin-scope
- bsm policy
- static-rp
- c-rp intf_type intf_name
- intvl-time
- holdtime
- log

- show running-configure
- show ip pim-sm bsr-router
- show ip pim-sm sz-info
- show ip pim-sm interface
- show ip pim-sm neighbor
- show ip pim-sm rp
- show ip pim-sm rp-hash
- show ip pim-sm anycast-rp
- show ip pim-sm protocol
- show ip mroute pim-sm
- show ip rpf pim-sm
- debug ip pim-sm alert
- debug ip pim-sm assert
- debug ip pim-sm bsr
- debug ip pim-sm rp
- debug ip pim-sm entry
- debug ip pim-sm event
- debug ip pim-sm hello
- debug ip pim-sm jp
- debug ip pim-sm nbr
- debug ip pim-sm packet
- debug ip pim-sm register
- debug ip pim-sm timer

4.1.1 ip pim-sm

Syntas

ip pim-sm

no ip pim-sm

Parameter

None

Default

Disable PIM-SM

Command Mode

Interface configuration

Usage Guidelines

To enable PIM-SM function on an interface.You will enable PIM-SM when you configure the routers first in the router interface .you can cancle PIM-SM configure in the last interface to stop PIM-SM running .
Configure ip multicast-routing at first and then enable pimsm in the Global configuration.
If pim-sm is enabled for the first time, hello mechanism and IGMP will be enabled. In the first configuration, the interface will trigger hello packets. The trigger timer is an arbitrary value ranges from 0 to 5.
Following prompts will pop up:
WARNING: "ip multicast-routing" is not configured,IP Multicast packets will not be forwarded Pim-sm cannot be configured if the interface has configured other multicast protocols:

Example

The following example indicates the interface f0/0 will start PIM-SM multicast protocl.

```
Router_config_f0/0#ip pim-sm
```

Related Commands

None

4.1.2 ip pim-sm admin-scope

To configure the multicast administrator scope, run **ip pim-sm admin-scope *gaddr gmask***. The designated multicast address ranges between 239.0.0.0 and 239.255.255.255. This command is configured only on the edge routers which interlace other SZs.

ip pim-sm admin-scope *gaddr gmask*

no ip pim-sm admin-scope

Parameter

Name	English prompt	Description
admin-scope	admin-scope – pim-sm administrator scope	Only the C-BSRs and the ZBRs need to be configured to know about the existence of the scope zones. Other routers, including the C-RPs, learn of their existence from Bootstrap messages.
gaddr	A.B.C.D – private group address prefix	239.0.0.0 to 239.255.255.255
gmask	gmask – sz group mask	

Default value

The global domain is 224.0.0.0/4 by default.

Command Mode

Interface configuration

Instruction

This command is configured on the boundary of the PIM-SM administrator scope and used to check the BSM information which is received from the outside of the administrator scope. If the SZ scope of the received BSM information is smaller than or equal to the locally configured administrator scope, the received BSM information will be discarded. Otherwise, the received BSM information will enter the local administrator scope. When the BSM information is forwarded locally, the same principle is followed. At present, Huawei only supinterfaces the global domain and the private domain, but does not supinterface the covering of the group address. RP in SZ1 will not notify the global SZ of the C-RP-ADV information. But the global BSM information can get in.

Example

The following example shows how to configure the boundary scope on routerA to **pim-sm sz1(239.1.1.1/24)**.

RouterA_config_f0/0#ip pim-sm admin-scope 239.1.1.1 255.255.255.0
RouterB_config_ps# c-bsr interface lo1
RouterB_config_ps# c-bsr admin-scope 239.1.1.1 255.255.255.0

Related command

ip pim-sm bsr-border c-bsr intf_type intf_name

4.1.3 ip pim-sm asrt-hold

To configure the holdtime for the **assert** state on the interface corresponding to PIM-SM, run the following command.

ip pim-sm asrt-hold *intvl*

no ip pim-sm asrt-hold *[*intvl*]*

Parameter

Name	English prompt	Description
pim-sm	pim-sm - Enable PIM sparse mode operatioin	
asrt-hold	***asrt-hold*** – assert status hold timer	
intvl	<7-65535> - time value (second)	The default value is 180 seconds.

Default value

180 seconds

Command Mode

Interface configuration

Instruction

Example

The following example shows how to configure the timeout time in **assert** state on interface f0/0 to 200 seconds.

Router_config_f0/0#ip pim-sm holdtimer assert 200

4.1.4 ip pim-sm bsr-border

To prevent bootstrap router (BSR) messages from being sent or received through an interface, use the ip pim bsr-bordercommand in Interface configuration. To disable this configuration, use the no form of this command.

Syntas

ip pim-sm bsr-border

no ip pim-sm bsr-border

Parameter

Name	English prompt	Description
pim-sm	pim-sm - Enable PIM sparse mode operatioin	
bsr-border	bsr-border – BSR border	

Default

Disable

Command Mode

Interface configuration

Usage Guidelines

When this command is configured on an interface, no Protocol Independent Multicast (PIM) Version 2 BSR messages will be sent or received through the interface. Configure an interface bordering another PIM domain with this command to avoid BSR messages from being exchanged between the two domains. BSR messages should not be exchanged between different domains, because routers in one domain may elect rendezvous points (RPs) in the other domain, resulting in protocol malfunction or loss of isolation between the domains.

Examples

The following example configures the interface to be the PIM domain border:
Router_config_f0/0# ip pim-sm bsr-border

Related Commands

Command	Description
ip multicast boundary	Configures an administratively scoped boundary.
ip pim bsr-candidate	Configures the router to announce its candidacy as a BSR.

4.1.5 ip pim-sm dr-pri

Syntas

ip pim-sm dr-pri *pri-value* **no**

ip pim-sm dr-pri *pri-value*

Parameter

Name	English prompt	Description
dr-pri *Pri-value*	dr-pri - pim-sm interface DR priority <0-4294967294> - DR priority, preference given to larger value	

Default

DR priority is the default in global mode; DR priority is 1 by default in global mode.

Command Mode

Interface configuration

Usage Guidelines

To change interface DR priority, use “no”command to recovery default value.

The highest priority routers will be DR. If the priority is same, then the highest address is DR. Considering situations including assert status machine, (s,g) and (*,g) if DR becomes non-DR or vice verse4.

Examples

The following example sets the DR priority value to 200 for the pim-sm interface f0/0:

```
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm dr-pri 200
```

Related Commands

None

4.1.6 ip pim-sm hello-intvl

Syntas

ip pim-sm hello-intvl *seconds*

no pim-sm hello-intvl *[seconds]*

Parameter

Name	English prompt	Description
hello-intvl *seconds*	hello-intvl - pim-sm hello advertisement interval <1-65535> - periodic pim hello message are sent(unit:s)	

Default

The interval of sending Hello messages is 30s.

Command Mode

Interface configuration

Usage Guidelines

To configure hello message sending interval, use “no”command to renew default value. To change the hold-time of neighbor router, hold-time is 3.5 times of hello message

sending interval.

Examples

The following example sets the DR priority value to 200 for global pimsm configuration:

```
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm hello-intvl 40
```

4.1.7 ip pim-sm holdtime

To configure the interval of the hello timer on the PIM-SM interface, run the following first command. The value of the interval ranges between 4 and 65535.

ip pim-sm holdtime *seconds*

no pim-sm holdtime [*seconds*]

Parameter

Name	English prompt	Remarks
Holdtime	holdtime – keep alive time to neighbor	
seconds	<4-65535> - keep alive time value	

Default value

105 seconds

Command Mode

Interface configuration

Instruction

This command is first run in Interface configuration and then in Global configuration or the default value is chosen. If the value of the holdtime is smaller than that of Hello interval, the configured value is then invalid. The value of the holdtime is **hello-intvl***3.5.

Example

The following example sets the holdtime value to 100 for interface pimsm configuration:

```
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
```

Router_config_f0/0#ip pim-sm holdtime *100*

Related command

ip pim-sm hold-intvl

intvl-time hello *hlo-*

intvl

4.1.8 ip pim-sm horizon-split

To configure the horizon split strategy of the BSM packets on a interface, run the following first command.

ip pim-sm horizon-split

no ip pim-sm horizon-split

Parameter

Name	English prompt	Remarks
horizon-split	Horizon-split – permit interface horizon split	

Default value

The horizontal split is disabled by default.

Command Mode

Interface configuration

Instruction

After this command takes effect, you can set the corresponding label bit of the PIM-SM interface. The BSM packets that are received from a interface will not be transmitted from the interface.

Example

The following example sets the DR priority value to 200 for the interface f0/0:

Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm ***horizon-split***

Related command

bsm policy

4.1.9 ip pim-sm jp-hold

To configure the holdtime for the **join-prune** state on the interface corresponding to PIM-SM, run the following first command.

ip pim-sm jp-hold *intvl*

no ip pim-sm jp-hold *[intvl]*

Parameter

Name	English prompt	Remarks
pim-sm *jp-hold*	pim-sm - Enable PIM sparse mode operation Join-prune –join-prune status hold timer <1-65535> - time value (second)	The default value is 210 seconds.

Default value

210 seconds

Command Mode

Interface configuration

Instruction

Example

The following example shows how to configure the timeout time in **join** state on interface f0/0 to 200 seconds.

Router_config_f0/0#ip pim-sm jp-hold 200

4.1.10 ip pim-sm jp-intvl

To set the interval of transmitting the **join** or **prune** packets periodically, run the following first command. The interval, whose unit is second, ranges between 1 and 65535.

ip pim-sm jp-intvl [*seconds*]

***no* ip pim-sm jp-intvl**

Parameter

Name	English prompt	Remarks
pim-sm	pim-sm - Enable PIM sparse mode operatioin	The default value is 60 seconds.
jp-intvl	jp-intvl – regular Join/Prune message interval (unit:s)	
Second	<1-65535> - time value (second)	

Default value

60 seconds

Command Mode

Interface configuration

Instruction

*At each configuration the PIM-SM database must be entirely searched for the **(s, g)** pairs or the **(*, g)** pairs; if the configured interface is an upstream one, the interval of the **jp** timer of the corresponding **(s, g)** or **(*, g)** pair should be reset. The interval in Interface configuration is prior to the **join/prune** interval in global mode.* If the **Join** packets from the downstream neighbor have not been received in three JP timeout periods, the downstream that corresponds to the multicast item will be shifted to the **prune** state. The default holdtime is 3 minutes. If this value is changed randomly, CPU shock and service-forwarding shock may be caused.

Example

The following example changes the PIM join message interval to 90 seconds:

```
Router_config_f0/0# ip pim-sm jp-intvl 90
```

Related command

ip pim-sm jp-hold

4.1.11 ip pim-sm lan-delay

To designate the prune delay time of the PIM-SM interface, run the following first command.

ip pim-sm lan-delay *delay-intvl*

no pim-sm lan-delay

Parameter

Name	English prompt	Remarks
lan-delay	lan-delay - pim-sm prune delay	
delay-intvl	<1-32767> - prune delay time out interval(unit:ms)	The default value is 500 milliseconds.

Default value

500ms

Command Mode

Interface configuration

Instruction

If the local interface is the downstream interface, the finally calculated prune delay time is based on all maximum values reinterfaceed by downstream neighbors. In this case, the override timer of transmitting the **join** packets towards the upstream neighbors will be affected. If the **prune_delay** option is not supinterfaceed by all downstream neighbors, the default value will be used as the overtime interval of the **prune pending** timer. If the interval of the **prune delay** timer is locally set, it will be reinterfaceed to upstream neighbors through the HELLO packets.

