Configuring Multicast VPN

The Multicast VPN (MVPN) feature provides the ability to support multicast over a Layer 3 VPN. As enterprises extend the reach of their multicast applications, service providers can accommodate these enterprises over their Multiprotocol Label Switching (MPLS) core network. IP multicast is used to stream video, voice, and data to an MPLS VPN network core.

Historically, point-to-point tunnels were the only way to connect through a service provider network. Although such tunneled networks tend to have scalability issues, they represented the only means of passing IP multicast traffic through a VPN.

Because Layer 3 VPNs support only unicast traffic connectivity, deploying MPLS in conjunction with a Layer 3 VPN allows service providers to offer both unicast and multicast connectivity to Layer 3 VPN customers.

Prerequisites for Configuring Multicast VPN

Enable IP multicast and configure the PIM interfaces using the tasks described in the “Configuring Basic IP Multicast” module.

Restrictions for Configuring Multicast VPN

- Byte Count information is not displayed in the OIF stats when using **show platform hardware multicast ipv4/ipv6** <*group*> <*source*> command on the Cisco ASR 903 RSP3 module.
- Unicast and Multicast stats counters do not match for triggers that lead to modifications in MLDP programming. This is noticed on MLDP, for any counters.
  - There are two separate counters counting the same packets (with a single counter there is no reference to compare).
  - With more counters, the load on the counter thread is increased and also the difference adds up.

Following are the triggers that are applicable:

- root_node_switchover
- p2mp_mdt_flap
- clear_mldp_nbr
- clear_bgp
- clear_ip_vrf_route
- clear_ip_route
- OSPF_shut_noshut
- core_loopback_intf_flap
- vrf_loopback_intf_flap
- core_loopback_default_add
- core_intf_flap
- Toggle_access_mcast_routing
- bud_node_OSPF_reconverge

- The update source interface for the Border Gateway Protocol (BGP) peerings must be the same for all BGP peerings configured on the router in order for the default multicast distribution tree (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.
- MVPN does not support multiple BGP peering update sources.
- Multiple BGP update sources are not supported and configuring them can break MVPN reverse path forwarding (RPF) checking. The source IP address of the MVPN tunnels is determined by the highest IP address used for the BGP peering update source. If this IP address is not the IP address used as the BGP peering address with the remote provider edge (PE) router, MVPN will not function properly.
- PIM Dense mode is not supported on core network.
- Extra traffic is noticed when the router acts as MVPN PE without any receivers attached. It is recommended to create an ACL and attach it to VRF to drop extra forwarded packets.
- A maximum of 20 multicast VRFs are supported.
- A maximum of 255 OIFs are supported.
- Generic Routing Encapsulation (GRE) based Multicast VPN (MVPN) is supported on RSP2 for IPv4 from Cisco IOS XE Release 3.17.0S onwards. MVPN GRE is supported only in video template.

Effective Cisco IOS XE Everest 16.5.1, the following restrictions are applicable on the Cisco ASR 900 RSP2 Module: :

- The transmission and receive (Tx and Rx) SPAN are not supported on provider edge (PE) routers configured with MVPN GRE.
- Only single encapsulation per core per WAN interface can be used.

- MVPN GRE with BDI interfaces in core is supported.
- In case of sparse mode (SM) in VRF, rendezvous point (RP) must be in ENCAP PE.
- IPv6 is not supported on MVPN GRE.
- MVPN GRE and mLDP cannot be configured on the same VRF.

Effective Cisco IOS XE Everest 16.6.1, the following restrictions are applicable on the Cisco ASR 900 RSP3 Module:

- MVPN bidirectional PIM is not supported.
- The following GREs are not supported:
  - Routing field
  - Sequence number
  - Scrict source number
  - Recursion Control Field
  - Checksum
- MVPN with core interface pseudowire is not supported.
- A maximum of 20 OIFs towards core are supported.
- IPv6 is not supported.
- Route leaking is not supported.
- Only one EFP per BDI per physical port is supported.
- MVPN GREs and mLDPs are not supported on the same VRF.
- NETCONF/YANG is not supported.
- In case of sparse mode (SM) in VRF, rendezvous point (RP) must be in ENCAP PE. This restriction is applicable on Cisco RSP3 module only.

Note This restriction is not applicable on Cisco IOS XE Amsterdam 17.3.1 and later releases.

- The following table shows the scaling numbers for MVPN-GRE:
- ***Table 1: Scaling Numbers for MVPN-GRE***

Scale Scenario	RSP1A	RSP1B	RSP2	RSP3
Number of supported data MDT per VRF	255	255	255	255

Scale Scenario	RSP1A	RSP1B	RSP2	RSP3
Number of supported data MDT overall	1000	1000	1000	Overall 4000. No restriction for data MDT.
Number of supported mroutes	SM-500 SSM-1000	SM-2000 SSM-4000	SM-1000 SSM-2000	4000
Number of VRF supported	20	20	20	20

- When PIM is enabled on ingress PE with ASM traffic for dual-homes GRE MVPN, packets are duplicated on the egress PEs. This limitation is also applicable when assert winner ingress PE is different from the ingress PE through which the traffic is forwarded to the egress PE. This is only applicable to Cisco RSP2 module.

Information About Configuring Multicast VPN

Multicast VPN Operation

MVPN IP allows a service provider to configure and support multicast traffic in an MPLS VPN environment. This feature supports routing and forwarding of multicast packets for each individual VRF instance, and it also provides a mechanism to transport VPN multicast packets across the service provider backbone.

A VPN is network connectivity across a shared infrastructure, such as an ISP. Its function is to provide the same policies and performance as a private network, at a reduced cost of ownership, thus creating many opportunities for cost savings through operations and infrastructure.

