



Configuring SPB-PIM Gateway

Release 6.0.1
NN47500-512
Issue 02.01
December 2016

© 2016, Avaya, Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/LICENSEINFO) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR

IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/LICENSEINFO), UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at <https://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the

documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE

WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <https://support.avaya.com> or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <https://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: New in this document	7
Release 6.0.1.....	7
Chapter 2: SPB-PIM Gateway fundamentals	8
IP Multicast over Fabric Connect in Protocol Independent Multicast networks.....	8
SPB-PIM Gateway.....	11
SPB-PIM GW components.....	13
SPB-PIM Gateway Controller Node.....	13
SPB-PIM Gateway Node.....	15
MSDP overview.....	17
Source Active messages.....	17
Reverse Path Forwarding check.....	18
SA redistribution and filtering.....	18
MSDP and SPB-PIM GW.....	19
Full mesh group.....	20
Chapter 3: Multicast Source Discovery Protocol configuration	21
Basic MSDP configuration using CLI	21
Configuring the MSDP originator ID.....	21
Configuring MSDP on a VRF.....	22
Enabling MSDP globally.....	22
Creating an MSDP peer.....	22
MSDP peer configuration using CLI	24
Configuring a peer description.....	24
Securing control messages.....	24
Configuring the MSDP peer SA limit.....	25
Limiting which packets the router sends	26
Configuring the MSDP peer keep alive messages.....	27
Configuring the MSDP peer connect-retry period.....	28
Clearing the peer connection.....	29
Deleting an MSDP peer.....	29
MSDP message control using CLI	30
Filtering PIM routes.....	30
Filtering SA messages.....	31
Configuring MSDP mesh groups.....	32
Clearing the MSDP SA cache.....	32
MSDP verification using CLI	33
Displaying the peer information.....	33
Displaying the SA cache.....	35
Displaying the MSDP count.....	36
Displaying the MSDP summary.....	37

Displaying the RPF peer information.....	38
Displaying the MSDP mesh group information.....	38
Displaying the SA check information.....	39
Displaying all MSDP information.....	40
Basic MSDP configuration using EDM.....	43
Configuring the MSDP originator ID.....	43
Enabling MSDP.....	44
Creating an MSDP peer.....	45
MSDP peer configuration using EDM.....	49
Securing control messages.....	49
Configuring the MSDP peer SA limit.....	52
Configuring a peer description.....	56
Configuring the MSDP peer time to live threshold.....	60
Configuring the MSDP peer keepalive messages.....	64
Configuring the MSDP peer connect-retry period.....	68
Changing the MSDP peer status.....	71
Deleting an MSDP peer.....	75
MSDP message control using EDM.....	78
Filtering PIM routes.....	78
Filtering SA messages.....	80
Configuring the MSDP mesh groups.....	83
Clearing the MSDP SA cache.....	84
MSDP verification using EDM.....	85
Viewing peer information.....	85
Viewing the local SA cache.....	88
Viewing the foreign SA cache.....	89
Viewing the mesh group.....	90
Chapter 4: Controller configuration.....	91
Controller configuration using CLI	91
Enabling the Controller.....	91
Displaying the Controller admin status.....	92
Displaying the active Controller and Gateway Nodes.....	92
Configuring a static foreign source on the global router.....	94
Configuring a static foreign source on a VRF.....	95
Displaying foreign sources.....	95
Displaying Multicast over Fabric Connect sources.....	97
Controller configuration using EDM.....	99
Enabling the Controller.....	99
Displaying the Controller and Gateway admin status.....	99
Displaying active Controller and Gateway nodes.....	100
Configuring a static foreign source globally.....	100
Configuring a static foreign source on a VRF.....	101
Displaying foreign sources.....	102

Displaying Multicast over Fabric Connect sources.....	103
Chapter 5: Gateway configuration.....	104
Gateway Configuration using CLI.....	104
Enabling the Gateway.....	104
Displaying the Gateway admin status.....	105
Displaying the active Controller and Gateway Nodes.....	108
Gateway Configuration using EDM.....	110
Enabling the Gateway globally.....	110
Displaying the Controller and Gateway admin status.....	110
Displaying foreign sources.....	111
Displaying active Controller and Gateway nodes.....	111
Chapter 6: SPB-PIM Gateway interface configuration.....	113
SPB-PIM Gateway interface configuration using CLI.....	113
Enabling SPB-PIM Gateway on a VLAN.....	113
Enabling SPB-PIM Gateway on a brouter port interface.....	114
Configuring the SPB-PIM Gateway VLAN optional parameters.....	115
Configuring the SPB-PIM Gateway brouter port optional parameters.....	115
Displaying the SPB-PIM Gateway brouter port information.....	116
Displaying the SPB-PIM Gateway VLAN information.....	117
Displaying the SPB-PIM Gateway neighbor information.....	118
Displaying the SPB-PIM Gateway multicast routes.....	119
Displaying the IP mroute routes.....	121
SPB-PIM Gateway interface configuration using EDM.....	122
Enabling SPB-PIM Gateway on a VLAN.....	122
Enabling SPB-PIM Gateway on a Brouter port interface.....	122
Configuring SPB-PIM Gateway VLAN optional parameters.....	123
Configuring the SPB-PIM Gateway Brouter port optional parameters.....	124
Displaying the SPB-PIM Gateway interface default values.....	124
Displaying the SPB-PIM Gateway brouter port information.....	125
Displaying the SPB-PIM Gateway VLAN information.....	126
Displaying the SPB-PIM Gateway neighbor information.....	126
Displaying the IP mroute routes.....	127
Chapter 7: SPB-PIM Gateway deployment scenarios.....	129
SPB-PIM Gateway base case deployment scenario.....	129
Source Specific Multicast.....	134
Peer Mesh Group.....	135
Multi domain.....	137
SPB domain interconnect.....	137
Glossary.....	139

Chapter 1: New in this document

Configuring SPB-PIM Gateway is a new document for Release 6.0 so all the features are new in this release.

Release 6.0.1

This document is updated to include minor edits.

Release 6.0

SPB-PIM Gateway

SPB-PIM Gateway (SPB-PIM GW) provides multicast inter-domain communication between an SPB network and a Protocol Independent Multicast (PIM) network. SPB-PIM GW accomplishes this inter-domain communication across a special gateway VLAN. The gateway VLAN communicates with the PIM network through the PIM protocol messaging and translates the PIM network requirements into SPB language and vice versa.

Chapter 2: SPB-PIM Gateway fundamentals

This section provides conceptual content to help you configure and customize SPB-PIM Gateway (SPB-PIM GW) on the switch.

IP Multicast over Fabric Connect in Protocol Independent Multicast networks

IP Multicast over Fabric Connect provides simplicity in provisioning and deploying IP multicast bridging and routing. Also, due to the fact that only one control plane protocol (IS-IS) exists, convergence times in the event of a network failure, are typically sub second.

IP Multicast over Fabric Connect

IP Multicast over Fabric Connect introduces extensions to the SPBM IS-IS control plane to exchange IP multicast stream advertisement and membership information. IP Multicast over Fabric Connect uses these extensions, along with the Internet Group Management Protocol (IGMP) Snooping and Querier functions at the edge of the SPBM cloud, to create sub-trees of the VSN SPB for each multicast group to transport IP multicast data.

With IP Multicast over Fabric Connect, the switch supports the following:

- Layer 2 Virtual Services Network with IGMP support on the access networks for optimized forwarding of IP multicast traffic in a bridged network (Layer 2 VSN with IP Multicast over Fabric Connect). Example application: Multicast in data centers.
- IP multicast routing support for IP Shortcuts using SPBM in the core and IGMP on the access (IP Shortcuts with IP Multicast over Fabric Connect). Example applications: Video surveillance, TV/Video/Ticker/Image distribution, VX-LAN.
- Layer 3 Virtual Services Network with VRF based routing support for IP Multicast over Fabric Connect in the core and IGMP on the access (Layer 3 VSN with IP Multicast over Fabric Connect). Example applications: Video surveillance, TV/Video/Ticker/Image Distribution, VXLAN, Multi-tenant IP multicast.

Important:

Sources must be IGMP enabled to support discovery functions specific to the multicast applications in use.

For more information on Multicast over Fabric Connect, see *Configuring Fabric Connect*.

IP Multicast over Fabric Connect restrictions

- IP Multicast over Fabric Connect cannot connect to an IP Multicast router outside the SPB network.
- You can only deploy IP Multicast over Fabric Connect in environments where there are no multicast routers between the edge of the SPB network and the IP Multicast hosts that connect to the network.
- An existing network which is Protocol Independent Multicast (PIM) based cannot participate in the SPB network either by connecting to SPB originated streams or by injecting PIM network streams into the SPB network.
- In certain environments it is not possible to deploy an SPB network all the way to the point where the SPB network directly connects to an IGMP edge.

You encounter these restrictions during the following typical deployment scenarios:

- **Scenario 1:** You deployed IP Multicast using PIM and want to expand the network by deploying SPB for the new portion of the network. You want multicast applications to work across the old and new portion of the network.
- **Scenario 2:** Multicast traffic is exchanged between independent network operators at the boundary between their networks. PIM is the multicast routing protocol. A network operator wants to upgrade or replace the existing network to an SPB network. The inter-domain multicast traffic exchanges with other networks should not be disrupted.

The following figure shows the traditional Multicast over Fabric Connect environment with no PIM routers.

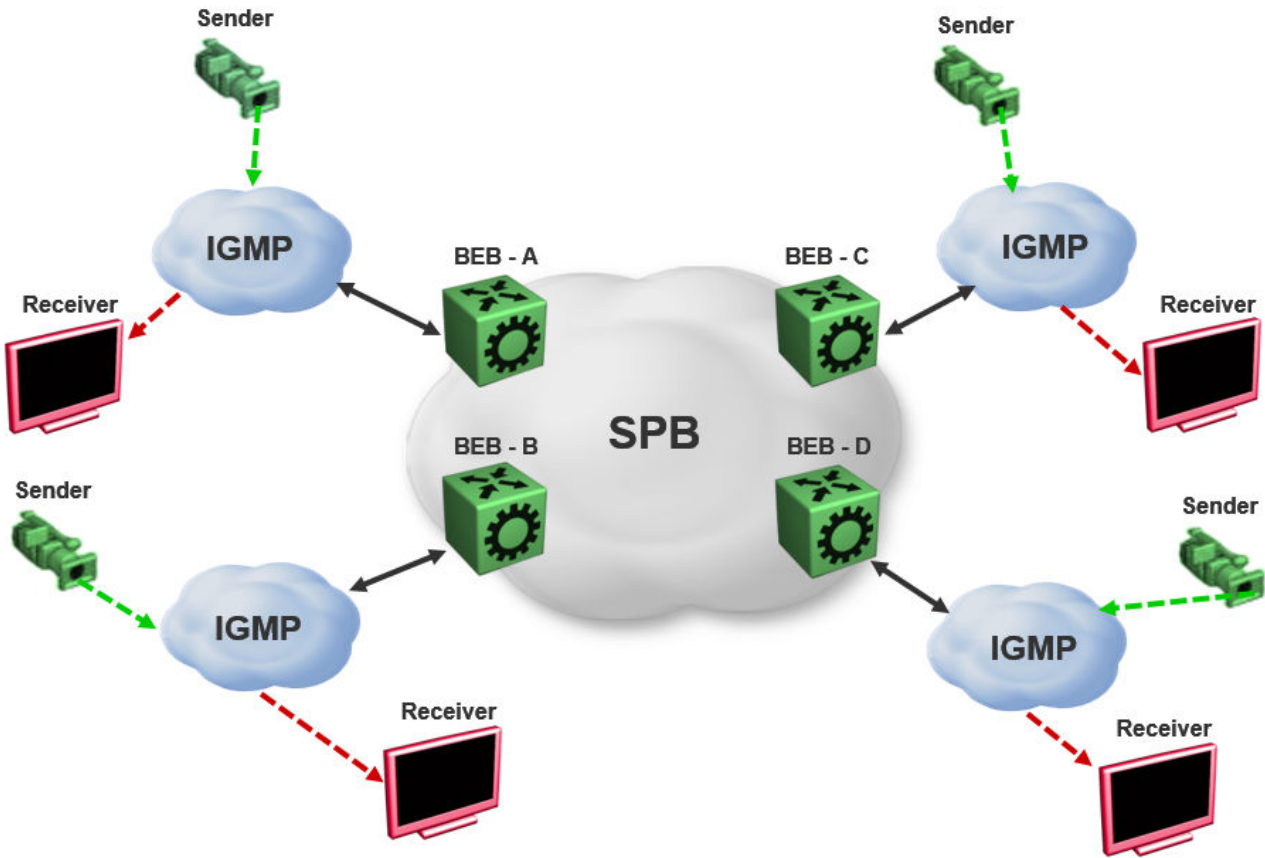


Figure 1: IP Multicast over Fabric Connect streams

In the above figure, sources and receivers on the edges of the SPB network are IGMP hosts and sources of multicast data. Hence, the traditional Multicast over Fabric Connect host-to-host deployment works.

The following figure shows the traditional Multicast over Fabric Connect environment with PIM routers.

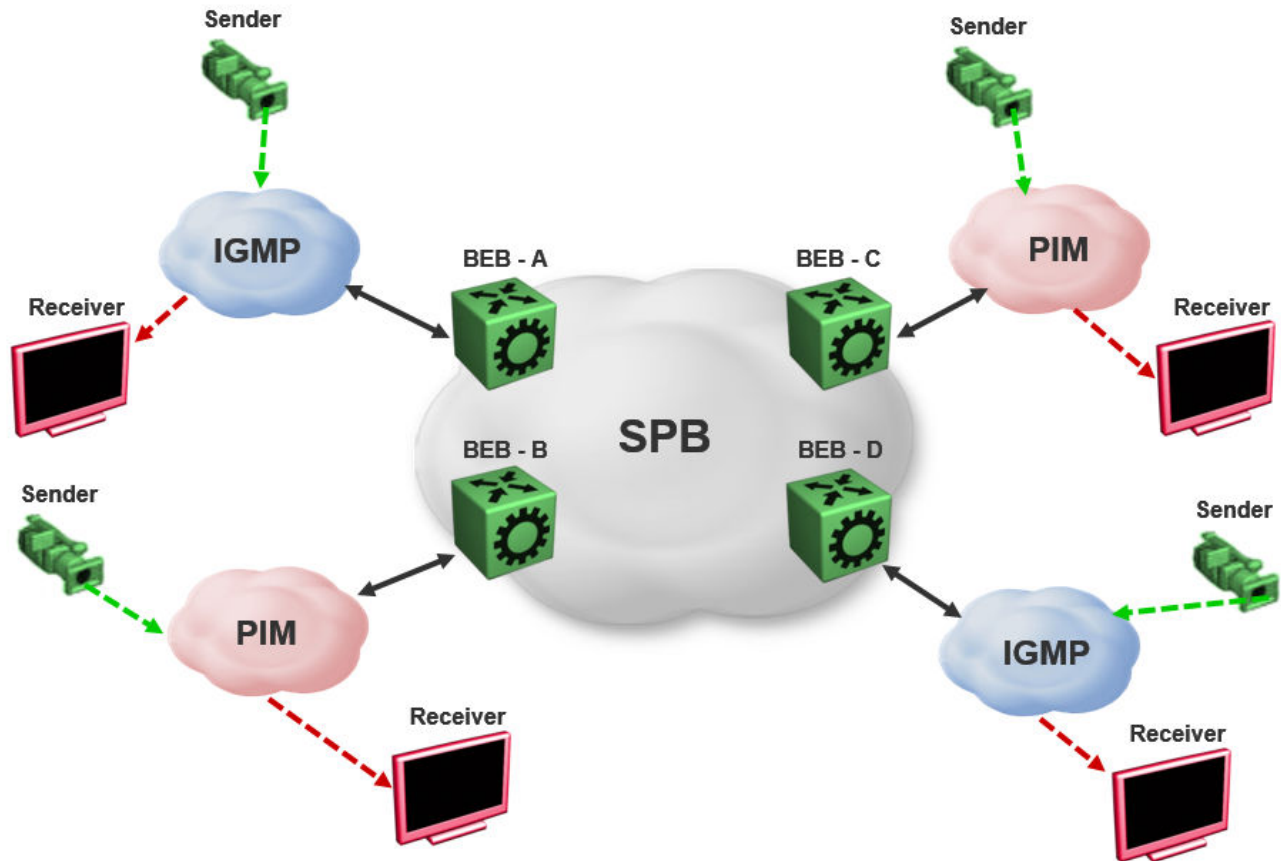


Figure 2: IP Multicast over Fabric Connect Streams

In the above figure, sources and receivers on the edges of the SPB network, which are IGMP or source hosts can communicate over the SPB network. Sources and receivers connected to PIM routers cannot participate in the SPB network.

SPB-PIM Gateway

Multicast over Fabric Connect cannot connect to a PIM router that is external to the SPB network. When a receiver joins the SPB network for a specific group, the receiver must receive multicast streams in the neighboring multicast domains (PIM network). Similarly, a receiver in the neighboring multicast domain (PIM network) must receive multicast streams from sources in the SPB network. SPB-PIM Gateway (SPB-PIM GW) provides multicast inter-domain communication between an SPB network and a PIM network. SPB-PIM GW accomplishes this inter-domain communication across a special gateway VLAN. The gateway VLAN communicates with the PIM network through a subset of the full protocol messaging required for RFC 4601 compliance of a PIM interface, and translates the PIM network requirements into SPB language and vice versa.

SPB-PIM GW provides the following functionality:

- One or more SPB domains can share streams with one or more PIM domains.
- SPB-PIM GW can connect two independent SPB domains. The independent SPB domains connected by SPB-PIM GW share a subset of multicast streams without a PIM network in between.

Multicast over Fabric Connect with SPB-PIM GW

In a Multicast over Fabric Connect environment with SPB-PIM GW, the SPB network connects sources and receivers from one or more PIM networks. The multicast traffic is then delivered across the domain boundaries through a path that transports the multicast traffic.

Multicast over Fabric Connect with SPB-PIM GW functionality consists of SPB nodes, which act as SPB-PIM Controller nodes and SPB-PIM Gateway nodes. The SPB Controller uses the Multicast Source Discovery Protocol (MSDP) to discover foreign sources.

The following figure shows the Multicast over Fabric Connect environment with SPB-PIM GW.

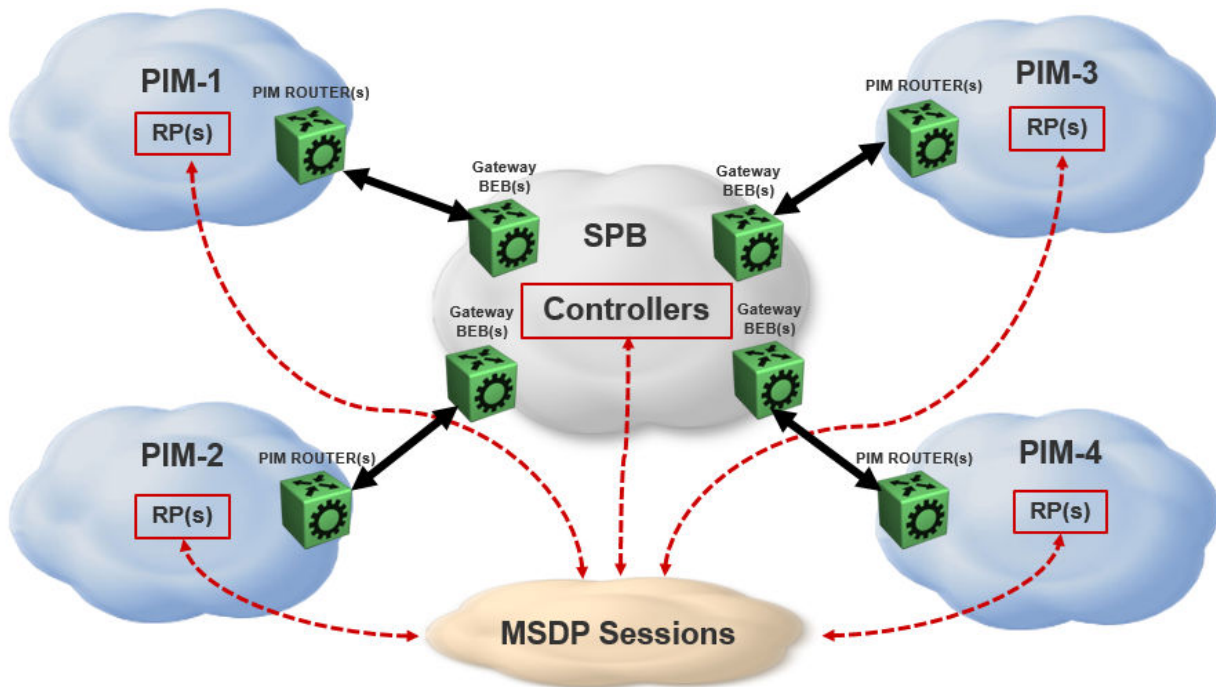


Figure 3: Multicast over Fabric Connect with SPB-PIM GW

SPB-PIM GW components

SPB-PIM GW has two functional components:

- SPB-PIM Gateway Controller Nodes (Controller), which are used for multicast source discovery.
- SPB-PIM Gateway Nodes (Gateway), on which the SPB-PIM Gateway interfaces reside.

*** Note:**

The Controller and Gateway can reside in a single node.

The following figure shows the SPB-PIM GW components.

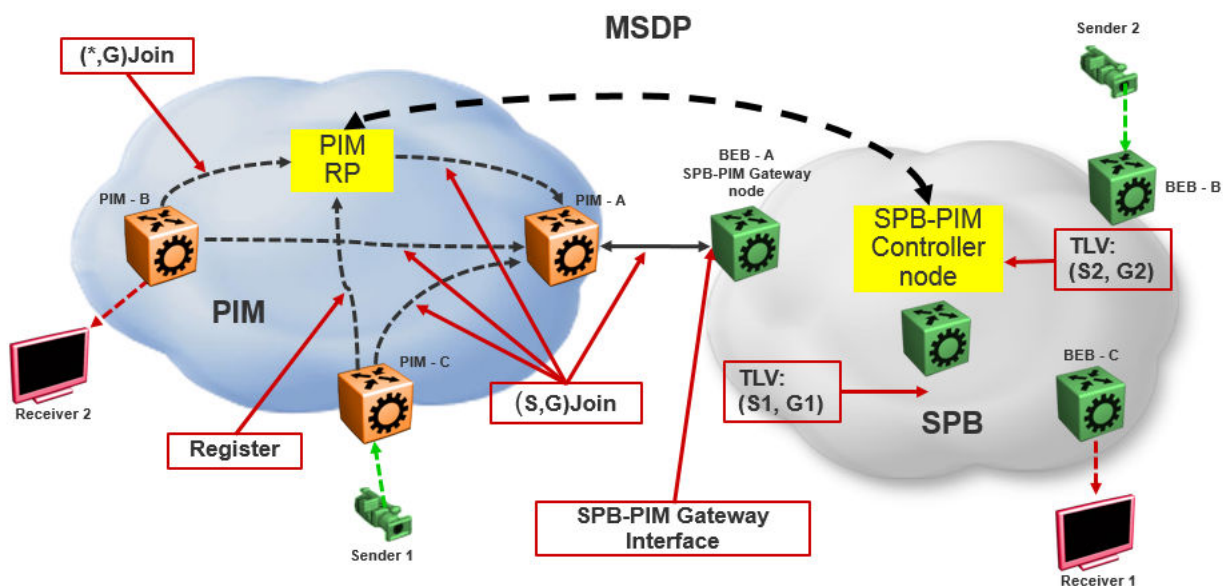


Figure 4: SPB-PIM GW components

SPB-PIM Gateway Controller Node

SPB-PIM Gateway Controller Node (Controller) shares stream information between the local SPB domain and a foreign domain. The foreign domain is the PIM network Rendezvous point (RP) or another SPB domain Controller.

The Controller functionality is outlined below:

- The Controller discovers PIM sources for a specific multicast group and distributes them to the Gateways.

*** Note:**

PIM source discovery is either through MSDP or static configuration of foreign streams at the Controller.

- The Controller advertises local SPB originated streams through MSDP to another PIM domain or another SPB domain.
- The Controller references the Unicast IP route table to determine which Gateway has the best route to the PIM source. The Controller then assigns the stream to the selected Gateway.

The Controller Node has the following components:

- Source Discovery (MSDP and static configuration)
- Gateway Selection Controller

Source Discovery (MSDP and static configuration)

MSDP resides in the Controller BEB or Controller BCB and PIM network RP that wish to advertise multicast source information between domains.

You can implement SPB-PIM GW under the following scenarios:

- The multicast source resides in the Protocol Independent Sparse Module (PIM-SM) domain. The multicast source must be discovered by MSDP residing on the Gateway Controller in the SPB domain.
- The multicast source resides in the SPB domain. The multicast source must be advertised to the neighboring PIM domain through MSDP peers.

For more information on MSDP, see [MSDP overview](#) on page 17.

*** Note:**

You can also configure multicast sources statically on the Controller. Static configuration is useful for SSM multicast group range streams in the foreign domain, which are not advertised by MSDP. Static configuration is also useful for when two SPB domains are connected through a PIM Gateway, and want to only advertise a subset of streams to each other, without enabling MSDP.

Gateway Selection Controller

The Gateway Selection Controller resides in the Controller BEB or Controller BCB node in the SPB network. The Gateway Selection Controller receives source information from MSDP or through static configuration. The source information consists of the following components:

- Sender IP address (S)
- Group IP address (G)
- VRF ID of the stream
- RP of the source (optional)

Gateway Selection Controller finds the best BEB (Gateway Node) in the SPB network through which the sender sends traffic to group G. The Gateway Selection Controller performs the following tasks:

- The Gateway Selection Controller uses Layer 3 reachability information to reach S, which is retrieved from the ISIS IP Shortcuts (IPSC) database.
- The VSN identifier (ISID) is determined by using the VRF ID provided by MSDP.

- The Gateway Selection Controller uses the VRF ID and searches the IP shortcut database to determine which Gateway is closest to S.

