



# Configuring Multicast VPN Support

This chapter describes how to configure Multicast Virtual Private Network (MVPN) support on Cisco 7600 series routers. MVPN is supported when a PFC3B, PFC3BXL, PFC3C, or PFC3CXL is installed in the router.



**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the Cisco 7600 Series Routers Command References at this URL:

[http://www.cisco.com/en/US/products/hw/routers/ps368/prod\\_command\\_reference\\_list.html](http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html)

This chapter contains these sections:

- [Understanding How MVPN Works, page 27-1](#)
- [MVPN Configuration Guidelines and Restrictions, page 27-7](#)
- [Configuring MVPN, page 27-8](#)

## Understanding How MVPN Works

These sections describe MVPN:

- [MVPN Overview, page 27-1](#)
- [Multicast Routing and Forwarding and Multicast Domains, page 27-2](#)
- [Multicast Distribution Trees, page 27-2](#)
- [Multicast Tunnel Interfaces, page 27-5](#)
- [PE Router Routing Table Support for MVPN, page 27-6](#)
- [Multicast Distributed Switching Support, page 27-6](#)
- [Hardware-Assisted IPv4 Multicast, page 27-6](#)

## MVPN Overview

MVPN is a standards-based feature that transmits IPv4 multicast traffic across an MPLS VPN cloud. MVPN on Cisco 7600 series routers uses the existing PFC hardware support for IPv4 multicast traffic to forward multicast traffic over VPNs at wire speeds. MVPN adds support for IPv4 multicast traffic over Layer 3 IPv4 VPNs to the existing IPv4 unicast support.

MVPN routes and forwards multicast packets for each individual VPN routing and forwarding (VRF) instance, as well as transmitting the multicast packets through VPN tunnels across the service provider backbone.

MVPN is an alternative to IP-in-IP generic route encapsulation (GRE) tunnels. GRE tunnels are not a readily scalable solution and they are limited in the granularity they provide to customers.

## Multicast Routing and Forwarding and Multicast Domains

MVPN adds multicast routing information to the VPN routing and forwarding table. When a provider-edge (PE) router receives multicast data or control packets from a customer-edge (CE) router, forwarding is performed according to the information in the multicast VRF (MVRF).

**Note**

MVRF is also commonly referred to as multicast over VRF-lite.

Each MVRF maintains the routing and forwarding information that is needed for its particular VRF instance. An MVRF is created and configured in the same way as existing VRFs, except multicast routing is also enabled on each MVRF.

A multicast domain constitutes the set of hosts that can send multicast traffic to each other within the MPLS network. For example, the multicast domain for a customer that wanted to send certain types of multicast traffic to all global employees would consist of all CE routers associated with that enterprise.

## Multicast Distribution Trees

The MVPN feature establishes at least one multicast distribution tree (MDT) for each multicast domain. The MDT provides the information needed to interconnect the same MVRFs that exist on the different PE routers.

MVPN supports two MDT types:

- **Default MDT**—The default MDT is a permanent channel for PIM control messages and low-bandwidth streams between all PE routers in a particular multicast domain. All multicast traffic in the default MDT is replicated to every other PE router in the domain. Each PE router is logically seen as a PIM neighbor (one hop away) from every other PE router in the domain.
- **Data MDT**—Data MDTs are optional. If enabled, they are dynamically created to provide optimal paths for high-bandwidth transmissions, such as full-motion video, that do not need to be sent to every PE router. This allows for on-demand forwarding of high-bandwidth traffic between PE routers, so as to avoid flooding every PE router with every high-bandwidth stream that might be created.

To create data MDTs, each PE router that is forwarding multicast streams to the backbone periodically examines the traffic being sent in each default MDT as follows:

1. Each PE router periodically samples the multicast traffic (approximately every 10 seconds for software switching, and 90 seconds for hardware switching) to determine whether a multicast stream has exceeded the configured threshold. (Depending on when the stream is sampled, this means that in a worst-case scenario, it could take up to 180 seconds before a high-bandwidth stream is detected.)

**Note**

Data MDTs are created only for (S, G) multicast route entries within the VRF multicast routing table. They are not created for (\*, G) entries.

2. If a particular multicast stream exceeds the defined threshold, the sending PE router dynamically creates a data MDT for that particular multicast traffic.
3. The sending PE router then transmits a DATA-MDT JOIN request (which is a User Datagram Protocol (UDP) message to port 3232) to the other PE routers, informing them of the new data MDT.
4. Receiving PE routers examine their VRF routing tables to determine if they have any customers interested in receiving this data stream. If so, they use the PIM protocol to transmit a PIM JOIN message for this particular data MDT group (in the global table PIM instance) to accept the stream. Routers that do not currently have any customers for this stream still cache the information, in case any customers request it later on.
5. Three seconds after sending the DATA-MDT JOIN message, the sending PE router removes the high-bandwidth multicast stream from the default MDT and begins transmitting it over the new data MDT.
6. The sending PE router continues to send a DATA-MDT JOIN message every 60 seconds, as long as the multicast stream continues to exceed the defined threshold. If the stream falls below the threshold for more than 60 seconds, the sending PE router stops sending the DATA-MDT JOIN messages, and moves the stream back to the default MDT.
7. Receiving routers age out the cache information for the default MDT when they do not receive a DATA-MDT JOIN message for more than three minutes.

Data MDTs allow for high-bandwidth sources inside the VPN while still ensuring optimal traffic forwarding in the MPLS VPN core.

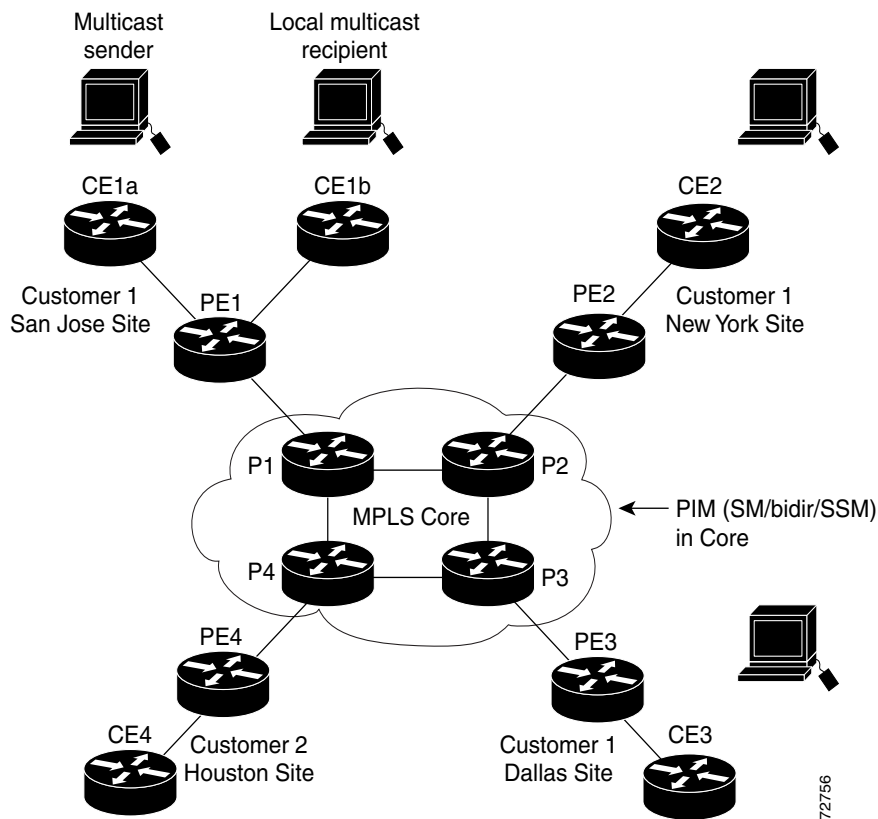
**Note**

For technical information about the DATA-MDT JOIN message and other aspects of the data MDT creation and usage, see the Internet-Draft, *Multicast in MPLS/BGP IP VPNs*, by Eric C. Rosen et al.

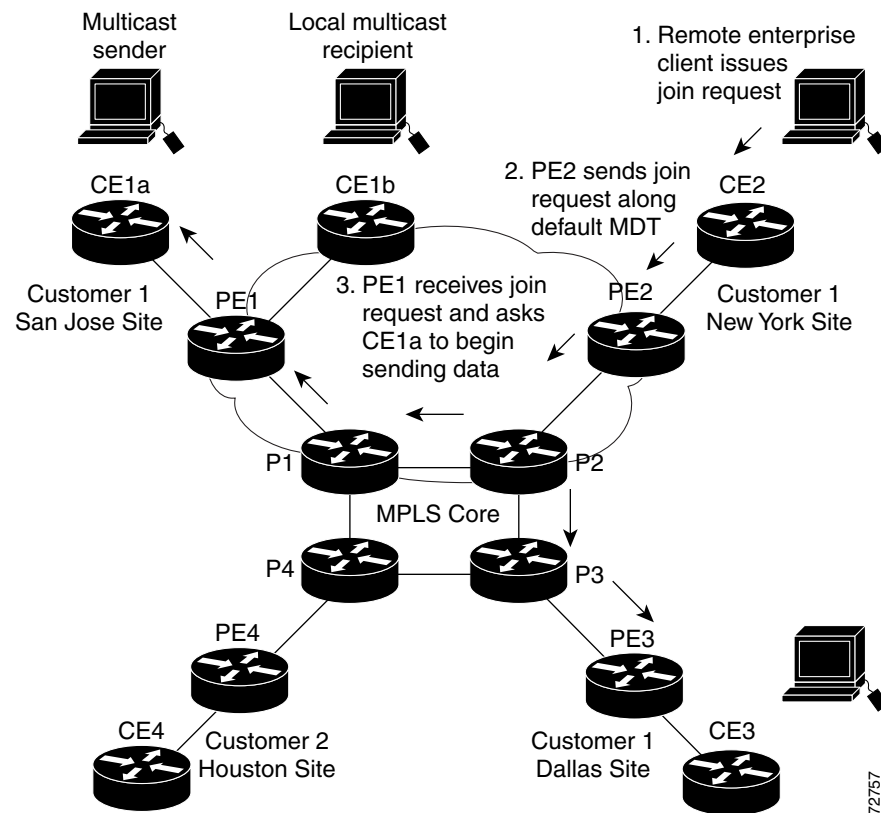
In the following example, a service provider has a multicast customer with offices in San Jose, New York, and Dallas. The San Jose site is transmitting a one-way multicast presentation. The service provider network supports all three sites associated with this customer, in addition to the Houston site of a different enterprise customer.