An MVPN allows an enterprise to transparently interconnect its private network across the network backbone of a service provider. The use of an MVPN to interconnect an enterprise network in this way does not change the way that enterprise network is administered, nor does it change general enterprise connectivity.

Benefits of Multicast VPN

- Provides a scalable method to dynamically send information to multiple locations.
- Provides high-speed information delivery.
- Provides connectivity through a shared infrastructure.

Multicast VPN Routing and Forwarding and Multicast Domains

MVPN introduces multicast routing information to the VPN routing and forwarding table. When a provider edge (PE) device receives multicast data or control packets from a customer edge (CE) router, forwarding is performed according to the information in the Multicast VPN routing and forwarding instance (MVRF). MVPN does not use label switching.

A set of MVRFs that can send multicast traffic to each other constitutes a multicast domain. 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

MVPN establishes a static default MDT for each multicast domain. The default MDT defines the path used by PE routers to send multicast data and control messages to every other PE router in the multicast domain.

If Source Specific Multicast (SSM) is used as the core multicast routing protocol, then the multicast IP addresses used for the default and data multicast distribution tree (MDT) must be configured within the SSM range on all PE routers.

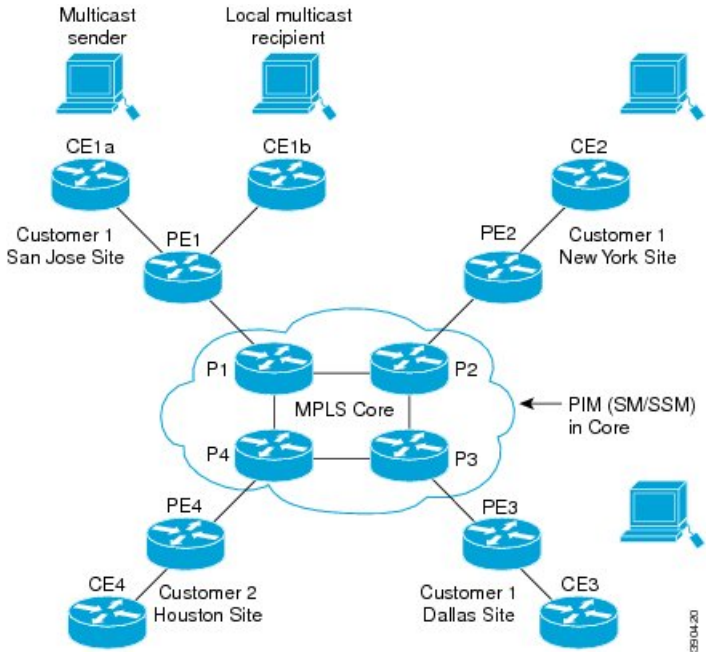
MVPN also supports the dynamic creation of MDTs for high-bandwidth transmission. Data MDTs are a feature unique to Cisco IOS software. Data MDTs are intended for high-bandwidth sources such as full-motion video inside the VPN to ensure optimal traffic forwarding in the MPLS VPN core. The threshold at which the data MDT is created can be configured on a per-router or a per-VRF basis. When the multicast transmission exceeds the defined threshold, the sending PE router creates the data MDT and sends a User Datagram Protocol (UDP) message, which contains information about the data MDT to all routers on the default MDT. The statistics to determine whether a multicast stream has exceeded the data MDT threshold are examined once every second. After a PE router sends the UDP message, it waits 3 more seconds before switching over; 13 seconds is the worst case switchover time and 3 seconds is the best case.

Data MDTs are created only for (S, G) multicast route entries within the VRF multicast routing table. They are not created for (*, G) entries regardless of the value of the individual source data rate.

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

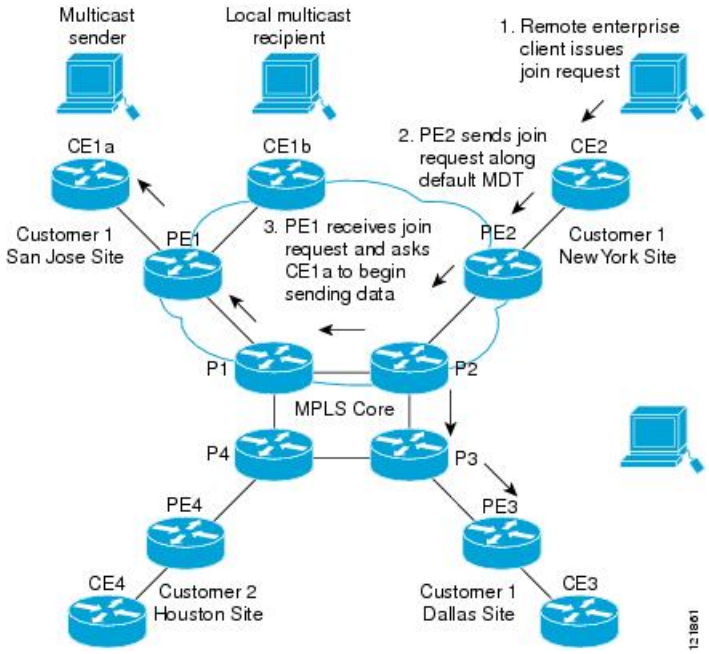
The default MDT for the enterprise customer consists of provider routers P1, P2, and P3 and their associated PE routers. PE4 is not part of the default MDT, because it is associated with a different customer. The figure shows that no data flows along the default MDT, because no one outside of San Jose has joined the multicast.