*** Note:**

If multiple BEBs have a route to S, the BEB with the lowest Layer 3 metric is selected as the Gateway.

*** Note:**

If a Gateway link fails or the cost of the route changes, the selection process identifies the link failure as a route change and selects another best Gateway BEB.

The selected Gateway BEB for a stream must satisfy the following criteria:

- The selected Gateway BEB for a stream must announce a route to the source of the foreign stream through ISIS.

*** Note:**

Among all the routes to the source of the foreign stream announced by different BEBs through ISIS, the route announced by the selected Gateway has the longest prefix match and has the lowest external route metric.

- If multiple BEBs meet the Gateway selection criteria, a deterministic hash function of system ID, source IP address, and group IP address is used. The deterministic hash function is computed for each of the BEBs that meet the Gateway selection criteria. The BEB that generates the lowest hash value is selected as the Gateway for the stream.

The result of the Gateway selection process is saved in the Gateway assignment table. The Gateway assignment table consists of VSN identifier or ISID, S, G, and the selected Gateway BEB. Having only one selected Gateway BEB ensures that traffic from source S is drawn into the SPB network by only one BEB, the selected Gateway BEB. The selection Controller then distributes the Gateway assignment table information to all the Gateway nodes.

SPB-PIM Gateway Node

The SPB-PIM Gateway Node (Gateway) has the following components:

- Gateway Selection Agent
- SPB-PIM Gateway interface

Gateway Selection Agent

The Gateway Selection Agent (Agent) resides in the Gateway BEB Node in the SPB network. The Gateway BEB has connections into the foreign network over SPB-PIM Gateway Interfaces. The Agent receives foreign network source information from the Controller BEB or the Controller BCB Node. The source information consists of the following components:

- Sender IP address (S)
- Group IP address (G)
- VSN identifier (ISID)
- Gateway assigned to the stream

The Agent interacts with SPB-PIM Gateway interface and creates the multicast path. The Agent receives foreign source information from the Controller and creates a foreign source address (SA) cache after validating the reachability to S. The Agent interacts with the SPB-PIM Gateway interface to validate that the next-hop ip address toward the source is a valid PIM adjacency. The foreign SA cache includes the following components:

- Source IP address (information received from the Gateway Controller)
- Group IP address (information received from the Gateway Controller)
- Ingress port (The port through which S is accessible)
- Upstream IP address (The next-hop IP address, which is also the PIM neighbor across the SPB-PIM Gateway interface which is used to reach S as indicated by the unicast routing entry)
- Ingress VLAN ID

If multiple next-hops are available, then the first valid PIM neighbor next-hop is used for the upstream.

*** Note:**

If the Agent receives the same source information from multiple Controllers, then the Agent takes action only for the information received from the preferred Controller. The Controller with the lowest system ID is the preferred Controller.

SPB-PIM Gateway interface

The SPB-PIM Gateway interface provides inter-domain multicast services. The SPB-PIM Gateway interface connects senders and receivers of multicast streams across a PIM Domain and a SPB network boundary over a Gateway interface. The SPB-PIM Gateway interface provides the following functionality:

- PIM HELLO exchanges
- Issuing Joins and Leaves
- Process received Joins and Leaves
- Implements the Gateway assignment table by acting as the Ingress BEB for streams for which the SPB-PIM Gateway interface is the selected Gateway
- Enforces the Gateway assignment table and does not forward streams for which the SPB-PIM Gateway interface is not the selected Gateway
- Forwards local and remote SPB streams to satisfy stream requests from neighboring multicast domains
- SPB-PIM Gateway Interfaces supports both SM and SSM multicast group range joins and prunes. *G joins are only supported in SM group range.

The PIM Gateway interface resides in the SPB-PIM Gateway Node (Gateway). The SPB-PIM Gateway interface connects to a PIM router in a PIM network or to another Gateway BEB in an SPB network. Local hosts (IGMP member hosts and multicast data source hosts) are not supported on SPB-PIM Gateway interfaces, only PIM Routers or another SPB BEB with SPB-PIM Gateway interface configured. Multicast data from local source hosts and IGMP reports from local hosts are dropped. An SPB Node must be configured as a SPB-PIM Gateway Node if the SPB Node is connected to a foreign PIM network or a foreign SPB network. A single Gateway Node can have multiple SPB-PIM Gateway interfaces. The SPB-PIM Gateway interface can be a VLAN or a brouter port, can reside on an MLT and is fully virtualized. The SPB-PIM Gateway interface is a translation mechanism between the PIM protocol and SPB TLVs.

*** Note:**

- Only PIM protocol messages are communicated over the SPB-PIM Gateway interface
- Only SPB TLVs are communicated over Fabric Connect over SPB
- The SPB-PIM Gateway interface is the only component that handles the translation mechanism

The SPB-PIM Gateway interface communicates with the PIM router through the standard PIM protocol messaging HELLO, JOIN, and PRUNE. The SPB-PIM Gateway interface then forms a normal PIM adjacency with the PIM router or another SPB Gateway Node. The SPB-PIM Gateway Interface processes received SG joins and prunes, *G joins and prunes, and SG-RPT joins and prunes. The SPB-PIM Gateway interface transmits SG joins and prunes, but never *G joins. The SPB-PIM Gateway Interface does not have RP capabilities, and therefore has no need for group-to-RP mapping configurations. A *G JOIN received on a SPB-PIM Gateway Interface is accepted if the destination IP is the IP address of the interface or of a neighbor on the interface if the neighbor is learned on another port in the interface. However, the RP address within the *G JOIN message is ignored by the SPB-PIM Gateway Interface.

MSDP overview

MSDP enables advertisement of multicast source information between different PIM-SM domains. This function of MSDP in SPB-PIM GW topologies is to advertise multicast source information between SPB domains and PIM domains. MSDP routers in a PIM-SM or SPB domain have a peering relationship with MSDP peers in another domain. The peering relationship is a TCP connection in which the control information is exchanged. The TCP connection between peers uses the underlying unicast routing system.

Source Active messages

In a PIM domain, MSDP enabled routers are RPs. MSDP routers form adjacencies through TCP port 639 to share multicast source information. This functionality is similar to the Border Gateway Protocol (BGP). When an MSDP router receives multicast source information, the routers use reachability information to perform Reverse Path Forwarding (RPF) checks. The reachability information is exchanged through BGP or any other unicast routing protocol.

When a RP router learns of a new (S,G), the RP router saves the (S,G) information and the RP address in the MSDP Source Active (SA) local cache. The RP router learns the new (S,G) through a directly connected source or PIM register message. The RP router then sends an SA update message which contains (S,G,RP) information to the MSDP peers. The MSDP peers broadcast the SA to RPs in their local domains and to their MSDP peers in other PIM-SM domains.

*** Note:**

A PIM domain is a set of routers in a single Autonomous System (AS), which uses the same RP for any given multicast group.

When an SPB-PIM Gateway Controller in the SPB domain learns of a new (S,G) in its own domain, the Controller saves the (S,G) information in the local SA cache. The Controller learns the new (S,G) through a directly connected source or Intermediate-System-to-Intermediate-System (IS-IS). The controller sends an SA update message to the MSDP peers in the PIM domain. SA uses the CLIP address configured on the controller as the RP address.

*** Note:**

Configure CLIP before you enable MSDP. Peer connections use the CLIP address as the local address.

Reverse Path Forwarding check

When an MSDP peer receives the SA from a peer, the MSDP performs an RPF check. The RPF check ensures that the SA received from the MSDP peer is the closest to the originating RP. An RPF check prevents SA loops.

*** Note:**

This RPF check is different from the multicast routing RPF check.

If the RPF checks pass, then the receiving MSDP enabled router saves the SA information in the SA foreign cache and makes it available to the local domain. Each MSDP peer floods the SA information away from the originating RP. The flooding process is called peer RPF flooding.

SA redistribution and filtering

Redistribution and filtering is used to control SA flooding. The MSDP redistribute policy is applied on the MSDP node that originates the SAs to control which SAs are advertised on all MSDP peers. An SA filter is applied to a specific MSDP peer in the inbound direction or outbound directions or both inbound and outbound direction on any MSDP router. Filtering is multicast group based.

When configuring MSDP redistribution, use prefix lists to create the route policies. When a route policy is created it must match the group prefix with the name of the prefix list created for the group address. If deny action is set for the lists in the route-policy, the policy blocks the matching groups from all the sources. If permit action is set for the lists in the route-policy, the policy accepts the matching groups from all the sources. MSDP redistribution does not refer to the redistribution of SPB domain sources to MSDP. MSDP redistribution refers to SAs which needs to be redistributed to other MSDP peers.

*** Note:**

MSDP redistribution is applied globally to all MSDP peers. SA filtering is used to filter SAs on a peer-to-peer level.

MSDP and SPB-PIM GW

The SPB-PIM GW functional component for MSDP resides in the SPB-PIM Gateway Controller node (Controller).

Overview

Controllers from an SPB network discover sources through MSDP sessions with RPs from a PIM network. Once the SA packet is received at the MSDP module of the Controller, the IP routing table is examined to determine which peer is the next hop towards the originating RP of the SA message. Once the SA RPF test passes, the SA packet is saved in the foreign cache and passed to the Controller.

The Controller nodes also distribute the sources from an SPB domain to a PIM domain through an MSDP session with RPs in the PIM network. Similar to RP, when a Controller in the SPB domain learns of a new (S,G), through a directly connected source or ISIS, the Controller saves the new (S,G) in its local SA cache. The Controller then transmits an SA update message for this source to its MSDP peers in the PIM domain. The Controller that sends the SA to the MSDP is viewed as the RP (circuitless IP interface is used).

MSDP as part of SPB-PIM GW

MSDP does not work with the traditional PIM implementation. MSDP communicates only with the Controller and should be configured as an IP endpoint.

MSDP configuration considerations:

- A circuitless IP interface (CLIP) is used in the context of global router or VRF, hence at least one CLIP in each VRF should be configured.
- MSDP should use a single CLIP address as the source for establishing all MSDP connections in the same VRF.
- For SPB sources, this CLIP is used as the RP in all SA messages advertised.
- MSDP source IP address should be one of the CLIP interfaces pre-configured on the global router or VRF.
- The originator-id should be configured before enabling MSDP.

* Note:

MSDP transmits encapsulated multicast data packets inside forwarded MSDP messages. If the received SA is an encapsulated SA, then the switch parses the TTL value of the encapsulated data and compares it against the configured value. If the configured value is less than or equal to the parsed value, then the switch forwards the encapsulated data along with the SA, otherwise the switch forwards the SA alone by stripping the encapsulate data. By default, MSDP forwards encapsulated data along with the SA message. MSDP does not forward the encapsulated data to the local receivers.

When MSDP generates SA messages for SPB sources, the local cache miss data cannot be encapsulated into the SA messages that are sent to the peers.

The switch supports forwarding SA messages with encapsulated data from sources to MSDP peers but not from MSDP peers to the receivers.

For more information on MSDP configuration, see [Multicast Source Discovery Protocol configuration](#) on page 21.

Full mesh group

MSDP mesh groups are full mesh of MSDP peers and is a subset of MSDP speakers. MSDP mesh groups are used for SA flooding which is similar to the BGP route reflector concept. MSDP floods the SA to all the members of the mesh group when:

- The MSDP peers are fully meshed
- The MSDP enabled router learns a new SA from a non-member of its mesh group
- The SA passes the RPF check

The receiving routers accept the SA and forwards it only to any non-mesh Group MSDP peers.

The SPB-PIM Gateway is deployed in two models:

- Model 1: All multicast networks have peering agreements with one another. The full mesh MSDP is setup.
- Model 2 : An inter-domain multicast provider exists. All multicast networks setup MSDP peering with the provider.

The controllers relay SA messages between individual networks.

* Note:

Consider the following when you deploy SPB-PIM Gateway:

- It is recommended to use mesh group of MSDP peers (PIM RP's and SPB-PIM Gateway Controller nodes) to avoid flooding and RPF failure.

* Note:

Since MSDP uses CLIP interface in its peering relation, the MSDP peer may not fall in any of the RFC rules and the MSDP SA messages will be rejected.

- Controllers from the same SPB network must not have MSDP sessions with each other, regardless of whether mesh groups are used or not.
- When using mesh groups, all Controllers within one SPB domain should peer with the same set of RPs and Controllers in adjacent domains, ie, one Controller should not peer with an RP that the other Controllers do not peer with.

Chapter 3: Multicast Source Discovery Protocol configuration

This section provides procedures to configure Multicast Source Discovery Protocol (MSDP) using the Command Line Interface (CLI) and Enterprise Device Manager (EDM).

Basic MSDP configuration using CLI

Configuring the MSDP originator ID

Configure the originator ID to set the Rendezvous Point (RP) address inside the Source Active (SA) message. The RP address must be a pre-configured CLIP interface on the global router or a VRF. The RP address is also the local IP address in all peer relations.

*** Note:**

To delete the originator ID, you must first disable MSDP.

Procedure

1. Enter either Global Configuration mode or VRF Router Configuration mode for a specific VRF context:

```
enable
configure terminal
router vrf WORD<1-16>
```

2. Configure the MSDP originator ID:

```
ip msdp originator-id {A.B.C.D}
```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ip msdp originator-id 2.0.2.2
```

Variable definitions

Use the data in the following table to use the `ip msdp originator-id` command.

Variable	Value
{A.B.C.D}	Specifies the MSDP source IP address. The IP address must be one of the CLIP interfaces configured on the global router or a VRF.

Configuring MSDP on a VRF

Create an MSDP instance on a user defined VRF to allow further configuration to take place. This command does not exist in the Global Configuration mode because the MSDP instance for a default VRF is created by default.

Procedure

1. Enter VRF Router Configuration mode for a specific VRF context:

```
enable
configure terminal
router vrf WORD<1-16>
```

2. Create the MSDP instance:

```
ip msdp
```

Enabling MSDP globally

Enable or disable MSDP globally on the device to allow further configuration to take place.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable MSDP globally on the switch:

```
ip msdp enable
```

Creating an MSDP peer

Create an MSDP peer to establish a peer relationship between the local MSDP enabled router and a peer in another domain.

! Important:

Do not enable more than 20 active peers.

Procedure

1. Enter either Global Configuration mode or VRF Router Configuration mode for a specific VRF context:

```
enable
configure terminal
router vrf WORD<1-16>
```

2. Create an MSDP peer:

```
ip msdp peer {A.B.C.D}
```

3. Enable an MSDP peer:

```
ip msdp peer {A.B.C.D} enable
```

*** Note:**

MSDP peer is disabled by default.

4. **(Optional)** Specify the remote autonomous system (AS) number of the MSDP peer:

```
ip msdp peer {A.B.C.D} remote-as WORD<0-11>
```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ip msdp peer 21.0.0.2
Switch:1(config)#ip msdp peer 21.0.0.2 enable
Switch:1(config)#ip msdp peer remote-as 1
```

Variable definitions

Use the data in the following table to use the `ip msdp peer` command.

Variable	Value
{A.B.C.D}	Specifies the MSDP peer IP address.
WORD<0-11>	Specifies the AS number of the MSDP peer, 0-65535 (2-Byte AS) 0-4294967295 (4-Byte AS).

MSDP peer configuration using CLI

Configuring a peer description

Configure a peer description to add descriptive text to an MSDP peer for easy identification of a peer.

Procedure

1. Enter either Global Configuration mode or VRF Router Configuration mode for a specific VRF context:

```
enable
configure terminal
router vrf WORD<1-16>
```

2. Configure the peer description:

```
ip msdp description {A.B.C.D} WORD<1-255>
```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ip msdp peer 21.0.0.2 primary
```

Variable definitions

Use the data in the following table to use the `ip msdp description` command.

Variable	Value
{A.B.C.D}	Specifies the MSDP peer IP address.
WORD<1-255>	Specifies a descriptive text to a MSDP peer in the range of 1-255 characters. To include spaces in the peer description, enclose the text string in quotation marks.

Securing control messages

Configure Message Digest (MD) 5 authentication to secure control messages on the TCP connection between MSDP peers.

Procedure

1. Enter either Global Configuration mode or VRF Router Configuration mode for a specific VRF context:


```
enable
configure terminal
router vrf WORD<1-16>
```

2. Enable MD5 authentication:

```
ip msdp md5-authentication {A.B.C.D} [enable]
```

3. Specify the case sensitive password for MD5 authentication:

```
ip msdp password peer {A.B.C.D} WORD<1-80>
```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ip msdp md5-authentication 21.0.0.2 enable
Switch:1(config)#ip msdp password peer 21.0.0.2 helloworld
```

Variable definitions

Use the data in the following table to use the `ip msdp` command.

Variable	Value
{A.B.C.D}	Specifies the MSDP peer IP address.
WORD<1-80>	Specifies the MD5 authentication password.

Configuring the MSDP peer SA limit

Configure the SA limit to limit the number of SA messages from an MSDP peer that the router saves in the SA cache. The default value is 6,144 messages.

Procedure

1. Enter either Global Configuration mode or VRF Router Configuration mode for a specific VRF context:

```
enable
configure terminal
router vrf WORD<1-16>
```

2. Configure the SA limit:

```
ip msdp sa-limit {A.B.C.D} <0-6144>
```

Example

```
Switch:1>enable
Switch:1#configure terminal
```

```
Switch:1(config)#ip msdp sa-limit 21.0.0.2 6100
```

Variable definitions

Use the data in the following table to use the `ip msdp sa-limit` command.

Variable	Value
{A.B.C.D}	Specifies the MSDP peer IP address.
<0-6144>	Specifies the maximum number of SA messages to keep in SA cache.

Limiting which packets the router sends

Configure the time-to-live (TTL) threshold to limit which multicast data packets the router encapsulated in SA Message forwarded to an MSDP peer. The TTL limits the number of hops a packet can take before the router drops the packet. The router sends out SA Messages with encapsulated data only if TTL equals or exceeds the value you configure. If the TTL is lower than the value you configure, the router drops the data packet and forwards the SA Message without the encapsulated data.

* Note:

MSDP transmits encapsulated multicast data packets inside forwarded MSDP messages. If the received SA is an encapsulated SA, then the switch parses the TTL value of the encapsulated data and compares it against the configured value. If the configured value is less than or equal to the parsed value, then the switch forwards the encapsulated data along with the SA, otherwise the switch forwards the SA alone by stripping the encapsulate data. By default, MSDP forwards encapsulated data along with the SA message. MSDP does not forward the encapsulated data to the local receivers.

When MSDP generates SA messages for SPB sources, the local cache miss data cannot be encapsulated into the SA messages that are sent to the peers.

The switch supports forwarding SA messages with encapsulated data from sources to MSDP peers but not from MSDP peers to the receivers.

Procedure

1. Enter either Global Configuration mode or VRF Router Configuration mode for a specific VRF context:

```
enable
configure terminal
router vrf WORD<1-16>
```

2. Configure the MSDP peer TTL threshold:

```
ip msdp ttl-threshold {A.B.C.D} <1-255>
```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ip msdp ttl-threshold 21.0.0.2 10
```

Variable definitions

Use the data in the following table to use the `ip msdp ttl-threshold` command.

Variable	Value
{A.B.C.D}	Specifies the MSDP peer IP address.
<1-255>	Specifies the TTL value.

Configuring the MSDP peer keep alive messages

Configure keepalive messages to adjust the interval in seconds at which an MSDP peer sends keep alive messages (default is 60 seconds) and the interval at which the MSDP peer waits for keep alive messages from other peers before it declares them down (default is 75 seconds).

*** Note:**

In a peer relationship, the keep alive interval configured on one peer must be at least 1 second less than the hold time configured on the other side of the peer relationship. This is not applicable when the hold time is set to 0 seconds.

Procedure

1. Enter either Global Configuration mode or VRF Router Configuration mode for a specific VRF context:

```
enable
configure terminal
router vrf WORD<1-16>
```

2. Configure the MSDP peer keep alive interval:


```
ip msdp keepalive {A.B.C.D} <0-21845> <0-65535>
```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ip msdp keepalive 21.0.0.2 70 71
```

Variable definitions

Use the data in the following table to use the `ip msdp keepalive` command.

Variable	Value
{A.B.C.D}	Specifies the MSDP peer IP address.
<0-21845>	Specifies the keep alive interval in seconds. The default is 60 seconds.
<0-65535>	Specifies the hold time interval in seconds. The default is 75 seconds.  Note: 0 seconds means the peer never expires. Values 1 and 2 are not allowed.

Configuring the MSDP peer connect-retry period

Configure the connect-retry period to specify the amount of time, in seconds, between connection attempts for peering sessions. The default is 30 seconds.

Procedure

1. Enter either Global Configuration mode or VRF Router Configuration mode for a specific VRF context:

```
enable
configure terminal
router vrf WORD<1-16>
```

2. Configure the MSDP peer connect-retry period:

```
ip msdp connect-retry {A.B.C.D} <1-65535>
```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ip msdp connect-retry 21.0.0.2 40
```

Variable definitions

Use the data in the following table to use the `ip msdp connect-retry` command.

Variable	Value
{A.B.C.D}	Specifies the MSDP peer IP address.
<1-65535>	Specifies the connect-retry interval in seconds. The default is 30 seconds.

Clearing the peer connection

Clear the peer connection to clear the TCP connection to the specified MSDP peer, and reset all MSDP message counters.

*** Note:**

This procedure does not clear the SA cache entries the router learns from the peer.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Clear the peer connection:

```
clear ip msdp peer {A.B.C.D} [vrf WORD<0-16>] [vrfids WORD<0-512>]
```

Example

```
Switch:1>enable
```

```
Switch:1#configure terminal
```

```
Switch:1(config)#clear ip msdp peer 21.0.0.2
```

Variable definitions

Use the data in the following table to use the `clear ip msdp peer` command.

Variable	Value
{A.B.C.D}	Specifies the MSDP peer IP address.
vrf WORD<0-16>	Specifies the VRF name.
vrfids WORD<0-512>	Specifies the VRF ID.

Deleting an MSDP peer

Use this procedure to delete an MSDP peer.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Clear the peer connection:

```
no ip msdp peer {A.B.C.D}
```

Example

```
Switch:1>enable
```

```
Switch:1#configure terminal
Switch:1(config)#no ip msdp peer 21.0.0.2
```

MSDP message control using CLI

Filtering PIM routes

Filter SPB routes to filter which (S,G,RP) entries sent out to all MSDP peers. This procedure applies only to the rendezvous point (RP) that originates the MSDP SA messages and not the intermediate MSDP peers that forward the received SA messages.

Procedure

1. Enter either Global Configuration mode or VRF Router Configuration mode for a specific VRF context:

```
enable
configure terminal
router vrf WORD<1-16>
```

2. Create the MSDP filter:

```
ip msdp redistribute
```

3. Create the route policy name:

```
ip msdp redistribute route-policy WORD<1-64>
```

4. Apply the redistribution filters:

```
ip msdp apply redistribute
```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ip msdp redistribute
Switch:1(config)#ip msdp redistribute route-policy helloworld
Switch:1(config)#ip msdp apply redistribute
```

Variable definitions

Use the data in the following table to use the `clear ip redistribute` command.

Variable	Value
<i>WORD</i> <1-64>	Specifies the route policy name.

Filtering SA messages

Filter SA messages to determine which SA messages to accept from a peer and which SA messages to send to a peer. By default, no inbound or outbound filter exists.

Procedure

1. Enter either Global Configuration mode or VRF Router Configuration mode for a specific VRF context:

```
enable
configure terminal
router vrf WORD<1-16>
```

2. Create the inbound filter:

```
ip msdp sa-filter in {A.B.C.D}
```

3. Create the inbound filter route policy name:

```
ip msdp sa-filter in {A.B.C.D} route-policy WORD<1-64>
```

4. Create the outbound filter:

```
ip msdp sa-filter out {A.B.C.D}
```

5. Create the outbound filter route policy name:

```
ip msdp sa-filter out {A.B.C.D} route-policy WORD<1-64>
```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ip msdp sa-filter in 21.0.0.2 route-policy helloworld
```

Variable definitions

Use the data in the following table to use the `ip msdp sa-filter` command.

Variable	Value
{ <i>A.B.C.D</i> }	Specifies the MSDP peer IP address.
route-policy <i>WORD</i> <1-64>	Specifies the route policy name for an inbound or outbound filter.

Configuring MSDP mesh groups

Configure mesh groups to reduce SA flooding. A mesh group does not forward SA messages to other group members. The originator, which is also a mesh group member, forwards SA messages to all group members. Create MSDP mesh groups from a group of meshed MSDP speakers from a domain.

*** Note:**

The MSDP router does not belong to any mesh group by default.

Procedure

1. Enter either Global Configuration mode or VRF Router Configuration mode for a specific VRF context:

```
enable
configure terminal
router vrf WORD<1-16>
```

2. Configure the MSDP mesh group:

```
ip msdp mesh-group WORD<1-64> {A.B.C.D}
```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ip msdp mesh-group helloworld 21.0.0.2
```

Variable definitions

Use the data in the following table to use the `ip msdp mesh-group` command.

Variable	Value
<code>WORD<1-64></code>	Specifies the mesh group name.
<code>{A.B.C.D}</code>	Specifies the MSDP peer IP address.

Clearing the MSDP SA cache

Clear the SA cache to clear the SA entries the router learns from all peers or a specific peer.

*** Note:**

This procedure clears the foreign cache. This procedure does not clear the local cache.

Procedure

1. Enter Privileged EXEC mode:


```
enable
```

2. Clear the SA cache for all peers:

```
clear ip msdp sa-cache [vrf WORD<0-16>] [vrfids WORD<0-512>]
```

3. Clear the SA cache for a specific peer:

```
clear ip msdp sa-cache peer {A.B.C.D} [vrf WORD<0-16>] [vrfids WORD<0-512>]
```

4. Clear the SA cache for a specific group range, source range, and RP.

```
clear ip msdp sa-cache [source prefix/len] [group prefix/len] [rp {A.B.C.D}] [vrf WORD<0-16>] [vrfids WORD<0-512>]
```

Example

```
Switch:1>enable
```

```
Switch:1#configure terminal
```

```
Switch:1(config)#clear ip msdp sa-cache peer 21.0.0.2
```

Variable definitions

Use the data in the following table to use the `clear ip msdp sa-cache` command.