The default MDT for the enterprise customer consists of provider routers P1, P2, and P3 and their associated PE routers. Although PE4 is interconnected to these other routers in the MPLS core, PE4 is associated with a different customer and is therefore not part of the default MDT.

Figure 27-1 shows the situation in this network when no one outside of San Jose has joined the multicast broadcast, which means that no data is flowing along the default MDT. Each PE router maintains a PIM relationship with the other PE routers over the default MDT, as well as a PIM relationship with its directly attached PE routers.

**Figure 27-1** *Default Multicast Distribution Tree Overview*

If an employee in New York joins the multicast session, the PE router associated for the New York site sends a join request that flows across the default MDT for the multicast domain. The PE router associated with the multicast session source (PE1) receives the request. [Figure 27-2](#) shows how the PE router forwards the request to the CE router associated with the multicast source (CE1a).

**Figure 27-2** *Initializing the Data MDT*

The CE router (CE1a) starts sending the multicast data to the associated PE router (PE1), which recognizes that the multicast data exceeds the bandwidth threshold at which a data MDT should be created. PE1 then creates a data MDT and sends a message to all routers using the default MDT that contains information about the data MDT.

Approximately three seconds later, PE1 begins sending the multicast data for that particular stream using the data MDT. Because only PE2 has receivers who are interested in this source, only PE2 joins the data MDT and receives traffic on it.

## Multicast Tunnel Interfaces

The PE router creates a multicast tunnel interface (MTI) for each multicast VRF (MVRF) in the multicast domain. The MVRF uses the tunnel interface to access the multicast domain to provide a conduit that connects an MVRF and the global MVRF.

On the router, the MTI is a tunnel interface (created with the **interface tunnel** command) with a class D multicast address. All PE routers that are configured with a default MDT for this MVRF create a logical network in which each PE router appears as a PIM neighbor (one hop away) to every other PE router in the multicast domain, regardless of the actual physical distance between them.

The MTI is automatically created when an MVRF is configured. The BGP peering address is assigned as the MTI interface source address, and the PIM protocol is automatically enabled on each MTI.

When the router receives a multicast packet from the customer side of the network, it uses the incoming interface's VRF to determine which MVRFs should receive it. The router then encapsulates the packet using GRE encapsulation. When the router encapsulates the packet, it sets the source address to that of the BGP peering interface and sets the destination address to the multicast address of the default MDT, or to the source address of the data MDT if configured. The router then replicates the packet as needed for forwarding on the appropriate number of MTI interfaces.

When the router receives a packet on the MTI interface, it uses the destination address to identify the appropriate default MDT or data MDT, which in turn identifies the appropriate MVRF. It then decapsulates the packet and forwards it out the appropriate interfaces, replicating it as many times as are necessary.

**Note**

- Unlike other tunnel interfaces that are commonly used on Cisco routers, the MVPN MTI is classified as a LAN interface, not a point-to-point interface. The MTI interface is not configurable, but you can use the **show interface tunnel** command to display its status.
- The MTI interface is used exclusively for multicast traffic over the VPN tunnel.
- The tunnel does not carry unicast routed traffic.

## PE Router Routing Table Support for MVPN

Each PE router that supports the MVPN feature uses the following routing tables to ensure that the VPN and MVPN traffic is routed correctly:

- Default routing table—Standard routing table used in all Cisco routers. This table contains the routes that are needed for backbone traffic and for non-MPLS VPN unicast and multicast traffic (including Generic Routing Encapsulation (GRE) multicast traffic).
- VPN routing/forwarding (VRF) table—Routing table created for each VRF instance. Responsible for routing the unicast traffic between VPNs in the MPLS network.
- Multicast VRF (MVRF) table—Multicast routing table and multicast routing protocol instance created for each VRF instance. Responsible for routing the multicast traffic in the multicast domain of the network. This table also includes the multicast tunnel interfaces that are used to access the multicast domain.

## Multicast Distributed Switching Support

MVPN supports multicast distributed switching (MDS) for multicast support on a per-interface and a per-VRF basis. When configuring MDS, you must make sure that no interface (including loopback interfaces) has the **no ip mroute-cache** command configured.

## Hardware-Assisted IPv4 Multicast

The PFC supports hardware acceleration for IPv4 multicast over VPN traffic, which forwards multicast traffic to the appropriate VPNs at wire speed without increased MSFC3 CPU utilization.

In a customer VRF, PFC hardware acceleration supports multicast traffic in PIM dense, PIM sparse, PIM bidirectional, and PIM Source Specific Multicast (SSM) modes.

In the service provider core, PFC hardware acceleration supports multicast traffic in PIM sparse, PIM bidirectional, and PIM SSM modes. In the service provider core, PFC hardware acceleration does not support multicast traffic in PIM dense mode.

## MVPN Configuration Guidelines and Restrictions

When configuring MVPN, follow these guidelines and restrictions:

- The Cisco 7600 series router must have a PFC3B, PFC3BXL, PFC3C, or PFC3CXL installed to run MVPN.
- All PE routers in the multicast domain need to be running a Cisco IOS software image that supports the MVPN feature. There is no requirement for MVPN support on the P and CE routers.
- Support for IPv4 multicast traffic must also be enabled on all backbone routers.
- The Border Gateway Protocol (BGP) routing protocol must be configured and operational on all routers supporting multicast traffic. In addition, BGP extended communities must be enabled (using the **neighbor send-community both** or **neighbor send-community extended** command) to support the use of MDTs in the network.
- Only ingress replication is supported when MVPN is configured. If the router is currently configured for egress replication, it is forced into ingress replication when the first MVRF is configured.
- When the router is acting as a PE, and receives a multicast packet from a customer router with a time-to-live (TTL) value of 2, it drops the packet instead of encapsulating it and forwarding it across the MVPN link. Because such packets would normally be dropped by the PE at the other end of the MVPN link, this does not affect traffic flow.
- If the core multicast routing uses SSM, then the data and default multicast distribution tree (MDT) groups must be configured within the SSM range of IPv4 addresses.
- The update source interface for the BGP peerings must be the same for all BGP peerings configured on the router in order for the default MDT to be configured properly. If you use a loopback address for BGP peering, then PIM sparse mode must be enabled on the loopback address.
- The **ip mroute-cache** command must be enabled on the loopback interface used as the BGP peering interface in order for distributed multicast switching to function on the platforms that support it. The **no ip mroute-cache** command must *not* be present on these interfaces.
- Data MDTs are not created for VRF PIM dense mode multicast streams because of the flood and prune nature of dense mode multicast flows and the resulting periodic bring-up and tear-down of such data MDTs.
- Data MDTs are not created for VRF PIM bidirectional mode because source information is not available.
- MVPN does not support multiple BGP peering update sources, and configuring them can break MVPN RPF checking. The source IPv4 address of the MVPN tunnels is determined by the highest IPv4 address used for the BGP peering update source. If this IPv4 address is not the IPv4 address used as the BGP peering address with the remote PE router, MVPN will not function properly.
- MDT tunnels do not carry unicast traffic.
- Although MVPN uses the infrastructure of MPLS VPN networks, you cannot apply MPLS tags or labels to multicast traffic over the VPNs.

- Each MVRF that is configured with a default MDT uses three hidden VLANs (one each for encapsulation, decapsulation, and interface), in addition to external, user-visible VLANs. This means that an absolute maximum of 1,000 MVRFs are supported on each router. (MVRFs without a configured MDT still use one internal VLAN, so unused MVRFs should be deleted to conserve VLAN allocation.)
- Because MVPN uses MPLS, MVPN supports only the RPR and RPR+ redundancy modes. MPLS can coexist with NSF with SSO redundancy mode, but there is no support for stateful MPLS switchover.
- If your MPLS VPN network already contains a network of VRFs, you do not need to delete them or recreate them to be able to support MVRF traffic. Instead, configure the **mdt default** and **mdt data** commands, as listed in the following procedure, to enable multicast traffic over the VRF.
- BGP should be already configured and operational on all routers that are sending or receiving multicast traffic. In addition, BGP extended communities must be enabled (using the **neighbor send-community both** or **neighbor send-community extended** command) to support the use of MDTs in the network.
- The same MVRF must be configured on each PE router that is to support a particular VPN connection.
- Each PE router that supports a particular MVRF must be configured with the same **mdt default** command.
- In Cisco IOS Release 15.0(1)S egress and ingress replication modes are supported when MVPN is configured on the Cisco 7600 series router. The router can be configured either for ingress or egress replication mode.
- 20k is the maximum supported scale for native multicast.

