1 Multicast VPN

1.1 Overview

Multicast VPN is based on the BGP/MPLS L3VPN network to spread the multicast data in the VPN.

Multicast VPN establishes multicast IP tunnels between sites, and completes the function of transmitting multicast data between sites by encapsulating multicast messages in the private network.

In the current enterprise networks such as e-government network and power data, almost all are based on the BGP/MPLS L3VPN architecture, which realizes data isolation between departments by dividing different departments into different VPNs. Similarly, VPN isolation is also required for multicast services such as video conferencing and data sharing within the department. Therefore, there is an increasingly urgent need for multicast VPN.

MD (Multicast-Domain, multicast domain) is an implementation scheme of multicast VPN.

Protocol specification

draft-rosen-vpn-mcast12.txt

1.2 typical application

typical application	Scene description
Single AS Multicast VPN	Realize multicast VPN data transmission in a single AS BGP/MPLS L3VPN environment.

1.2.1 Single AS Multicast VPN

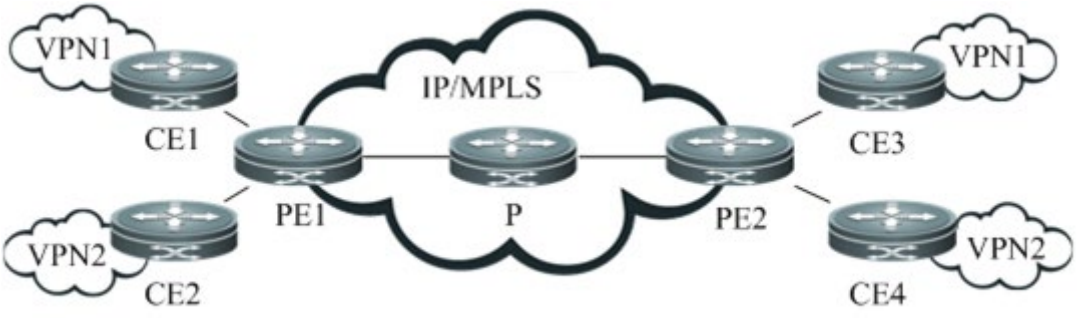
Application scenario

In a single-AS BGP/MPLS L3VPN environment, it supports multicast applications within the VPN.

The following figure is an example, PE1, PE2, PLocated in a single AS public network. CE1 and CE3 are located at VPN1 site, and CE2 and CE4 are located at VPN2 site.

Multicast data exchange between two VPN1 sites. Multicast data exchange between two VPN2 sites. The multicast data is isolated between the VPN1 site and the VPN2 site.

picture1-1



【Notes】
P is the core router.
PE1 and PE2 are edge routers of the backbone network.
CE1, CE2, CE3, and CE4 are edge routers of the private network.

Functional subordinate

On the public network of a single AS, support PIM-SM to create multicast VPN in ASM mode or SSM mode

1、 Create multicast VPN in ASM mode

- At P,PE1,The upper part of PE2, CE1, CE2, CE3, and CE4 belongs to IP BGP/MPLS L3VPN.
- At P,PE1,PE2, CE1, CE2, CE3, CE4 run the PIM-SM protocol to implement multicast routing.
- Configure multicast VPN on PE1 and PE2.

2、 Create multicast VPN in SSM mode

- At P,PE1,The upper part of PE2, CE1, CE2, CE3, and CE4 belongs to IP BGP/MPLS L3VPN.
- At P,PE1,PE2, CE1, CE2, CE3, CE4 run the PIM-SM protocol to implement multicast routing.
- Configure multicast VPN on PE1 and PE2.
- Enable BGP MDT-SAFI routing on PE1 and PE2.
- Enable SSM on PE1 and PE2

1.3 basic concept

P

P is the core device located in the ISP backbone network.

PE

PE is the edge device of the ISP backbone network, which accesses the user network and provides VPN services. The PE can be a router, ATM switch, frame relay switch, etc.

CE

CE is the edge device of the user network, and is connected to the PE device of the ISP backbone network. The CE can be a host, a router, or a switch.

