Multicast Overlay Routing

Table 1: Feature History

Feature Name	Release Information	Description
Support for Multicast Overlay Routing Protocols	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature enables efficient distribution of one-to-many traffic. The multicast routing protocols like, IPv4 Multicast, IGMPv3, PIM SSM, PIM ASM, Auto RP, and Static RP distribute data (for example, audio/video streaming broadcasts) to multiple recipients. Using multicast overlay protocols, a source can send a single packet of data to a single multicast address, which is then distributed to an entire group of recipients.
Multicast over L3 TLOC Extension	Cisco IOS XE Release 17.3.2 Cisco vManage Release 20.3.1	This feature enables support for transport location (TLOC) which allows addition of the peers transport to avoid the extra cost of additional IP and allows the use of dynamic load balance across multiple transports.
Multicast Support for Hub and Spoke Topologies	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	This feature enables efficient distribution of traffic on edge devices using hub-and-spoke network topology. The multicast routing protocols like, IPv4 Multicast, IGMPv3, PIM SSM, PIM ASM, Auto RP, and Static RP distribute data to multiple recipients.

Information About Multicast Overlay Routing

The Cisco IOS XE Catalyst SD-WAN multicast overlay software extends Protocol Independent Multicast Source-Specific Multicast (PIM-SSM) over the Cisco Catalyst SD-WAN overlay using Overlay Management Protocol (OMP). Protocol Independent Multicast Sparse-Mode (PIM-SM) is deployed in the customer VPNs, and the Cisco IOS XE MVPN is used to integrate PIM in customer VPNs and OMP in the overlay. The OMP replicator is used in overlay multicast to optimize the multicast distribution tree across the overlay topology. The Cisco IOS XE Catalyst SD-WAN router supports IGMPv2 and IGMPv3 reports and advertises receiver's multicast interest to remote Cisco Catalyst SD-WAN routers using OMP. Depending on the level of optimization required, the Cisco Catalyst SD-WAN routers join or prune to or from the replicators, and replicators use OMP to relay the join or prune to the Cisco Catalyst SD-WAN router providing overlay connectivity to the PIM-RP or source.

The Cisco IOS XE Catalyst SD-WAN multicast overlay implementation extends native multicast by creating a secure optimized multicast tree that runs on top of the overlay network.

Multicast Overlay Supported Features

- IPv4 Overlay Multicast (PIM SSM)
- IPv4 Overlay Multicast (PIM ASM)
- PIM-RP on IOS XE VPN
- Replicator with geo-location (GPS)
- Static RP and Auto-RP
- PIM Bootstrap Router (BSR)
- IGMP v2, IGMP v3, and PIM on service side
- IPSec and GRE Encapsulation
- vEdge and IOS XE Catalyst SD-WAN Interop
- Overlay Multicast Signaling using OMP

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.3.2, TLOC extension with multicast and multicast application-aware route policy features are supported.

Restrictions for Multicast Overlay Routing

Multicast overlay routing does not support the following features:

- MSDP/Anycast-RP on Cisco Catalyst SD-WAN routers
- IPv6 overlay and IPv6 underlay
- Dynamic BFD tunnel for multicast
- Multicast with asymmetric unicast routing

- Multicast overlay working does not support Data Policy. In case data policy is configured, then only required traffic is matched and not multicast traffic.
- The Cisco vEdge device is used only as Last Hop Router (LHR), where as Cisco Catalyst SD-WAN devices can be used in all multicast roles (FHR, LHR, RP and Replicator roles).
- Bidirectional PIM is not supported with hub-and-spoke. It is not supported with full-mesh as well.
- On Cisco 1000 Series Integrated Services Routers, when IGMP snooping is enabled and there are no local receivers for multicast traffic in the VLAN, the multicast traffic floods to all ports in the VLAN.

Restrictions for Multicast Routing with Hub-and-Spoke Topology

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1

- You can configure multicast rendezvous point and replicator node on hub-site devices only. Replicator cannot be configured on spoke-site devices.
- MSDP interconnect feature is not supported with hub-and-spoke multicast deployment.
- You can configure multicast routing on hub-and-spoke using CLI add-on template only.
- On-demand tunnel between spoke sites is not supported with multicast.
- Multicast supported only with centralized control policy based hub-and-spoke deployment, intent based configuration as described in Hub-and-Spoke chapter is not supported.

Supported Protocols

The Cisco IOS XE Catalyst SD-WAN overlay multicast network supports the Protocol Independent Multicast (PIM) and Internet Group Management Protocol (IGMP) and multicast template configurations on all the platforms.

PIM

Cisco IOS XE Catalyst SD-WAN overlay multicast supports PIM version 2 (defined in RFC 4601), with some restrictions.

On the service side, the Cisco IOS XE Catalyst SD-WAN software supports native multicast. A router appears as a native PIM router and establishes PIM neighborship with other PIM routers at a local site. A Cisco IOS XE SD-WAN router supports a directly connected local source, referred as a first hop router (FHR). Receivers residing downstream of a router can join multicast streams by exchanging IGMP membership reports directly with the device, and no other routers are required. Additionally, the Cisco Catalyst SD-WAN router can act as the PIM-RP for the local site.

On the transport side, PIM-enabled Cisco IOS XE Catalyst SD-WAN routers originate multicast service routes (called multicast autodiscover routes), sending them using OMP to the Cisco Catalyst SD-WAN Controllers. The multicast autodiscover routes indicate whether the router is a replicator and the local threshold. Each PIM router also conveys information learned from the PIM join messages sent by local-site multicast-enabled routers, including multicast group state, source information, and RPs. These routes assist Cisco IOS XE Catalyst SD-WAN routers in performing optimized joins across the overlay when joining existing multicast sources.

Cisco IOS XE Catalyst SD-WAN routers support both PIM source-specific mode (SSM) and ASM (Any Source Multicast) mode.

Rendezvous Points

The root of a PIM multicast shared tree resides on a router configured to be a rendezvous point (RP). In the Cisco Catalyst SD-WAN solution, RPs can be Cisco Catalyst SD-WAN routers or non-Cisco Catalyst SD-WAN routers that reside in the local site.

Cisco IOS XE Catalyst SD-WAN supports the following modes of RP discovery:

- Static RP
- Auto-RP
- Auto-RP Proxy

Dynamic RP-group mappings are propagated in the Cisco IOS XE Catalyst SD-WAN solution using Auto-RP. ACLs can be used to control or map certain group ranges to a specific RP. With this information, each PIM router has the ability to forward joins to the correct RP for the group that a downstream IGMP client is attempting to join. Auto-RP updates are propagated to downstream PIM routers if such routers are present in the local site and across the overlay to the remote sites that belong to the same VPN. While using Auto-RP, Replicator Node should be configured as the Auto-RP mapping agent.

Another RP selection model called bootstrap router (BSR) was introduced after Auto-RP in PIM-SM version 2. Auto-RP is a Cisco proprietary protocol, whereas PIM BSR is part of the PIM version 2 specification. BSR performs similarly to Auto-RP in that it uses candidate routers for the RP function and for relaying the RP information for a group.

Replicators

For efficient use of WAN bandwidth, strategic Cisco IOS XE Catalyst SD-WAN routers can be deployed and configured as replicators throughout the overlay network. Replicators mitigate the requirement for a Cisco Catalyst SD-WAN router with local sources or the PIM-RP to replicate a multicast stream once for each receiver. As discussed above, replicators advertise themselves, using OMP multicast-autodiscover routes, to the Cisco Catalyst SD-WAN Controllers in the overlay network. The controllers then forward the replicator location information to the PIM-enabled Cisco IOS XE Catalyst SD-WAN routers that are in the same VPN as the replicator.

A replicator Cisco IOS XE Catalyst SD-WAN router receives streams from multicast sources, replicates them, and forwards them to other Cisco Catalyst SD-WAN routers with multicast receivers in the same VPN. The details of the replication process are discussed below, in the section Multicast Traffic Flow through the Overlay Network. A replicator is typically a Cisco IOS XE Catalyst SD-WAN router located at a colo-site or another site with a higher-speed connection to the WAN transport network.

Multicast Service Routes

Cisco IOS XE Catalyst SD-WAN routers send multicast service routes to the Cisco Catalyst SD-WAN Controller using OMP. From these routes, the controller processes and forwards joins for requested multicast groups towards the source address or PIM-RP as specified in the original PIM join message that resulted in a Cisco Catalyst SD-WAN router advertising the OMP multicast service route. The source address can be either the IP address of an RP if the originating router is attempting to join the PIM shared tree or the IP address of the actual source of the multicast stream if the originating router is attempting to join the source tree.