## Configuring MVPN

These sections describe how to configure MVPN:

- [Configuring Egress and Ingress Multicast Replication Mode, page 27-8](#)
- [Configuring a Multicast VPN Routing and Forwarding Instance, page 27-10](#)
- [Configuring Multicast VRF Routing, page 27-16](#)
- [Configuring Interfaces for Multicast Routing to Support MVPN, page 27-20](#)



### Note

These configuration tasks assume that BGP is already configured and operational on all routers that are sending or receiving the multicast traffic. In addition, BGP extended communities must be enabled (using the **neighbor send-community both** or **neighbor send-community extended** command) to support the use of MDTs in the network.

## Configuring Egress and Ingress Multicast Replication Mode

To configure either egress or ingress multicast replication mode, use the following commands:



	Command	Purpose
<b>Step 1</b>	Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	Router(config)# <b>ip multicast hardware-switching replication-mode {egress   ingress}</b> or Router(config)# <b>no ip multicast hardware-switching replication-mode {egress   ingress}</b>	Configures ingress multicast replication mode and disables automatic detection of the replication mode (enabled by default). Restores the system to automatic detection mode.
<b>Step 3</b>	Router(config)# <b>show platform software multicast ip capability</b>	Verifies the configuration.

The following is a sample output of the running-configuration, when the ingress replication mode is changed to egress replication mode:

```
Router(config)# ip multicast hardware-switching replication-mode ingress
Warning: This command will change the replication mode for all address families.

Router(config)# do sh runn | i ingress
ip multicast hardware-switching replication-mode ingress
ipv6 multicast hardware-switching replication-mode ingress

Router(config)# ip multicast hardware-switching replication-mode egress
Warning: This command will change the replication mode for all address families.
Warning: Egress replication-mode forced by CLI in presence of an egress-incapable card
*Apr 19 05:07:30.180: %CONST_MFIB_RP-6-REPLICATION_MODE_CHANGE: Replication Mode Change
Detected.
Current system replication mode is Egress

Router(config)# do sh runn | i egress
ip multicast hardware-switching replication-mode egress
```

This example shows how to verify the multicast replication mode:

```
Router# show platform software multicast ip capability
Current System HW Replication Mode : Egress
Auto-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
 2 Egress Egress
 3 Egress Egress
 4 Egress Egress
 6 Egress Egress
```

If the current replication mode is egress or if any of the switching modules are capable of egress replication mode, configure ingress replication mode during a scheduled maintenance period to minimize the disruption of customer traffic.

To configure ingress multicast replication mode, perform this task:

	Command	Purpose
<b>Step 1</b>	Router# <b>configure terminal</b>	Enters global configuration mode.

	Command	Purpose
Step 2	Router(config)# <b>ip multicast hardware-switching replication-mode {egress   ingress}</b>	Configures ingress multicast replication mode and disables automatic detection of the replication mode (enabled by default).
	Router(config)# <b>no ip multicast hardware-switching replication-mode ingress</b>	Enables automatic detection of the replication mode.
Step 3	Router(config)# <b>show platform software multicast ip capability</b>	Verifies the configuration.

This example shows how to configure ingress multicast replication mode and verify the configuration:

```
Router(config)# ip multicast hardware-switching replication-mode ingress
Router(config)# show platform software multicast ip capability
Current System HW Replication Mode : Ingress
Auto-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
  2 Ingress Ingress
  3 Ingress Ingress
  4 Ingress Ingress
  6 Ingress Ingress
Router#
```

## Configuring a Multicast VPN Routing and Forwarding Instance

These sections describe how to configure a multicast VPN routing and forwarding (MVRF) instance for each VPN connection on each PE router that is to handle the traffic for each particular VPN connection that is to transmit or receive multicast traffic:

- [Configuring a VRF Entry, page 27-10](#)
- [Configuring the Route Distinguisher, page 27-11](#)
- [Configuring the Route-Target Extended Community, page 27-11](#)
- [Configuring the Default MDT, page 27-12](#)
- [Configuring Data MDTs \(Optional\), page 27-13](#)
- [Enabling Data MDT Logging, page 27-13](#)
- [Sample Configuration, page 27-13](#)
- [Displaying VRF Information, page 27-14](#)

### Configuring a VRF Entry

To configure a VRF entry, perform this task:

	Command or Action	Purpose
Step 1	Router# <b>configure terminal</b>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	Router(config)# <b>ip vrf</b> <i>vrf_name</i>	Configures a VRF routing table entry and a Cisco Express Forwarding (CEF) table entry and enters VRF configuration mode.
	Router(config)# <b>no ip vrf</b> <i>vrf_name</i>	Deletes the VRF entry.
Step 3	Router(config-vrf)# <b>do show ip vrf</b> <i>vrf_name</i>	Verifies the configuration.

This example show how to configure a VRF named blue and verify the configuration:

```
Router# configure terminal
Router(config)# ip vrf blue
Router(config-vrf)# do show ip vrf blue
Name                               Default RD          Interfaces
blue                               <not set>
```

## Configuring the Route Distinguisher

To configure the route distinguisher, perform this task:

	Command or Action	Purpose
Step 1	Router(config-vrf)# <b>rd</b> <i>route_distinguisher</i>	Specifies the route distinguisher for a VPN IPv4 prefix.
	Router(config-vrf)# <b>no rd</b> <i>route_distinguisher</i>	Deletes the route distinguisher.
Step 2	Router(config-vrf)# <b>do show ip vrf</b> <i>vrf_name</i>	Verifies the configuration.

When configuring the route distinguisher, enter the route distinguisher in one of the following formats:

- 16-bit AS number:your 32-bit number (101:3)
- 32-bit IPv4 address:your 16-bit number (192.168.122.15:1)

This example show how to configure 55:1111 as the route distinguisher and verify the configuration:

```
Router(config-vrf)# rd 55:1111
Router(config-vrf)# do show ip vrf blue
Name                               Default RD          Interfaces
blue                               55:1111
```

## Configuring the Route-Target Extended Community

To configure the route-target extended community, perform this task:

	Command or Action	Purpose
Step 1	Router(config-vrf)# <b>route-target</b> [ <b>import</b>   <b>export</b>   <b>both</b> ] <i>route_target_ext_community</i>	Configures a route-target extended community for the VRF.
	Router(config-vrf)# <b>no route-target</b> [[ <b>import</b>   <b>export</b>   <b>both</b> ] <i>route_target_ext_community</i> ]	Deletes the route-target extended community.
Step 2	Router(config-vrf)# <b>do show ip vrf detail</b>	Verifies the configuration.

When configuring the route-target extended community, note the following information:

- **import**—Imports routing information from the target VPN extended community.

- **export**—Exports routing information to the target VPN extended community.
- **both**—Imports and exports.
- *route\_target\_ext\_community*—Adds the 48-bit route-target extended community to the VRF. Enter the number in one of the following formats:
  - 16-bit AS number:your 32-bit number (101:3)
  - 32-bit IPv4 address:your 16-bit number (192.168.122.15:1)

This example shows how to configure 55:1111 as the import and export route-target extended community and verify the configuration:

```
Router(config-vrf)# route-target both 55:1111
Router(config-vrf)# do show ip vrf detail
VRF blue; default RD 55:1111; default VPNID <not set>
VRF Table ID = 1
  No interfaces
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:55:1111
  Import VPN route-target communities
    RT:55:1111
  No import route-map
  No export route-map
  CSC is not configured.
```

## Configuring the Default MDT

To configure the default MDT, perform this task:

Command or Action	Purpose
Router(config-vrf)# <b>mdt default</b> <i>group_address</i>	Configures the default MDT.
Router(config-vrf)# <b>no mdt default</b>	Deletes the default MDT.

When configuring the default MDT, note the following:

- The *group\_address* is the multicast IPv4 address of the default MDT group. This address serves as an identifier for the MVRF community, because all provider-edge (PE) routers configured with this same group address become members of the group, which allows them to receive the PIM control messages and multicast traffic that are sent by other members of the group.
- This same default MDT must be configured on each PE router to enable the PE routers to receive multicast traffic for this particular MVRF.

This example shows how to configure 239.1.1.1 as the default MDT:

```
Router(config-vrf)# mdt default 239.1.1.1
```

## Configuring Data MDTs (Optional)

To configure optional data MDTs, perform this task:

Command or Action	Purpose
Router(config-vrf)# <b>mdt data</b> <i>group_address</i> <i>wildcard_bits</i> [ <b>threshold</b> <i>threshold_value</i> ] [ <b>list</b> <i>access_list</i> ]	(Optional) Configures a data MDTs for the specified range of multicast addresses.
Router(config-vrf)# <b>no mdt data</b>	Deletes the data MDT.

