



ExtremeSwitching™

Configuring Fabric Multicast Services on VSP Operating System Software

Release 6.1 (VSP 8600)
9035289
February 2018

© 2017-2018, Extreme Networks, 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, Extreme Networks, Inc. assumes no liability for any errors. Extreme Networks, Inc. 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. Extreme Networks 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 Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks' 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

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks 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. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

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

"Hosted Service" means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks 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 Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, 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 EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS, INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS 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 EXTREME NETWORKS, INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE ("EXTREME NETWORKS").

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. 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 Extreme Networks or an Extreme Networks 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 set of Designated Processors that hosts (physically or virtually) 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.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks 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 Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

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 Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks 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 Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks 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, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks 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 Extreme Networks' website at: <http://www.extremenetworks.com/support/policies/software-licensing> or such successor site as designated by Extreme Networks. 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 EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS 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 EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS 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 Extreme Networks 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.

Security Vulnerabilities

Information about Extreme Networks' security support policies can be found in the Global Technical Assistance Center Knowledgebase at <https://gtacknowledge.extremenetworks.com/>.

Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: <http://documentation.extremenetworks.com>, or such successor site as designated by Extreme Networks.

Contact Extreme Networks Support

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

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 Extreme Networks are the registered or unregistered Marks of Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks 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 Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

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

For additional information on Extreme Networks trademarks, please see: <http://www.extremenetworks.com/company/legal/>

Contents

Chapter 1: Preface	7
Purpose.....	7
Training.....	7
Providing Feedback to Us.....	7
Getting Help.....	8
Extreme Networks Documentation.....	9
Subscribing to Service Notifications.....	9
Chapter 2: New in this document	10
Notice about feature support.....	10
Chapter 3: SPBM and IS-IS configuration workflow	11
Chapter 4: IP Multicast over Fabric Connect basic configuration	12
IP Multicast over Fabric Connect fundamentals.....	12
IP Multicast over Fabric Connect.....	12
How IP Multicast over Fabric Connect works.....	13
BEB as IGMP Querier.....	15
Network Load Balancing (NLB)	15
Switch clustering at the edge of the SPBM network.....	16
Considerations when you connect an IP Multicast over Fabric Connect network to a PIM network.....	19
IP Multicast over Fabric Connect restrictions.....	20
IP Multicast over Fabric Connect configuration using the CLI.....	21
Enabling IP Multicast over Fabric Connect globally.....	21
Displaying IP Multicast over Fabric Connect information.....	23
Displaying the IP unicast FIB, multicast FIB, unicast FIB, and unicast tree.....	26
IP Multicast over Fabric Connect configuration using the EDM.....	31
Configuring IP Multicast over Fabric Connect globally.....	31
Displaying IP Multicast over Fabric Connect routes.....	32
Displaying the UNI ports for IP multicast routes.....	33
Displaying the multicast FIB.....	34
IP Multicast over Fabric Connect configuration examples.....	35
IP multicast over Fabric Connect global configuration.....	35
Chapter 5: IP Multicast over Fabric Connect services configuration	37
Layer 2 VSN configuration.....	37
Layer 2 VSN configuration fundamentals.....	37
Layer 2 VSN configuration using the CLI.....	38
Layer 2 VSN configuration using EDM.....	56
Layer 2 VSN configuration examples.....	59
IP Shortcuts configuration.....	60
IP Multicast over Fabric Connect within the GRT.....	60

IP Shortcuts configuration using the CLI.....	62
IP Shortcuts configuration using EDM.....	79
IP shortcuts configuration example.....	82
Layer 3 VSN configuration.....	83
Layer 3 VSN fundamentals.....	83
Layer 3 VSN configuration using the CLI.....	84
Layer 3 VSN configuration using EDM.....	106
Layer 3 VSN configuration example.....	113
Chapter 6: SPB-PIM Gateway configuration.....	115
SPB-PIM Gateway fundamentals.....	115
IP Multicast over Fabric Connect in Protocol Independent Multicast networks.....	115
SPB-PIM Gateway.....	118
SPB-PIM GW components.....	119
MSDP overview.....	124
Multicast Source Discovery Protocol configuration.....	127
Basic MSDP configuration using CLI	127
MSDP peer configuration using CLI	130
MSDP message control using CLI	136
MSDP verification using CLI	139
Basic MSDP configuration using EDM.....	148
MSDP peer configuration using EDM.....	154
MSDP message control using EDM.....	187
MSDP verification using EDM.....	193
Controller configuration.....	198
Controller configuration using CLI	199
Controller configuration using EDM.....	206
Gateway configuration.....	210
Gateway Configuration using CLI.....	211
Gateway Configuration using EDM.....	216
SPB-PIM Gateway interface configuration.....	218
SPB-PIM Gateway interface configuration using CLI.....	218
SPB-PIM Gateway interface configuration using EDM.....	226
SPB-PIM Gateway deployment scenarios.....	232
SPB-PIM Gateway base case deployment scenario.....	232
Source Specific Multicast.....	238
Peer Mesh Group.....	239
Multi domain.....	240
SPB domain interconnect.....	241
Glossary.....	243

Chapter 1: Preface

Purpose

This document provides information on features in VSP Operating System Software (VOSS). VOSS runs on the following product families:

- Extreme Networks Virtual Services Platform 4000 Series
- Extreme Networks Virtual Services Platform 7200 Series
- Extreme Networks Virtual Services Platform 8000 Series (includes VSP 8200 and VSP 8400 Series)
- Extreme Networks Virtual Services Platform 8600

This document provides information and instructions to configure Fabric Multicast services on the switch, such as IP Multicast over Fabric Connect, IP Shortcuts, Layer 2 and Layer 3 Virtual Services Networks (VSN), and SPB-PIM Gateway.

Examples and network illustrations in this document may illustrate only one of the supported platforms. Unless otherwise noted, the concept illustrated applies to all supported platforms.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.extremenetworks.com/education/.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at internalinfodev@extremenetworks.com

Getting Help

Product purchased from Extreme Networks

If you purchased your product from Extreme Networks, use the following support contact information to get help.

If you require assistance, contact Extreme Networks using one of the following methods:

- [GTAC \(Global Technical Assistance Center\) for Immediate Support](#)
 - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- [GTAC Knowledge](#) – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- [The Hub](#) – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- [Support Portal](#) – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Product purchased from Avaya

If you purchased your product from Avaya, use the following support contact information to get help.

Go to the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service

request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for previous versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

Subscribing to Service Notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

About this task

You can modify your product selections at any time.

Procedure

1. In an Internet browser, go to <http://www.extremenetworks.com/support/service-notification-form/>.
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

Chapter 2: New in this document

This document, which was *Configuring SPB-PIM Gateway*, is now renamed to *Configuring Fabric Multicast Services*.

The following sections detail what is new in *Configuring Fabric Multicast Services*.

Migration of content

This document contains content that has been migrated from the reorganized *Configuring Fabric Basics and Layer 2 Services* document.

Notice about feature support

This document includes content for multiple hardware platforms across different software releases. As a result, the content can include features not supported by your hardware in the current software release.

If a documented command, parameter, tab, or field does not appear on your hardware, it is not supported.

For information about feature support, see *Release Notes*.

For information about physical hardware restrictions, see your hardware documentation.

Chapter 3: SPBM and IS-IS configuration workflow

The following section describes the generic work flow to configure SPBM and IS-IS infrastructure and services on your network.

*** Note:**

This section is an overview. For further details on the SPBM and IS-IS infrastructure and configuration, see the documents described in the Documentation sources section below.

1. Infrastructure configuration:

As a first step, you must configure your basic infrastructure for Shortest Path Bridging MAC (SPBM).

2. Services configuration:

After you complete the infrastructure configuration, you configure the appropriate services for your network to run on top of your base architecture. This includes:

- Layer 2 and Layer 3 VSNs
- IP Shortcuts
- Inter-VSN routing

3. Operations and Management:

To debug connectivity issues and isolate network faults in the SPBM network, you can use Connectivity Fault Management (CFM).

Documentation sources:

- For information on basic SPBM infrastructure and IS-IS configuration and Layer 2 services, see *Configuring Fabric Basics and Layer 2 Services*.

This document also contains information on configuring Fabric Extend, which enables your enterprise to extend Fabric Connect technology over Layer 2 or Layer 3 core networks.

- For information on Fabric Layer 3 services configuration, see *Configuring Fabric Layer 3 Services*.
- For information on IP Multicast over Fabric Connect configuration and services, see *Configuring Fabric Multicast Services*. This document also contains information about configuring the SPB-PIM Gateway (SPB-PIM GW), which provides multicast inter-domain communication between an SPB network and a PIM network. The SPB-PIM GW can also connect two independent SPB domains.
- For information on CFM, see *Troubleshooting*.

Chapter 4: IP Multicast over Fabric Connect basic configuration

IP Multicast over Fabric Connect fundamentals

IP Multicast over Fabric Connect

Extreme Networks is leading the industry with a new approach to transporting IP multicast using IP Multicast over Fabric Connect. IP Multicast over Fabric Connect greatly simplifies multicast deployment, with no need for any multicast routing protocols such as Protocol Independent Multicast-Sparse Mode (PIM-SM) or Protocol Independent Multicast-Source Specific Multicast (PIM-SSM). A BEB can forward a multicast stream anywhere in an SPBM network where IS-IS advertises the stream to the rest of the fabric.

The advantage of this solution over traditional approaches is the 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.

You can compare the quick convergence times for IP Multicast over Fabric Connect to Interior Gateway Protocols like Open Shortest Path First (OSPF) combined with PIM-SM or PIM-SSM. OSPF combined with PIM-SM or PIM-SSM can have recovery times that are sub optimal with convergence times that take tens of seconds. PIM experiences longer convergence times, in part, because unicast IP routing protocols must converge before PIM can converge. PIM also maintains the network state for every multicast group and uses a mechanism based on each hop to update the network about state changes, which affects scalability.

IP Multicast over Fabric Connect is extremely scalable because you only apply the multicast bridging and routing functionality at the SPBM fabric edge, with the streams mapped to SPBM multicast trees in the fabric.

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, VX-LAN, Multi-tenant IP multicast.

IP Multicast over Fabric Connect and DvR

You must enable IP multicast over Fabric Connect globally on all DvR enabled nodes (Controllers and Leaf nodes) in a DvR domain.

For more information on DvR, see *Configuring IPv4 Routing*.

How IP Multicast over Fabric Connect works

The BEBs act as the boundary between the multicast domain (currently only IGMP dynamic or static) and the SPBM domain. Multicast senders (sources) and receivers connect directly or indirectly (using Layer 2 switches) to the BEBs. You can enable IP Multicast over Fabric Connect services at the Layer 2 VSN level or the Layer 3 VSN level (including the GRT).

The following figure shows how multicast senders and receivers connect to the SPBM cloud using BEBs.

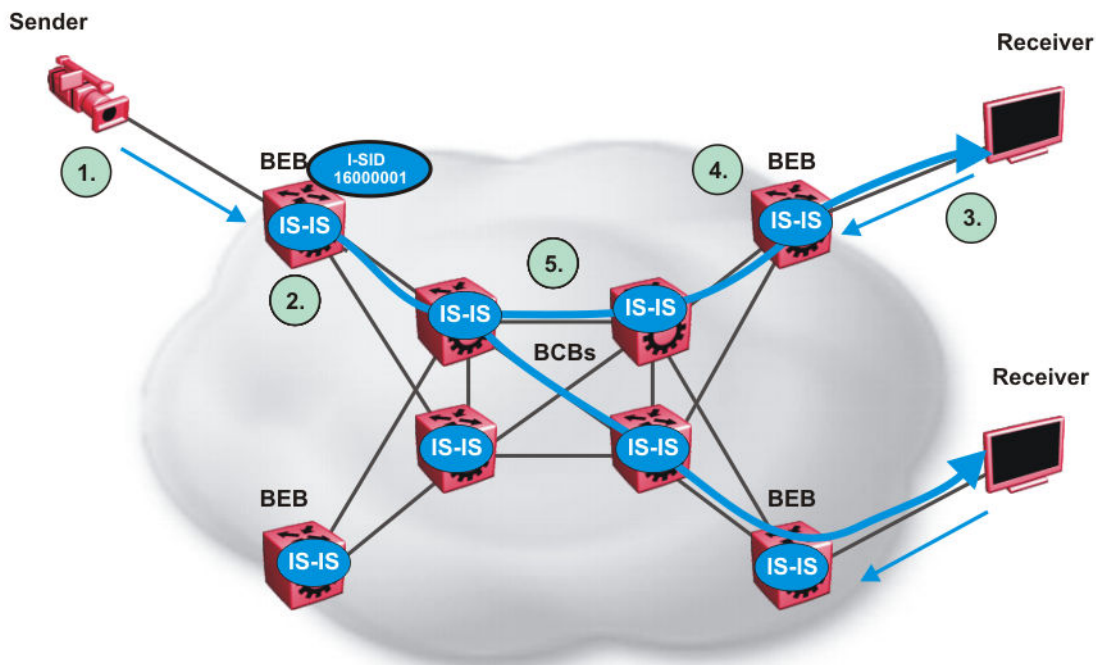


Figure 1: IP Multicast over Fabric Connect streams

The following list describes how multicast senders and receivers connect to the SPBM cloud using BEBs in the preceding diagram:

1. The sender transmits multicast traffic with group IP address 233.252.0.1.
2. After the BEB receives the IP multicast stream from the sender, the BEB allocates data I-SID 16000001 for the S,G multicast stream. The BEB sends an LSP with the TLV 185 (for Layer 2 VSN multicast and Layer 3 VSN multicast) or TLV 186 (for IP Shortcuts multicast) with the transmit bit set. The BEB also sends an IS-IS service identifier and unicast address sub-TLV (where the unicast address has the multicast bit set and the I-SID is the Data I-SID).
3. The receiver sends a join request to Group 233.252.0.1.
4. The BEB (acting as the IGMP Querier) queries the IS-IS database to find all senders for group 233.252.0.1. If the group exists, the BEB sends an LSP with the IS-IS service identifier and unicast address sub-TLV (where the unicast address has the multicast bit set and the nickname is the stream transmitter BEB and the I-SID is the data I-SID).
5. The multicast tree is calculated for the data I-SID and the data starts flowing from the sender.

Scope level

IP Multicast over Fabric Connect constrains all multicast streams within the level in which they originate, which is called the scope level. In other words, if a sender transmits a multicast stream to a BEB on a C-VLAN (a VLAN that is mapped to an I-SID, for instance, a L2 VSN) with IP Multicast over Fabric Connect enabled, only receivers that are part of the same Layer 2 VSN can receive that stream. Similarly, if a sender transmits a multicast stream to a BEB on a VLAN that is part of the GRT or a Layer 3 VSN with IP Multicast over Fabric Connect enabled, only receivers that are part of the same Layer 3 instance (GRT or L3 VSN) can receive that stream.

*** Note:**

In the context of IP Multicast over Fabric Connect, scope is either the Global Routing Table or the I-SID value of the Layer 2 or Layer 3 VSN associated with the local VLAN on which the IP multicast data was received.

Data I-SID

After the BEB receives the IP multicast stream from the sender, a BEB allocates a data Service Identifier (I-SID) in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the S,G, V tuple, which is the source IP address, the group IP address, and the local VLAN the multicast stream is received on.

The BEB propagates this information through the SPBM cloud by using IS-IS TLV updates in LSPs, which results in the creation of a multicast tree for that stream. All BEBs now know what data I-SID to use for that stream and its scope. The data I-SID is a child of the scope or VSN I-SID. If no receiver requests the IP multicast stream, the ingress BEB does not forward the multicast stream.

IGMP

After a BEB receives an IGMP join message from a receiver, a BEB queries the IS-IS database to check if a sender exists for the requested stream within the scope of the receiver. If the requested stream does not exist, the IGMP information is kept, but no further action is taken. If the requested stream exists, the BEB sends an IS-IS TLV update to its neighbors to inform them of the presence of a receiver, and this information is propagated through the SPBM cloud.

IS-IS acts dynamically using the TLV information it receives from BEBs that connect to the sender and the receivers to create a multicast tree between them. IS-IS creates very efficient multicast trees for the data I-SID allocated at the sender edge of the SPBM cloud to transport data between

the sender and the receivers. The data I-SID uses Tx/Rx bits to signify whether the BEB uses the I-SID to transmit, receive, or both transmit and receive data on that I-SID. After IS-IS creates the multicast tree, the sender transports data to the receiver across the SPBM cloud using the data I-SID.

The trigger to send IS-IS updates to announce a multicast stream into the SPBM cloud is the multicast traffic arriving at the BEB. Because the BEB only interacts with IGMP and not PIM, all multicast traffic must be drawn towards the BEB for the stream to be announced, which SPBM accomplishes by making the BEB an IGMP Querier. In a VLAN, the IGMP Querier sends out periodic IGMP queries.

*** Note:**

The BEB must be the only IGMP Querier in the VLAN. If the BEB receives an IGMP query from any other device, it causes unexpected behavior, including traffic loss.

BEB as IGMP Querier

The BEB acts as the IGMP Querier and creates tables for links that need IP multicast streams. IGMP and IGMP Snooping cannot work without an IGMP Querier that sends out periodic IGMP queries.

The BEB only interacts with IGMP messages and not PIM. All multicast traffic must enter the BEB for the data stream to be announced.

The BEB must be the only IGMP Querier in the VLAN. If the BEB receives an IGMP query from any other device, unexpected behavior results, including traffic loss.

The IGMP query message is an IP packet and requires a source IP address. However, Layer 2 IGMP Snooping with SPBM by default turns on the service without the configuration of an IP address on the VLAN. By default, the BEB sends an IGMP query message with an IP source address of 0.0.0.0. If there are interoperability issues with third party vendors as a result of the 0.0.0.0 IP address, then you can configure the querier address under IGMP, without having to configure an IP address for the Layer 2 VSN VLAN.

IGMP Snooping, operating on the Layer 2 VSN, listens to conversations between hosts and routers, and maintains a table for links that need IP multicast streams.

For IGMP Snooping, ensure that the IGMP version used by multicast hosts and other devices in the network is the same as the IGMP version configured on the IGMP Snooping VLAN, or that you enable compatibility mode.

For more conceptual and configuration information on IGMP, see *Configuring IP Multicast Routing Protocols*.

Network Load Balancing (NLB)

SPBM supports Network Load Balancing (NLB) Unicast and Multicast modes.

*** Note:**

This feature is not supported on all hardware platforms. If you do not see this command in the command list or EDM, the feature is not supported on your hardware. For more information about feature support, see *Release Notes*.

NLB is a clustering technology available with Microsoft Windows 2000, Microsoft Windows 2003, Microsoft Windows 2008, and Microsoft Windows 2012 server family of operating systems. You can use NLB to share the workload among multiple clustering servers. NLB uses a distributed algorithm to load balance TCP/IP network traffic across a number of hosts, enhancing the scalability and availability of mission critical, IP based services, such as Web, VPN, streaming media, and firewalls. NLB also provides high availability by detecting host failures and automatically redistributing traffic to remaining operational hosts.

For more information on NLB, see *Configuring VLANs, Spanning Tree, and NLB*.

Switch clustering at the edge of the SPBM network

Typical customer deployments require redundancy all the way to the access side of the network. IP Multicast over Fabric Connect supports switch clustering, Split Multilink Trunking (SMLT) technology, at the edge of the SPBM fabric, providing redundancy to the access Layer 2 switch where you can attach multicast senders and receivers. Typical SPBM fabric deployments use two or more B-VLANs for Equal Cost Multipath (ECMP) and resiliency. For simplicity in understanding how the SPBM network works, assume that there are two B-VLANs (primary and secondary).

The following figure shows how multicast senders and receivers connect to the SPBM cloud using BEBs.