Example

The following example sets the prune delay value to 200 ms for the pim-sm interface.

f0/0:

```
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm lan-delay 20
```

Related command

ip pim-sm override

4.1.12 ip pim-sm nbma-mode

If the following first command is configured on all NBMA interfaces, the central node will forward all information that is transmitted from the sub-nodes and the other sub-nodes can obtain the corresponding information.

ip pim-sm nbma-mode

no ip pim-sm nbma-mode

Parameter

Name	English prompt	Remarks
nbma-mode	nbma-mode - Use Non-Broadcast Multi-Access (NBMA) mode on interface	Currently our products do not supinterface this function.

Default value

Disable

Command Mode

Interface configuration

Instruction

Traditional NBMA networks (frame relay, ATM and SMDS) adopt the point-to-multipoint mode; when a sub-node need be pruned, it will reinterface this information directly to the central node and other sub-nodes, however, can not receive this information. In this case, other sub-nodes cannot respond and the interface of the central node will be incorrectly pruned.

If the following first command is configured on all NBMA interfaces, the central node will forward all information that is transmitted from the sub-nodes and the other sub-nodes can obtain the corresponding information.

This command cannot be used in multicast LANs, such as Ethernet or FDDI.

Example

The following example configures an interface to be in NBMA mode:

```
Router_config#interface s1/0
Router_config_s1/0#ip address 10.0.1.2 255.255.255.0
Router_config_s1/0#ip pim-sm nbma-mode
```

Related command

4.1.13 ip pim-sm nbr-filter

To stop a device from being added to PIM, run the following first command; to cancel this function, run the following second command.

ip pim-sm nbr-filter *acl-name*

no ip pim-sm nbr-filter

Parameter

Name	English prompt	Remarks
nbr-filter	nbr-filter - PIM peering filter	
acl-name	WORD – ip stand access list name	

Default value

Disable

Command Mode

Interface configuration

Instruction

If this command is configured, the neighbors need be filtered when Hello packets are received and then a new neighbor can be created. If it is in **deny** state, the corresponding new neighbor need not be created. Multiple neighbor access lists can be configured (New CISCO bin only allows to configure a neighbor access list; old bin allows to configure multiple neighbor access lists). Once a neighbor is filtered, the neighbor is then denied.

Example

The following example shows how to configure stub multicast routing on router A and how router B uses access list 1 to filter all PIM information from router A.

Router A Configuration

```
Router_config# ip multicast-routing
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.0.1 255.255.255.0
Router_config#interface f0/1
Router_config_f0/1# ip igmp-helper 10.0.0.2
```

Router B Configuration

Router_config# ip multicast-routing
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.0.2 255.255.255.0
Router_config_f0/0# ip pim-sm nbr-filter 1
Router_config#ip access-list standard 1
Router_config_std_nacl# deny 10.0.0.1
Router_config_std_nacl# permit any

Related command

ip pim-sm jp-intvl

4.1.14 ip pim-sm nbr-track

To forbid the limitation of the JOIN packets globally and enable neighbor tracking, run the following first command:

ip pim-sm nbr-track

no ip pim-sm nbr-track

Parameter

Name	Prompt	Remarks
nbr-track	nbr-track - pim-sm interface neighbor tracking	

Default value

If the global congfigration mode is not configured, neighbor tracking is forbidden.

Command Mode

Interface configuration

Instruction

This command is used to forbid the limitation function of the **join** packets and enable neighbor tracking.

Example

The following example sets the DR priority value to 200 for the interface f0/0:

Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm nbr-track

Related command

None

4.1.15 ip pim-sm override

To designate the prune deny time of the PIM-SM interface, run the following first command.

ip pim-sm override *override-intvl*

no ip pim-sm override

Parameter

Name	Prompt	Remarks
override	override - pim-sm override timer	
override-intvl	<1-65535> - override time out interval(unit:100ms)	

Default value

2.5s

Command Mode

Interface configuration

Instruction

The finally calculated prune deny time is based on the maximum value among all the values reinterfaceed by all neighbors. If some neighbor does not supinterface prune deny, the default value is selected. If OT is enabled, the value can be random. If the interval of the **prune deny** timer is locally set, it will be reinterfaceed to upstream neighbors through the HELLO packets.

Example

The following example sets the override value to 2000 ms for pim-sm interface f0/0 configuration:

Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm override 200

Related command

ip pim-sm lan-delay

4.1.16 router pim-sm

To enter the global PIM-SM view, under which there is common attributes, run the following first command:

router pim-sm

no router pim-sm

Parameter

None

Default value

The system will not generate the PIM-SM view by default.

Command Mode

Global configuration

Instruction

If the **router pim-sm** command is configured globally or the PIM-SM related configuration is first configured on the interface, the global PIM-SM view will be created. If there is some PIM-SM related configuration on the interface, the global view cannot be deleted.

Example

The following command shows how to create the global PIM-SM view:
Router_config#router pim-sm
Router_config_ps#

Related command

ip pim-sm

4.1.17 hello-option

To configure in the global PIM-SM view, the global DR priority, the prune delay time, the transmission interval of HELLO packets, the prune deny time, neighbor tracking and neighbor timeout time, run the following command:

hello-option { dr-pri *pri-value* | lan-delay *delay-intvl* |
override *override-intvl* | nbr-track | holdtime *hold-intvl* }

no hello-option [dr-pri | lan-delay | override | nbr-track | holdtime]

Parameter

Name	Prompt	Remarks
dr-pri	dr-pri - pim-sm global DR priority	
pri-value	<0-4294967294> - DR priority, preference given to larger value	If this command is not configured, the default DR priority of this process is 1.
lan-delay	lan-delay - pim-sm prune delay time	Configures the prune delay time.
override	Override – override for rcvd prune	Configures the prune deny.
delay-intvl	**<0-32767>** – value for prune delay	The default prune delay time is 500ms.
override-intvl	**<0-65535>** – value for override delay	The default prune deny time is 2500ms.
nbr-track	**nbr-track – neighbor track enable**	If this command is configured, the JOIN packets will not be limited.

Name	Prompt	Remarks
holdtime	**holdtime – neighbor keep alive timer**	
hold-intvl	**<4-65535>** – value for neighbor timeout	In normal case, its value is 3.5 times larger than the Hello interval on a interface. The default neighbor holdtime is 105 seconds.

Default value

See the table above.

Command

Mode Global PIM-

SM view

Instruction

If there is no corresponding configuration items on a interface, the globally configured attributes will be used as the corresponding attributes on the interface. The change of the global DR priority may affect the new DR selection.

The rules of DR selection are shown below:

1. The highest DR priority on a interface will be selected as the DR of the network segment to which this interface belongs; if there are many same DR values, the relatively large IP address among the main IP address on the local interface and the main IP address of the neighbor will be selected as DR.

2. If there are neighbors on an interface or the DR priority is not supinterfaceed on a interface, the relatively large mainaddress will serve as DR.

Example

The following example sets the DR priority value to 200 for global pimsm configuration:

```
Router_config#Router pim-sm
Router_config_ps#dr-priority 200
```

4.1.18 accept bsm-adv

You can run **accept bsm-adv** in global mode to set the filtration list. The filtration list settings is especially for filtrating specific BSM source addresses and receive the designated BSM source address. To cancel the filtration, you can run **no accept bsm-adv [*list* *std-acl*]**.

accept bsm-adv *list* *std-acl*

no accept bsm-adv [*list* *std-acl*]

Parameter

Name	Prompt	Remarks

accept	Accept – configure accept policy	
bsm-adv	bsm-adv - BSM packet source address accept filter	
list	list - IP access-list for bsm source-list	
std-acl	WORD -- stand access list name	It is used to limit the range of the BSM source address.

Default value

This filtration is disabled by default.

Command Mode

pim-sm global view

Instruction

Only one filtration command can be set.

Example

The following example shows that the BSM notifications only from network segment 192.2.2.0/30 can be received.

```
Router_config#router pim-sm
Router_config_ps#accept bsm-adv list adv-
src Router_config_ps#exit
Router_config#ip access-list stand adv-src
Router_config_std_nacl#permit 192.2.2.0 255.255.255.252
```

4.1.19 accept crp-adv

To set the filtration list specially for filtrating the address range of specific groups, limiting to receive the C-RP-ADV packets from specific candidate rp unicast, and specifying the group address' range in the received packets through ACL. To cancel the filtration, you can run **no accept crp-adv *.*.*.*** *[std-acl]*.

accept crp-adv *.*.*.* *[std-acl]*

no accept crp-adv *.*.*.* *[std-acl]*

Parameter

Name	Prompt	Remarks
accept	Accept – configure accept policy	
c-rp-adv	crp-adv – C-RP-ADV accept filter c	
A.B.C.D	A.B.C.D - IP address of candidate RP for group	
std-acl	WORD – ip stand access-list name for group	

Default value

Disable (not filtrating C-RP-ADV from c-rp)

Command Mode

pim-sm global view

Instruction

After this command is set, BSR only processes C-RP-ADV from RP. Additionally, the range of the group address must be allowed by the standard ACL.

Example

The following example states that the router will accept c-rp messages RP address is 100.1.1.1 for the multicast group 224.2.2.2:

```
Router_config#router pim-sm
Router_config_ps#accept crp-adv 100.1.1.1 grp-acl
Router_config#ip access-list stand grp-acl
Router_config_std_nacl#permit 224.2.2.2 255.255.255.255
```

4.1.20 accept rp-addr

Run **accept-rp** in Global configuration to set the filtration list to filter the specific group address range, deciding whether the join/prune of (*, G) is acceptable and responding to the registration information of specific destination group addresses. To cancel this setting above, run the “no” form of this command.

accept rp-addr *A.B.C.D [std-acl]*

no accept rp-addr *A.B.C.D*[*std-acl*]

Parameter

Name	Prompt	Remarks
accept	Accept – configure accept policy Accept – Configure the policy of packet reception.	
rp-addr	rp-addr - RP address accept filter rp-addr – Configure the acceptable RP address filter.	
A.B.C.D	A.B.C.D - IP address of RP for group A.B.C.D – Designate the RP address of a multicast group.	
std-acl	WORD – ip stand access-list name for group WORD – Stands for the standard access list that is used for multicast group filtration.	If omitting it, the router will process all the PIM-SM message to any group which is mapped to the RP.

Default value

Disable (All Join, Prune or Register packets will be processed)

Command Mode

pim-sm global view

Instruction

After this command is set, the router processes only those Join packets which are mapped to the designated RP. Another point deserving attention is that the range of the group address must be allowed by the standard access list. The aggregation point of the corresponding group must be the calculated RP, and when the aggregation point matches up with the RP can the access filtration list be applied. If the group address is denied, RP will reject the Join and Register packets; after the Register packets are received, RP will return a Register Stop packet to the registration packet generator.

This command can be set many times if the **rp-addr** parameters in this command are different. If the RP that the group address is mapped to is not in the configured range, the RP will be denied directly.

Example

The following example states that the router will accept join or prune messages destined for the RP at address 100.1.1.1 for the multicast group 224.2.2.2:

```
Router_config#router pim-sm
Router_config_ps#accept rp 100.1.1.1 no-ssm-range
```

Router_config#ip access-list extended no-ssm-range
Router_config_std_nacl#permit 224.2.2.2

%PIM-6-INVALID_RP_JOIN: Received (, 238.1.1.1) Join from 192.17.20.173 for invalid RP 1.1.1.1*
Router#show ip mroute
(, 238.1.1.1), 00:02:52/00:00:07, RP 1.1.1.1, flags: S*
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
FastEthernet0/0, Forward/Sparse, 00:02:52/00:00:07
It can be seen that the previous address, *.238.1.1.1, ages after the filtration is set.

4.1.21 accept register

When the Register range list is set on C-RP, the selection is RP and the PIM-SM Register packet is received, the filtration list should be used to filter the Register packets. In this case, you should run **accept-register**, and if you want to cancel the filtration, run the “no” form of this command.