Variable	Value
{A.B.C.D}	Specifies the MSDP peer IP address.
vrf WORD<0-16>	Specifies the VRF names.
vrfids WORD<0-512>	Specifies the VRF ID.

MSDP verification using CLI

Displaying the peer information

Use the following procedure to display the peer configuration and SA message information.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display the peer information:

```
show ip msdp peer {A.B.C.D} [vrf WORD<0-16>] [vrfids WORD<0-512>]
```

Example

```
Switch:#enable
Switch:1#show ip msdp peer 2.2.2.2
=====
                          MSDP Peer - GlobalRouter
=====
MSDP Peer 2.2.2.2, AS 109Admin Status: Enabled
Operational Status: Enabled
Description:
Connection status:
FSM State: Established, Establish Count: 9,
Connection source: 2.2.2.17
Uptime (Downtime): 1d10h, Messages sent/received:
436765/429062
Connection and counters cleared 1w2d ago
SA Filtering:
Input (S,G) route-policy: none
Output (S,G) route-policy: none
SA In count: SA out Count:
SA-Requests:
Input filter: none
Sending SA-Requests to peer: disabled
SA Request In Count: SA Request out Count:
SA Response In Count: SA Response out Count:
Peer ttl threshold: 0
SAs learned from this peer: 32, SAs limit: 500
Peer RPF failure Count:
KeepAlive In Count:
KeepAlive out count:
Encapsulated Data packets In:
Encapsulated Data Packets out:
KeepAlive Timer:
Peer Hold timer:
Connection Retry timer:
Encapsulation type:
MD5 Authentication: Enabled, MD5 Password:
%d462277d77
Peer FSM Established Time:
Peer In Message Time:
Remote port: Local port:
Number of connection Attempts:
Discontinuity timeout:
Too Short MSDP message Rx count:
Bad MSDP message Rx count:
```

Variable definitions

Use the data in the following table to use the `show ip msdp peer` command.

Variable	Value
{A.B.C.D}	Specifies the MSDP peer IP address.
vrf WORD<0-16>	Displays configuration info for a particular VRF.
vrfids WORD<0-512>	Displays configuration info for a particular VRF ID.

Displaying the SA cache

Use the following procedure to display the (S,G) state learned from MSDP peers and the local (S,G) state. The local (S,G) is the SPB (S,G) sent to MSDP.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display the SA cache:

```
show ip msdp sa-cache [local] [vrf WORD<0-16>] [vrfids WORD<0-512>]
[group {A.B.C.D}] [rp {A.B.C.D}] [source {A.B.C.D}]
```

Example

```
Switch:#enable
Switch:1#show ip msdp sa-cache local
=====
MSDP Foreign SA Cache - GlobalRouter
=====
MSDP Source-Active Foreign Cache - 8 entries
(2.10.1.100, 224.5.5.0), RP 3.3.3.3, BGP/AS 1,
00:01:53/00:05:35
(2.10.1.100, 224.5.6.0), RP 3.3.3.3, BGP/AS 1,
00:01:53/00:05:35
(2.10.1.100, 224.5.7.0), RP 3.3.3.3, BGP/AS 1,
00:01:53/00:05:35
(2.10.1.100, 224.5.8.0), RP 3.3.3.3, BGP/AS 1,
00:01:53/00:05:35
(2.11.2.100, 224.6.5.0), RP 3.3.3.3, BGP/AS 1,
00:01:53/00:05:35
(2.11.2.100, 224.6.6.0), RP 3.3.3.3, BGP/AS 1,
00:01:53/00:05:35
(2.11.2.100, 224.6.7.0), RP 3.3.3.3, BGP/AS 1,
00:01:53/00:05:35
(2.11.2.100, 224.6.8.0), RP 3.3.3.3, BGP/AS 1,
00:01:53/00:05:35

Switch:1#show ip msdp vrf msdpvrf
=====
MSDP Local SA Cache - VRF msdpVrf
=====
MSDP Source-Active Local Cache - 12 entries
(5.12.5.100, 224.7.5.0), RP 5.5.5.5
(5.12.5.100, 224.7.6.0), RP 5.5.5.5
(5.12.5.100, 224.7.7.0), RP 5.5.5.5
(5.12.5.100, 224.7.8.0), RP 5.5.5.5
(5.13.7.100, 224.8.5.0), RP 5.5.5.5
(5.13.7.100, 224.8.6.0), RP 5.5.5.5
(5.13.7.100, 224.8.7.0), RP 5.5.5.5
(5.13.7.100, 224.8.7.0), RP 5.5.5.5
(5.13.7.100, 224.8.7.0), RP 5.5.5.5
(7.14.8.100, 224.9.6.0), RP 5.5.5.5
(7.14.8.100, 224.9.7.0), RP 5.5.5.5
(7.14.8.100, 224.9.8.0), RP 5.5.5.5
```

Variable definitions

Use the data in the following table to use the `show ip msdp sa-cache` command.

Variable	Value
group{A.B.C.D}	Displays all SA cache entries that match the group IP address.
local	Displays the local SA cache.
rp{A.B.C.D}	Displays all SA cache entries that match the RP IP address.
source{A.B.C.D}	Displays all SA cache entries that match the source IP address.
vrf WORD<0-16>	Displays configuration information for a particular VRF.
vrfids WORD<0-512>	Displays configuration information for a particular VRF ID.

Displaying the MSDP count

Use the following procedure to display the number of sources and groups sent and received.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display the MSDP count:

```
show ip msdp count [vrf WORD<0-16>] [vrfids WORD<0-512>] [<0-65535>]
```

Example

```
Switch:#enable
Switch:1#show ip msdp count
=====
MSDP Count - GlobalRouter
=====
SA state per peer Counters, <peer>: <# SA learned>
192.135.250.116: 24
144.228.240.253: 3964
172.17.253.19: 10
172.17.170.110: 11
SA state per ASN Counters, <asn>: <# SA-count>
Total entries: 4009
?: 192, 9: 1, 14: 107, 17: 5
18: 4, 25: 23, 26: 39, 27: 2
32: 19, 38: 2, 52: 4, 57: 1
68: 4, 73: 12, 81: 19, 87: 9
```

Variable definitions

Use the data in the following table to use the `show ip msdp count` command.

Variable	Value
<0-65535>	Specifies the AS number.
vrf WORD<0-16>	Displays configuration information for a particular VRF.
vrfids WORD<0-512>	Displays configuration information for a particular VRF ID.

Displaying the MSDP summary

Use the following procedure to display the MSDP global and peer status.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display the MSDP summary:

```
show ip msdp summary [vrf WORD<0-16>] [vrfids WORD<0-512>]
```

Example

```
Switch:#enable
Switch:1#show ip msdp summary
=====
                          MSDP Summary - GlobalRouter
=====
MSDP Status Summary
  MSDP Global Status: enabled
cache status: enabled
cache-lifetime: 390 seconds
cache-count: 8
Originator id: 5.5.5.5
Redistribute: route-policy:
SA Limit: 6144

MSDP Peer Status Summary

Peer Address AS State      Uptime/  Established SA
                Downtime Count      Count
4.5.35.3      1  Established 00:00:27 3          8
5.7.56.7      2  Established 00:00:31 2          0
```

Variable definitions

Use the data in the following table to use the `show ip msdp summary` command.

Variable	Value
vrf WORD<0-16>	Displays configuration information for a particular VRF.
vrfids WORD<0-512>	Displays configuration information for a particular VRF ID.

Displaying the RPF peer information

Use the following procedure to display the MSDP peer information for a specific RP. The SA messages are received from the MSDP peer.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display the RPF peer information:

```
show ip msdp rpf {A.B.C.D} [vrf WORD<0-16>] [vrfids WORD<0-512>]
```

Example

```
Switch:#enable
Switch:1#show ip msdp rpf 172.16.10.13
=====
MSDP RPF - GlobalRouter
=====
RPF peer information for (172.16.10.13)
RPF peer: (172.16.121.10)
RPF route/mask: 172.16.0.0/255.255.0.0
RPF rule: Peer is IGP next hop of best route
RPF type: unicast (ospf)
```

Variable definitions

Use the data in the following table to use the `show ip msdp rpf` command.

Variable	Value
{A.B.C.D}	Specifies the RP IP address.
vrf WORD<0-16>	Displays configuration information for a particular VRF.
vrfids WORD<0-512>	Displays configuration information for a particular VRF ID.

Displaying the MSDP mesh group information

Use the following procedure to display the configured mesh groups.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display the MSDP mesh group information:

```
show ip msdp mesh-group [vrf WORD<0-16>] [vrfids WORD<0-512>]
[WORD<1-64>]
```

Example

```
Switch:#enable
Switch:1#show ip msdp mesh-group
=====
MSDP Mesh Group - GlobalRouter
=====
NAME                ADDRESS
-----
test                1.1.1.1
=====
```

Variable definitions

Use the data in the following table to use the `show ip msdp mesh-group` command.

Variable	Value
vrf <i>WORD</i> <0-16>	Displays configuration information for a particular VRF.
vrfids <i>WORD</i> <0-512>	Displays configuration information for a particular VRF ID.
<i>WORD</i> <1-64>	Specifies the mesh group name.

Displaying the SA check information

Use the following procedure to display the peer information from which the router accepts SA originating from the RP. The following procedure also checks if the specified (S,G,RP) will be accepted from the peer.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display the SA check information:

```
show ip msdp sa-check source {A.B.C.D} group {A.B.C.D} rp {A.B.C.D}
[peer {A.B.C.D}] [vrf WORD<0-16>] [vrfids WORD<0-512>]
```

Example

```
Switch:#enable
Switch:1#show ip msdp sa-check source 10.10.10.1 group 225.1.1.1 rp 172.16.10.13 peer
3.3.3.1
MSDP SA Check - GlobalRouter
=====
RPF peer information for (172.16.10.13)
RPF peer: (172.16.121.10)
RPF route/mask: 172.16.0.0/255.255.0.0
RPF rule: Peer is IGP next hop of best route
RPF type: unicast (ospf)
(10.10.10.1, 225.1.1.1, 172.16.10.13) - SA Accepted
Switch:1#show ip msdp sa-check source 5.5.5.1 group 225.1.1.1 rp 172.16.10.13 vrf msdpvrf
=====
```

Multicast Source Discovery Protocol configuration

```
MSDP SA Check- VRF msdpVrf
=====
RPF peer information for (172.16.10.13)
RPF peer: (172.16.121.10)
RPF route/mask: 172.16.0.0/255.255.0.0
RPF rule: Peer is IGP next hop of best route
RPF type: unicast (ospf)
(5.5.5.1, 225.1.1.1, 172.16.10.13) - SA Filtered by IN
filter route-policy abc

Switch:1#show ip msdp sa-check source 5.5.5.1 group 225.1.1.1 rp 59.59.59.1 peer 3.3.3.1
=====
MSDP SA Check - GlobalRouter
=====
(5.5.5.1, 225.1.1.1, 172.16.10.13) - SA not accepted due
to RPF peer mismatch
```

Variable definitions

Use the data in the following table to use the `show ip msdp sa-check` command.

Variable	Value
group {A.B.C.D}	Specifies the group IP address.
peer {A.B.C.D}	Specifies the MSDP peer IP address.
rp {A.B.C.D}	Specifies the RP IP address.
source {A.B.C.D}	Specifies the source IP address.
vrf WORD<0-16>	Displays configuration information for a particular VRF.
vrfids WORD<0-512>	Displays configuration information for a particular VRF ID.

Displaying all MSDP information

Use the following procedure to display all the MSDP information.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display all MSDP information:

```
show ip msdp show-all [file WORD<1-99>] [vrf WORD<0-16>] [vrfids
WORD<0-512>]
```

Example

```
Switch:#enable
Switch:1#show ip msdp show-all
```

```
=====
MSDP Show-all - GlobalRouter
```



```

=====
# show ip msdp count
SA State per Peer Counters, Peer: # SA learned
  4.5.35.3: 8
  5.7.56.7: 0
AS Num : SA Count
  1: 8

# show ip msdp mesh-group
  No Mesh Group exists

# show ip msdp peer

MSDP Peer 4.5.35.3, AS 1
Admin Status : enabled
Operational Status : enabled
Description:
Connection status:
  FSM State: Established, Established Count: 3,
Connection source: 4.5.35.5
  Uptime (Downtime): 00:00:20 ago, Messages
sent/received: 10839/174
  Connection and counters cleared 00:00:27 ago
SA Filtering:
  Input (S,G) route-policy:
  Output (S,G) route-policy:
  SA In count: 8 SA out Count: 10836
SA-Requests:
  Input filter: none
  Sending SA-Requests to peer: disabled
  SA Request In Count: 0 SA Request out Count: 0
  SA Response In Count: 0 SA Response out Count: 0
Peer ttl threshold: 0
SAs learned from this peer: 8, SAs limit: 6144
Peer RPF failure Count: 0
KeepAlive In Count: 166
KeepAlive out count: 3
Encapsulated Data packets In: 8
Encapsulated Data Packets out: 6152
KeepAlive Timer: 60
Peer Hold timer: 75
Connection Retry timer: 30
Encapsulation type: 6
MD5 Authentication: enable
Md5 password: %d462277d77
Peer FSM Established Time: 01:20:57
Peer In Message Time: 01:21:00
Remote port: 49156 Local port: 639
Number of connection Attempts: 0
Discontinuity timeout:01:20:50
Too Short MSDP message Rx count: 0
Bad MSDP message Rx count: 0

MSDP Peer 5.7.56.7, AS 2
Admin Status : enabled
Operational Status : enabled
Description:
Connection status:
  FSM State: Established, Established Count: 2,
Connection source: 5.7.56.5
  Uptime (Downtime): 00:00:27 ago, Messages
sent/received: 4677/77
  Connection and counters cleared 00:00:30 ago
SA Filtering:

```

Multicast Source Discovery Protocol configuration

```
Input (S,G) route-policy:
Output (S,G) route-policy:
SA In count: 0 SA out Count: 4675
SA-Requests:
  Input filter: none
  Sending SA-Requests to peer: disabled
  SA Request In Count: 0 SA Request out Count: 0
  SA Response In Count: 0 SA Response out Count: 0
Peer ttl threshold: 0
SAs learned from this peer: 0, SAs limit: 6144
Peer RPF failure Count: 0
KeepAlive In Count: 77
KeepAlive out count: 2
Encapsulated Data packets In: 0
Encapsulated Data Packets out: 8
KeepAlive Timer: 60
Peer Hold timer: 75
Connection Retry timer: 30
Encapsulation type: 6
MD5 Authentication: disable
Md5 password:
Peer FSM Established Time: 01:20:53
Peer In Message Time: 01:20:53
Remote port: 639 Local port: 49164
Number of connection Attempts: 3
Discontinuity timeout:01:20:50
Too Short MSDP message Rx count: 0
Bad MSDP message Rx count: 0

# show ip msdp sa-cache

MSDP Source-Active Foreign Cache - 8 entries
(2.10.1.100, 224.5.5.0), RP 3.3.3.3, BGP/AS 1,
00:00:22/00:06:07
(2.10.1.100, 224.5.6.0), RP 3.3.3.3, BGP/AS 1,
00:00:22/00:06:07
(2.10.1.100, 224.5.7.0), RP 3.3.3.3, BGP/AS 1,
00:00:22/00:06:07
(2.10.1.100, 224.5.8.0), RP 3.3.3.3, BGP/AS 1,
00:00:22/00:06:07
(2.11.2.100, 224.6.5.0), RP 3.3.3.3, BGP/AS 1,
00:00:23/00:06:06
(2.11.2.100, 224.6.6.0), RP 3.3.3.3, BGP/AS 1,
00:00:22/00:06:07
(2.11.2.100, 224.6.7.0), RP 3.3.3.3, BGP/AS 1,
00:00:22/00:06:07
(2.11.2.100, 224.6.8.0), RP 3.3.3.3, BGP/AS 1,
00:00:22/00:06:07

# show ip msdp summary
MSDP Status Summary
  MSDP Global Status: enabled
cache status: enabled
cache-lifetime: 390 seconds
cache-count: 8
Originator id: 5.5.5.5
Redistribute: route-policy:
SA Limit: 6144
MSDP Peer Status Summary

Peer Address AS State      Uptime/  Established SA
                Downtime Count    Count
4.5.35.3      1 Established 00:00:27 3          8
5.7.56.7      2 Established 00:00:31 2          0
```

```
MSDP Source-Active Local Cache - 12 entries
(5.12.5.100, 224.7.5.0), RP 5.5.5.5
(5.12.5.100, 224.7.6.0), RP 5.5.5.5
(5.12.5.100, 224.7.7.0), RP 5.5.5.5
(5.12.5.100, 224.7.8.0), RP 5.5.5.5
(5.13.7.100, 224.8.5.0), RP 5.5.5.5
(5.13.7.100, 224.8.6.0), RP 5.5.5.5
(5.13.7.100, 224.8.7.0), RP 5.5.5.5
(5.13.7.100, 224.8.8.0), RP 5.5.5.5
(7.14.8.100, 224.9.5.0), RP 5.5.5.5
(7.14.8.100, 224.9.6.0), RP 5.5.5.5
(7.14.8.100, 224.9.7.0), RP 5.5.5.5
```

Variable definitions

Use the data in the following table to use the `show ip msdp show-all` command.

Variable	Value
file <i>WORD</i> <1–99>	Specifies the file name to save the display output.
vrf <i>WORD</i> <0–16>	Displays configuration information for a particular VRF.
vrfids <i>WORD</i> <0–512>	Displays configuration information for a particular VRF ID.

Basic MSDP configuration using EDM

Configuring the MSDP originator ID

Configure the originator ID to set the RP address inside the SA message. The RP address must be a pre-configured CLIP interface on the global router or a VRF. The RP address is also the local IP address in all peer relations.

 **Note:**


Originator ID cannot be deleted if MSDP is enabled.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Globals** tab.
4. In the **RPAddress** box, type the IP address to use as the originator ID.
5. Click **Apply**.

Global field descriptions

Use the data in the following table to use the Globals tab.

Name	Description
Enabled	Enables MSDP. If you clear this check box, you disable MSDP. The default setting is clear (disabled).
CacheLifetime	Configures the lifetime given to SA cache entries when created or refreshed.
NumSACacheEntries	Displays the total number of entries in the SA cache.
RPAddress	Specifies the IP address to use as the originator ID. If the address is not a system local address, the system rejects the configuration.
RouteMapName	Specifies the name of the optional route policy to create or modify. You do not need to create a route policy to use the redistribution filter.  Note: To delete the route map name, clear the field and click Apply .
RedistributeFilterEnabled	Filters the (S,G,RP) entries provided by PIM to MSDP. The default is clear (disabled).
RedistruteFilterApply	Applies the changes made to the redistribute filter.
StatsClear	Clears MSDP statistics.

Enabling MSDP

Enable or disable MSDP globally on the switch to allow further configuration to take place.

Before you begin


You must configure the originator ID before you enable MSDP.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Globals** tab.
4. Select the **Enabled** check box to enable MSDP.
5. Click **Apply**.

Global field descriptions

Use the data in the following table to use the Globals tab.

Name	Description
Enabled	Enables MSDP. If you clear this check box, you disable MSDP. The default setting is clear (disabled).
CacheLifetime	Configures the lifetime given to SA cache entries when created or refreshed.
NumSACacheEntries	Displays the total number of entries in the SA cache.
RPAddress	Specifies the IP address to use as the originator ID. If the address is not a system local address, the system rejects the configuration.
RouteMapName	Specifies the name of the optional route policy to create or modify. You do not need to create a route policy to use the redistribution filter.  Note: To delete the route map name, clear the field and click Apply .
RedistributeFilterEnabled	Filters the (S,G,RP) entries provided by PIM to MSDP. The default is clear (disabled).
RedistruteFilterApply	Applies the changes made to the redistribute filter.
StatsClear	Clears MSDP statistics.

Creating an MSDP peer

Create an MSDP peer to establish a peer relationship between the local MSDP enabled router and a peer in another domain.

Important:

Do not enable more than 20 active peers.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Peers** tab.
4. Click **Insert**.
5. In the **RemoteAddress** box, type the IP address of the peer.
6. Click **Insert**.

Peers field descriptions

Use the data in the following table to use the Peers tab.

Name	Description
RemoteAddress	Shows the IP address of the remote MSDP peer.
State	Shows the state of the default peer. An MSDP node only accepts SA messages from an operational default peer. Only one default peer can be operational; the configured default peers provide redundancy.
AdminEnabled	Changes the peer status to administratively enable or disable a configured peer. The default value is disabled (false).
ConnectRetryInterval	Specifies the connection retry period, in seconds, for this peer. The default value is 30 seconds.
HoldTimeConfigured	The default value is 75 seconds.
KeepAliveConfigured	Specifies the keepalive period, in seconds, configured for this MSDP speaker with this peer. If the value is 0 seconds, no periodic keepalive messages are sent to the peer after the MSDP connection is established. The default value is 60 seconds.
DataTtl	Specifies the time-to-live value, from 0–255. The default value is 0, which means that the router forwards all SA messages with encapsulated data.
InSAFilterEnabled	Activates the inbound SA filter for the peer.
InSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter accepts only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all inbound SA messages from this peer.
OutSAFilterEnabled	Activates the outbound SA filter for the peer.
OutSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter sends only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all outbound SA messages from this peer.
Description	Specifies the text description, up to 255 characters, for the peer.
SALimit	Specifies the maximum number of SA messages from an MSDP peer to keep in the SA cache. The valid values are from 0–6144; the default value is 6144.
Md5AuthEnabled	Activates MD5 authentication on the TCP connection between peers. The default is false.

Table continues...

Name	Description
Md5AuthPassword	Specifies a case-sensitive password, up to 80 characters, for MD5 authentication.
RemotePort	Shows the remote port for the TCP connection between the MSDP peers.
LocalPort	Shows the local port for the TCP connection between the MSDP peers.
OperEnabled	Shows the operational status of the peer.
RPFFailures	Shows the number of SA messages received from this peer that failed the Peer-RPF check. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAs	Shows the number of MSDP SA messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAs	Shows the number of MSDP SA messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSARquests	Shows the number of MSDP SA-Request messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSARquests	Shows the number of MSDP SA-Request messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAResponses	Shows the number of MSDP SA-Response messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAResponses	Shows the number of MSDP SA-Response messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InControlMessages	Shows the total number of MSDP messages received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutControlMessages	Shows the total number of MSDP messages transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.

Table continues...

Name	Description
InDataPackets	Shows the total number of encapsulated packets received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutDataPackets	Shows the total number of encapsulated packets transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
FsmEstablishedTransitions	Shows the total number of times the BGP transitioned to the established state.
FsmEstablishedTime	Shows the time when the peer transitioned to the established state.
InMessageTime	Shows the time when the last MSDP message was received from the peer.
ConnectionAttempts	Shows the number of times the state machine has transitioned from inactive to connecting.
DiscontinuityTime	Shows the sysUpTime value (the time, in hundredths of a second, since the network management portion of the system last reinitialized) when one or more of the counters for this entry suffered a discontinuity. Discontinuities can occur at peer connection establishment. If no discontinuities occurred since the last reinitialization of the local management subsystem, the value is zero.
AsNumber	Specifies the autonomous system number of the MSDP peer. A peer can appear to be in another autonomous system (other than the one in which it really resides) if you use an MSDP peering session but do not use a Border Gateway Protocol peer session with that peer. If another autonomous system injects the prefix of the peer, the prefix appears as the autonomous system number of the peer.
TooShortMessages	Shows the number of short messages received from this peer.
InBadMessages	Shows the number of bad MSDP messages received from this peer.
InKeepAliveMessages	Shows the number of keepalive messages received from this peer.
OutKeepAliveMessages	Shows the number of keepalive messages transmitted to this peer.
SAsLearnedFromThisPeer	Shows the total number of SAs learned from this peer.

Table continues...

Name	Description
SAsAdvertisedToThisPeer	Shows the total number of SAs advertised from this peer.
UpOrDownTime	Shows the duration a peer has been up or down.
ConnAndStatsClearedTime	Shows the duration of connection and statistics cleared.

MSDP peer configuration using EDM

Securing control messages

Configure Message Digest (MD) 5 authentication to secure control messages on the TCP connection between MSDP peers.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Peers** tab.
4. In the row for the peer, double-click the **Md5AuthEnabled** field, and then select true.
5. In the row for the peer, double-click the **Md5AuthPassword** field, and then type a password.
6. Click **Apply**.

Peers field descriptions

Use the data in the following table to use the Peers tab.

Name	Description
RemoteAddress	Shows the IP address of the remote MSDP peer.
State	Shows the state of the default peer. An MSDP node only accepts SA messages from an operational default peer. Only one default peer can be operational; the configured default peers provide redundancy.
AdminEnabled	Changes the peer status to administratively enable or disable a configured peer. The default value is disabled (false).
ConnectRetryInterval	Specifies the connection retry period, in seconds, for this peer. The default value is 30 seconds.

Table continues...

Name	Description
HoldTimeConfigured	The default value is 75 seconds.
KeepAliveConfigured	Specifies the keepalive period, in seconds, configured for this MSDP speaker with this peer. If the value is 0 seconds, no periodic keepalive messages are sent to the peer after the MSDP connection is established. The default value is 60 seconds.
DataTtl	Specifies the time-to-live value, from 0–255. The default value is 0, which means that the router forwards all SA messages with encapsulated data.
InSAFilterEnabled	Activates the inbound SA filter for the peer.
InSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter accepts only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all inbound SA messages from this peer.
OutSAFilterEnabled	Activates the outbound SA filter for the peer.
OutSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter sends only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all outbound SA messages from this peer.
Description	Specifies the text description, up to 255 characters, for the peer.
SALimit	Specifies the maximum number of SA messages from an MSDP peer to keep in the SA cache. The valid values are from 0–6144; the default value is 6144.
Md5AuthEnabled	Activates MD5 authentication on the TCP connection between peers. The default is false.
Md5AuthPassword	Specifies a case-sensitive password, up to 80 characters, for MD5 authentication.
RemotePort	Shows the remote port for the TCP connection between the MSDP peers.
LocalPort	Shows the local port for the TCP connection between the MSDP peers.
OperEnabled	Shows the operational status of the peer.
RPFFailures	Shows the number of SA messages received from this peer that failed the Peer-RPF check. Discontinuities in the value of this counter can occur at reinitialization of the management system.