MD

One VPN corresponds to one MD, which connects all PEs connected to the VPN site. The user network can regard MD as a shared network segment. When a private network multicast stream is sent from a PE to the MD, other PEs connected to the MD will receive the multicast stream. In fact, the private network multicast protocol messages and data messages are uniformly converted to public network multicast data messages on the PE, and forwarded to the remote PE along the MDT (Multicast Distribution Tree), and then Restore the multicast protocol packets and data packets of the private network from the remote PE.

Default-MDT

A Default-MDT corresponds to a VPN, connects all PEs connected to the VPN site, and forwards private network multicast streams to these PEs. Default-MDT can forward all private network multicast streams in this VPN, using a PG (group address for public network propagation) to uniquely identify a Default-MDT.

The PE first converts the multicast message belonging to the VPN into a data message of the PG, and then sends it to every other PE along the Default-MDT. On the remote PE, first restore the PG data message, and then decide whether to forward the message according to whether there is a demand in the connected VPN site. If not, the packet is discarded.

MVRF

A PE may be connected to multiple VPNs and needs to perform forwarding of multicast packets for each VPN. In order to isolate the multicast streams of different VPNs and solve the problem of multicast routing conflicts, PE maintains an MVRF (Multicast VPN Routing and Forwarding) for each VPN. When the PE receives the private network multicast message, it forwards it according to the corresponding MVRF.

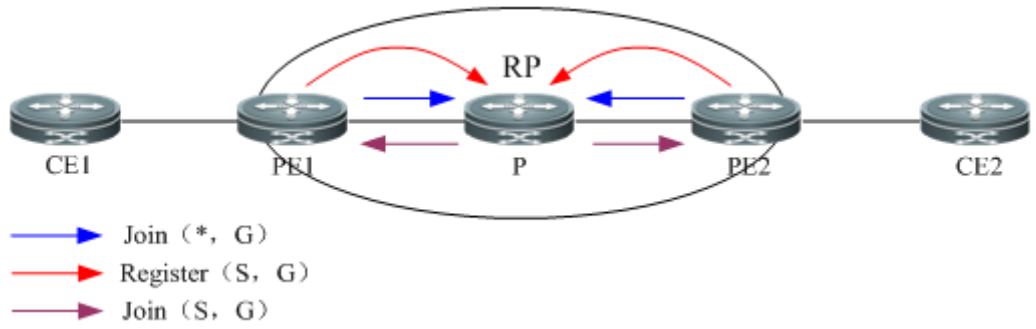
On the PE, each VRF corresponds to an MTI (Multicast Tunnel Interface), which belongs to the GRE Tunnel interface. On the MTI of the ingress PE, the private network multicast stream is converted to the public network multicast stream, and then forwarded along the MDT. On the egress PE, the public network multicast stream is converted into a private network multicast stream, and then sent to the corresponding VPN site.

Single AS Multicast VPN

On the public network of a single AS, PIM-SM is supported to create Default-MDT in ASM mode or SSM mode.

1、 Create Default-MDT in ASM mode

picture1-4 Create Default-MDT in ASM mode



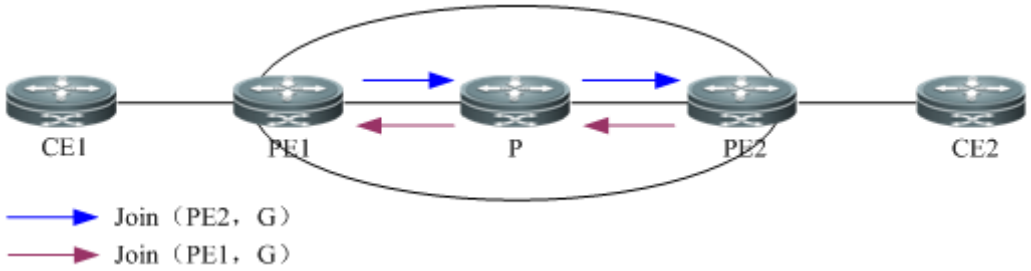
As shown in the figure above, P serves as the RP in the AS. The creation process of Default-MDT is as follows:

- Take PE1 and PE2 as multicast receivers. PE1 and PE2 initiate a (*,G) joining process to P. G is the group address of Default-MDT.
- Use PE1 as the multicast source. PE1 initiates the (S, G) registration process to P, and P initiates the (S, G) joining process to PE1. S is the address of PE1, and G is the group address of Default-MDT.
- Use PE2 as the multicast source. PE2 initiates the (S, G) registration process to P, and P initiates the (S, G) joining process to PE2. S is the address of PE2, and G is the group address of Default-MDT.