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

no **accept register** [***list*** *ext-acl* **|** ***route-map*** *map-name*]

Parameter

Name	Prompt	Remarks
accept	Accept – configure accept policy Accept – Configure the policy of packet reception.	
register	register - Registers accept filter Register – Stands for the filter of receiving the Register message.	
list	list – access list list – stands for the access list.	
route-map	Route-map – route map route-map – stands for the route map list.	
ext-acl	WORD – IP extend access list name WORD – stands for the name of the extensible IP access control list.	
map-name	WORD – route map name WORD – stands for the name of the route map list.	

Default value

The access list filtration or the route-map filtration will not be conducted to the Register packets.

Command Mode

pim-sm global view

Instruction

This command is used to prevent those unauthenticated data source from sending the Register packets to RP. If an unauthenticated data source sends a Register packet to RP, RP will return a Register Stop packet at once. This command takes effect only on the machine that runs as RP.

Example

The following example shows how to restrict the RP from allowing sources in the Source Specific Multicast (SSM) range of addresses to register with the RP.

Router_config#router pim-sm Router_config_ps#accept
register list no-ssm-range Router_config#ip access-list
extended no-ssm-range Router_config_std_nacl#deny ip any
232.0.0.0 0.255.255.255
Router_config_std_nacl#permit ip any any

Related command

reg-src

4.1.22 anycast-rp

Through configuring **anycast-rp** and the corresponding neighbor address, you can specify the corresponding peer neighbor to share the load of RP. To cancel this setting above, run the “no” form of this command.

anycast-rp *A.B.C.D* **nbr *.*.*.***

no **anycast-rp** *A.B.C.D* **nbr *.*.*.***

Parameter

Name	Prompt	Remarks

anycast-rp	anycast-rp –anycast rp for pim-sm	

Name	Prompt	Remarks
A.B.C.D	*A.B.C.D – anycast rp address*	
nbr	nbr – anycast rp neighbor	
.*.*.	*A.B.C.D – anycast rp neighbor address*	

Default value

This command takes no effect by default.

Command Mode

pim-sm global view

Instruction

PIM-SM only regulates the standards of the single RP, but a big data flow can cause single RP overload easily. In this case, this command will be used to solve the overload of RP in the PIM-SM domain.

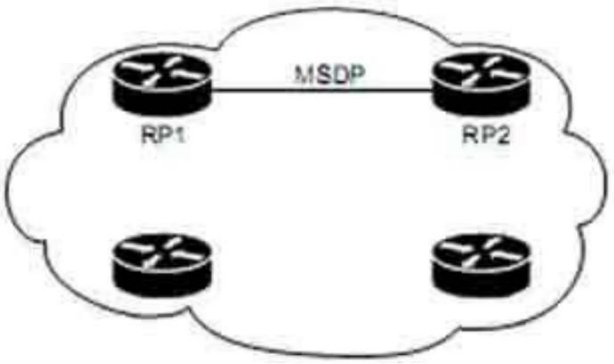
Note:

1. You'd better configure this command on the equipment with good connectivity in the PIM domain in the backbone network. That is, this command is not suitable to be set on the mute terminal router that connects other PIM equipments in the PIM domain through dial-up.

2. If the inside-domain MSDP is not used, the machine that specifies **anycast rp** must at the same time specify the address of a neighbor with the same RP address so as to facilitate the processing of the register.
3. The command, **anycast-rp A.B.C.D nbr**, is used on those devices that have no MSDP settings and provide an address as the static RP. All peer neighbors need be specified. The neighbors are reachable to one another.
4. If MSDP is set, the device, if it has provided the static RP address, need not specify **anycast rp nbr**.

Example

1. The following example shows how to set the **anycast-rp** address when MSDP is used.



RP1:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.1 255.255.255.255
I
ip msdp peer 10.1.1.2 connect-source loopback 1
ip msdp originator-id loopback 1

RP2:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.2 255.255.255.255
I
ip msdp peer 10.1.1.1 connect-source loopback 1
ip msdp originator-id loopback 1
Designate the static RP address on other devices, for example, do it on router Ra: Ra:
router pim-sm
static-rp 10.0.0.1

2. The following example shows how to make settings when the MSDP is not used.

RP1:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.1 255.255.255.255
router pim-sm
anycast-rp 10.0.0.1 nbr 10.1.1.1
anycast-rp 10.0.0.1 nbr 10.1.1.2

static-rp 10.0.0.1

RP2:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.2 255.255.255.255
router pim-sm
anycast-rp 10.0.0.1 nbr 10.1.1.1
anycast-rp 10.0.0.1 nbr 10.1.1.2
static-rp 10.0.0.1
Designate the static RP address on other devices, for example, do it on router Ra:

Ra:
router pim-sm
static-rp 10.0.0.1

Related command

4.1.23 reg-rate-limit

As to (s, g), if you want to set the regeneration rate limit of the PIM-SM registration packets per second, you should use the **reg-rate-limit** command; to cancel this settings , you can run **no reg-rate-limit [*rate*]**.

reg-rate-limit *rate*

no reg-rate-limit [*rate*]

Parameter

Name	Prompt	Remarks
reg-rate-limit *rate*	reg-rate-limit - Rate limit for PIM data registers <1-65535> Packets per second	

Default value

The regeneration rate of the registration packets of any (s,g) can be limited to one packet per second.

Command Mode

pim-sm global view

Instruction

This command can be used to limit the regeneration rate of registration packets of (s.g) on the DR router. After this command is enabled, the load of the DR router will be limited. At the initial establishment of multicast path, the sudden eruption of large traffic of the multicast source may lead to packet loss due to the rate limit and the multicast receiver cannot receive all the multicast packets.

Example

The following example shows how to do the corresponding settings to let each (s.g) generate two registration packets per second.

```
Router_config#router pim-sm
Router_config_ps#reg-rate-limit 2
```

4.1.24 reg-src

To specify an IP address of a interface to run as the source address for DR to transmit the PIM-SM registration packets, replacing the default interface's address that connects the data source, run **reg-src**. If you use the **reg-src** command, the specified interface must be active. To cancel these settings, you can run **no reg-src [***intf-type intf-number***]**.

reg-src *intf-type intf-number*

no reg-src [*intf-type intf-number***]**

Parameter

Name	Prompt	Remarks
reg-src	reg-src - Source address for PIM Register	
intf-type *intf-number*	Type of the designated interface and its name	If a interface has no main IP address or has no ID, the settings will take no effect. The L3 protocol of a designated interface must be up.

Default value

By default, the interface that connects DR and the data source will be used as the source address of the Register packet to conduct packet encapsulation.

Command Mode

pim-sm global view

Instruction

When the default source address of the Register packet is not the only routable destination address for RP to return the Register Stop packet, you should use this command to set a new source address for the Register packet. For example, in cases that the source address of the Register packet will be filtered on RP by ACL or the source address is not the only IP address, the Register Stop packet returned by RP may not reach the corresponding DR correctly and then the PIM-SM registration finally may fail.

If the source address of the Register packet is not specified or the specified source address takes no effect, DR will choose the interface, which connects the data source, as the source address of the Register packet. Therefore, it is recommended to set for the PIM-SM domain a unique routable address on the loopback interface as the source address of the Register packet.

Example

The following example shows how to designate the address of the loopback3 interface of DR

as the source address of the Register packet.

```
Router_config#router pim-sm
Router_config_ps#reg-src loopback 3
```

4.1.25 spt-threshold

To set the traffic threshold for a flow to switch over to the shortest path tree, run **spt-threshold** in PIM-SM configuration mode. To disable this feature, run **no spt-threshold**.

spt-threshold *{**infinity**/kbps} [stand-acl]*

no **spt-threshold**

Parameter

Name	Prompt	Remarks
spt-threshold	spt-threshold - Source-tree switching threshold	
infinity	Infinity - Never switch to source-tree	
kbps	<0-4294967> Traffic rate in kilobits per second	

Name	Prompt	Remarks
stand-acl	*stand-acl – ip standard access list name for group*	

Default value

There is no traffic limit for switchover. When the downstream receiver tries to join the data source, the data source will switch over to the SPT forwarding when it receives the data.

Command Mode

pim-sm global view

Instruction

If the forwarding rate of a multicast source reaches or exceeds the designated threshold, the leaf node will send a (s,g) Join packet to the multicast source for constructing the source tree—the shortest path tree.

If the threshold is set to **infinity**, all multicast sources for the designated group take the sharing tree for packet forwarding. The group access list designates which groups use the configured threshold for SPT switchover. If the message flow from the data source is less than the designated threshold, the PIM-SM router of the leaf node will be switched back to the sharing tree after a period of time and then send the Prune message to the source tree.

Example

The following example sets a threshold of 4 kbps, above which traffic to a group from a source will cause the router to router to the shortest path tree to that source:

```
Router_config#router pim-sm
Router_config_ps# spt-threshold 4
```

Related command

None

4.1.26 ssm

To set the range of a specific multicast group, run **ssm {default | range** *std-acl}*. To cancel the designated SSM range, run **no ssm**.

ssm {default | range *std-acl}* no **ssm**

Parameter

Name	Prompt	Remarks
ssm	ssm - Configure Source Specific Multicast	
Default	default - Use 232/8 group range for SSM	
Range	range - ACL for group range to be used for SSM	
std-acl	WORD - *ip standard access list name*	

Default value

Disable

Command Mode

pim-sm global view

Instruction

When PIM-SM is enabled, the default or configured range of the multicast group address can be used. If the multicast group is in the designated SSM range, the locally corresponding (,g) must be canceled. This requires the same strategic SSM shall be set in the whole PIM-SM.*

Note:

1. The same SSM strategy shall be set in the whole PIM-SM, otherwise the configured SSM will take no effect on preventing (*,g) Join for IGMPv3 can also specify the addition of (s,g) Join. Additionally, the (*,g) collision may be caused.
2. PIM-SM cannot be used together with other protocols. The configuration of SSM prevents the transmission of (*,g) Join and (*,*,rp) Join, and the PMBR device cannot send specific (s,g) Join to the upstream devices.
3. After SSM is set, MSDP cannot generate or receive SAs belonging to the designated range of the multicast group address. Our solution is that MSDP notification will be omitted if the group in the (S,G) items of PIM-SM is in the designated SSM group range,.
4. If the group range covers BIDIR group range, the previous configuration will be kept, and display error message to the later(not supinterface now).

Example

The following example shows how to configure SSM service for the IP address range defined by access list 4:

Router_config#router pim-sm
Router_config_ps# ssm range grp_range
Router_config#ip access-list stand grp_range
Router_config_std_nacl# permit 224.2.151.141

Related command

None

4.1.27 c-bsr intf_type intf_name

To set a router to be a candidate BSR router, run the first of the following two commands; to cancel this settings, run the second one of the following two commands.

c-bsr *intf_type intf_name* [*hash-length* [*priority*]]

no **c-bsr** *[intf_type][intf_name][hash-length][priority]*

Parameter

Parameter	Description
number	Maximum Number of Routes. Value ranges: 512~4096.

Default value

Dynamic BSR selection is disabled.

Command Mode

pim-sm global view

Instruction

After this command is set, the designated address of a interface will be used as the BSR address and it will send BSM (bootstrap messages) to all PIM-SM neighbors on the local machine. Each neighbor will compare the previously received BSM with the currently received BSM, and if the BSR address in the current BSM is larger than or equal to that in the previously received BSM, the locally stored BSM will be updated and the current BSM will be forwarded; otherwise, the current BSM will be dropped directly. Before the candidate BSR receives the BSM with higher priority, it always regards itself as the BSM router in the corresponding management domain.

Note:

1. You'd better configure this command on the equipment with good connectivity in the PIM domain in the backbone network. That is, this command is not suitable to be set on the

mute terminal router that connects other PIM equipments in the PIM domain through dial-up.

2. On accepting C-RP-Adv, BSR only accepts those contents that satisfy the SZ range; if the content exceeds the SZ range, it will be omitted.