Figure 1: Default Multicast Distribution Tree Overview



An employee in New York joins the multicast session. The PE router associated with the New York site sends a join request that flows across the default MDT for the multicast domain of the customer. PE1, the PE router associated with the multicast session source, receives the request. The figure depicts that the PE router forwards the request to the CE router associated with the multicast source (CE1a).

Figure 2: Initializing the Data MDT



The CE router (CE1a) begins to send the multicast data to the associated PE router (PE1), which sends the multicast data along the default MDT. Through default MDT, traffic from CE1a is sent to all the PEs. Immediately sending the multicast data, PE1 recognizes that the multicast data exceeds the bandwidth threshold for which a data MDT should be created. Therefore, PE1 creates a data MDT, sends a message to all routers using the default MDT that contains information about the data MDT, and, three seconds later, begins sending the multicast data for that particular stream using the data MDT. Only PE2 has interested receivers for this source, so only PE2 will join the data MDT and receive traffic on it.

The other PE routers also receive traffic from the default MDT.

PE routers maintain a PIM relationship with other PE routers over the default MDT and a PIM relationship with its directly attached PE routers.

Multicast Tunnel Interface

An MVRF, which is created per multicast domain, requires the device to create a tunnel interface from which all MVRF traffic is sourced. A multicast tunnel interface is an interface that the MVRF uses to access the multicast domain. It can be thought of as a conduit that connects an MVRF and the global MVRF. One tunnel interface is created per MVRF.

MDT Address Family in BGP for Multicast VPN

The **mdt** keyword has been added to the **address-family ipv4** command to configure an MDT address-family session. MDT address-family sessions are used to pass the source PE address and MDT group address to PIM using Border Gateway Protocol (BGP) MDT Subaddress Family Identifier (SAFI) updates.

BGP Advertisement Methods for Multicast VPN Support

In a single autonomous system, if the default MDT for an MVPN is using PIM sparse mode (PIM-SM) with a rendezvous point (RP), then PIM is able to establish adjacencies over the Multicast Tunnel Interface (MTI) because the source PE and receiver PE discover each other through the RP. In this scenario, the local PE (the source PE) sends register messages to the RP, which then builds a shortest-path tree (SPT) toward the source PE. The remote PE, which acts as a receiver for the MDT multicast group, then sends (*, G) joins toward the RP and joins the distribution tree for that group.

However, if the default MDT group is configured in a PIM Source Specific Multicast (PIM-SSM) environment rather than a PIM-SM environment, the receiver PE needs information about the source PE and the default MDT group. This information is used to send (S, G) joins toward the source PE to build a distribution tree from the source PE (without the need for an RP). The source PE address and default MDT group address are sent using BGP.

BGP Extended Community

When BGP extended communities are used, the PE loopback (source address) information is sent as a VPNv4 prefix using Route Distinguisher (RD) Type 2 (to distinguish it from unicast VPNv4 prefixes). The MDT group address is carried in a BGP extended community. Using a combination of the embedded source in the VPNv4 address and the group in the extended community, PE routers in the same MVRF instance can establish SSM trees to each other.

Note Prior to the introduction of MDT SAFI support, the BGP extended community attribute was used as an interim solution to advertise the IP address of the source PE and default MDT group before IETF standardization. A BGP extended community attribute in an MVPN environment, however, has certain limitations: it cannot be used in inter-AS scenarios (because the attribute is nontransitive), and it uses RD Type 2, which is not a supported standard and not supported effective with Cisco IOS Release 15.5(1)T and Cisco IOS Release 15.4(3)S.

BGP MDT SAFI

Cisco software releases that support the MDT SAFI, the source PE address and the MDT group address are passed to PIM using BGP MDT SAFI updates. The RD type has changed to RD type 0, and BGP determines the best path for the MDT updates before passing the information to PIM.

Note To prevent backward-compatibility issues, BGP allows the communication of the older style updates with peers that are unable to understand the MDT SAFI address family.

Cisco software releases that support the MDT SAFI, the MDT SAFI address family needs to be explicitly configured for BGP neighbors using the **address-family ipv4 mdt** command. Neighbors that do not support the MDT SAFI still need to be enabled for the MDT SAFI in the local BGP configuration. Prior to the introduction of the MDT SAFI, additional BGP configuration from the VPNv4 unicast configuration was not needed to support MVPN.

Because the new MDT SAFI does not use BGP route-target extended communities, the regular extended community methods to filter these updates no longer apply. As a result, the **match mdt-group** route-map configuration command has been added to filter on the MDT group address using access control lists (ACLs). These route maps can be applied—inbound or outbound—to the IPv4 MDT address-family neighbor configuration.

Automigration to the MDT SAFI

When migrating a Cisco IOS release to the MDT SAFI, existing VPNv4 neighbors will be automatically configured for the MDT SAFI upon bootup based on the presence of an existing default MDT configuration (that is, pre-MDT SAFI configurations will be automatically converted to an MDT SAFI configuration upon bootup). In addition, when a default MDT configuration exists and a VPNv4 neighbor in BGP is configured, a similar neighbor in the IPv4 MDT address family will be automatically configured.

Note Because there is no VRF configuration on route reflectors (RRs), automigration to the MDT SAFI will not be triggered on RRs. The MDT SAFI configuration, thus, will need to be manually configured on RRs. Having a uniform MDT transmission method will reduce processing time on the routers (because MDT SAFI conversion is not necessary).

Guidelines for Configuring the MDT SAFI

- We recommend that you configure the MDT SAFI on all routers that participate in the MVPN. Even though the benefits of the MDT SAFI are for SSM tree building, the MDT SAFI must also be configured when using MVPN with the default MDT group for PIM-SM. From the multicast point of view, the

MDT SAFI is not required for MVPN to work within a PIM-SM core. However, in certain scenarios, the new address family must be configured in order to create the MTI. Without this notification, the MTI would not be created and MVPN would not function (even with PIM-SM).