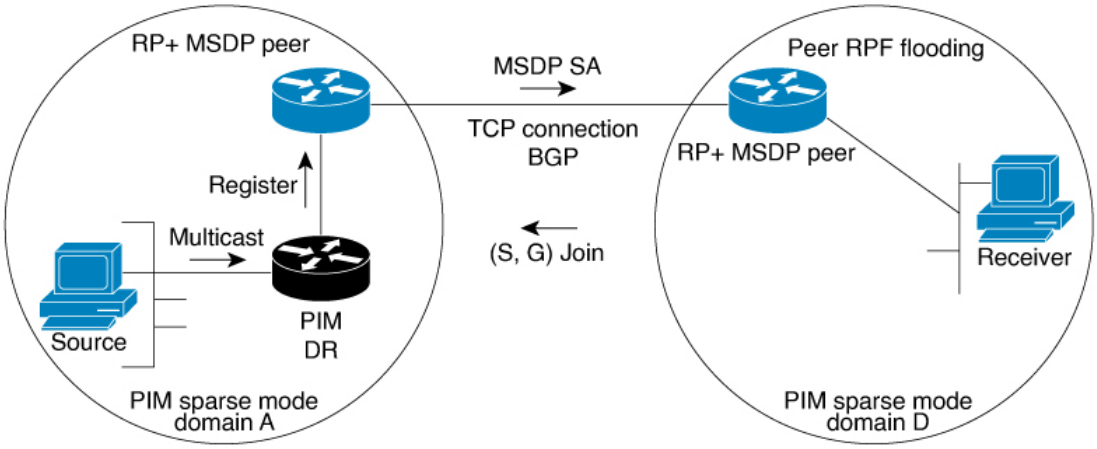
IGMP

Cisco IOS XE Catalyst SD-WAN routers support the Internet Group Management Protocol (IGMP) V2 and V3 protocol. IGMP is used by IPv4 hosts and routers to indicate their interest and in receiving multicast traffic for particular multicast groups. IGMP v3 report is used to indicate interest for a particular multicast group traffic from a specific source. From these membership reports, Cisco IOS XE Catalyst SD-WAN routers originate the corresponding PIM join or OMP service route advertisements.

MSDP

Multicast Source Discovery Protocol (MSDP) is a method of connecting multiple PIM-SM domains, and it is used to discover multicast sources in other PIM domains. When MSDP is configured in a network, rendezvous points (RP) exchange source information with RPs in other domains by maintaining MSDP peer relationships with MSDP-enabled routers in other domains. This peering relationship occurs over a TCP connection. A Cisco IOS XE Catalyst SD-WAN device can be configured as a RP so that it discover active sources outside of its domain.

Figure 1: MSDP



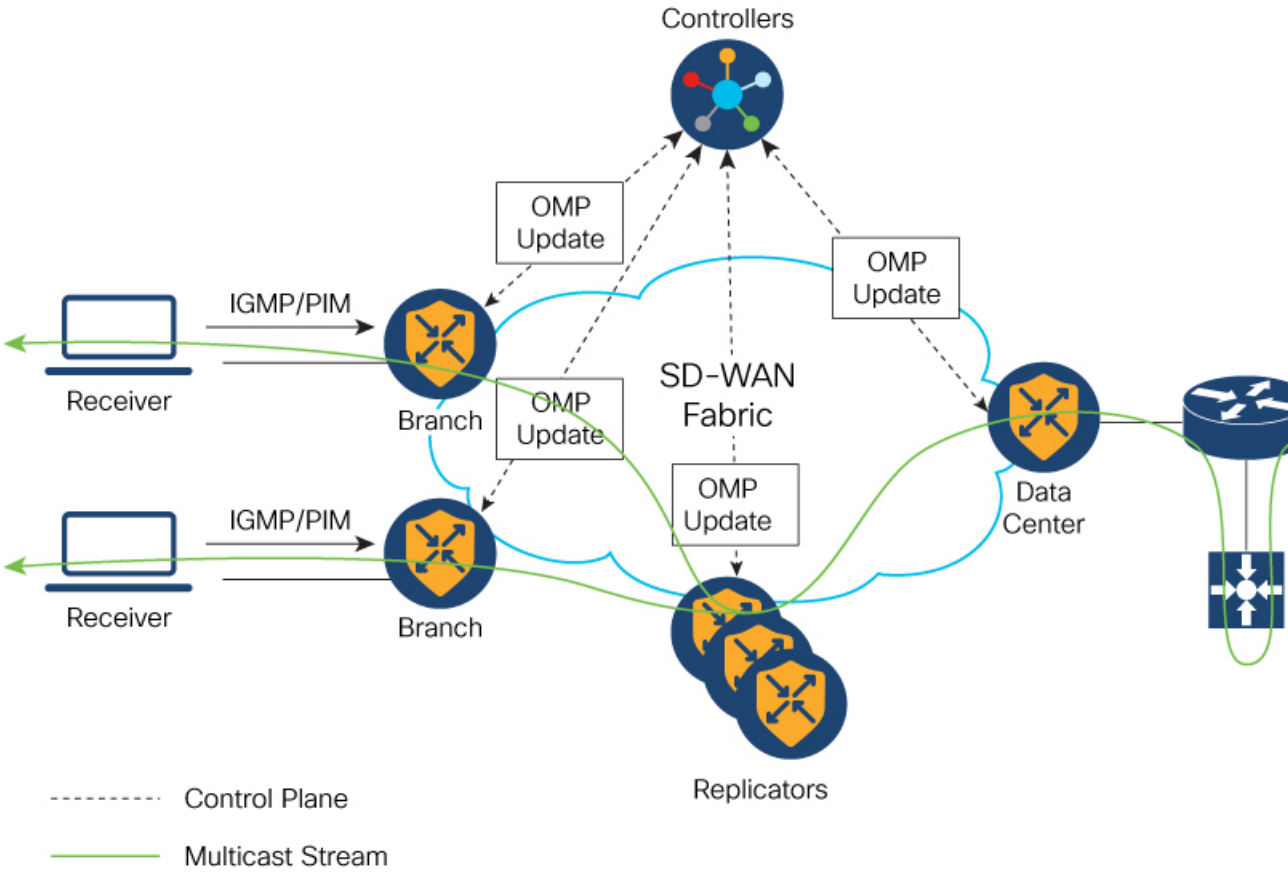
Here is an illustration of the sequence of events that occur when MSDP is implemented:

1. When a PIM designated router (DR) in domain A registers a source with its RP in domain A, the RP sends a Source Active (SA) message to all of its RP MSDP peers. The SA message identifies the source address, the group that the source is sending to, and the address or the originator ID of the RP, if configured.
2. The RP MSDP peer in domain B when it receives the SA message sends the SA message to all of its peers downstream.
3. The RP MSDP peer in domain B checks if there are any receivers of the advertised groups in its domain. If there are receivers in the group, the RP MSDP peer in domain B sends an (S, G) join toward the source. As a result, a connection is established between domain A and domain B. As multicast packets arrive at the RP, they are then forwarded down to the receivers in the RP's domain. When the receivers receiving the multicast traffic learns of the source outside the PIM-SM domain (through the arrival of a multicast packet from the source), it can then send a PIM join toward the source and join source's domain to receive the multicast traffic.

Traffic Flow in Multicast Overlay Routing

The following illustration represents the example topology for multicast overlay routing on Cisco IOS XE Catalyst SD-WAN devices:

Figure 2: Multicast Overlay Routing Topology



Configure Multicast Overlay Routing

For any Cisco IOS XE SD-WAN routers to be able to participate in the multicast overlay network, you must configure PIM on those routers.

Prerequisites

1. If you want to limit rendezvous point (RP) selection, configure an IPv4 ACL using a CLI add-on template. Configure an IPv4 ACL using a standard or extended access list and attach it to your device before enabling PIM. You must have created a valid standard or extended ACL prior to using the ACL in your multicast configuration.

Note You cannot configure an ACL for a PIM feature template using Cisco SD-WAN Manager. You must configure the ACL using a CLI add-on template. The Cisco IOS XE Catalyst SD-WAN multicast overlay implementation supports IOS XE standard or extended access lists.

2. At least one replicator is mandatory for overlay multicast configuration.
3. You can optionally configure IGMP to allow individual hosts on the service side to join multicast groups within a particular VPN.

Configure Multicast

When a Cisco IOS XE Catalyst SD-WAN router is used as a replicator, use the following steps to configure multicast:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **Create Template**.
4. From the **Create Template** drop-down list, choose **From Feature Template**.
5. From the **Device Model** drop-down list, choose the type of device for which you are creating the template.
6. Click **Service VPN** in the **Service VPN** section.
7. Click the **Service VPN** drop-down list.
8. Under **Additional VPN Templates**, click **Multicast**.
9. To enable **Local Replicator** on the device, choose **On** (otherwise keep it **Off**).
10. To configure replicator, choose the **Threshold**. (Optional, keep it default if you are not configuring replicator).
11. Save feature template.
12. Attach feature template to device template.
13. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to **Default** (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down list to the left of the parameter field and select the value.

Configure Multicast Using Configuration Groups

From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a you have the option to configure multicast using Configuration Groups.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click **Service Profile**.
4. Click **Add Feature**.
5. From the feature drop-down list, choose **Multicast**.