When configuring optional data MDTs, note the following information:

- *group\_address1*—Multicast group address. The address can range from 224.0.0.1 to 239.255.255.255, but cannot overlap the address that has been assigned to the default MDT.
- *wildcard\_bits*—Wildcard bitmask to be applied to the multicast group address to create a range of possible addresses. This allows you to limit the maximum number of data MDTs that each MVRF can support.
- **threshold** *threshold\_value*—(Optional) Defines the threshold value in kilobits, at which multicast traffic should be switched from the default MDT to the data MDT. The *threshold\_value* parameter can range from 1 through 4294967 kilobits.
- **list** *access\_list*—(Optional) Specifies an access list name or number to be applied to this traffic.

This example shows how to configure a data MDT:

```
Router(config-vrf)# mdt data 239.1.2.0 0.0.0.3 threshold 10
```

## Enabling Data MDT Logging

To enable data MDT logging, perform this task:

Command or Action	Purpose
Router(config-vrf)# <b>mdt log-reuse</b>	(Optional) Enables the recording of data MDT reuse information, by generating a SYSLOG message whenever a data MDT is reused. Frequent reuse of a data MDT might indicate a need to increase the number of allowable data MDTs by increasing the size of the wildcard bitmask that is used in the <b>mdt data</b> command.
Router(config-vrf)# <b>no log-reuse</b>	Disables data MDT logging.

This example shows how to enable data MDT logging:

```
Router(config-vrf)# mdt log-reuse
```

## Sample Configuration

The following excerpt from a configuration file shows typical VRF configurations for a range of VRFs. To simplify the display, only the starting and ending VRFs are shown.

```
!
ip vrf mvpn-cus1
rd 200:1
```

```

route-target export 200:1
route-target import 200:1
mdt default 239.1.1.1
!
ip vrf mvpn-cus2
rd 200:2
route-target export 200:2
route-target import 200:2
mdt default 239.1.1.2
!
ip vrf mvpn-cus3
rd 200:3
route-target export 200:3
route-target import 200:3
mdt default 239.1.1.3
!
...

ip vrf mvpn-cus249
rd 200:249
route-target export 200:249
route-target import 200:249
mdt default 239.1.1.249
mdt data 239.1.1.128 0.0.0.7

```

## Displaying VRF Information

To display all of the VRFs that are configured on the router, use the **show ip vrf** command:

```
Router# show ip vrf
```

Name	Default RD	Interfaces
green	1:52	GigabitEthernet6/1
red	200:1	GigabitEthernet1/1
		GigabitEthernet3/16
		Loopback2

```
Router#
```

To display information about the MDTs that are currently configured for all MVRFs, use the **show ip pim mdt** command. The following example shows typical output for this command:

```
Router# show ip pim mdt
```

MDT Group	Interface	Source	VRF
* 227.1.0.1	Tunnel1	Loopback0	BIDIR01
* 227.2.0.1	Tunnel2	Loopback0	BIDIR02
* 228.1.0.1	Tunnel3	Loopback0	SPARSE01
* 228.2.0.1	Tunnel4	Loopback0	SPARSE02



### Note

To display information about a specific tunnel interface, use the **show interface tunnel** command. The IPv4 address for the tunnel interface is the multicast group address for the default MDT of the MVRF.

To display entries for a specific VRF, use the **show platform software multicast ip vrf** command. The following example shows typical output for this command:

```
Router# show platform software multicast ip vrf
```

```

State: H - Hardware Installed, I - Install Pending, D - Delete Pending,
      Z - Zombie

```

VRF	MMLS VPN-ID	MDT INFO	MDT Type	State
BIDIR01HWRP	1	(10.10.10.9, 227.1.0.1)	default	H
BIDIR01SWRP	2	(10.10.10.9, 227.2.0.1)	default	H
SPARSE01HWRP	3	(10.10.10.9, 228.1.0.1)	default	H
SPARSE01SWRP	4	(10.10.10.9, 228.2.0.1)	default	H
red	5	(6.6.6.6, 234.1.1.1)	default	H
red	5	(131.2.1.2, 228.1.1.75)	data (send)	H
red	5	(131.2.1.2, 228.1.1.76)	data (send)	H
red	5	(131.2.1.2, 228.1.1.77)	data (send)	H
red	5	(131.2.1.2, 228.1.1.78)	data (send)	H

Router#

To display routing information for a particular VRF, use the **show ip route vrf** command:

Router# **show ip route vrf red**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
 \* - candidate default, U - per-user static route, o - ODR  
 P - periodic downloaded static route

Gateway of last resort is not set

```

      2.0.0.0/32 is subnetted, 1 subnets
C      2.2.2.2 is directly connected, Loopback2
      3.0.0.0/32 is subnetted, 1 subnets
B      3.3.3.3 [200/0] via 3.1.1.3, 00:20:09
C      21.0.0.0/8 is directly connected, GigabitEthernet3/16
B      22.0.0.0/8 [200/0] via 3.1.1.3, 00:20:09

```

Router#

To display information about the multicast routing table and tunnel interface for a particular MVRF, use the **show ip mroute vrf** command. The following example shows typical output for a MVRF named BIDIR01:

Router# **show ip mroute vrf BIDIR01**

```

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
      L - Local, P - Pruned, R - RP-bit set, F - Register flag,
      T - SPT-bit set, J - Join SPT, M - MSDP created entry,
      X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
      U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
      Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.1.0.1), 00:16:25/stopped, RP 10.10.10.12, flags: SJCF
  Incoming interface: Tunnel1, RPF nbr 10.10.10.12, Partial-SC
  Outgoing interface list:
    GigabitEthernet3/1.3001, Forward/Sparse-Dense, 00:16:25/00:02:49, H
(6.9.0.100, 228.1.0.1), 00:14:13/00:03:29, flags: FT
  Incoming interface: GigabitEthernet3/1.3001, RPF nbr 0.0.0.0, RPF-MFD
  Outgoing interface list:
    Tunnel1, Forward/Sparse-Dense, 00:14:13/00:02:46, H

```

Router#

**Note**

In this example, the **show ip mroute vrf** command shows that Tunnel1 is the MDT tunnel interface (MTI) being used by this VRF.

## Configuring Multicast VRF Routing

These sections describe how to configure multicast routing to support MVPN:

- [Enabling IPv4 Multicast Routing Globally, page 27-16](#)
- [Enabling IPv4 Multicast VRF Routing, page 27-17](#)
- [Configuring a PIM VRF Register Message Source Address, page 27-17](#)
- [Specifying the PIM VRF Rendezvous Point \(RP\) Address, page 27-17](#)
- [Configuring a Multicast Source Discovery Protocol \(MSDP\) Peer, page 27-18](#)
- [Enabling IPv4 Multicast Header Storage, page 27-18](#)
- [Configuring the Maximum Number of Multicast Routes, page 27-19](#)
- [Sample Configuration, page 27-19](#)
- [Displaying IPv4 Multicast VRF Routing Information, page 27-20](#)

**Note**

BGP should be already configured and operational on all routers that are sending or receiving multicast traffic. In addition, BGP extended communities must be enabled (using the **neighbor send-community both** or **neighbor send-community extended** command) to support the use of MDTs in the network.

## Enabling IPv4 Multicast Routing Globally

To enable IPv4 multicast routing globally, perform this task:

	Command or Action	Purpose
<b>Step 1</b>	Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	Router(config)# <b>ip multicast-routing</b>	Enables IPv4 multicast routing globally.
	Router(config)# <b>no ip multicast-routing</b>	Disables IPv4 multicast routing globally.

This example show how to enable IPv4 multicast routing globally:

```
Router# configure terminal
Router(config)# ip multicast-routing
```



## Enabling IPv4 Multicast VRF Routing

To enable IPv4 multicast VRF routing, perform this task:

Command or Action	Purpose
Router(config)# <b>ip multicast-routing vrf</b> <i>vrf_name</i> [ <b>distributed</b> ]	Enables IPv4 multicast VRF routing.
Router(config)# <b>no ip multicast-routing</b>	Disables IPv4 multicast VRF routing.

When enabling IPv4 multicast VRF routing, note the following information:

- *vrf\_name*—Specifies a particular VRF for multicast routing. The *vrf\_name* should refer to a VRF that has been previously created, as specified in the “[Configuring a Multicast VPN Routing and Forwarding Instance](#)” section on page 27-10.
- **distributed**—(Optional) Enables Multicast Distributed Switching (MDS).

This example show how to enable IPv4 multicast VRF routing:

```
Router# configure terminal
Router(config)# ip multicast-routing vrf blue
```

## Configuring a PIM VRF Register Message Source Address

To configure a PIM VRF register message source address, perform this task:

Command or Action	Purpose
Router(config)# <b>ip pim vrf</b> <i>vrf_name</i> <b>register-source</b> <i>interface_type interface_number</i>	(Optional) Configures a PIM VRF register message source address. You can configure a loopback interface as the source of the register messages.
Router(config)# <b>no ip pim vrf</b> <i>vrf_name</i> <b>register-source</b>	Disables IPv4 multicast VRF routing.