2、 Create Default-MDT in SSM mode

On the public network of a single AS, PIM-SM is supported to create Default-MDT in ASM mode or SSM mode.

picture1-5 Create Default-MDT in SSM mode



As shown in the figure above, the creation process of Default-MDT is as follows:

- With PE1 as the multicast receiver and PE2 as the multicast source, PE1 initiates an (S, G) join process to PE2. S is the address of PE2, and G is the group address of Default-MDT.
- With PE2 as the multicast receiver and PE1 as the multicast source, PE2 initiates an (S, G) join process to PE1. S is the address of PE1, and G is the group address of Default-MDT.

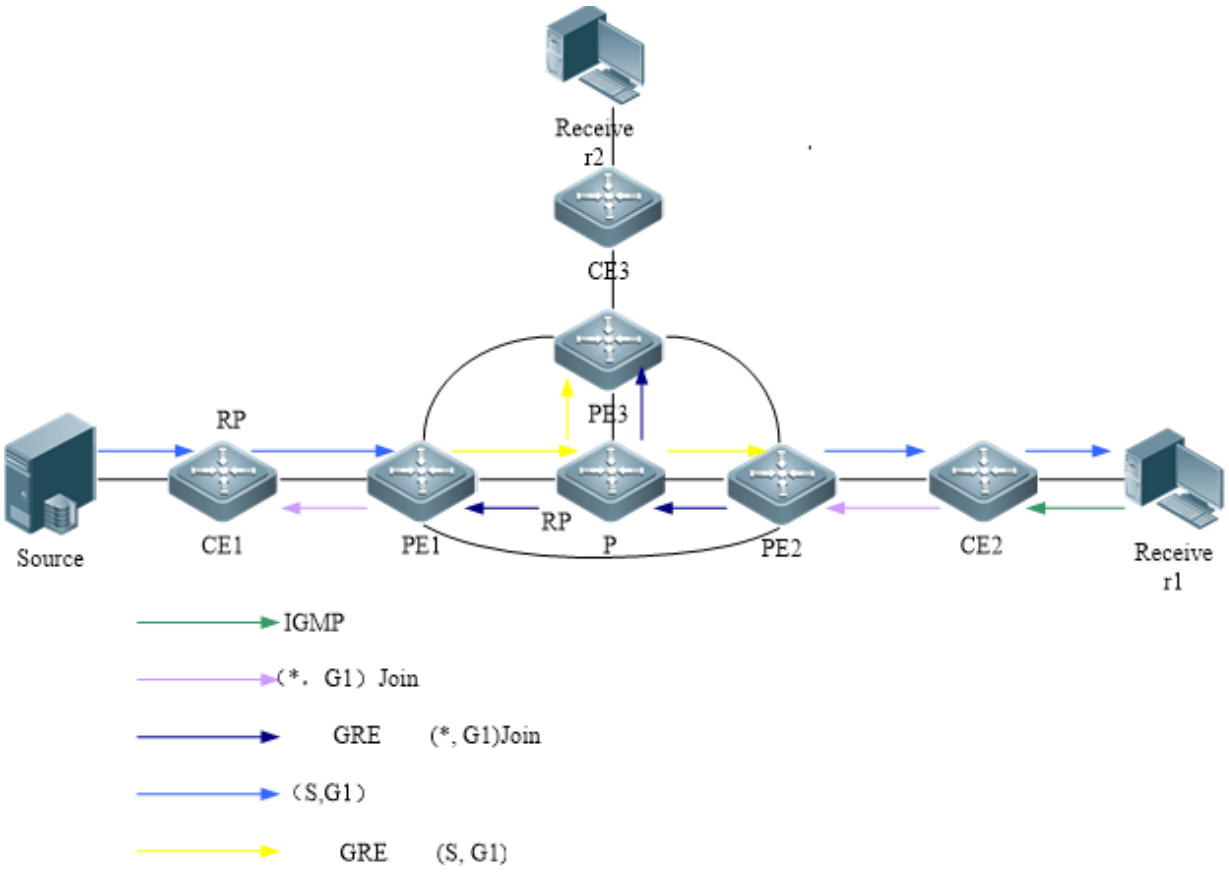
1.4 Detailed function

Features	effect
Default-MDT forwarding multicast stream	Use the Default-MDT multicast group to forward multicast streams on the public network.