3. You can specify only one interface of a device as the BSR address; if multiple commands are set, the previously configured candidate BSRs will be replaced.
4. The condition for this command to be effective is that the IP address of the designated interface is in PIM-SM state and the protocol is up.

Example

The following example configures the IP address of the router on Ethernet interface 0 to be a candidate BSR with priority of 10:

```
Router_config# router pim-sm
Router_config_ps# c-bsr f0/0 10 100
```

Related command

c-bsr admin-scope {global |*gaddr gmask***} [*hash-length* [*priority*]]**

4.1.28 c-bsr admin-scope

To set a candidate BSR in the administration domain, run the first one of the following two commands.

c-bsr admin-scope {global |*gaddr gmask***} [*hash-length* [*priority*]]**

no **c-bsr *admin-scope***

Parameter

Name	Prompt	Remarks

c-bsr	c-bsr –Candidate bootstrap router (candidate BSR)	
admin-scope	admin-scope – pim-sm administrator scope	
global	global – global range	224.0.0.0/255.0.0.0
gaddr	gaddr – sz group address	239.0.0.0 to 239.255.255.255
gmask	gmask – sz group mask	
hash-length	<0-32> - Hash Mask length for RP selection	
Priority	<0-255> - Priority value for candidate bootstrap router	

Default value

The global domain is 224.0.0.0/4 by default.

Command Mode

pim-sm global view

Instruction

This command is used to set the candidate BSR in the administration domain. This command corresponds to the **admin-scope** command in the domain boundary and is used to specify the range of the administration domain.

Note:

1. If the command, c-bsr intf type intf name, is not configured, this command takes no effect.
2. It is recommended to set this command in the administration range (239.0.0.0--239.255.255.255).

Example

The following example shows that C-BSR only takes effect in the administration domain 239.1.1.0/24:

```
Router_config# router pim-sm
Router_config_ps#c-bsr f0/0 10 250
Router_config_ps#c-bsr admoni-scope 239.1.1.1 255.255.255.0
```

Related command

c-bsr *intf_type intf_name* [*hash-length* [*priority*]]

4.1.29 bsm-policy

To set the BSM reception policy, run the first one of the following two commands in PIM-SM configuration mode. To disable this feature, run the other command.

bsm-policy { unicast *{rcvd* | *send}*| *forward-all* | *backward}*
no **bsm-policy** { unicast ***{rcvd* | *send}* |** *forward-all }*

Parameter

Name	Prompt	Remarks
bsm *policy*	bsm –bsm packet received	
unicast	Policy – the policy for BSM receive and forward	
	unicast –unicast bsm packet	The default value allows the reception of the unicast BSM packets.
rvd		The backward compatibility supinterfaces the transmission of unicast BSM.
forward-all	*rcvd*-permit receive bsm message	
	forward-all – forward all bsm packet	The horizontal division interface will not forward all BSM packets, including unicast or no-forward-bit reset packets.
backward	***backward -*** backwards compatibility supinterface send unicast BSM.	

Default value

There is no BSM reception or transmission policy.

Command Mode

pim-sm global view

Instruction

Refer to the description of this command.

Example

The following example configures the local router can receive bsm unicasted from neighbor:

```
Router_config# router pim-sm
Router_config_ps# bsm-policy   unicast rcvd
```

Related command

None

4.1.30 static-rp

To set the static RP of PIM-SM, run the first one of the following two commands; to resume the default settings, run the other command.

static-rp ***rp-addr*** **[*std-acl*] [override][bidir]**

no **static-rp** *rp-addr*

Parameter

Name	Prompt	Remarks

static	static - configure static rp-address for pim-sm	
rp-addr	A.B.C.D – pim-sm rp-address (Rendezvous Point)	
std-acl	WORD – IP stand access list	
override	override –If conflict,the static rp prevails over the dynamic RP	When static RP goes against dynamic RP, if the parameter is not designated, the dynamic RP will be chosen first, and if no dynamic RP exists or dynamic RP takes no effect can static RP take effect.
bidir	bidir - Group range treated in bidirectional shared-tree mode	It is not supinterfaceed currently.

Default value

disable

Command Mode

pim-sm global view

Instruction

The designated IP address of static RP must be legal unicast address and cannot be the loopback address (127.0.0.0/8). If ACL is designated, the configured static RP will serve the matched multicast group; if ACL is not designated, the configured static RP will serve all multicast groups (224.0.0.0/4). When static RP goes against dynamic RP, the former will be first chosen.

In PIM-SM or BIDIR mode, each group will be provided with an RP. All routers in the same administration domain must follow the identical rule to set RP for the group. RP can be obtained through two mechanisms: static configuration of the RP address or the BSR mechanism's dynamic learning of RP address. The **static rp-address** command can be used to set an RP to be the aggregation point of multiple groups. The ACL configured by static RP defines the RP application range. If the standard ACL is not set, the designated static RP will be applied to all groups. One PIM router can use multiple RPs, but it can use the only RP for a specific group.

If multiple **static rp-address** commands are set, the matchup rules of group-to-rp are listed below:

1. If a group matches up with multiple static RP rules, suitable RPs can be chosen according to the longest matchup principle specified by the standard ACL. As to the static configuration without designated ACL, it can be applied to all groups, but the entries in the ACL must be first set.

2. If a group and multiple ACLs accord to the longest matchup principle, the IP addresses of RPs must be compared and those RPs with big IP addresses come prior in choice.
3. If the static RP configuration is adopted, the reachability test will not be conducted to the designated RP. If an RP is selected, the RP with a comparatively low RP will not be chosen even though the route of the selected RP does not exist locally.
4. Each command can be used to specify a static RP address. If the designated static RP address or ACL rule is same during configuration, the new configuration will replace the previous configurations.

In case static RP and dynamic RP are used together, the rules of group-to-rp are listed below:

1. When the override is not specified, the RPs, dynamically learned through the BSR mechanism, come prior to static RPs.
2. If dynamic RP is used, the **c-rp intf_type intf_name** command must be set.

Note:

1. The same RP cannot be used simultaneously on BIDIR and PIM-SM.
2. The statically configured RP only supinterfaces global SZ or provides supinterface even if global SZ has not yet created.

Example

The following example shows how to designate 198.92.37.33 to be the static RP address.

```
Router_config#router pim-sm
Router_config_ps#static-rp 198.92.37.33
```

Related command

c-rp intf_type intf_name

4.1.31 Spt-always

To configure pim-sm spt-always, run the following command:
router pim-sm
Spt-always

Default

Disable

Command Mode

pim-sm global view

Usage Guidelines

A multicast flow will directly join the source SPT, ignoring the process of joining rpt first and then switching to spt.

Example

```
Router_config#router pim-sm
Router_config_ps#spt-always
```

4.1.32 c-rp intf_type intf_name

To set a interface to be C-RP and to send the unicast notification periodically to a designated BSR router in the PIM-SM domain, run the first one of the following two commands. To disable this feature, run the other command.

c-rp *intf-type intf-name* **[group-list** *std-acl***] [bidir][intvl** ***seconds*****][pri** ***pri-value*****]**

no **c-rp** *intf-type intf-name*

Parameter

Name	Prompt	Remarks
c-rp	c-rp - To be a PIMv2 RP candidate	
intf-type ***intf-name***	Designating the interface type and the interface's name	PIM-SM must be enabled on C-RP.
group-list ***std-acl*** **bidir**	group-list – ip access list for group-list WORD – ip stand access list bidir - Group range treated in bidirectional shared-tree mode	It is the prefix of the group address. It is not supinterfaceed currently.
intvl *Seconds*	Interval - RP candidate advertisement interval <1-32767> - number of seconds	
pri *pri-value*	pri – RP priority <0-255> - RP priority value	The smaller the value is, the higher the priority is. The default value is 192.

Default value

Dynamic RP selection is disabled.

Command Mode

pim-sm global view

Instruction

This command is used to notify all BSRs on C-RP. The range of the group address is listed in a form of the standard ACL.

Note:

1. PIM-SM must be enabled on the interface that serves as C-RP.
2. You'd better set C-RP on the main PIM-SM domain to avoid static configuration on similar routers or the on-demand dialup stub routers.
3. If C-RP is not specified with a multicast group range, C-RP will serve all multicast groups.
4. If you want to set a router to be C-RP for multiple group ranges, you need to represent multiple group ranges with multiple rules when configuring STD-AC1 that group-list corresponds to.
5. One interface can only be set to one C-RP and the following configuration will replace the previous configuration, including the replacement of STD-AC1.
6. You can set C-RP for multiple interfaces on the same PIM-SM router.
7. Multiple C-RPs can use the same standard ACL.
8. If this command is run many times on a same interface, the previous configuration will be replaced.
9. If multiple SZs are known on C-RP, unicast C-RP-Adv will be sent to the BSR of each SZ. It is noted that the established group range cannot exceed the group range of the destination SZ.
10. If C-RP itself is the ZBR of an SZ, the Admin Scope Bit in the C-RP-Adv packet must be reset; otherwise, this bit will not be reset. At present, it is used for BSR to record logs but possible to be used for protocol expansion.

Example

The following example shows how to designate lo172 and lo173 to be C-RP interfaces, the former limiting to provide RP to the group of prefix 239.1/16.

```
Router_config#router pim-sm
Router_config_ps# c-rp loopback172 group-list grp-
range Router_config# ip access-list standard grp-range
Router_config_std_nacl# permit 239.1.0.0 255.255.0.0
Router_config_ps# c-rp loopback173
```

Related command

None

4.1.33 intvl-time

To enable the periodical transmission of join/prune packets and set the interval of periodically transmitting the Hello, BSM or C-RP-Adv packets, run the first of the following two commands:

intvl-time { join-prune *jp-intvl* | *hello hlo-intvl* | *c-bsr cbsr-intvl* |*crp-adv crp-intvl*| *spt-check [spt-intvl]}*

no **intvl-time** {**join-prune** [*jp-intvl]* **|** ***hello* [*hlo-intvl]* |*c-bsr[****cbsr-intvl****]*| ***crp-adv*** **[***crp-intvl****]*** **|** ***spt-check [****spt-intvl****]}***

Parameter

Name	Prompt	Remarks
join-prune	**join-prune -** pim-sm regular join/prune packet periodic	
jp-intvl	<1-65535> - value for JP timer	The default interval of transmitting Join/Prune packets is 60 seconds.
Hello	hello – pim-sm hello advertisement interval	Sets the interval of transmitting the Hello packets.
hlo-intvl	<1-65535> - value for JP timer	The default interval of transmitting Hello packets is 30 seconds.
c-bsr	c-bsr –Candidate bootstrap router (candidate BSR)	
cbsr-intvl	<1-65535> - value for c-bsr timer	The default interval of self selecting packets is 60 seconds.
crp-adv	crp-adv – pim-sm C-RP-ADV interval	Sets the interval of transmitting the C-RP-Adv packets.
crp-intvl	<1-65535> - value for CRP timer	The default interval of transmitting Reinterface packets is 60 seconds.
spt-check	Spt-check – spt switch timer	
spt-intvl	<1-65535> - value for spt switch query timer	

Default value

See the above-mentioned table.

Command Mode

pim-sm global view

Instruction

If the holdtime of Join-prune packet is not set and the **Join** packets from the downstream neighbor have not been received in three JP timeout periods, the downstream that corresponds to the multicast entry will be shifted to the **prune** state. The default holdtime is 3 minutes. The interval in Interface configuration is prior to the **join/prune** interval in global mode.