This example show how to configure a PIM VRF register message source address:

```
Router(config)# ip pim vrf blue register-source loopback 3
```

## Specifying the PIM VRF Rendezvous Point (RP) Address

To specify the PIM VRF RP address, perform this task:

Command or Action	Purpose
Router(config)# <b>ip pim vrf</b> <i>vrf_name</i> <b>rp-address</b> <i>rp_address</i> [ <i>access_list</i> ] [ <b>override</b> ] [ <b>bidir</b> ]	Specifies the PIM RP IPv4 address for a (required for sparse PIM networks):
Router(config)# <b>no ip pim vrf</b> <i>vrf_name</i> <b>rp-address</b> <i>rp_address</i>	Clears the PIM RP IPv4 address.

When specifying the PIM VRF RP address, note the following information:

- **vrf** *vrf\_name*—(Optional) Specifies a particular VRF instance to be used.
- *rp\_address*—Unicast IP address for the PIM RP router.

- *access\_list*—(Optional) Number or name of an access list that defines the multicast groups for the RP.
- **override**—(Optional) In the event of conflicting RP addresses, this particular RP overrides any RP that is learned through Auto-RP.
- **bidir**—(Optional) Specifies that the multicast groups specified by the *access\_list* argument are to operate in bidirectional mode. If this option is not specified, the groups operate in PIM sparse mode.
- Use bidirectional mode whenever possible, because it offers better scalability.

This example show how to specify the PIM VRF RP address:

```
Router(config)# ip pim vrf blue rp-address 198.196.100.33
```

## Configuring a Multicast Source Discovery Protocol (MSDP) Peer

To configure an MSDP peer, perform this task:

Command or Action	Purpose
Router(config)# <b>ip msdp vrf</b> <i>vrf_name</i> <b>peer</b> { <i>peer_name</i>   <i>peer_address</i> } [ <b>connect-source</b> <i>interface_type interface_number</i> ] [ <b>remote-as</b> <i>ASN</i> ]	(Optional) Configures an MSDP peer.
Router(config)# <b>no ip msdp vrf</b> <i>vrf_name</i> <b>peer</b> { <i>peer_name</i>   <i>peer_address</i> } [ <b>connect-source</b> <i>interface_type interface_number</i> ] [ <b>remote-as</b> <i>ASN</i> ]	Clears the PIM RP IPv4 address.

When configuring an MSDP peer, note the following information:

- **vrf** *vrf\_name*—Specifies a particular VRF instance to be used.
- {*peer\_name* | *peer\_address*}—Domain Name System (DNS) name or IP address of the MSDP peer router.
- **connect-source** *interface\_type interface\_number*—Interface name and number for the interface whose primary address is used as the source IP address for the TCP connection.
- **remote-as** *ASN*—(Optional) Autonomous system number of the MSDP peer. This is for display-only purposes.

This example show how to configure an MSDP peer:

```
Router(config)# ip msdp peer router.cisco.com connect-source fastethernet 1/1 remote-as 109
```

## Enabling IPv4 Multicast Header Storage

To enable IPv4 multicast header storage, perform this task:

Command or Action	Purpose
Router(config)# <b>ip multicast vrf</b> <i>vrf_name</i> <b>cache-headers</b> [ <b>rtp</b> ]	(Optional) Enables a circular buffer to store IPv4 multicast packet headers.
Router(config)# <b>no ip multicast vrf</b> <i>vrf_name</i> <b>cache-headers</b> [ <b>rtp</b> ]	Disables IPv4 multicast header storage.

When enabling IPv4 multicast header storage, note the following information:

- **vrf vrf\_name**—Allocates a buffer for the specified VRF.
- **rtp**—(Optional) Also caches Real-Time Transport Protocol (RTP) headers.
- The buffers can be displayed with the **show ip mpacket** command.

This example show how to enable IPv4 multicast header storage:

```
Router(config)# ip multicast vrf blue cache-headers
```

## Configuring the Maximum Number of Multicast Routes

To configure the maximum number of multicast routes, perform this task:

Command or Action	Purpose
Router(config)# <b>ip multicast vrf vrf_name route-limit limit [threshold]</b>	(Optional) Configures the maximum number of multicast routes that can be added for multicast traffic.
Router(config)# <b>no ip multicast vrf vrf_name route-limit limit [threshold]</b>	Clears the configured maximum number of routes.

When configuring the maximum number of routes, note the following information:

- **vrf vrf\_name**— Enables route limiting for the specified VRF.
- **limit**—The number of multicast routes that can be added. The range is from 1 to 2147483647, with a default of 2147483647.
- **threshold**—(Optional) Number of multicast routes that can be added before a warning message occurs. The valid range is from 1 to the value of the *limit* parameter.

This example show how to configure the maximum number of multicast routes:

```
Router(config)# ip multicast vrf blue route-limit 200000 20000
```

## Configuring IPv4 Multicast Route Filtering

To configure IPV4 multicast route filtering, perform this task:

Command or Action	Purpose
Router(config)# <b>ip multicast mrimfo-filter access_list</b>	(Optional) Configures IPV4 multicast route filtering with an access list. The <i>access_list</i> parameter can be the name or number of a access list.
Router(config)# <b>no ip multicast mrimfo-filter</b>	Clears the configured maximum number of routes.

This example show how to configure IPV4 multicast route filtering:

```
Router(config)# ip multicast mrimfo-filter 101
```

## Sample Configuration

The following excerpt from a configuration file shows the minimum configuration that is needed to support multicast routing for a range of VRFs. To simplify the display, only the starting and ending VRFs are shown.

```
!
```

```

ip multicast-routing
ip multicast-routing vrf lite
ip multicast-routing vrf vpn201
ip multicast-routing vrf vpn202

...

ip multicast-routing vrf vpn249
ip multicast-routing vrf vpn250
ip multicast cache-headers

...

ip pim rp-address 192.0.1.1
ip pim vrf lite rp-address 104.1.1.2
ip pim vrf vpn201 rp-address 192.200.1.1
ip pim vrf vpn202 rp-address 192.200.2.1

...

ip pim vrf vpn249 rp-address 192.200.49.6
ip pim vrf vpn250 rp-address 192.200.50.6
...

```

## Displaying IPv4 Multicast VRF Routing Information

To display the known PIM neighbors for a particular MVRF, use the **show ip pim vrf neighbor** command:

```
Router# show ip pim vrf 98 neighbor
```

```

PIM Neighbor Table
Neighbor      Interface      Uptime/Expires    Ver    DR
Address                               Prio/Mode
40.60.0.11    Tunnel96       00:00:31/00:01:13 v2      1 / S
40.50.0.11    Tunnel96       00:00:54/00:00:50 v2      1 / S

```

```
Router#
```

## Configuring Interfaces for Multicast Routing to Support MVPN

These sections describe how to configure interfaces for multicast routing to support MVPN:

- [Multicast Routing Configuration Overview, page 27-20](#)
- [Configuring PIM on an Interface, page 27-21](#)
- [Configuring an Interface for IPv4 VRF Forwarding, page 27-22](#)
- [Sample Configuration, page 27-22](#)

## Multicast Routing Configuration Overview

Protocol Independent Multicast (PIM) must be configured on all interfaces that are being used for IPv4 multicast traffic. In a VPN multicast environment, you should enable PIM on at least all of the following interfaces:

- Physical interface on a provider edge (PE) router that is connected to the backbone.
- Loopback interface that is used for BGP peering.

- Loopback interface that is used as the source for the sparse PIM rendezvous point (RP) router address.

In addition, you must also associate MVRFs with those interfaces over which they are going to forward multicast traffic.

BGP should be already configured and operational on all routers that are sending or receiving multicast traffic. In addition, BGP extended communities must be enabled (using the **neighbor send-community both** or **neighbor send-community extended** command) to support the use of MDTs in the network.

## Configuring PIM on an Interface

To configure PIM on an interface, perform this task:

	Command or Action	Purpose
Step 1	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 2	Router(config)# <b>interface</b> <i>type {slot/port   number}</i>	Enters interface configuration mode for the specified interface.
Step 3	Router(config-if)# <b>ip pim {dense-mode   sparse-mode   sparse-dense-mode}</b>	Enables PIM on the interface.
	Router(config)# <b>no ip pim {dense-mode   sparse-mode   sparse-dense-mode}</b>	Disables PIM.

When configuring PIM on an interface, note the following information:

- You can use one of these interface types:
  - A physical interface on a provider edge (PE) router that is connected to the backbone.
  - A loopback interface that is used for BGP peering.
  - A loopback interface that is used as the source for the sparse PIM network rendezvous point (RP) address.
- These are the PIM modes:
  - **dense-mode**—Enables dense mode of operation.
  - **sparse-mode**—Enables sparse mode of operation.
  - **sparse-dense-mode**—Enables sparse mode if the multicast group has an RP router defined, or enables dense mode if an RP router is not defined.
- Use **sparse-mode** for the physical interfaces of all PE routers that are connected to the backbone, and on all loopback interfaces that are used for BGP peering or as the source for RP addressing.

This example shows how to configure PIM sparse mode on a physical interface:

```
Router# configure terminal
interface gigabitethernet 10/1
Router(config-if)# ip pim sparse-mode
```

This example shows how to configure PIM sparse mode on a loopback interface:

```
Router# configure terminal
Router(config)# interface loopback 2
Router(config-if)# ip pim sparse-mode
```

## Configuring an Interface for IPv4 VRF Forwarding

To configure an interface for IPv4 VRF forwarding, perform this task:

Command or Action	Purpose
Router(config-if)# <b>ip vrf forwarding</b> <i>vrf_name</i>	(Optional) Associates the specified VRF routing and forwarding tables with the interface. If this is not specified, the interface defaults to using the global routing table.  <b>Note</b> Entering this command on an interface removes the IP address, so reconfigure the IP address.
Router(config-if)# <b>no ip vrf forwarding</b> [ <i>vrf_name</i> ]	Disables IPv4 VRF forwarding.