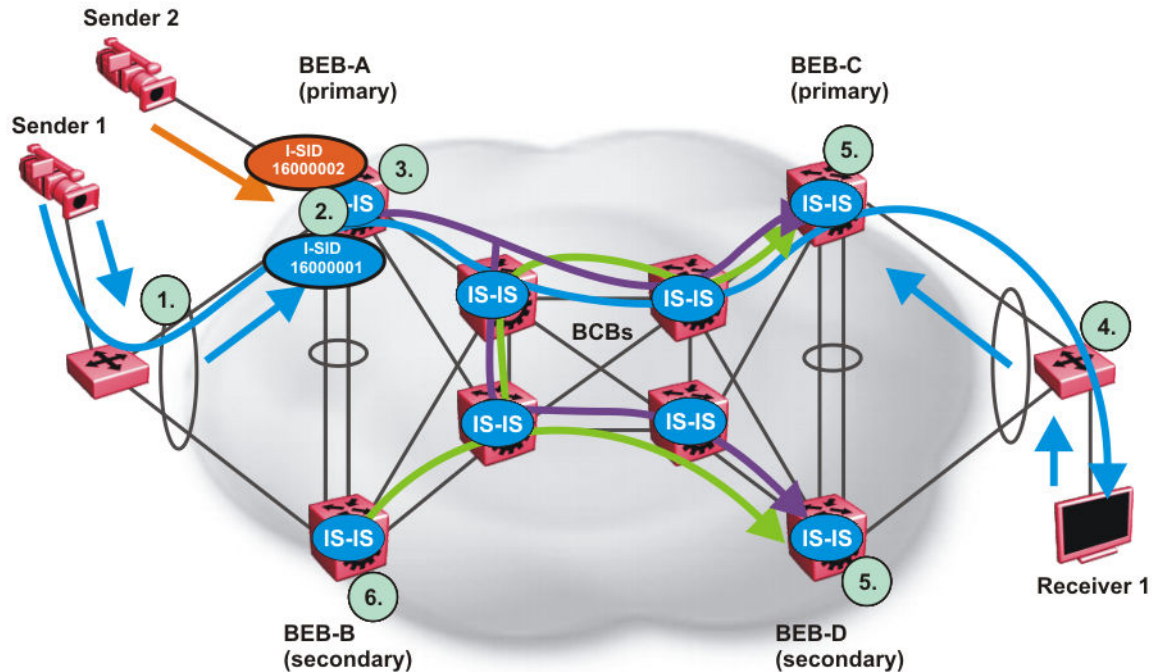


Figure 2: IP Multicast over Fabric Connect streams in an SMLT configuration

The following list describes the preceding diagram:

1. The edge switch hashes the sender multicast data to a specific MLT link.
2. A multicast stream received at the edge of the SPBM fabric is mapped to a dedicated multicast data I-SID.
3. For the non-SMLT attached sender 2, the stream is hashed to the primary or secondary B-VLAN based on whether the data I-SID is even or odd numbered. For the SMLT attached to sender 1, IS-IS advertises the stream to the rest of the fabric on the primary B-VLAN and synchronizes information to the vIST peer.
4. The edge switch hashes the receiver IGMP join to a specific MLT link.
5. Both BEBs on both B-VIDs advertise the IGMP join.
6. The multicast tree is built for (S1,G1), which is rooted in the primary sender BEB. The multicast tree is built for (S1,G1), which is rooted in the secondary sender BEB.

IGMP Snooping is widely used on Layer 2 access switches to prune multicast traffic. In IP Multicast over Fabric Connect, BEBs are the IGMP Queriers, therefore access switches forward multicast data from the senders as well as IGMP control messages from receivers to the BEBs.

Multicast sender

When a sender transmits multicast data to the Layer 2 access switch that has an MLT to the switch cluster, it is hashed towards one or the other BEBs in the switch cluster. The receiving BEB allocates a data I-SID and sends a TLV update on either the primary B-VLAN or the secondary B-VLAN, depending on whether the BEB is the primary or secondary switch. The primary switch uses the primary B-VLAN, whereas, the secondary switch uses the secondary B-VLAN. This information is propagated through the SPBM fabric so all BEBs are aware of this stream availability.

The sender information is also synchronized over the vIST to the peer switch. Then the peer switch allocates a data I-SID for the multicast stream and sends a TLV update on the appropriate B-VLAN to announce the availability of the stream. The data I-SIDs allocated by the primary and secondary switch cluster peers may be the same or different, as they are allocated independently by each switch.

*** Note:**

If a sender attaches to only one BEB in a switch cluster, the sender information is not synchronized over the vIST because it is not SMLT attached. The sender information is advertised, and data is sent on either the primary or secondary B-VLAN. The odd-numbered data I-SIDs use the primary B-VLAN, and the even-numbered data I-SIDs use the secondary B-VLAN. The same hashing rules apply to the forwarding of multicast data.

Multicast receiver

When a receiver sends an IGMP join message to the Layer 2 access switch that has an MLT to the switch cluster, it is hashed towards one or the other BEBs in the switch cluster. The receiving BEB queries the IS-IS Link State Database (LSDB) to check if a sender exists for the requested stream within the scope of the receiver.

If the requested stream does not exist, the BEB keeps the IGMP information but no further action is taken. If the requested stream exists, the BEB sends an IS-IS Link State Packet (LSP), with TLV update information, for both primary and secondary B-VLANs to its neighbors to inform them of the presence of a receiver. The BEB propagates this information through LSPs through the SPBM cloud. The receiver information is also synchronized over the vIST to the peer switch. The peer switch then queries its IS-IS Link State Database (LSDB) and, if the requested stream exists, it sends an IS-IS LSP, with a TLV update, for both primary and secondary B-VLANs to its neighbors to inform them of the presence of the receiver.

IS-IS uses these TLV updates in LSPs to create multicast shortest path first trees in the SPBM fabric. IS-IS creates a shortest path first tree for the primary and secondary B-VLANs, but only one of the B-VLANs transports multicast data with the other in active standby in case of failures at the SPBM edge. After IS-IS creates the trees, multicast data flows between senders and receivers.

IP Multicast over Fabric Connect and SMLT

The following section summarizes the IP Multicast over Fabric Connect actions in an SMLT environment. The BEBs on the sender side behave as follows:

- Primary SMLT peer BEB always advertises the streams it receives, and sends data for them on the primary B-VLAN.
- Secondary SMLT peer BEB always advertises the streams it receives, and sends data for them on the secondary B-VLAN.
- Non-SMLT BEBs or SMLT BEBs with single attached senders advertise streams, and send data on the primary or secondary B-VLAN based on hash criteria (odd-numbered data I-SIDs use primary B-VLAN; even-numbered data I-SIDs use secondary B-VLAN).

The BEBs on the receiver side behave as follows:

- The primary SMLT peer BEB that receives multicast data on the primary B-VLAN sends it to both SMLT and non-SMLT SPBM access (UNI) links.
- The primary SMLT peer BEB that receives multicast data on the secondary B-VLAN sends it to non-SMLT SPBM access (UNI) links only.

- The secondary SMLT peer BEB that receives multicast data on primary B-VLAN sends it to non-SMLT SPBM access (UNI) links only.
- The secondary SMLT peer BEB that receives multicast data on secondary B-VLAN sends data to both SMLT and non-SMLT SPBM access (UNI) links.
- The non-SMLT BEB that receives multicast data on primary or secondary B-VLAN sends data to all SPBM access (UNI) links.

Layer 2 Querier behavior for a switch cluster

In ERS 8800, VSP 4000 Series, VSP 7200 Series, and VSP 8000 Series, for C-VLANs in an SMLT environment, the vIST ports are not part of the VLAN.

IGMP on a C-VLAN behaves as follows to account for the fact that vIST peers do not see the membership queries of each other:

- The vIST peer with the higher IP address sends the queries out all SMLT and non-SMLT ports on SPBM access links.
- The vIST peer with the lower IP address only sends out queries on its non-SMLT ports. This includes SMLT ports whose remote ports are down (SMLT state of 'norm').
- With the existence of an vIST peer with a higher IP address and an vIST peer with a lower IP address, it means two queriers exist within the C-VLAN. Having two queriers poses no problems in this SPB environment, as all SMLT access devices see the vIST peer with the higher IP address as the querier, and non-SMLT access devices see the directly connected vIST peer as the querier. Non-SMLT access devices that connect on either side of the vIST peers can talk to each other using the SPBM cloud.

Considerations when you connect an IP Multicast over Fabric Connect network to a PIM network

IP Multicast over Fabric Connect does not integrate PIM functionality. Apply the following considerations when you connect to a PIM network:

- You must configure static IGMP receivers on the BEB access interface that faces the PIM network when the sender is on the SPBM access network and the receiver is on the PIM network.

*** Note:**

The PIM router must have a configuration option to accept streams with non-local sources or the router drops the packets. The switch does not support a configuration option to accept streams with non-local sources.

You must configure static IGMP receivers on the PIM interface that face the IP Multicast over Fabric Connect network when the sender is on the PIM network and the receiver is on the SPBM access network.

*** Note:**

For security reasons and to limit unnecessary multicast streams from being injected into the SPBM domain, you should configure ACLs on the BEB facing the PIM network.

IP Multicast over Fabric Connect restrictions

Review the following restrictions for the IP Multicast over Fabric Connect feature.

IGMP

The BEB must be the only IGMP querier in the network. If the BEB receives an IGMP query from any other device, it causes unpredictable behavior, including traffic loss.

SPBM supports IGMP Snooping on a C-VLAN, but it does not support PIM on a C-VLAN. If you enable IGMP Snooping on a C-VLAN, then its operating mode is Layer 2 VSN with IP Multicast over Fabric Connect.

SPBM supports Network Load Balancing (NLB) unicast and multicast modes. SPBM does not support NLB Multicast operation with IGMP.

* Note:

The NLB Multicast operation feature is not supported on all hardware platforms. If you do not see this command in the command list or EDM, the feature is not supported on your hardware. For more information about feature support, see *Release Notes*.

You must enable SSM snoop before you configure IGMP version 3, and you must enable both ssm-snoop and snooping for IGMPv3.

For IGMP Snooping, ensure that the IGMP version used by multicast hosts and other devices in the network is either the same as the IGMP version configured on the IGMP Snooping VLAN, or that compatibility mode is enabled.

SSM

If you delete any `ssm-map` in a static range group, the switch deletes the entire static range group. For example, create an `ssm-map` for 232.122.122.122 to 232.122.122.128 and after that configure this same range in a static group. If you delete any `ssm-map` between 232.122.122.122. to 232.122.122.128, the switch deletes the entire static range group.

PIM

There can be no interaction with PIM and multicast routers on the access.

The BEB only interacts with IGMP messages and not PIM, so all multicast traffic must be drawn towards the BEB, which acts as the IGMP querier, for the stream to be announced.

IP Multicast over Fabric Connect does not integrate PIM functionality so the following considerations apply when connecting to a PIM network:

- You must configure static IGMP receivers on the BEB access interface facing the PIM network when the sender is on the SPBM access network and the receiver is on the PIM network. Static IGMP receivers make the PIM router accept streams and avoid a Reverse Path Forwarding (RPF) check that can change the source of the stream.
- You must configure static IGMP receivers on the PIM interface facing the IP Multicast over Fabric Connect network when the sender is on the PIM network and the receiver is on the SPBM access network.
- You must configure Access Control Lists (ACLs) on the BEB facing the PIM network for security.

Data I-SID

The BEB matches a single multicast stream to a particular data I-SID. As a result there is a one-to-one mapping between the S,G to data I-SID for each BEB.

Supported services

The switch does not support IP Multicast over Fabric Connect routing on inter-VSN routing interfaces.

The switch supports the following modes of IP Multicast over Fabric Connect:

- Layer 2 VSN multicast service — Multicast traffic remains within the same Layer 2 VSN across the SPBM cloud.
- Layer 3 VSN multicast service — Multicast traffic remains within the same Layer 3 VSN across the SPBM cloud.
- IP Shortcuts multicast service — Multicast traffic can cross VLAN boundaries but remains confined to the subset of VLANs with the Global Routing Table that have IP Multicast over Fabric Connect enabled.

IP Multicast over Fabric Connect configuration using the CLI

Enabling IP Multicast over Fabric Connect globally

Use this procedure to enable IP Multicast over Fabric Connect globally on the Backbone Edge Bridges (BEBs) that directly or indirectly (using Layer 2 switches) connect to IP multicast senders or receivers. By default, IP Multicast over Fabric Connect is disabled. There is no need to enable IP Multicast over Fabric Connect on the Backbone Core Bridges (BCBs).

You must configure IP Multicast over Fabric Connect at the global level, and then enable it on the service option or options you choose.

*** Note:**

IP Multicast over Fabric Connect uses I-SIDs starting at 16,000,000 and above. If Layer 2 or Layer 3 I-SIDs are in this range, the system displays an error message and the switch does not enable IP Multicast over Fabric Connect.

*** Note:**

You must enable IP multicast over Fabric Connect globally on all DvR enabled nodes (Controllers and Leaf nodes) in a DvR domain.

For more information on DvR, see *Configuring IPv4 Routing*.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must create the customer VLANs (C-VLANs) and add slots/ports.
- You must add IST slot/ports to the C-VLAN for an SMLT topology.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Verify no I-SIDs exist in the default reserved range:

- a. For Layer 2 use the following command:

```
show vlan i-sid
```

- b. For Layer 3 use the following command:

```
show ip ipvpn vrf WORD<1-16>
```

3. Enter IS-IS Router Configuration mode:

```
enable
```

```
configure terminal
```

```
router isis
```

4. Enable IP Multicast over Fabric Connect globally:

```
spbm <1-100> multicast enable
```

*** Note:**

The switch only supports one SPBM instance.

5. **(Optional)** Disable IP Multicast over Fabric Connect globally:

```
no spbm <1-100> multicast enable
```

```
default spbm <1-100> multicast enable
```

Example

Enable IP Multicast over Fabric Connect globally:

```
Switch:1(config)#show vlan i-sid
```

```
=====
                        Vlan I-SID
=====
VLAN_ID    I-SID
-----
1
50          200
51
52
53
54
55
56
57
```

```

9 out of 9 Total Num of Vlans displayed
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#router isis
Switch:1(config-isis)#spbm 1 multicast enable

```

Variable definitions

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

Variable	Value
<1-100>	<p>Enables IP Multicast over Fabric Connect globally. The default is disabled.</p> <p>Specifies the SPBM instance. The switch only supports one instance.</p>

Displaying IP Multicast over Fabric Connect information

Use this procedure to display IP Multicast over Fabric Connect summary information.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the status of the global IP Multicast over Fabric Connect configuration:

```
show isis spbm multicast
```

3. Display IP Multicast over Fabric Connect summary information for each S, G, V tuple:

```
show isis spb-mcast-summary [host-name WORD<0-255>][lspid
<xxxx.xxxx.xxxx.xx-xx>]
```

4. Display information about the multicast routes on the switch:

```
show ip mroute route [vrf WORD<0-16>][vrfids WORD<0-255>]
```

Example

Display IP Multicast over Fabric Connect global configuration information:

```

Switch:1>enable
Switch:1#show isis spbm multicast

                multicast : enable
                fwd-cache-timeout(seconds) : 210

Switch:1#show isis spb-mcast-summary

=====
                SPB multicast - Summary
=====
SCOPE   SOURCE      GROUP      DATA      LSP  HOST
I-SID   ADDRESS     ADDRESS    I-SID     BVID  FRAG  NAME
-----
GRT     192.0.2.102 233.252.0.1 16000001  63   0x0   DIST5A

```

IP Multicast over Fabric Connect basic configuration

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

```
=====
Mroute Route - GlobalRouter
=====
GROUP          SOURCE          SRCMASK          UPSTREAM_NBR    IF      EXPIR  PROT
-----
233.252.0.1    0.0.0.0         0.0.0.0         0.0.0.0        V3      30     spb-access
233.252.0.1    198.51.100.99  255.255.255.0  0.0.0.0        -       0      spb-network
Total 4
```

Variable definitions

Use the data in the following table to use the **show isis spb-mcast-summary** command.

Variable	Value
host-name <i>WORD</i> <0–255>	Displays the IP Multicast over Fabric Connect summary information for a specific host-name.
lspid <xxx.xxx.xxx.xx-xx>	Displays the IP Multicast over Fabric Connect summary information for the specified LSP ID that you enter in xxx.xxx.xxx.xx-xx — 8 byte format.

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

Variable	Value
vrf <i>WORD</i> <1–32>	Specifies a VRF.
vrfids <i>WORD</i> <0–255>	Specifies the VRF ID

Job aid

The following table describes the fields in the output for the **show isis spbm multicast** command.

Parameter	Description
multicast	Specifies if multicast is enabled.
fwd-cache-timeout (seconds)	Specifies the forward cache timeout value in seconds.

The following table describes the fields in the output for the **show isis spb-mcast-summary** command.

Parameter	Description
SCOPE I-SID	Indicates the I-SID that specifies the multicast streams when the scope is either the Layer 3 VSN or the Layer 2 VSN or any combination.
SOURCE ADDRESS	Indicates the IP multicast source address that maps to the I-SID.

Table continues...

Parameter	Description
GROUP ADDRESS	Indicates the IP multicast group address that maps to the I-SID.
DATA I-SID	Indicates the data I-SID for the IP multicast route, which includes the source IP address, group IP address, and the local VLAN that the stream is received on (S,G,V tuple). SPBM uses the data I-SID to create the multicast tree.
BVID	Indicates the ID of the SPBM backbone VLAN (B-VLAN) on which the multicast stream forwards in the SPBM cloud.
LSP FRAG	Indicates the fragment number of the LSP ID.
HOST-NAME	Indicates the host name of the router.

The following table describes the fields in the output for the `show ip mroute route` command.


Parameter	Description
GROUP	Indicates the IP multicast group for this multicast route.
SOURCE	Indicates the network address that, when combined with the corresponding value of SRCMASK, identifies the sources for this multicast route.
SRCMASK	Indicates the network mask that, when combined with the corresponding value of SOURCE, identifies the sources for this multicast route.
UPSTREAM_NBR	Indicates the address of the upstream neighbor from which IP datagrams from these sources to this multicast address are received. The field displays the value of 0.0.0.0 if the (S,G) source is local or if the RP for this the (*,G) group is an address on this router.
IF	Indicates the value of ifindex for the interface that receives IP datagrams sent by these sources to this multicast address. A value of 0 in a (*,G) route indicates that datagrams are not subject to an incoming interface check, but datagrams can be received on any interface.
EXPIR	Indicates the minimum amount of time remaining before this entry ages out. The value 0 indicates that the entry is not subject to aging.  Note: The value you configure for fwd-cache-timeout applies only to the locally learned sender; it

Table continues...

Parameter	Description
	does not apply to SMLT synchronized sender records.
PROT	Indicates the multicast protocol through which the switch learned this route. The spb-access and spb-network values indicate the stream learned when IP Multicast over Fabric Connect is configured on the VLAN. The spb-access value indicates that it was learned on the access. The spb-network value indicates it was learned over the SPBM cloud.

Displaying the IP unicast FIB, multicast FIB, unicast FIB, and unicast tree

Use the following procedure to display SPBM IP unicast Forwarding Information Base (FIB), SPBM multicast FIB, unicast FIB, and the unicast tree.

In SPBM, Backbone MAC (B-MAC) addresses are carried within the IS-IS link-state database. To do this, SPBM supports an IS-IS Type-Length-Value (TLV) that advertises the Service Instance Identifier (I-SID) and B-MAC information across the network. Each node has a System ID, which also serves as B-MAC of the switch. These B-MAC addresses are populated into the SPBM Forwarding Information Base (FIB).

When the network topology is discovered and stored in the IS-IS link-state database, each node calculates shortest path trees for each source node, so that a unicast path now exists from every node to every other node. With this information, each node populates unicast information received from SPBM into the FIB for forwarding purposes.

I-SIDs are only used for virtual services (Layer 2 VSNs and Layer 3 VSNs). If you only enable IP Shortcuts on the Backbone Edge Bridges, I-SIDs are never exchanged in the network as IP Shortcuts allow Global Routing Table (GRT) IP networks to be transported across IS-IS.

The `show isis spbm ip-unicast-fib` command displays all of the IS-IS routes in the IS-IS LSDB. The IP ROUTE PREFERENCE column in the `show isis spbm ip-unicast-fib` command displays the IP route preference.