- For backward compatible sessions, extended communities must be enabled on all MDT SAFI peers. In a pure MDT SAFI environment, there is no need to configure extended communities explicitly for MVPN. However, extended communities will be needed for VPNv4 interior BGP (iBGP) sessions to relay the route-target. In a hybrid (MDT SAFI and pre-MDT SAFI) environment, extended communities must be configured to send the embedded source in the VPNv4 address and the MDT group address to MDT SAFI neighbors.

Guidelines for Upgrading a Network to Support the MDT SAFI

When moving from a pre-MDT SAFI to an MDT SAFI environment, the upmost care should be taken to minimize the impact to the MVPN service. The unicast service will not be affected, other than the outage due to the reload and recovery. To upgrade a network to support the MDT SAFI, we recommend that you perform the following steps:

1. Upgrade the PEs in the MVPN to a Cisco IOS release that supports the MDT SAFI. Upon bootup, the PE configurations will be automigrated to the MDT SAFI. For more information about the automigration to the MDT SAFI functionality, see Automigration to the MDT SAFI, on page 8 section.
2. After the PEs have been upgraded, upgrade the RRs and enable the MDT SAFI for all peers providing MVPN service. Enabling or disabling the MDT SAFI will reset the BGP peer relationship for all address families; thus, a loss of routing information may occur.

Note A multihomed BGP RR scenario, one of the RRs must be upgraded and configured last. The upgraded PEs will use this RR to relay MDT advertisements while the other RRs are being upgraded.

Supported Policy

The following policy configuration parameters are supported under the MDT SAFI:

- Mandatory attributes and well-known attributes, such as the AS-path, multiexit discriminator (MED), BGP local-pref, and next-hop attributes.
- Standard communities, community lists, and route maps.

How to Configure Multicast VPN

Configuring a Default MDT Group for a VRF

Perform this task to configure a default MDT group for a VRF.

The default MDT group must be the same group configured on all devices that belong to the same VPN. The source IP address will be the address used to source the BGP sessions.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing distributed** **Example:** `Device(config)# ip multicast-routing distributed`	Enables multicast routing.
Step 4	**ip multicast-routing vrf** *vrf-name* **distributed** **Example:** `Device(config)# ip multicast-routing vrf vrf1 distributed`	Supports the MVPN VRF instance.
Step 5	**ip vrf** *vrf-name* **Example:** `Device(config)# ip vrf vrf1`	Enters VRF configuration mode and defines the VPN routing instance by assigning a VRF name. See the Example: Configuring the MDT Address Family in BGP for Multicast VPN, on page 20 section for an alternate command.
Step 6	**mdt default** *group-address* **Example:** `Device(config-vrf)# mdt default 232.0.0.1`	Configures the multicast group address for the default MDT for a VRF. • A tunnel interface is created as a result of this command. • By default, the destination address of the tunnel header is the *group-address* value.

Configuring the MDT Address Family in BGP for Multicast VPN

Perform this task to configure an MDT address family session on PE devices to establish MDT peering sessions for MVPN.

Before you begin

Before MVPN peering can be established through an MDT address family, MPLS and Cisco Express Forwarding (CEF) must be configured in the BGP network and multiprotocol BGP on PE devices that provide VPN services to CE devices.

Note The following policy configuration parameters are not supported:

- Route-originator attribute
- Network Layer Reachability Information (NLRI) prefix filtering (prefix lists, distribute lists)
- Extended community attributes (route target and site of origin)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *as-number* **Example:** `Device(config)# router bgp 65535`	Enters router configuration mode and creates a BGP routing process.
Step 4	**address-family ipv4 mdt** **Example:** `Device(config-router)# address-family ipv4 mdt`	Enters address family configuration mode to create an IP MDT address family session.
Step 5	**neighbor** *neighbor-address* **activate** **Example:** `Device(config-router-af)# neighbor 192.168.1.1 activate`	Enables the MDT address family for this neighbor.
Step 6	**neighbor** *neighbor-address* **send-community** [**both** | **extended** | **standard**] **Example:** `Device(config-router-af)# neighbor 192.168.1.1 send-community extended`	Enables community and (or) extended community exchange with the specified neighbor.
Step 7	**exit** **Example:**	Exits address family configuration mode and returns to router configuration mode.

	Command or Action	Purpose
	`Device(config-router-af)# exit`	
Step 8	**address-family vpnv4** **Example:** `Device(config-router)# address-family vpnv4`	Enters address family configuration mode to create a VPNv4 address family session.
Step 9	**neighbor** *neighbor-address* **activate** **Example:** `Device(config-router-af)# neighbor 192.168.1.1 activate`	Enables the VPNv4 address family for this neighbor.
Step 10	**neighbor** *neighbor-address* **send-community** [**both** | **extended** | **standard**] **Example:** `Device(config-router-af)# neighbor 192.168.1.1 send-community extended`	Enables community and (or) extended community exchange with the specified neighbor.
Step 11	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and enters privileged EXEC mode.

Configuring the Data Multicast Group

A data MDT group can include a maximum of 256 multicast groups per VPN per VRF per PE device. Multicast groups used to create the data MDT group are dynamically chosen from a pool of configured IP addresses.