Example

The following example sets the join/prune advertisement interval value to 30 for global pimsm configuration:

Router_config#Router pim-sm
Router_config_ps#timer join-prune 30

Related command

holdtime

4.1.33 holdtime

To set the interval of the timeout timer of PIM-SM, run the first one of the following two commands. To disable this feature, run the other command.

holdtime {join-prune *jp-hold* | assert *asrt-hold* | c-bsr *cbsr-hold* | **crp-adv *crp-hold* | sz *sz-hold*}**

no **holdtime {join-prune** [*jp-hold*] **| assert** [*asrt-hold*] **| c-bsr** [*cbsr-hold*] **| crp-adv** [*crp-hold*] **| *sz*** [*sz-hold*]**}**

Parameter

Name	Prompt	Remarks
holdtime	holdtime – hold timer for keep the status	
join-prune	Join-prune –join-prune status hold timer	

Name	Prompt	Remarks
jp-hold	<1-65535> - time value (second)	The default value is 210 seconds.
assert	assert – assert status hold timer	
asrt-hold	<7-65535> - time value (second)	The default value is 180 seconds.
c-bsr	c-bsr –Candidate bootstrap router (candidate BSR)	
cbsr-hold	<1-65535> - time value (second)	By default, it is as follows: holdtime timeout time= holdtime's interval*2+10 By default, the holdtime's interval is 60 seconds and the holdtime's timeout time is therefore 130 seconds.
c-rp	c-bsr –Candidate bootstrap router (candidate BSR)	
crp-hold	<1-65535> - time value (second)	The default value is 150 seconds. Because non-BSR updates its timeout time through the BSR's holdtime packets, the timeout time of C-RP must not be less than the interval of holdtime packet transmission. It is best when the former is 2.5
sz	sz –scope zone timer	intervals or beyond.
sz-hold	<10-4294967295> - time value (second)	The default value is 1300 seconds.

Default value

See the above-mentioned table.

Command Mode

pim-sm global view

Instruction

If the holdtime is set on a interface, first comes the configuration of this interface and then the global configuration; finally, if neither configuration is done, the default configuration will be chosen.

Note:

* When configuring the holdtime of C-RP, you should set the timeout time of C-RP to 2.5 holdtime transmission intervals or beyond to prevent the C-RP loss in the BSR holdtime packet.
* The timeout time of SZ must be longer than the BSR timeout time and you'd better set it to be 10 BSR timeout times.

Example

The following example shows how to set the holdtime of C-RP to 150 seconds, among which C-RP and C-BSR are not set on Ra.

Ra_config# router pim-sm
Ra_config_ps# holdtime c-rp 200

Related command

intvl-time

4.1.34 log

To enable the log switch to record DR's change, neighbor's up or down, address conflict and abnormal packets, run the first one of the following two commands:

log { nbr-change | ipaddr-conflict | pkt-conflict }
no **log *{ nbr-change* | *ipaddr-conflict* | pkt-*conflict }***

Parameter

Name	Prompt	Remarks
Log	log - To log conflict	
nbr-change	nbr-change – neighbor up/donw or DR changes	
ipaddr-conflict	ipaddr-conflict –secondary ip address is conflict with the another neighbor	

Name	Prompt	Remarks
pkt-conflict	pkt-conflict – pim-sm mroute items conflict in the pimsm pkt	

Default value

The log function is disabled.

Command Mode

pim-sm global view

Instruction

If there is the log server, the corresponding logs will be recorded to the log server.

Example

The following example configures the router to log the conflict when the exist secondary ip address is also contained in hello packet when receivd from another neighbor.

Router_config_ps# log nbr-change

Related command

None

4.1.35 show running-configure

To display the global PIM-SM information and the main configuration information about a interface, run the following command:

show running-configure

Parameter

None

Default value

None

Command Mode

EXEC

Instruction

According to the output information, you can check the configuration information about the current PIM-SM.

Example

4.1.36 show ip pim-sm bsr-router

Syntas

show ip pim-sm bsr

Parameter

Name	English Prompt	Remarks
pim-sm	pim-sm -- protocol independent multi-cast protocol sparse mode.	
bsr-router	Bsr-router -- display bootstrap (BSR) information	

Default

None

Command Mode

Management mode

Usage Guidelines

Display PIM-SM router BSR message.

Example

The following is a sample output of command "**show ip pim-sm bsr-router**":

```
Router #show ip pim-s bsr
PIMv2 BSR information:
I am BSR in sz 224.0.0.0/4
  CBSR-STM state (0-c,1-p,2-e):2.
  Address of BSR:       172.1.1.172
  BSR Priority:         64
  Hash Mask Length:     30
```

```
  Uptime: 05:18:00 BSR will
  expires in 00:00:13
Candidate-RP: 173.1.1.173(Loopback173)
  Interval of Advertisements: 60 seconds Next
  Advertisement will be sent in 00:00:07
```

Field Descriptions

Field	Description
sz	Range of current administer field
CBSR-STM state	Current local BSR state
Address of BSR	Current address of BSR
BSR Priority	Priority as configured in the **ip pim bsr-candidate** command.
Hash Mask Length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. This value is configured in the **ip pim bsr-candidate** command.
Uptime	Length of time that this router has been up (in hours, minutes, and seconds).
BSR will expires	BSR expire time
Candidate-RP	List of IP addresses of RPs.
Interval of Advertisements	Interval of C-RP-ADV advertisements
Next Advertisement	Timeout interval of next advertisement

Related Commands

None

4.1.37 show ip pim-sm interface

Shows information about the interfaces on which PIM is running.

Syntas

show ip pim-sm interface [**type** *number*]

Parameter

Name	English prompt	Description
pim-sm	pim-sm -- protocol independent multi-cast protocol sparse mode.	
interface	interface -- IP-PIM interfaces	

Name	English prompt	Description
Type number	See interfaces provided by CMD module.	(Optional) Interface type and number
count	count -- (Optional) Number of packets received and sent out the interface.	
Detail	Detail – (Optional) PIM details of each interface	

Default

None

Command Mode

Management mode

Usage Guidelines

Display PIM-SM router interface imformation.

Example

```
R142#show ip pim-sm interface
Address         Interface   Ver/   Nbr    Query   DR DR
                            Mode   Count  Intvl   Prior
192.168.21.142  Serial2/0   v2/S          30      1      192.168.21.144
192.168.100.142 Ethernet1/1 v2/S          30      100    192.168.100.142
192.166.100.142 Loopback0   v2/S          30      1      192.166.100.142
```

Related Commands

None

4.1.40 show ip pim-sm neighbor

Syntas

show ip pim-sm neighbor [**type** *number*]

Parameter

Name	English Prompt	Description
Pim-sm	Pim-sm -- protocol independent multi-cast protocol sparse mode.	
neighbor	neighbor – PIM-SM neighbor information	

Name	English Prompt	Description
Type number	See interfaces provided by CMD module.	(Optional) Interface type and number

Default

None

Command Mode

Management mode

Usage Guidelines

Display PIM-SM router neighbor information.

Example

The following is sample output from the **show ip pim-sm neighbor** command:

```
Router#show ip pim-s nei
PIM-SMv2 Neighbor Table
Neighbor        Interface           Uptime/Expires      DR
Address                                                 Prior
172.20.21.173   Ethernet2/1         00:00:08/00:01:37 1(DR)
```

Field description:

Field	Description
Nbr Addr	IP address of the PIM-SM neighbor.
Interface	Interface type and number on which the neighbor is reachable.
Uptime	How long (in hours, minutes, and seconds) the entry has been in the PIM neighbor table.
Expires	How long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.
(DR)	Indicates that this neighbor is a designated router on the LAN.

Related Commands

None

4.1.41 show ip pim-sm rp

Show revelant information about pim-sm local RP-SET dynamic rp.

show ip pim-sm rp [mapping [*rp-address***]| metric [***rp-address***]| all-set]**

Parameter

Name	Englisgh Prompt	Description
pim-sm	pim-sm -- protocol independent multi-cast protocol sparse mode.	
rp	rp – displays RP information	
mapping	mapping -- (Optional) Displays all group-to-RP mappings.	(Optional) Displays all group-to-RP mappings of which the router is aware (either configured or learned from Auto-RP).
metric	metric -- (Optional) Displays the unicast routing metric to the RPs.	(Optional) Displays the unicast routing metric to the RPs configured statically or learned via Auto-RP or the bootstrap router (BSR).
rp-address	*rp-address* -- (Optional) IP address of RP.	
All-set	*all-set -- Displays the whole rp set*	
<cr>	*<cr> -- Displays all (*,g) current rp status*	

Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The command is used to show revelant information about pim-sm local RP-SET dynamic rp.

Example

The following is sample output of the **show ip pim-sm rp** command:

```
Router# show ip pim-s rp
GROUP: 227.1.1.1
  RP: 173.1.1.173
  local c-rp

R173_config#show ip pim-s rp
GROUP: 227.1.1.1
  RP: 173.1.1.173
  Uptime/Expires: 06:21:49/00:02:06
```

The following is sample output of the **show ip pim-sm rp all** command:

```
Router# show ip pim-s rp all
sz range:224.0.0.0/4
```

```
RP-SET node:224.0.0.0/4
  c-rp:173.1.1.173(pri:10)
```

Field description:

Field	Description
sz range	Range of administer field
RP-SET node	RP-SET node
Group	Address of the multicast group about which to display RP information
RP	Address of the RP for that group
Local c-rp	Configure local c-rp
Uptime	Length of time the RP has been up (in days and hours). If less than 1 day, time is expressed in hours:minutes:seconds.
expires	Time in (hours, minutes, and seconds) in which the entry will expire.
Metric Pref	The preference value used for selecting the unicast routing metric to the RP announced by the designated forwarder (DF).
Metric	Unicast routing metric to the RP announced by the DF.
Flags	Indicates the flags set for the specified RP. The following are descriptions of possible flags: C—RP is configured. L—RP learned via Auto-RP or the BSR.
RPF Type	Routing table from which this route was obtained, either unicast, Distance Vector Multicast Routing Protocol (DVMRP), or static mroute.
Interface	Interface type and number that is configured to run PIM-SM.

4.1.42 show ip pim-sm rp-hash

To display which rendezvous point (RP) is being selected for a specified group, use the show ip pim rp-hash command in EXEC mode.

show ip pim rp-hash {group-address | group-name} **show ip pim-sm rp-hash** *gaddr* [gmask]

Parameter

Name	English Prompt	Remarks
pim-sm	pim-sm -- protocol independent multi-cast protocol sparse mode.	
rp-hash	rp-hash – RP according to the hash	

Name	English Prompt	Remarks
gaddr	*A.B.C.D* -- Displays the RP information for the specified group address	
gmask	*A.B.C.D* -- Displays the RP information for the specified group mask	

Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

This command displays which RP was selected for the group specified. It also shows whether this RP was selected by Auto-RP or the PIM version 2 bootstrap mechanism.

Example

The following is sample output from the show ip pim rp-hash command with the group address 239.1.1.1 specified:

```
Router#show ip pim-sm rp-hash 239.1.1.1
  RP: 173.1.1.173 for 239.1.1.1/0, v2
    Info Source: 173.1.1.173, pri 10, holdtime
  150 PIMv2 Hash Value:
    RP 173.1.1.173, via local BSR, pri 10, hash value 1268904765
```

Field description:

Field	Description
RP: 173.1.1.173	Address of the RP for the group specified (239.1.1.1)
Info source: 173.1.1.173	Indicates from which system the router learned this RP information
holdtime	RP holdtime
via local BSR	Local BSR
pri	Corresponding rp priority.
hash value	hash value

4.1.43 show ip pim-sm anycast-rp

To show information of anycast-rp, run the following command:

show ip rip database

Parameter

Name	English Prompt	Remarks
Pim-sm	Pim-sm -- protocol independent multi-cast protocol sparse mode.	
Anycast-rp	anycast-rp –*anycast rp information*	

Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The command is used to output information about the status of local anycast-rp receiving and forwarding register packets.

Example

The following is a sample output of command "**show ip pim-sm anycast-rp**".

```
Router# show ip pim-sm anycast-rp
anycast-rp 2.2.2.2 nbr 192.168.18.1 status: REG_SEND
```

Field description

Field	Description
anycast-rp	anycast-rp address: 2.2.2.2
nbr	Neighbor address: 192.168.18.1
status: REG_SEND	It means forwards register packets to the neighbor.