1.4.1 Default-MDT forwarding multicast stream

Take the ASM mode as an example to introduce the process of using Default-MDT to transmit private network multicast streams.

picture1-7



In the above figure, the RP in the VPN is located in CE1, Recevier1 joins group G1, and Source sends a multicast stream to group G1.

- Recevier1 sends an IGMP Report message to CE2, and CE2 forms an (*, G1) entry.
- CE2 sends a Join (*, G1) message to CE1. It is encapsulated as a public network multicast packet on the MTI of PE2, and reaches PE1 and PE3 along the Default-MDT. Decapsulate on the MTI of PE1 and reach CE1. Decapsulate it on the MTI of PE3, and then discard it. Thus, an RPT tree is formed from CE1 to PE1, and then from PE2 to CE2.
- Source sends out (S, G1) message, reaches CE1, and then reaches PE1 along the RPT tree. It is encapsulated as a public network multicast packet on the MTI of PE1, and reaches PE2 and PE3 along the Default-MDT. Decapsulate on the MTI of PE2, follow the RPT tree to CE2, and then to Recevier1. On the MTI of PE3, it is discarded after decapsulation.

It can be seen that using Default-MDT to transmit private network multicast streams has the problem of wasting bandwidth.

1.5 Detailed configuration

Configuration item	Configuration suggestions & related commands	
Configure basic multicast VPN functions	Must be configured.	
	ip multicast-routing vrf*vrf-name*	Start multicast routing on the VRF.
	ip pim vrf *vrf-name* **rp-address** *rp-address* [access_list]	(Optional) Configure a static RP on the VRF.
	ip pim sparse-mode	Start PIM-SM on the interface belonging to this VRF.
	mdt default group_address	Set the Default-MDT group address.
	md_loopback	Set the md_loopback interface.

1.5.1 Configure Default-MDT function

Configuration effect

- The multicast VPN is realized, that is, the multicast data in the VPN is transmitted based on the BGP/MPLS L3VPN network.

Precautions

- A unicast VPN must be implemented, that is, the unicast data in the VPN is transmitted based on the BGP/MPLS L3VPN network.
- Multicast routing must be implemented in each VPN site.
- Multicast routing must be implemented in the public network.

Configuration method

Start multicast routing on VRF

On each PE, start multicast routing on each VRF.

【Command format】	**ip multicast-routing vrf***vrf-name*
【Parameter Description】	**vrf** *vrf-name*:Specify the name of the VRF.
[Default configuration]	closure
【Command Mode】	Global mode
【User guides】	-

Start PIM-SM on the interface belonging to the VRF

On each PE, start PIM-SM on each interface belonging to the VRF.

【Command format】	**ip pim sparse-mode**
【Parameter Description】	-
[Default configuration]	closure
【Command Mode】	Interface mode
【User guides】	PIM-SM can only be started on Layer 3 interfaces, including: router interface, L3AP, SVI, loopback interface. All PIM interfaces should be reachable by IPv4 unicast routes.

Configure static RP on VRF

ifIf a static RP is used in the VPN site, the corresponding VRF on the PE also needs to be configured with a static RP.

【Command format】	**ip pim vrf** *vrf-name* **rp-address** *rp-address* [access_list]
【Parameter Description】	**vrf** *vid*:Specify VRF. *rp-address*: StaticRPthe address of. *access_list*:useACLLimit the staticRPService groupaddressScope. The default is to serve all groups.
[Default configuration]	without
【Command Mode】	Global mode

【User guides】 This command is used to indicate where the static RP in the VPN site is.

Start SSM mode on VRF

ifIf the SSM mode is activated in the VPN site, the SSM mode must also be activated on the corresponding VRF on the PE.