Before you begin

- Before configuring a default MDT group, the VPN must be configured for multicast routing as described in the "Configuring a Default MDT Group for a VRF" section.
- All access lists needed when using the tasks in this module should be configured prior to beginning the configuration task. For information about how to configure an access list, see the “Creating an IP Access List and Applying It to an Interface” module.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf** *vrf-name* **Example:** `Device(config)# ip vrf vrf1`	Enters VRF configuration mode and defines the VPN routing instance by assigning a VRF name. See the Example: Configuring MVPN and SSM, on page 20 section for an alternate command.
Step 4	**mdt data** *group-address-range wildcard-bits* [**threshold** *kbps*] [**list** *access-list*] **Example:** `Device(config-vrf)# mdt data 239.192.20.32 0.0.0.15 threshold 1`	Specifies a range of addresses to be used in the data MDT pool. • For the *group-address-range* and *wildcard-bits* arguments, specify a a multicast group address range. The range is from 224.0.0.1 to 239.255.255.255. Because the range of addresses used in the data MDT pool are multicast group addresses (Class D addresses), there is no concept of a subnet; therefore, you can use all addresses in the mask (wildcard) range that you specify for the *wildcard-bits* argument. • The threshold is in *kbps*. The range is from 1 through 4294967. • Use the optional **list** keyword and *access-list* argument to define the (S, G) MVPN entries to be used in a data MDT pool, which would further limit the creation of a data MDT pool to the particular (S, G) MVPN entries defined in the access list specified for the *access-list* argument
Step 5	**mdt log-reuse** **Example:** `Device(config-vrf)# mdt log-reuse`	(Optional) Enables the recording of data MDT reuse and generates a syslog message when a data MDT has been reused.
Step 6	**end** **Example:** `Device(config-vrf)# end`	Returns to privileged EXEC mode.

Configuring Multicast Routes and Information

Perform this task to limit the number of multicast routes that can be added in a device.

Before you begin

- Before configuring a default MDT group, the VPN must be configured for multicast routing as described in the "Configuring a Default MDT Group for a VRF" section.
- All access lists needed when using the tasks in this module should be configured prior to beginning the configuration task. For information about how to configure an access list, see the " Creating an IP Access List and Applying It to an Interface " module.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast vrf** *vrf-name* **route-limit** *limit* [*threshold*] **Example:** `Device(config)# ip multicast vrf cisco route-limit 500 50`	Sets the mroute limit and the threshold parameters.
Step 4	**ip multicast mrinfo-filter** *access-list* **Example:** `Device(config)# ip multicast mrinfo-filter 4`	Filters the multicast device information request packets for all sources specified in the access list.

Verifying Information for the MDT Default Group

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ip pim mdt bgp**

Example:

```
Device# show ip pim mdt bgp

MDT (Route Distinguisher + IPv4)              Router ID         Next Hop
  MDT group 238.2.2.0
   2:200:50.0.0.4                             0.0.0.0           0.0.0.0
  MDT group 239.1.1.1
   2:200:50.0.0.4                             50.0.0.4          50.0.0.4
```

Displays information about the BGP advertisement of the RD for the MDT default group.

Step 3 **show ip pim vrf** *vrf-name* **mdt history interval** *minutes*

Example:

```
Device# show ip pim vrf vrf1 mdt history interval 20

   MDT-data send history for VRF - vrf1 for the past 20 minutes
MDT-data group        Number of reuse
     10.9.9.8           3
     10.9.9.9           2
```

Displays the data MDTs that have been reused during the past configured interval.

Troubleshoot

The following are some troubleshooting tips for MVPN:

- Use the **show ip pim vrf neighbor** command to check that PE routers established a PIM neighbor relationship through the dynamic tunnel interface. If they did, then the Default MDT operates properly.
- If the Default MDT does not function, use the **show ip pim mdt bgp** command to check that loopbacks of remote PE routers participating in MVPN are known by the local router. If they are not, verify that PIM is enabled on interfaces used as a source of MP BGP sessions.

Verifying Information for the Data Multicast Group

Procedure

Step 1 **show ip pim** [**vrf** *vrf-name*] **mdt send**

Example:

```
Device# show ip pim vrf VPN_A mdt send

MDT-data send list for VRF: VPN_A
  (source, group)                     MDT-data group/num   ref_count
  (80.0.0.10, 232.1.1.1)              238.2.2.0            1
```

Displays detailed information about the MDT data group including MDT advertisements that the specified device has made.

Step 2 **show ip pim** [**vrf** *vrf-name*] **mdt receive**

Example:

```
Device# show ip pim vrf VPN_A mdt receive
Joined MDT-data [group/mdt number : source]  uptime/expires for VRF: VPN_A
 [238.2.2.0 : 50.0.0.4]  00:51:27/00:02:32
```

Displays detailed information about the MDT data group joined.

Verifying Information for the Multicast Routes

Procedure

Step 1 **show ip mroute**

Example:

```
Device# show ip mroute
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, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.1.1.1), 05:06:08/stopped, RP 0.0.0.0, flags: DCZ
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    TenGigabitEthernet0/2/0, Forward/Sparse-Dense, 01:08:04/stopped
    MVRF VPN_A, Forward/Sparse-Dense, 05:06:08/stopped

(50.0.0.4, 239.1.1.1), 01:04:27/00:01:31, flags: TZ
  Incoming interface: TenGigabitEthernet0/2/0, RPF nbr 60.0.0.3
  Outgoing interface list:
    MVRF VPN_A, Forward/Sparse-Dense, 01:04:27/stopped

(50.0.0.2, 239.1.1.1), 05:06:07/00:02:42, flags: T
  Incoming interface: Loopback50, RPF nbr 0.0.0.0
  Outgoing interface list:
    TenGigabitEthernet0/2/0, Forward/Sparse-Dense, 01:08:04/stopped

(*, 238.2.2.0), 00:52:26/stopped, RP 0.0.0.0, flags: DCZ
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
```

```
    TenGigabitEthernet0/2/0, Forward/Sparse-Dense, 00:52:26/stopped
    MVRF VPN_A, Forward/Sparse-Dense, 00:52:26/stopped

(*, 224.0.1.40), 05:09:15/00:02:47, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    TenGigabitEthernet0/2/0, Forward/Sparse-Dense, 01:08:04/stopped
    Loopback50, Forward/Sparse-Dense, 05:09:15/stopped
```

Displays the contents of the IP multicast routing table in the provider's core.