4.1.44 show ip pim-sm protocol

To show information about pimsm protocol,run the following command:

show ip pim-sm protocol

Parameter

Name	English Prompt	Remarks
pim-sm	Pim-sm -- protocol independent multi-cast protocol sparse mode.	
protocol	protocol –*iminterfaceant info for pimsm protocol*	

Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The command is used to output information about pimsm protocol's activated state, number of interfaces, neighbors and packets and BSM keeptime.

Example

An example from output of command "show ip pim-sm protocol":

```
Router# show ip pim-sm protocol
PIM-SM is active
pim-sm interface number:3
pim-sm neighbor number:1
pim-sm receive pkt num:133; bad pkt
num:0 PIM-SM current glb jp_intvl: 60(s)
PIM-SM current glb hello intvl: 30(s)
PIM-SM current glb BSM update timer intvl:
60(s) PIM-SM current glb crp_intvl: 60(s)
PIM-SM current glb spt_intvl: 2(s)
PIM-SM BSM hold timeout: 130(s)
```

4.1.45 show ip mroute pim-sm

To show pimsm route information, run the following command:

show ip mroute pim-sm [*gaddr* |*saddr***][***detail***][***summary***]**

Parameter

Name	English Prompt	Remarks
mroute	Mroute – IP Multicast routing table.	
pim-sm	pim-sm -- protocol independent multi-cast protocol sparse mode.	
gaddr	*A.B.C.D -- Group address*	
saddr	*A.B.C.D -- Source address*	
detail	*detail -- show pimsm inner database*	
summary	summary – Displays a abbreviated summary of PIM-SM entries.	

Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

None

Example

1.Show pim-sm route information

```
router# show ip mroute pim-sm 227.1.1.1
IP PIM-SM Multicast Routing Table:

(*, 227.1.1.1) RP:173.1.1.173 creat time:3d02h00m *G
  Upstream interface: Null0, rpf' nbr: 0.0.0.0
  ps imm_olist list:
    Ethernet2/1,
    Loopback174,
```

2. Show pim-sm route summary

```
information show ip mroute pim-s sum
IP PIM-SM Multicast Routing Table summary:
number of (* * RP) entry: 0
number of (* G) entry: 2
number of (s, g) spt entry: 0
number of (s, g) rpt entry: 0

(*, 237.1.1.1)        RP:175.1.1.173       creat time:00:29:44  *G
  Upstream interface: Null0, rpf' nbr: 0.0.0.0
  ps imm_olist list:
    FastEthernet0/1,

(*, 239.255.255.250)  RP:175.1.1.173       creat time:00:29:29 *G
  Upstream interface: Null0, rpf' nbr: 0.0.0.0
  ps imm_olist list:
    FastEthernet0/0,
```

Field description

Field	Description
Upstream interface	Number of upstream interface
ps imm_olist	interfaces of pimsm route items
rpf' nbr	Upstream RPF neighbor
creat time	Keep time from created to now.

4.1.46 show ip rpf pim-sm

To show the reverse path of pimsm corresponding multicast source address:

show ip rpf pim-sm {*source-address* } [metric]

Parameter

Name	English Prompt	Remarks
pim-sm	Pim-sm -- protocol independent multi-cast protocol sparse mode.	
source-address	*source-address* – source address	
metric	metric – Displays the unicast routing metric.	

Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The command is used to output information about the reverse path of multicast source address.

Example

A sample output of command "**show ip rpf pim-sm**":

```
Router#show ip rpf pim-sm 172.1.1.1
PIM-SM: show ip rpf pim-sm 172.1.1.1
PIM-SM RPF information for 172.1.1.1 :
  RPF_interface:       FastEthernet0/1
  RPF_neighbor:        172.20.21.172
  RPF route/mask(type): 172.1.1.0/24(rip)
```

A sample output of command "**show ip rpf pim-sm**"with keyword "metric":

```
Router#show ip rpf pim-sm 172.1.1.1 metric
PIM-SM: show ip rpf pim-sm 172.1.1.1 metric
PIM-SM RPF information for 172.1.1.1 :
  RPF_interface: FastEthernet0/1
 RPF_neighbor: 172.20.21.172 RPF
 route/mask(type): 172.1.1.0/24(rip)
 Metric preference: 120
 Metric: 1
```

Field description:

Field	Description
RPF information for source address	Multicast source address
RPF interface	Specified RPF interface

RPF neighbor	Specified multicast source data from the neighbor
RPF route/mask	RPF route
RPF type	RPF type (for instance, unicast, DVMRP route and static multicast route)
Metric preference	Metric preference
Metric	Metric

4.1.47 debug ip pim-sm alert

To display the alert information from mrouting or IP, run the first one of the following two commands.

debug ip pim-sm alert

no debug ip pim-sm alert

Parameter

None

Default value

None

Command Mode

EXEC

Instruction

VTY will be exinterfaceed if the alart information from mrouting or aged (s,g).

Example

The following example shows that the route event of RIP is monitored.

router# debug ip rip database

RIP-DB: Adding summary route 192.1.1.0/24 <metric 0> to RIP database

The fields in the previous example are explained in the following table:

Domain	Description
summary	Route type which is added to the routing table
192.1.1.0/24	Route which is added to the routing table
<metric 0>	Value of the route's metric

4.1.48 debug ip pim-sm assert

To monitor the Assert event of PIM-SM, run the first one of the following two commands:

debug ip pim-sm assert [packet | state- machine | A.B.C.D **] no**

debug ip pim-sm assert [packet | state- machine | A.B.C.D **]**

Parameter

Name	Prompt	Remarks
state- machine	Show state machine activity debug information	
packet	Trace information about packet	
A.B.C.D	Group address for stm and packet output	

Default value

None

Command Mode

EXEC

Instruction

According to the output information, you can check the current assert event of PIM-SM.

Result

- Show (S,G) Assert State-machine Actions
- Show (*,G) Assert Message State Machine actions
- Show activity after timer timerout
- Show packet activity

4.1.49 debug ip pim-sm bsr

To monitor the BSM event of PIM-SM, the C-RP-ADV event or the BSR state machine, run the first one of the following two commands:

debug ip pim-sm assert [packet | state- machine**]**

no debug ip pim-sm assert [packet | state- machine**]**

Parameter

Name	Prompt	Remarks
state- machine	Show state machine activity debug information	
packet	Trace information about packet	

Default value

None

Command Mode

EXEC

Instruction

According to the output information, you can check the BSM event of PIM-SM, the C-RP-ADV event or the BSR state machine.

Example

4.1.50 debug ip pim-sm rp

To monitor the related events and packets about PIM-SM-RP-SET change, run the first one of the following two commands:

debug ip pim-sm rp

no debug ip pim-sm rp

Parameter

None

Default value

None

Command Mode

EXEC

Instruction

This command is used to exinterface the reception and transmission of C-RP-ADV and the RP-SET change. As to the change of static RP, no debugging information will be exinterfaceed at present.

Example

4.1.51 debug ip pim-sm entry

To exinterface the creation and update of (*,*,rp), (*,g), (s,g,rpt) and (s,g,spt) and their simultaneous change of them at the time of RP change, run the first one of the following two commands.

debug ip pim-sm entry

no debug ip pim-sm entry

Parameter

None

Default value

None

Command Mode

EXEC

Instruction

According to the output information, you can browse the information about PIMSM creation and update of multicast routing entries.

Example

4.1.52 debug ip pim-sm event

To exinterface all events that PIMSM main task receives, run the first one of the following two commands.

debug ip pim-sm event

no debug ip pim-sm event

Parameter

None

Default value

None

Command Mode

EXEC

Instruction

According to the output information, you can browse all events of current PIMSM.

Example

4.1.53 debug ip pim-sm hello

To display the Hello packet received or transmitted by PIM-SM for debugging the neighbor's information, run the first one of the following two commands.

debug ip pim-sm hello

no debug ip pim-sm hello

Parameter

Name	Prompt	Remarks
pim-sm	Show state machine activity debug information	
hello	Show information about packet sending and receiving	

Default value

None

Command Mode

EXEC

Instruction

According to the output information, you can browse the Hello packets, including those received or transmitted by PIM-SM, to know what's going on the local machine or the neighbors.

Results

- The interfaces, source addresses and genid of the currently received or transmitted Hello packets can be displayed.

Example

4.1.54 debug ip pim-sm jp

To trace the Join/Prune event of (*,g) or (s,g), run the first one of the following two commands.

debug ip pim-sm jp [packet | state- machine | A.B.C.D **]**

no debug ip pim-sm jp [packet | state- machine | A.B.C.D **]**

Parameter

Name	Prompt	Remarks
state- machine	Show state machine activity debug information	
packet	Trace information about packet	
A.B.C.D	Group address for stm and packet output	

Default value

None

Command Mode

EXEC

Instruction

Example

4.1.55 debug ip pim-sm nbr

To trace the related events of a neighbor, such as the addition of neighbor, aging deletion or DR selection, run the first one of the following two 1` commands.

debug ip pim-sm nbr

no debug ip pim-sm nbr

Parameter

None

Default value

None

Command Mode

EXEC

Instruction

According to the output information of this command, you can browse neighbor change, neighbor refreshment, GENID change and DR selection.

Example

4.1.56 debug ip pim-sm packet

To trace the protocol control packets received or transmitted by PIM-SM, run the following command.

debug ip pim-sm packet

Parameter

None

Default value

None

Command Mode

EXEC

Instruction

After this command is run, the PIM-SM packet's type will be displayed.

Example

4.1.57 debug ip pim-sm register

To display the registration packet and register state event of PIM-SM, run the first one of the following two commands.

debug ip pim-sm register [packet | state- machine | A.B.C.D **]**

no debug ip pim-sm register [packet | state- machine | A.B.C.D **]**

Parameter

Name	Prompt	Remarks
state- machine	Show state machine activity debug information	
packet	Trace information about packet	
A.B.C.D	Group address for stm and packet output	

Default value

None

Command Mode

EXEC

Instruction

According to the output information, you can check the register event of PIM-SM.

Example

4.1.58 debug ip pim-sm timer

To display the change of all PIM-SM timers, including creation, deletion, stop and timeout, run the first one of the following two commands.

debug ip pim-sm timer

no debug ip pim-sm timer

Parameter

None

Default value

None

Command Mode

EXEC

Instruction

The PIM-SM timers include the Hello timer, the neighbor timeout timer, the Join/Prune timer, the override timer, the prune pending timer, the keepalive timer, the assert timer, the register timer, the register limit timer, the BSM timer, and so on.

Example

None

Chapter 5 DVMRP Configuration Commands

5.1.1 clear ip dvmrp neighbor

To clear dvmrp neighbor, run the following command in EXEC mode: **clear ip dvmrp neighbor** [*ip-address* | **interface-type** *interface-number*]

Parameter

Parameter	Description
ip-address	(optional) DVMRP neighbor address
interface-type/ *interface-number*	(optional) interface type and interface number. This parameter enables all neighbors on the interface to reset.

Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The command is used to clear the neighbor of specified interface or address.

Example

The following example shows how to clear all neighbors on E1/1.

```
clear ip dvmrp neighbor E1/1
```

Related commands

show ip dvmrp neighbor

5.1.2 clear ip dvmrp route

To clear specified unicast route,run the following command in EXEC mode: **clear ip dvmrp route** [*network-address* [*network-mask*]]

Parameter

Parameter	Description
network-address	(optional) unicast route network address
network-mask	(optional) unicast route network mask

Default

The network mask is the natural one by default.

Command Mode

EXEC

Usage Guidelines

The command is used to clear specified unicast route.The network mask is the natural one when the network mask is not specified. Note: The command is not available to direct route.