The Cisco IOS XE Catalyst SD-WAN overlay multicast network supports the following protocols:

- Protocol Independent Multicast (PIM)
- Internet Group Management Protocol (IGMP)
- MSDP

The following tables describe the options for configuring the Multicast feature.

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.

Table 2: Basic Configuration

Field	Description
SPT Only	Enable this option to ensure that the Rendezvous Points (RPs) can communicate with each other using the shortest-path tree.
Local Replicator	Enable this option to configure the Cisco IOS XE Catalyst SD-WAN device as a multicast replicator.
Threshold	Specify a value. Optional, keep it set to the default value if you are not configuring a replicator.

Table 3: PIM

Field	Description
Source Specific Multicast (SSM)	Enable this option to configure SSM.

Field	Description
ACL	Specify an access control list value. An access control list allows you to filter multicast traffic streams using the group and sometimes source IPv4 or IPv6 addresses. Configure an IPv4 access control list using a standard or extended access list and attach it to your device before enabling PIM. You must have created a valid standard or extended ACL before using the ACL in your multicast configuration. **Note** You cannot configure an ACL for a PIM feature template using Cisco SD-WAN Manager. You must configure the ACL using a CLI add-on template. For information on configuring ACL using the CLI add-on template, see the section **Configure an ACL for Multicast Using a CLI Add-On Template** in chapter **Multicast Overlay Routing** of the Cisco SD-WAN Routing Configuration Guide.
SPT Threshold	Specify the traffic rate, in kbps, at which to switch from the shared tree to the shortest-path tree (SPT). Configuring this value forces traffic to remain on the shared tree and travel via the RP instead of via the SPT.
Add Interface	
Interface Name	Enter the name of an interface that participates in the PIM domain, in the format **ge** *slot /port*.
Query Interval(sec)	Specify how often the interface sends PIM query messages. Query messages advertise that PIM is enabled on the router.
Join/Prune Interval(sec)	Specify how often PIM multicast traffic can join or be removed from a rendezvous point tree (RPT) or shortest-path tree (SPT). Cisco IOS XE Catalyst SD-WAN device send join and prune messages to their upstream RPF neighbor.
How do you want to configure your Rendezvous Point (RP) Cisco IOS XE SD-WAN supports the following modes:	
Static	Click this check box to a specify the static IP address of a rendezvous point (RP).
Add Static RP	
IP Address	Specify the static IP address of a rendezvous point (RP).
ACL	Specify an ACL value.

Field	Description
Override	Enable this option for cases when dynamic and static group-to-RP mappings are used together and there is an RP address conflict. In this case, the RP address configured for a static group-to-RP mapping takes precedence. If you do not enable this option, and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings.
Auto RP	Click this check box to enable reception of PIM group-to-RP mapping updates. This enables reception on the Auto-RP multicast groups, 224.0.1.39 and 224.0.1.40.
RP Announce	Click this check box to enable transmission of Auto-RP multicast messages.
RP Discovery	Click this check box to enable Auto-RP automatic discovery of rendezvous points (RPs) in the PIM network so that the router can serve as an Auto-RP mapping agent. An Auto-RP mapping receives all the RPs and their respective multicast groups and advertise consistent group-to-RP mapping updates.
Interface	Specify the source interface for Auto-RP RP Announcements or RP Discovery messages.
Scope	Specify the IP header Time-to-Live (TTL) for Auto-RP RP Announcements or RP Discovery messages.
PIM-BSR	Configure a PIM BSR.
RP Candidate	
Interface Name	Choose the interface that you used for configuring the PIM feature template.
Access List	Add an access list value if you have configured the access list with a value.
Interval	Add an interval value if you have configured the interval with a value.
Priority	Specify a higher priority on the Cisco IOS XE SD-WAN device than on the service-side device.
BSR Candidate (Maximum: 1)	
Interface Name	Chose the same interface from the drop-down list that you used for configuring the PIM feature template.
Hash Mask Length	Specify the hash mask length. Valid values for hash mask length are 0–32.
Priority	Specify a higher priority on the Cisco IOS XE Catalyst SD-WAN device than on the service-side device.
RP Candidate Access List	Add a value if you have configured the RP candidate access list with a value. An RP candidate uses a standard ACL where you can enter the name for the access list.

Table 4: IGMP

Field	Description
Add IGMP	
Interface	Enter the name of the interface to use for IGMP. To add another interface, click **Add**.
Version	Specify a version number. Optional, keep it set to the default version number.
Group Address	Enter a group address to join a multicast group.
Source Address	Enter a source address to join a multicast group.
Add	Click **Add** to add the IGMP for the group.

Table 5: MSDP

Field	Description
Originator-ID	Specify the ID of the originating device. This ID is the IP address of the interface that is used as the RP address.
Connection Retry Interval	Configure an interval at which MSDP peers will wait after peering sessions are reset before attempting to re-establish the peering sessions.
Mesh Group	
Mesh Group Name	Enter a mesh group name. This configures an MSDP mesh group and indicates that an MSDP peer belongs to that mesh group. **Note** All MSDP peers present on a device that participate in a mesh group must be in a full mesh with all other MSDP peers in the group. Each MSDP peer on each device must be configured as a peer using the **ip msdp peer** command, and as a member of the mesh group using the **ip msdp mesh-group** command.
Peer-IP	Configure an MSDP peer specified by an IP address.
Advanced Settings	
Connect-Source Interface	Enter the primary address of a specified local interface that is used as the source IP address for the TCP connection.
Peer Authentication Password	Enables MD5 password encryption for a TCP connection between two MSDP peers. **Note** MD5 authentication must be configured with the same password on both MSDP peers. Otherwise, a connection between them cannot be established.

Field	Description
Keep Alive	Configure an interval at which an MSDP peer will send keepalive messages.
Hold-Time	Configure an interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them as down.
Remote AS	Specifies the autonomous system number of the MSDP peer. This keyword and argument are used for display purposes only.
SA Limit	Limits the number of SA messages allowed in the SA cache from the specified MSDP.
Default Peer	Configure a default peer from which to accept all MSDP SA messages.

Configure Multicast Using the CLI

To configure multicast, perform the following:

```
sdwan multicast address-family ipv4 vrf 1
replicator [threshold <num>]
```

Sample multicast configuration:

```
Device(config)# sdwan
Device(config)# multicast
  Device(config)# address-family ipv4 vrf 1
  Device(config)# replicator threshold 7500
  Device(config)# !
 !
```

Configure an ACL for Multicast Using a CLI Add-On Template

You can configure an ACL to limit RP and Bootstrap Router (BSR) selection using a CLI add-on template. An ACL allows you to filter multicast traffic streams using the group and sometimes source IPv4 or IPv6 addresses.

Once you create the CLI add-on template, you attach it to the device.

(Optional) You can configure the same standard and extended ACL values in Cisco SD-WAN Manager, which generates the following example configurations:

```
ip pim vrf 1 bsr-candidate Loopback0 32 100 accept-rp-candidate 101
ip pim vrf 1 rp-candidate Loopback0 group-list 27 interval 30 priority 0
```

Note The example configurations are based on the example CLI add-on configuration shown in the procedure.

1. To configure an ACL for multicast, Create a CLI add-on feature template and attach it to the device template.

   This section provides an example configuration.

   ```
   ip access-list standard 27
   1 permit 225.0.0.0 0.255.255.255
   ```

```
2 permit 226.0.0.0 0.255.255.255
3 permit 227.0.0.0 0.255.255.255
4 permit 228.0.0.0 0.255.255.255
5 deny 229.0.0.0 0.255.255.255
6 permit any
ip access-list extended 101
1 permit pim 172.16.10.0 0.0.0.255 any
2 permit pim 10.1.1.0 0.0.0.255 any
```

2. From the **Configuration** > **Templates** window, choose **Feature**.
3. Edit the **Cisco PIM** feature template that you configured for the RP or the BSR candidate by clicking **…** and then clicking **Edit**.

   For more information, see Configure a PIM BSR.
4. (Optional) In the **Access List** field for the configured RP candidate, enter the same ACL value as you configured in the CLI add-on template.
5. (Optional) In the **RP Candidate Access List** field for the configured BSR candidate, enter the same ACL value as you configured in the CLI add-on template.
6. Update the feature template and attach the feature template to the device template.

Configure PIM

Use the PIM template for all Cisco IOS XE Catalyst SD-WAN devices.

Configure the PIM Sparse Mode (PIM-SM) protocol using Cisco SD-WAN Manager templates so that a router can participate in the Cisco IOS XE Catalyst SD-WAN multicast overlay network:

1. Create a PIM feature template to configure PIM parameters.
2. Optionally, create an IGMP feature template to allow individual hosts on the service side to join multicast groups within a particular VPN. For more information, see Configure IGMP.
3. Optionally, create a multicast feature template to configure a Cisco IOS XE Catalyst SD-WAN to be a multicast replicator.
4. Create a VPN feature template to configure parameters for the VPN that is running PIM.