Routes within the same VSN are added to the LSDB with a default preference of 7. Inter-VSN routes are added to the LSDB with a route preference of 200. IS-IS accept policies allow you to change the route preference for incoming routes. If the same route is learned from multiple sources with different route preferences, then the routes are not considered equal cost multipath (ECMP) routes. The route with the lowest route preference is the preferred route. In Layer 2, in the event of a tie-break between routes from multiple sources, the tie-breaking is based on cost and hop count.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display the SPBM IP unicast FIB:

```
show isis spbm ip-unicast-fib [all] [id <1-16777215>] [spbm-nh-as-
mac]
```

* **Note:**

To display the IPv6 unicast FIB, use the `show isis spbm ipv6-unicast-fib` command.

3. Display the SPBM multicast FIB:

```
show isis spbm multicast-fib [vlan <1-4059>] [i-sid <1-16777215>]
[nick-name <x.xx.xx>] [summary]
```

4. Display the SPBM unicast FIB:

```
show isis spbm unicast-fib [b-mac <0x00:0x00:0x00:0x00:0x00:0x00>]
[vlan <1-4059>] [summary]
```

5. Display the SPBM unicast tree:

```
show isis spbm unicast-tree <1-4059> [destination <xxxx.xxxx.xxxx>]
```

Example

```
Switch# show isis spbm ip-unicast-fib
```

```
=====
SPBM IP-UNICAST FIB ENTRY INFO
=====
VRF   VRF  DEST          OUTGOING  SPBM   PREFIX  PREFIX  IP ROUTE
VRF   ISID ISID  Destination  NH BEB  VLAN  INTERFACE COST   COST   TYPE   PREFERENCE
-----
GRT   -    -    10.133.136.0/24  4K3(*)  4058  1/3      10    1    Internal  7
GRT   -    -    10.133.136.0/24  4K3(*)  4059  1/3      10    1    Internal  7
GRT   -    -    10.133.136.0/24  4K4(*)  4058  to_4k4   10000 1    Internal  7
GRT   -    -    10.133.136.0/24  4K4(*)  4059  to_4k4   10000 1    Internal  7
-----
Total number of SPBM IP-UNICAST FIB entries 4
=====
```

```
Switch# show isis spbm ip-unicast-fib id 10002
```

```
=====
SPBM IP-UNICAST FIB ENTRY INFO
=====
VRF   VRF  DEST          OUTGOING  SPBM   PREFIX  PREFIX  IP ROUTE
VRF   ISID ISID  Destination  NH BEB  VLAN  INTERFACE COST   COST   TYPE   PREFERENCE
-----
vrf2  -    10002 65.2.2.0/24  ESS2   1000  1/13    20    20    Internal  7
vrf2  -    10002 65.2.2.0/24  ESS2   1001  1/18    20    20    Internal  7
-----
Total number of SPBM IP-UNICAST FIB entries 2
=====
```

```
Switch# show isis spbm ip-unicast-fib all
```

```
=====
SPBM IP-UNICAST FIB ENTRY INFO
=====
VRF   VRF  DEST          OUTGOING  SPBM   PREFIX  PREFIX  IP ROUTE
VRF   ISID ISID  Destination  NH BEB  VLAN  INTERFACE COST   COST   TYPE   PREFERENCE
-----
```

IP Multicast over Fabric Connect basic configuration

```
-----
GRT      -      -      1.0.0.1/32      ESP0      1000 1/13      20      1      Internal  7
GRT      -      -      1.0.0.1/32      ESP0      1000 1/18      20      1      Internal  7
vrf2    - 10002 65.2.2.0/24      ESS2      1000 1/13      20      20     Internal  7
vrf2    - 10002 65.2.2.0/24      ESS2      1001 1/18      20      20     Internal  7
-----
Total number of SPBM IP-UNICAST FIB entries 4
-----
```

```
Switch#show isis spbm multicast-fib
=====
SPBM MULTICAST FIB ENTRY INFO
=====
MCAST DA          ISID      BVLAN SYSID          HOST-NAME OUTGOING-INTERFACES  INCOMING
INTERFACE
-----
03:00:07:e4:e2:02 15000066 1001  0077.0077.0077 Switch-25      1/33           MLT-2
03:00:08:e4:e2:02 15000066 1001  0088.0088.0088 Switch-33      1/50,1/33     40.40.40.40
03:00:41:00:04:4d 1101      4058  00bb.0000.4100 Switch-1(*)    1/3,1/49,0.0.0.0
Tunnel_to_HQ
03:00:41:00:04:4f 1103      4058  00bb.0000.4100 Switch-1(*)    1/3,1/49,0.0.0.0 cpp
-----
Total number of SPBM MULTICAST FIB entries 4
-----
```

```
Switch# show isis spbm unicast-fib
=====
SPBM UNICAST FIB ENTRY INFO
=====
DESTINATION        BVLAN SYSID          HOST-NAME  OUTGOING  COST
ADDRESS           INTERFACE
-----
00:16:ca:23:73:df 1000  0016.ca23.73df  SPBM-1    1/21      10
00:16:ca:23:73:df 2000  0016.ca23.73df  SPBM-1    1/21      10
00:18:b0:bb:b3:df 1000  0018.b0bb.b3df  SPBM-2    MLT-2     10
00:14:c7:e1:33:e0 1000  0018.b0bb.b3df  SPBM-2    MLT-2     10
00:18:b0:bb:b3:df 2000  0018.b0bb.b3df  SPBM-2    MLT-2     10
-----
Total number of SPBM UNICAST FIB entries 5
-----
```

Variable definitions

Use the data in the following table to use the `show isis spbm ip-unicast-fib` command.


Variable	Value
all	<p>Displays entries for the Global Routing Table (GRT) and all Virtual Routing and Forwarding (VRF) instances.</p> <p> Note:</p> <p>If you use the command <code>show isis spbm ip-unicast-fib</code> the device displays only GRT entries. The command shows IP routes from remote Backbone Edge Bridges (BEBs).</p>

Table continues...

Variable	Value
id <1-16777215>	Displays IS-IS SPBM IP unicast Forwarding Information Base (FIB) information by Service Instance Identifier (I-SID) ID.
spbm-nh-as-mac	Displays the next hop B-MAC of the IP unicast FIB entry.

Use the data in the following table to use the **show isis spbm multicast-fib** command.

Variable	Value
vlan <1-4059>	Displays the FIB for the specified SPBM VLAN.
i-sid <1-16777215>	Displays the FIB for the specified I-SID.
nick-name <x.xx.xx>	Displays the FIB for the specified nickname.
summary	Displays a summary of the FIB.

Use the data in the following table to use the **show isis spbm unicast-fib** command.

Variable	Value
b-mac <0x00:0x00:0x00:0x00:0x00:0x00>	Displays the FIB for the specified B-MAC.
vlan <1-4059>	Displays the FIB for the specified SPBM VLAN.
summary	Displays a summary of the FIB.

Use the data in the following table to use the **show isis spbm unicast-tree** command.

Variable	Value
<1-4059>	Specifies the SPBM B-VLAN ID.
destination <xxxx.xxxx.xxxx>	Displays the unicast tree for the specified destination.

Job aid

The following sections describe the fields in the outputs for SPBM multicast FIB, unicast FIB, and unicast tree show commands.

show isis spbm ip-unicast-fib

The following table describes the fields in the output for the **show isis spbm ip-unicast-fib** command.

Parameter	Description
VRF	Specifies the VRF ID of the IP unicast FIB entry, 0 indicates NRE.
VRF ISID	Specifies the I-SID of the IP unicast FIB entry.
DEST ISID	Specifies the destination I-SID of the IP unicast FIB entry.

Table continues...

Parameter	Description
Destination	Specifies the destination IP address of the IP unicast FIB entry.
NH BEB	Specifies the next hop B-MAC of the IP unicast FIB entry.
VLAN	Specifies the VLAN of the IP unicast FIB entry.
OUTGOING INTERFACE	Specifies the outgoing port of the IP unicast FIB.
SPBM COST	Specifies the B-MAC cost of the IP unicast FIB entry.
PREFIX COST	Specifies the prefix cost of the IP unicast FIB entry.
PREFIX TYPE	Specifies the prefix type of the IP unicast FIB entry.
IP ROUTE PREFERENCE	Specifies the IP route preference of the IP unicast FIB entry.

show isis spbm multicast-fib

The following table describes the fields in the output for the `show isis spbm multicast-fib` command.

Parameter	Description
MCAST DA	Indicates the multicast destination MAC address of the multicast FIB entry.
ISID	Indicates the I-SID of the multicast FIB entry.
BVLAN	Indicates the B-VLAN of the multicast FIB entry.
SYSID	Indicates the system identifier of the multicast FIB entry.
HOST-NAME	Indicates the host name of the multicast FIB entry.
OUTGOING INTERFACE	Indicates the outgoing port of the multicast FIB entry.
INCOMING INTERFACE	Indicates the outgoing port of the multicast FIB entry.

show isis spbm unicast-fib

The following table describes the fields in the output for the `show isis spbm unicast-fib` command.

Parameter	Description
DESTINATION ADDRESS	Indicates the destination MAC Address of the unicast FIB entry.
BVLAN	Indicates the B-VLAN of the unicast FIB entry.
SYSID	Indicates the destination system identifier of the unicast FIB entry.
HOST-NAME	Indicates the destination host name of the unicast FIB entry.
OUTGOING INTERFACE	Indicates the outgoing interface of the unicast FIB entry.
COST	Indicates the cost of the unicast FIB entry.

IP Multicast over Fabric Connect configuration using the EDM

Configuring IP Multicast over Fabric Connect globally

Use this procedure to globally enable IP Multicast over Fabric Connect on the Backbone Edge Bridges (BEBs) that directly or indirectly (using Layer 2 switches) connect to IP multicast senders or receivers. By default, IP Multicast over Fabric Connect is disabled. There is no need to enable IP Multicast over Fabric Connect on the Backbone Core Bridges (BCBs).

You must configure IP Multicast over Fabric Connect at the global level, and then enable it on the service option or options you choose.

Important:

IP Multicast over Fabric Connect uses I-SIDs that start at 16,000,000 and above. The device displays an error message if the Layer 2 and Layer 3 I-SIDs are within this range and the system does not enable IP Multicast over Fabric Connect.

Note:

You must enable IP multicast over Fabric Connect globally on all DvR enabled nodes (Controllers and Leaf nodes) in a DvR domain.

For more information on DvR, see *Configuring IPv4 Routing*.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must create the customer VLANs (C-VLANs) and add slots/ports.

Procedure

1. Determine if any I-SIDs are within the default range reserved for multicast. In the navigation pane, expand the following folders: **Configuration > IS-IS > SPBM**.
2. Click the **I-SID** tab to determine if the I-SIDs are within the default range reserved for multicast.
3. In the navigation pane, expand the **Configuration > IS-IS > SPBM** folders.
4. Click the **SPBM** tab.
5. If you want to enable multicast on an SPBM instance that already exists, in the **Mcast** column in the table, select **enable**.
6. If you want to enable multicast on an SPBM instance that does not yet exist, click **Insert**.
7. In the **Mcast** box, select **enable** to enable IP Multicast over Fabric Connect globally.
8. Click **Insert**.

9. Click **Apply**.

SPBM field descriptions

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

Name	Description
Id	Specifies the SPBM instance ID. Only one SPBM instance is supported.
NodeNickName	Specifies a nickname for the SPBM instance globally.
PrimaryVlan	Specifies the primary SPBM B-VLAN to add to the SPBM instance.
Vlans	Specifies the SPBM B-VLANs to add to the SPBM instance.
LsdbTrap	Specifies if the LSDB update trap is enabled on this SPBM instance. The default is disabled.
IpShortcut	Specifies if SPBM IP Shortcuts is enabled. The default is disabled.
SmltSplitBEB	Specifies the SMLT split BEB for this SPBM instance.
SmltVirtualBmac	Specifies the SMLT virtual MAC for this SPBM instance.
SmltPeerSysId	Specifies the SMLT peer system ID for this SPBM instance.
Mcast	Specifies if IP multicast over Fabric Connect is enabled. The default is disabled.
McastFwdCacheTimeout	Specifies the global forward cache timeout in seconds. The default is 210 seconds.

Displaying IP Multicast over Fabric Connect routes

Use this procedure to display IP Multicast over Fabric Connect routes.

Procedure

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

IpMcastRoutes field descriptions

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

Name	Description
VsnIsid	Specifies the VSN I-SID. Layer 2 VSN and Layer 3 VSN each require a VSN I-SID.
Group	Specifies the group IP address for the IP Multicast over Fabric Connect route.
Source	Specifies the IP address where the IP Multicast over Fabric Connect route originated.
NickName	Specifies the nick name used to filter criteria.

Table continues...

Name	Description
SourceBeb	Specifies the source BEB for the IP multicast route.
VlanId	Specifies the ID for the C-VLAN.
VrfName	Specifies the VRF name.
Datalsid	Specifies the data I-SID for the IP Multicast over Fabric Connect route. A a BEB receives IP multicast data from a sender, a BEB allocates a data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
Type	Specifies the type for the IP Multicast over Fabric Connect route.
Bvlan	Specifies the B-VLAN for the IP Multicast over Fabric Connect route.
NniInterfaces	Specifies the NNI ports for the IP multicast route. SPBM runs in the core on the ports that connect to the core. These ports are NNI ports. Ports that face a customer VLAN are user-to-network interface (UNI) ports.

Displaying the UNI ports for IP multicast routes

Use this procedure to display UNI ports associated with particular IP multicast routes.

Procedure

1. In the navigation pane, expand the **Configuration > IS-IS > SPBM** folders.
2. Click the **IpMcastRoutes** tab.
3. Select the desired row and click the **UNI Ports** tab to display the UNI ports associated with a particular stream.

IpMcastRoutes Uni Ports field descriptions

Use the data in the following table to use the **IpMcastRoutes Uni Ports** tab.

Name	Description
Group	Specifies the group IP address for the IP Multicast over Fabric Connect route.
Source	Specifies the IP address where the IP Multicast over Fabric Connect route originated.

Table continues...

Name	Description
Vsnlsid	Specifies the VSN I-SID. Layer 2 VSN and Layer 3 VSN each require a VSN I-SID.
Datalsid	Specifies the data I-SID for the IP multicast route. After a BEB receives the IP multicast data from a sender, a BEB allocates a data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
SourceBeb	Specifies the source BEB for the IP multicast route.
VlanId	Specifies the ID for the C-VLAN.
VrfName	Specifies the VRF name.
NniPorts	Specifies the NNI ports for the IP multicast route. SPBM runs in the core on the ports that connect to the core. These ports are NNI ports. Ports facing a customer VLAN are user-to-network interface (UNI) ports.
Type	Specifies the type for the IP multicast route.
Bvlan	Specifies the B-VLANs for the IP multicast route.

Displaying the multicast FIB

Use the following procedure to display the multicast FIB.

In SPBM, B-MAC addresses are carried within the IS-IS link-state database. To do this, SPBM supports an IS-IS TLV that advertises the I-SID and B-MAC information across the network. Each node has a System ID, which also serves as Backbone MAC address (B-MAC) of the switch. These Backbone MAC addresses are populated into the SPBM VLAN Forwarding Information Base (FIB).

When the network topology is discovered and stored in the IS-IS link-state database, each node calculates shortest path trees for each source node, so that a unicast path now exists from every node to every other node. With this information, each node populates unicast information received from SPBM into the FIB for forwarding purposes.

The multicast FIB is not produced until virtual services are configured and learned.

Procedure

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

Multicast FIB field descriptions

Use the data in the following table to use the **Multicast FIB** tab.

Name	Description
SysId	System ID of the node where the multicast FIB entry originated.
Vlan	VLAN of the multicast FIB entry.
McastDestMacAddr	Multicast destination MAC Address of the multicast FIB entry
Isid	I-SID of the multicast FIB entry.
HostName	Host name of the node where the multicast FIB entry originated.
OutgoingInterfaces	Specifies the switched UNI port outgoing interface of multicast FIB entry.
IncomingInterface	Specifies the incoming interface (port or MLT) of the multicast FIB entry.

IP Multicast over Fabric Connect configuration examples

IP multicast over Fabric Connect global configuration

The following sections show the steps required to configure IP multicast over Fabric Connect at a global level

SwitchC

```
enable
configure terminal
prompt SwitchC

ISIS SPBM CONFIGURATION
router isis
spbm 1 multicast enable
exit
```

SwitchG

```
enable
configure terminal
prompt SwitchG

ISIS SPBM CONFIGURATION
router isis
spbm 1 multicast enable
exit
```

SwitchD

```
enable
configure terminal
prompt SwitchD

ISIS SPBM CONFIGURATION
```

IP Multicast over Fabric Connect basic configuration

```
router isis
spbm 1 multicast enable
exit
```

Chapter 5: IP Multicast over Fabric Connect services configuration

Layer 2 VSN configuration

Layer 2 VSN configuration fundamentals

This section provides fundamentals concepts for Layer 2 VSN.

Layer 2 VSN IP Multicast over Fabric Connect

IP Multicast over Fabric Connect supports Layer 2 VSN functionality where multicast traffic is bridged over the SPBM core infrastructure. An application for Layer 2 VSNs using IP Multicast over Fabric Connect is multicast traffic in data centers.

For more information on Layer 2 VSN configuration, see *Configuring Fabric Basics and Layer 2 Services*.

After you configure `ip igmp snooping` on a VLAN that has an I-SID configured (a C-VLAN), that VLAN is automatically enabled for IP Multicast over Fabric Connect services. No explicit configuration exists separate from that to enable Layer 2 VSN IP Multicast over Fabric Connect.

Multicast traffic remains in the same Layer 2 VSN across the SPBM cloud for Layer 2 VSN IP Multicast over Fabric Connect. IP Multicast over Fabric Connect constrains all multicast streams within the scope level in which they originate. If a sender transmits a multicast stream to a BEB on a Layer 2 VSN with IP Multicast over Fabric Connect enabled, only receivers that are part of the same Layer 2 VSN can receive that stream.

I-SIDs

After a BEB receives IP multicast data from a sender, the BEB allocates a data service instance identifier (I-SID) in the range of 16,000,000 to 16,512,000 for the multicast stream. The stream is identified by the S, G, V tuple, which is the source IP address, the group IP address and the local VLAN the multicast stream is received on. The data I-SID uses Tx/Rx bits to signify whether the BEB uses the I-SID to transmit, receive, or both transmit and receive data on that I-SID.

In the context of Layer 2 VSNs with IP Multicast over Fabric Connect, the scope is the I-SID value of the Layer 2 VSN associated with the local VLAN on which the IP multicast data was received.

TLVs

This information is propagated through the SPBM cloud using IS-IS Link State Packets (LSPs), which carry TLV updates, that result in the multicast tree creation for that stream. For Layer 2 VSNs, the LSPs carry I-SID information and information about where IP multicast stream senders and receivers exist using TLV 144 and TLV 185.

IS-IS acts dynamically using the TLV information received from BEBs that connect to the sender and the receivers to create a multicast tree between them.

IGMP

After a BEB receives an IGMP join message from a receiver, a BEB queries the IS-IS database to check if a sender exists for the requested stream within the scope of the receiver. If the requested stream does not exist, the IGMP information is kept, but no further action is taken. If the request stream exists, the BEB sends an IS-IS TLV update to its neighbors to inform them of the presence of a receiver and this information is propagated through the SPBM cloud.

For IGMP Snooping, ensure that the IGMP version used by multicast hosts and other devices in the network is the same as the IGMP version configured on the IGMP Snooping VLAN, or that you enable compatibility mode.

Layer 2 VSN configuration using the CLI

This section provides procedures to configure Layer 2 VSNs using the CLI.

Configuring Layer 2 VSN IP Multicast over Fabric Connect

Use this procedure to configure IP Multicast over Fabric Connect for Layer 2 VSN functionality. With Layer 2 VSN IP Multicast over Fabric Connect, multicast traffic remains in the same Layer 2 VSN across the SPBM cloud.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must create the customer VLANs (C-VLANs) and add slots/ports.
- You must assign the same I-SID to the C-VLANs on all the BEBs where you configure the C-VLAN.
- You must enable IP Multicast over Fabric Connect globally.

About this task

Traffic is only delivered to UNIs on the Layer 2 VSN where the switch receives IGMP joins and reports. Traffic does not cross the Layer 2 VSN boundary.

Configuring `ip igmp snooping` on a VLAN that has an I-SID configured (a C-VLAN) automatically enables that VLAN for IP Multicast over Fabric Connect services. No explicit configuration exists separate from that to enable Layer 2 VSN IP Multicast over Fabric Connect.