Example

The following example shows how to delete unicast route 192.168.20.0/24.

clear ip dvmrp route 192.168.20.0

Related Commands

show ip dvmrp route

5.1.3 clear ip mroute dvmrp

To delete specified multicast route,run the following command in EXEC mode: **clear ip mroute dvmrp** {***** | *source-address* [*group-address*] }

Parameter

Parameter	Description
*	Delete all multicast routes.
source-address	The source address of the multicast route.
group-address	(optional) group address of the multicast route

Default

You don't need to input the group address by default. Delete all multicast routes of specified multicast source.

Command Mode

EXEC

Usage Guidelines

The command can be used to delete specified multicast routes. Delete all multicast routes of specified multicast source when the group address is not specified.

Example

The following example shows how to delete the multicast route (192.168.20.141, 224.0.0.10).

clear ip mroute dvmrp 192.168.20.141 224.0.0.10

Related Commands

show ip mroute dvmrp

5.1.4 debug ip dvmrp mroute

To trace information about DVMRP creation and deletion, run the following command in EXEC mode. To disable this feature, use the no form of this command. **debug ip dvmrp mroute**
no debug ip dvmrp mroute

Parameter

None

Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The command is used to find network faults.

Example

The following example shows how to trace information about tracing multicast route.

debug ip dvmrp mroute

Output information
Example：

DVMRP: create a mroute(192.168.20.141,224.1.1.10) with 192.168.20.0/24
DVMRP: add downstream interface Ethernet1/1 for (192.168.20.141, 224.1.1.10)
DVMRP: delete downstream interface Ethernet1/1 for (192.168.20.141, 224.1.1.10)
DVMRP: resend prune for (192.168.20.141, 224.1.1.10) with lifetime 7200
DVMRP: downstream neighbor 200.1.1.143 changes to prune state for (192.168.20.141, 224.1.1.10) with lifetime 100
DVMRP: received prune from 200.1.1.143 for (192.168.20.141, 224.1.1.10) with lifetime 100
DVMRP: create a mroute(192.169.1.220,225.1.1.70) with none unicast route
DVMRP: delete (192.169.1.220, 225.1.1.70) for mroute expired

Related Commands

show ip mroute dvmrp

5.1.5 debug ip dvmrp neighbor

To trace DVMRP maintenance information,run the following command in EXEC mode.To disable this feature, use the no form of this command.
debug ip dvmrp neighbor no
debug ip dvmrp neighbor

Parameter

None

Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The command is used to find network faults.

Example

The following example shows how to trace DVMRP maintenance information.

debug ip dvmrp neighbor

Output information

Example

```
DVMRP:    delete    neighbor    200.1.1.143      for    manually    cleared
DVMRP:    delete    neighbor    202.117.93.144   for    manually    cleared
DVMRP:    add       neighbor    200.1.1.143      for    new         adjacency
DVMRP:    add       neighbor    202.117.93.144   for    new         adjacency
DVMRP: add neighbor 192.168.20.148 for new adjacency
```

Related Commands

show ip mroute neighbor

5.1.6 debug ip dvmrp route

To trace DVMRP unicast route information,run the following command in EXEC mode. To disable this feature, use the no form of this command.

debug ip dvmrp route no

debug ip dvmrp route

Parameter

None

Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The command is used to find network faults.

Example

The following example shows how to trace DVMRP unicast route information.

debug ip dvmrp route

Output information

Example：

```
DVMRP:  depend  metric[34/34]  for  192.168.20.0/24  from  200.1.1.143
DVMRP:  infinite  metric[32/32]  for  200.1.1.0/24  from  200.1.1.143
DVMRP:  depend  metric[34/34]  for  202.117.93.0/24  from  200.1.1.143
DVMRP:  DF  wins  with  172.168.0.0/16  in  Serial1/0  for  202.117.93.142
DVMRP:  DF  wins  with  172.168.0.0/16  in  Ethernet2/1  for  192.168.20.142
DVMRP:  add  entry  172.168.0.0/16
DVMRP:  send  flash  reinterface  packet
DVMRP: delete entry 10.1.1.0/24
```

Field description

finite/infinite/depend metric:	finite(<32)/infinite(=32)/depend（>32 and <64）
[34/34]:	Local cost/ neighbor reinterface cost of the route
DF wins:	The system acquires the access of designating and forwarding the route.
DF loses:	The system loses the access of designating and forwarding the route (The result is the route in this interface has no dependent neighbor in the downstream.)

Related Commands

show ip mroute route

5.1.7 debug ip dvmrp packet

To trace the information of receiving and forwarding DVMRP packets,run the first one of the following two commands in EXEC mode:

debug ip dvmrp packet [**graft** | **graft-ack** | **reinterface** | **probe** | **prune**] **no debug ip dvmrp packet** [**graft** | **graft-ack** | **reinterface** | **probe** | **prune**]

Parameter

Parameter	Parameter
graft	(optional) trace graft packets
graft-ack	(optional) trace graft-ack packets
reinterface	(optional) trace unicast route update packets
probe	(optional) trace probe packets
prune	(optional) trace prune packets

Default

No default behavior or values.

Command Mode

EXEC

Usage Guidelines

The command is used to find network faults.

Example

The following example shows how to trace the information of receiving and forwarding DVMRP packets.

debug ip dvmrp packet

Output information Example：

DVMRP:sendprobepacketto 224.0.0.4 with length 24 in Ethernet2/1
DVMRP:sendprobepacketto 224.0.0.4 withlength16 inEthernet1/1
DVMRP: receive probe packet from 192.168.20.144 with length 24 in Ethernet2/1
DVMRP: receive probe packet from 200.1.1.143 with length 16 in Ethernet1/1
DVMRP: receive probe packet from 202.117.93.144 with length 16 in Serial1/0
DVMRP: send probe packet to 224.0.0.4 with length 16 in Serial1/0
DVMRP:sendprobepacketto 224.0.0.4 with length 24 in Ethernet2/1
DVMRP: receive probe packet from 192.168.20.148 with length 24 in Ethernet2/1
DVMRP: send probe packet to 224.0.0.4 with length 16 in Ethernet1/1
DVMRP: receive reinterface packet from 192.168.20.144 with length 37 in Ethernet2/1 DVMRP: receive probe packet from 192.168.20.144 with length 24 in Ethernet2/1

Related Commands

show ip mroute route

5.1.8 ip dvmrp

To run DVMRP on the interface, use the following command. To disable this feature, use the no form of this command.

ip dvmrp no
ip dvmrp

Parameter

None

Default

No default behavior or values.

Command Mode

Interface Configuration

Usage Guidelines

The command can be used to activate or disable DVMRP on the interface. Similar to PIM-SM and PIM-DM, the system will enable DVMRP once one interface activates DVMRP.

Following prompts will pop up if “ip multicast-routing”is not configured before configuring the command.

WARNING: "ip multicast-routing" is not configured, IP Multicast packets will not be forwarded"

But DVMRP process can be enabled normally (except multicast learning is unavailable).

Once the function is enabled, the interface will not run DVMRP, but other configurations of DVMRP will not be influenced. All DVMRP configurations remain effective when the interface run DVMRP again.

Example

The following example shows how to activate DVMRP on the interface E1/1.

```
R142_config_e1/1# ip dvmrp
```

Related Commands

show ip dvmrp interface

5.1.9 ip dvmrp advert-metric

To configure advert-metric offset, run the following command. To disable this feature, use the no form of this command.

ip dvmrp advert-metric offset [**access-list** *acl-name*] **no**
ip dvmrp advert-metric offset [**access-list** *acl-name*]

Parameter

Parameter	Description
offset	Offset cost
access-list	(optional) access-list cost
acl-name	(optional) acl-name

Default

There is no the default value of the interface cost by default.

Command Mode

Interface Configuration

Usage Guidelines

The command is used to configure multiple access lists. The default value of the interface cost should be the first “permit”in accordance with the configuration sequence of the access list. For non-configured route, the default value of the interface should be in accordance with “ip dvmrp advert-metric offset”. Refer to the example.

The command is only applied to standard access list. Configure expansion access list equivals to configure"permit all" standard access lists.

Example

The following example shows how to add a value of the interface cost to the route forwarded from the interface E2/1. Suppose interface E2/1 forwards three routes: 192.168.20.0/24, 192.168.30.0/24 and 192.167.20.0/24.
Though 192.168.20.0/24 meets the criteria of the second access list "per16", “per24”is configured before it, the value of the interface cost is 4.
As 192.168.30.0/24 only meets the criteria of the second access list “per16”, the value of the interface cost is 3.
As 192.167.20.0/24 does not meet the criteria of any acess list, the value of the interface cost belongs to unconfigured acess list, that is 2.

Example

```
!
interface Ethernet2/1
ip address 192.167.20.142 255.255.255.0
ip dvmrp
ip dvmrp advert-metric 2
ip dvmrp adver-metric 4 access-list per24
ip dvmrp adver-metric 3 access-list per16
!
ip access-list standard per24
permit 192.168.20.0 255.255.255.0
!
ip access-list standard per16
permit 192.168.0.0 255.255.0.0
!
```

Related Commands

show ip dvmrp route

5.1.10 ip dvmrp auto-summary

To configure DVMRP summarization automatically, run the following command. To disable this feature, use the no form of this command:

ip dvmrp auto-summary no
ip dvmrp auto-summary

Parameter

None

Default

By default, the software performs some level of DVMRP summarization automatically.

Command Mode

Interface Configuration

Usage Guidelines

The automatic summarization and the manual summarization are not interplayed. The summary route will not occur in the routing table here.

If two interfaces of the router have constituted route loop with other routers, it is recommended to configure or cancel the auto-summary of the two interfaces simultaneously.

Example

The following example shows how to cancel the automatic summarization on interface E2/1:

```
R142_config_e2/1# no ip dvmrp auto-summary
```

Related Commands

ip dvmrp summary-address

5.1.11 ip dvmrp default-information

To configure interface defaut route, run the following command. To disable this feature, use the no form of this command:
ip dvmrp default-information no
ip dvmrp default-information

Parameter

None

Default

The default route is not forwarded by default.

Command Mode

Interface Configuration

Usage Guidelines

The default route occurs in the DVMRP routing table in spite of default route'configuration.
If two interfaces of the router have constituted route loop with other routers, it is recommended to configure or cancel the auto-summary of the two interfaces simultaneously.

Example

The following example shows how to configure default routing function on interface E2/1:

```
R142_config_e2/1# ip dvmrp default-information
```

Related Commands

show ip dvmrp route

5.1.12 ip dvmrp force-leaf

To configure DVMRP mandatory leaf node, run the following command. To disable this feature, use the no form of this command.
ip dvmrp force-leaf no
ip dvmrp force-leaf

Parameter

None

Default

There is no mandatory leaf node by default.

Command Mode

Interface Configuration

Usage Guidelines

The command is used to isolate the information interaction of two physically connected routers.

Example

The following example shows how to configure the mandatory leaf node on interface E2/1:

```
R142_config_e2/1# ip dvmrp force-leaf
```

Related Commands

show ip dvmrp neighbor

5.1.13 ip dvmrp metric

To configure which sources are advertised and which metrics, run the following command in Interface configuration.To disable this feature, use the no form of this command.

ip dvmrp metric offset [**access-list** *acl-name*] **no**
ip dvmrp metric offset [**access-list** *acl-name*]

Parameter

Parameter	Description
offset	Offset cost
access-list	Access-list cost
acl-name	(optional) acl-name

Default

The meric offset is one by default.

Command Mode

Interface Configuration

Usage Guidelines

The command is used to configure multiple access lists. The default value of the interface cost should be the first “permit”in accordance with the configuration sequence of the access list. For non-configured route, the default value of the interface should be in accordance with “ip dvmrp advert-metric offset”. Refer to the example.

The command is only applied to standard access list. Configure expansion access list equivals to configure"permit all" standard access lists.