【Command format】 **ip pim vrf** *vid* **ssm {default | range** *access-list***}**

【Parameter Description】 **vrf** *vid*:Specify VRF.
default:SSM default group address range: 232.0.0.0/8.
range *access_list*:Quote ACL to limit the SSM group address range. Support number ACL range from 1-99; also support named ACL.

[Default configuration] Turn off SSM mode

【Command Mode】 Global mode

【User guides】 If you need to implement SSM applications in the PIM-SM network, you must configure this command.

Set the default-MDT group address of the VRF

On each PE, set one for each VRFDefault-MDT group address.

【Command format】 **mdt default** *group_address*

【Parameter Description】 *group_address:*Default-MDT group address.

[Default configuration] without

【Command Mode】 VRF mode

【User guides】 Different VPNs should use different Default-MDT group addresses.
For the same VPN, the same Default-MDT group address should be configured on each PE.
After configuring this command, the PE will automatically generate an MTI interface for this VRF and start PIM-SM on the MTI interface.
The destination address of the packet encapsulated by this MTI interface is the group address.

Set md_ loopback interface

On each PE, set oneThe md_ loopback interface is used for the secondary routing of mvpn data.

【Command format】 **md_ loopback**

【Parameter Description】 without

[Default configuration] without

【Command Mode】 Interface mode

【User guides】 Each PE device needs to be configured with an md_loopback interface for secondary routing of mvpn data.
The md_ loopback interface needs to configure an IP address and enable ip pim sparse-mode
To avoid too much MVPN data and insufficient bandwidth of the md_ loopback interface to cause packet loss, it is recommended that md_ loopback be configured on a 40G interface.

Testing method

Use the show run command on the PE to check whether the Default-MDT group is configured.

Use the show ip pim mdt command on the PE to view the effective mdt default information.

Use the show ip pim sparse-mode vrf vpn1 mroute command on the PE to view the private network multicast packet forwarding.

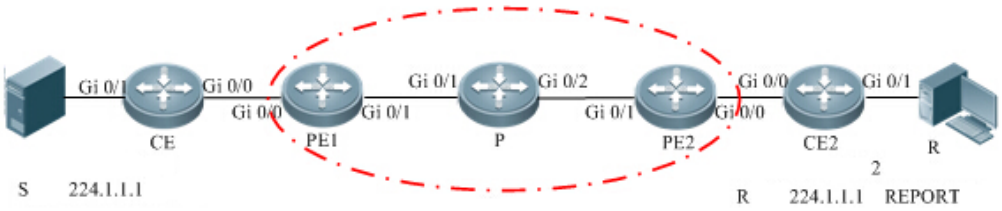
Use the show ip pim sparse-mode mroute command on the PE to view the public network multicast packet forwarding.

Configuration example

Configure Default-MDT function

【Web environment】

picture1-9



[Configuration method]

- Configure an IPv4 unicast routing protocol (such as OSPF) on each router in the private network 1, private network 2, and public network. slightly.
- Start the BGP protocol on the PE device. slightly.
- Enable the IPv4 multicast routing function and enable the multicast interface on each router in the private network 1, private network 2, and public network. slightly.
- Configure C-BSR and C-RP on the public network, and configure C-BSR and C-RP on the two private networks. slightly.
- Configure Default-MDT on the PE device.

P

```
P# configure terminal
P(config)#ip multicast-routing
P(config)#interface GigabitEthernet 0/1
P(config-if)#ip pim sparse-mode
P(config-if)#ip address 192.168.2.3 255.255.255.0
P(config-if)#mpls ip
P(config-if)#label-switching
P(config-if)#exit
P(config)#interface GigabitEthernet 0/2
P(config-if)#ip pim sparse-mode
P(config-if)#ip address 192.168.5.3 255.255.255.0
P(config-if)#mpls ip
P(config-if)#label-switching
P(config-if)#exit
P(config)#ip pim rp-address 192.168.2.3
P(config)router ospf 1
P(config-router)network 0.0.0.0 255.255.255.255 area 0
P(config-if)# exit
```