This example shows how to configure the interface for VRF blue forwarding:

```
Router(config-if)# ip vrf forwarding blue
```

## Sample Configuration

The following excerpt from a configuration file shows the interface configuration, along with the associated MVRP configuration, to enable multicast traffic over a single MVRP:

```
ip multicast-routing vrf blue
ip multicast-routing

ip vrf blue
rd 100:27
route-target export 100:27
route-target import 100:27
mdt default 239.192.10.2

interface GigabitEthernet1/1
description blue connection
ip vrf forwarding blue
ip address 192.168.2.26 255.255.255.0
ip pim sparse-mode

interface GigabitEthernet1/15
description Backbone connection
ip address 10.8.4.2 255.255.255.0
ip pim sparse-mode

ip pim vrf blue rp-address 192.7.25.1
ip pim rp-address 10.1.1.1
```

## Sample Configurations for MVPN

This section contains the following sample configurations for the MVPN feature:

- [MVPN Configuration with Default MDTs Only, page 27-23](#)
- [MVPN Configuration with Default and Data MDTs, page 27-24](#)

## MVPN Configuration with Default MDTs Only

The following excerpt from a configuration file shows the lines that are related to the MVPN configuration for three MVRFs. (The required BGP configuration is not shown.)

```
!  
version 12.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
service compress-config  
!  
hostname MVPN Router  
!  
boot system flash slot0:  
logging snmp-authfail  
!  
ip subnet-zero  
!  
!  
no ip domain-lookup  
ip host tftp 223.255.254.238  
!  
ip vrf mvpn-cus1  
  rd 200:1  
  route-target export 200:1  
  route-target import 200:1  
  mdt default 239.1.1.1  
!  
ip vrf mvpn-cus2  
  rd 200:2  
  route-target export 200:2  
  route-target import 200:2  
  mdt default 239.1.1.2  
!  
ip vrf mvpn-cus3  
  rd 200:3  
  route-target export 200:3  
  route-target import 200:3  
  mdt default 239.1.1.3  
!  
ip multicast-routing  
ip multicast-routing vrf mvpn-cus1  
ip multicast-routing vrf mvpn-cus2  
ip multicast-routing vrf mvpn-cus3  
ip multicast multipath  
frame-relay switching  
mpls label range 4112 262143  
mpls label protocol ldp  
mpls ldp logging neighbor-changes  
mpls ldp explicit-null  
mpls traffic-eng tunnels  
tag-switching tdp discovery directed-hello accept from 1  
tag-switching tdp router-id Loopback0 force  
ip multicast hardware-switching replication-mode ingress  
mls ip multicast flow-stat-timer 9  
mls ip multicast bidir gm-scan-interval 10  
mls flow ip destination  
no mls flow ipv6  
mls rate-limit unicast cef glean 10 10  
mls qos  
mls cef error action freeze
```

```

...

vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 2001-2101,3501-3700,4001,4051-4080,4093
!
!
!
interface Loopback0
 ip address 201.252.1.14 255.255.255.255
 ip pim sparse-dense-mode
!
interface Loopback1
 ip address 209.255.255.14 255.255.255.255
!
interface Loopback10
 ip vrf forwarding mvpn-cus1
 ip address 210.101.255.14 255.255.255.255
!
interface Loopback11
 ip vrf forwarding mvpn-cus1
 ip address 210.111.255.14 255.255.255.255
 ip pim sparse-dense-mode
!
interface Loopback12
 ip vrf forwarding mvpn-cus1
 ip address 210.112.255.14 255.255.255.255
...
!
interface GigabitEthernet3/3
 mtu 9216
 ip vrf forwarding mvpn-cus3
 ip address 172.10.14.1 255.255.255.0
 ip pim sparse-dense-mode
!
...
!
interface GigabitEthernet3/19
 ip vrf forwarding mvpn-cus2
 ip address 192.16.4.1 255.255.255.0
 ip pim sparse-dense-mode
 ip igmp static-group 229.1.1.1
 ip igmp static-group 229.1.1.2
 ip igmp static-group 229.1.1.4
!
interface GigabitEthernet3/20
 ip vrf forwarding mvpn-cus1
 ip address 192.16.1.1 255.255.255.0
 ip pim sparse-dense-mode
!
...

```

## MVPN Configuration with Default and Data MDTs

The following sample configuration includes three MVRFs that have been configured for both default and data MDTs. Only the configuration that is relevant to the MVPN configuration is shown.

```

...
!
ip vrf v1
 rd 1:1

```



```
route-target export 1:1
route-target import 1:1
mdt default 226.1.1.1
mdt data 226.1.1.128 0.0.0.7 threshold 1
!
ip vrf v2
rd 2:2
route-target export 2:2
route-target import 2:2
mdt default 226.2.2.1
mdt data 226.2.2.128 0.0.0.7
!
ip vrf v3
rd 3:3
route-target export 3:3
route-target import 3:3
mdt default 226.3.3.1
mdt data 226.3.3.128 0.0.0.7
!
ip vrf v4
rd 155.255.255.1:4
route-target export 155.255.255.1:4
route-target import 155.255.255.1:4
mdt default 226.4.4.1
mdt data 226.4.4.128 0.0.0.7
!
ip multicast-routing
ip multicast-routing vrf v1
ip multicast-routing vrf v2
ip multicast-routing vrf v3
ip multicast-routing vrf v4
mpls label protocol ldp
mpls ldp logging neighbor-changes
tag-switching tdp router-id Loopback1
ip multicast hardware-switching replication-mode ingress
mls ip multicast bidir gm-scan-interval 10
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
!
!
!
!
...
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
interface Loopback1
ip address 155.255.255.1 255.255.255.255
ip pim sparse-mode
!
interface Loopback4
ip vrf forwarding v4
ip address 155.255.4.4 255.255.255.255
ip pim sparse-mode
!
interface Loopback11
ip vrf forwarding v1
ip address 155.255.255.11 255.255.255.255
ip pim sparse-dense-mode
!
interface Loopback22
```

```

ip vrf forwarding v2
ip address 155.255.255.22 255.255.255.255
ip pim sparse-mode
!
interface Loopback33
ip vrf forwarding v3
ip address 155.255.255.33 255.255.255.255
ip pim sparse-mode
!
interface Loopback44
no ip address
!
interface Loopback111
ip vrf forwarding v1
ip address 1.1.1.1 255.255.255.252
ip pim sparse-dense-mode
ip ospf network point-to-point
!
interface GigabitEthernet1/1
description Gi1/1 - 155.50.1.155 255.255.255.0 - peer dut50 - mpls
mtu 9216
ip address 155.50.1.155 255.255.255.0
ip pim sparse-mode
tag-switching ip
!
interface GigabitEthernet1/2
ip vrf forwarding v1
ip address 155.1.2.254 255.255.255.0
ip pim sparse-mode
!
interface GigabitEthernet1/3
description Gi1/3 - 185.155.1.155/24 - vrf v1 stub peer 185.Gi1/3
ip vrf forwarding v1
ip address 185.155.1.155 255.255.255.0
ip pim sparse-mode
!
...

!
interface GigabitEthernet1/48
ip vrf forwarding v1
ip address 157.155.1.155 255.255.255.0
ip pim bsr-border
ip pim sparse-dense-mode
!
interface GigabitEthernet6/1
no ip address
shutdown
!
interface GigabitEthernet6/2
ip address 9.1.10.155 255.255.255.0
media-type rj45
!
interface Vlan1
no ip address
shutdown
!
router ospf 11 vrf v1
router-id 155.255.255.11
log-adjacency-changes
redistribute connected subnets tag 155
redistribute bgp 1 subnets tag 155
network 1.1.1.0 0.0.0.3 area 155