Create a PIM Feature Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **Create Template**.
4. From the **Create Template** drop-down list, choose **From Feature Template**.
5. From the **Device Model** drop-down list, choose the type of device for which you are creating the template.

6. Click **Service VPN** located directly beneath the **Description** field, or scroll to the **Service VPN** section.
7. Click the **Service VPN** drop-down list.
8. Under **Additional VPN Templates**, click **PIM**.
9. From the **PIM** drop-down list, click **Create Template**. The PIM template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining PIM parameters.
10. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
11. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
12. Click **Basic Configuration** and configure SSM – On/Off.
13. Configure access list (if already defined).
14. Configure RP option – Auto-RP or static RP.
15. Configure RP Announce settings.
16. Configure the interface name on the service side.
17. Save feature template and attach feature template to a device template.

When you first open a feature template, for each parameter that has a default value, the scope is set to **Default** (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down list to the left of the parameter field and select the value.

Table 6:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco IOS XE Catalyst SD-WAN device to a device template. When you click **Device Specific**, the **Enter Key** box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. You upload the CSV file when you attach a Cisco IOS XE Catalyst SD-WAN device to a device template. To change the default key, type a new string and move the cursor out of the **Enter Key** box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configure Basic PIM

To configure PIM, click **Basic Configuration** and configure the following parameters. Parameters marked with an asterisk are required to configure PIM.

Table 7:

Parameter Name	Description
Auto-RP	Click **On** to enable Auto-RP to enable reception of PIM group-to-RP mapping updates. This will enable reception on the Auto-RP multicast group, 224.0.1.39 and 224.0.1.40. By default, Auto-RP is disabled.
Auto-RP RP Announce	Click **On** to enable transmission of Auto-RP multicast messages. By default, RP Announce is disabled.
Auto-RP RP Discovery	Click **On** to enable Auto-RP automatic discovery of rendezvous points (RPs) in the PIM network so that the router can serve as an Auto-RP mapping agent. An Auto-RP mapping will receive all the RPs and their respective multicast groups and advertise consistent group-to-RP mapping updates. By default, RP Discovery is disabled.
Static-RP	Specify the IP address of a rendezvous point (RP).
SPT Threshold	Specify the traffic rate, in kbps, at which to switch from the shared tree to the shortest-path tree (SPT). Configuring this value forces traffic to remain on the shared tree and travel via the RP instead of via the SPT.
Interface	Specify the source interface for Auto-RP RP Announcements or RP Discovery messages.
Scope	Specify the IP header Time-to-Live (TTL) for Auto-RP RP Announcements or RP Discovery messages.

To save the feature template, click **Save**.

Configure PIM Interfaces

If the router is just a multicast replicator and is not part of a local network that contains either multicast sources or receivers, you do not need to configure any PIM interfaces. The replicator learns the locations of multicast sources and receivers from the OMP messages it exchanges with the Cisco Catalyst SD-WAN Controller. These control plane messages are exchanged in the transport VPN (VPN 0). Similarly, other Cisco IOS XE Catalyst SD-WAN devices discover replicators dynamically, through OMP messages from the Cisco Catalyst SD-WAN Controller.

To configure PIM interfaces, click **Interface**. Then click **Add New Interface** and configure the following parameters:

Table 8:

Parameter Name	Description
Name	Enter the name of an interface that participates in the PIM domain, in the format **ge** *slot /port*.

Parameter Name	Description
Hello Interval	Specify how often the interface sends PIM hello messages. Hello messages advertise that PIM is enabled on the router. Range: 1 through 3600 seconds Default: 30 seconds
Join/Prune Interval	Specify how often PIM multicast traffic can join or be removed from a rendezvous point tree (RPT) or shortest-path tree (SPT). Cisco IOS XE Catalyst SD-WAN send join and prune messages to their upstream RPF neighbor. Range: 0 through 600 seconds Default: 60 seconds

To edit an interface, click the pencil icon to the right of the entry.

To delete an interface, click the trash icon to the right of the entry.

To save the feature template, click **Save**.

Rendezvous Point Selection Process by a PIM BSR

Table 9: Feature History

Feature Name	Release Information	Description
Dynamic Rendezvous Point (RP) Selection by a PIM BSR	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature adds support for automatic selection of an RP candidate using a PIM BSR in an IPv4 multicast overlay. There is no single point of failure because every site has a local RP. A Cisco IOS XE Catalyst SD-WAN device is selected as the RP, not a service-side device.

PIM uses a BSR to discover and announce RP-set information for each group prefix to all the routers in a PIM domain. This is the same function performed by Auto-RP, but a BSR is part of the PIM version 2 specification.

Note Cisco Auto-RP cannot co-exist with PIM BSR. Cisco Auto-RP mode must be disabled with spt-only mode.

To avoid a single point of failure, you can configure several candidate BSRs in a PIM domain. A BSR is selected among the candidate BSRs automatically. The BSRs use bootstrap messages to discover which BSR has the highest priority. This router then announces to all PIM routers in the PIM domain that it is the BSR. Any router in the network can be a BSR candidate.

The elected BSR receives candidate-RP messages from all the candidate RPs in the domain. The bootstrap message sent by a BSR includes information about all of the candidate RPs.

An RP acts as the meeting place for sources and receivers of multicast data. In a PIM-SM network, sources must send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree.

By default, when the first hop router of the receiver learns about the source, it sends a join message directly to the source, creating a source-based distribution tree from the source to the receiver. This source tree does not include a RP unless the RP is located within the shortest path between the source and the receiver.

Note For a BSR to work for any multicast stream that spans across Cisco Catalyst SD-WAN sites, SPT-only mode is mandatory. For a BSR within a local-site multicast stream within a Cisco Catalyst SD-WAN site, it is not necessary to enable SPT-only mode.

Note If you have two Cisco IOS XE Catalyst SD-WAN devices in the same site, every Cisco IOS XE Catalyst SD-WAN device needs to be configured as a replicator for traffic to flow.

Features and Benefits

- IPv4 support.
- Dynamic rather than static selection of an RP.
- Automatic failover if one RP is not available.
- RP discovery is handled by a BSR.
- Configuration of multiple RP candidates for the same group range.
- Selection of a Cisco IOS XE Catalyst SD-WAN device as the RP.