PE1

```
PE1# configure terminal
PE1(config)#ip vrf vpn1
PE1(config-vrf)#rd 1:100
PE1(config-vrf)#route-target both 1:100
PE1(config-vrf)# mdt default 239.1.1.1
PE1(config-vrf)#alloc-label per-route
PE1(config-vrf)#exit
PE1(config)# ip multicast-routing
PE1(config)# ip multicast-routing vrf vpn1
PE1(config)#vlan 1
PE1(config)#interface GigabitEthernet 0/0
```

```
PE1(config-if)#ip vrf forwarding vpn1
PE1(config-if)#ip pim sparse-mode
PE1(config-if)#ip address 192.168.3.1 255.255.255.0
PE1(config-if)#interface GigabitEthernet 0/1
PE1(config-if)#ip address 192.168.2.1 255.255.255.0
PE1(config-if)#mpls ip
PE1(config-if)#label-switching
PE1(config-if)#ip pim sparse-mode
PE1(config-if)#interface Loopback 0
PE1(config-if)#ip address 1.1.1.1 255.255.255.255
PE1(config-if)#ip pim sparse-mode
PE1(config-if)#exit
PE1(config)#router bgp 1
PE1(config-router)#bgp log-neighbor-changes
PE1(config-router)# bgp graceful-restart restart-time 120
PE1(config-router)# bgp graceful-restart stalepath-time 360
PE1(config-router)# bgp graceful-restart
PE1(config-router)# neighbor 2.2.2.2 remote-as 1
PE1(config-router)# neighbor 2.2.2.2 update-source Loopback 0
PE1(config-router)# address-family ipv4
PE1(config-router-af)# maximum-prefix 10000
PE1(config-router-af)# neighbor 2.2.2.2 activate
PE1(config-router-af)# neighbor 2.2.2.2 send-community both
PE1(config-router-af)# exit-address-family
PE1(config-router)# address-family vpnv4 unicast
PE1(config-router-af)# neighbor 2.2.2.2 activate
PE1(config-router-af)# neighbor 2.2.2.2 send-community both
PE1(config-router-af)# exit-address-family
PE1(config-router)#!
PE1(config-router)# address-family ipv4 vrf vpn1
PE1(config-router-af)# maximum-prefix 10000
PE1(config-router-af)# redistribute connected
PE1(config-router-af)# redistribute ospf 100 match internal
PE1(config-router-af)# exit-address-family
PE1(config-router)#exit
PE1(config)#router ospf 1
PE1(config-router)# graceful-restart
PE1(config-router)# network 0.0.0.0 255.255.255.255 area 0
PE1(config-router)#exit
PE1(config)#router ospf 100 vrf vpn1
PE1(config-router)# graceful-restart
PE1(config-router)# network 0.0.0.0 255.255.255.255 area 0
PE1(config)#
PE1(config)#mpls router ldp
PE1(config-mpls-router)# ldp router-id interface Loopback 0 force
PE1(config-mpls-router)# graceful-restart
PE1(config-mpls-router)#exit
PE1(config)#ip pim rp-address 192.168.2.3
PE1(config)#ip pim vrf vpn1 rp-address 192.168.3.1
PE1(config)# interface fortyGigabitEthernet 0/49
PE1(config-if-FortyGigabitEthernet 0/49)# md_loopback
PE1(config-if-FortyGigabitEthernet 0/49)# ip address 10.10.10.10/30
PE1(config-if-FortyGigabitEthernet 0/49)# ip pim sparse-mode
PE1(config-if-FortyGigabitEthernet 0/49)# exit
```