Example

The following example shows how to add a value of the interface cost to the route forwarded from the interface E2/1. Suppose interface E2/1 forwards three routes: 192.168.20.0/24, 192.168.30.0/24 and 192.167.20.0/24.

Though 192.168.20.0/24 meets the criteria of the second access list "per16", “per24”is configured before it, the value of the interface cost is 4.

As 192.168.30.0/24 only meets the criteria of the second access list “per16”, the value of the interface cost is 3.

As 192.167.20.0/24 does not meet the criteria of any acess list, the value of the interface cost belongs to unconfigured acess list, that is 1.

Example

```
!
interface                                                    Ethernet2/1
ip              address                 192.167.20.142       255.255.255.0
ip                                                           dvmrp
ip      dvmrp           metric          4       access-list  per24
ip      dvmrp           metric          3       access-list  per16
!
ip              access-list                     standard     per24
permit                          192.168.20.0                 255.255.255.0
!
ip              access-list                     standard     per16
permit                          192.168.0.0                  255.255.0.0
!
```

Related Commands

show ip dvmrp route

5.1.14 ip dvmrp prune-lifetime

To configure the maximum default lifetime of prunes in seconds, run the following command. To disable this feature, use the no form of this command.

ip dvmrp prune-lifetime *lifetime*

no ip dvmrp prune-lifetime [*lifetime*]

Parameter

Parameter	Description
lifetime	prune-lifetime

Default

If ip dvmrp prune-lifetime is not specified, it is the same as if the user had specified the following for neighbors that support Generation ID:
The prune lifetime is 7200 seconds by default if there is no downstream prune. Otherwise, the prune lifetime is the minimum of all received prune time.

Command Mode

Interface Configuration

Usage Guidelines

The ip dvmrp prune-lifetime command configures the maximum value to be placed into a prune message.The actual lifetime value is the minimum of all the downstream prunes for the source and a randomized value that falls between one-half the prune lifetime and the prune lifetime. The value is in seconds.
The negative form of this command, no dvmrp prune-lifetime, removes the configured time-seconds value and returns this to its default value of 7200 seconds for neighbors that support Generation ID.

Example

The following example shows how to configure the prune-lifetime to 1000 seconds forwarded from interface E2/1:

```
R142_config_e2/1# ip dvmrp prune-lifetime 1000
```

Related Commands

show ip mroute dvmrp

5.1.15 ip dvmrp route-filter

To configure interface receiving and forwarding route, run the following command. To disable this feature, use the no form of this command.
ip dvmrp route-filter { **in** | **out** } *acl-name* **no**
ip dvmrp route-filter { **in** | **out** } *acl-name*

Parameter

Parameter	Description
in	Fiters the receving route from the interface
out	Filters the forwarding route from the interface.
acl-name	Acl-name

Default

None

Command Mode

Interface Configuration

Usage Guidelines

The command enables every interface to configure only one filter for forwarding and receiving packets. The command is only applied to standard access list. Configure expansion access list equivals to configure"permit all" standard access lists.

Example

The following example shows how to deny the range of access list from interface E2/1:

Example

```
!
interface                                                    Ethernet2/1
ip          address          192.167.20.142          255.255.255.0
ip                                                              dvmrp
ip          dvmrp          route-filter          in          per24
!
ip          access-list                standard                per24
permit                192.168.20.0                255.255.255.0
!
```

Related Commands

show ip dvmrp route

5.1.16 ip dvmrp summary-address

To configure DVMRP summary address, run the following command. To disable this feature, use the no form of this command:
ip dvmrp summary-address *network-address mask-address*
no ip dvmrp auto-summary *network-address mask-address*

Parameter

Parameter	Description
network-address	Manual summary network number
mask-address	Manual summary network submask

Default

None

Command Mode

Interface Configuration

Usage Guidelines

The automatic summarization and the manual summarization are not interplayed. The summary route will not occur in the routing table here.
If two interfaces of the router have constituted route loop with other routers, it is recommended to configure or cancel the auto-summary of the two interfaces simultaneously.

Example

The following example shows how to configure maual summary 192.168.0.0/16 on interface E2/1:

```
R142_config_e2/1# ip dvmrp summary-address 192.168.0.0 255.255.0.0
```

Related Commands

ip dvmrp auto-summary

5.1.17 show ip dvmrp interface

To show specified interface information, run the following command:
show ip dvmrp interface [**interface-type** *interface-number*]

Parameter

Parameter	Description
interface-type	(optional) interface type
interface-number	(optional) interface number

Default

None

Command Mode

Other modes except the user mode

Usage Guidelines

The command is only used to configure DVMRP interface. All DVMRP interface information will be displayed if there is no specified interface.

Example

The following example shows how to display DVMRP all interface information:

```
R142_config#show ip dvmrp interface
DVMRP interface information
 Address        interface       flags   neighbors  200.1.1.142   Ethernet1/1          0x0000   1  202.117.
93.142  Serial1/0       0x0000   1     192.168.20.142  Ethernet2/1      0x0000       4
```

Related Commands

ip dvmrp

5.1.18 show ip dvmrp neighbor

To show specified interface neighbor information, run the following command: **show ip dvmrp neighbor** [**interface-type** *interface-number*]

Parameter

Parameter	Description
interface-type	(optional) interface type
interface-number	(optional) interface number

Default

None

Command Mode

Other modes except the user mode.

Usage Guidelines

The command is used to show DVMRP neighbor information of all specified interfaces.

Example

The following example shows DVMRP all neighbor information.

```
R142_config#show ip dvmrp neighbor
DVMRP neighbor information
 Address       interface       flags  version  hold/Expire time
 200.1.1.143   Ethernet1/1   0x010F    3.255 1d16h21m/00:00:31
 202.117.93.144 Serial1/0    0x010F    3.255 1d16h04m/00:00:27
 192.168.20.144 Ethernet2/1   0x010F    3.255  23:42:04/00:00:33
 192.168.20.148 Ethernet2/1   0x010E    3.255  23:41:57/00:00:34
 192.168.20.204 Ethernet2/1   0x040A    12.3    23:41:09/00:02:14
 192.168.20.156 Ethernet2/1   0x040A    12.3    18:31:14/00:01:29
```

Flags field description:

Field	Bit	Description
flags	0x0001	The neighbor supports leaf node
	0x0002	The neighbor supports prune packets
	0x0004	The neighbor probe packets include GenID field
	0x0008	The neighbor supports mtrace
	0x0010	The neighbor supports SNMP
	0x0020	The neighbor prune packet , graft packet and graft ack packet support network submask
	0x0100	The neighbor supports bi-drectional link
	0x0200	Receives the neighbor probe packets, but the bidirectional link is not established

	0x0400	Indicates the neighbor is the router

Related Commands

ip dvmrp
show ip dvmrp interface
debug ip dvmrp neighbor

5.1.19 show ip dvmrp route

To show specified route information, run the following command:
show ip dvmrp route [*network-address* [*network-mask*]]

Parameter

Parameter	Description
network-address	(optional) route network address
network-mask	(optional) rpite network mask

Default

None

Command Mode

Other modes except the user mode

Usage Guidelines

The command is used to show DVMRP specified route information. The network mask is the natural mask by default if the network address is configured but the network mask is not.

Example

Example
1. Show all route information:

```
R142_config_e2/1#show ip dvmrp route
  DVMRP topology information
H  10.1.1.0/24, from 202.117.93.144(Serial1/0) with metric
     3 Create Time 00:01:03, Expire Time 00:02:17
     Downstream interface:
       DF Ethernet1/1, 1 neighbors
          Ethernet2/1, 0 neighbors, DF neighbor 192.168.20.204, DF metric 1
   172.168.0.0/16, from 200.1.1.143(Ethernet1/1) with metric 11
     Create Time 1d16h57m, Expire Time
     00:02:11 Downstream interface:
       DF Serial1/0, 0 neighbors DF
       Ethernet2/1, 4 neighbors
   172.168.30.0/24, from 202.117.93.144(Serial1/0) with metric
     3 Create Time 00:01:03, Expire Time 00:02:17
     Downstream interface:
       DF Ethernet1/1, 0 neighbors
          Ethernet2/1, 0 neighbors, DF neighbor 192.168.20.148, DF metric 1
```

```
192.168.20.0/24, from Local(Ethernet2/1) with metric 1
  Create Time 1d00h18m
  Downstream interface:
    DF Ethernet1/1, 1 neighbors
    DF Serial1/0, 0 neighbors
```

Field description:

Identifier	Description
H	The route is in Hold-Down state or the route is in normal state.
DF	The route has specified forwarding function on the interface or the route has no specified forwarding function.

Example

2. Show specified route information (172.168.30.0/24)

```
R142_config_e2/1#show ip dvmrp route 172.168.30.0
 255.255.255.0 DVMRP topology information
  172.168.30.0/24, from 202.117.93.144(Serial1/0) with metric
    3 Create Time 00:07:28, Expire Time 00:01:52
    Downstream interface:
      DF Ethernet1/1, 0 neighbors
        Ethernet2/1, 0 neighbors, DF neighbor 192.168.20.148, DF metric 1
```

Related Commands

show ip dvmrp neighbor
show ip mroute dvmrp
debug ip dvmrp route

5.1.20 show ip mroute dvmrp

To show mroute dvmrp information:
show ip mroute dvmrp [**interface-type** *interface-number*| *source-address* [*group-address*]]

Parameter

Parameter	Description
interface-type	(optional) interface type
interface-number	(optional) interface number
source-address	(optional) multicast route source address
group-address	(optional) multicast route group address

Default

None

Command Mode

Other modes except the user mode

Usage Guidelines

The command is used to show DVMRP specified multicast routing information.

Example

Example

3. Show all multicast routing information.

```
R142_config_e2/1#show ip mroute dvmrp
IP Multicast Routing Table
(192.168.20.2, 224.1.1.10), 1d00h34m/00:00:00
  Incoming interface: Ethernet2/1, RPF nbr 192.168.20.142
  Outgoing interface list: Null
(192.169.1.220, 225.1.1.70), 00:00:30/00:00:00
  Incoming interface: Ethernet2/1, RPF nbr 192.168.20.142
  Outgoing interface list: Null
(192.168.20.141, 239.255.255.250), 21:14:00/00:00:00
  Incoming interface: Ethernet2/1, RPF nbr 192.168.20.142
  Outgoing interface list:
    Ethernet1/1, Forward/DVMRP, 19:45:51/00:00:00
```

Example

2 Show specified multicast routing information (192.168.20.2, 224.1.1.10).

```
R142_config_e2/1#show ip mroute dvmrp 192.168.20.2
IP Multicast Routing Table
(192.168.20.2, 224.1.1.10), 1d00h36m/00:00:00, Owner,
  Prune Incoming interface: Ethernet2/1, RPF nbr
  192.168.20.142 relate route: 192.168.20.0/24, 2/2
  downstream interfaces Outgoing interface list:
   Ethernet1/1, 1/1 neighbors, Prune
   Serial1/0, 0/0 neighbors, Prune
```

Related Commands

show ip dvmrp neighbor
debug ip dvmrp mroute
debug ip dvmrp route

5.1.21 show ip rpf dvmrp

To show how multicast route reverse forwards the path,run the following command: **show ip rpf dvmrp** *source-address*

Parameter

Parameter	Description
source-address	Show specified RFP information of source address.

Default

None

Command Mode

Other modes except the user mode

Usage Guidelines

The command is used to inform the reverse path forwarding information to the user multicast source.

Example

The following example shows how to show the reverse path forwarding information of the multicast source 192.168.20.2.

```
R142_config_e2/1#show ip rpf dvmrp 192.168.20.2
RPF information for (192.168.20.2)
  RPF interface:  Ethernet2/1
  RPF neighbor:   directly connected
  RPF route/mask: 192.168.20.0/24
  RPF type:       unicast (connected)
```

Related Commands

show ip mroute dvmrp