SPBM supports enabling IGMP Snooping on a C-VLAN, but it does not support enabling Protocol Independent Multicast (PIM) on a C-VLAN. If you enable IGMP snooping on a C-VLAN, then its operating mode is Layer 2 Virtual Services Network with IGMP support on the access networks for optimized forwarding of IP multicast traffic in a bridged network.

The switch only supports IPv4 multicast traffic.

Procedure

1. Enter VLAN Interface Configuration mode:

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

2. Enable proxy snoop:

```
ip igmp proxy
```

3. Enable IGMP snooping:

```
ip igmp snooping
```

4. **(Optional)** If you want to configure an address for the IGMP queries, enter the following command:

```
ip igmp snoop-querier-addr <A.B.C.D>
```

This step is not always required. The IGMP Querier on the BEB uses a source address 0.0.0.0 by default. When you do not configure this, a BEB sends IGMP queries on the UNI ports with 0.0.0.0 as the source IP address. Some Layer 2 edge switches do not support a 0.0.0.0 querier. You can use a fictitious IP address as the querier address, and use the same address on all BEBs in the network.

5. **(Optional)** Enable IGMPv3 at a VLAN level by enabling SSM-snooping and IGMPv3:

```
ip igmp ssm-snoop
ip igmp version 3
```

You must enable SSM snoop before you configure IGMP version 3 and both ssm-snoop and snooping must be enabled for IGMPv3.

For IGMP Snooping, ensure that the IGMP version used by multicast hosts and other devices in the network is the same as the IGMP version configured on the IGMP Snooping VLAN, or that you enable compatibility mode.

Example

Enable IGMPv2 at a VLAN level:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config-if)#interface vlan 501
Switch:1(config-if)#ip igmp proxy
Switch:1(config-if)#ip igmp snooping
Switch:1(config-if)#ip igmp snoop-querier-addr 192.0.2.1
```

Enable IGMPv3 at a VLAN level:

```
Switch:>enable
Switch:#configure terminal
Switch:1(config)#interface vlan 2256
Switch:1(config-if)#ip igmp proxy
```

```
Switch:1(config-if)#ip igmp snooping
Switch:1(config-if)#ip igmp snoop-querier-addr 192.0.2.1
Switch:1(config-if)#ip igmp version 3
Switch:1(config-if)#ip igmp ssm-snoop
```

Viewing Layer 2 VSN IP Multicast over Fabric Connect information

Use the following options to display Layer 2 VSN information to confirm proper configuration.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display all IP Multicast over Fabric Connect route information:

```
show isis spbm ip-multicast-route [all]
```
3. Display detailed IP Multicast over Fabric Connect route information:

```
show isis spbm ip-multicast-route [detail]
```
4. Display IP multicast route information by VLAN:

```
show isis spbm ip-multicast-route [vlan <1-4059>]
```
5. Display IP Multicast over Fabric Connect route information by VSN I-SID:

```
show isis spbm ip-multicast-route [vsn-isid <1-16777215>]
```
6. Display IP Multicast over Fabric Connect route information by group address:

```
show isis spbm ip-multicast-route [group {A.B.C.D}]
```
7. Display IP Multicast over Fabric Connect route information by source address:

```
show isis spbm ip-multicast-route [source {A.B.C.D}]
```

Important:

When you use the command `show isis spbm ip-multicast-route` without parameters or use the `detail` or `group` optional parameters without specifying a VLAN ID or VSN-ISID, the command output displays Layer 3 context only. No Layer 2 context is displayed.

8. Display summary information for each S, G, V tuple with the corresponding scope, data I-SID, and the host name of the source:

```
show isis spbm-mcast-summary [host-name WORD<0-255>][lspid
<xxxx.xxxx.xxxx.xx-xx>]
```

Example

```
Switch:1#show isis spbm ip-multicast-route all
=====
          SPBM IP-MULTICAST ROUTE INFO ALL
=====
Type   VrfName   Vlan Source      Group      VSN-ISID  Data ISID  BVLAN Source-BEB
-----
snoop  GRT       501 192.0.2.1    233.252.0.1  5010     16300001  10    e12
snoop  GRT       501 192.0.2.1    233.252.0.2  5010     16300002  20    e12
snoop  GRT       501 192.0.2.1    233.252.0.3  5010     16300003  10    e12
```



```
snoop GRT 501 192.0.2.1 233.252.0.4 5010 16300004 20 e12
snoop GRT 501 192.0.2.1 233.252.0.5 5010 16300005 10 e12
snoop GRT 501 192.0.2.1 233.252.0.6 5010 16300006 20 e12
snoop GRT 501 192.0.2.1 233.252.0.7 5010 16300007 10 e12
snoop GRT 501 192.0.2.1 233.252.0.8 5010 16300008 20 e12
snoop GRT 501 192.0.2.1 233.252.0.9 5010 16300009 10 e12
snoop GRT 501 192.0.2.1 233.252.0.10 5010 16300010 20 e12
```

 Total Number of SPBM IP MULTICAST ROUTE Entries: 10

Switch:1#show isis spbm ip-multicast-route vlan 501

```
=====
SPBM IP-MULTICAST ROUTE INFO ALL
=====
Type VrfName Vlan Source Group VSN-ISID Data ISID BVLAN Source-BEB
-----
snoop GRT 501 192.0.2.1 233.252.0.1 5010 16300001 10 e12
snoop GRT 501 192.0.2.1 233.252.0.2 5010 16300002 20 e12
snoop GRT 501 192.0.2.1 233.252.0.3 5010 16300003 10 e12
snoop GRT 501 192.0.2.1 233.252.0.4 5010 16300004 20 e12
snoop GRT 501 192.0.2.1 233.252.0.5 5010 16300005 10 e12
snoop GRT 501 192.0.2.1 233.252.0.6 5010 16300006 20 e12
snoop GRT 501 192.0.2.1 233.252.0.7 5010 16300007 10 e12
snoop GRT 501 192.0.2.1 233.252.0.8 5010 16300008 20 e12
snoop GRT 501 192.0.2.1 233.252.0.9 5010 16300009 10 e12
snoop GRT 501 192.0.2.1 233.252.0.10 5010 16300010 20 e12
```

 Total Number of SPBM IP MULTICAST ROUTE Entries: 10

Switch:1# show isis spbm ip-multicast-route vsn-isid 5010

```
=====
SPBM IP-MULTICAST ROUTE INFO - VLAN ID : 501, VSN-ISID : 5010
=====
Source Group Data ISID BVLAN Source-BEB
-----
192.0.2.1 233.252.0.1 16300001 10 e12
192.0.2.1 233.252.0.2 16300002 20 e12
192.0.2.1 233.252.0.3 16300003 10 e12
192.0.2.1 233.252.0.4 16300004 20 e12
192.0.2.1 233.252.0.5 16300005 10 e12
192.0.2.1 233.252.0.6 16300006 20 e12
192.0.2.1 233.252.0.7 16300007 10 e12
192.0.2.1 233.252.0.8 16300008 20 e12
192.0.2.1 233.252.0.9 16300009 10 e12
192.0.2.1 233.252.0.10 16300010 20 e12
```

 Total Number of SPBM IP MULTICAST ROUTE Entries: 10

Switch:1# show isis spbm ip-multicast-route vsn-isid 5010 detail

```
=====
SPBM IP-MULTICAST ROUTE INFO - TYPE : SNOOP , VLAN ID : 501, VSN-ISID : 5010
=====
Source Group Data ISID BVLAN NNI Rcvrs UNI Rcvrs Source-BEB
-----
192.0.2.1 233.252.0.1 16300001 10 1/3 V501:9/38 e12
192.0.2.1 233.252.0.2 16300002 20 1/2,1/3 V501:9/38 e12
192.0.2.1 233.252.0.3 16300003 10 1/3 V501:9/38 e12
```

IP Multicast over Fabric Connect services configuration

```

192.0.2.1 233.252.0.4 16300004 20 1/2,1/3 V501:9/38 e12
192.0.2.1 233.252.0.5 16300005 10 1/3 V501:9/38 e12
192.0.2.1 233.252.0.6 16300006 20 1/2,1/3 V501:9/38 e12
192.0.2.1 233.252.0.7 16300007 10 1/3 V501:9/38 e12
192.0.2.1 233.252.0.8 16300008 20 1/2,1/3 V501:9/38 e12
192.0.2.1 233.252.0.9 16300009 10 1/3 V501:9/38 e12
192.0.2.1 233.252.0.10 16300010 20 1/2,1/3 V501:9/38 e12
-----
Total Number of SPBM IP MULTICAST ROUTE Entries: 10
-----

Switch:1# show isis spb-mcast-summary
-----
SPB Multicast - Summary
-----
SCOPE SOURCE GROUP DATA LSP HOST
I-SID ADDRESS ADDRESS I-SID BVID FRAG NAME
-----
5010 192.0.2.1 233.252.0.1 16300001 10 0x0 e12
5010 192.0.2.1 233.252.0.3 16300003 10 0x0 e12
5010 192.0.2.1 233.252.0.5 16300005 10 0x0 e12
5010 192.0.2.1 233.252.0.7 16300007 10 0x0 e12
5010 192.0.2.1 233.252.0.9 16300009 10 0x0 e12
5010 192.0.2.1 233.252.0.2 16300002 20 0x0 e12
5010 192.0.2.1 233.252.0.4 16300004 20 0x0 e12
5010 192.0.2.1 233.252.0.6 16300006 20 0x0 e12
5010 192.0.2.1 233.252.0.8 16300008 20 0x0 e12
5010 192.0.2.1 233.252.0.10 16300010 20 0x0 e12

Switch:1# show isis spbm ip-multicast-route vsn-isid 5010 detail
-----
SPBM IP-MULTICAST ROUTE INFO - TYPE : SNOOP , VLAN ID : 501, VSN-ISID : 5010
-----
Source Group Data ISID BVLAN NNI Rcvrs UNI Rcvrs Source-BEB
-----
192.0.2.1 233.252.0.1 16300001 10 1/4,MLT-35 V501:9/32-9/33 e12
192.0.2.1 233.252.0.3 16300002 20 - V501:9/32-9/33 e12
192.0.2.1 233.252.0.5 16300003 10 1/4,MLT-35 V501:9/32-9/33 e12
192.0.2.1 233.252.0.7 16300004 20 - V501:9/32-9/33 e12
192.0.2.1 233.252.0.9 16300005 10 1/4,MLT-35 V501:9/32-9/33 e12
192.0.2.1 233.252.0.2 16300006 20 - V501:9/32-9/33 e12
192.0.2.1 233.252.0.4 16300007 10 1/4,MLT-35 V501:9/32-9/33 e12
192.0.2.1 233.252.0.6 16300008 20 - V501:9/32-9/33 e12
192.0.2.1 233.252.0.8 16300009 10 1/4,MLT-35 V501:9/32-9/33 e12
192.0.2.1 233.252.0.10 16300010 20 - V501:9/32=9/33 e12
-----
Total Number of SPBM IP MULTICAST ROUTE Entries: 10
-----

```

Variable definitions

Use the data in the following table to use the `show isis spbm ip-multicast-route` command.

Variable	Value
all	Displays all IP Multicast over Fabric Connect route information.
detail	Displays detailed IP Multicast over Fabric Connect route information.

Table continues...

Variable	Value
group {A.B.C.D} source {A.B.C.D}	Displays information on the group IP address for the IP Multicast over Fabric Connect route. If you select source it will also display the source IP address.
vlan <0–4084>	Displays IP Multicast over Fabric Connect route information by VLAN.
vrf WORD<1–16>	Displays IP Multicast over Fabric Connect route information by VRF.
vsn-isid <1–16777215>	Displays IP Multicast over Fabric Connect route information by I-SID.

Use the data in the following table to use the `show isis spb-mcast-summary` command.

Variable	Value
host-name WORD<0–255>	Displays the IP Multicast over Fabric Connect summary for a given host-name.
lspid <xxxx.xxxx.xxxx.xx-xx>	Displays the IP Multicast over Fabric Connect summary for a given LSP ID.

Job aid

The following table describes the fields for the `show isis spbm ip-multicast-route all` command.

Parameter	Description
Type	Specifies the type of interface. The options include: <ul style="list-style-type: none"> • routed— For IP Shortcuts and Layer 3 VSNs. • snoop— For Layer 2 VSNs.
VrfName	Specifies the VRF name of the interface.
Vlan Id	Specifies the VLAN ID of the interface.
Source	Specifies the group IP address for the IP Multicast over Fabric Connect route.
Group	Specifies the group IP address for the IP Multicast over Fabric Connect route.
VSN-ISID	Specifies the VSN I-SID for Layer 2 VSNs and Layer 3 VSNs. Specifies the GRT for IP Shortcuts with IP Multicast over Fabric Connect because IP Shortcuts IP Multicast over Fabric Connect does not use a VSN I-SID.
Data ISID	Specifies the data I-SID for the IP Multicast over Fabric Connect route. After a BEB receives IP multicast data from a sender, the BEB allocates a

Table continues...

Parameter	Description
	data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
BVLAN	Specifies the B-VLAN for the IP Multicast over Fabric Connect route.
Source-BEB	Specifies the source BEB for the IP Multicast over Fabric Connect route.

The following table describes the fields for the `show isis spbm ip-multicast-route vsn-
isid` command.

Parameter	Description
Source	Specifies the group IP address for the IP Multicast over Fabric Connect route.
Group	Specifies the group IP address for the IP Multicast over Fabric Connect route.
Data ISID	Specifies the data I-SID for the IP Multicast over Fabric Connect route. After a BEB receives the IP Multicast over Fabric Connect data from a sender, the BEB allocates a data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
BVLAN	Specifies the B-VLAN for the IP Multicast over Fabric Connect route.
Source-BEB	Specifies the source BEB for the IP Multicast over Fabric Connect route.

The following table describes the fields for the `show isis spbm ip-multicast-route vsn-
isid <1-16777215> detail` command.

Parameter	Description
Source	Specifies the group IP address for the IP multicast route.
Group	Specifies the group IP address for the IP multicast route.
Data ISID	Specifies the data I-SID for the IP multicast route. After a BEB receives IP multicast data from a sender, the BEB allocates a data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group

Table continues...

Parameter	Description
	IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
BVLAN	Specifies the B-VLAN for the IP multicast route.
NNI Rcvrs	Specifies the NNI receivers.
UNI Rcvrs	Specifies the UNI receivers.
Source-BEB	Specifies the source BEB for the IP multicast route.

The following table describes the fields for the `show isis spb-mcast-summary` command.

Parameter	Description
SCOPE I-SID	Specifies the scope I-SID. Layer 2 VSN and Layer 3 VSN each require a scope I-SID.
SOURCE ADDRESS	Specifies the group IP address for the IP Multicast over Fabric Connect route.
GROUP ADDRESS	Specifies the group IP address for the IP Multicast over Fabric Connect route.
DATA I-SID	Specifies the data I-SID for the IP Multicast over Fabric Connect route. After a BEB receives the IP Multicast over Fabric Connect data from a sender, the BEB allocates a data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
BVID	Specifies the Backbone VLAN ID associated with the SPBM instance.
LSP FRAG	Specifies the LSP fragment number.
HOST NAME	Specifies the host name listed in the LSP, or the system name if the host is not configured.

Viewing IGMP information for Layer 2 VSN multicast

Use the following commands to display IGMP information.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display information about the interfaces where IGMP is enabled:

```
show ip igmp interface [gigabitethernet {slot/port[/sub-port]}[-slot/
port[/sub-port]][,...]] [vlan <1-4059>[vrf WORD<1-16>] [vrfrids
WORD<0-512>]
```

Ensure that the output displays `snoop-spb` under `MODE`.

3. Display information about the IGMP cache:

```
show ip igmp cache [vrf WORD<1-16>][vrfids WORD<0-512>]
```

4. Display information about the IGMP group:

```
show ip igmp group [count][group {A.B.C.D}][member-subnet {A.B.C.D/X}][vrf WORD<1-16>][vrfids WORD<0-512>]
```

5. Display information about the IGMP sender:

```
show ip igmp sender [count][group {A.B.C.D}][member-subnet {A.B.C.D/X}][vrf WORD<1-16>][vrfids WORD<0-512>]
```

6. Display information about IGMP snoop-trace information:

```
show ip igmp snoop-trace [group {A.B.C.D}][source {A.B.C.D}][vrf WORD<1-16>][vrfids WORD<0-512>]
```

Example

```
Switch:#enable
Switch:1#show ip igmp interface

=====
                          IgmP Interface - GlobalRouter
=====
IF          QUERY      OPER      QUERY      WRONG      LASTMEM
INTVL      STATUS  VERS.  VERS  QUERIER    MAXRSPT  QUERY  JOINS  ROBUST  QUERY  MODE
-----
V100      125      activ  2      2  0.0.0.0    100     0     0     2     10     snoop-spb

1 out of 1 entries displayed

Switch:1(config)#show ip igmp interface vlan 1

=====
                          Vlan Ip IgmP
=====
VLAN QUERY  QUERY  ROBUST  VERSION  LAST  PROXY  SNOOP  SSM  FAST  FAST
ID   INTVL  MAX    RESP    QUERY  MEMB  SNOOP  SNOOP  SNOOP  LEAVE  LEAVE
      INTVL  RESP   ADDR    QUERY  ENAB  ENAB  ENAB  ENAB  ENAB  ENAB  PORTS
-----
1     125    100    2       2       10   false false false false

VLAN SNOOP  SNOOP      DYNAMIC  COMPATIBILITY  EXPLICIT
ID   QUERIER  QUERIER    DOWNGRADE  MODE           HOST
      ENAB  ADDR      VERSION    MODE           TRACKING
-----
1     false  0.0.0.0    enable     disable        disable

Switch:1# show ip igmp sender

=====
                          IGMP Sender - GlobalRouter
=====
GRPADDR      IFINDEX  MEMBER      PORT/  MLT  STATE
-----
233.252.0.1  Vlan 501  192.2.0.1   9/5    NOTFILTERED
233.252.0.2  Vlan 501  192.2.0.1   9/5    NOTFILTERED
```

```

233.252.0.3   Vlan 501  192.2.0.1  9/5   NOTFILTERED
233.252.0.4   Vlan 501  192.2.0.1  9/5   NOTFILTERED
233.252.0.5   Vlan 501  192.2.0.1  9/5   NOTFILTERED
233.252.0.6   Vlan 501  192.2.0.1  9/5   NOTFILTERED
233.252.0.7   Vlan 501  192.2.0.1  9/5   NOTFILTERED
233.252.0.8   Vlan 501  192.2.0.1  9/5   NOTFILTERED
233.252.0.9   Vlan 501  192.2.0.1  9/5   NOTFILTERED
233.252.0.10  Vlan 501  192.2.0.1  9/5   NOTFILTERED
  
```

10 out of 10 entries displayed

Switch:1# show ip igmp group

```

=====
IGMP Group - GlobalRouter
=====
GRPADDR      INPORT      MEMBER      EXPIRATION  TYPE
-----
233.252.0.1  V501-9/16  192.2.0.1  204         Dynamic
233.252.0.2  V501-9/16  192.2.0.1  206         Dynamic
233.252.0.3  V501-9/16  192.2.0.1  206         Dynamic
233.252.0.4  V501-9/16  192.2.0.1  207         Dynamic
233.252.0.5  V501-9/16  192.2.0.1  204         Dynamic
233.252.0.6  V501-9/16  192.2.0.1  209         Dynamic
233.252.0.7  V501-9/16  192.2.0.1  206         Dynamic
233.252.0.8  V501-9/16  192.2.0.1  206         Dynamic
233.252.0.9  V501-9/16  192.2.0.1  211         Dynamic
233.252.0.10 V501-9/16  192.2.0.1  207         Dynamic
  
```

10 out of 10 group Receivers displayed

Total number of unique groups 10

Switch:1# show ip igmp sender