PE2

```
PE2# configure terminal
PE2(config)#ip vrf vpn1
PE2(config-vrf)#rd 1:100
PE2(config-vrf)#route-target both 1:100
PE2(config-vrf)# mdt default 239.1.1.1
PE2(config-vrf)#alloc-label per-route
PE2(config-vrf)#exit
PE2(config)# ip multicast-routing
```

```
PE2(config)# ip multicast-routing vrf vpn1
PE2(config)#vlan 1
PE2(config)#interface GigabitEthernet 0/0
PE2(config-if)#ip vrf forwarding vpn1
PE2(config-if)#ip pim sparse-mode
PE2(config-if)#ip address 192.168.6.1 255.255.255.0
PE2(config-if)#interface GigabitEthernet 0/1
PE2(config-if)#ip address 192.168.5.1 255.255.255.0
PE2(config-if)#mpls ip
PE2(config-if)#label-switching
PE2(config-if)#ip pim sparse-mode
PE2(config-if)#interface Loopback 0
PE2(config-if)#ip address 2.2.2.2 255.255.255.255
PE2(config-if)#ip pim sparse-mode
PE2(config-if)#exit
PE2(config)#router bgp 1
PE2(config-router)#bgp log-neighbor-changes
PE2(config-router)# bgp graceful-restart restart-time 120
PE2(config-router)# bgp graceful-restart stalepath-time 360
PE2(config-router)# bgp graceful-restart
PE2(config-router)# neighbor 1.1.1.1 remote-as 1
PE2(config-router)# neighbor 1.1.1.1 update-source Loopback 0
PE2(config-router)# address-family ipv4
PE2(config-router-af)# maximum-prefix 10000
PE2(config-router-af)# neighbor 1.1.1.1 activate
PE2(config-router-af)# neighbor 1.1.1.1 send-community both
PE2(config-router-af)# exit-address-family
PE2(config-router)# address-family vpnv4 unicast
PE2(config-router-af)# neighbor 1.1.1.1 activate
PE2(config-router-af)# neighbor 1.1.1.1 send-community both
PE2(config-router-af)# exit-address-family
PE2(config-router)#!
PE2(config-router)# address-family ipv4 vrf vpn1
PE2(config-router-af)# maximum-prefix 10000
PE2(config-router-af)# redistribute connected
PE2(config-router-af)# redistribute ospf 100 match internal
PE2(config-router-af)# exit-address-family
PE2(config-router)#exit
PE2(config)#router ospf 1
PE2(config-router)# graceful-restart
PE2(config-router)# network 0.0.0.0 255.255.255.255 area 0
PE2(config-router)#exit
PE2(config)#router ospf 100 vrf vpn1
PE2(config-router)# graceful-restart
PE2(config-router)# network 0.0.0.0 255.255.255.255 area 0
PE2(config)#
PE2(config)#mpls router ldp
PE2(config-mpls-router)# ldp router-id interface Loopback 0 force
PE2(config-mpls-router)# graceful-restart
PE2(config-mpls-router)#exit
PE2(config)#ip pim rp-address 192.168.2.3
PE2(config)#ip pim vrf vpn1 rp-address 192.168.3.1
PE2(config)# interface fortyGigabitEthernet 0/49
PE2(config-if-FortyGigabitEthernet 0/49)# md_loopback
PE2(config-if-FortyGigabitEthernet 0/49)# ip address 20.20.20.20/30
PE2(config-if-FortyGigabitEthernet 0/49)# ip pim sparse-mode
PE2(config-if-FortyGigabitEthernet 0/49)# exit
```

CE1

```
CE1# configure terminal
CE1(config)# ip multicast-routing
CE1(config)#interface GigabitEthernet 0/0
CE1(config-if)#ip pim sparse-mode
CE1(config-if)#ip address 192.168.3.2 255.255.255.0
```

CE2

```
CE1(config-if)#interface GigabitEthernet 0/1
CE1(config-if)#ip address 192.168.9.1 255.255.255.0
CE1(config-if)#ip pim sparse-mode
CE1(config)#router ospf 1
CE1(config-router)# graceful-restart
CE1(config-router)# network 0.0.0.0 255.255.255.255 area 0
CE1(config-router)#exit
CE1(config)#ip pim rp-address 192.168.3.1
CE1# configure terminal
CE1(config)# ip multicast-routing
CE1(config)#interface GigabitEthernet 0/0
CE1(config-if)#ip pim sparse-mode
CE1(config-if)#ip address 192.168.6.2 255.255.255.0
CE1(config-if)#interface GigabitEthernet 0/1
CE1(config-if)#ip address 192.168.10.1 255.255.255.0
CE1(config-if)#ip pim sparse-mode
CE1(config)#router ospf 1
CE1(config-router)# graceful-restart
CE1(config-router)# network 0.0.0.0 255.255.255.255 area 0
CE1(config-router)#exit
CE1(config)#ip pim rp-address 192.168.3.1
```