Table continues...

Name	Description
InSAs	Shows the number of MSDP SA messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAs	Shows the number of MSDP SA messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSARequests	Shows the number of MSDP SA-Request messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSARequests	Shows the number of MSDP SA-Request messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAResponses	Shows the number of MSDP SA-Response messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAResponses	Shows the number of MSDP SA-Response messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InControlMessages	Shows the total number of MSDP messages received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutControlMessages	Shows the total number of MSDP messages transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InDataPackets	Shows the total number of encapsulated packets received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutDataPackets	Shows the total number of encapsulated packets transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
FsmEstablishedTransitions	Shows the total number of times the BGP transitioned to the established state.
FsmEstablishedTime	Shows the time when the peer transitioned to the established state.

Table continues...

Name	Description
InMessageTime	Shows the time when the last MSDP message was received from the peer.
ConnectionAttempts	Shows the number of times the state machine has transitioned from inactive to connecting.
DiscontinuityTime	Shows the sysUpTime value (the time, in hundredths of a second, since the network management portion of the system last reinitialized) when one or more of the counters for this entry suffered a discontinuity. Discontinuities can occur at peer connection establishment. If no discontinuities occurred since the last reinitialization of the local management subsystem, the value is zero.
AsNumber	Specifies the autonomous system number of the MSDP peer. A peer can appear to be in another autonomous system (other than the one in which it really resides) if you use an MSDP peering session but do not use a Border Gateway Protocol peer session with that peer. If another autonomous system injects the prefix of the peer, the prefix appears as the autonomous system number of the peer.
TooShortMessages	Shows the number of short messages received from this peer.
InBadMessages	Shows the number of bad MSDP messages received from this peer.
InKeepAliveMessages	Shows the number of keepalive messages received from this peer.
OutKeepAliveMessages	Shows the number of keepalive messages transmitted to this peer.
SAsLearnedFromThisPeer	Shows the total number of SAs learned from this peer.
SAsAdvertisedToThisPeer	Shows the total number of SAs advertised from this peer.
UpOrDownTime	Shows the duration a peer has been up or down.
ConnAndStatsClearedTime	Shows the duration of connection and statistics cleared.

Configuring the MSDP peer SA limit

Configure the SA limit to limit the number of SA messages from an MSDP peer. The router saves the SA messages in the local cache.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Peers** tab.
4. In the row for the peer, double-click the **SALimit** field, and then type a value.
5. Click **Apply**.

Peers field descriptions

Use the data in the following table to use the Peers tab.

Name	Description
RemoteAddress	Shows the IP address of the remote MSDP peer.
State	Shows the state of the default peer. An MSDP node only accepts SA messages from an operational default peer. Only one default peer can be operational; the configured default peers provide redundancy.
AdminEnabled	Changes the peer status to administratively enable or disable a configured peer. The default value is disabled (false).
ConnectRetryInterval	Specifies the connection retry period, in seconds, for this peer. The default value is 30 seconds.
HoldTimeConfigured	The default value is 75 seconds.
KeepAliveConfigured	Specifies the keepalive period, in seconds, configured for this MSDP speaker with this peer. If the value is 0 seconds, no periodic keepalive messages are sent to the peer after the MSDP connection is established. The default value is 60 seconds.
DataTtl	Specifies the time-to-live value, from 0–255. The default value is 0, which means that the router forwards all SA messages with encapsulated data.
InSAFilterEnabled	Activates the inbound SA filter for the peer.
InSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter accepts only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all inbound SA messages from this peer.
OutSAFilterEnabled	Activates the outbound SA filter for the peer.
OutSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter sends only the SA

Table continues...

Name	Description
	messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all outbound SA messages from this peer.
Description	Specifies the text description, up to 255 characters, for the peer.
SALimit	Specifies the maximum number of SA messages from an MSDP peer to keep in the SA cache. The valid values are from 0–6144; the default value is 6144.
Md5AuthEnabled	Activates MD5 authentication on the TCP connection between peers. The default is false.
Md5AuthPassword	Specifies a case-sensitive password, up to 80 characters, for MD5 authentication.
RemotePort	Shows the remote port for the TCP connection between the MSDP peers.
LocalPort	Shows the local port for the TCP connection between the MSDP peers.
OperEnabled	Shows the operational status of the peer.
RPFFailures	Shows the number of SA messages received from this peer that failed the Peer-RPF check. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAs	Shows the number of MSDP SA messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAs	Shows the number of MSDP SA messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSARquests	Shows the number of MSDP SA-Request messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSARquests	Shows the number of MSDP SA-Request messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAResponses	Shows the number of MSDP SA-Response messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.

Table continues...

Name	Description
OutSAResponses	Shows the number of MSDP SA-Response messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InControlMessages	Shows the total number of MSDP messages received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutControlMessages	Shows the total number of MSDP messages transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InDataPackets	Shows the total number of encapsulated packets received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutDataPackets	Shows the total number of encapsulated packets transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
FsmEstablishedTransitions	Shows the total number of times the BGP transitioned to the established state.
FsmEstablishedTime	Shows the time when the peer transitioned to the established state.
InMessageTime	Shows the time when the last MSDP message was received from the peer.
ConnectionAttempts	Shows the number of times the state machine has transitioned from inactive to connecting.
DiscontinuityTime	Shows the sysUpTime value (the time, in hundredths of a second, since the network management portion of the system last reinitialized) when one or more of the counters for this entry suffered a discontinuity. Discontinuities can occur at peer connection establishment. If no discontinuities occurred since the last reinitialization of the local management subsystem, the value is zero.
AsNumber	Specifies the autonomous system number of the MSDP peer. A peer can appear to be in another autonomous system (other than the one in which it really resides) if you use an MSDP peering session but do not use a Border Gateway Protocol peer session with that peer. If another autonomous system injects the prefix of the peer, the prefix

Table continues...

Name	Description
	appears as the autonomous system number of the peer.
TooShortMessages	Shows the number of short messages received from this peer.
InBadMessages	Shows the number of bad MSDP messages received from this peer.
InKeepAliveMessages	Shows the number of keepalive messages received from this peer.
OutKeepAliveMessages	Shows the number of keepalive messages transmitted to this peer.
SAsLearnedFromThisPeer	Shows the total number of SAs learned from this peer.
SAsAdvertisedToThisPeer	Shows the total number of SAs advertised from this peer.
UpOrDownTime	Shows the duration a peer has been up or down.
ConnAndStatsClearedTime	Shows the duration of connection and statistics cleared.

Configuring a peer description

About this task

Configure a peer description to add a descriptive text to an MSDP peer, for easy identification of a peer.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Peers** tab.
4. In the row for the peer, double-click the **Description** field, and then type a description for the peer.
5. Click **Apply**.

Peers field descriptions

Use the data in the following table to use the Peers tab.

Name	Description
RemoteAddress	Shows the IP address of the remote MSDP peer.

Table continues...

Name	Description
State	Shows the state of the default peer. An MSDP node only accepts SA messages from an operational default peer. Only one default peer can be operational; the configured default peers provide redundancy.
AdminEnabled	Changes the peer status to administratively enable or disable a configured peer. The default value is disabled (false).
ConnectRetryInterval	Specifies the connection retry period, in seconds, for this peer. The default value is 30 seconds.
HoldTimeConfigured	The default value is 75 seconds.
KeepAliveConfigured	Specifies the keepalive period, in seconds, configured for this MSDP speaker with this peer. If the value is 0 seconds, no periodic keepalive messages are sent to the peer after the MSDP connection is established. The default value is 60 seconds.
DataTtl	Specifies the time-to-live value, from 0–255. The default value is 0, which means that the router forwards all SA messages with encapsulated data.
InSAFilterEnabled	Activates the inbound SA filter for the peer.
InSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter accepts only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all inbound SA messages from this peer.
OutSAFilterEnabled	Activates the outbound SA filter for the peer.
OutSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter sends only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all outbound SA messages from this peer.
Description	Specifies the text description, up to 255 characters, for the peer.
SALimit	Specifies the maximum number of SA messages from an MSDP peer to keep in the SA cache. The valid values are from 0–6144; the default value is 6144.
Md5AuthEnabled	Activates MD5 authentication on the TCP connection between peers. The default is false.

Table continues...

Name	Description
Md5AuthPassword	Specifies a case-sensitive password, up to 80 characters, for MD5 authentication.
RemotePort	Shows the remote port for the TCP connection between the MSDP peers.
LocalPort	Shows the local port for the TCP connection between the MSDP peers.
OperEnabled	Shows the operational status of the peer.
RPFFailures	Shows the number of SA messages received from this peer that failed the Peer-RPF check. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAs	Shows the number of MSDP SA messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAs	Shows the number of MSDP SA messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSARquests	Shows the number of MSDP SA-Request messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSARquests	Shows the number of MSDP SA-Request messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAResponses	Shows the number of MSDP SA-Response messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAResponses	Shows the number of MSDP SA-Response messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InControlMessages	Shows the total number of MSDP messages received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutControlMessages	Shows the total number of MSDP messages transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.

Table continues...

Name	Description
InDataPackets	Shows the total number of encapsulated packets received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutDataPackets	Shows the total number of encapsulated packets transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
FsmEstablishedTransitions	Shows the total number of times the BGP transitioned to the established state.
FsmEstablishedTime	Shows the time when the peer transitioned to the established state.
InMessageTime	Shows the time when the last MSDP message was received from the peer.
ConnectionAttempts	Shows the number of times the state machine has transitioned from inactive to connecting.
DiscontinuityTime	Shows the sysUpTime value (the time, in hundredths of a second, since the network management portion of the system last reinitialized) when one or more of the counters for this entry suffered a discontinuity. Discontinuities can occur at peer connection establishment. If no discontinuities occurred since the last reinitialization of the local management subsystem, the value is zero.
AsNumber	Specifies the autonomous system number of the MSDP peer. A peer can appear to be in another autonomous system (other than the one in which it really resides) if you use an MSDP peering session but do not use a Border Gateway Protocol peer session with that peer. If another autonomous system injects the prefix of the peer, the prefix appears as the autonomous system number of the peer.
TooShortMessages	Shows the number of short messages received from this peer.
InBadMessages	Shows the number of bad MSDP messages received from this peer.
InKeepAliveMessages	Shows the number of keepalive messages received from this peer.
OutKeepAliveMessages	Shows the number of keepalive messages transmitted to this peer.
SAsLearnedFromThisPeer	Shows the total number of SAs learned from this peer.

Table continues...

Name	Description
SAsAdvertisedToThisPeer	Shows the total number of SAs advertised from this peer.
UpOrDownTime	Shows the duration a peer has been up or down.
ConnAndStatsClearedTime	Shows the duration of connection and statistics cleared.

Configuring the MSDP peer time to live threshold

Configure the time-to-live (TTL) threshold to limit which multicast data packets the router encapsulated in SA Message forwarded to an MSDP peer. The TTL limits the number of hops a packet can take before the router drops the packet. The router sends out SA Messages with encapsulated data only if TTL equals or exceeds the value you configure. If the TTL is lower than the value you configure, the router drops the data packet and forwards the SA Message without the encapsulated data.

* Note:

MSDP transmits encapsulated multicast data packets inside forwarded MSDP messages. If the received SA is an encapsulated SA, then the switch parses the TTL value of the encapsulated data and compares it against the configured value. If the configured value is less than or equal to the parsed value, then the switch forwards the encapsulated data along with the SA, otherwise the switch forwards the SA alone by stripping the encapsulate data. By default, MSDP forwards encapsulated data along with the SA message. MSDP does not forward the encapsulated data to the local receivers.

When MSDP generates SA messages for SPB sources, the local cache miss data cannot be encapsulated into the SA messages that are sent to the peers.

The switch supports forwarding SA messages with encapsulated data from sources to MSDP peers but not from MSDP peers to the receivers.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Peers** tab.
4. In the row for the peer, double-click the **Md5AuthEnabled** field, and then select true.
5. In the row for the peer, double-click the **DataTtl** field, and then type a value.
6. Click **Apply**.

Peers field descriptions

Use the data in the following table to use the Peers tab.

Name	Description
RemoteAddress	Shows the IP address of the remote MSDP peer.
State	Shows the state of the default peer. An MSDP node only accepts SA messages from an operational default peer. Only one default peer can be operational; the configured default peers provide redundancy.
AdminEnabled	Changes the peer status to administratively enable or disable a configured peer. The default value is disabled (false).
ConnectRetryInterval	Specifies the connection retry period, in seconds, for this peer. The default value is 30 seconds.
HoldTimeConfigured	The default value is 75 seconds.
KeepAliveConfigured	Specifies the keepalive period, in seconds, configured for this MSDP speaker with this peer. If the value is 0 seconds, no periodic keepalive messages are sent to the peer after the MSDP connection is established. The default value is 60 seconds.
DataTtl	Specifies the time-to-live value, from 0–255. The default value is 0, which means that the router forwards all SA messages with encapsulated data.
InSAFilterEnabled	Activates the inbound SA filter for the peer.
InSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter accepts only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all inbound SA messages from this peer.
OutSAFilterEnabled	Activates the outbound SA filter for the peer.
OutSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter sends only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all outbound SA messages from this peer.
Description	Specifies the text description, up to 255 characters, for the peer.
SALimit	Specifies the maximum number of SA messages from an MSDP peer to keep in the SA cache. The valid values are from 0–6144; the default value is 6144.
Md5AuthEnabled	Activates MD5 authentication on the TCP connection between peers. The default is false.

Table continues...

Name	Description
Md5AuthPassword	Specifies a case-sensitive password, up to 80 characters, for MD5 authentication.
RemotePort	Shows the remote port for the TCP connection between the MSDP peers.
LocalPort	Shows the local port for the TCP connection between the MSDP peers.
OperEnabled	Shows the operational status of the peer.
RPFFailures	Shows the number of SA messages received from this peer that failed the Peer-RPF check. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAs	Shows the number of MSDP SA messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAs	Shows the number of MSDP SA messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSARquests	Shows the number of MSDP SA-Request messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSARquests	Shows the number of MSDP SA-Request messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAResponses	Shows the number of MSDP SA-Response messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAResponses	Shows the number of MSDP SA-Response messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InControlMessages	Shows the total number of MSDP messages received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutControlMessages	Shows the total number of MSDP messages transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.

Table continues...

Name	Description
InDataPackets	Shows the total number of encapsulated packets received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutDataPackets	Shows the total number of encapsulated packets transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
FsmEstablishedTransitions	Shows the total number of times the BGP transitioned to the established state.
FsmEstablishedTime	Shows the time when the peer transitioned to the established state.
InMessageTime	Shows the time when the last MSDP message was received from the peer.
ConnectionAttempts	Shows the number of times the state machine has transitioned from inactive to connecting.
DiscontinuityTime	Shows the sysUpTime value (the time, in hundredths of a second, since the network management portion of the system last reinitialized) when one or more of the counters for this entry suffered a discontinuity. Discontinuities can occur at peer connection establishment. If no discontinuities occurred since the last reinitialization of the local management subsystem, the value is zero.
AsNumber	Specifies the autonomous system number of the MSDP peer. A peer can appear to be in another autonomous system (other than the one in which it really resides) if you use an MSDP peering session but do not use a Border Gateway Protocol peer session with that peer. If another autonomous system injects the prefix of the peer, the prefix appears as the autonomous system number of the peer.
TooShortMessages	Shows the number of short messages received from this peer.
InBadMessages	Shows the number of bad MSDP messages received from this peer.
InKeepAliveMessages	Shows the number of keepalive messages received from this peer.
OutKeepAliveMessages	Shows the number of keepalive messages transmitted to this peer.
SAsLearnedFromThisPeer	Shows the total number of SAs learned from this peer.

Table continues...

Name	Description
SAsAdvertisedToThisPeer	Shows the total number of SAs advertised from this peer.
UpOrDownTime	Shows the duration a peer has been up or down.
ConnAndStatsClearedTime	Shows the duration of connection and statistics cleared.

Configuring the MSDP peer keepalive messages

Configure keepalive messages to adjust the interval in seconds at which an MSDP peer sends keep alive messages (default is 60 seconds) and the interval at which the MSDP peer waits for keep alive messages from other peers before it declares them down (default is 75 seconds).

*** Note:**

In a peer relationship, the keep alive interval configured on one peer must be at least 1 second less than the hold time configured on the other side of the peer relationship. This is not applicable when the hold time is set to 0 seconds.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Peers** tab.
4. In the row for the peer, double-click the **KeepAliveConfigured** field, and then type the interval at which to send keepalive messages.
5. In the row for the peer, double-click the **HoldTimeConfigured** field, and then type the interval at which to wait for keepalive messages.
6. Click **Apply**.

Peers field descriptions

Use the data in the following table to use the Peers tab.

Name	Description
RemoteAddress	Shows the IP address of the remote MSDP peer.
State	Shows the state of the default peer. An MSDP node only accepts SA messages from an operational default peer. Only one default peer can be operational; the configured default peers provide redundancy.

Table continues...

Name	Description
AdminEnabled	Changes the peer status to administratively enable or disable a configured peer. The default value is disabled (false).
ConnectRetryInterval	Specifies the connection retry period, in seconds, for this peer. The default value is 30 seconds.
HoldTimeConfigured	The default value is 75 seconds.
KeepAliveConfigured	Specifies the keepalive period, in seconds, configured for this MSDP speaker with this peer. If the value is 0 seconds, no periodic keepalive messages are sent to the peer after the MSDP connection is established. The default value is 60 seconds.
DataTtl	Specifies the time-to-live value, from 0–255. The default value is 0, which means that the router forwards all SA messages with encapsulated data.
InSAFilterEnabled	Activates the inbound SA filter for the peer.
InSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter accepts only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all inbound SA messages from this peer.
OutSAFilterEnabled	Activates the outbound SA filter for the peer.
OutSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter sends only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all outbound SA messages from this peer.
Description	Specifies the text description, up to 255 characters, for the peer.
SALimit	Specifies the maximum number of SA messages from an MSDP peer to keep in the SA cache. The valid values are from 0–6144; the default value is 6144.
Md5AuthEnabled	Activates MD5 authentication on the TCP connection between peers. The default is false.
Md5AuthPassword	Specifies a case-sensitive password, up to 80 characters, for MD5 authentication.
RemotePort	Shows the remote port for the TCP connection between the MSDP peers.
LocalPort	Shows the local port for the TCP connection between the MSDP peers.

Table continues...

Name	Description
OperEnabled	Shows the operational status of the peer.
RPFFailures	Shows the number of SA messages received from this peer that failed the Peer-RPF check. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAs	Shows the number of MSDP SA messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAs	Shows the number of MSDP SA messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSARequests	Shows the number of MSDP SA-Request messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSARequests	Shows the number of MSDP SA-Request messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAResponses	Shows the number of MSDP SA-Response messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAResponses	Shows the number of MSDP SA-Response messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InControlMessages	Shows the total number of MSDP messages received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutControlMessages	Shows the total number of MSDP messages transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InDataPackets	Shows the total number of encapsulated packets received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutDataPackets	Shows the total number of encapsulated packets transmitted on this TCP connection. Discontinuities

Table continues...

Name	Description
	in the value of this counter can occur at reinitialization of the management system.
FsmEstablishedTransitions	Shows the total number of times the BGP transitioned to the established state.
FsmEstablishedTime	Shows the time when the peer transitioned to the established state.
InMessageTime	Shows the time when the last MSDP message was received from the peer.
ConnectionAttempts	Shows the number of times the state machine has transitioned from inactive to connecting.
DiscontinuityTime	Shows the sysUpTime value (the time, in hundredths of a second, since the network management portion of the system last reinitialized) when one or more of the counters for this entry suffered a discontinuity. Discontinuities can occur at peer connection establishment. If no discontinuities occurred since the last reinitialization of the local management subsystem, the value is zero.
AsNumber	Specifies the autonomous system number of the MSDP peer. A peer can appear to be in another autonomous system (other than the one in which it really resides) if you use an MSDP peering session but do not use a Border Gateway Protocol peer session with that peer. If another autonomous system injects the prefix of the peer, the prefix appears as the autonomous system number of the peer.
TooShortMessages	Shows the number of short messages received from this peer.
InBadMessages	Shows the number of bad MSDP messages received from this peer.
InKeepAliveMessages	Shows the number of keepalive messages received from this peer.
OutKeepAliveMessages	Shows the number of keepalive messages transmitted to this peer.
SAsLearnedFromThisPeer	Shows the total number of SAs learned from this peer.
SAsAdvertisedToThisPeer	Shows the total number of SAs advertised from this peer.
UpOrDownTime	Shows the duration a peer has been up or down.
ConnAndStatsClearedTime	Shows the duration of connection and statistics cleared.

Configuring the MSDP peer connect-retry period

Configure the connect-retry period to specify the amount of time, in seconds, between connection attempts for peering sessions. The default is 30 seconds.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Peers** tab.
4. In the row for the peer, double-click the **ConnectRetryInterval** field, and then type the interval.
5. Click **Apply**.

Peers field descriptions

Use the data in the following table to use the Peers tab.

Name	Description
RemoteAddress	Shows the IP address of the remote MSDP peer.
State	Shows the state of the default peer. An MSDP node only accepts SA messages from an operational default peer. Only one default peer can be operational; the configured default peers provide redundancy.
AdminEnabled	Changes the peer status to administratively enable or disable a configured peer. The default value is disabled (false).
ConnectRetryInterval	Specifies the connection retry period, in seconds, for this peer. The default value is 30 seconds.
HoldTimeConfigured	The default value is 75 seconds.
KeepAliveConfigured	Specifies the keepalive period, in seconds, configured for this MSDP speaker with this peer. If the value is 0 seconds, no periodic keepalive messages are sent to the peer after the MSDP connection is established. The default value is 60 seconds.
DataTtl	Specifies the time-to-live value, from 0–255. The default value is 0, which means that the router forwards all SA messages with encapsulated data.
InSAFilterEnabled	Activates the inbound SA filter for the peer.
InSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter accepts only the SA

Table continues...

Name	Description
	messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all inbound SA messages from this peer.
OutSAFilterEnabled	Activates the outbound SA filter for the peer.
OutSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter sends only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all outbound SA messages from this peer.
Description	Specifies the text description, up to 255 characters, for the peer.
SALimit	Specifies the maximum number of SA messages from an MSDP peer to keep in the SA cache. The valid values are from 0–6144; the default value is 6144.
Md5AuthEnabled	Activates MD5 authentication on the TCP connection between peers. The default is false.
Md5AuthPassword	Specifies a case-sensitive password, up to 80 characters, for MD5 authentication.
RemotePort	Shows the remote port for the TCP connection between the MSDP peers.
LocalPort	Shows the local port for the TCP connection between the MSDP peers.
OperEnabled	Shows the operational status of the peer.
RPFFailures	Shows the number of SA messages received from this peer that failed the Peer-RPF check. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAs	Shows the number of MSDP SA messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAs	Shows the number of MSDP SA messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSARquests	Shows the number of MSDP SA-Request messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.

Table continues...

Name	Description
OutSARRequests	Shows the number of MSDP SA-Request messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAResponses	Shows the number of MSDP SA-Response messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAResponses	Shows the number of MSDP SA-Response messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InControlMessages	Shows the total number of MSDP messages received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutControlMessages	Shows the total number of MSDP messages transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InDataPackets	Shows the total number of encapsulated packets received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutDataPackets	Shows the total number of encapsulated packets transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
FsmEstablishedTransitions	Shows the total number of times the BGP transitioned to the established state.
FsmEstablishedTime	Shows the time when the peer transitioned to the established state.
InMessageTime	Shows the time when the last MSDP message was received from the peer.
ConnectionAttempts	Shows the number of times the state machine has transitioned from inactive to connecting.
DiscontinuityTime	Shows the sysUpTime value (the time, in hundredths of a second, since the network management portion of the system last reinitialized) when one or more of the counters for this entry suffered a discontinuity. Discontinuities can occur at peer connection establishment. If no discontinuities occurred since the last reinitialization of the local management subsystem, the value is zero.

Table continues...

Name	Description
AsNumber	Specifies the autonomous system number of the MSDP peer. A peer can appear to be in another autonomous system (other than the one in which it really resides) if you use an MSDP peering session but do not use a Border Gateway Protocol peer session with that peer. If another autonomous system injects the prefix of the peer, the prefix appears as the autonomous system number of the peer.
TooShortMessages	Shows the number of short messages received from this peer.
InBadMessages	Shows the number of bad MSDP messages received from this peer.
InKeepAliveMessages	Shows the number of keepalive messages received from this peer.
OutKeepAliveMessages	Shows the number of keepalive messages transmitted to this peer.
SAsLearnedFromThisPeer	Shows the total number of SAs learned from this peer.
SAsAdvertisedToThisPeer	Shows the total number of SAs advertised from this peer.
UpOrDownTime	Shows the duration a peer has been up or down.
ConnAndStatsClearedTime	Shows the duration of connection and statistics cleared.

Changing the MSDP peer status

Change the peer status to administratively enable or disable a configured peer. Disable the peer to stop the peering relationship.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Peers** tab.
4. In the row for the peer, double-click the **AdminEnabled** field, and then select true.
5. Click **Apply**.

Peers field descriptions

Use the data in the following table to use the Peers tab.