Step 2 **show ip mroute vrf** *vrf name*

Example:

```
Device# show ip mroute vrf VPN_A
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, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(80.0.0.10, 232.1.1.1), 00:53:04/00:02:59, flags: sTIY
  Incoming interface: Tunnel0, RPF nbr 50.0.0.4, MDT:238.2.2.0/00:02:55
  Outgoing interface list:
    BDI1101, Forward/Sparse-Dense, 00:53:04/00:02:59

(*, 224.0.1.40), 05:06:46/00:02:15, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 05:06:46/stopped
```

Displays the multicast routing table in the client's VRF.

Displaying Multicast Forwarding Counters

```
router#show ip mfib vrf test
Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
                ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
                MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
                MS  - MoFRR  Entry in Sync, MC - MoFRR entry in MoFRR Client.
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
```

```
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
VRF test
 (*,224.0.0.0/4) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
   BDI1101 Flags: NS
   Tunnel0, MDT/232.0.0.1 Flags: NS
 (*,224.0.1.40) Flags: C HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
   Tunnel0, MDT/232.0.0.1 Flags: F IC NS
     Pkts: 0/0
 (*,232.0.0.0/8) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
 (10.11.11.2,232.10.0.1) Flags: ET HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   571756659/1420644/68/754717, Other: 0/0/0
   BDI1101 Flags: A
   Tunnel0, MDT/232.5.1.0 Flags: F NS
     Pkts: 0/0
```

Displaying Per-Prefix Forwarding Counters for Native Multicast

Table 2: Feature History

Feature Name	Release	Description
Native Multicast SLA Measurement	Cisco IOS XE Amsterdam 17.3.1	Outgoing interface (OIF) statistics in a native multicast setup implements an extra output to include the packet count sent over the (S,G) entry and the traffic rate.

OIF stat in a native multicast setup implements an extra output to include the packet count sent over the (S,G) entry and the traffic rate.

- Per-prefix OIF stats are supported on BDI and routed interfaces on the RSP2 module
- Per-prefix OIF stats are supported only on BDI interface in the RSP3 module

```
router#show ip mfib 203.0.0.1
/* OIF Stats - BDI */
 (192.1.1.2,203.0.0.1) Flags: HW
   SW Forwarding: 1/0/1478/0, Other: 0/0/0
   HW Forwarding:   4983/34/1478/397, Other: 0/0/0
   BDI100 Flags: A
   BDI20 Flags: F NS
     Pkts: 5235/0/0    Rate: 34 pps

/* OIF Stats - Routerd port */
 (192.1.1.2,203.0.0.1) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   490/34/1478/397, Other: 0/0/0
   BDI100 Flags: A
   TenGigabitEthernet0/0/25 Flags: F NS
     Pkts: 584/0/0    Rate: 34 pps
```

Displaying Aggregate Interface Multicast Stats

Table 3: Feature History

Feature Name	Release	Description
Multicast SLA Measurment with MLDP	Cisco IOS XE Bengaluru 17.4.1	Display of aggregated egress multicast stats for BDI interfaces on Head node, which is part of the MLDP core is supported.
Aggregated Interface Statistics on Bundle	Cisco IOS XE Amsterdam 17.3.1	Aggregate multicast packet count is implemented for all the (S,G) entries for which the given BDI serves as the OIF.

Aggregate multicast statistics (packet count) is implemented for all the (S,G) entries for which the given BDI serves as the OIF.

For example, if the outgoing BDI is common for all the groups then the packets are aggregated. No SDM templates are required on the RSP2 module. But to view the aggregate BDI ingress stats on RSP3 module using the SDM template, use **enable_multicast_stats** command.

No tail-node aggregate BDI stats are supported (neither ingress nor egress) on the RSP3 module. Only aggregate BDI ingress stats is supported on the core-facing interface when the RSP2 module acts as 'Tail-Node' in a MLDP or Multicast VPN setup (no egress stats support).

Aggregate stats are supported only on BDI interfaces and are implemented as part of the output broadcast and output IP multicast packet counts.

Note From Cisco IOS XE Bengaluru 17.4.1 release, the Cisco RSP3 module, MLDP aggregated BDI egress stats is supported on the head node. Ingress stats is not supported. On the Cisco RSP3 module, MLDP aggregated BDI stats is not supported on Tail node.

```
Router# show interface bdi 103 | i broad
/* Send or Receive (native multicast) */
     Received 0 broadcasts (5 IP multicasts)
     Output 0 broadcasts (17153 IP multicasts)

Router# show interface bdi 102 | i broad
/* You grep for broad here because the output IP multicasts are present in the same line
*/
     Received 0 broadcasts (34356 IP multicasts)
     Output 0 broadcasts (41 IP multicasts)

/* BDI stats – Receive(MLDP Tail-Node) */

Router#show ip mfib vrf
MCAST 255.1.1.2
VRF MCAST
(*,255.1.1.2) Flags: C HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   1000/0/1478/0, Other: 0/0/0
   Lspvif29, LSM/C4, RPF-ID: *, Flags: A NS
   BDI25 Flags: F NS
     Pkts: 52/0/0    Rate: 5 pps
(10.1.1.2,255.1.1.2) Flags: HW
```

```
   SW Forwarding: 43/0/1478/0, Other: 0/0/0
   HW Forwarding:   1000/100/1478/1154, Other: 0/0/0
   Lspvif29, LSM/C4, RPF-ID: *, Flags: A
   BDI25 Flags: F NS
     Pkts: 1000/0/43    Rate: 100 pps

Router# show interface bdi 105
Received 0 broadcasts (1000 IP multicasts)
Output 0 broadcasts (11 IP multicasts)
```