【Testing method】

Check the Default-MDT configuration information on each PE device.

```
QSW# show ip pim mdt
* implies group is the MDT default group
 MDT Group Interface Source VRF
* 239.1.1.1 Tunnel 0  Loopback 0 vpn1
```

Check the neighbor establishment of the private network on the PE1 device, and check it through the show ip pim sparse-mode neighbor command.

```
QSW# show ip pim sparse-mode vrf vpn1 neighbor
Neighbor Interface Uptime/Expires Ver DR
Address Priority/Mode
192.168.0.1 Gigabitethernet 0/1 00:00:01/00:01:44 v2 1/P
2.2.2.2 Tunnel 0 14:59:27/00:01:18 v2 1 / DR P
```

View the establishment of public network entries on the PE2 device, through show ip pim sparse-mode **mr**Command to view.

```
QSW#show ip pim sparse-mode mr
IP Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 2
(S,G,rpt) Entries: 2
FCR Entries: 0
REG Entries: 0

(*, 239.1.1.1)
RP: 192.168.2.1
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0.. I.............................
1 . . . . . .
2 . . . . . .
3.............................
4.............................
5.............................
6.............................
7.............................
```

```
Joined
0. J.........................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
Asserted
0.........................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
FCR:

(1.1.1.1, 239.1.1.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
kat expires in 133 seconds
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0.........................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
Joined
0.........................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
Asserted
0.........................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
Outgoing
0. Oo.......................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
```

```
6.........................
7.........................

(1.1.1.1, 239.1.1.1, rpt)
RP: 192.168.2.1
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: NOT PRUNED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0.........................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
Pruned
0.........................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
Outgoing
0. Oo.....................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................

(2.2.2.2, 239.1.1.1)
RPF nbr: 192.168.2.2
RPF idx: GigabitEthernet 0/1
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 39 seconds
kat expires in 157 seconds
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0.........................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
Joined
0.........................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
```

```
5.........................
6.........................
7.........................
Asserted
0.........................
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
Outgoing
0.. 0.......................
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................

(2.2.2.2, 239.1.1.1, rpt)
RP: 192.168.2.1
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: PRUNED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0.........................
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
Pruned
0. P.......................
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
Outgoing
0.. 0.......................
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................

QSW#
```

View the establishment of the RPT tree of the private network on the PE2 device, and view it through the show ip pim sparse-mode vrf vpn1 mr command.

```
QSW#show ip pim sparse-mode vrf vpn1 mr
IP Multicast Routing Table
```

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

(*, 225.1.1.1)
RP: 192.168.3.1
RPF nbr: 2.2.2.2
RPF idx: Tunnel 0
Upstream State: JOINED
jt_timer expires in 30 seconds
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0. I.........................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
Joined
0.........................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
Asserted
0.........................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
FCR:
Source: 192.168.3.56
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Outgoing
0. O.........................
1 . . . . . .
2 . . . . . .
3.........................
4.........................
5.........................
6.........................
7.........................
KAT timer running, 150 seconds remaining
 Packet count 1

QSW#
```

Common mistakes

- A static RP is used in the VPN site, but no static RP is configured on the VRF of the PE.
- Different VPNs are configured with the same default-mdt group address on the PE.
- In the same VPN, different default-mdt group addresses are configured on each PE.
- The md_loopback interface is not configured with an ip address, or ip pim sparse-mode is not enabled.

1.6 Monitoring and maintenance

Check the operation

effect	Order
Display MDT information.	**show ip pim mdt**
Display the MDT information advertised by BGP.	**show ip pim mdt bgp**
Display the MDT Join message sent by the specified VRF.	**show ip pim vrf** *vrf-name* **mdt send**
Display the MDT Join received by the specified VRF.	**show ip pim vrf** *vrf-name* **mdt receive** [detail]
Display MDT summary messages.	**show ip pim [vrf** *vrf-name*] **mdt summary**

View debugging information

effect	Order
Displays the opening status of the MD debugging switch.	**show debugging**
Turn on the debugging switch of MD events.	**debug ip pim mdt event**
Turn on the debugging switch of MD join.	**debug ip pim mdt join**
Turn on the debugging switch of MD nsm.	**debug ip pim mdt nsm**
Turn on the debugging switch of MD tunnel.	**debug ip pim mdt tunnel**