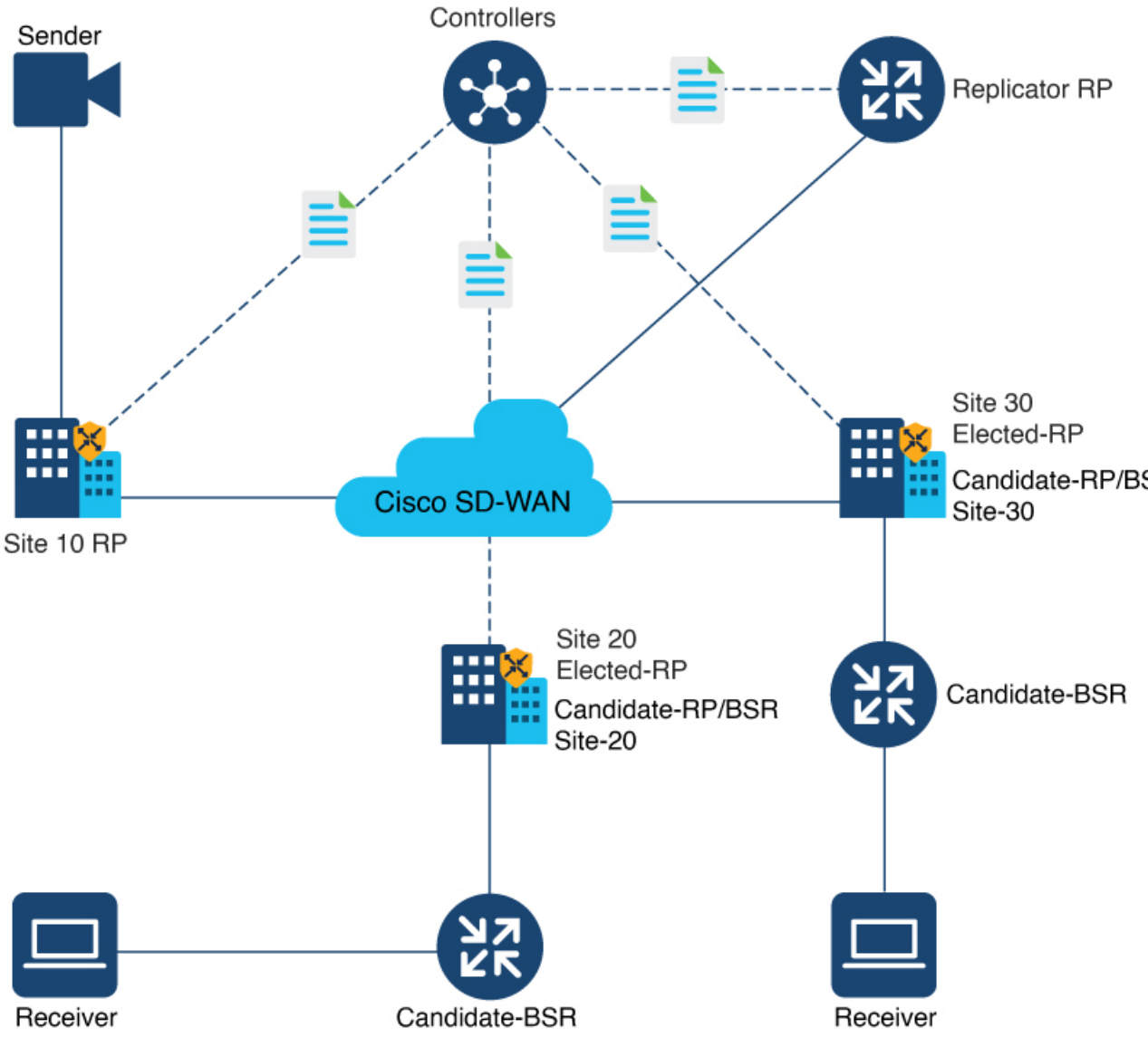
Restrictions for PIM BSR

- IPv6 is not supported.
- Bidirectional PIM is not supported for IPv4.
- BSR is not supported in a hub-and-spoke topology on Cisco IOS XE Catalyst SD-WAN devices.

Sample Topology for RP Selection by a PIM BSR

The following is a sample topology for RP selection by a PIM BSR on Cisco IOS XE Catalyst SD-WAN devices.

Figure 3: Topology for PIM BSR Selection



Configure a PIM BSR

Prerequisites for Configuring a BSR Candidate

- Every Cisco Catalyst SD-WAN site must have its own RP.
- SPT-only mode must be enabled on all Cisco Catalyst SD-WAN sites.

Note For a BSR to work for any multicast stream that spans across Cisco Catalyst SD-WAN sites, SPT-only mode is mandatory. For a BSR within a local-site multicast stream within a Cisco Catalyst SD-WAN site, it is not necessary to enable SPT-only mode.

Workflow

For a PIM BSR to elect the RP, configure the following in Cisco SD-WAN Manager:

1. Multicast feature template with **SPT Only** set to **On** for the selected Cisco IOS XE Catalyst SD-WAN device.
2. PIM feature template with an interface.
3. RP candidate.
4. BSR candidate.

Configure Shortest-Path Tree (SPT-Only) Mode for a Multicast Feature Template

In Cisco SD-WAN Manager, configure **SPT Only** mode to ensure that the RPs can communicate with each other using the shortest-path tree.

Note When configuring a BSR, configuration of **SPT Only** mode is mandatory.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. From the **Select Devices** drop-down list, choose a Cisco IOS XE Catalyst SD-WAN device.
5. Under **Other Templates**, choose **Cisco Multicast**.
6. In the **Template Name** field, enter a name for the template.
7. In the **Description** field, enter a description of the template.

   The description can be up to 2048 characters and can contain only alphanumeric characters.
8. Under the **Basic Configuration** section for **SPT Only**, choose **On**.
9. To enable the **Local Replicator** on the device, choose **On** (otherwise keep it set to **Off**).
10. To configure a replicator, choose **Threshold**, and specify a value. (Optional, keep it set to the default value if you are not configuring a replicator).

11. Click **Save**.

Configure a PIM Feature Template and Add an Interface

Configure a PIM feature template and add an interface for an RP and the BSR candidate.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. From the **Select Devices** drop-down list, choose a Cisco IOS XE Catalyst SD-WAN device.
5. Under **Other Templates**, choose **Cisco PIM**.
6. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
7. In the **Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
8. Click **Interface**.

   For information on how to configure a PIM interface, see Configure PIM.
9. Click **New Interface**.
10. In the **Interface Name** field, specify an interface with a value.
11. In the **Query Interval (seconds)** field, the field auto-populates.
12. In the **Join/Prune Interval (seconds)** field, the field auto-populates.
13. Click **Add**.
14. Click **Save**.

Configure the RP Candidate

Configure the same Cisco IOS XE Catalyst SD-WAN device as the candidate RP for all multicast groups or selective groups.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Edit the PIM feature template that you created by clicking **...** and then clicking **Edit**.
4. Click **Basic Configuration**.

5. Click **RP Candidate**.
6. Click **New RP Candidate**.
7. From the **Interface** drop-down list, choose the interface that you used for configuring the PIM feature template.
8. (Optional) In the **Access List** field, if you have configured the access list with a value, add the same value.
9. (Optional) In the **Interval** field, if you have configured the interval with a value, add the same interval value.
10. In the **Priority** field, specify a higher priority on the Cisco IOS XE Catalyst SD-WAN device than on the service-side device.
11. Click **Add**.
12. Click **Update** to save your configuration changes.

Configure the BSR Candidate

1. Repeat Step 1 through Step 4 from the *Configure the RP Candidate* section.
2. Click **BSR Candidate**.
3. In the **BSR Candidate** field, chose the same interface from the drop-down list that you used for configuring the PIM feature template.
4. (Optional) In the **Hash Mask Length** field, specify the hash mask length.

   Valid values for hash mask length are from 0 – 32.
5. In the **Priority** field, specify a higher priority on the Cisco IOS XE Catalyst SD-WAN device than on the service-side device.
6. (Optional) In the **RP Candidate Access List** field, if you have configured the RP candidate access list with a value, add the same value.

   An RP candidate uses a standard access control list (ACL) where you can enter the name for the access list.
7. Click **Update** to save your configuration changes.

CLI Configurations for PIM BSR Selection

Configure a BSR Candidate

1. Configure a Cisco IOS XE Catalyst SD-WAN device as a candidate BSR:

```
Device(config)# ip pim vrf 1 bsr-candidate Loopback 99
```

Note The Loopback interface is used only as an example here. Loopback is one of many interface types that can be used for configuring an RP candidate.

2. Use the **show ip pim vrf bsr-router** command to view information about the BSR:

```
Device# show ip pim vrf 1 bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 10.1.10.2 (?)
  Uptime:      15:46:38, BSR Priority: 100, Hash mask length: 32
  Next bootstrap message in 00:00:52
  Candidate RP: 10.1.10.2(Loopback0)
    Holdtime 75 seconds
    Advertisement interval 30 seconds
    Next advertisement in 00:00:18
    Group acl: 27
```

Configure an RP Candidate

1. Configure a Cisco IOS XE Catalyst SD-WAN device as a candidate RP for all multicast groups or selective groups:

```
Device(config)# ip pim vrf 1 rp-candidate Loopback 1 priority 0
```

or

```
Device(config)# ip pim vrf 1 rp-candidate Loopback 1 group-list acl1 priority 0
Device(config)# ip pim vrf 1 rp-candidate Loopback 2 group-list acl2 priority 0
```

2. Use the **show ip pim vrf 1 rp mapping** command to verify the RP mapping assignments:

```
Device# show ip pim vrf 1 rp mapping
PIM Group-to-RP Mappings
This system is a candidate RP (v2)
This system is the Bootstrap Router (v2)

Group(s) 224.0.0.0/4
  RP 10.1.10.2 (?), v2
    Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
         Uptime: 15:46:47, expires: 00:00:57
Group(s) 225.0.0.0/8
  RP 10.1.10.2 (?), v2
    Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
         Uptime: 15:46:47, expires: 00:00:57
  RP 10.1.10.1 (?), v2
    Info source: 10.1.10.1 (?), via bootstrap, priority 10, holdtime 75
         Uptime: 15:45:45, expires: 00:00:59
Group(s) 226.0.0.0/8
  RP 10.1.10.2 (?), v2
    Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
         Uptime: 15:46:55, expires: 00:00:49
  RP 10.1.10.1 (?), v2
    Info source: 10.1.10.1 (?), via bootstrap, priority 10, holdtime 75
         Uptime: 15:46:02, expires: 00:01:09
Group(s) 227.0.0.0/8
  RP 10.1.10.2 (?), v2
    Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
         Uptime: 15:47:13, expires: 00:00:59
  RP 10.1.10.1 (?), v2
    Info source: 10.1.10.1 (?), via bootstrap, priority 10, holdtime 75
         Uptime: 15:46:20, expires: 00:00:53
Group(s) 228.0.0.0/8
  RP 10.1.10.2 (?), v2
    Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
         Uptime: 15:47:31, expires: 00:01:13
```

Configure a Cisco IOS XE Catalyst SD-WAN Device as SPT-Only

1. Configure a Cisco IOS XE Catalyst SD-WAN device as spt-only:

```
Device(config)# sdwan multicast address-family ipv4 vrf 1
spt-only
```