```

```
network 155.255.255.11 0.0.0.0 area 155
network 155.0.0.0 0.255.255.255 area 155
network 157.155.1.0 0.0.0.255 area 0
!
router ospf 22 vrf v2
router-id 155.255.255.22
log-adjacency-changes
network 155.255.255.22 0.0.0.0 area 155
network 155.0.0.0 0.255.255.255 area 155
network 157.155.1.0 0.0.0.255 area 0
!
router ospf 33 vrf v3
router-id 155.255.255.33
log-adjacency-changes
network 155.255.255.33 0.0.0.0 area 155
!
router ospf 1
log-adjacency-changes
network 155.50.1.0 0.0.0.255 area 0
network 155.255.255.1 0.0.0.0 area 155
!
router bgp 1
bgp router-id 155.255.255.1
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 175.255.255.1 remote-as 1
neighbor 175.255.255.1 update-source Loopback1
neighbor 185.255.255.1 remote-as 1
neighbor 185.255.255.1 update-source Loopback1
!
address-family vpnv4
neighbor 175.255.255.1 activate
neighbor 175.255.255.1 send-community extended
neighbor 185.255.255.1 activate
neighbor 185.255.255.1 send-community extended
exit-address-family
!
address-family ipv4 vrf v4
no auto-summary
no synchronization
exit-address-family
!
address-family ipv4 vrf v3
redistribute ospf 33
no auto-summary
no synchronization
exit-address-family
!
address-family ipv4 vrf v2
redistribute ospf 22
no auto-summary
no synchronization
exit-address-family
!
address-family ipv4 vrf v1
redistribute ospf 11
no auto-summary
no synchronization
exit-address-family
!
ip classless
ip route 9.255.254.1 255.255.255.255 9.1.10.254
no ip http server
ip pim bidir-enable
```

```

ip pim rp-address 50.255.2.2 MCAST.MVPN.MDT.v2 override bidir
ip pim rp-address 50.255.3.3 MCAST.MVPN.MDT.v3 override bidir
ip pim rp-address 50.255.1.1 MCAST.MVPN.MDT.v1 override bidir
ip pim vrf v1 spt-threshold infinity
ip pim vrf v1 send-rp-announce Loopback11 scope 16 group-list MCAST.GROUP.BIDIR bidir
ip pim vrf v1 send-rp-discovery Loopback11 scope 16
ip pim vrf v1 bsr-candidate Loopback11 0
ip msdp vrf v1 peer 185.255.255.11 connect-source Loopback11
ip msdp vrf v1 cache-sa-state
!
!
ip access-list standard MCAST.ANYCAST.CE
permit 2.2.2.2
ip access-list standard MCAST.ANYCAST.PE
permit 1.1.1.1
ip access-list standard MCAST.BOUNDARY.VRF.v1
deny 226.192.1.1
permit any
ip access-list standard MCAST.GROUP.BIDIR
permit 226.192.0.0 0.0.255.255
ip access-list standard MCAST.GROUP.SPARSE
permit 226.193.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.BOUNDARY.DATA.MDT
deny 226.1.1.128
permit any
ip access-list standard MCAST.MVPN.MDT.v1
permit 226.1.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.MDT.v2
permit 226.2.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.MDT.v3
permit 226.3.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.RP.v4
permit 227.0.0.0 0.255.255.255
!
access-list 1 permit 226.1.1.1
access-list 2 deny 226.1.1.1
access-list 2 permit any
...

```

# IPv6 Multicast Virtual Private Network (MVPNv6)

To provide layer 3 multicast services to customers with multiple distributed sites, service providers need a secure and scalable mechanism to transmit multicast traffic across the service provider network. IPv4 Multicast VPN(MVPN) provides such services for IPv4 multicast traffic over a shared service provider backbone.

Since many service providers are migrating to IPv6, they also need the same services for IPv6 multicast traffic. IPv6 Multicast Virtual Private Network (MVPNv6) provides multiple VPN support that enables service providers to provide multicast enabled private IPv6 networks to their customers using the same IPv4 back bone. In MVPNv6 implementation, the IPv6 multicast traffic is carried over the same IPv4 based core network and hence both the IPv4 and IPv6 VPN traffic are carried over the same tunnels simultaneously. Effective with Cisco IOS release 15.2(4)S, MVPNv6 is supported on Cisco 7600 series routers.

## Restrictions for the MVPNv6 Feature

Following restrictions apply to MVPNv6 on the Cisco 7600 series routers:

- Support up to 8000 IPv6 routes in VRF.
- Support up to 60 multicast VRFs.
- For MVPNv6 support, MVPNv4 should co-exist.
- All core facing cards should be ES+ line cards.
- Point to Point GRE tunnel as output interface in VRF for MVPNv6 is not supported.
- Default Multicast Distribution Tree (MDT) and data MDT are supported.
- An IPv6 protocol inside a VRF should operate in ingress replication mode irrespective of the configured replication mode. IPv4 backbone can operate in both ingress and egress replication modes.
- Effective with Cisco IOS Release 15.3(1)S, if replication mode is Egress, the entries in v6-vrf lite is installed as Egress. Before this release, it was Ingress.
- MVRF with MDT default configured on IPv4 and IPv6 address families (dual stack) does not support SVI as core facing interface.

## Configurng MPVNv6

Configuring MVPNv6 includes the following procedures:

1. [Configuring Multicast VRF Instances on PE Routers](#)
2. [Configuring Multicast Routing](#)
3. [Configuring Multicast VRF Interfaces on PE Routers](#)
4. [Configuring Routing Protocols Between the PE and CE Routers](#)

**Note**

These configuration tasks assume that BGP is already configured and operational on all routers sending or receiving the multicast traffic. Additionally, BGP extended communities must be enabled (using the neighbor send-community both or neighbor send-community extended command) to support the use of MDTs in the network.

## Configuring Multicast VRF Instances on PE Routers

Complete these steps to configure Multicast VRFs on PE routers.

### Summary Steps

1. **enable**
2. **configure terminal**
3. **mls ipv6 vrf**
4. **vrf definition** *vrf-name*
5. **rd** *route-distinguisher*
6. **route-target** {import | export | both} *route-target-ext-community*
7. **exit**
8. **address-family ipv4**
9. **mdt default** *group\_address*
10. **mdt data** *group\_address wildcard\_bits* [**threshold** *threshold\_value*] [**list** *access\_list*]
11. **exit**
12. **address-family ipv6**
13. **mdt default** *group\_address*
14. **mdt data** *group\_address wildcard\_bits* [**threshold** *threshold\_value*] [**list** *access\_list*]
15. **exit**

### Detailed Steps

	Command	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router(config)# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>mls ipv6 vrf</b>  <b>Example:</b> Router(config)# mls ipv6 vrf	Enables IPv6 globally in a VRF.
<b>Step 4</b>	<b>vrf definition</b> <i>vrf-name</i>  <b>Example:</b> Router(config)# vrf definition vrf1	Configures a VPN VRF routing table and enters VRF configuration mode.
<b>Step 5</b>	<b>rd</b> <i>route-distinguisher</i>  <b>Example:</b> Router(config-vrf)# rd 100:1	Specifies the route distinguisher (RD) for a VRF.

	Command	Purpose
Step 6	<b>route-target {import   export   both}</b> <i>route-target-ext-community</i>  <b>Example:</b> Router(config-vrf)# route target import 100:10	Specifies the route target VPN extended communities for both IPv4 and IPv6.
Step 7	<b>exit</b>  <b>Example:</b> Router(config-vrf)# exit	Exits VRF configuration mode.
Step 8	<b>address-family ipv4</b>  <b>Example:</b> Router(config-vrf)# address-family ipv4	Enters address family configuration mode to configure a routing session using standard IPv4 address prefixes.
Step 9	<b>mdt default group_address</b>  <b>Example:</b> Router(config-vrf-af)# mdt default 232.1.1.1	Configures the default IPv4 MDT address.
Step 10	<b>mdt data group_address wildcard_bits [threshold threshold_value] [list access_list]</b>  <b>Example:</b> Router(config-vrf-af)# mdt data 232.20.24.1 0.0.0.0 threshold 10	<p>(Optional) Configures data MDTs for the specified range of multicast addresses.</p> <p><b>group_address</b> —Multicast group address. The address can range from 224.0.0.1 to 239.255.255.255, but cannot overlap the address that has been assigned to the default MDT.</p> <p><b>wildcard_bits</b> —Wildcard bitmask to be applied to the multicast group address to create a range of possible addresses. This allows you to limit the maximum number of data MDTs that each MVRF can support.</p> <p><b>threshold_value</b>—(Optional) Defines the threshold value in kilobits, at which multicast traffic should be switched from the default MDT to the data MDT. The threshold_value parameter can range from 1 to 4294967 kilobits.</p> <p><b>access_list</b>—(Optional) Specifies an access list name or number to be applied to this traffic.</p>
Step 11	<b>exit</b>  <b>Example:</b> Router(config-vrf-af)# exit	Exits address family configuration mode on this VRF.
Step 12	<b>address-family ipv6</b>  <b>Example:</b> Router(config-vrf)# address-family ipv6	Enters address family configuration mode for configuring routing sessions that use standard IPv6 address prefixes.
Step 13	<b>mdt default group_address</b>  <b>Example:</b> Router(config-vrf-af)# mdt-default 232.1.1.1	Configures the default MDT address.

	Command	Purpose
<b>Step 14</b>	<b>mdt data</b> <i>group_address wildcard_bits</i> [ <b>threshold</b> <i>threshold_value</i> ] [ <b>list</b> <i>access_list</i> ]  <b>Example:</b> Router(config-vrf-af)# mdt data 232.12.24.1 0.0.0.0 threshold 10	Configures data MDTs for the specified range of multicast addresses.
<b>Step 15</b>	<b>exit-address-family</b>  <b>Example:</b> Router(config-vrf-af)# exit-address-family	Exits address family configuration mode

## Configuring Multicast Routing

Complete these steps to configure multicast routing.

### Summary Steps

1. **configure terminal**
2. **ip multicast-routing**
3. **ip multicast-routing** [*vrf vrf-name*]
4. **ipv6 multicast-routing**
5. **ipv6 multicast-routing** [*vrf vrf-name*]
6. **exit**

### Detailed Steps

	Command	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Router(config)# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ip multicast-routing</b>  <b>Example:</b> Router(config)# ip multicast-routing	Enables IPv4 multicast routing.
<b>Step 3</b>	<b>ip multicast-routing vrf</b> <i>vrf-name</i>  <b>Example:</b> Router(config)# ip multicast-routing vrf blue	Enables IPv4 multicast routing for the Multicast VPN routing and forwarding (MVRP) instance.
<b>Step 4</b>	<b>ipv6 multicast-routing</b>  <b>Example:</b> Router(config)# ipv6 multicast-routing	Enables IPv6 multicast routing.