Configuration Examples for Multicast VPN

Example: Configuring MVPN and SSM

In the following example, PIM-SSM is configured in the backbone. Therefore, the default and data MDT groups are configured within the SSM range of IP addresses. Inside the VPN, PIM-SM is configured and only Auto-RP announcements are accepted.

```
ip vrf vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 mdt default 232.0.0.1
 mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
!
ip pim ssm default
ip pim vrf vrf1 accept-rp auto-rp
```

In the following example, an alternate command is used to configure MVPN and SSM:

```
vrf definition vrf1
rd 101:1
route-target export 101:1
route-target import 101:1
!
address-family ipv4
mdt default 232.1.1.1
mdt data 232.5.1.1 0.0.0.255 threshold 500 list 101
exit-address-family
!
ip pim ssm default
ip pim vrf vrf1 accept-rp auto-rp
```

Example: Enabling a VPN for Multicast Routing

In the following example, multicast routing is enabled with a VPN routing instance named vrf1:

```
ip multicast-routing vrf vrf1 distributed
```

Example: Configuring the MDT Address Family in BGP for Multicast VPN

In the following example, an MDT address family session is configured on a PE router to establish MDT peering sessions for MVPN.

```
!
ip vrf test
 rd 55:2222
 route-target export 55:2222
 route-target import 55:2222
 mdt default 232.0.0.1
!
ip multicast-routing distributed
ip multicast-routing vrf test distributed
!
router bgp 55
.
.
.
!
 address-family vpnv4
 neighbor 192.168.1.1 activate
 neighbor 192.168.1.1 send-community both
!
 address-family ipv4 mdt
 neighbor 192.168.1.1 activate
 neighbor 192.168.1.1 send-community both
!
```

In the following example, an alternate command is used to configure an MDT address family session on a PE router to establish MDT peering sessions for MVPN:

```
vrf definition vrf1
rd 101:1
route-target export 101:1
route-target import 101:1
!
address-family ipv4
mdt default 232.1.1.1
.
.
.

ip multicast-routing distributed
ip multicast-routing vrf test distributed
!
router bgp 55
.
.
.
!
address-family vpnv4
neighbor 192.168.1.1 activate
neighbor 192.168.1.1 send-community both
!
address-family ipv4 mdt
neighbor 192.168.1.1 activate
neighbor 192.168.1.1 send-community both
```

Example: Configuring the Multicast Group Address Range for Data MDT Groups

In the following example, the VPN routing instance is assigned a VRF named VPN_A. The MDT default group for a VPN VRF is 239.1.1.1, and the multicast group address range for MDT groups is 239.2.2.0 with wildcard bits of 0.0.0.255:

```
ip vrf VPN_A
```

```
rd 2:200
route-target export 2:200
route-target import 2:200
mdt default 239.1.1.1
mdt data 239.2.2.0 0.0.0.255
```

The following is an alternate command to assign VRF to the VPN routing instance.

```
vrf definition VPN_A
rd 101:1
route-target export 101:1
route-target import 101:1
!
address-family ipv4
mdt default 232.1.1.1
mdt data 232.5.1.1 0.0.0.255 threshold 500 list 101
```

Example: Limiting the Number of Multicast Routes

In the following example, the number of multicast routes that can be added to a multicast routing table is set to 500 and the threshold value of the number of mroutes that will cause a warning message to occur is set to 50:

```
ip multicast route-limit 500 50
ip multicast vrf VPN_A route-limit 500 50
no mpls traffic-eng auto-bw timers
!
```

Example: Configuring MVPN on VRF

```
ip multicast-routing distributed
ip multicast-routing vrf VPN_A distributed
!

ip pim ssm default
ip pim vrf VPN_A ssm default
!

interface loopback50
ip address 50.0.0.2 255.255.255.255
ip pim sparse-dense-mode
ip ospf 1 area 0
exit
!
```

Example: Configuring Access-Interface

```
interface GigabitEthernet0/1/0
no ip address
negotiation auto
service instance 1101 ethernet
encapsulation dot1q 1101
rewrite ingress tag pop 1 symmetric
bridge-domain 1101
!
interface BDI1101
ip vrf forwarding VPN_A
ip address 40.0.0.2 255.255.255.0
```

```
ip pim sparse-dense-mode
ip igmp version 3
ip ospf 2 area 0
end
```

The following is an alternate method to configure a physical interface or BDI under specified VRF:

```
interface GigabitEthernet0/1/0
no ip address
negotiation auto
service instance 1101 ethernet
encapsulation dot1q 1101
rewrite ingress tag pop 1 symmetric
bridge-domain 1101
!
interface BDI1101
vrf forwarding VPN_A
ip address 40.0.0.2 255.255.255.0
ip pim sparse-dense-mode
ip igmp version 3
ip ospf 2 area 0
end
```

Example: Configuring Core Interfaces

```
interface ten 0/2/0
ip address 60.0.0.2 255.255.255.0
ip pim sparse-dense-mode
ip igmp version 3
ip ospf 1 area 0
end
```