2. Use the **show platform software sdwan multicast remote-nodes vrf** command to verify that system IP addresses are configured with spt-only mode:

```
Device# show platform software sdwan multicast remote-nodes vrf 1

Multicast SDWAN Overlay Remote Nodes (* - Replicator):
                                          Received               Sent
                 SPT-Only               (X,G)      (S,G)      (X,G)      (S,G)
 System IP       Mode         Label   Join/Prune Join/Prune Join/Prune Join/Prune
 172.16.255.11   Yes          1003        0/0        0/0        0/0        0/0
 172.16.255.14   Yes          1003        0/0        0/0        1/0      10/10
 172.16.255.16   Yes          1003        0/0        0/0        0/0        0/0
 172.16.255.21   Yes          1003        0/0        0/0        0/0        0/0
```

Sample Multicast Configuration With SPT-Only

```
Device(config)# sdwan
Device(config)# multicast
Device(config)# address-family ipv4 vrf 1
Device(config)# spt-only
!
```

Verify VRRP-Aware PIM Using the CLI

Sample VRRP-aware PIM configuration on router 1:

```
interface Vlan13
no shutdown
arp timeout 1200
vrf forwarding 1
ip address 10.0.0.1 255.255.255.0
ip pim sparse-mode
ip pim redundancy 1 vrrp dr-priority 200
ip tcp adjust-mss 1350
ip mtu 1500
ip igmp version 3
vrrp 1 address-family ipv4
vrrpv2
address 10.0.0.3
priority 200
timers advertise 100
track omp shutdown
vrrs leader 1
exit
```

Sample VRRP-aware PIM configuration on router 2:

```
interface Vlan13
no shutdown
arp timeout 1200
vrf forwarding 1
ip address 10.0.0.2 255.255.255.0
ip pim sparse-mode
ip pim redundancy 1 vrrp dr-priority 200
ip tcp adjust-mss 1350
ip mtu 1500
```

```
ip igmp version 3
vrrp 1 address-family ipv4
vrrpv2
address 10.0.0.3
priority 200
timers advertise 100
track omp shutdown
vrrs leader 1
exit
```

Configure IGMP

Use the IGMP template for all Cisco IOS XE Catalyst SD-WAN devices. Internet Group Management Protocol (IGMP) allows routers to join multicast groups within a particular VPN.

To configure IGMP using Cisco SD-WAN Manager templates:

1. Create an IGMP feature template to configure IGMP parameters.
2. Create the interface in the VPN to use for IGMP. See the VPN-Interface-Ethernet help topic.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

Navigate to the Template Window and Name the Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.x.7 and earlier releases, **Device Templates** is titled **Device**.

3. Click **Create Template**.
4. From the **Create Template** drop-down list, choose **From Feature Template**.
5. From the **Device Model** drop-down list, choose the type of device for which you are creating the template.
6. Click **Service VPN** located directly beneath the **Description** field, or scroll to the **Service VPN** section.
7. Click the **Service VPN** drop-down list.
8. Under **Additional VPN Templates**, click **IGMP**.
9. From the **IGMP** drop-down list, click **Create Template**. The IGMP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining IGMP parameters.
10. Add interface name on the service side to enable IGMP.
11. (Optional) In the **Join Group And Source Address** field, click on **Add Join Group and Source Address**. The **Join Group and Source Address** window displays.
12. (Optional) Enter group address to join and source address.

13. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
14. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to **Default** (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select the value.

Table 10:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco IOS XE Catalyst SD-WAN device to a device template. When you click **Device Specific**, the **Enter Key** box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. You upload the CSV file when you attach a Cisco IOS XE Catalyst SD-WAN device to a device template. To change the default key, type a new string and move the cursor out of the **Enter Key** box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configure Basic IGMP Parameters

To configure IGMP, click **Basic Configuration** to enable IGMP. Then, click **Interface**, and click **Add New Interface** to configure IGMP interfaces. All parameters listed below are required to configure IGMP.

Table 11:

Parameter Name	Description
Interface Name	Enter the name of the interface to use for IGMP. To add another interface, click the plus sign (+).
Join Group Address	Optionally, click **Add Join Group Address** to enter a multicast group. Click **Add** to add the IGMP for the group.

To save the feature template, click **Save**.

Configure PIM and IGMP Using the CLI

For a Cisco IOS XE Catalyst SD-WAN router located at a site that contains one or more multicast sources, enable PIM on the service-side interface or interfaces. These are the interfaces that connect to the service-side network. To enable PIM or IGMP per VPN, you must configure PIM or IGMP and its interfaces for all VPNs support multicast services. PIM configuration is not required in VPN 0 (the transport VPN facing the overlay network) or in VPN 512 (the management VPN).

If a source interface is specified in the **send-rp-discovery** container, ensure that the interface already has an IP address and PIM configured.

Sample configuration:

```
vrf definition 1
 rd 1:1
 address-family ipv4
  exit-address-family
 !
!
ip pim vrf 1 autorp listener
ip pim vrf 1 send-rp-announce Loopback1 scope 12 group-list 10
ip pim vrf 1 send-rp-discovery Loopback1 scope 12
ip pim vrf 1 ssm default
ip access-list standard 10
 10 permit 10.0.0.1 0.255.255.255
!
ip multicast-routing vrf 1 distributed
interface GigabitEthernet0/0/0.1
 no shutdown
 encapsulation dot1Q 1
 vrf forwarding 1
 ip address 172.16.0.0 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 ip ospf 1 area 0
exit
interface GigabitEthernet0/0/2
 no shutdown
 vrf forwarding 1
 ip address 172.16.0.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 1 area 0
exit
interface Loopback1
 no shutdown
 vrf forwarding 1
 ip address 192.0.2.255 255.255.255.255
 ip pim sparse-mode
 ip ospf 1 area 0
exit
sdwan
 multicast
  address-family ipv4 vrf 1
   replicator threshold 7500

   exit
```

Configure MSDP Using a CLI Template

Before You Begin

Note By enabling an MSDP peer, you implicitly enable MSDP.

- IP multicast routing must be enabled and PIM-SM must be configured. For more information, see Configure PIM, on page 13.

Configure MSDP Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure MSDP.

1. Enable MSDP and configure an MSDP peer as specified by the DNS name or IP address.

   ip msdp peer *peer ip address* **connect-source**

   If you specify the **connect-source** keyword, the primary address of the specified local interface type and number values are used as the source IP address for the TCP connection. The **connect-source** keyword is recommended, especially for MSDP peers on a border that peer with a device inside of a remote domain.

2. Configure an originating address.

   Perform this optional task to allow an MSDP speaker that originates an SA message to use the IP address of its interface as the RP address in the SA message.

   You can also change the originator ID for any one of the following reasons:

   - If you configure multiple devices in an MSDP mesh group for Anycast RP.
   - If you have a device that borders a PIM-SM domain and a PIM-DM domain. If a device borders a PIM-SM domain and a PIM-DM domain and you want to advertise active sources within the PIM-DM domain, configure the RP address in SA messages to be the address of the originating device's interface.

   ip msdp originator-id *type number*

3. Configure an MSDP Mesh Group.

   Configures an MSDP mesh group and indicates that an MSDP peer belongs to that mesh group.

Note You can configure multiple mesh groups per device.

```
ip msdp mesh-group mesh name{peer-ip address | peer name}
```

Note All MSDP peers on a device that participate in a mesh group must be fully meshed with all other MSDP peers in the group. Each MSDP peer on each device must be configured as a peer using the **ip msdp peer** command and also as a member of the mesh group using the **ip msdp mesh-group** command.

Support for MSDP to Interconnect Cisco SD-WAN and Non-SD-WAN

Table 12: Feature History

Feature Name	Release Information	Feature Description
Support for MSDP to Interconnect Cisco SD-WAN and Non-SD-WAN Domains	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature enables Multicast Source Discovery Protocol (MSDP) interoperability between Cisco IOS XE Catalyst SD-WAN devices in Cisco Catalyst SD-WAN and the devices in a non-SD-WAN setup. **Note** This feature does not provide support for MSDP peers formed between Cisco IOS XE Catalyst SD-WAN devices in the overlay network.