Name	Description
RemoteAddress	Shows the IP address of the remote MSDP peer.
State	Shows the state of the default peer. An MSDP node only accepts SA messages from an operational default peer. Only one default peer can be operational; the configured default peers provide redundancy.
AdminEnabled	Changes the peer status to administratively enable or disable a configured peer. The default value is disabled (false).
ConnectRetryInterval	Specifies the connection retry period, in seconds, for this peer. The default value is 30 seconds.
HoldTimeConfigured	The default value is 75 seconds.
KeepAliveConfigured	Specifies the keepalive period, in seconds, configured for this MSDP speaker with this peer. If the value is 0 seconds, no periodic keepalive messages are sent to the peer after the MSDP connection is established. The default value is 60 seconds.
DataTtl	Specifies the time-to-live value, from 0–255. The default value is 0, which means that the router forwards all SA messages with encapsulated data.
InSAFilterEnabled	Activates the inbound SA filter for the peer.
InSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter accepts only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all inbound SA messages from this peer.
OutSAFilterEnabled	Activates the outbound SA filter for the peer.
OutSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter sends only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all outbound SA messages from this peer.
Description	Specifies the text description, up to 255 characters, for the peer.
SALimit	Specifies the maximum number of SA messages from an MSDP peer to keep in the SA cache. The valid values are from 0–6144; the default value is 6144.
Md5AuthEnabled	Activates MD5 authentication on the TCP connection between peers. The default is false.

Table continues...

Name	Description
Md5AuthPassword	Specifies a case-sensitive password, up to 80 characters, for MD5 authentication.
RemotePort	Shows the remote port for the TCP connection between the MSDP peers.
LocalPort	Shows the local port for the TCP connection between the MSDP peers.
OperEnabled	Shows the operational status of the peer.
RPFFailures	Shows the number of SA messages received from this peer that failed the Peer-RPF check. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAs	Shows the number of MSDP SA messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAs	Shows the number of MSDP SA messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSARquests	Shows the number of MSDP SA-Request messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSARquests	Shows the number of MSDP SA-Request messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAResponses	Shows the number of MSDP SA-Response messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAResponses	Shows the number of MSDP SA-Response messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InControlMessages	Shows the total number of MSDP messages received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutControlMessages	Shows the total number of MSDP messages transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.

Table continues...

Name	Description
InDataPackets	Shows the total number of encapsulated packets received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutDataPackets	Shows the total number of encapsulated packets transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
FsmEstablishedTransitions	Shows the total number of times the BGP transitioned to the established state.
FsmEstablishedTime	Shows the time when the peer transitioned to the established state.
InMessageTime	Shows the time when the last MSDP message was received from the peer.
ConnectionAttempts	Shows the number of times the state machine has transitioned from inactive to connecting.
DiscontinuityTime	Shows the sysUpTime value (the time, in hundredths of a second, since the network management portion of the system last reinitialized) when one or more of the counters for this entry suffered a discontinuity. Discontinuities can occur at peer connection establishment. If no discontinuities occurred since the last reinitialization of the local management subsystem, the value is zero.
AsNumber	Specifies the autonomous system number of the MSDP peer. A peer can appear to be in another autonomous system (other than the one in which it really resides) if you use an MSDP peering session but do not use a Border Gateway Protocol peer session with that peer. If another autonomous system injects the prefix of the peer, the prefix appears as the autonomous system number of the peer.
TooShortMessages	Shows the number of short messages received from this peer.
InBadMessages	Shows the number of bad MSDP messages received from this peer.
InKeepAliveMessages	Shows the number of keepalive messages received from this peer.
OutKeepAliveMessages	Shows the number of keepalive messages transmitted to this peer.
SAsLearnedFromThisPeer	Shows the total number of SAs learned from this peer.

Table continues...

Name	Description
SAsAdvertisedToThisPeer	Shows the total number of SAs advertised from this peer.
UpOrDownTime	Shows the duration a peer has been up or down.
ConnAndStatsClearedTime	Shows the duration of connection and statistics cleared.

Deleting an MSDP peer

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Peers** tab.
4. Select a row from the peer to delete.
5. Click **Delete**.
6. Click **Yes**.

Peers field descriptions

Use the data in the following table to use the Peers tab.

Name	Description
RemoteAddress	Shows the IP address of the remote MSDP peer.
State	Shows the state of the default peer. An MSDP node only accepts SA messages from an operational default peer. Only one default peer can be operational; the configured default peers provide redundancy.
AdminEnabled	Changes the peer status to administratively enable or disable a configured peer. The default value is disabled (false).
ConnectRetryInterval	Specifies the connection retry period, in seconds, for this peer. The default value is 30 seconds.
HoldTimeConfigured	The default value is 75 seconds.
KeepAliveConfigured	Specifies the keepalive period, in seconds, configured for this MSDP speaker with this peer. If the value is 0 seconds, no periodic keepalive messages are sent to the peer after the MSDP connection is established. The default value is 60 seconds.

Table continues...

Name	Description
DataTtl	Specifies the time-to-live value, from 0–255. The default value is 0, which means that the router forwards all SA messages with encapsulated data.
InSAFilterEnabled	Activates the inbound SA filter for the peer.
InSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter accepts only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all inbound SA messages from this peer.
OutSAFilterEnabled	Activates the outbound SA filter for the peer.
OutSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter sends only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all outbound SA messages from this peer.
Description	Specifies the text description, up to 255 characters, for the peer.
SALimit	Specifies the maximum number of SA messages from an MSDP peer to keep in the SA cache. The valid values are from 0–6144; the default value is 6144.
Md5AuthEnabled	Activates MD5 authentication on the TCP connection between peers. The default is false.
Md5AuthPassword	Specifies a case-sensitive password, up to 80 characters, for MD5 authentication.
RemotePort	Shows the remote port for the TCP connection between the MSDP peers.
LocalPort	Shows the local port for the TCP connection between the MSDP peers.
OperEnabled	Shows the operational status of the peer.
RPFFailures	Shows the number of SA messages received from this peer that failed the Peer-RPF check. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAs	Shows the number of MSDP SA messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAs	Shows the number of MSDP SA messages sent on this connection. Discontinuities in the value of this

Table continues...

Name	Description
	counter can occur at reinitialization of the management system.
InSARquests	Shows the number of MSDP SA-Request messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSARquests	Shows the number of MSDP SA-Request messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAResponses	Shows the number of MSDP SA-Response messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAResponses	Shows the number of MSDP SA-Response messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InControlMessages	Shows the total number of MSDP messages received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutControlMessages	Shows the total number of MSDP messages transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InDataPackets	Shows the total number of encapsulated packets received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutDataPackets	Shows the total number of encapsulated packets transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
FsmEstablishedTransitions	Shows the total number of times the BGP transitioned to the established state.
FsmEstablishedTime	Shows the time when the peer transitioned to the established state.
InMessageTime	Shows the time when the last MSDP message was received from the peer.
ConnectionAttempts	Shows the number of times the state machine has transitioned from inactive to connecting.

Table continues...

Name	Description
DiscontinuityTime	Shows the sysUpTime value (the time, in hundredths of a second, since the network management portion of the system last reinitialized) when one or more of the counters for this entry suffered a discontinuity. Discontinuities can occur at peer connection establishment. If no discontinuities occurred since the last reinitialization of the local management subsystem, the value is zero.
AsNumber	Specifies the autonomous system number of the MSDP peer. A peer can appear to be in another autonomous system (other than the one in which it really resides) if you use an MSDP peering session but do not use a Border Gateway Protocol peer session with that peer. If another autonomous system injects the prefix of the peer, the prefix appears as the autonomous system number of the peer.
TooShortMessages	Shows the number of short messages received from this peer.
InBadMessages	Shows the number of bad MSDP messages received from this peer.
InKeepAliveMessages	Shows the number of keepalive messages received from this peer.
OutKeepAliveMessages	Shows the number of keepalive messages transmitted to this peer.
SAsLearnedFromThisPeer	Shows the total number of SAs learned from this peer.
SAsAdvertisedToThisPeer	Shows the total number of SAs advertised from this peer.
UpOrDownTime	Shows the duration a peer has been up or down.
ConnAndStatsClearedTime	Shows the duration of connection and statistics cleared.

MSDP message control using EDM

Filtering PIM routes

Configure MSDP global filter for which the SA local cache are distributed to all MSDP peers. All SA local cache entries generate SA messages.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Globals** tab.
4. Select the **RedistributeFilterEnabled** check box.
5. Type the name of the route policy in the **RouteMapName** field.
6. Select the **RedistributeFilterApply** check box to apply the changes to the redistribute filter.


You do not need to apply the changes in the following situations:

- You create the redistribute filter without a route policy.
- You disable the redistribute filter.
- You remove a route policy from the redistribute filter.

7. Click **Apply**.

Global field descriptions

Use the data in the following table to use the Globals tab.

Name	Description
Enabled	Enables MSDP. If you clear this check box, you disable MSDP. The default setting is clear (disabled).
CacheLifetime	Configures the lifetime given to SA cache entries when created or refreshed.
NumSACacheEntries	Displays the total number of entries in the SA cache.
RPAddress	Specifies the IP address to use as the originator ID. If the address is not a system local address, the system rejects the configuration.
RouteMapName	Specifies the name of the optional route policy to create or modify. You do not need to create a route policy to use the redistribution filter.  Note: To delete the route map name, clear the field and click Apply .
RedistributeFilterEnabled	Filters the (S,G,RP) entries provided by PIM to MSDP. The default is clear (disabled).
RedistruteFilterApply	Applies the changes made to the redistribute filter.
StatsClear	Clears MSDP statistics.

Filtering SA messages

Filter SA messages to determine which SA messages to accept from a peer and which SA messages to send to a peer. By default, no inbound or outbound filter exists.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Peers** tab.
4. In the row for the peer, double-click the **InSAFilterEnabled** field, and then select true.
5. In the row for the peer, double-click the **InSAFilterRouteMapName** field, and then type the route map name for the IN SA Filter of the peer.
6. In the row for the peer, double-click the **OutSAFilterEnabled** field, and then select true.
7. In the row for the peer, double-click the **OutSAFilterRouteMapName** field, and then type the route map name for the OUT SA Filter of the peer.
8. Click **Apply**.

Peers field descriptions

Use the data in the following table to use the Peers tab.

Name	Description
RemoteAddress	Shows the IP address of the remote MSDP peer.
State	Shows the state of the default peer. An MSDP node only accepts SA messages from an operational default peer. Only one default peer can be operational; the configured default peers provide redundancy.
AdminEnabled	Changes the peer status to administratively enable or disable a configured peer. The default value is disabled (false).
ConnectRetryInterval	Specifies the connection retry period, in seconds, for this peer. The default value is 30 seconds.
HoldTimeConfigured	The default value is 75 seconds.
KeepAliveConfigured	Specifies the keepalive period, in seconds, configured for this MSDP speaker with this peer. If the value is 0 seconds, no periodic keepalive messages are sent to the peer after the MSDP connection is established. The default value is 60 seconds.

Table continues...

Name	Description
DataTtl	Specifies the time-to-live value, from 0–255. The default value is 0, which means that the router forwards all SA messages with encapsulated data.
InSAFilterEnabled	Activates the inbound SA filter for the peer.
InSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter accepts only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all inbound SA messages from this peer.
OutSAFilterEnabled	Activates the outbound SA filter for the peer.
OutSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter sends only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all outbound SA messages from this peer.
Description	Specifies the text description, up to 255 characters, for the peer.
SALimit	Specifies the maximum number of SA messages from an MSDP peer to keep in the SA cache. The valid values are from 0–6144; the default value is 6144.
Md5AuthEnabled	Activates MD5 authentication on the TCP connection between peers. The default is false.
Md5AuthPassword	Specifies a case-sensitive password, up to 80 characters, for MD5 authentication.
RemotePort	Shows the remote port for the TCP connection between the MSDP peers.
LocalPort	Shows the local port for the TCP connection between the MSDP peers.
OperEnabled	Shows the operational status of the peer.
RPFFailures	Shows the number of SA messages received from this peer that failed the Peer-RPF check. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAs	Shows the number of MSDP SA messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAs	Shows the number of MSDP SA messages sent on this connection. Discontinuities in the value of this

Table continues...

Name	Description
	counter can occur at reinitialization of the management system.
InSARquests	Shows the number of MSDP SA-Request messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSARquests	Shows the number of MSDP SA-Request messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAResponses	Shows the number of MSDP SA-Response messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAResponses	Shows the number of MSDP SA-Response messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InControlMessages	Shows the total number of MSDP messages received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutControlMessages	Shows the total number of MSDP messages transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InDataPackets	Shows the total number of encapsulated packets received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutDataPackets	Shows the total number of encapsulated packets transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
FsmEstablishedTransitions	Shows the total number of times the BGP transitioned to the established state.
FsmEstablishedTime	Shows the time when the peer transitioned to the established state.
InMessageTime	Shows the time when the last MSDP message was received from the peer.
ConnectionAttempts	Shows the number of times the state machine has transitioned from inactive to connecting.

Table continues...

Name	Description
DiscontinuityTime	Shows the sysUpTime value (the time, in hundredths of a second, since the network management portion of the system last reinitialized) when one or more of the counters for this entry suffered a discontinuity. Discontinuities can occur at peer connection establishment. If no discontinuities occurred since the last reinitialization of the local management subsystem, the value is zero.
AsNumber	Specifies the autonomous system number of the MSDP peer. A peer can appear to be in another autonomous system (other than the one in which it really resides) if you use an MSDP peering session but do not use a Border Gateway Protocol peer session with that peer. If another autonomous system injects the prefix of the peer, the prefix appears as the autonomous system number of the peer.
TooShortMessages	Shows the number of short messages received from this peer.
InBadMessages	Shows the number of bad MSDP messages received from this peer.
InKeepAliveMessages	Shows the number of keepalive messages received from this peer.
OutKeepAliveMessages	Shows the number of keepalive messages transmitted to this peer.
SAsLearnedFromThisPeer	Shows the total number of SAs learned from this peer.
SAsAdvertisedToThisPeer	Shows the total number of SAs advertised from this peer.
UpOrDownTime	Shows the duration a peer has been up or down.
ConnAndStatsClearedTime	Shows the duration of connection and statistics cleared.

Configuring the MSDP mesh groups

Configure mesh groups to reduce SA flooding. A mesh group does not forward SA messages to other group members in the same mesh group. The originator, which is also a mesh group member, forwards SA messages to all group members. Create MSDP mesh groups from a group of meshed MSDP speakers from a domain. Do not create MSDP peerings between Controllers within the same SPB domain.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.

2. Click **MSDP**.
3. Click the **Mesh Group** tab.
4. Click **Insert**.
5. In the **Name** field, type a name for the mesh group.
6. In the **PeerAddress** field, type the IP address of the peer to add the mesh group.
7. Click **Insert**.

Mesh Group field descriptions

Use the data in the following table to use the Mesh Group tab.

Name	Description
Name	Specifies the mesh group ID; the name of the mesh group from 1-64 characters.
PeerAddress	Specifies the IP address of the MSDP router that is the peer.

Clearing the MSDP SA cache

Clear the SA cache to clear the SA entries the router learns from all the peers or a specific peer.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **SA-Cache** tab.
4. Click **Clear SA-Cache**.

SA-Cache field descriptions

Use the data in the following table to use the SA-Cache tab.

Name	Description
GroupAddr	Shows the group IP address of the SA cache entry.
SourceAddr	Shows the source IP address of the SA cache entry.
OriginRP	Shows the RP address of the SA cache entry.
PeerLearnedFrom	Shows the peer from which this SA cache entry was accepted.
RPFPeer	Shows the peer from which an SA message corresponding to the cache entry is accepted.
InSAs	Discontinuities in the value of this counter can occur at reinitialization of the management system.

Table continues...

Name	Description
InDataPackets	Shows the number of MSDP encapsulated data packets received that are relevant to this cache entry.
UpTime	Shows the time since this entry was first placed in the SA cache.
ExpiryTime	Shows the time remaining before this entry expires from the SA cache.

MSDP verification using EDM

Viewing peer information

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Peers** tab.

Peers field descriptions

Use the data in the following table to use the Peers tab.

Name	Description
RemoteAddress	Shows the IP address of the remote MSDP peer.
State	Shows the state of the default peer. An MSDP node only accepts SA messages from an operational default peer. Only one default peer can be operational; the configured default peers provide redundancy.
AdminEnabled	Changes the peer status to administratively enable or disable a configured peer. The default value is disabled (false).
ConnectRetryInterval	Specifies the connection retry period, in seconds, for this peer. The default value is 30 seconds.
HoldTimeConfigured	The default value is 75 seconds.
KeepAliveConfigured	Specifies the keepalive period, in seconds, configured for this MSDP speaker with this peer. If the value is 0 seconds, no periodic keepalive messages are sent to the peer after the MSDP

Table continues...

Name	Description
	connection is established. The default value is 60 seconds.
DataTtl	Specifies the time-to-live value, from 0–255. The default value is 0, which means that the router forwards all SA messages with encapsulated data.
InSAFilterEnabled	Activates the inbound SA filter for the peer.
InSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter accepts only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all inbound SA messages from this peer.
OutSAFilterEnabled	Activates the outbound SA filter for the peer.
OutSAFilterRouteMapName	Specifies the name of the route map. If you configure the route map name, the filter sends only the SA messages that meet the match criteria in the route map map-name with a permit keyword. If you do not configure the route map name, the system blocks all outbound SA messages from this peer.
Description	Specifies the text description, up to 255 characters, for the peer.
SALimit	Specifies the maximum number of SA messages from an MSDP peer to keep in the SA cache. The valid values are from 0–6144; the default value is 6144.
Md5AuthEnabled	Activates MD5 authentication on the TCP connection between peers. The default is false.
Md5AuthPassword	Specifies a case-sensitive password, up to 80 characters, for MD5 authentication.
RemotePort	Shows the remote port for the TCP connection between the MSDP peers.
LocalPort	Shows the local port for the TCP connection between the MSDP peers.
OperEnabled	Shows the operational status of the peer.
RPFFailures	Shows the number of SA messages received from this peer that failed the Peer-RPF check. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAs	Shows the number of MSDP SA messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.

Table continues...

Name	Description
OutSAs	Shows the number of MSDP SA messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSARquests	Shows the number of MSDP SA-Request messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSARquests	Shows the number of MSDP SA-Request messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InSAResponses	Shows the number of MSDP SA-Response messages received on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutSAResponses	Shows the number of MSDP SA-Response messages sent on this connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InControlMessages	Shows the total number of MSDP messages received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutControlMessages	Shows the total number of MSDP messages transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
InDataPackets	Shows the total number of encapsulated packets received on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
OutDataPackets	Shows the total number of encapsulated packets transmitted on this TCP connection. Discontinuities in the value of this counter can occur at reinitialization of the management system.
FsmEstablishedTransitions	Shows the total number of times the BGP transitioned to the established state.
FsmEstablishedTime	Shows the time when the peer transitioned to the established state.
InMessageTime	Shows the time when the last MSDP message was received from the peer.

Table continues...

Name	Description
ConnectionAttempts	Shows the number of times the state machine has transitioned from inactive to connecting.
DiscontinuityTime	Shows the sysUpTime value (the time, in hundredths of a second, since the network management portion of the system last reinitialized) when one or more of the counters for this entry suffered a discontinuity. Discontinuities can occur at peer connection establishment. If no discontinuities occurred since the last reinitialization of the local management subsystem, the value is zero.
AsNumber	Specifies the autonomous system number of the MSDP peer. A peer can appear to be in another autonomous system (other than the one in which it really resides) if you use an MSDP peering session but do not use a Border Gateway Protocol peer session with that peer. If another autonomous system injects the prefix of the peer, the prefix appears as the autonomous system number of the peer.
TooShortMessages	Shows the number of short messages received from this peer.
InBadMessages	Shows the number of bad MSDP messages received from this peer.
InKeepAliveMessages	Shows the number of keepalive messages received from this peer.
OutKeepAliveMessages	Shows the number of keepalive messages transmitted to this peer.
SAsLearnedFromThisPeer	Shows the total number of SAs learned from this peer.
SAsAdvertisedToThisPeer	Shows the total number of SAs advertised from this peer.
UpOrDownTime	Shows the duration a peer has been up or down.
ConnAndStatsClearedTime	Shows the duration of connection and statistics cleared.

Viewing the local SA cache

View the local SA cache to display the (S, G) state the router learns from local Protocol Independent Multicast - Sparse Mode (PIM-SM) entries.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.

3. Click the **SA-Cache-Records** tab.

SA-Cache-Records field descriptions

Use the data in the following table to use the SA-Cache-Records tab.

Name	Description
TypeInformation	Shows the SA cache type. The SA cache type can be local or foreign cache.
GroupAddr	Shows the group IP address of the SA cache entry.
SourceAddr	Shows the source IP address of the SA cache entry.
OriginRP	Shows the RP address of the SA cache entry.
OriginatorAsNumber	Shows the AS number of the originator.
RouteType	Shows the type of route used for Reverse Path Forwarding checking. The value can be rip (1), ospf (2), static (3), bgp (4), isis(5) or none (6).

Viewing the foreign SA cache

View the foreign SA cache to display the (S, G) state the router learns from SA messages.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **SA-Cache-Records** tab.

SA-Cache-Records field descriptions

Use the data in the following table to use the SA-Cache-Records tab.

Name	Description
TypeInformation	Shows the SA cache type. The SA cache type can be local or foreign cache.
GroupAddr	Shows the group IP address of the SA cache entry.
SourceAddr	Shows the source IP address of the SA cache entry.
OriginRP	Shows the RP address of the SA cache entry.
OriginatorAsNumber	Shows the AS number of the originator.
RouteType	Shows the type of route used for Reverse Path Forwarding checking. The value can be rip (1), ospf (2), static (3), bgp (4), isis(5) or none (6).

Viewing the mesh group

Configure Message Digest (MD) 5 authentication to secure control messages on the TCP connection between MSDP peers.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **MSDP**.
3. Click the **Mesh Group** tab.

Mesh Group field descriptions

Use the data in the following table to use the Mesh Group tab.

Name	Description
Name	Specifies the mesh group ID; the name of the mesh group from 1-64 characters.
PeerAddress	Specifies the IP address of the MSDP router that is the peer.

Chapter 4: Controller configuration

This section provides procedures to configure the Controller using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

The Controller functionality is configured at the global (switch-wide) level.

Controller configuration using CLI

Enabling the Controller

Enable the Controller globally.

Procedure

1. Enter IS-IS Router Configuration mode:

```
enable
configure terminal
router isis
```

2. Enable the Controller globally:

```
spbm <1-100> multicast spb-pim-gw controller enable
```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#router isis
Switch:1(config-isis)#spbm 1 multicast spb-pim-gw controller enable
```

Variable definitions

Use the data in the following table to use the **spb** command.

Variable	Value
<1-100>	Specifies the isis spbm instance-id to create the spbm instance.
controller <i>enable</i>	Enables the SPB-PIM Gateway Controller.

Displaying the Controller admin status

Use the following procedure to display the admin status of the Controller.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the Controller Status:

```
show isis spbm
```

Example

*** Note:**

The SPB-PIM-GW column displays either Controller, Gateway, or Controller/Gateway if the Controller and or Gateway functionality is configured.

```
Switch:1>show isis spbm
```

```

=====
                        ISIS SPBM Info
=====
SPBM      B-VID      PRIMARY      NICK      LSDB      IP      IPV6      MULTICAST      SPB-PIM-GW
INSTANCE  INSTANCE
-----
1         10,20        10          0.00.77   disable  enable  disable  enable        controller
-----
                        ISIS SPBM SMLT Info
=====
SPBM      SMLT-SPLIT-BEB      SMLT-VIRTUAL-BMAC      SMLT-PEER-SYSTEM-ID
INSTANCE
-----
1         primary              00:00:00:00:00:00
-----

Total Num of SPBM instances: 1
=====

```

Displaying the active Controller and Gateway Nodes

Use the following procedure to display the active Controllers and Gateways in the SPBM domain.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the SPB-PIM Gateway active Controller and Gateway Nodes:

```
show ip spb-pim-gw node [controller | gateway] [spb-node-as-mac]
```

Example

Display all node lists:

```
Switch:1>show ip spb-pim-gw node
```

```
=====
                               Spb-pim-gw Active Controller/Gateway
=====
HOST-NAME      Role
-----
BEB3-4037      Gateway
BEB5-4011      Controller
Total Number of Nodes = 2/2
=====
```

Display Controller node lists only:

```
Switch:1>show ip spb-pim-gw node controller
```

```
=====
                               Spb-pim-gw Active Controller/Gateway
=====
HOST-NAME      Role
-----
BEB5-4011      Controller
Total Number of Nodes = 1/2
=====
```

Display Gateway node lists only:

```
Switch:1>show ip spb-pim-gw node gateway
```

```
=====
                               Spb-pim-gw Active Controller/Gateway
=====
HOST-NAME      Role
-----
BEB3-4037      Gateway
Total Number of Nodes = 1/2
=====
```

Display all node lists with MAC address:

```
Switch:1>show ip spb-pim-gw node spb-node-as-mac
```

```
=====
                               Spb-pim-gw Active Controller/Gateway
=====
HOST-NAME      Role      Mac Address
-----
=====
```

Controller configuration

```
BEB3-4037      Gateway      00:37:00:37:00:37
BEB5-4011      Controller   00:11:00:11:00:11
Total Number of Nodes = 2/2
```

Display Controller node lists with MAC address:

```
Switch:1>show ip spb-pim-gw node controller spb-node-as-mac
```

```
=====
                               Spb-pim-gw Active Controller/Gateway
=====
HOST-NAME      Role          Mac Address
-----
BEB5-4011      Controller    00:11:00:11:00:11
Total Number of Nodes = 1/2
=====
```

Display Gateway node lists with MAC address:

```
Switch:1>show ip spb-pim-gw node gateway spb-node-as-mac
```

```
=====
                               Spb-pim-gw Active Controller/Gateway
=====
HOST-NAME      Role          Mac Address
-----
BEB3-4037      Gateway       00:37:00:37:00:37
Total Number of Nodes = 1/2
=====
```

Configuring a static foreign source on the global router

Configure a static foreign source on the global router. Configuration is done at the Controller. Statically configure foreign sources, such as streams in a Source Specific Multicast (SSM) group range that are not advertised by the foreign network through MSDP. Non-SSM range group multicast address streams are advertised by MSDP and do not need to be statically configured.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure a static foreign source:

```
ip spb-pim-gw foreign-source {A.B.C.D} group {A.B.C.D}
```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ip spb-pim-gw foreign-source 10.0.0.1 group 240.0.0.1
```

Variable definitions

Use the data in the following table to use the `ip spb-pim-gw` command.