```

=====
IGMP Sender - GlobalRouter
=====
GRPADDR      IFINDEX     MEMBER      PORT/      STATE
              MLT
-----
233.252.0.1  Vlan 501   192.2.0.1  spb        NOTFILTERED
233.252.0.2  Vlan 501   192.2.0.1  spb        NOTFILTERED
233.252.0.3  Vlan 501   192.2.0.1  spb        NOTFILTERED
233.252.0.4  Vlan 501   192.2.0.1  spb        NOTFILTERED
233.252.0.5  Vlan 501   192.2.0.1  spb        NOTFILTERED
233.252.0.6  Vlan 501   192.2.0.1  spb        NOTFILTERED
233.252.0.7  Vlan 501   192.2.0.1  spb        NOTFILTERED
233.252.0.8  Vlan 501   192.2.0.1  spb        NOTFILTERED
233.252.0.9  Vlan 501   192.2.0.1  spb        NOTFILTERED
233.252.0.10 Vlan 501   192.2.0.1  spb        NOTFILTERED
  
```

10 out of 10 entries displayed

Switch:1# show ip igmp snoop-trace

Switch:1#show ip igmp snoop-trace

```

=====
Snoop Trace - GlobalRouter
=====
GROUP      SOURCE      IN  IN  OUT  OUT  TYPE
-----
  
```

ADDRESS	ADDRESS	VLAN	PORT	VLAN	PORT	
233.252.0.1	192.2.0.1	501	spb	501	1/7,1/9	NETWORK
233.252.0.2	192.2.0.1	501	spb	501	1/7,1/9	NETWORK
233.252.0.3	192.2.0.1	501	spb	501	1/7,1/9	NETWORK
233.252.0.4	192.2.0.1	501	spb	501	1/7,1/9	NETWORK
233.252.0.5	192.2.0.1	501	spb	501	1/7,1/9	NETWORK
233.252.0.6	192.2.0.1	501	spb	501	1/7,1/9	NETWORK
233.252.0.7	192.2.0.1	501	spb	501	1/7,1/9	NETWORK
233.252.0.8	192.2.0.1	501	spb	501	1/7,1/9	NETWORK
233.252.0.9	192.2.0.1	501	spb	501	1/7,1/9	NETWORK
233.252.0.10	192.2.0.1	501	spb	501	1/7,1/9	NETWORK

Variable definitions

Use the data in the following table to use the **show ip igmp interface** command.

Variable	Value
gigabitethernet {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.
vlan <1-4059>	Specifies the VLAN.
vrf WORD<1-16>	Specifies the VRF by name.
vrfids WORD<0-512>	Specifies the VRF by VRF ID.

Use the data in the following table to use the **show ip igmp cache** command.

Variable	Value
vrf WORD<1-16>	Specifies the VRF by name.
vrfids WORD<0-512>	Specifies the VRF by VRF ID.

Use the data in the following table to use the **show ip igmp group** command.

Variable	Value
count	Specifies the number of entries.
group {A.B.C.D}	Specifies the group address.
member-subnet {A.B.C.D/X}	Specifies the IP address and network mask.
vrf WORD<1-16>	Displays the multicast route configuration for a particular VRF by name.
vrfids WORD<0-512>	Displays the multicast route configuration for a particular VRF by VRF ID.

Use the data in the following table to use the **show ip igmp sender** command.

Variable	Value
count	Specifies the number of entries.
group {A.B.C.D}	Specifies the group address.
member-subnet {A.B.C.D/X}	Specifies the IP address and network mask.
vrf WORD<1–16>	Displays the multicast route configuration for a particular VRF by name.
vrfids WORD<0–512>	Displays the multicast route configuration for a particular VRF by VRF ID.

Use the data in the following table to use the `show ip igmp snoop-trace` command.

Variable	Value
group {A.B.C.D}	Specifies the group address.
source {A.B.C.D}	Specifies the source address.
vrf WORD<1–16>	Displays the multicast route configuration for a particular VRF by name.
vrfids WORD<0–512>	Displays the multicast route configuration for a particular VRF by VRF ID.

Job aid

The following table describes the fields for the `show ip igmp interface` command.

Parameter	Description
IF	Indicates the interface where IGMP is configured.
QUERY INTVL	Indicates the frequency at which IGMP host query packets transmit on this interface.
STATUS	Indicates the activation of a row, which activates IGMP on the interface. The destruction of a row disables IGMP on the interface.
VERS.	Indicates the version of IGMP that runs on this interface. This object configures a router capable of running either version. For IGMP to function correctly, you must configure all routers on a LAN to run the same version of IGMP.
OPER VERS	Indicates the operational version of IGMP.
QUERIER	Indicates the address of the IGMP Querier on the IP subnet to which this interface attaches.
QUERY MAXRSPT	Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.
WRONG QUERY	Indicates the number of queries received where the IGMP version does not match the interface version.

Table continues...

Parameter	Description
	You must configure all routers on a LAN to run the same version of IGMP. If queries are received with the wrong version, a configuration error occurs.
JOINS	Indicates the number of times this interface added a group membership.
ROBUST	Indicates the robustness variable, which you can configure for the expected packet loss on a subnet. If you expect packet loss on a subnet, increase the robustness variable.
LASTMEM QUERY	Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This variable does not apply to IGMPv1.
MODE	Indicates the protocol configured on the VLAN added. If routed-spb displays in the MODE column, then IP Multicast over Fabric Connect is enabled on the Layer 3 VSN or for IP shortcuts. If snoop-spb displays in the MODE column, then IGMP is enabled on a VLAN with an associated I-SID (Layer 2 VSN).

The following table describes the fields for the `show ip igmp interface vlan` command.

Parameter	Description
VLAN ID	Identifies the VLAN where IGMP is configured.
QUERY INTVL	Indicates the frequency at which IGMP host query packets transmit on this interface.
QUERY MAX RESP	Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.
ROBUST	Indicates the robustness variable, which you can configure for the expected packet loss on a subnet. If you expect packet loss on a subnet, increase the robustness variable.
VERSION	Indicates the version of IGMP that runs on this interface. This object configures a router capable of running either version. For IGMP to function correctly, you must configure all routers on a LAN to run the same version of IGMP.
LAST MEMB QUERY	Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in

Table continues...

Parameter	Description
	response to leave group messages, and is also the amount of time between group specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This variable does not apply to IGMPv1.
PROXY SNOOP ENABLE	Indicates if proxy snoop is enabled on the interface.
SNOOP ENABLE	Indicates if snoop is enabled on the interface.
SSM SNOOP ENABLE	Indicates if SSM snoop is enabled on the interface.
FAST LEAVE ENABLE	Indicates if fast leave mode is enabled on the interface.
FAST LEAVE PORTS	Indicates the set of ports that are enabled for fast leave.
VLAN ID	Identifies the VLAN where IGMP is configured.
SNOOP QUERIER ENABLE	Indicates if the IGMP Layer 2 Querier feature is enabled.
SNOOP QUERIER ADDRESS	Indicates the IP address of the IGMP Layer 2 Querier.
DYNAMIC DOWNGRADE VERSION	Indicates if the dynamic downgrade feature is enabled.
COMPATIBILITY MODE	Indicates if compatibility mode is enabled.
EXPLICIT HOST TRACKING	Indicates if explicit host tracking is enabled to track all the source and group members.

The following table describes the fields for the `show ip igmp cache` command.

Parameter	Description
GRPADDR	Indicates the multicast group address (Class D) that others want to join. Many incoming ports can use the same group address.
INTERFACE	Indicates the physical interface or a logical interface (VLAN), which received group reports from various sources.
LASTREPORTER	Indicates the IP address of the source of the last membership report received for this IP multicast group address on this interface. If the interface does not receive a membership report, this object uses the value 0.0.0.0.
EXPIRATION	Indicates the minimum amount of time that remains before this entry ages out.

Table continues...

Parameter	Description
V1HOSTIMER	Indicates the time that remains until the local router assumes that no IGMPv1 members exist on the IP subnet attached to this interface.
TYPE	Indicates whether the entry is learned dynamically or is added statically.
STATICPORTS	Indicates the list of statically-defined ports.

The following table describes the fields for the **show ip igmp group** command.

Parameter	Description
GRPADDR	Indicates the multicast group address (Class D) that others want to join. Many incoming ports can use the same group address.
INPORT	Indicates the physical interface or a logical interface (VLAN), which received group reports from various sources.
MEMBER	Indicates the IP address of a source that sent a group report to join this group.
EXPIRATION	Indicates the minimum amount of time that remains before this entry ages out.
TYPE	Indicates whether the entry is learned dynamically or is added statically.

The following table describes the fields for the **show ip igmp sender** command.

Parameter	Description
GRPADDR	Indicates the IP multicast address.
IFINDEX	Indicates the interface index number.
MEMBER	Indicates the IP address of the host.
PORT/MLT	Indicates the IGMP sender ports.
STATE	Indicates if a sender exists because of an IGMP access filter. Options include filtered and nonfiltered.

The following table describes the fields for the **show ip igmp snoop-trace** command.

Parameter	Description
GROUP ADDRESS	Indicates the IP multicast group address for which this entry contains information.
SOURCE ADDRESS	Indicates the source of the multicast traffic.
IN VLAN	Indicates the incoming VLAN ID.
IN PORT	Indicates the incoming port number.
OUT VLAN	Indicates the outgoing VLAN ID.

Table continues...

Parameter	Description
OUT PORT	Indicates the outgoing port number.
TYPE	Indicates where the stream is learned. ACCESS indicates the stream is learned on UNI ports. NETWORK indicates the stream is learned over the SPBM network.

Viewing TLV information for Layer 2 VSN IP Multicast over Fabric Connect

Use the following commands to check TLV information.

For Layer 2 VSN with IP multicast over Fabric Connect, TLV 185 on the BEB where the source is located, displays the multicast source and group addresses and has the Tx bit set. Each multicast group has its own unique data I-SID with a value between 16,000,000 to 16,512,000. TLV 144 on the BEB bridge, where the sender is located, has the Tx bit set. All BEB bridges, where a receiver exists, have the Rx bit set.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display IS-IS Link State Database information by Type-Length-Value (TLV):

```
show isis lsdb tlv <1-236> [sub-tlv <1-3>][detail]
```

3. Display IS-IS Link State Database information by Link State Protocol ID:

```
show isis lsdb lspid <xxxx.xxxx.xxxx.xx-xx>tlv <1-236> [sub-tlv <1-3>] [detail]
```

Example

```
Switch:1# show isis lsdb tlv 185 detail
```

```
=====
                ISIS LSDB (DETAIL)
=====
Level-1LspID: 000c.f803.83df.00-00 SeqNum: 0x000001ae Lifetime: 898
Chksum: 0xcebe PDU Length: 522
Host_name: Switch
Attributes: IS-Type 1
TLV:185 SPBM IPVPN :
VSN ISID:5010
BVID :10
    Metric:0
    IP Source Address: 192.0.2.1
    Group Address : 233.252.0.1
    Data ISID : 16300001
    TX : 1
    Metric:0
    IP Source Address: 192.0.2.1
    Group Address : 233.252.0.3
    Data ISID : 16300003
    TX : 1
    Metric:0
    IP Source Address: 192.0.2.1
    Group Address : 233.252.0.5
    Data ISID : 16300005
    TX : 1
```

IP Multicast over Fabric Connect services configuration

```
Metric:0
IP Source Address: 192.0.2.1
Group Address : 233.252.0.7
Data ISID : 16300007
TX : 1
Metric:0
IP Source Address: 192.0.2.1
Group Address : 233.252.0.9
Data ISID : 16300009
TX : 1
VSN ISID:5010
BVID :20
Metric:0
IP Source Address: 192.0.2.1
Group Address : 233.252.0.2
Data ISID : 16300002
TX : 1
Metric:0
IP Source Address: 192.0.2.1
Group Address : 233.252.0.4
Data ISID : 16300004
TX : 1
Metric:0
IP Source Address: 192.0.2.1
Group Address : 233.252.0.6
Data ISID : 16300006
TX : 1
Metric:0
IP Source Address: 192.0.2.1
Group Address : 233.252.0.8
Data ISID : 16300008
TX : 1
Metric:0
IP Source Address: 192.0.2.1
Group Address : 233.252.0.10
Data ISID : 16300010
TX : 1
```

```
Switch:1# show isis lsdb lspid 000c.f803.83df.00-05 tlv 144 detail
```

```
=====
ISIS LSDB (DETAIL)
=====
```

```
-----
Level-1 LspID: 000c.f803.83df.00-00 SeqNum: 0x00000477 Lifetime: 903
Chksum: 0x200b PDU Length: 522
Host name: Switch
Attributes: IS-Type 1
  Instance: 0
  Metric: 0
  B-MAC: 03-00-00-00-00-00
  BVID:10
  Number of ISID's:5
    16000001 (Tx),16000003 (Tx),16000005 (Tx),16000007 (Tx),16000009 (Tx)
  Instance: 0
  Metric: 0
  B-MAC: 03-00-00-00-00-00
  BVID:20
  Number of ISID's:5
    16000002 (Tx),16000004 (Tx),16000006 (Tx),16000008 (Tx),16000010 (Tx)
```

Variable definitions

Use the data in the following table to use the `show isis lsdb` command.

Variable	Value
detail	Displays detailed information about the IS-IS Link State database.
level {1, 12, 112}	Displays information on the IS-IS level. The IEEE 802.1aq standard currently only defines the use of one hierarchy, Level 1. Level 2 and combined Level 1 and 2 (112) function is disabled.
local	Displays information on the local LSDB.
lspid <xxxx.xxxx.xxxx.xx-xx>	Specifies information about the IS-IS Link State database by LSP ID.
sub-tlv <1-3>	Specifies information about the IS-IS Link State database by sub-TLV.
sysid <xxxx.xxxx.xxxx>	Specifies information about the IS-IS Link State database by System ID.
tlv <1-236>	Specifies information about the IS-IS Link State database by TLV.

Job aid

The following table describes the fields for the `show isis lsdb` command.

Parameter	Description
LSP ID	Indicates the LSP ID assigned to external IS-IS routing devices.
LEVEL	Indicates the level of the external router: 11, 12, or 112.
LIFETIME	Indicates the maximum age of the LSP. If the max-lsp-gen-interval is set to 900 (default) then the lifetime value begins to count down from 1200 seconds and updates after 300 seconds if connectivity remains. If the timer counts down to zero, the counter adds on an additional 60 seconds, and then the LSP for that router is lost. This situation happens because of the zero age lifetime, which is detailed in the RFC standards.
SEQNUM	Indicates the LSP sequence number. This number changes each time the LSP is updated.
CKSUM	Indicates the LSP checksum. The checksum is an error checking mechanism used to verify the validity of the IP packet.
HOST-NAME	Indicates the host-name.

Layer 2 VSN configuration using EDM

This section provides procedures to configure Layer 2 Virtual Services Networks (VSNs) using Enterprise Device Manager (EDM).

Viewing the IGMP interface table

Use the Interface tab to view the IGMP interface table. When an interface does not use an IP address, it does not appear in the IGMP table.

Procedure

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

Interface field descriptions

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


Name	Description
IfIndex	Shows the interface where IGMP is enabled.
QueryInterval	Configures the frequency (in seconds) at which the interface transmits IGMP host query packets. The default is 125.
Status	Shows the IGMP row status. If an interface uses an IP address and PIM-SM is enabled, the status is active. Otherwise, it is notInService.
Version	Configures the version of IGMP (1, 2, or 3) that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. The default is version 2.
OperVersion	Shows the version of IGMP that currently runs on this interface.
Querier	Shows the address of the IGMP querier on the IP subnet to which this interface attaches.
QueryMaxResponseTime	<p>Configures the maximum response time (in tenths of a second) advertised in IGMPv2 general queries on this interface. You cannot configure this value for IGMPv1.</p> <p>Smaller values allow a router to prune groups faster. The default is 100 tenths of a second (equal to 10 seconds.)</p> <p> Important: You must configure this value lower than the QueryInterval.</p>
WrongVersionQueries	Shows the number of queries received with an IGMP version that does not match the interface. You must configure all routers on a LAN to run the same version of IGMP. If the interface receives queries with the wrong version, this value indicates a version mismatch.

Table continues...

Name	Description
Joins	Shows the number of times this interface added a group membership, which is the same as the number of times an entry for this interface is added to the cache table. This number gives an indication of the amount of IGMP activity over time.
Robustness	<p>Tunes for the expected packet loss of a network. This value is equal to the number of expected query packet losses for each serial query interval, plus 1. If you expect a network to lose query packets, increase the robustness value.</p> <p>The default value of 2 means that the switch drops one query for each query interval without the querier aging out.</p>
LastMembQueryIntvl	<p>Configures the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages. This value is also the time between group-specific query messages. You cannot configure this value for IGMPv1.</p> <p>Decrease the value to reduce the time to detect the loss of the last member of a group. The range is from 0–255 and the default is 10 tenths of second. It is recommended that you configure this parameter to values greater than 3. If you do not need a fast leave process, you can configure values greater than 10. (The value 3 is equal to 0.3 seconds and 10 is equal to 1 second.)</p>
OtherQuerierPresent Timeout	Shows the length of time that must pass before a multicast router determines that no other querier exists. If the local router is the querier, the value is 0.
FlushAction	<p>Configures the flush action to one of the following:</p> <ul style="list-style-type: none"> • none • flushGrpMem • flushMrouter • flushSender
RouterAlertEnable	<p>Instructs the router to ignore IGMP packets that do not contain the router alert IP option. If you disable this variable (default configuration), the router processes IGMP packets regardless of the status of the router alert IP option.</p> <p>! Important:</p> <p>To maximize network performance, configure this parameter according to the version of IGMP currently in use.</p> <ul style="list-style-type: none"> • IGMPv1—Disable • IGMPv2—Enable • IGMPv3—Enable
SsmSnoopEnable	Enables SSM snoop.
SnoopQuerierEnable	Enables IGMP Layer 2 Querier.

Table continues...

Name	Description
SnoopQuerierAddr	Specifies the pseudo address of the IGMP snoop querier.
ExplicitHostTrackingEnable	Enables or disables IGMPv3 to track hosts for each channel or group. The default is disabled. You must select this field if you want to use fast leave for IGMPv3.
McastMode	Indicates the protocol configured on the VLAN. <ul style="list-style-type: none"> • snoop — Indicates IGMP snooping is enabled on a VLAN. • snoop-spb — Indicates IGMP is enabled on a VLAN with an associated I-SID (IP multicast over Fabric Connect for a Layer 2 VSN). • pim — Indicates PIM is enabled. • routed-spb — Indicates IP multicast over Fabric Connect is enabled on the Layer 3 VSN or for IP Shortcuts.

Configuring IP Multicast over Fabric Connect on a Layer 2 VSN

Use this procedure to enable IP Multicast over Fabric Connect for a Layer 2 VSN. With Layer 2 VSN IP Multicast over Fabric Connect, multicast traffic remains in the same Layer 2 VSN across the SPBM cloud.

No explicit configuration exists for a Layer 2 VSN. After you configure IP IGMP snooping on a VLAN that has an I-SID configured, the device enables that VLAN for IP Multicast over Fabric Connect services.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must create the C-VLANs and add slots/ports.
- You must enable IP Multicast over Fabric Connect globally.

About this task

SPBM supports enabling IGMP snooping on a C-VLAN, but it does not support enabling PIM on a C-VLAN. If you enable IGMP snooping on a C-VLAN, then its operating mode is Layer 2 VSN with IGMP support on the access networks for optimized forwarding of IP multicast traffic in a bridged network.

This switch only supports IPv4 multicast traffic.

Procedure

1. In the navigation pane, expand the **Configuration > VLAN** folders.
2. Click **VLANs**.
3. Click the **Basic** tab.
4. Select a VLAN.
5. Click **IP**.

6. Select the **IGMP** tab.
7. Select the **SnoopEnable** check box.
8. **(Optional)** Select the **SsmSnoopEnable** check box, if you use IGMP version 3.
9. **(Optional)** Select the **ProxySnoopEnable** check box.
10. **(Optional)** If you want to enable IGMP version 3, select version3 in the **Version** check box.
You must enable SSM snoop before you configure IGMP version 3 and both ssm-snoop and snooping must be enabled for IGMPv3.
11. If you want to enable IGMP version 2, select version2 in the **Version** check box.
For IGMP Snooping, ensure that the IGMP version used by multicast hosts and other devices in the network is the same as the IGMP version configured on the IGMP Snooping VLAN, or that you enable compatibility mode.
12. **(Optional)** If you want to enable snoop querier, select **SnoopQuerierEnable**.
13. **(Optional)** If you want to configure an address for IGMP queries, enter the IP address in **SnoopQuerierAddr**.

*** Note:**

This step is not always required. The IGMP Querier on the BEB uses a source address 0.0.0.0 by default. When you do not configure this, a BEB sends IGMP queries on the UNI ports with 0.0.0.0 as the source IP address. Some Layer 2 edge switches do not support a 0.0.0.0 querier. You can use a fictitious IP address as the querier address, and use the same address on all BEBs in the network.

14. Click **Apply**.

Layer 2 VSN configuration examples

Layer 2 VSN with IP Multicast over Fabric Connect configuration example

The example below shows the configuration steps to enable IP Multicast over Fabric Connect support on C-VLAN 1001 that is part of a Layer 2 VSN, including the querier address.