	Command	Purpose
Step 5	<b>ipv6 multicast-routing vrf</b> <i>vrf-name</i>  <b>Example:</b> Router(config)# ipv6 multicast-routing vrf blue	Enables IPv4 multicast routing for the Multicast VPN routing and forwarding (MVRF) instance.
Step 6	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits from the configuration mode.

## Configuring Multicast VRF Interfaces on PE Routers

Complete these steps to configure IPv6 Multicast VRF interfaces.

### Summary Steps

1. **interface** *type number*
2. **vrf forwarding** *vrf-name*
3. **bandwidth** *bandwidth-value*
4. **ip address** *ip-address*
5. **no ip redirects**
6. **no ip proxy-arp**
7. **ip pim sparse-dense-mode**
8. **delay** *tens-of-microseconds*
9. **ipv6 address** *ipv6-address link-local*
10. **ipv6 address** *ipv6-address/prefix*
11. **ipv6 pim**
12. **exit**
13. **ip pim rp-address** *ip-address*
14. **ipv6 pim vrf** *vrf-name rp-address ipv6-address*

### Detailed Steps

	Command	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Router(config)# configure terminal	Enters global configuration mode.
Step 2	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface GigabitEthernet 3/0/3	Specifies the interface to configure and enters interface configuration mode.  <ul style="list-style-type: none"> <li>• <b>type</b> - The type argument specifies the type of interface to be configured.</li> <li>• <b>number</b> - The number argument specifies the port, connector, or interface card number.</li> </ul>

	Command	Purpose
<b>Step 3</b>	<b>vrf forwarding</b> <i>vrf-name</i>  <b>Example:</b> Router(config-if)# vrf forwarding blue	Associates a VRF with the specified interface.
<b>Step 4</b>	<b>bandwidth</b> <i>bandwidth-value</i>  <b>Example:</b> Router(config-if)# bandwidth 1000	Specifies a bandwidth.
<b>Step 5</b>	<b>ip address</b> <i>ip-address mask</i>  <b>Example:</b> Router(config-if)# ip address 10.1.0.1 255.255.0.0	Configures an IPv4 address on the interface.
<b>Step 6</b>	<b>no ip redirects</b>  <b>Example:</b> Router(config-if)# no ip redirects	Disables sending redirect messages.
<b>Step 7</b>	<b>no ip proxy-arp</b>  <b>Example:</b> Router(config-if)# no ip proxy-arp	Disables proxy ARP on the interface.
<b>Step 8</b>	<b>ip pim sparse-mode</b>  <b>Example:</b> Router(config-if)# ip pim sparse-mode	Enables Protocol-Independent Multicast (PIM) on the interface.
<b>Step 9</b>	<b>delay</b> <i>tens-of-microseconds</i>  <b>Example:</b> Router(config-if) delay 1000	Sets a delay value for the interface.
<b>Step 10</b>	<b>ipv6 address</b> <i>ipv6-address link-local</i>  <b>Example:</b> Router(config-if)# ipv6 address FE80::20:1:1 link-local	Specifies a link local IPv6 address. This address is used instead of the link local address that is automatically configured when IPv6 is enabled on the interface.
<b>Step 11</b>	<b>ipv6 address</b> <i>ipv6-address/prefix</i>  <b>Example:</b> Router(config-if)# ipv6 address 20::1:1:1/64	Specifies an IPv6 address on the interface.
<b>Step 12</b>	<b>ipv6 pim</b>  <b>Example:</b> Router(config-if)# ipv6 pim	Enables PIM for IPv6.
<b>Step 13</b>	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	Exits the interface configuration mode.
<b>Step 14</b>	<b>ip pim rp-address</b> <i>ip-address</i>  <b>Example:</b> Router(config)# ip pim rp-address 11.11.11.11	Configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for multicast groups.
<b>Step 15</b>	<b>ipv6 pim vrf</b> <i>vrf-name</i> <b>rp-address</b> <i>ipv6-address</i>  <b>Example:</b> Router(config)# ipv6 pim vrf blue rp-address 20::1:1:1	Configures the IPv6 address of a PIM RP and associates with the MVRF instance.

## Configuring Routing Protocols Between the PE and CE Routers

Configure the PE router with the same routing protocol that the CE router uses. In this configuration, EIGRP is used as the routing protocol between PE and CE routers. Complete these steps to configure EIGRP as the routing protocol between PE and CE Routers.

### Summary Steps

1. **router bgp** *as-number*
2. **address-family ipv6 vrf** *vrf-name*
3. **redistribute connected**
4. **redistribute eigrp** *as-number*
5. **redistribute static**
6. **exit-address-family**

### Detailed Steps

	Command	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Router(config)# configure terminal	Enters global configuration mode.
Step 2	<b>router bgp</b> <i>as-number</i>  <b>Example:</b> Router(config)# router bgp 55	Specifies the number of an autonomous system that identifies the router to other BGP routers.
Step 3	<b>address-family ipv6 vrf</b> <i>vrf-name</i>  <b>Example:</b> Router(config-router)# address-family ipv6 vrf blue	Specifies the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.
Step 4	<b>redistribute connected</b>  <b>Example:</b> Router(config-router-af)# redistribute connected	Redistributes the directly connected networks to BGP.
Step 5	<b>redistribute eigrp</b> <i>as-number</i>  <b>Example:</b> Router(config-router-af)# redistribute eigrp 11	Redistributes the EIGRP routes into BGP.
Step 6	<b>redistribute static</b>  <b>Example:</b> Router(config-router-af)# redistribute static	Redistribute the static routes into BGP.

	Command	Purpose
Step 7	<b>exit-address-family</b>  <b>Example:</b> Router(config-router-af)# exit-address-family	Exits the address family configuration mode.
Step 8	<b>exit</b>  <b>Example</b> Router(config-router)# exit	Exits the BGP configuration mode.

## Configuration Examples

This example shows how to configure MVPNv6 on the Cisco 7600 series routers. In this example, EIGRP is used as the routing protocol between PE and CE routers.



### Note

These configuration tasks are based on the assumption that BGP is already configured and operational on all routers sending or receiving the multicast traffic.

```

Router> enable
Router# configure terminal
Router(config)# mls ipv6 vrf
Router(config)# vrf definition blue

Router(config-vrf)# rd 55:1111
Router(config-vrf)# route target export 55:1111
Router(config-vrf)# route target import 55:1111
Router(config-vrf)# address-family ipv4
Router(config-vrf-af)# mdt default 232.1.1.1
Router(config-vrf-af)# mdt data 232.20.24.1 0.0.0.0 threshold 10
Router(config-vrf-af)# exit
Router(config-vrf)# address-family ipv6
Router(config-vrf-af)# mdt default 232.1.1.1
Router(config-vrf-af)# mdt data 232.12.24.1 0.0.0.0 threshold 10
Router(config-vrf-af)# exit-address-family
Router(config-vrf)# exit
Router(config)# ip multicast-routing
Router(config)# ip multicast-routing vrf blue
Router(config)# ipv6 multicast-routing
Router(config)# ipv6 multicast-routing vrf blue
Router(config)# interface GigabitEthernet 3/0/3
Router(config-if)# vrf forwarding blue
Router(config-if)# bandwidth 1000
Router(config-if)# ip address 10.1.0.1 255.255.0.0

Router(config-if)# no ip redirects
Router(config-if)# ip pim sparse-mode
Router(config-if)# delay 100
Router(config-if)# ipv6 address FE80::20:1:1 link-local
Router(config-if)# ipv6 address 20::1:1:1/64
Router(config-if)# ipv6 pim
Router(config-if)# exit
Router(config)# ip pim rp-address 11.11.11.11
Router(config)# ipv6 pim vrf blue rp-address 20::1:1:1
Router(config)# router bgp 55
Router(config-router)# address-family ipv6 vrf blue
Router(config-router-af)# redistribute connected
Router(config-router-af)# redistribute eigrp 11
Router(config-router-af)# redistribute static
Router(config-router-af)# exit-address-family

```

```
Router(config-router)# exit
```

## Verifying MVPNv6 Configuration

Use these commands to verify the MVPNv6 configuration.

Command	Purpose
<b>show ipv6 pim vrf</b> <i>vrf-name</i> <b>neighbor</b>	Displays the PIM neighbors discovered.
<b>show ipv6 pim vrf</b> <i>vrf-name</i> <b>mdt</b>	Displays information about MDT data streams.
<b>show ipv6 mroute vrf</b> <i>vrf-name</i> <i>source-ip-address group-ip-address</i>	Displays the contents of the IPv6 multicast routing table.
<b>show ipv6 mfib vrf</b> <i>vrf-name source-ip-address</i> <i>group-address</i> <b>verbose</b>	Displays MFIB entries, forwarding interfaces, and traffic statistics.
<b>show ipv6 pim vrf</b> <i>vrf-name</i> <b>mdt send</b>	Displays the data MDT groups in use.
<b>show ipv6 pim vrf</b> <i>vrf-name</i> <b>mdt receive detail</b>	Displays the data multicast distribution tree MDT group mappings received from other PE routers.