Variable	Value
foreign-source{A.B.C.D}	Specifies the multicast foreign source IP address.
group{A.B.C.D}	Specifies the group IP address.

Configuring a static foreign source on a VRF

Configure a static foreign source on a VRF, configuration is done at the Controller.

Procedure

1. Enter VRF Router Configuration mode for a specific VRF context:

```
enable
configure terminal
router vrf WORD<1-16>
```

2. Configure a static foreign source:

```
ip spb-pim-gw foreign-source {A.B.C.D} group {A.B.C.D}
```

Example

In the following example, vrf-10 is configured with vrf id 10.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#router vrf vrf-10
Switch:1(router-vrf)#ip spb-pim-gw foreign-source 10.0.0.1 group
240.0.0.1
```

Variable definitions

Use the data in the following table to use the `ip spb-pim-gw` command.

Variable	Value
foreign-source{A.B.C.D}	Specifies the multicast foreign source IP address.
group{A.B.C.D}	Specifies the group IP address.

Displaying foreign sources

Use the following procedure to display the foreign sources learned from MSDP or statically configured at the Controller.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the foreign source information:

```
show ip spb-pim-gw foreign-source [all] [controller | gateway] [vrf
WORD<0-16>] [vrfrids WORD<0-512>] [source {A.B.C.D}] [group
{A.B.C.D}] [static | msdp] [spb-node-as-mac]
```

Example

* Note:

The command **show ip spb-pim-gw**, which specifies the parameter controller, the OWNER column displays the RP address of the MSDP peer from which the foreign source was learned. If the gateway parameter is specified, then the OWNER column displays MSDP rather than the actual RP address.

```
Switch:1>show ip spb-pim-gw foreign-source controller
=====
SPB-PIM-GW Controller Foreign Source
=====
SOURCE      GROUP      SPB-PIM-GW      VRF          OWNER
-----
10.0.0.1    240.0.0.1  beb-1           GlobalRouter  47.17.0.1
10.0.0.2    240.0.0.2  beb-1           GlobalRouter  static
10.0.0.3    240.0.0.3  -               GlobalRouter  47.17.0.2
=====
```

Display the foreign sources from a specific VRF:


```
Switch:1>show ip spb-pim-gw foreign-source controller vrf green
=====
SPB-PIM-GW Controller Foreign Source
=====
SOURCE      GROUP      SPB-PIM-GW      VRF          OWNER
-----
10.0.0.1    240.0.0.1  beb-1           green        47.17.0.1
10.0.0.2    240.0.0.2  beb-1           green        static
10.0.0.3    240.0.0.3  -               green        47.17.0.2
=====
```

Display all the foreign sources at the Controller with the Gateway in the SPB-PIM-GW shown as a mac address rather than a nickname:

```
Switch:1>show ip spb-pim-gw foreign-source controller vrf green spb-node-as-mac
=====
SPB-PIM-GW Controller Foreign Source
=====
SOURCE      GROUP      SPB-PIM-GW      VRF          OWNER
-----
10.0.0.1    240.0.0.1  00:0b:eb:00:00:a1 green        47.17.0.1
10.0.0.2    240.0.0.2  00:0b:eb:00:00:a1 green        static
10.0.0.3    240.0.0.3  -               green        47.17.0.2
=====
```


Variable definitions

Use the data in the following table to use the `show ip spb-pim-gw foreign source` command.

Variable	Value
<i>all</i>	Displays information for all the VRF IDs from the Controller and Gateway foreign source database.
<i>controller</i>	Displays information from the Controller foreign source database. Only displays information on nodes configured as Controller.
<i>gateway</i>	Displays information from the Gateway foreign source database. Only displays information on nodes configured as Gateway.
vrf <i>WORD<0-16></i>	Displays information from the Controller foreign source database for a specific VRF name.
vrfids <i>WORD<0-512></i>	Displays information from the Controller foreign source database for a range of VRF IDs.  Note: Enter a single VRF ID or multiple VRF IDs separated by ',' or enter a range of VRF IDs 'x-y'.
source <i>{A.B.C.D}</i>	Displays information for the specific source IP address from the Controller foreign source database.
group <i>{A.B.C.D}</i>	Displays information for the specific multicast group IP address from the Controller foreign source database.
<i>static</i>	Displays information from the Controller foreign source database that is configured statically.
<i>msdp</i>	Displays information from the Controller foreign source database that is learned through MSDP.
<i>spb-node-as-mac</i>	Displays the MAC address for the assigned SPB-PIM Gateway.

Displaying Multicast over Fabric Connect sources

Use the following procedure to display all the SPB Multicast over Fabric Connect sources distributed to MSDP. This procedure is only valid on a Controller node.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the SPB source information:

```
show ip spb-pim-gw spbmc-source [vrf WORD<0-16>] [vrfids
WORD<0-512>] [source {A.B.C.D}] [group {A.B.C.D}] [originator
WORD<1-32>] [spb-node-as-mac]
```

Example

```
Switch:1>show ip spb-pim-gw spbmc-source
=====
SPB-PIM-GW SPB Source
=====
SOURCE          GROUP          VRF            ORIGINATOR
-----
10.0.0.1        240.0.0.1     GlobalRouter   bcb-1
10.0.0.2        240.0.0.2     GlobalRouter   bcb-2
10.0.0.3        240.0.0.3     GlobalRouter   bcb-2
=====
```

Display the SPB Multicast over Fabric Connect from a specific VRF:

```
Switch:1>show ip spb-pim-gw spbmc-source vrf green
=====
SPB-PIM-GW Foreign Source
=====
SOURCE  GROUP    SPB-PIM-GW    VRF      OWNER    CONTROLLER
-----
10.0.0.1 240.0.0.1 beb-1          green    47.17.0.1 bcb-2
10.0.0.2 240.0.0.2 beb-1          green    static    bcb-2
10.0.0.3 240.0.0.3 -              green    47.17.0.2 bcb-2
=====
```

Display all the SPB Multicast over Fabric Connect sources advertised to MSDP with the originator value shown as a MAC address rather than a host name:

```
Switch:1>show ip spb-pim-gw spbmc-source vrf green spb-node-as-mac
=====
=
SPB-PIM-GW SPB Source
=====
=
SOURCE          GROUP          VRF            ORIGINATOR
-----
-
10.0.0.1        240.0.0.1     green          00:0b:cb:00:00:c2
10.0.0.2        240.0.0.2     green          00:0b:cb:00:00:c2
10.0.0.3        240.0.0.3     green          00:0b:cb:00:00:c2
=====
-
```

Variable definitions

Use the data in the following table to use the `show ip spb-pim-gw spbmc-source` command.

Variable	Value
vrf WORD<0-16>	Displays SPB originated sources for a specific VRF.
vrfids WORD<0-512>	Displays SPB originated sources for a range of VRF IDs. <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> Note:</div> <div>Enter a single VRF ID or multiple VRF IDs separated by ',' or enter a range of VRF IDs 'x-y'.</div> </div>

Table continues...

Variable	Value
source {A.B.C.D}	Displays information for a specific source IP address from SPB originated sources database.
group {A.B.C.D}	Displays information for a specific multicast group IP address from SPB originated sources database.
originator WORD<0-32>	Displays information for a specific originator host name from SPB originated sources database.
spb-node-as-mac	Displays the originator of SPB originated sources as a MAC address rather than a nickname.

Controller configuration using EDM

Enabling the Controller

Enable the Controller globally.

Procedure

1. In the navigation pane, expand the **Configuration > IS-IS** folders.
2. Click **SPBM**.
3. In the row for the SPBM, double click the **McastSpbPimGwControllerEnable** field, and then select true.
4. Click **Apply**.

Related links

[Controller configuration](#) on page 91

SPBM field descriptions

Use the data in the following table to use the SPBM tab.

Name	Description
McastSpbPimGwControllerEnable	Enables or disables the ISIS multicast SPM-PIM Gateway Controller node.
McastSpbPimGWGatewayEnable	Enables or disables the ISIS multicast SPM-PIM Gateway node.

Displaying the Controller and Gateway admin status

Use the following procedure to display the admin status of the Controller and Gateway.

Procedure

1. In the navigation pane, expand the **Configuration > IS-IS** folders.
2. Click **SPBM**.
3. Click the **SPBM** tab.

Displaying active Controller and Gateway nodes

Use the following procedure to display the active Controllers and Gateways in the SPBM domain.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **SPB-PIM-GW**.
3. Click the **Node** tab.

Configuring a static foreign source globally

Configure a static foreign source on the global router. Configuration is done at the Controller.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **SPB-PIM-GW**.
3. Click the **Controller-Foreign-Source** tab.
4. Click **Insert**.
5. In the **SourceAddress** box, type the multicast foreign source IP address.
6. In the **GroupAddress** box, type the group IP address.
7. Click **Insert**.

Controller-Foreign-Source field descriptions

Use the data in the following table to use the Controller-Foreign-Source tab.

Name	Description
SourceAddress	Specifies the source IP address from a foreign multicast domain.
GroupAddress	Specifies the multicast group IP address associated with the foreign source.
GatewaySysId	Displays the system ID of the node selected as the Gateway for this foreign source. GatewaySysId field

Table continues...

Name	Description
	will have a valid value if the Gateway is assigned to a source. If the Gateway is not assigned to a source the value is 0.
GatewayHostName	Displays the host name of the node selected as the Gateway for this foreign source. GatewayHostName field will have valid values if the Gateway is assigned to a source. If the Gateway is not assigned to a source the value is NULL.
Type	Displays the owner type for this source.
Owner	Displays the IP address of the MSDP peer if the foreign source is MSDP.

Configuring a static foreign source on a VRF

Configure a static foreign source on a VRF. Configuration is done at the Controller.

Procedure

1. In the navigation pane, expand the **Configuration > VRF Context View** folders.
2. Click **Set VRF Context view**.
3. Select a row and click **Launch VRF Context view**.
4. Select a switch port in the **Device Physical View** tab.
5. In the navigation pane, expand the **Configuration > IP** folders.
6. Click **SPB-PIM-GW**.
7. Click the **Controller-Foreign-Source** tab.
8. Click **Insert**.
9. In the **SourceAddress** box, type the multicast foreign source IP address.
10. In the **GroupAddress** box, type the group IP address.
11. Click **Insert**.

Controller-Foreign-Source field descriptions

Use the data in the following table to use the Controller-Foreign-Source tab.

Name	Description
SourceAddress	Specifies the source IP address from a foreign multicast domain.
GroupAddress	Specifies the multicast group IP address associated with the foreign source.

Table continues...

Name	Description
GatewaySysId	Displays the system ID of the node selected as the Gateway for this foreign source. GatewaySysId field will have a valid value if the Gateway is assigned to a source. If the Gateway is not assigned to a source the value is 0.
GatewayHostName	Displays the host name of the node selected as the Gateway for this foreign source. GatewayHostName field will have valid values if the Gateway is assigned to a source. If the Gateway is not assigned to a source the value is NULL.
Type	Displays the owner type for this source.
Owner	Displays the IP address of the MSDP peer if the foreign source is MSDP.

Displaying foreign sources

Use the following procedure to display the foreign sources learned from MSDP or statically configured at the Controller.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **SPB-PIM-GW**.
3. Click the **Controller-Foreign-Source** tab.

Controller-Foreign-Source field descriptions

Use the data in the following table to use the Controller-Foreign-Source tab.

Name	Description
SourceAddress	Specifies the source IP address from a foreign multicast domain.
GroupAddress	Specifies the multicast group IP address associated with the foreign source.
GatewaySysId	Displays the system ID of the node selected as the Gateway for this foreign source. GatewaySysId field will have a valid value if the Gateway is assigned to a source. If the Gateway is not assigned to a source the value is 0.
GatewayHostName	Displays the host name of the node selected as the Gateway for this foreign source. GatewayHostName field will have valid values if the Gateway is assigned

Table continues...

Name	Description
	to a source. If the Gateway is not assigned to a source the value is NULL.
Type	Displays the owner type for this source.
Owner	Displays the IP address of the MSDP peer if the foreign source is MSDP.

Displaying Multicast over Fabric Connect sources

Use the following procedure to display all the SPB Multicast over Fabric Connect sources distributed to MSDP.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **SPB-PIM-GW**.
3. Click the **spbm-source** tab.

Spbmc-Source field descriptions

Use the data in the following table to use the Spbmc-Source tab.

Name	Description
SourceAddress	Displays the source IP address from SPBM multicast domain.
GroupAddress	Displays the multicast group IP address associated with the SPBM source.
OriginatorSysId	Displays the system ID of the node from which the source originates.
OriginatorHostName	Displays the host name of the node from which the source originates.

Chapter 5: Gateway configuration

This section provides procedures to configure the Gateway using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

The Gateway functionality is configured at the global (switch-wide) level. SPB-PIM Gateway Interfaces are configured at the interface level. For more information on SPB-PIM Gateway Interfaces configuration, see [SPB-PIM Gateway interface configuration](#) on page 113.

Gateway Configuration using CLI

Enabling the Gateway

Enable the Gateway at the global (switch-wide) level.

Procedure

1. Enter IS-IS Router Configuration mode:

```
enable
configure terminal
router isis
```

2. Enable the Gateway globally:

```
spb <1-100> multicast spb-pim-gw gateway enable
```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#router isis
Switch:1(config-isis)#spb 1 multicast spb-pim-gw gateway enable
```

Variable definitions

Use the data in the following table to use the `spb` command.

Variable	Value
<1-100>	Specifies the isis spbm instance-id to create the spbm instance.
gateway enable	Enables the SPB-PIM Gateway.

Displaying the Gateway admin status

Use the following procedure to display the admin status of the Gateway.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the Gateway admin status:

```
show isis spbm
```

Example

```
Switch:1>show isis spbm
```

```

=====
                        ISIS SPBM Info
=====
SPBM      B-VID      PRIMARY      NICK      LSDB      IP      IPV6      MULTICAST      SPB-PIM-GW
INSTANCE  VLAN        VLAN        NAME      TRAP
-----
1         10,20       10          0.00.77   disable   enable   disable   enable         Gateway
=====
                        ISIS SPBM SMLT Info
=====
SPBM      SMLT-SPLIT-BEB      SMLT-VIRTUAL-BMAC      SMLT-PEER-SYSTEM-ID
INSTANCE
-----
1         primary              00:00:00:00:00:00
=====
Total Num of SPBM instances: 1
=====

```

If the controller and gateway are both enabled on the node

```
Switch:1>show isis spbm
```

```

=====
                        ISIS SPBM Info
=====
SPBM      B-VID      PRIMARY      NICK      LSDB      IP      IPV6      MULTICAST      SPB-PIM-GW
INSTANCE  VLAN        VLAN        NAME      TRAP
-----
1         10,20       10          0.00.77   disable   enable   disable   enable
controller
                                     /gateway
=====

```

```

=====
                        ISIS SPBM SMLT Info
=====
SPBM          SMLT-SPLIT-BEB          SMLT-VIRTUAL-BMAC          SMLT-PEER-SYSTEM-ID
INSTANCE
-----
1             primary                00:00:00:00:00:00
-----

Total Num of SPBM instances: 1
=====

```

Displaying foreign sources information

Use the following procedure to display the Gateway foreign sources database. If executed on a Gateway node, it displays the foreign sources assigned to the Gateway by the Controller. Foreign sources are originally learned from MSDP or statically configured on the Controller.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the foreign sources information:

```

show ip spb-pim-gw foreign-source [all] [controller | gateway] [vrf
WORD<0-16>] [vrffids WORD<0-512>] [source {A.B.C.D}] [group
{A.B.C.D}] [from-controller <0x00:0x00:0x00:0x00:0x00:0x00> |
preferred][static | msdp] [spb-node-as-mac]

```

Example

```
Switch:1>show ip spb-pim-gw foreign-source gateway
```

```
=====
SPB-PIM-GW Gateway Foreign Source
=====
```

SOURCE	GROUP	SPB-PIM-GW	VRF	PORT	VLAN	CONTROLLER	OWNER
10.0.0.1	240.0.0.1	beb-2	GlobalRouter	1/1	200	bcb-2	msdp
10.0.0.2	240.0.0.2	beb-2	GlobalRouter	1/1	200	bcb-2	static
10.0.0.3	240.0.0.3	beb-2	GlobalRouter	-	-	bcb-2	msdp

* Note:

The SPB-PIM-GW column displays the node that is selected as the Gateway for the particular source or group stream. The OWNER column displays either msdp or static depending on how the source was originally learned at the assigning Controller. The PORT and VLAN columns represent the port or VLAN toward the source.

Display the foreign sources from a specific VRF:

```
Switch:1>show ip spb-pim-gw foreign-source gateway vrf green
```

```
=====
SPB-PIM-GW Gateway Foreign Source
=====
```

SOURCE	GROUP	SPB-PIM-GW	VRF	PORT	VLAN	CONTROLLER	OWNER
10.0.0.1	240.0.0.1	beb-2	green	1/1	200	bcb-2	msdp
10.0.0.2	240.0.0.2	beb-2	green	1/1	200	bcb-2	static
10.0.0.3	240.0.0.3	beb-2	green	-	-	bcb-2	msdp

Display all the foreign sources available at the Gateway with SPB-PIM-GW and Controller as mac:

```
Switch:1>show ip spb-pim-gw foreign-source gateway vrf green spb-node-as-mac
```

```
=====
```

```
SPB-PIM-GW Gateway Foreign Source
```

```
=====
```

SOURCE	GROUP	SPB-PIM-GW	VRF	PORT	VLAN	CONTROLLER	OWNER
10.0.0.1	240.0.0.1	00:0b:eb:00:00:a2	green	1/1	200	00:0b:cb:00:00:c2	msdp
10.0.0.2	240.0.0.2	00:0b:eb:00:00:a2	green	1/1	200	00:0b:cb:00:00:c2	static
10.0.0.3	240.0.0.3	00:0b:eb:00:00:a2	green	-	-	00:0b:cb:00:00:c2	msdp

Display all the foreign sources available at the Gateway which are statically configured at the Controller:

```
Switch:1>show ip spb-pim-gw foreign-source gateway vrf green static
```

```
=====
```

```
SPB-PIM-GW Gateway Foreign Source
```

```
=====
```

SOURCE	GROUP	SPB-PIM-GW	VRF	PORT	VLAN	CONTROLLER	OWNER
10.0.0.2	240.0.0.2	beb-2	green	1/1	200	bcb-2	static

Variable definitions

Use the data in the following table to use the `show ip spb-pim-gw foreign source` command.


Variable	Value
<i>all</i>	Displays information for all the VRF IDs from the Controller and Gateway foreign source database.
<i>controller</i>	Displays information from the Controller foreign source database. Only displays information on nodes configured as Controller.
<i>gateway</i>	Displays information from the Gateway foreign source database. Only displays information on nodes configured as Gateway.
<i>vrf WORD<0-16></i>	Displays information from the Gateway foreign source database for a specific VRF name.
<i>vrfids WORD<0-512></i>	Displays information from the Gateway foreign source database for a range of VRF IDs.  Note: Enter a single VRF ID or multiple VRF IDs separated by ',' or enter a range of VRF IDs 'x-y'.

Table continues...

Variable	Value
source {A.B.C.D}	Displays information for the specific source IP address from the Gateway foreign source database.
group {A.B.C.D}	Displays information for the specific multicast group IP address from the Gateway foreign source database.
from-controller 0x00:0x00:0x00:0x00:0x00:0x00	Displays information filtering on a specific Controllers assignments, where the Controller is specified as a mac address.
from-controller preferred	Displays information from Gateway source database filtering on a preferred Controller or chosen by the Gateway.
static	Displays information from the Gateway foreign source database that is configured statically at the assigning Controller.
msdp	Displays information from the Gateway foreign source database that is learned through MSDP.
spb-node-as-mac	Displays the MAC address for the assigned PIM-GW.

Displaying the active Controller and Gateway Nodes

Use the following procedure to display the active Controllers and Gateways in the SPBM domain.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the SPB-PIM Gateway active Controller and Gateway Nodes:

```
show ip spb-pim-gw node [controller | gateway] [spb-node-as-mac]
```

Example

Display all node lists:

```
Switch:1>show ip spb-pim-gw node
```

```
=====
                               Spb-pim-gw Active Controller/Gateway
=====
HOST-NAME           Role
-----
BEB3-4037           Gateway
BEB5-4011           Controller

Total Number of Nodes = 2/2
=====
```

Display Controller node lists only:

```
Switch:1>show ip spb-pim-gw node controller
```

```
=====
                               Spb-pim-gw Active Controller/Gateway
=====
```

```
=====
HOST-NAME      Role
-----
BEB5-4011      Controller
Total Number of Nodes = 1/2
=====
```

Display Gateway node lists only:

```
Switch:1>show ip spb-pim-gw node gateway
```

```
=====
                                Spb-pim-gw Active Controller/Gateway
=====
HOST-NAME      Role
-----
BEB3-4037      Gateway
Total Number of Nodes = 1/2
=====
```

Display all node lists with MAC address:

```
Switch:1>show ip spb-pim-gw node spb-node-as-mac
```

```
=====
                                Spb-pim-gw Active Controller/Gateway
=====
HOST-NAME      Role      Mac Address
-----
BEB3-4037      Gateway   00:37:00:37:00:37
BEB5-4011      Controller 00:11:00:11:00:11
Total Number of Nodes = 2/2
=====
```

Display Controller node lists with MAC address:

```
Switch:1>show ip spb-pim-gw node controller spb-node-as-mac
```

```
=====
                                Spb-pim-gw Active Controller/Gateway
=====
HOST-NAME      Role      Mac Address
-----
BEB5-4011      Controller 00:11:00:11:00:11
Total Number of Nodes = 1/2
=====
```

Display Gateway node lists with MAC address:

```
Switch:1>show ip spb-pim-gw node gateway spb-node-as-mac
```

```
=====
                                Spb-pim-gw Active Controller/Gateway
=====
HOST-NAME      Role      Mac Address
-----
BEB3-4037      Gateway   00:37:00:37:00:37
=====
```

Total Number of Nodes = 1/2

Gateway Configuration using EDM

Enabling the Gateway globally

Use this procedure to enable the Gateway at the global (switch-wide) level.

Procedure

1. In the navigation pane, expand the **Configuration > IS-IS** folders.
2. Click **SPBM**.
3. In the row for the SPBM, double click the **McastSpbPimGwGatewayEnable** field, and then select true.
4. Click **Apply**.

SPBM field descriptions

Use the data in the following table to use the SPBM tab.

Name	Description
McastSpbPimGwControllerEnable	Enables or disables the ISIS multicast SPM-PIM Gateway Controller node.
McastSpbPimGWGatewayEnable	Enables or disables the ISIS multicast SPM-PIM Gateway node.

Displaying the Controller and Gateway admin status

Use the following procedure to display the admin status of the Controller and Gateway.

Procedure

1. In the navigation pane, expand the **Configuration > IS-IS** folders.
2. Click **SPBM**.
3. Click the **SPBM** tab.

Displaying foreign sources

Use the following procedure to display the Gateway foreign source database. Foreign sources are originally learned from MSDP or statically configured on the Controller.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **SPB-PIM-GW**.
3. Click the **Gateway-Foreign-Source** tab.

Gateway-Foreign-Source field descriptions

Use the data in the following table to use the Gateway-Foreign-Source tab.

Name	Description
SourceAddress	Displays the foreign source IP address.
GroupAddress	Displays the multicast group IP address associated with the foreign source.
ControllerSysId	Displays the system ID of the controller node that sends this foreign source.
ControllerHostName	Displays the host name of the controller node that sends this foreign source.
GatewaySysId	Displays the system ID of the node selected as the gateway for this foreign source.
GatewayHostName	Displays the host name of the node selected as the gateway for this foreign source.
InVid	Displays the VLAN ID of the SPB-PIM Gateway interface through which the source of this source is reachable.
InPort	Displays the physical interface through which the source of this source is reachable.
Owner	Displays the RP of the MSDP peer if the owner is MSDP. If the owner is not an MSDP then the value is 0.0.0.0.

Displaying active Controller and Gateway nodes

Use the following procedure to display the active Controllers and Gateways in the SPBM domain.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **SPB-PIM-GW**.

3. Click the **Node** tab.

Chapter 6: SPB-PIM Gateway interface configuration

This section provides procedures to configure the SPB-PIM Gateway interface using the Command Line Interface (CLI) and Enterprise Device Manager (EDM).

The SPB-PIM Gateway interface is either a VLAN or a Brouter port interface. An SPB-PIM Gateway interface is configured separately from the global (switch-wide) Gateway functionality. The global Gateway configuration does not affect the administrative or the operational state of the SPB-PIM Gateway interfaces which function independently. However, the Gateway node functionality works in conjunction with the Gateway Interface functionality. Configure SPB-PIM Gateway on an interface that connects to a router in a foreign PIM or SPB multicast domain.

SPB-PIM Gateway interface configuration using CLI

Enabling SPB-PIM Gateway on a VLAN

Enable SPB-PIM Gateway on a VLAN interface.

Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <1-4059>
```

2. Enable SPB-PIM Gateway on a VLAN:

```
ip spb-pim-gw enable
```

 **Note:**

SPB-PIM Gateway cannot be enabled under the following circumstances:

- If the IP interface does not exist on the VLAN. An IP Address must first be configured on the VLAN.

- If the `spbm_config_mode` boot flag is set to false.
- If the VLAN is configured with a circuitless IP.
- If the interface is a management VLAN.
- If `ip igmp snooping` is enabled.
- If the spb-multicast is enabled on the VLAN.
- If the VLAN has SMLT ports.
- If the VLAN has an i-sid configured.
- If the VLAN is a vIST VLAN.

Enabling SPB-PIM Gateway on a brouter port interface

Enable SPB-PIM Gateway on a brouter port.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

```
enable  
  
configure terminal  
  
interface GigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-  
port]][,...]}
```

*** Note:**

If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Enable SPB-PIM Gateway on a brouter port:

```
ip spb-pim-gw enable
```

*** Note:**

SPB-PIM Gateway cannot be enabled under the following circumstances:

- If the IP interface is not configured using the `brouter` command
- If the IP interface does not exist on the brouter port
- If the `spbm_config_mode` boot flag is set to false
- If `ip igmp snooping` is enabled
- If the spb-multicast is enabled on the brouter port
- If the brouter port is part of an SMLT or vIST Vlan
- If the brouter port has an i-sid configured

Configuring the SPB-PIM Gateway VLAN optional parameters

Configure the SPB-PIM Gateway interface parameters on a VLAN.

Procedure

1. Enter VLAN Interface Configuration mode:


```
enable
configure terminal
interface vlan <1-4059>
```
2. Configure the SPB-PIM Gateway VLAN HELLO interval:


```
ip spb-pim-gw hello-interval <0-18724>
```
3. Configure the SPB-PIM Gateway VLAN JOIN PRUNE interval:


```
ip spb-pim-gw ip join-prune-interval <1-18724>
```

Variable definitions

Use the data in the following table to use the `ip spb-pim-gw` command.

Variable	Value
hello-interval<0-18724>	Specifies the HELLO interval in seconds. The default value is 30 seconds.
join-prune-interval<1-18724>	Specifies the JOIN PRUNE interval in seconds. The default value is 60 seconds.

Configuring the SPB-PIM Gateway router port optional parameters

Configure the SPB-PIM Gateway interface parameters on a router port.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:


```
enable
configure terminal
interface GigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}
```

*** Note:**

If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Configure the SPB-PIM Gateway router port HELLO interval:

```
ip spb-pim-gw hello-interval <0-18724>
```

3. Configure the SPB-PIM Gateway router port JOIN PRUNE interval:

```
ip spb-pim-gw join-prune-interval <1-18724>
```

Variable definitions

Use the data in the following table to use the `ip spb-pim-gw` command.

Variable	Value
hello-interval<0-18724>	Specifies the HELLO interval in seconds. The default value is 30 seconds.
join-prune-interval<1-18724>	Specifies the JOIN PRUNE interval in seconds. The default value is 60 seconds.

Displaying the SPB-PIM Gateway interface default values

Use the following procedure to display the default values used for the SPB-PIM Gateway interface HELLO and JOIN PRUNE intervals unless specifically configured on the individual interface.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the SPB-PIM Gateway interface default values:

```
show ip spb-pim-gw
```

Example

```
Switch:1>show ip spb-pim-gw
```

```
=====
                        Spb-pim-gw General Group
=====
Hello Interval           : 30
Join-Prune Interval     : 60
```

Displaying the SPB-PIM Gateway router port information

Use the following procedure to display the SPB-PIM Gateway router port information. This procedure displays the administrative (configured) state of the interface as well as the operational state, and the HELLO and JOIN PRUNE intervals. An interface can be administratively ENABLED but operationally DISABLED if, for example, mvpn is not enabled on the VRF, or `spbmn <spbmn-instance> multicast enable` is not configured.

Procedure

1. Log on to the switch to enter User EXEC mode.

2. Display the SPB-PIM Gateway interface information:

```
show ip spb-pim-gw interface [gigabitethernet {slot/port[/sub-port]
[-slot/port[/sub-port]] [,...]] [vrf WORD<0-16>] [vrfids
WORD<0-512>]
```

Example

```
Switch:1#show ip spb-pim-gw interface gigabitethernet 1/2

=====
Port Ip Spb-pim-gw
=====
PORT-NUM  OPSTATE    ADMINSTATE  HELLOINT  JPINT
=====
1/2       Disabled    Enabled     30        60
=====
```

Variable definitions

Use the data in the following table to use the `show ip spb-pim-gw interface gigabit` command.

Variable	Value
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
vrf WORD<0-16>	Displays SPB-PIM Gateway interface information for a specific VRF.
vrfids WORD<0-512>	Displays SPB-PIM Gateway interface information for a range of VRF IDs. * Note: Enter a single VRF ID or multiple VRF IDs separated by ',' or enter a range of VRF IDs 'x-y'.

Displaying the SPB-PIM Gateway VLAN information

Use the following procedure to display the SPB-PIM Gateway VLAN interface information.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the SPB-PIM Gateway VLAN interface information:

```
show ip spb-pim-gw interface [vlan]
```

Example

```
Switch:1>show ip spb-pim-gw interface
=====
                               Spb-pim-gw Interface - GlobalRouter
=====
IF          ADDR          MASK          JPINT        HELLOINT     OPSTATE      ADMINSTATE
Vlan50     50.1.1.1      255.255.255.0 60           30           Disabled     Enabled
Vlan123    123.1.1.1    255.255.255.0 60           30           Disabled     Disabled
Vlan142    142.1.1.1    255.255.255.0 60           30           Enabled      Enabled
Vlan400    100.1.1.2    255.255.255.0 60           30           Disabled     Disabled

Total spb-pim-gw Interfaces Displayed 4/4
```

Variable definitions

Use the data in the following table to use the `show ip spb-pim-gw interface` command.

Variable	Value
vlan-id	The VLAN ID of an interface to display.

Displaying the SPB-PIM Gateway neighbor information

Use the following procedure to display the SPB-PIM Gateway interfaces neighbor information.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the SPB-PIM Gateway neighbor information:

```
show ip spb-pim-gw neighbor [vrf WORD<0-16>] [vrfids WORD<0-512>]
```


Example

```
Switch:1>show ip spb-pim-gw neighbor
=====
                               Spb-pim-gw Neighbor - GlobalRouter
=====
INTERFACE ADDRESS          UPTIME          EXPIRE
Vlan26     26.1.1.10      0 day(s), 00:11:36 0 day(s), 00:01:28

Total SPB-PIM-GW Neighbors Displayed = 1/1
=====
```

Variable definitions

Use the data in the following table to use the `show ip spb-pim-gw neighbor` command.

Variable	Value
vrf <i>WORD</i> <0-16>	Displays the SPB-PIM Gateway interface neighbor information for a specific VRF name.
vrfids <i>WORD</i> <0-512>	Displays the SPB-PIM Gateway interface neighbor information for a range of VRF IDs.  Note: Enter a single VRF ID or multiple VRF IDs separated by ',' or enter a range of VRF IDs 'x-y'.

Displaying the SPB-PIM Gateway multicast routes

Use the following procedure to display the SPB-PIM Gateway multicast routes. This procedure displays upstream (toward the foreign source) information and downstream (receiver) information on the SPB-PIM Gateway interfaces. This command does not display the following information:

- Upstream information for streams ingressing on spb-multicast interfaces
- Upstream information for streams ingressing from a remote SPB node
- Receivers in spb-multicast interfaces

Use the `show isis spbm ip-multicast-route` command to display information on all multicast streams and the multicast streams ingress interfaces and egress interfaces.

Use the `show ip spb-pim-gw mroute` command to display information only on SPB-PIM Gateway interfaces.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the SPB-PIM Gateway multicast routes:

```
show ip spb-pim-rw mroute [source {A.B.C.D}] [group {A.B.C.D}] [vrf
WORD<1-16>] [vrfids WORD<0-512>]
```

Example

Note:

The `show ip spb-pim-gw mroute` command displays active upstream information and active downstream information per (*,g) and (s,g) per port, which includes *G Join or Prune pending state, SG join or prune pending state, and SG Rpt PRUNE or PRUNE pending state.. There can be upstream information for a specific SG and no downstream, and vice-versa, as the information in the command `show ip spb-pim-gw mroute` reflects only information known on the SPB-PIM Gateway interfaces. For example, there might be downstream receivers on a SPB-PIM Gateway Interface for a particular stream which is ingressing on an spb-multicast interface; thus, the upstream information will not be displayed using this command.

```
Switch:1>show ip spb-pim-gw mroute
```

```
=====
Spb-pim-gw Active PIM Multicast Route - GlobalRouter
```

SPB-PIM Gateway interface configuration

```

=====
Src: 0.0.0.0      Grp: 225.1.1.1
Flags: WC
Joined Ports:
Vlan    Ports          Join Timer
----    -
Vlan30  1/3                155
-----

Src: 123.1.1.101  Grp: 225.1.1.1  Upstream: 50.1.1.1  Incoming Port: Vlan50-1/5
Flags: SG
SG Joined Ports:
Vlan    Ports          Join Timer
----    -
Vlan30  1/3                184

SG Prune Pending Ports:
Vlan    Ports          Prune Pending Timer
----    -
Vlan40  1/4                180

SG Rpt Pruned Ports:
Vlan    Ports          RPT Prune Timer
----    -
Vlan90  1/9                156


SG Rpt Prune Pending Ports:
Vlan    Ports          RPT Prune Pending Timer
----    -
Vlan60  1/6                164
-----

Total Num of Entries Displayed 2/2
Flags Legend:
WC=(*,Grp) entry, SG=(Src,Grp) entry

```

Variable definitions

Use the data in the following table to use the `show ip spb-pim-gw mroute` command.

Variable	Value
vrf <i>WORD</i> <0-16>	Displays the SPB-PIM Gateway mroute information for a specific VRF name.
vrfids <i>WORD</i> <0-512>	Displays the SPB-PIM Gateway interface mroute information for a range of VRF IDs.  Note: Enter a single VRF ID or multiple VRF IDs separated by ',' or enter a range of VRF IDs 'x-y'.
group { <i>A.B.C.D</i> }	Displays mroute information specific to a group IP address.
source { <i>A.B.C.D</i> }	Displays mroute information specific to a source IP address.

Displaying the IP mroute routes

Use the following procedure to display multicast routes ingressing on either SPB-PIM Gateway interfaces or SPB multicast interfaces.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the multicast routes:

```
show ip mroute mroute
```

Example

* Note:

The UPSTREAM_NBR field is populated only if the stream was learned across a spb-pim-gw interface, and the upstream neighbor is the PIM neighbor IP address toward the source. The PROT field equals spb-pim-gw when the stream's source is learned on a VLAN configured for protocol spb-pim-gw. If the stream's source is learned on a VLAN configured for spb-multicast, the PROT field equals spb.

```
Switch:1>show ip mroute route
```

```
=====
Mroute Route - GlobalRouter
=====
GROUP      SOURCE      SRCMASK      UPSTREAM_NBR      IF      EXPIR      PROT
-----
225.1.1.1   123.1.1.101  255.255.255.255 123.1.1.4      Vlan123   173      spb-pim-gw
1 out of 1 total mroute entries displayed
```

Variable definitions

Use the data in the following table to use the `show ip mroute route` command.

Variable	Value
vrf <i>WORD</i> <0-16>	Displays the multicast mroute information for a specific VRF name.
vrfids <i>WORD</i> <0-512>	Displays the multicast mroute information for a range of VRF IDs. * Note: Enter a single VRF ID or multiple VRF IDs separated by ',' or enter a range of VRF IDs 'x-y'.

SPB-PIM Gateway interface configuration using EDM

Enabling SPB-PIM Gateway on a VLAN

Enable SPB-PIM Gateway on a VLAN interface.

Procedure

1. In the navigation pane, expand the **Configuration > VLAN** folders.
2. Click **VLANs**.
3. Click the **Advanced** tab.
4. In the row for the VLANs, double click the **SpbPimGatewayMulticast** field, and then select enable from the drop down menu.
5. Click **Apply**.

Enabling SPB-PIM Gateway on a Brouter port interface

Enable SPB-PIM Gateway on a Brouter port.

Procedure

1. In the Device Physical View tab, select the port you need to configure.
2. In the navigation pane, expand the **Configuration > Edit > Port** folders.
3. Click **IP**.
4. Click the **SPB-PIM-GW** tab.
5. Select the **Enable** check box to enable SPB-PIM Gateway on a Brouter port interface.
6. Click **Apply**.

SPB-PIM-GW field descriptions

Use the data in the following table to use the SPB-PIM-GW tab.

Name	Description
OperState	Displays the current operational state of this SPB-PIM Gateway interface.
Address	Displays the primary IP address of this router on this SPB-PIM Gateway interface.
AddressMask	Displays the primary IP address mask of this router on this SPB-PIM Gateway interface.
HelloInterval	Configures the PIM HELLO transmission interval.

Table continues...

Name	Description
JoinPruneInterval	Configures the PIM JOIN PRUNE transmission interval.

Configuring SPB-PIM Gateway VLAN optional parameters

Configure the SPB-PIM Gateway interface parameters on a VLAN.

Procedure

1. In the navigation pane, expand the **Configuration > VLAN** folders.
2. Click **VLANs**.
3. Select a row from the VLAN and click the **IP** tab.
4. Click the **SPB-PIM-GW** tab.
5. In the **HelloInterval** field, type the hello transmission interval.
6. In the **JoinPruneInterval** field, type the join prune transmission interval.
7. Click **Apply**.

SPB-PIM-GW field descriptions

Use the data in the following table to use the SPB-PIM-GW tab.

Name	Description
OperState	Displays the current operational state of this SPB-PIM Gateway interface.
Address	Displays the primary IP address of this router on this SPB-PIM Gateway interface.
AddressMask	Displays the primary IP address mask of this router on this SPB-PIM Gateway interface.
HelloInterval	Configures the PIM HELLO transmission interval. This SPB-PIM Gateway VLAN level interval setting overrides the inherited global SPB-PIM Gateway HELLO interval setting. Setting the HELLO Interval to 0 causes the neighbors to never expire its neighborhood with this local SPB-PIM Gateway interface.
JoinPruneInterval	Configures the PIM JOIN PRUNE transmission interval. This SPB-PIM Gateway VLAN level interval setting overrides the inherited global level JOIN PRUNE transmission interval setting.

Configuring the SPB-PIM Gateway Brouter port optional parameters

Configure the SPB-PIM Gateway interface parameters on a brouter port.

Procedure

1. In the Device Physical View tab, select the port you need to configure.
2. In the navigation pane, expand the **Configuration > IP** folders.
3. Click **SPB-PIM-GW**.
4. Click the **Interfaces** tab.
5. In the row for the interfaces, double-click the **HelloInterval** box, and then type the hello interval in seconds.
6. In the row for the interfaces, double-click the **JoinPruneInterval** box, and then type the join prune interval in seconds.

SPB-PIM-GW field descriptions

Use the data in the following table to use the SPB-PIM-GW tab.

Name	Description
OperState	Displays the current operational state of this SPB-PIM Gateway interface.
Address	Displays the primary IP address of this router on this SPB-PIM Gateway interface.
AddressMask	Displays the primary IP address mask of this router on this SPB-PIM Gateway interface.
HelloInterval	Configures the PIM HELLO transmission interval.
JoinPruneInterval	Configures the PIM JOIN PRUNE transmission interval.

Displaying the SPB-PIM Gateway interface default values

Use the following procedure to display the default values used for the SPB-PIM Gateway interface HELLO and JOIN PRUNE intervals unless specifically configured on the individual interface.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **SPB-PIM-GW**.
3. Click the **Globals** tab.

Globals field descriptions

Use the data in the following table to use the Globals tab.

Name	Description
HelloInterval	Displays the PIM HELLO transmission interval.
JoinPruneInterval	Displays the PIM JOIN PRUNE transmission interval.

Displaying the SPB-PIM Gateway router port information

Use the following procedure to display the SPB-PIM Gateway interface information.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **SPB-PIM-GW**.
3. Click the **Interfaces** tab.

Interfaces field descriptions

Use the data in the following table to use the Interfaces tab.

Name	Description
IfIndex	Displays the VLAN ID.
OperState	Displays the current operational state of this SPB-PIM Gateway interface.
AddressType	Displays the address type of this SPB-PIM Gateway interface.
Address	Displays the primary IP address of this router on this SPB-PIM Gateway interface.
AddressMask	Displays the primary IP address mask of this router on this SPB-PIM Gateway interface.
HelloInterval	Configures the PIM HELLO transmission interval. This SPB-PIM Gateway VLAN level interval setting overrides the inherited global SPB-PIM Gateway HELLO interval setting. Setting the HELLO Interval to 0 causes the neighbors to never expire its neighborship with this local SPB-PIM Gateway interface.
JoinPruneInterval	Configures the PIM JOIN PRUNE transmission interval. This SPB-PIM Gateway VLAN level interval setting overrides the inherited global level JOIN PRUNE transmission interval setting.

Displaying the SPB-PIM Gateway VLAN information

Use the following procedure to display the SPB-PIM Gateway VLAN information.

Procedure

1. In the navigation pane, expand the **Configuration > VLAN** folders.
2. Click **VLANs**.
3. Select a row from the VLAN and click the **IP** tab.
4. Click the **SPB-PIM-GW** tab.

SPB-PIM-GW field descriptions

Use the data in the following table to use the SPB-PIM-GW tab.

Name	Description
OperState	Displays the current operational state of this SPB-PIM Gateway interface.
Address	Displays the primary IP address of this router on this SPB-PIM Gateway interface.
AddressMask	Displays the primary IP address mask of this router on this SPB-PIM Gateway interface.
HelloInterval	Configures the PIM HELLO transmission interval. This SPB-PIM Gateway VLAN level interval setting overrides the inherited global SPB-PIM Gateway HELLO interval setting. Setting the HELLO Interval to 0 causes the neighbors to never expire its neighborship with this local SPB-PIM Gateway interface.
JoinPruneInterval	Configures the PIM JOIN PRUNE transmission interval. This SPB-PIM Gateway VLAN level interval setting overrides the inherited global level JOIN PRUNE transmission interval setting.

Displaying the SPB-PIM Gateway neighbor information

About this task

Use the following procedure to display the SPB-PIM Gateway neighbor information

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **SPB-PIM-GW**.
3. Click the **Neighbors** tab.

Neighbors field descriptions

Use the data in the following table to use the Neighbors tab.

Name	Description
IfIndex	Specifies the IfIndex for the interface which is used to reach this SPB-PIM Gateway neighbor.
AddressType	Specifies the address type of this SPB-PIM Gateway neighbor.
Address	Specifies the primary IP address of this router on this SPB-PIM Gateway neighbor.
UpTime	Specifies the time since this SPB-PIM Gateway neighbor last became a neighbor of the local router.
ExpiryTime	Specifies the minimum time remaining before this SPB-PIM Gateway neighbor times out.

Displaying the IP mroute routes

Use the following procedure to display multicast routes ingressing on either SPB-PIM Gateway interfaces or SPB multicast interfaces.

Procedure

1. In the navigation pane, expand the **Configuration > IP** folders.
2. Click **Multicast**.
3. Click the **Routes** tab.

Routes field descriptions

Use the data in the following table to use the **Routes** tab.

Name	Description
Group	Displays the IP multicast group address for this entry that contains multicast routing information.
Source	Displays the network address that, when combined with the corresponding route SourceMask value, identifies the source that contains multicast routing information.
SourceMask	Displays the network mask that, when combined with the corresponding route Source value, identifies the multicast source.
UpstreamNeighbor	Shows the address of the upstream neighbor from which the IP datagrams from these sources are received. The address is 0.0.0.0 if the network is local.

Table continues...

Name	Description
Interface	Displays the interface, slot and portnumber, or VLAN ID where IP datagrams sent by these multicast sources to this multicast address are received.
ExpiryTime	Displays the amount of time that remains before this entry ages out. The value 0 indicates that the entry is not subject to aging.
Protocol	Displays the protocol as one of the following: <ul style="list-style-type: none"> • other(1): none of the following • local(2): manually configured • netmgmt(3): configured by a network management protocol • pimSparseMode(8): PIM-SMv2 • igmpOnly(10) • pimSsmMode(11) • spb (12) • spbpimgw(13)

Chapter 7: SPB-PIM Gateway deployment scenarios

SPB-PIM Gateway base case deployment scenario

There are several different customer topology scenarios for the SPB-PIM Gateway (SPB-PIM GW) feature deployment. The customer topology scenarios are described in this chapter. One of these scenarios, shown in [Figure 5](#) on page 130, is fully described here, along with configuration details, and display information.

The deployment scenario described here has two domains:

- SPB domain
- PIM domain

The PIM network has 5 PIM routers:

- RP
- PIM-A1
- PIM-A2
- PIM-B
- PIM-C

The RP router is the PIM-SM rendezvous point. PIM router PIM-B has receiver host R2 attached to it and source S1 is connected to PIM router PIM-C.

The SPB domain has the following components:

- SPB-PIM Gateway Controller node
- Two Gateway nodes, BEB-A1 and BEB-A2
- BEB-A1 is connected to the PIM network through a SPB-PIM Gateway interface to the PIM router PIM-A1
- BEB-A2 is connected to the PIM network through a SPB-PIM Gateway interface to the PIM router PIM-A2

 **Note:**

PIM-A1 and PIM-A2 routers attached to the BEBs SPB-PIM Gateway interface have standard PIM configured on their side of the interface.

- The SPB cloud has a BEB-B to which the source S2 is connected

- The SPB cloud has a BEB-C to which a receiver R1 is connected

*** Note:**

You can place the controller anywhere in the SPB cloud. The controller can be in the boundary or the core. Anywhere there is a connection into the PIM network from the SPB network, there must be a Gateway node(s) and Gateway interface(s).

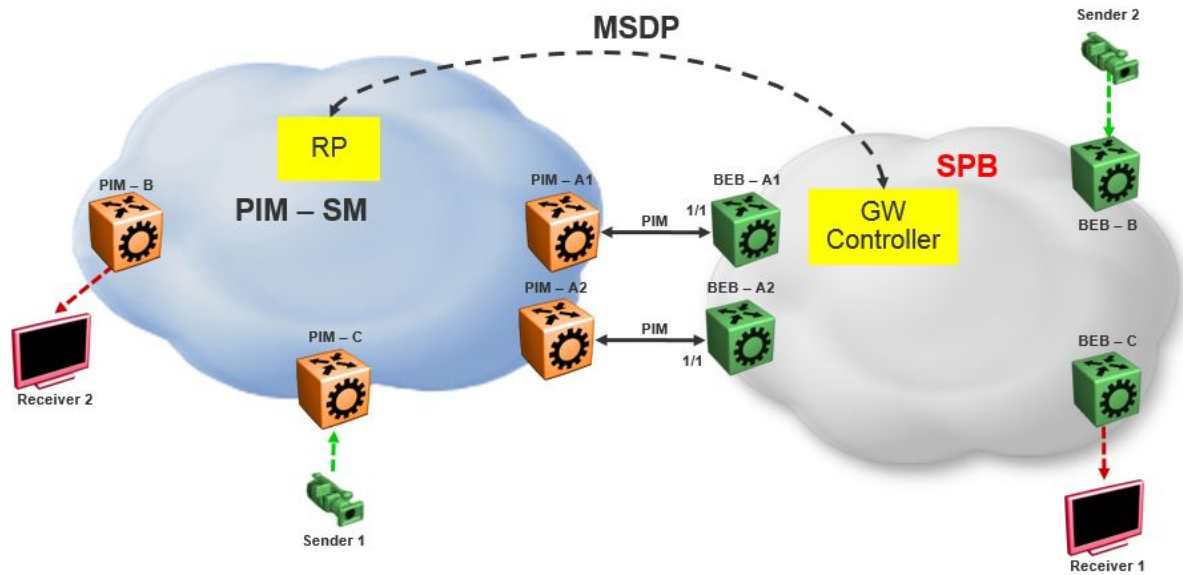


Figure 5: SPB-PIM Gateway base case configuration

The SPB-PIM Gateway nodes BEB-A1 and BEB-A2 from the SPB cloud are connected to the PIM network. The connection is established by SPB-PIM Gateway interface connections to PIM routers PIM-A1 and PIM-A2. A MSDP connection is established between the RP from the PIM domain and the SPB-PIM Gateway Controller from the SPB domain. A MSDP connection is established to exchange the multicast source information between the RP and the SPB Controller. Unicast routing or reachability is setup before establishing the MSDP connection between the RP and the Gateway controller. The Unicast setup is not shown in the above figure.

SPB-PIM Gateway base case configuration example

Before you begin

- The Shortest Path Bridging (SPB) infrastructure must be configured and setup in the SPB domain (not shown in this example)
- Protocol Independent Multicast (PIM) infrastructure must be configured and setup in the PIM domain (not shown in this example)

- Unicast routing table must be setup in the PIM domain to ensure reachability of the Multicast Source Discovery Protocol (MSDP) peer and source S2 from the SPB network
- Unicast routing table must be setup in the SPB domain to ensure reachability of the MSDP peer and source S1 from the PIM network

Example

Node: Gateway controller

Configure ISIS and SPBM:

```
Switch:1#configure terminal
Switch:1(config)#spbm
Switch:1(config)#router isis
Switch:1(config-isis)#system-id 0026.0026.0026
Switch:1(config-isis)#manual-area 01.0202.0303.04
Switch:1(config-isis)#spbm 1
Switch:1(config-isis)#spbm 1 nick-name 0.00.26
Switch:1(config-isis)#spbm 1 b-vid 10,20 primary 10
Switch:1(config-isis)#vlan create 10 name bvlan1 type spbm-bvlan
Switch:1(config)#vlan create 20 name bvlan2 type spbm-bvlan
Switch:1(config)#router isis enable
```

NNI Configuration:

```
Switch:1(config)#interface gigabitEthernet 1/1
Switch:1(config-if)#isis
Switch:1(config-if)#isis spbm 1
Switch:1(config-if)#isis enable
Switch:1(config-if)#no shutdown
```

- Enable IPSC to setup Unicast route table. This setup ensures reachability of Rendezvous Point (RP) in the PIM network
- Create a loopback interface 2.0.2.2 to enable IPSC and MSDP originator-id
- Enable Multicast over Fabric Connect
- Configure static route and direct route redistribution
- Apply the static route and direct route redistribution

* Note:

Static route is used to reach RP for the below sample configuration.

```
Switch:1(config)#interface loopback 1
Switch:1(config-if)#ip address 2.0.2.2/32
Switch:1(config)#router isis
Switch:1(config-isis)#ip-source-address 2.0.2.2
Switch:1(config-isis)#spbm 1 ip enable
Switch:1(config-isis)#spbm 1 multicast enable
Switch:1(config-isis)#
Switch:1(config-isis)#redistribute static
Switch:1(config-isis)#redistribute static enable
Switch:1(config-isis)#redistribute direct
Switch:1(config-isis)#redistribute direct enable
Switch:1(config-isis)#
Switch:1(config-isis)#end
Switch:1#isis apply redistribute static
Switch:1#isis apply redistribute direct
```

MSDP Configuration:

Create an instance for the MSDP session. This IP interface is used for establishing an MSDP session with an RP in the PIM network. The source IP address used for the MSDP session must not

be the newly created IP interface. The originator-id specifically configured for MSDP is used as the source IP address to establish the MSDP session. The originator-id is also used by the RP in the source active (SA) messages sent to the MSDP peers. The CLIP configured earlier is used as the originator-id.