Example: Configuring BGP

```
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 50.0.0.4 remote-as 100
neighbor 50.0.0.4 update-source Loopback50
!
address-family ipv4
neighbor 50.0.0.4 activate
exit-address-family

address-family vpnv4
neighbor 50.0.0.4 activate
neighbor 50.0.0.4 send-community extended
exit-address-family

address-family ipv4 mdt
neighbor 50.0.0.4 activate
neighbor 50.0.0.4 send-community extended
exit-address-family

address-family ipv4 vrf VPN_A
redistribute connected
redistribute static
redistribute ospf 2
exit-address-family
!
!
router ospf 2 vrf VPN_A
redistribute connected subnets
```

```
redistribute static subnets
redistribute bgp 100 subnets
exit
```

-

Multicast VPN over Routed Pseudowire

Routed Pseudowire and Virtual Private LAN Services (VPLS) configuration can route layer 3 traffic as well as layer 2 traffic for pseudowire connections between Provider Edge (PE) devices using VPLS multipoint PE. The ability to route frames to and from these interfaces supports termination of pseudowires into the layer 3 network (VPN or global) on the same switch, or to the tunnel layer 3 frames over a layer 2 tunnel (VPLS).

Limitations of Multicast VPN over Routed Pseudowire

- MVPN-GRE over routed pseudowire feature is supported from Cisco IOS XE Fuji 16.9.1 onwards.
- The update source interface for the Border Gateway Protocol (BGP) peerings must be the same for all BGP peerings configured on the router in order to configure the default Multicast Distribution Tree (MDT) accurately.
- If you use a loopback address for BGP peering, the PIM sparse mode must be enabled on the loopback address.
- Multiple BGP update sources are *not* supported and configuring them can break MVPN Reverse Path Forwarding (RPF) checking.
- PIM Dense mode is *not* supported on core network.
- IGMP snooping should be disabled in PE nodes for multicast to work over routed pseudowire.
- Only PIM-SSM is supported with MVPN-GRE over routed pseudowire.
- Only one PW under a VFI is supported.
- A maximum of 15 routed pseudowires are supported for MPVN-GRE over routed pseudowire.

Configuring Multicast VPN over Routed Pseudowire

To configure Multicast VPN over routed pseudowire:

```
enable
configure terminal
ip multicast-routing distributed
ip multicast-routing vrf vrf-name distributed
ip vrf cu1
mdt default 232.0.0.1
router bgp 100
address-family ipv4 mdt
neighbor 2.2.2.2 activate
exit
address-family vpnv4
neighbor 2.2.2.2 activate
ip vrf cu1
mdt data 232.0.0.5 0.0.0.0
```

```
mdt data threshold 1000
l2 vfi VPLS_A manual
vpn id 1000
bridge-domain 1000
neighbor 2.2.2.2 encapsulation mpls
interface bdi 1000
ip address 39.1.1.1 255.255.255.0
ip pim sparse-mode
ip ospf 1 area 0
```

Note MDT pools are multicast group addresses.

The range of threshold is from 1 to 4294967 kbps.

Use the optional list keyword and access-list argument to define the (S, G) MVPN entries to be used in a data MDT pool, which further limits the creation of a data MDT pool to the particular (S, G) MVPN entries defined in the access list specified for the access-list argument.

Verification of MVPN over Routed Pseudowire Configuration

Use **show ip igmp snooping** command to check IGMP snooping is disabled.

```
Router#show ip igmp snooping
Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping Oper State     : Disabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000
Check TTL=1                  : No
Check Router-Alert-Option    : No

Vlan 401:
--------
IGMP snooping Admin State           : Enabled
IGMP snooping Oper State            : Disabled
IGMPv2 immediate leave              : Disabled
Report suppression                  : Enabled
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
Check TTL=1                         : Yes
Check Router-Alert-Option           : Yes
```

Use **show ip pim neighbor** command to check core PIM response.

```
Router#show ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable,
      L - DR Load-balancing Capable
Neighbor          Interface               Uptime/Expires    Ver   DR
Address                                                           Prio/Mode
40.1.1.2          BDI3000                 05:55:07/00:01:23 v2    1 / DR S P G
39.1.1.2          BDI2000                 05:47:37/00:01:32 v2    1 / DR S P G
```

Use **show ip pim vrf** command to check the PIM neighbors in the VRF configured.

```
Router#show ip pim vrf VRF_101 ne
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable,
      L - DR Load-balancing Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
44.44.44.3        Tunnel0                  05:51:40/00:01:34 v2    1 / DR S P G
22.22.22.3        Tunnel0                  05:59:32/00:01:31 v2    1 / S P G
```

Use the **show ip mroute vrf** command to check the mroute entry in the VRF configured.

```
Router#show ip mroute vrf VRF_101
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, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group, c - PFP-SA cache created entry
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(50.1.1.2, 232.1.1.16), 05:47:24/00:02:47, flags: sTy
  Incoming interface: GigabitEthernet0/1/7, RPF nbr 21.1.1.2
  Outgoing interface list:
    Tunnel0, Forward/Sparse, 05:47:24/00:02:47
```

Use the **show ip mroute vrf** command to find the data MDT allocated for multicast group:

```
Router#show ip mroute vrf VRF_101 verbose

(50.1.1.2, 232.1.1.16), 05:49:25/00:03:29, flags: sTyp
  Incoming interface: GigabitEthernet0/1/7, RPF nbr 21.1.1.2
  Outgoing interface list:
    Tunnel0, GRE MDT: 232.5.101.31 (data), Forward/Sparse, 05:49:25/00:03:29, p
```

Use the **show mpls l2 vc** command to check if Pseudowire is up:

```
Router#show mpls l2 vc

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
VFI PE1-VPLS-A  \
               vfi                        2.2.2.2         3000       UP
VFI PE1-VPLS-B  \
               vfi                        4.4.4.4         2000       UP
```