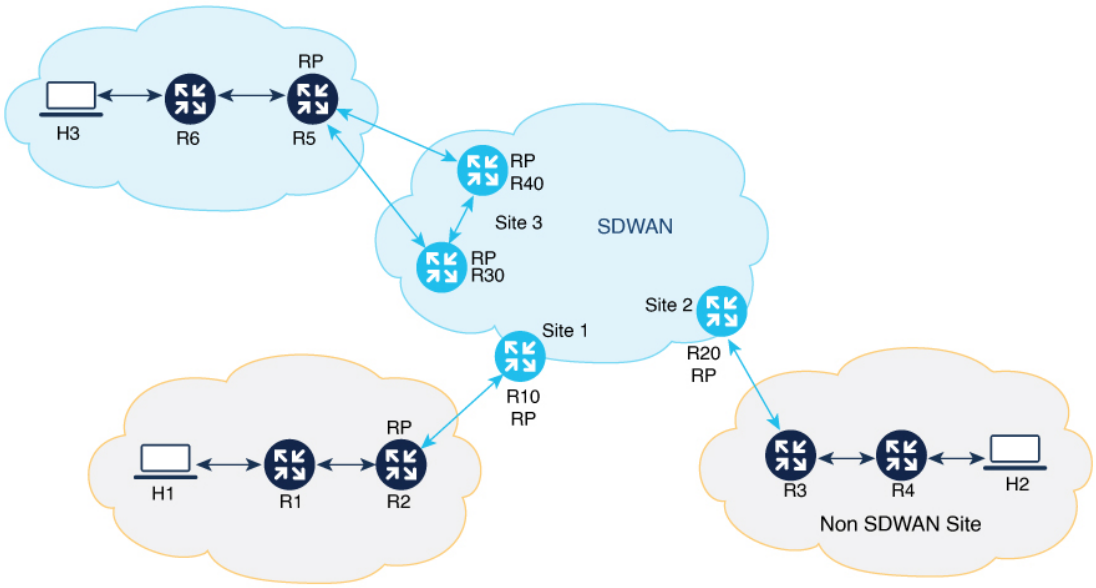
Information About Support for MSDP to Interconnect Cisco SD-WAN and Non-SD-WAN

MSDP facilitates interconnection of multiple Protocol Independent Multicast Sparse-Mode (PIM-SM) domains. When MSDP is enabled on Cisco IOS XE Catalyst SD-WAN devices, a rendezvous point (RP) in a PIM-SM domain maintains MSDP peering relationships with MSDP-enabled routers in other domains. For more information about MSDP, see MSDP, on page 5.

From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, you can configure Cisco IOS XE Catalyst SD-WAN devices for MSDP interoperability with other devices. When Cisco IOS XE Catalyst SD-WAN devices are configured for MSDP interoperability, they convert Source Active (SA) messages received from MSDP peers into OMP routes, and vice-versa.

The following illustration depicts MSDP interoperability between Cisco IOS XE Catalyst SD-WAN devices in Cisco Catalyst SD-WAN and devices in a non-SD-WAN setup.

Figure 4: MSDP Interoperability



Single Homed Network

In the sample topology, MSDP interoperability is enabled on the Cisco IOS XE Catalyst SD-WAN device, R20, at site 2. R3 is configured as an RP for its PIM domain at the non-SD-WAN site. MSDP peering is established between R3 at the non-SD-WAN site and on R20 at site 2. When source H2 sends traffic to R4, R4 initiates a data registration with R3, and thereafter, R3 sends an MSDP SA message to R20. As MSDP interoperability is enabled in R20, R20 converts the received MSDP SA message to OMP SA routes, and then advertises them to all Cisco IOS XE Catalyst SD-WAN devices located at other sites through the Cisco SD-WAN Controller serving the Cisco IOS XE Catalyst SD-WAN devices. When the Cisco IOS XE Catalyst SD-WAN device R10 at site 1 receives this OMP SA route, R10 converts the OMP SA route into MSDP SA message and advertises the MSDP SA message to its MSDP peer R2 at the non-SD-WAN site. If R2 has any receivers interested in the group advertised in MSDP SA message, then R2 sends a (S,G) join towards the source. As a result, a inter-domain source tree is established across Cisco Catalyst SD-WAN. As multicast packets arrive at R2 (RP), they are then forwarded down its own shared tree to the group members in the RP's domain. R20 withdraws the advertised OMP SA route only when the MSDP SA message expires.

Dual-Homed Network

A dual home network is where there are two Cisco IOS XE Catalyst SD-WAN devices configured for MSDP interoperability. In the dual-homed Cisco Catalyst SD-WAN site 3, MSDP peering must be established between the Cisco IOS XE Catalyst SD-WAN devices R30, R40, and the non-SDWAN device R5. When the source registers its traffic with the RP R5, R5 sends a MSDP SA message to both R30 and R40. When R30 receives the MSDP SA message, it converts the MSDP SA message into OMP SA routes and then advertises to all the Cisco IOS XE Catalyst SD-WAN devices located at other sites, and to R40 within the same, site 3. MSDP SA filter must be configured between R30 and R40 to drop the SA message received from other Cisco IOS XE Catalyst SD-WAN devices and sites through the Overlay Management Protocol (OMP). The Cisco IOS XE Catalyst SD-WAN device R10 at site 1 receives two OMP SA routes for the same Source Group (S, G) and caches them both. R10 then converts the OMP SA route into MSDP SA message and advertises to its MSDP peer R2 at the non-SD-WAN site. If R2 has any receivers interested in the group advertised in MSDP

SA message, then R2 sends a (S,G) join towards the source. As a result, a inter-domain source tree is established across Cisco Catalyst SD-WAN.

MSDP supports the following scenarios where Cisco IOS XE Catalyst SD-WAN devices at the Cisco Catalyst SD-WAN sites are configured for MSDP interoperability with other devices located in the non-SD-WAN sites.

- Source devices located at the Cisco Catalyst SD-WAN sites, and receivers at the Cisco Catalyst SD-WAN and non-SD-WAN sites.
- Source devices located in the non-SD-WAN sites, and receivers at the Cisco Catalyst SD-WAN and non-SD-WAN sites.
- In Dual border sites, where two devices are configured for MSDP interoperability in Cisco Catalyst SD-WAN where sources and receivers are located in the Cisco Catalyst SD-WAN sites.
- In dual border sites, where two devices are configured for MSDP interoperability in non-SD-WAN, and where sources and receivers are located at the non-SD-WAN sites.
- A Replicator can be any Cisco IOS XE Catalyst SD-WAN device located in the Cisco Catalyst SD-WAN site. For more information about Replicators, see the **Replicators** section in PIM, on page 3.

Benefits of Support for MSDP to Interconnect Cisco SD-WAN and non-SD-WAN

Facilitates MSDP interoperability between devices located at the Cisco SD-WAN sites and devices at the non-SD-WAN sites.

Prerequisites for Support for MSDP to Interconnect Cisco SD-WAN and Non-SD-WAN

- For MSDP interoperability to work, you must enable shortest-path tree (SPT) SPT-only mode on a Cisco IOS XE Catalyst SD-WAN device, and the device must be selected as an RP. For more information, see the **Basic Configuration** section in Configure Multicast Using Configuration Groups, on page 8.
- For MSDP interoperability, the peer devices must be set up in a mesh group.
- In a dual-homed setup, configure an MSDP SA filter on a Cisco IOS XE Catalyst SD-WAN device to drop MSDP SA messages from the other Cisco IOS XE Catalyst SD-WAN device.

Restrictions for Support for MSDP to Interconnect Cisco SD-WAN and Non-SD-WAN

- Only one MSDP mesh group is supported per site in Cisco Catalyst SD-WAN.
- The MSDP peer devices must be located at the same site and cannot be spread across sites.

Configure MSDP to Interconnect Cisco SD-WAN and Non-SD-WAN

Note You cannot configure the MSDP interoperability using the feature template or the configuration groups in Cisco SD-WAN Manager.

Perform the following tasks to configure MSDP interoperability on Cisco IOS XE Catalyst SD-WAN device:

1. Enable MSDP on Cisco IOS XE Catalyst SD-WAN device. For more information, see Configure MSDP Using a CLI Template, on page 27.
2. Configure MSDP interworking using a CLI template. For more information see Configure MSDP to Interconnect Cisco SD-WAN and Non-SD-WAN Using a CLI Template, on page 31.

Configure MSDP to Interconnect Cisco SD-WAN and Non-SD-WAN Using a CLI Template

Use the CLI templates to configure the MSDP interoperability feature in Cisco Catalyst SD-WAN. For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

1. Enable MSDP on a Cisco IOS XE Catalyst SD-WAN device. For more information, see Configure MSDP Using a CLI Template, on page 27
2. Configure a Cisco IOS XE Catalyst SD-WAN device for MSDP interoperability with other devices in the non-SD-WAN sites.

```
multicast address-family ipv4 vrf vrf-name
spt-only
msdp-interworking
```

The following is a complete configuration example to configure MSDP interoperability in Cisco Catalyst SD-WAN:

```
sdwan
 multicast address-family ipv4 vrf 1
  spt-only

  msdp-interworking
```

Verify MSDP Configuration to Interconnect Cisco SD-WAN and Non-SD-WAN

The following is a sample output from the **show platform software sdwan multicast remote-nodes vrf***1* command, which shows if MSDP interoperability is enabled or not.

```
Device# show platform software sdwan multicast remote-nodes vrf 1
 Multicast SDWAN Overlay Remote Nodes (* - Replicator, ^ - Delete Pending):
                                                  Received                Sent
                       SPT-Only MSDP               (X,G)      (S,G)      (X,G)      (S,G)
          System IP    Mode     I-Work Label   Join/Prune Join/Prune Join/Prune Join/Prune
         10.16.255.11 No       No     1003      0/0        0/0        0/0        1/0
         10.16.255.15 No       No     1003      1/0        1/0        0/0        0/0
         10.16.255.16 Yes      No     1003      1/0        1/0        0/0        0/0
         10.16.255.21 Yes      Yes    1003      0/0        0/0        0/0        0/0
```