```
Switch:1#configure terminal
Switch:1(config)#vlan create 2100 type port-mstprstp 1
Switch:1(config)#vlan members add 2100 1/3 portmember
Switch:1(config)#interface vlan 2100
Switch:1(config-if)#ip address 21.0.0.1/24
Switch:1(config-if)#exit

Switch:1(config)#ip msdp originator-id 2.0.2.2
Switch:1(config)#ip msdp enable
Switch:1(config)#ip msdp peer 21.0.0.2
Switch:1(config)#ip msdp peer 21.0.0.2 enable
```

SPB-PIM Gateway Controller configuration:

Enable SPB-PIM Gateway Controller

```
Switch:1(config)#router isis
Switch:1(config-isis)#spbm 1 multicast spb-pim-gw controller enable
```

Node: BEB-A1 (SPB-PIM Gateway)

Configure ISIS and SPBM:

```
Switch:1#configure terminal
Switch:1(config)#spbm
Switch:1(config)#
Switch:1(config)#router isis
Switch:1(config-isis)#system-id 0015.0015.0015
Switch:1(config-isis)#manual-area 01.0202.0303.04
Switch:1(config-isis)#spbm 1
Switch:1(config-isis)#spbm 1 nick-name 0.00.15
Switch:1(config-isis)#spbm 1 b-vid 10,20 primary 10
Switch:1(config-isis)#
Switch:1(config-isis)#vlan create 10 name bvlan1 type spbm-bvlan
Switch:1(config)#vlan create 20 name bvlan2 type spbm-bvlan
Switch:1(config)#router isis enable
```

NNI Configuration:

```
Switch:1(config)#interface gigabitEthernet 1/1
Switch:1(config-if)#isis
Switch:1(config-if)#isis spbm 1
Switch:1(config-if)#isis enable
Switch:1(config-if)#no shutdown
```

- Enable IP Shortcuts (IPSC) to setup Unicast route table. This setup ensures reachability of sources in the PIM network
- Create a loopback interface 1.0.1.1 to enable IPSC
- Enable Multicast over Fabric Connect
- Configure static route and direct route redistribution
- Apply the static route and direct route redistribution

*** Note:**

Static route is used to reach sources in the PIM network for the below sample configuration.

```
Switch:1(config)#interface loopback 1
Switch:1(config-if)#ip address 1.0.1.1/32
Switch:1(config-if)#router isis
Switch:1(config-isis)#ip-source-address 1.0.1.1
Switch:1(config-isis)#spbm 1 ip enable
Switch:1(config-isis)#spbm 1 multicast enable
Switch:1(config-isis)#
Switch:1(config-if)#router isis
Switch:1(config-isis)#redistribute static
Switch:1(config-isis)#redistribute static enable
Switch:1(config-isis)#redistribute direct
Switch:1(config-isis)#redistribute direct enable
Switch:1(config-isis)#
Switch:1(config-isis)#end
Switch:1#isis apply redistribute static
Switch:1#isis apply redistribute direct
```

SPB-PIM Gateway interface configuration:

- Create an IP interface
- Enable SPB-PIM Gateway on the IP interface

*** Note:**

For the sample configuration below, the SPB-PIM Gateway interface is on VLAN 2000 with IP address 20.0.0.1

```
Switch:1#configure terminal
Switch:1(config)#vlan create 2000 type port-mstprstp 1
Switch:1(config)#vlan members add 2000 1/1 portmember
Switch:1(config)#interface vlan 2000
Switch:1(config-if)#ip address 20.0.0.1/24
Switch:1(config-if)#ip spb-pim-gw enable
```

Enable SPB-PIM Gateway node functionality:

```
Switch:1(config-if)#router isis
Switch:1(config-isis)#spbm 1 multicast spb-pim-gw gateway enable
```

Similar configuration is done for the SPB-PIM Gateway node BEB-A2.

PIM Sparse Mode (PIM-SM) is enabled at the PIM routers PIM-A1 and PIM-A2 on the interfaces connecting SPB-PIM Gateway nodes BEB-A1 and BEB-A2. The SPB-PIM Gateway nodes BEB-A1 and BEB-A2 see the PIM routers PIM-A1 and PIM-A2 as PIM neighbors. The PIM routers PIM-A1 and PIM-A2 see the SPB-PIM Gateway nodes as PIM neighbors. The SPB-PIM Gateway nodes BEB-A1 and BEB-A2 have IP reachability to the PIM source S1 with PIM neighbors as the next hop.

The route to reach source S1 is distributed to the Gateway controller through IPSC. The Gateway controller uses this route information to select only one of the Gateways to which the source S1 will be assigned for a specific group. The Gateway node is the only node that can draw the source S1 stream into the SPB network on behalf of SPB receivers, by sending an SG Join across a Gateway Interface to the nexthop toward the source S1. This ensures that the data is not duplicated from multiple ingress interfaces from the PIM network. Other Gateway nodes that are not assigned as the Gateway to the source S1 will not establish multicast path.

When S1 from the PIM network sends traffic to G1, RP from the PIM network sends MSDP SA message for (S1,G1) to the Gateway Controller. If the Gateway Controller selects BEB-A1 as the Gateway for the foreign source S1 and group G1, the Gateway Controller assigns BEB-A1 to (S1,G1). The Gateway Controller then sends the Gateway assignment information to all the nodes. When BEB-A1 receives the assignment information, it sees that it is assigned as the Gateway to (S1,G1). The BEB-A1 then checks if the next hop to reach S1 is a valid PIM neighbor. If the next hop is a valid PIM neighbor, the BEB-A1 interacts with Multicast over Fabric Connect and advertises a sender TLV for the (S1,G1) into the SPB cloud. The BEB-A2 also receives the Gateway assignment information but silently saves the received Gateway assignment information since it is not the selected Gateway. If the interested receiver R1 is found at BEB-C, as part of Multicast over Fabric Connect processing, BEB-C sends receiver TLV for the group G1 to the advertising node, BEB-A1. Upon receiving this receiver TLV, BEB-A1 establishes the multicast stream through its Gateway interface which is upstream towards the PIM neighbor, by sending out a PIM SG Join message toward the source S1. This causes PIM-A1 node to forward multicast data from S1 to BEB-A1.

When the local source S2 (local to the SPB network) at BEB-B in the SPB network sends traffic to group G1, BEB-B advertises a sender TLV for (S1,G1). The controller sees this sender TLV and sends an MSDP SA message for (S2,G1) to the RP in the PIM network.

*** Note:**

The controller does not send SA messages for (S1,G1) to the PIM network since S1 is a foreign source.

When PIM network receiver R2 is interested in group G1, the PIM router PIM-B sends PIM a (*,G) Join message to the RP. RP in turn sends (S2,G1) Join towards the source S2. The unicast IP reachability to source S2 which is setup in the RP is used for sending (S2,G1) joins hop-by-hop towards the source. From the RP point of view, the next hop to reach the source S2 is one of the PIM routers PIM-A1 or PIM-A2 (depending on the unicast route table next hop address). For this example, the next hop is PIM-A1. The RP sends the (S2,G1) Join message towards the PIM-A1. PIM-A1 then sends an SG Join to BEB-A1. Upon receiving the Join for (S2,G1) from the PIM network, BEB-A1 sends a receiver TLV into the SPB network to the S2 advertising router BEB-B. When the BEB-B receives the receiver TLV, the BEB-B establishes the multicast stream from source S2 toward the receiver.

Source Specific Multicast

PIM-SSM does not use a Rendezvous Point to centralize the receivers and sources. A PIM-SSM router which has a receiver for a group multicast address in the SSM address range joins directly to a source for that group by sending an SG join toward the source, not a *G join toward the RP for the group. Because of this, MSDP is not required in order for the PIM Network to learn of an SSM range stream in the SPB network. However, in order for the SPB network to know where a PIM SSM source resides, it must statically configure S1,SSM-G1 at the controllers. In this way, a Gateway can be chosen for the stream, even in the absence of MSDP.

The following figure shows a non-MSDP SSM environment where stream PIM network source S1, for an SSM group, must be statically configured at the SPB Controllers:

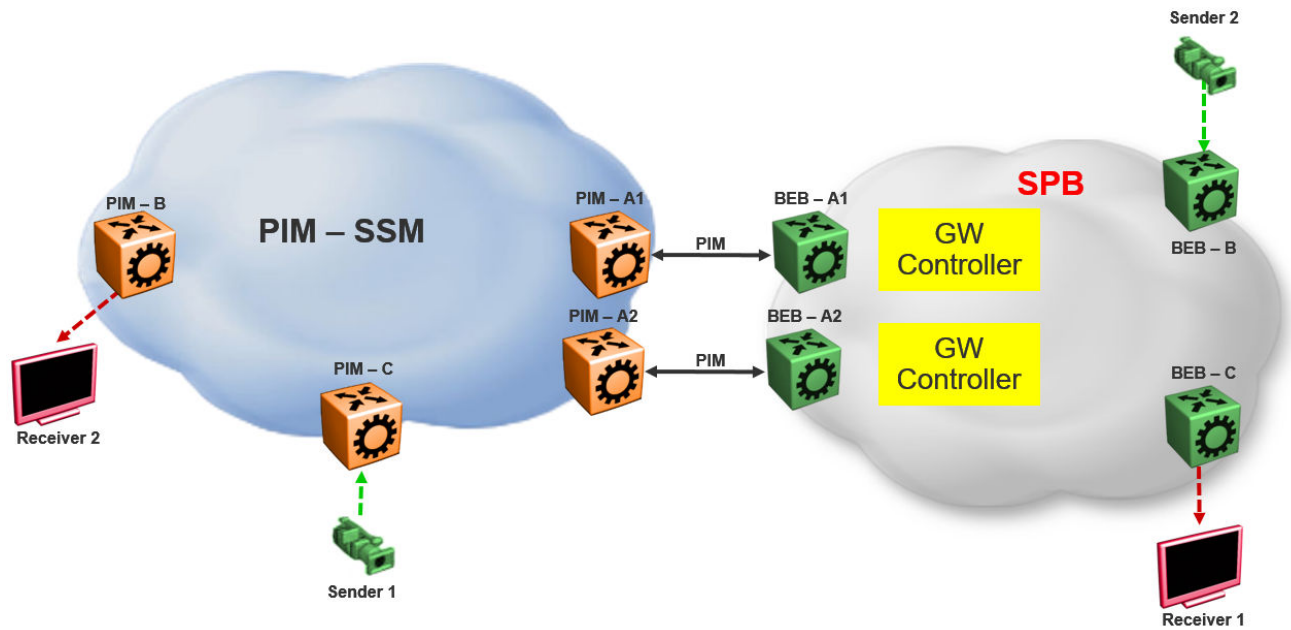


Figure 6: Static configuration of SSM groups in Controllers

Peer Mesh Group

The following figure shows the Peer Mesh Group configuration:

*** Note:**

Controllers within a single SPB network must never peer with each other, regardless of whether mesh groups exist. In addition, both Controllers must have the same peerings configured with other networks RPs.

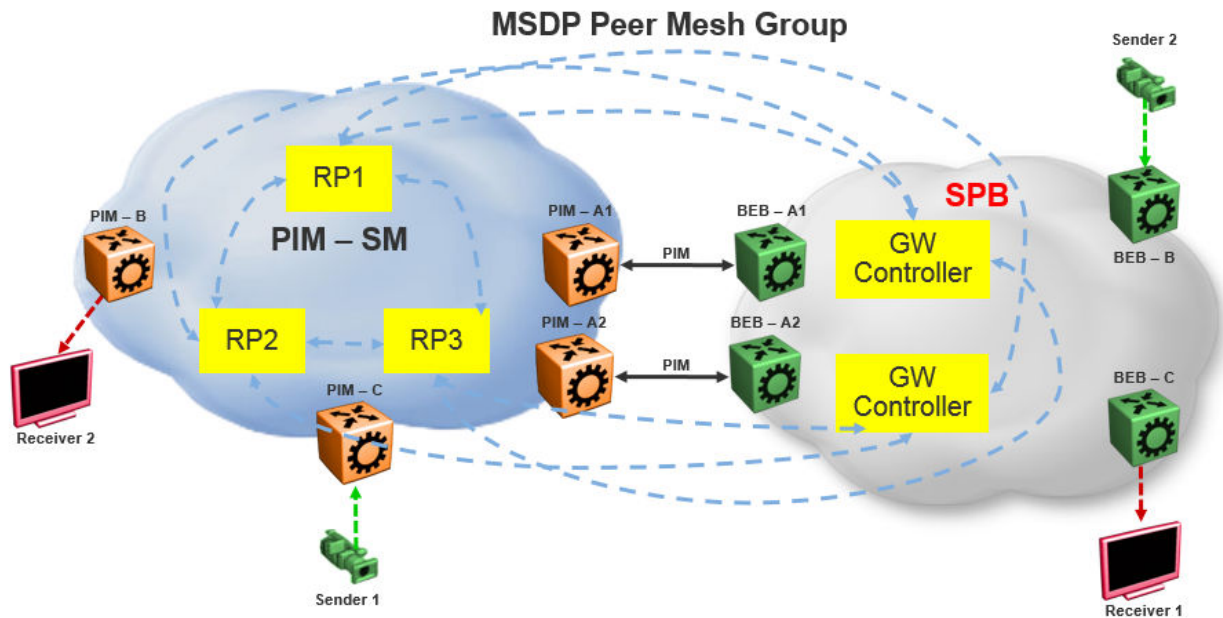


Figure 7: Peer Mesh Group

MSDP Peer Mesh Group configuration example

Example

Configure MSDP:

If the MSDP speakers are fully meshed, the speakers can be configured into a mesh group in order to prevent excessive SA forwarding and RPF checks. To configure a mesh group, specify a name along with the MSDP peer. For example, on router RP1, configure a mesh group which includes RP2, RP3, and both Gateway controllers. On RP2, configure the same mesh group with members RP1, RP3, and both Gateway controllers. On RP3, configure the same mesh group with members RP1, RP2, and both Gateway controllers. On each Gateway controller, configure the same mesh group with members RP1, RP2, and RP3, but never with another Gateway controller in the same SPB domain.

```
Switch:1(config)#ip msdp originator-id 2.0.2.2
Switch:1(config)#ip msdp enable
Switch:1(config)#ip msdp peer 21.0.0.2 enable
Switch:1(config)#ip msdp mesh-group mgTest 21.0.0.2
```


Multi domain

The following figure shows a multi domain scenario, where two PIM domains and one SPB domain share multicast streams:

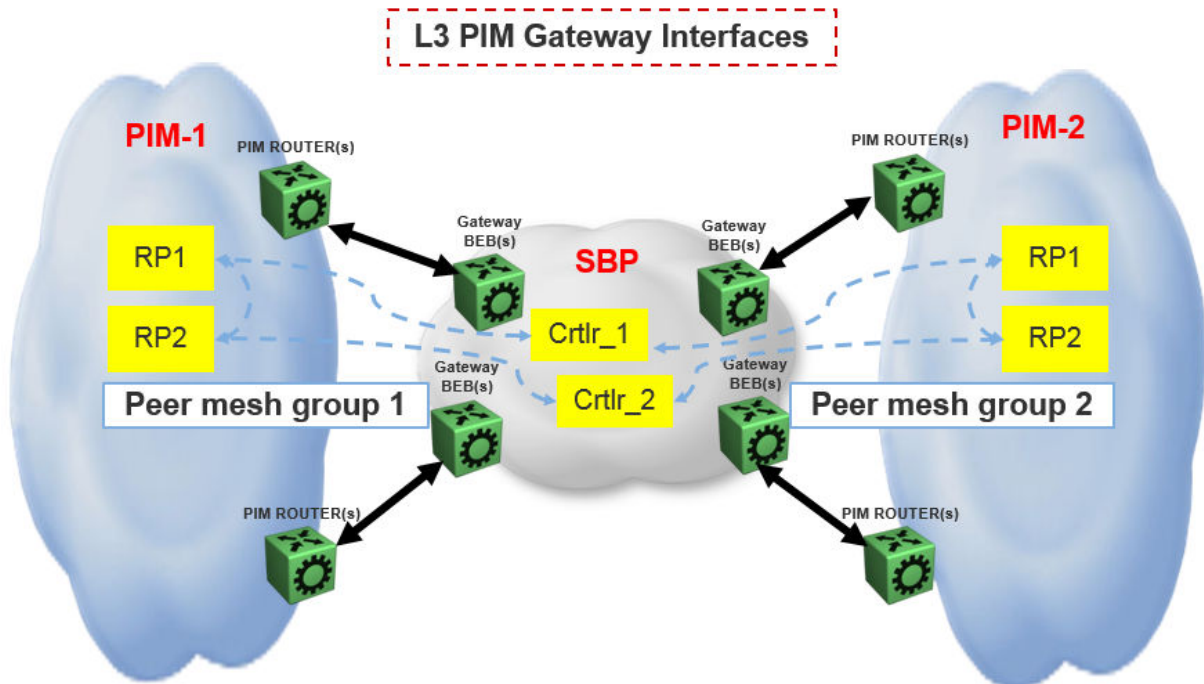


Figure 8: Multi domain configuration

SPB domain interconnect

The following figure shows the SPB domain interconnect configuration. In this scenario, two SPB domains are connected by PIM Gateway interfaces, and there is no traditional PIM Network involved. The Controllers from each SPB domain form MSDP adjacencies with the Controllers in the other domain (but not within the same domain) in order to share their multicast sources. The SPB-PIM Gateway nodes see the other SPB-PIM Gateway nodes as PIM neighbors on the SPB-PIM Gateway interfaces.

SPB-PIM Gateway deployment scenarios

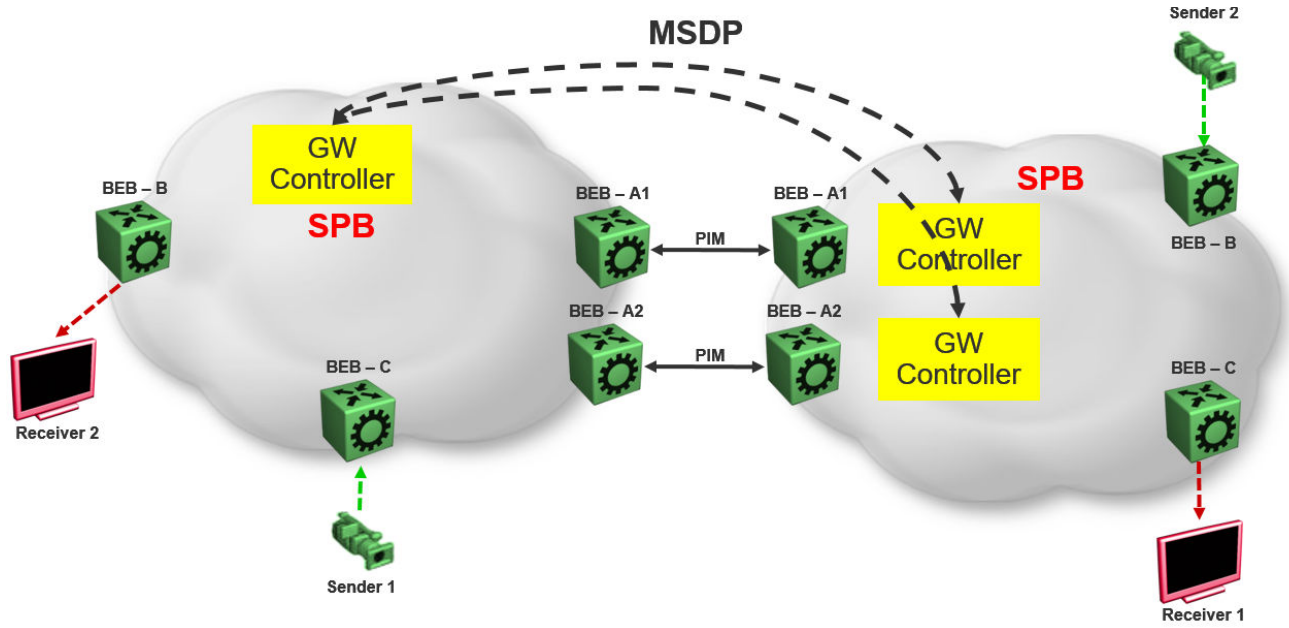


Figure 9: SPB domain interconnect

Glossary

Backbone Core Bridge (BCB)	Backbone Core Bridges (BCBs) form the core of the SPBM network. The BCBs are SPBM nodes that do not terminate the VSN services. BCBs forward encapsulated VSN traffic based on the Backbone MAC Destination Address (B-MAC-DA). A BCB can access information to send that traffic to any Backbone Edge Bridges (BEBs) in the SPBM backbone.
Backbone Edge Bridge (BEB)	Backbone Edge Bridges (BEBs) are SPBM nodes where Virtual Services Networks (VSNs) terminate. BEBs handle the boundary between the core MAC-in-MAC Shortest Path Bridging MAC (SPBM) domain and the edge customer 802.1Q domain. A BEB node performs 802.1ah MAC-in-MAC encapsulation and decapsulation for the Virtual Services Network (VSN).
Backbone MAC (B-MAC)	Provider Backbone Bridging (PBB) MAC-in-MAC encapsulation encapsulates customer MAC addresses in Backbone MAC (B-MAC) addresses. MAC-in-MAC encapsulation defines a BMAC-DA and BMAC-SA to identify the backbone source and destination addresses. The originating node creates a MAC header that SPBM uses for delivery from end to end. As the MAC header stays the same across the network, no need exists to swap a label or perform a route lookup at each node, allowing the frame to follow the most efficient forwarding path end to end. In Shortest Path Bridging MAC (SPBM), each node has a System ID, which is used in the topology announcement. This same System ID also serves as the switch Backbone MAC address (B-MAC), which is used as the source and destination MAC address in the SPBM network.
Customer MAC (C-MAC)	For customer MAC (C-MAC) addresses, which is customer traffic, to forward across the service provider back, SPBM uses IEEE 802.1ah Provider Backbone Bridging MAC-in-MAC encapsulation. The system encapsulates C-MAC addresses within a backbone MAC (B-MAC) address pair made up of a BMAC destination address (BMAC-DA) and a BMAC source address (BMAC-SA).
Customer VLAN (C-VLAN)	A traditional VLAN with MAC learning and flooding, where user devices connect to the network. In SPBM, C-VLANs are mapped to a Service Instance Identifier (I-SID) at the Backbone Edge Bridges (BEBs).
Fabric Connect	Fabric Connect is a single network-wide protocol that enables virtualized network segmentation across the network infrastructure.

Global Routing Table (GRT)	The Global Routing Table (GRT) is a table that maintains the information needed to forward an IP packet along the best route.
Layer 2 Virtual Services Network	The Layer 2 Virtual Services Network (L2 VSN) feature provides IP connectivity over SPBM for VLANs. Backbone Edge Bridges (BEBs) handle Layer 2 virtualization. At the BEBs you map the end-user VLAN to a Service Instance Identifier (I-SID). BEBs that have the same I-SID configured can participate in the same Layer 2 Virtual Services Network (VSN).
Layer 3 Virtual Services Network	The Layer 3 Virtual Services Network (L3 VSN) feature provides IP connectivity over SPBM for VRFs. Backbone Edge Bridges (BEBs) handle Layer 3 virtualized. At the BEBs through local provisioning, you map the end-user IP enabled VLAN or VLANs to a Virtualized Routing and Forwarding (VRF) instance. Then you map the VRF to a Service Instance Identifier (I-SID). VRFs that have the same I-SID configured can participate in the same Layer 3 Virtual Service Network (VSN).
Protocol Independent Multicast, Source Specific (PIM-SSM)	PIM-SSM is a multicast routing protocol for IP networks. PIM-SSM uses only shortest-path trees to provide multicast services based on subscription to a particular (source, group) channel. PIM-SSM eliminates the need for starting with a shared tree by immediately joining a source through the shortest path tree. This method enables PIM-SSM to avoid using a rendezvous point (RP) and RP-based shared tree, which can be a potential bottleneck.
Protocol Independent Multicast, Sparse Mode (PIM-SM)	PIM-SM is a multicast routing protocol for IP networks. PIM-SM provides multicast routing for multicast groups that can span wide-area and inter-domain networks, where receivers are not densely populated. PIM-SM sends multicast traffic only to those routers that belong to a specific multicast group and that choose to receive the traffic. PIM-SM adds a Rendezvous Point router to avoid multicast-data flooding. Use PIM-SM when receivers for multicast data are sparsely distributed throughout the network.
rendezvous point (RP)	The root of the shared tree. One RP exists for each multicast group. The RP gathers information about available multicast services through the reception of control messages and the distribution of multicast group information. Protocol Independent Multicast (PIM) uses RPs.
Shortest Path Bridging (SPB)	Shortest Path Bridging is a control Link State Protocol that provides a loop-free Ethernet topology. There are two versions of Shortest Path Bridge: Shortest Path Bridging VLAN and Shortest Path Bridging MAC. Shortest Path Bridging VLAN uses the Q-in-Q frame format and encapsulates the source bridge ID into the VLAN header. Shortest Path Bridging MAC uses the 802.1 ah MAC-in-MAC frame format and encapsulates the source bridge identifier into the B-MAC header.

**Shortest Path
Bridging MAC
(SPBM)**

Shortest Path Bridging MAC (SPBM) uses the Intermediate-System-to-Intermediate-System (IS-IS) link-state routing protocol to provide a loop-free Ethernet topology that creates a shortest-path topology from every node to every other node in the network based on node MAC addresses. SPBM uses the 802.1ah MAC-in-MAC frame format and encapsulates the source bridge identifier into the B-MAC header. SPBM eliminates the need for multiple overlay protocols in the core of the network by reducing the core to a single Ethernet-based link-state protocol, which can provide virtualization services, both layer 2 and layer 3, using a pure Ethernet technology base.