Monitor MSDP Configuration to Interconnect Cisco SD-WAN and Non-SD-WAN

Use the following show commands to monitor MSDP interoperability on Cisco IOS XE Catalyst SD-WAN devices:

```
Device# show ip msdp vrf 1 sa-cache
MSDP Source-Active Cache - 1 entries
(10.169.1.1, 12.169.1.1), RP 41.41.41.41, AS ?,6d20h/00:05:55, Peer 12.168.3.11
```

```
Device# show ip msdp vrf 1 count
SA State per Peer Counters, <Peer>: <# SA learned>
    12.168.3.11: 1
    12.168.11.15: 0
    12.168.12.12: 0
    12.168.14.14: 0
    12.168.5.24: 0
SA State per ASN Counters, <asn>: <# sources>/<# groups>
    Total entries: 1
    ?: 1/1
```

```
Device# show ip msdp vrf 1 summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
12.168.3.11      ?     Up       17w6d    0     1     ?
12.168.11.15     ?     Up       17w6d    0     0     ?
12.168.12.12     ?     Up       17w6d    0     0     ?
12.168.14.14     ?     Up       17w6d    0     0     ?
12.168.5.24      ?     Up       17w6d    1     0     ?
```

```
Device# show ip msdp vrf 1 peer 12.168.15.19 advertised-SAs
MSDP SA advertised to peer 12.168.15.19 (?) from mroute table

MSDP SA advertised to peer 12.168.15.19 (?) from SA cache

MSDP SA advertised to peer 12.168.15.19 (?) from mvpn sact table

20.169.1.1      13.169.1.1 RP 41.41.41.41 (?) 6d20h ref: 2
```

In the output above, the entry **MSDP SA advertised to peer 12.168.15.19 (?)** from **mvpn sact table** provides information about SA cache messages advertised to a peer based on the OMP SA routes received.

```
Device# show ip msdp vrf 1 peer 12.168.21.29
MSDP Peer 12.168.21.29 (?), AS ?
  Connection status:
    State: Up, Resets: 0, Connection source: GigabitEthernet5 (12.168.21.28)
    Uptime(Downtime): 16w4d, Messages sent/received: 169100/169106
```

```
  Output messages discarded: 82
  Connection and counters cleared 16w4d    ago
  Peer is member of mesh-group site3
SA Filtering:
  Input (S,G) filter: sa-filter, route-map: none
  Input RP filter: none, route-map: none
  Output (S,G) filter: none, route-map: none
  Output RP filter: none, route-map: none
SA-Requests:
  Input filter: none
Peer ttl threshold: 0
SAs learned from this peer: 0
Number of connection transitions to Established state: 1
  Input queue size: 0, Output queue size: 0
MD5 signature protection on MSDP TCP connection: not enabled
Message counters:
  RPF Failure count: 0
  SA Messages in/out: 10700/10827
  SA Requests in: 0
  SA Responses out: 0
  Data Packets in/out: 0/10
```

Troubleshooting

MSDP SA Cache Not Populated

Problem MSDP SA cache is not populated on a Cisco IOS XE Catalyst SD-WAN device when a source in a site sends traffic.

Possible Cause Check if there are any connectivity or configuration issues between the MSDP peers.

Solution To resolve the problem, do the following:

Solution Check the MSDP peering status between the Cisco IOS XE Catalyst SD-WAN device and the device in non-SD-WAN.

Solution Verity that these commands **msdp-interworking** and **spt-only** are configured in the Cisco IOS XE Catalyst SD-WAN device.

OMP SA Route Not Advertised

Problem A Cisco IOS XE Catalyst SD-WAN device does not advertise the OMP SA route when it receives a MSDP SA message from a MSDP peer.

Possible Cause **msdp-interworking** configuration could be missing.

Solution Configure the **msdp-interworking** command in the correct VRF.

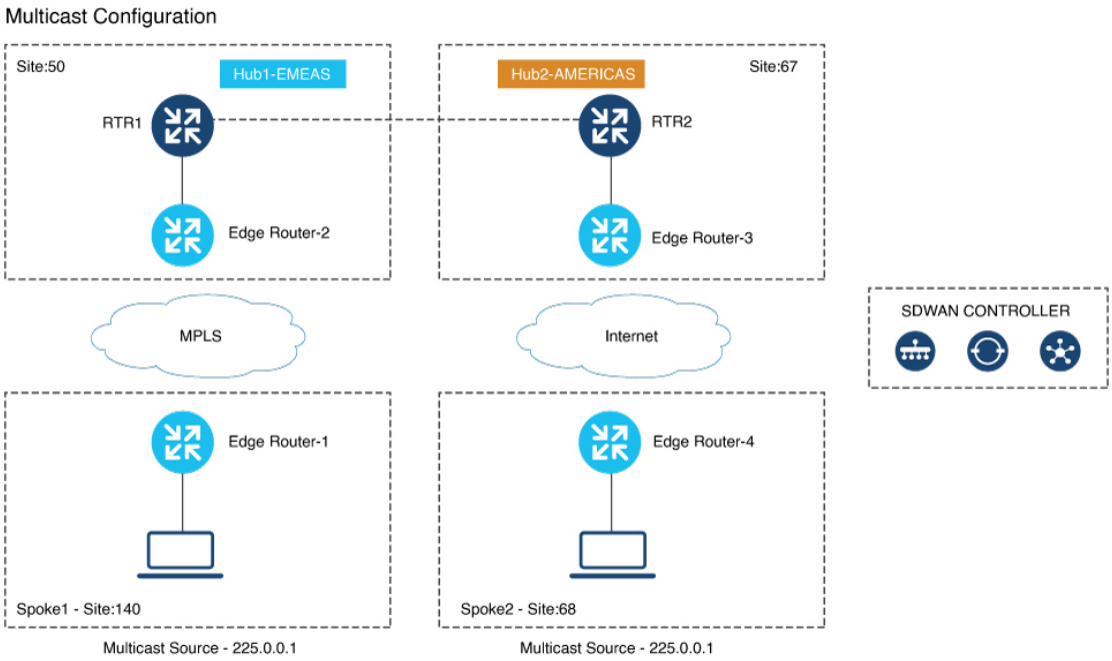
Support for Hub-and-Spoke Topology

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1

Using multicast overlay protocols in a hub-and-spoke topology, a source can send a single packet of data to a single multicast address, which is then distributed to an entire group of recipients.

Use case for Multicast Routing on Hub-and-Spoke

- A sender in a hub site sending multicast traffic to receivers in same or other hub sites.
- A sender in a hub site sending multicast traffic to receivers in spoke sites.
- A sender in a spoke site sending multicast traffic to receivers in hub sites.
- A sender in a spoke site sending multicast traffic to receivers in same/other spoke sites.



The illustration has the following configurations:

- Any Source Multicast (ASM) with static or AutoRP
- No BFD session between hub sites across different regions
- No BFD sessions between spoke sites
- BFD session must be present between hub sites and all the spoke sites across all regions
- For every site (both hub and spoke) define a control policy. The site-list of the policy specifies all hub and spoke sites excluding the site on which the policy is applied.
- The prefix-list assigns at least one unicast subnet to each remote hub site.

Configuration Example of Hub-and-spoke Multicast Using the CLI

The following example shows the configuration of centralized control policy for hub-and-spoke deployment:

```
policy
 lists
  tloc-list Hub-TLOCs
   tloc 10.10.10.2 color biz-internet encap ipsec
```

```
   tloc 192.0.2.1 color biz-internet encap ipsec
  !
  site-list Branches
   site-id 140
   site-id 68
  !
  site-list DCs
   site-id 50
   site-id 67
  !
 !
 control-policy Hub-Control-Policy
  sequence 11
   match tloc
    site-list DCs
   !
   action accept
   !
  !
  sequence 31
   match route
    site-list DCs
   !
   action accept
   !
  !
  default-action reject
 !
 control-policy Spoke-Control-Policy
  sequence 1
   match tloc
    site-list Branches
   !
   action reject
   !
  !
  sequence 11
   match tloc
    site-list DCs
   !
   action accept
   !
  !
  default-action reject
 !
!
apply-policy
 site-list Branches
  control-policy Spoke-Control-Policy out
 !
 site-list DCs
  control-policy Hub-Control-Policy out
 !
!
```

The following example shows the spoke configuration for hub-and-spoke multicast deployment:

```
sdwan
 multicast
  address-family ipv4 vrf 1
   spoke
  !
 !
!
```

Verify Multicast Routing on Hub-and-Spoke

Use the command **show platform software sdwan multicast active-sources vrf** on spokes to verify multicast source active route next-hop pointing to the selected replicator.

```
Device# show platform software sdwan multicast active-sources vrf 1

Multicast SDWAN Overlay Received Source-Active Routes:
  (10.0.0.0, 255.0.0.0) next-hop: 192.168.255.254
      src-orig-count: 1, rp-addr: 10.0.0.1
```