```
enable
configure terminal

ISIS SPBM CONFIGURATION

router isis
spbm 1 multicast enable

VLAN CONFIGURATION

interface vlan 9
ip igmp snooping
ip igmp snoop-querier-addr 192.0.2.201
exit
```

When using IGMPv3, the configuration is:

```
enable
configure terminal

ISIS SPBM CONFIGURATION

router isis
spbm 1 multicast enable

VLAN CONFIGURATION

interface vlan 19
ip igmp snooping
ip igmp version 3
ip igmp ssm-snoop
ip igmp snoop-querier-addr 192.0.2.201
exit
```

*** Note:**

You must enable SSM snoop before you configure IGMP version to version 3, and you must enable both `ssm-snoop` and `snooping` for IGMPv3.

*** Note:**

You must configure basic SPBM and IS-IS infrastructure.

IP Shortcuts configuration

This section provides fundamentals concepts for IP Shortcuts configuration. For more information on IP Shortcuts basic configuration, see *Configuring Fabric Layer 3 Services*.

IP Multicast over Fabric Connect within the GRT

IP Multicast over Fabric Connect within the GRT enables you to exchange IP multicast traffic with all or a subset of VLANs that are in the Global Routing Table (GRT). This restriction is called the *scope level*, which IP Multicast over Fabric Connect uses to constrain the multicast streams within the level in which they originate. For example, if a sender transmits a multicast stream to a BEB on a VLAN that is part of the GRT with IP Multicast over Fabric Connect enabled, only receivers that are part of the same GRT can receive that stream.

Applications that can use IP Multicast over Fabric Connect within the GRT include: Video surveillance, TV/Video/Ticker/Image distribution, VX-LAN.

Both **IP Shortcuts** and **IP Multicast over Fabric Connect within the GRT** use the GRT for the scope level to constrain multicast streams. However, they are separate features that work independently from each other.

! Important:

You do not have to enable IP Shortcuts to support IP Multicast over Fabric Connect within the GRT.

With IP Multicast over Fabric Connect within the GRT, routing of IP multicast traffic is allowed within the subset of VLANs in the GRT that have IP Multicast over Fabric Connect enabled. When you enable IP Multicast over Fabric Connect on a VLAN, the VLAN automatically becomes a multicast routing interface.

You must enable `ip spb-multicast` on each of the VLANs within the GRT that need to support IP multicast traffic. Enable IP Multicast over Fabric Connect on all VLANs to which IP multicast senders and receivers attach. IP Multicast over Fabric Connect is typically configured only on BEBs.

*** Note:**

If no IP interface exists on the VLAN, then you create one. (The IP interface must be in the same subnet as the IGMP hosts that connect to the VLAN).

I-SIDs

Unlike IP Shortcuts with unicast, a data I-SID (for mac-in-mac encapsulation of the multicast traffic) is required for IP Multicast over Fabric Connect within the GRT. When the multicast stream reaches the BEB, the BEB assigns a data I-SID to the stream. The data I-SID uses Tx/Rx bits to signify whether the BEB uses the I-SID to transmit, receive, or both transmit and receive data on that I-SID.

Unlike Layer 2 VSNs and Layer 3 VSNs, IP Multicast over Fabric Connect within the GRT does not have a scope I-SID to determine the scope of the multicast traffic. Instead the scope is the Global Routing Table.

TLVs

The scope and data I-SID information is propagated through the SPBM cloud using IS-IS Link State Packets (LSPs), which carry TLV updates, and result in the multicast tree creation for that stream. For IP Multicast over Fabric Connect within the GRT, the LSPs carry I-SID information and information about where IP multicast stream senders and receivers exist using TLV 144 and TLV 186.

IGMP

After you configure `ip spb-multicast enable`, you cannot enable IGMP, IGMP Snooping, or IGMP proxy on the interface. If you try to enable IGMP Snooping or proxy on any interface where IP Multicast over Fabric Connect is enabled, an error message appears.

After you configure `ip spb-multicast enable` on each of the VLANs within the GRT that need to support IP multicast traffic, any IGMP functions required for IP Multicast over Fabric Connect within the GRT are automatically enabled. You do not need to configure anything IGMP related.

DvR

When you enable `ip spb-multicast` on the Controller nodes, the configuration is automatically pushed to all the Leaf nodes within the domain.

For more information on DvR, see *Configuring IPv4 Routing*.

IP Shortcuts configuration using the CLI

This section provides procedures to configure IP Shortcuts using the CLI.

Configuring IP Multicast over Fabric Connect within the GRT

Use this procedure to configure IP Multicast over Fabric Connect within the GRT. The default is disabled.

Note:

- You do not have to enable IP Shortcuts to support IP multicast routing in the GRT using SPBM.
- You cannot enable IP PIM when IP Multicast over Fabric Connect is enabled on the VLAN.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must create the C-VLANs and add slots/ports.
- You must enable IP Multicast over Fabric Connect globally.
- If no IP interface exists on the VLAN, then you create one. (The IP interface must be the same subnet as the IGMP hosts that connect to the VLAN).

About this task

With IP Multicast over Fabric Connect within the GRT, routing of IP multicast traffic is allowed within the subset of VLANs in the GRT that have IP Multicast over Fabric Connect enabled. When you enable IP Multicast over Fabric Connect on a VLAN, the VLAN automatically becomes a multicast routing interface.

You must configure `ip spb-multicast enable` on each of the VLANs within the GRT that need to support IP multicast traffic. The default is disabled. After you enable IP Multicast over Fabric Connect on each of the VLANs within the GRT that need to support IP multicast traffic, any IGMP functions required for IP Multicast over Fabric Connect within the GRT are automatically enabled. You do not need to configure anything IGMP related.

If you only want to use IP Multicast over Fabric Connect, you do not need to enable the Layer 3 VSN or redistribute unicast routes into or out of IS-IS. IP Multicast over Fabric Connect routing does not depend on unicast routing, which allows for you to more easily migrate from a PIM environment to IP Multicast over Fabric Connect. You can migrate a PIM environment to IP Multicast over Fabric Connect first and then migrate unicast separately or not at all.

The switch only supports IPv4 addresses with IP Multicast over Fabric Connect.

Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
```

```
interface GigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-
port]] [,...]} or interface vlan <1-4059>
```

*** 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. Create an IP interface on the VLAN:

```
ip address <A.B.C.D/X>
```

3. Enable IP Multicast over Fabric Connect:

```
ip spb-multicast enable
```

*** Note:**

After you configure `ip spb-multicast enable`, you cannot enable IGMP, IGMP Snooping, or IGMP proxy on the interface. If you try to enable IGMP Snooping or proxy on any interface where IP Multicast over Fabric Connect is enabled, an error message appears.

*** Note:**

When you configure `ip spb-multicast enable` on the Controller node of a DvR domain, the configuration is automatically pushed to the Leaf nodes within the domain.

For information on DvR, see *Configuring IPv4 Routing*.

4. **(Optional)** Disable IP Multicast over Fabric Connect:

```
no ip spb-multicast enable
default ip spb-multicast enable
```

5. Ensure IP Multicast over Fabric Connect within the GRT is configured properly:

```
show ip igmp interface
```

If `routed-spb` appears under mode, IP Multicast over Fabric Connect within the GRT is properly enabled on the VLAN.

Example

Enable IP Multicast over Fabric Connect within the GRT:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface vlan 500
Switch:1(config-if)#ip address 192.0.2.1 255.255.255.0
Switch:1(config-if)#ip spb-multicast enable
Switch:1(config)#show ip igmp interface
```

```
=====
                        Igmp Interface - GlobalRouter
=====
IF      QUERY      OPER      QUERY      WRONG      LASTMEM
INTVL  STATUS  VERS.  VERS  QUERIER  MAXRSPT  QUERY  JOINS  ROBUST  QUERY  MODE
=====
```

v500	125	active	2	2	0.0.0.0	100	0	0	2	10	routed-spb
v2000	125	inact	2	2	0.0.0.0	100	0	0	2	10	

Variable definitions

Use the data in the following table to use the **interface vlan** command.

Variable	Value
<1-4059>	Specifies the VLAN ID.

Use the data in the following table to use the **interface GigabitEthernet** 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.

Use the data in the following table to use the **ip address** command.

Variable	Value
<A.B.C.D/X>	Specifies the address and mask.

Configuring the VRF timeout value

Use this procedure to configure the VRF timeout value. The timeout value ages out the sender when there is no multicast stream on the VRF. The default is 210 seconds.

* Note:

You can use this procedure for Layer 3 VSN with IP Multicast over Fabric Connect services and IP Multicast over Fabric Connect for IP Shortcuts.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must create the C-VLANs and add slots/ports.
- You must enable IP Multicast over Fabric Connect globally.

Procedure

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

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

2. Configure the timeout value on the VRF:


```
mvpn fwd-cache-timeout(seconds) <10-86400>
```

3. (Optional) Configure the timeout value to the default value of 210 seconds:

```
no mvpn fwd-cache-timeout
default mvpn fwd-cache-timeout(seconds)
```

Example

Configure the timeout value on the VRF to 500 seconds:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#router vrf green
Switch:1(router-vrf)#mvpn fwd-cache-timeout(seconds) 500
```

Variable definitions

Use the data in the following table to use the **router vrf** command.

Variable	Value
WORD<1-16>	Specifies the VRF name.

Use the data in the following table to use the **mvpn fwd-cache-timeout(seconds)** command.

Variable	Value
<10-86400>	Specifies the timeout value. The default is 210 seconds.

Configuring the Global Routing Table timeout value

Use this procedure to configure the timeout value in the GRT. The timeout value ages out the sender when there are no multicast streams coming from the sender for a specified period of time in seconds. The default timeout value is 210 seconds.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must create the C-VLANs and add slots/ports.
- You must enable IP Multicast over Fabric Connect globally.

Procedure

1. Enter IS-IS Router Configuration mode:

```
enable
configure terminal
router isis
```

2. Configure the IP Multicast over Fabric Connect forward-cache timeout:

```
spbm <1-100> multicast fwd-cache-timeout(seconds) <10-86400>
```

3. **(Optional)** Configure the IP Multicast over Fabric Connect forward-cache timeout to the default value of 210 seconds:

```
default spbm <1-100> multicast fwd-cache-timeout(seconds)
no spbm <1-100> multicast fwd-cache-timeout(seconds)
```

Example

Configure the IP Multicast over Fabric Connect forward-cache timeout to 300:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#router isis
Switch:1(config-isis)#spbm 1 multicast 1 fwd-cache-timeout 300
```

Variable definitions

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

Variable	Value
<1-100>	Specifies the SPBM instance. The switch only supports one instance.
<10-86400>	Specifies the IP Multicast over Fabric Connect forward-cache timeout in seconds. The default is 210 seconds.

Viewing IP Multicast over Fabric Connect within the GRT information

Use the following options to display IP Multicast over Fabric Connect within the GRT information to confirm proper configuration.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display all IP Multicast over Fabric Connect route information:


```
show isis spbm ip-multicast-route [all]
```
3. Display detailed IP Multicast over Fabric Connect route information:


```
show isis spbm ip-multicast-route [detail]
```
4. Display the IP Multicast over Fabric Connect multicast group and source address information:


```
show isis spbm ip-multicast-route [group {A.B.C.D}] [source {A.B.C.D}] [source-beb WORD<0-255>]
```
5. Display summary information for each S, G, V tuple with the corresponding scope, data I-SID, and the host name of the source:

```
show isis spb-mcast-summary [host-name WORD<0-255>][lspid <xxxx.xxxx.xxxx.xx-xx>]
```

Example

Display IP Multicast over Fabric Connect within the GRT information:

```
Switch:1#show isis spbm ip-multicast-route all
```

```
=====
                        SPBM IP-multicast ROUTE INFO ALL
=====
```

Type	VrfName	Vlan	Source	Group	VSN-ISID	Data	ISID	BVLAN	Source-BEB
routed	GRT	501	192.0.2.1	233.252.0.1	5010	16300001	10		e12
routed	GRT	501	192.0.2.1	233.252.0.2	5010	16300002	20		e12
routed	GRT	501	192.0.2.1	233.252.0.3	5010	16300003	10		e12
routed	GRT	501	192.0.2.1	233.252.0.4	5010	16300004	20		e12
routed	GRT	501	192.0.2.1	233.252.0.5	5010	16300005	10		e12
routed	GRT	501	192.0.2.1	233.252.0.6	5010	16300006	20		e12
routed	GRT	501	192.0.2.1	233.252.0.7	5010	16300007	10		e12
routed	GRT	501	192.0.2.1	233.252.0.8	5010	16300008	20		e12
routed	GRT	501	192.0.2.1	233.252.0.9	5010	16300009	10		e12
routed	GRT	501	192.0.2.1	233.252.0.10	5010	16300010	20		e12

```
-----
Total Number of SPBM IP multicast ROUTE Entries: 10
-----
```

```
Switch:1#show isis spbm ip-multicast-route detail
```

```
=====
                        SPBM IP-MULTICAST ROUTE INFO
=====
```

Source	Group	Data	ISID	BVLAN	NNI	Rcvrs	UNI	Rcvrs	Source-BEB
192.0.2.10	233.252.0.1	16300001	10		1/3	V604:9/38			e12
192.0.2.10	233.252.0.2	16300002	20		1/2,1/3	V604:9/38			e12
192.0.2.10	233.252.0.3	16300003	10		1/3	V604:9/38			e12
192.0.2.10	233.252.0.4	16300004	20		1/2,1/3	V604:9/38			e12
192.0.2.10	233.252.0.5	16300005	10		1/3	V604:9/38			e12
192.0.2.10	233.252.0.6	16300006	20		1/2,1/3	V604:9/38			e12
192.0.2.10	233.252.0.7	16300007	10		1/3	V604:9/38			e12
192.0.2.10	233.252.0.8	16300008	20		1/2,1/3	V604:9/38			e12
192.0.2.10	233.252.0.9	16300009	10		1/3	V604:9/38			e12
192.0.2.10	233.252.0.10	16300010	20		1/2,1/3	V604:9/38			e12

```
-----
Total Number of SPBM IP MULTICAST ROUTE Entries: 10
-----
```

```
Switch:1# show isis spb-mcast-summary
```

```
=====
                        SPB multicast - Summary
=====
```

SCOPE	SOURCE	GROUP	DATA	LSP	HOST
I-SID	ADDRESS	ADDRESS	I-SID	BVID	FRAG NAME
GRT	192.0.2.1	233.252.0.1	16300001	10	0x0 e12
GRT	192.0.2.1	233.252.0.3	16300003	10	0x0 e12
GRT	192.0.2.1	233.252.0.5	16300005	10	0x0 e12
GRT	192.0.2.1	233.252.0.7	16300007	10	0x0 e12
GRT	192.0.2.1	233.252.0.9	16300009	10	0x0 e12
GRT	192.0.2.1	233.252.0.2	16300002	20	0x0 e12

```
GRT 192.0.2.1 233.252.0.4 16300004 20 0x0 e12
GRT 192.0.2.1 233.252.0.6 16300006 20 0x0 e12
GRT 192.0.2.1 233.252.0.8 16300008 20 0x0 e12
GRT 192.0.2.1 233.252.0.10 16300010 20 0x0 e12
```

Variable definitions

Use the data in the following table to use the `show isis spbm ip-multicast-route` command.

Variable	Value
all	Displays all IP Multicast over Fabric Connect route information.
detail	Displays detailed IP Multicast over Fabric Connect route information.
group {A.B.C.D} source {A.B.C.D} [source-beb WORD<0–255>]	Displays information on the group IP address for the IP Multicast over Fabric Connect route. If you select source it will also display the source IP address. Specifies the source BEB name.
vlan	Displays IP Multicast over Fabric Connect route information by VLAN.
vrf	Displays IP Multicast over Fabric Connect route information by VRF.
vsn-isid	Displays IP Multicast over Fabric Connect route information by I-SID.

Use the data in the following table to use the `show isis spb-mcast-summary` command.

Variable	Value
host-name WORD<0–255>	Displays the IP Multicast over Fabric Connect summary for a given host-name.
lspid <xxxx.xxxx.xxxx.xx-xx>	Displays the IP Multicast over Fabric Connect summary for a given LSP ID.

Job aid

The following table describes the fields for the `show isis spbm ip-multicast-route all` command.

Parameter	Description
Type	Specifies the type of interface. The options include: <ul style="list-style-type: none"> routed—For GRT and Layer 3 VSN. snoop—For Layer 2 VSN.
VrfName	Specifies the VRF name of the interface.
Vlan Id	Specifies the VLAN ID of the interface.

Table continues...

Parameter	Description
Source	Specifies the group IP address for the IP Multicast over Fabric Connect route.
Group	Specifies the group IP address for the IP Multicast over Fabric Connect route.
VSN-ISID	Specifies the GRT because IP Multicast over Fabric Connect within the GRT does not use a VSN I-SID.
Data ISID	Specifies the data I-SID for the IP Multicast over Fabric Connect route. After a BEB receives IP multicast data from a sender, the BEB allocates a data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
BVLAN	Specifies the B-VLAN for the IP Multicast over Fabric Connect route.
Source-BEB	Specifies the source BEB for the IP Multicast over Fabric Connect route.

The following table describes the fields for the **show isis spbm ip-multicast-route detail** command.

Parameter	Description
Source	Specifies the group IP address for the IP Multicast over Fabric Connect route.
Group	Specifies the group IP address for the IP Multicast over Fabric Connect route.
Data ISID	Specifies the data I-SID for the IP Multicast over Fabric Connect route. After a BEB receives IP multicast data from a sender, the BEB allocates a data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
BVLAN	Specifies the B-VLAN for the IP Multicast over Fabric Connect route.
NNI Rcvrs	Specifies the NNI receivers.
UNI Rcvrs	Specifies the UNI receivers.
Source-BEB	Specifies the source BEB for the IP Multicast over Fabric Connect route.

The following table describes the fields for the **show isis spb-mcast-summary** command.

Parameter	Description
SCOPE I-SID	Specifies the scope I-SID. Layer 2 VSN and Layer 3 VSN each require a scope I-SID.
SOURCE ADDRESS	Specifies the group IP address for the IP Multicast over Fabric Connect route.
GROUP ADDRESS	Specifies the group IP address for the IP Multicast over Fabric Connect route.
DATA I-SID	Specifies the data I-SID for the IP multicast route. After a BEB receives IP multicast data from a sender, the BEB allocates a data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
BVID	Specifies the Backbone VLAN ID associated with the SPBM instance.
LSP FRAG	Specifies the LSP fragment number.
HOST NAME	Specifies the host name listed in the LSP, or the system name if the host is not configured.

Viewing IGMP information for IP multicast over Fabric Connect within the GRT

Use the following commands to display IGMP information.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display information about the interfaces where IGMP is enabled:

```
show ip igmp interface [gigabitethernet {slot/port[/sub-port]}[-slot/
port[/sub-port]][,...]] [vlan <1-4059>] [vrf WORD<1-16>] [vrfids
WORD<0-512>]
```

Ensure that the output displays `routed-spb` under `MODE`.

3. Display information about the IGMP cache:

```
show ip igmp cache [vrf WORD<1-16>] [vrfids WORD<0-512>]
```

4. Display information about the IGMP group:

```
show ip igmp group [count] [group {A.B.C.D}] [member-subnet default|
{A.B.C.D/X}] [vrf WORD<1-16>] [vrfids WORD<0-512>]
```

5. Display information about the IGMP sender:

```
show ip igmp sender [count][group {A.B.C.D}][member-subnet default|
{A.B.C.D/X}][vrf WORD<1-16>][vrfids WORD<0-512>]
```

Example

Display IGMP information for IP multicast over Fabric Connect within the GRT:

```
Switch:#enable
Switch:1#show ip igmp interface

=====
                          Igmp Interface - GlobalRouter
=====
IF          QUERY      OPER          QUERY  WRONG          LASTMEM
INTVL      STATUS  VERS.  VERS  QUERIER  MAXRSPT  QUERY  JOINS  ROBUST  QUERY  MODE
-----
Vl100     125      activ  2     2    0.0.0.0    100   0     0     2     10    routed-spb

1 out of 1 entries displayed

Switch:1(config)#show ip igmp interface vlan 1

=====
                          Vlan Ip Igmp
=====
VLAN QUERY  QUERY  ROBUST  VERSION  LAST  PROXY  SNOOP  SSM  FAST  FAST
ID   INTVL  MAX    RESP    QUERY  MEMB  SNOOP  ENABLE  SNOOP  LEAVE  LEAVE
      RESP  ADDRESS  QUERY  ENABLE  ENABLE  ENABLE  ENABLE  ENABLE  PORTS
-----
1     125    100    2       2       10    false  false  false  false

VLAN SNOOP  SNOOP          DYNAMIC  COMPATIBILITY  EXPLICIT
ID   QUERIER  QUERIER        DOWNGRADE  MODE           HOST
      ENABLE  ADDRESS        VERSION    MODE           TRACKING
-----
1     false   0.0.0.0        enable     disable        disable

Switch:1# show ip igmp sender

=====
                          IGMP Sender - GlobalRouter
=====
GRPADDR          IFINDEX  MEMBER          PORT/
MLT              STATE
-----
233.252.0.1     Vlan 501  192.2.0.1       9/16        NOTFILTERED
233.252.0.2     Vlan 501  192.2.0.1       9/16        NOTFILTERED
233.252.0.3     Vlan 501  192.2.0.1       9/16        NOTFILTERED
233.252.0.4     Vlan 501  192.2.0.1       9/16        NOTFILTERED
233.252.0.5     Vlan 501  192.2.0.1       9/16        NOTFILTERED
233.252.0.6     Vlan 501  192.2.0.1       9/16        NOTFILTERED
233.252.0.7     Vlan 501  192.2.0.1       9/16        NOTFILTERED
233.252.0.8     Vlan 501  192.2.0.1       9/16        NOTFILTERED
233.252.0.9     Vlan 501  192.2.0.1       9/16        NOTFILTERED
233.252.0.10    Vlan 501  192.2.0.1       9/16        NOTFILTERED

10 out of 10 entries displayed

Switch:1# show ip igmp group

=====
                          IGMP Group - GlobalRouter
=====
```

IP Multicast over Fabric Connect services configuration

GRPADDR	INPORT	MEMBER	EXPIRATION	TYPE
233.252.0.1	V501-9/16	192.2.0.1	204	Dynamic
233.252.0.2	V501-9/16	192.2.0.1	206	Dynamic
233.252.0.3	V501-9/16	192.2.0.1	206	Dynamic
233.252.0.4	V501-9/16	192.2.0.1	207	Dynamic
233.252.0.5	V501-9/16	192.2.0.1	204	Dynamic
233.252.0.6	V501-9/16	192.2.0.1	209	Dynamic
233.252.0.7	V501-9/16	192.2.0.1	206	Dynamic
233.252.0.8	V501-9/16	192.2.0.1	206	Dynamic
233.252.0.9	V501-9/16	192.2.0.1	211	Dynamic
233.252.0.10	V501-9/16	192.2.0.1	207	Dynamic

10 out of 10 group Receivers displayed

Total number of unique groups 10

Variable definitions

Use the data in the following table to use the **show ip igmp interface** command.

Variable	Value
gigabitethernet {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.
vlan <1-4059>	Specifies the VLAN.
vrf WORD<1-16>	Specifies the VRF by name.
vrfids WORD<0-512>	Specifies the VRF by VRF ID.

Use the data in the following table to use the **show ip igmp cache** command.

Variable	Value
vrf WORD<1-16>	Specifies the VRF by name.
vrfids WORD<0-512>	Specifies the VRF by VRF ID.

Use the data in the following table to use the **show ip igmp group** command.

Variable	Value
count	Specifies the number of entries.
group {A.B.C.D}	Specifies the group address.
member-subnet {A.B.C.D/X}	Specifies the IP address and network mask.
vrf WORD<1-16>	Displays the multicast route configuration for a particular VRF by name.
vrfids WORD<0-512>	Displays the multicast route configuration for a particular VRF by VRF ID.

Use the data in the following table to use the **show ip igmp sender** command.

Variable	Value
count	Specifies the number of entries.
group {A.B.C.D}	Specifies the group address.
member-subnet {A.B.C.D/X}	Specifies the IP address and network mask.
vrf WORD<1–16>	Displays the multicast route configuration for a particular VRF by name.
vrfids WORD<0–512>	Displays the multicast route configuration for a particular VRF by VRF ID.

Job aid

The following table describes the fields for the **show ip igmp interface** command.

Parameter	Description
IF	Indicates the interface where IGMP is configured.
QUERY INTVL	Indicates the frequency at which IGMP host query packets transmit on this interface.
STATUS	Indicates the activation of a row, which activates IGMP on the interface. The destruction of a row disables IGMP on the interface.
VERS.	Indicates the version of IGMP that runs on this interface. This object configures a router capable of running either version. For IGMP to function correctly, you must configure all routers on a LAN to run the same version of IGMP.
OPER VERS	Indicates the operational version of IGMP.
QUERIER	Indicates the address of the IGMP Querier on the IP subnet to which this interface attaches.
QUERY MAXRSPT	Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.
WRONG QUERY	Indicates the number of queries received where the IGMP version does not match the interface version. You must configure all routers on a LAN to run the same version of IGMP. If queries are received with the wrong version, a configuration error occurs.
JOINS	Indicates the number of times this interface added a group membership.
ROBUST	Indicates the robustness variable, which you can configure for the expected packet loss on a subnet. If you expect packet loss on a subnet, increase the robustness variable.
LASTMEM QUERY	Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in

Table continues...

Parameter	Description
	response to leave group messages, and is also the amount of time between group specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This variable does not apply to IGMPv1.
MODE	Indicates the protocol configured on the VLAN added. If routed-spb displays in the MODE column, then IP Multicast over Fabric Connect is enabled on the Layer 3 VSN or for IP shortcuts. If snoop-spb displays in the MODE column, then IGMP is enabled on a VLAN with an associated I-SID (Layer 2 VSN).

The following table describes the fields for the `show ip igmp interface vlan` command.

Parameter	Description
VLAN ID	Identifies the VLAN where IGMP is configured.
QUERY INTVL	Indicates the frequency at which IGMP host query packets transmit on this interface.
QUERY MAX RESP	Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.
ROBUST	Indicates the robustness variable, which you can configure for the expected packet loss on a subnet. If you expect packet loss on a subnet, increase the robustness variable.
VERSION	Indicates the version of IGMP that runs on this interface. This object configures a router capable of running either version. For IGMP to function correctly, you must configure all routers on a LAN to run the same version of IGMP.
LAST MEMB QUERY	Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This variable does not apply to IGMPv1.
PROXY SNOOP ENABLE	Indicates if proxy snoop is enabled on the interface.
SNOOP ENABLE	Indicates if snoop is enabled on the interface.
SSM SNOOP ENABLE	Indicates if SSM snoop is enabled on the interface.
FAST LEAVE ENABLE	Indicates if fast leave mode is enabled on the interface.

Table continues...

Parameter	Description
FAST LEAVE PORTS	Indicates the set of ports that are enabled for fast leave.
VLAN ID	Identifies the VLAN where IGMP is configured.
SNOOP QUERIER ENABLE	Indicates if the IGMP Layer 2 Querier feature is enabled.
SNOOP QUERIER ADDRESS	Indicates the IP address of the IGMP Layer 2 Querier.
DYNAMIC DOWNGRADE VERSION	Indicates if the dynamic downgrade feature is enabled.
COMPATIBILITY MODE	Indicates if compatibility mode is enabled.
EXPLICIT HOST TRACKING	Indicates if explicit host tracking is enabled to track all the source and group members.

The following table describes the fields for the `show ip igmp cache` command.

Parameter	Description
GRPADDR	Indicates the multicast group address (Class D) that others want to join. Many incoming ports can use the same group address.
INTERFACE	Indicates the physical interface or a logical interface (VLAN), which received group reports from various sources.
LASTREPORTER	Indicates the IP address of the source of the last membership report received for this IP multicast group address on this interface. If the interface does not receive a membership report, this object uses the value 0.0.0.0.
EXPIRATION	Indicates the minimum amount of time that remains before this entry ages out.
V1HOSTIMER	Indicates the time that remains until the local router assumes that no IGMPv1 members exist on the IP subnet attached to this interface.
TYPE	Indicates whether the entry is learned dynamically or is added statically.
STATICPORTS	Indicates the list of statically-defined ports.

The following table describes the fields for the `show ip igmp group` command.

Parameter	Description
GRPADDR	Indicates the multicast group address (Class D) that others want to join. Many incoming ports can use the same group address.

Table continues...

Parameter	Description
INPORT	Indicates the physical interface or a logical interface (VLAN), which received group reports from various sources.
MEMBER	Indicates the IP address of a source that sent a group report to join this group.
EXPIRATION	Indicates the minimum amount of time that remains before this entry ages out.
TYPE	Indicates whether the entry is learned dynamically or is added statically.

The following table describes the fields for the `show ip igmp sender` command.

Parameter	Description
GRPADDR	Indicates the IP multicast address.
IFINDEX	Indicates the interface index number.
MEMBER	Indicates the IP address of the host.
PORT/MLT	Indicates the IGMP sender ports.
STATE	Indicates if a sender exists because of an IGMP access filter. Options include filtered and nonfiltered.

The following table describes the fields for the `show ip igmp snoop-trace` command.

Parameter	Description
GROUP ADDRESS	Indicates the IP multicast group address for which this entry contains information.
SOURCE ADDRESS	Indicates the source of the multicast traffic.
IN VLAN	Indicates the incoming VLAN ID.
IN PORT	Indicates the incoming port number.
OUT VLAN	Indicates the outgoing VLAN ID.
OUT PORT	Indicates the outgoing port number.
TYPE	Indicates where the stream is learned. ACCESS indicates the stream is learned on UNI ports. NETWORK indicates the stream is learned over the SPBM network.

Viewing TLV information for IP Multicast over Fabric Connect within the GRT

Use the following commands to check TLV information.

For IP Multicast over Fabric Connect within the GRT, TLV 186 on the BEB where the source is located displays the multicast source and group addresses and have the Tx bit set. Each multicast group has its own unique data I-SID with a value between 16,000,000 to 16,512,000. TLV 144 on

the BEB bridge, where the sender is located, has the Tx bit set while on all BEB bridges, where a receiver exists, has the Rx bit set.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display IS-IS Link State Database information by TLV:

```
show isis lsdb tlv <1-236> [sub-tlv <1-3>][detail]
```

3. Display IS-IS Link State Database information by Link State Protocol ID:

```
show isis lsdb lspid <xxxx.xxxx.xxxx.xx-xx> tlv <1-236> [sub-tlv <1-3>] [detail]
```

Example

Display TLV information:

```
Switch:1# show isis lsdb tlv 186 detail
=====
ISIS LSDB (DETAIL)
=====
Level-1 LspID: 000c.f803.83df.00-06 SeqNum: 0x000002eb Lifetime: 1113
Chksum: 0x7e3b PDU Length: 556
Host_name: Switch
Attributes: IS-Type 1
TLV:186 SPBM IP Multicast:
  GRT ISID
  Metric:0
  IP Source Address: 192.2.0.10
  Group Address : 233.252.0.1
  Data ISID : 16300012
  BVID : 20
  TX : 1
  Route Type : Internal
  GRT ISID
  Metric:0
  IP Source Address: 192.2.0.10
  Group Address : 233.252.0.2
  Data ISID : 16300013
  BVID : 10
  TX : 1
  Route Type : Internal
  GRT ISID
  Metric:0
  IP Source Address: 192.2.0.10
  Group Address : 233.252.0.3
  Data ISID : 16300014
  BVID : 20
  TX : 1
  Route Type : Internal
  GRT ISID
  Metric:0
  IP Source Address: 192.2.0.10
  Group Address : 233.252.0.4
  Data ISID : 16300015
  BVID : 10
  TX : 1
  Route Type : Internal
  GRT ISID
  Metric:0
```

```

IP Source Address: 192.2.0.10
Group Address : 233.252.0.5
Data ISID : 16300016
BVID : 20
TX : 1
Route Type : Internal
GRT ISID
Metric:0
IP Source Address: 192.2.0.10
Group Address : 233.252.0.6
Data ISID : 16300017
BVID : 10
TX : 1
Route Type : Internal
GRT ISID
Metric:0
IP Source Address: 192.2.0.10
Group Address : 233.252.0.7
Data ISID : 16300018
BVID : 20
TX : 1
Route Type : Internal
    
```

Variable definitions

Use the data in the following table to use the `show isis lsdb` command.

Variable	Value
detail	Displays detailed information about the IS-IS Link State database.
level {1, I2, I12}	Displays information on the IS-IS level. The IEEE 802.1aq standard currently only defines the use of one hierarchy, Level 1. Level 2 function is disabled.
local	Displays information on the local LSDB.
lspid <xxxx.xxxx.xxxx.xx-xx>	Specifies information about the IS-IS Link State database by LSP ID.
sub-tlv <1-3>	Specifies information about the IS-IS Link State database by sub-TLV.
sysid <xxxx.xxxx.xxxx>	Specifies information about the IS-IS Link State database by System ID.
tlv <1-236>	Specifies information about the IS-IS Link State database by TLV.

Job aid

The following table describes the fields for the `show isis lsdb tlv` command.

Parameter	Description
LSP ID	Indicates the LSP ID assigned to external IS-IS routing devices.
LEVEL	Indicates the level of the external router: I1, I2, or I12.

Table continues...

Parameter	Description
LIFETIME	Indicates the maximum age of the LSP. If the max-lsp-gen-interval is set to 900 (default) then the lifetime value begins to count down from 1200 seconds and updates after 300 seconds if connectivity remains. If the timer counts down to zero, the counter adds on an additional 60 seconds, then the LSP for that router is lost.
SEQNUM	Indicates the LSP sequence number. This number changes each time the LSP is updated.
CKSUM	Indicates the LSP checksum. This is an error checking mechanism used to verify the validity of the IP packet.
HOST-NAME	Specifies the host-name.

IP Shortcuts configuration using EDM

Configuring IP Multicast over Fabric Connect on a VLAN within the GRT

Use this procedure to enable IP Multicast over Fabric Connect on each of the VLANs within the GRT that need to support IP multicast traffic. The default is disabled.

To configure a VRF with IP Multicast over Fabric Connect, see [Configuring IP Multicast over Fabric Connect on a VLAN for Layer 3](#) on page 107.

Note:

- You do not have to enable IP Shortcuts to support IP multicast routing in the GRT using SPBM.
- You cannot enable IP PIM when IP Multicast over Fabric Connect is enabled on the VLAN.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must create the C-VLANs and add slots/ports.
- You must enable IP Multicast over Fabric Connect globally.
- If there is no IP interface on the VLAN, then you create one. (The IP interface must be in the same subnet as the IGMP hosts that connect to the VLAN).

About this task

With IP Multicast over Fabric Connect within the GRT, routing of IP multicast traffic is allowed within the subset of VLANs in the GRT that have IP Multicast over Fabric Connect enabled. When you enable IP Multicast over Fabric Connect on a VLAN, the VLAN automatically becomes a multicast routing interface.

You must enable IP Multicast over Fabric Connect on each of the VLANs within the GRT that need to support IP multicast traffic. After you enable IP Multicast over Fabric Connect on the VLANs, any

IGMP functions required for IP Multicast over Fabric Connect within the GRT are automatically enabled. You do not need to configure anything IGMP related.

If you only want to use IP Multicast over Fabric Connect, you do not need to enable the Layer 3 VSN or redistribute unicast routes into or out of IS-IS. IP Multicast over Fabric Connect routing within the GRT does not depend on unicast routing. This allows for you to more easily migrate from a PIM environment to IP Multicast over Fabric Connect. You can migrate a PIM environment to IP Multicast over Fabric Connect first and then migrate unicast separately or not at all.

The switch only supports IPv4 addresses with IP Multicast over Fabric Connect.

Procedure

1. In the navigation pane, expand the **Configuration > VLAN** folders.
2. Click **VLANs**.
3. Choose a VLAN, and then click the **IP** button.
4. Click the **SPB Multicast** tab.

*** Note:**

After you enable IP Multicast over Fabric Connect, you cannot enable IGMP, IGMP Snooping, or IGMP proxy on the interface. If you try to enable IGMP Snooping or proxy on any interface where SPBM multicast is enabled, an error message appears.

*** Note:**

When you enable IP Multicast over Fabric Connect on a Controller switch in a DvR domain, the configuration is automatically pushed to the Leaf nodes within the domain.

For information on DvR, see *Configuring IPv4 Routing*.

5. Click **Enable**.
6. Click **Apply**.

Configuring IP Multicast over Fabric Connect on a brouter port within the GRT

Use this procedure to enable IP Multicast over Fabric Connect on a brouter port IP interface. The default is enabled.

To configure a brouter port for a VRF with IP Multicast over Fabric Connect, see [Configuring IP Multicast over Fabric Connect on a brouter port for a Layer 3 VSN](#) on page 108.

*** Note:**

- You do not have to enable IP Shortcuts to support IP multicast routing in the GRT using SPBM.
- You cannot enable IP PIM when IP Multicast over Fabric Connect is enabled on the VLAN.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.

- You must create the C-VLANs and add slots/ports.
- You must enable IP Multicast over Fabric Connect globally.
- If there is no IP interface on the VLAN, then you create one. (The IP interface must be in the same subnet as the IGMP hosts that connect to the VLAN).

About this task

With IP Multicast over Fabric Connect within the GRT, routing of IP multicast traffic is allowed within the subset of VLANs in the GRT that have IP Multicast over Fabric Connect enabled. When you enable IP Multicast over Fabric Connect on a VLAN, the VLAN automatically becomes a multicast routing interface.

You must enable IP Multicast over Fabric Connect on each of the VLANs within the GRT that need to support IP multicast traffic. After you enable IP Multicast over Fabric Connect on the VLANs, any IGMP functions required for IP Multicast over Fabric Connect within the GRT are automatically enabled.

If you only want to use IP Multicast over Fabric Connect, you do not need to enable the Layer 3 VSN or redistribute unicast routes into or out of IS-IS. IP Multicast over Fabric Connect routing does not depend on unicast routing, which allows for you to more easily migrate from a PIM environment to Multicast over Fabric Connect. You can migrate a PIM environment to IP Multicast over Fabric Connect first, and then migrate unicast separately or not at all.

The switch only supports IPv4 addresses with IP Multicast over Fabric Connect.

Procedure

1. Select an enabled port on the Physical Device View.
2. In the navigation pane, expand the **Configuration > Edit > Port** folders.
3. Click **IP**.
4. Click the **SPB Multicast** tab.
5. Click **Enable**.

*** Note:**

When you enable IP Multicast over Fabric Connect on a DvR Controller switch in a DvR domain, the configuration is automatically pushed to the Leaf nodes within the domain.

For information on DvR, see *Configuring IPv4 Routing*.

6. Click **Apply**.

SPB Multicast field description

Use the data in the following table to use the SPB Multicast tab.

Name	Description
Enable	Enables or disables SPB Multicast. The default is disable.

Viewing the IGMP interface table

Use the Interface tab to view the IGMP interface table. When an interface does not use an IP address, it does not appear in the IGMP table.

Procedure

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

Configuring the Global Routing Table timeout value

Use this procedure to configure the timeout value in the GRT. The timeout value ages out the sender when there are no multicast streams coming from the sender for a specified period of time. The default timeout value is 210 seconds.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must create the C-VLANs and add slots/ports.
- You must enable IP Multicast over Fabric Connect globally.

Procedure

1. In the navigation pane, expand the **Configuration > IS-IS > SPBM** folders.
2. Click the **SPBM** tab.
3. Modify the **McastFwdCacheTimeout** value.
4. Click **Apply**.

IP shortcuts configuration example

IP multicast over SPBM within the GRT configuration example

The following example shows the configuration steps to enable IP multicast over SPBM support on VLANs 10 and 11 that are part of the GRT:

```
ISIS SPBM CONFIGURATION

router isis
spbm 1 multicast enable

VLAN CONFIGURATION - PHASE I

interface vlan 500
ip address 192.0.2.1 255.255.255.0
ip spb-multicast enable
exit

interface vlan 501
```

```
ip address 192.0.2.2 255.255.255.0
ip spb-multicast enable
exit
```

Layer 3 VSN configuration

Layer 3 VSN fundamentals

This section provides fundamentals concepts for Layer 3 VSN configuration. For more information on Layer 3 VSN basic configuration, see *Configuring Fabric Layer 3 Services*.

Layer 3 VSN with IP Multicast over Fabric Connect

IP Multicast over Fabric Connect supports Layer 3 VSN functionality where multicast traffic is bridged over the SPBM core infrastructure. Layer 3 VSN using IP Multicast over Fabric Connect is helpful when you need complete security and total isolation of data. No one outside of the Layer 3 VSN can join or even see the Layer 3 VSN. Applications that can use Layer 3 VSN with IP Multicast over Fabric Connect include: Video surveillance, TV/Video/Ticker/Image Distribution, VX-LAN, Multi-tenant IP multicast.

Configure the Layer 3 VSN (VRF) as a multicast VPN, and then enable IP Multicast over Fabric Connect on VRF VLANs to which IP multicast senders and receivers attach. This configuration automatically enables IGMP snooping and proxy on those VLANs. IGMPv2 at the VLAN level is the default setting, with no other configuration required. If you want to use IGMPv3, you must configure IGMPv3.

IP Multicast over Fabric Connect is only configured on BEBs.

*** Note:**

- You do not need to enable IP Shortcuts to support multicast routing in the Layer 3 VSN using SPBM. IPVPN creation and I-SID assignment for the IPVPN is required, but you do not need to enable IPVPN.
- If you only want to use IP Multicast over Fabric Connect, you do not need to enable the Layer 3 VSN or redistribute unicast routes into or out of IS-IS. IP Multicast over Fabric Connect routing does not depend on unicast routing for Layer 3 VSNs using VRFs, which allows you to more easily migrate from a PIM environment to IP Multicast over Fabric Connect. You can migrate a PIM environment to IP Multicast over Fabric Connect first and then migrate unicast separately or not at all.
- If no IP interface exists on the VLAN, then you create one. (The IP interface must be the same subnet as the IGMP hosts that connect to the VLAN).

With Layer 3 VSN with IP Multicast over Fabric Connect, multicast traffic remains in the same Layer 3 VSN across the SPBM cloud. For a Layer 3 VSN, traffic can cross VLAN boundaries but remains confined to the subset of VLANs within the VRF that has IP Multicast over Fabric Connect enabled.

If a sender transmits a multicast stream to a BEB on a Layer 3 VSN with IP Multicast over Fabric Connect enabled, only receivers that are part of the same Layer 3 VSN can receive that stream.

I-SIDs

After a BEB receives IP multicast data from a sender, the BEB allocates a data service instance identifier (I-SID) in the range of 16,000,000 to 16,512,000 for the multicast stream. The stream is identified by the S, G, V tuple, which is the source IP address, the group IP address and the local VLAN the multicast stream is received on. The data I-SID uses Tx/Rx bits to signify whether the BEB uses the I-SID to transmit, receive, or both transmit and receive data on that I-SID.

In the context of Layer 3 VSNs with IP Multicast over Fabric Connect, the scope is the I-SID value of the Layer 3 VSN associated with the local VLAN that the IP multicast data was received on.

TLVs

This information is propagated through the SPBM cloud using IS-IS Link State Packets (LSPs), which carry TLV updates, that result in the multicast tree creation for that stream. For Layer 3 VSNs, the LSPs carry I-SID information and information about where IP multicast stream senders and receivers exist using TLV 144 and TLV 185.

IS-IS acts dynamically using the TLV information received from BEBs that connect to the sender and the receivers to create a multicast tree between them.

IGMP

After a BEB receives an IGMP join message from a receiver, the BEB queries the IS-IS database to check if a sender exists for the requested stream within the scope of the receiver. If the requested stream does not exist, the IGMP information is kept, but no further action is taken. If the requested stream exists, the BEB sends an IS-IS TLV update to its neighbors to inform them of the presence of a receiver and this information is propagated through the SPBM cloud.

DvR

On DvR Controllers in a DvR domain, you must manually configure IP multicast over Fabric Connect on Layer 3 VSNs (VRFs). This configuration is then automatically pushed to the Leaf nodes in the DvR domain.

For more information on DvR, see *Configuring IPv4 Routing*.

Enable/disable ICMP Response on VRFs/Layer 3 VSNs

This feature supports VRFs/Layer 3 VSNs to operate in stealth mode by disabling ICMP responses on specific VRFs/Layer 3 VSNs.

If the ICMP response is disabled, the switch does not respond to any ICMP requests received on the VRFs/Layer 3 VSNs.

If the ICMP response is enabled, the switch responds to ICMP requests received on the VRF/Layer 3 VSNs.

Layer 3 VSN configuration using the CLI

This section provides a procedure to configure Layer 3 VSNs using the command line interface (CLI).

Configuring Layer 3 VSN with IP Multicast over Fabric Connect

Use this procedure to configure IP Multicast over Fabric Connect for a Layer 3 VSN.

Configure the Layer 3 VSN (VRF) as a multicast VPN, and then enable IP Multicast over Fabric Connect on VRF VLANs to which IP multicast senders and receivers attach. After you enable IP Multicast over Fabric Connect on VRF VLANs, snooping and proxy on those VLANs is enabled. IGMPv2 at the VLAN level is the default setting. No configuration is required.

* Note:

On DvR Controllers in a DvR domain, you must manually configure IP multicast over Fabric Connect on Layer 3 VSNs (VRFs). This configuration is then automatically pushed to the Leaf nodes in the DvR domain.

For more information on DvR, see *Configuring IPv4 Routing*.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must create the C-VLANs and add slots/ports.
- You must enable IP Multicast over Fabric Connect globally.
- You must assign an I-SID for the IPVPN.

About this task

With Layer 3 VSN IP Multicast over Fabric Connect, multicast traffic remains in the same Layer 3 VSN across the SPBM cloud.

For a Layer 3 VSN, traffic can cross VLAN boundaries but remains confined to the subset of VLANs within the VRF that have `ip spbm-multicast` enabled. The default is disabled.

All or a subset of VLANs within a Layer 3 VSN can exchange multicast traffic. The BEB only sends out traffic for a multicast stream on which IGMP joins and reports are received.

The switch only supports IPv4 multicast traffic.

* Note:

You cannot enable IP PIM when IP Multicast over Fabric Connect is enabled on the VLAN.

The IP VPN does not need to be enabled for Layer 3 VSN multicast to function.

Procedure

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

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

2. Enable Layer 3 VSN IP Multicast over Fabric Connect for a particular VRF:

```
mvpn enable
```

The default is disabled.

3. **(Optional)** If you want to disable Layer 3 VSN IP Multicast over Fabric Connect, enter:

```
no mvpn enable
default mvpn enable
```

4. Exit to Global Configuration mode:

```
exit
```

5. Enter Interface Configuration mode:

```
enable
configure terminal
interface GigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-
port]][, ...]} or interface vlan <1-4059>
```

*** 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.

6. Enable Layer 3 VSN IP Multicast over Fabric Connect for a particular VRF:

```
ip spb-multicast enable
```

7. **(Optional)** Disable Layer 3 multicast on the VRF:

```
no ip spb-multicast enable
```

8. **(Optional)** Enable IGMP version 3:

```
ip igmp snooping
ip igmp ssm-snoop
ip igmp compatibility-mode
ip igmp version 3
```

*** Note:**

IGMPv2 at the VLAN level is the default setting, with no other configuration required. You only need to use these commands if you use IGMPv3. You must enable SSM snoop before you configure IGMP version 3, and you must enable both ssm-snoop and snooping for IGMPv3.

For IGMP Snooping, ensure that the IGMP version used by multicast hosts and other devices in the network is the same as the IGMP version configured on the IGMP Snooping VLAN, or that you enable compatibility mode.

9. **(Optional)** Enable the IGMP Layer 2 Querier address:

```
ip igmp snoop-querier-addr {A.B.C.D}
```

*** Note:**

If the SPBM bridge connects to an edge switch, it can be necessary to add an IGMP query address. If you omit adding a query address, the SPB bridge sends IGMP queries with a source address of 0.0.0.0. Some edge switch models do not accept a query with a source address of 0.0.0.0.

Example

Configure IP Multicast over Fabric Connect for a Layer 3 VSN:

```
Switch:>enable
Switch:#configure terminal
Switch:(config)# router vrf green
Switch:(config-vrf)#mvpn enable
Switch:(config)#exit
Switch:(config)#interface vlan 500
Switch:(config-if)#ip spb-multicast enable
```

Variable definitions

Use the data in the following table to use the **router vrf** command.

Variable	Value
<i>WORD</i> <1–16>	Specifies the name of the VRF.

Use the data in the following table to use the **interface vlan** command.

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

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

Variable	Value
GigabitEthernet{ <i>slot/port[/sub-port] [-slot/port[/sub-port]] [...]</i> }	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.

Use the data in the following table to use the **ip igmp** command.

Variable	Value
<p>access-list <i>WORD</i><1–64> {A.B.C.D/X} <eny-tx deny-rx deny-both allow-only-tx allow-only-rx allow-only-both></p>	<p>Specifies the name of the access list from 1–64 characters.</p> <p>Creates an access control group entry for a specific IGMP interface. Specify the IP address of the host and the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the network for the host.</p> <p>Indicates the action for the specified IGMP interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic.</p>
<p>compatibility-mode</p>	<p>Activates v2-v3 compatibility mode. The default value is disabled, which means IGMPv3 is not compatible with IGMPv2. To use the default configuration, use the default option in the command:</p> <pre>default ip igmp compatibility-mode</pre> <p>, or use the no option to disable compatibility mode:</p> <pre>no ip igmp compatibility-mode</pre>
<p>dynamic-downgrade-version</p>	<p>Configures if the system downgrades the version of IGMP to handle older query messages. If the system downgrades, the host with IGMPv3 only capability does not work. If you do not configure the system to downgrade the version of IGMP, the system logs a warning. The system downgrades to the oldest version of IGMP on the network by default. To use the default configuration, use the default option in the command:</p> <pre>default ip igmp dynamic-downgrade-version</pre> <p>or use the no option to disable downgrade:</p> <pre>no ip igmp dynamic-downgrade-version</pre>
<p>igmpv3-explicit-host-tracking</p>	<p>Enables explicit host tracking on IGMPv3. The default state is disabled.</p>
<p>immediate-leave</p>	<p>Enables fast leave on a VLAN.</p>
<p>immediate-leave-members {<i>slot/port</i>[/<i>sub-port</i>] [-<i>slot/port</i>[/<i>sub-port</i>]] [...]}</p>	<p>Configures IGMP fast leave members on a VLAN to specify fast-leave-capable ports.</p>
<p>last-member-query-interval <0–255></p>	<p>Configures the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages. This value is also the time between group-specific query messages. You cannot configure this value for IGMPv1.</p> <p>Decreasing the value reduces the time to detect the loss of the last member of a group. The default is 10 tenths of a second. Configure this value between 3–10 (equal to 0.3 – 1.0 seconds).</p>

Table continues...

Variable	Value
mrdisc [maxadvertinterval <2–180> [maxinitadvertinterval <2–180> [maxinitadvertisements <2–15> [minadvertinterval <3–180> [neighdeadinterval <2–180>]	Configure the multicast router discovery options to enable the automatic discovery of multicast capable routers. The default parameter values are: <ul style="list-style-type: none"> • maxadvertinterval: 20 seconds • maxinitadvertinterval: 2 seconds • maxinitadvertisements: 3 • minadvertinterval: 15 seconds • neighdeadinterval: 60 seconds
mrouter {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Adds multicast router ports.
proxy	Activates the proxy-snoop option globally for the VLAN.
query-interval <1–65535>	Configures the frequency (in seconds) at which the VLAN transmits host query packets. The default value is 125 seconds.
query-max-response <0–255>	Configures the maximum response time (in tenths of a second) advertised in IGMPv2 general queries on this interface. You cannot configure this value for IGMPv1. Smaller values allow a router to prune groups faster. The default is 100 tenths of a second (equal to 10 seconds). <p>! Important:</p> You must configure this value lower than the query-interval.
robust-value <2–255>	Configures the expected packet loss of a network. The default value is 2 seconds. Increase the value if you expect the network to experience packet loss.
router-alert	Instructs the router to ignore IGMP packets that do not contain the router alert IP option. When disabled (default configuration), the router processes IGMP packets regardless of the status of the router alert IP option. <p>! Important:</p> To maximize network performance, configure this parameter according to the version of IGMP currently in use: <ul style="list-style-type: none"> • IGMPv1—Disable • IGMPv2—Enable • IGMPv3—Enable
snoop-querier	Enables the IGMP Layer 2 Querier feature on the VLAN. The default is disabled.
snoop-querier-addr {A.B.C.D}	Specifies the IGMP Layer 2 Querier source IP address.
snooping	Activates the snoop option for the VLAN.

Table continues...

Variable	Value
ssm-snoop	Activates support for SSM on the snoop interface.
static-group {A.B.C.D} {A.B.C.D} [port] {slot/port/sub-port} [-slot/port/sub-port] [...]] [static blocked]	Configures IGMP static members to add members to a snoop group. {A.B.C.D} {A.B.C.D} indicates the IP address range of the selected multicast group. [port] {slot/port/sub-port} [-slot/port/sub-port] [...]] adds ports to a static group entry. [static blocked] configures the route to static or blocked.
stream-limit stream-limit-max-streams <0-65535>	Configures multicast stream limitation on a VLAN to limit the number of concurrent multicast streams on the VLAN. The default is 4.
stream-limit-group {slot/port/sub-port} [-slot/port/sub-port] [...]] enable max-streams <0-65535>	Configures multicast stream limitation members on ports of a specific VLAN to limit the number of multicast groups that can join a VLAN. The default max-streams value is 4.
version <1-3>	Configures the version of IGMP that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. The default value is 2 (IGMPv2).

Configuring the VRF timeout value

Use this procedure to configure the VRF timeout value. The timeout value ages out the sender when there is no multicast stream on the VRF. The default is 210 seconds.

* Note:

You can use this procedure for Layer 3 VSN with IP Multicast over Fabric Connect services and IP Multicast over Fabric Connect for IP Shortcuts.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must create the C-VLANs and add slots/ports.
- You must enable IP Multicast over Fabric Connect globally.

Procedure

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

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

2. Configure the timeout value on the VRF:

```
mvpn fwd-cache-timeout(seconds) <10-86400>
```

3. (Optional) Configure the timeout value to the default value of 210 seconds:

```
no mvpn fwd-cache-timeout
default mvpn fwd-cache-timeout(seconds)
```

Example

Configure the timeout value on the VRF to 500 seconds:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#router vrf green
Switch:1(router-vrf)#mvpn fwd-cache-timeout(seconds) 500
```

Variable definitions

Use the data in the following table to use the `router vrf` command.

Variable	Value
WORD<1–16>	Specifies the VRF name.

Use the data in the following table to use the `mvpn fwd-cache-timeout(seconds)` command.

Variable	Value
<10–86400>	Specifies the timeout value. The default is 210 seconds.

Configuring the Global Routing Table timeout value

Use this procedure to configure the timeout value in the GRT. The timeout value ages out the sender when there are no multicast streams coming from the sender for a specified period of time in seconds. The default timeout value is 210 seconds.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must create the C-VLANs and add slots/ports.
- You must enable IP Multicast over Fabric Connect globally.

Procedure

1. Enter IS-IS Router Configuration mode:

```
enable
configure terminal
router isis
```

2. Configure the IP Multicast over Fabric Connect forward-cache timeout:

```
spbm <1-100> multicast fwd-cache-timeout(seconds) <10-86400>
```

3. (Optional) Configure the IP Multicast over Fabric Connect forward-cache timeout to the default value of 210 seconds:

```
default spbm <1-100> multicast fwd-cache-timeout(seconds)
no spbm <1-100> multicast fwd-cache-timeout(seconds)
```

Example

Configure the IP Multicast over Fabric Connect forward-cache timeout to 300:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#router isis
Switch:1(config-isis)#spbm 1 multicast 1 fwd-cache-timeout 300
```

Variable definitions

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

Variable	Value
<1-100>	Specifies the SPBM instance. The switch only supports one instance.
<10-86400>	Specifies the IP Multicast over Fabric Connect forward-cache timeout in seconds. The default is 210 seconds.

Viewing Layer 3 VSN with IP Multicast over Fabric Connect information

Use the following options to display Layer 3 VSN with IP Multicast over Fabric Connect information to confirm proper configuration.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display all the VRFs that have MVPN enabled and their corresponding forward cache timeout values:

```
show ip vrf mvpn
```

3. Display IP Multicast over Fabric Connect route information:

```
show isis spbm ip-multicast-route [all][detail]
```

4. Display IP Multicast over Fabric Connect by group and source address:

```
show isis spbm ip-multicast-route [group {A.B.C.D}][detail][source {A.B.C.D}]
```

5. Display IP Multicast over Fabric Connect route information by VRF:

```
show isis spbm ip-multicast-route [vrf WORD<1-16>] [group {A.B.C.D}]
```

6. Display IP Multicast over Fabric Connect route information by VLAN:

```
show isis spbm ip-multicast-route [vlan <1-4059>][detail][group {A.B.C.D}]
```

7. Display IP Multicast over Fabric Connect information by VSN I-SID:

```
show isis spbm ip-multicast-route [vsn-isid <1-16777215>][detail]
[group {A.B.C.D}]
```

8. Display summary information for each S, G, V tuple with the corresponding scope, Data I-SID, and the host name of the source:

```
show isis spb-mcast-summary [host-name WORD<0-255>][lspid
<xxxx.xxxx.xxxx.xx-xx>]
```

Example

Display Layer 3 VSN with IP Multicast over Fabric Connect information:

```
Switch:1>enable
Switch:1#show ip vrf mvpn

                Vrf name : green
                mvpn : enable
fwd-cache-timeout(seconds) : 210

                Vrf name : 4
                mvpn : enable
fwd-cache-timeout(seconds) : 210

                Vrf name : blue
                mvpn : enable
fwd-cache-timeout(seconds) : 210

Switch:1#show isis spbm ip-multicast-route all
=====
                SPBM IP-multicast ROUTE INFO ALL
=====
Type   VrfName  Vlan  Source      Group      VSN-ISID  Data ISID  BVLAN  Source-BEB
-----
routed GRT      501   192.0.2.1   233.252.0.1  5010      16300001  10     e12
routed GRT      501   192.0.2.1   233.252.0.2  5010      16300002  20     e12
routed GRT      501   192.0.2.1   233.252.0.3  5010      16300003  10     e12
routed GRT      501   192.0.2.1   233.252.0.4  5010      16300004  20     e12
routed GRT      501   192.0.2.1   233.252.0.5  5010      16300005  10     e12
routed GRT      501   192.0.2.1   233.252.0.6  5010      16300006  20     e12
routed GRT      501   192.0.2.1   233.252.0.7  5010      16300007  10     e12
routed GRT      501   192.0.2.1   233.252.0.8  5010      16300008  20     e12
routed GRT      501   192.0.2.1   233.252.0.9  5010      16300009  10     e12
routed GRT      501   192.0.2.1   233.252.0.10 5010      16300010  20     e12
-----
Total Number of SPBM IP multicast ROUTE Entries: 10
-----

Switch:1#show isis spbm ip-multicast-route vrf green
=====
                SPBM IP-MULTICAST ROUTE INFO
=====
Source      Group      Data ISID  BVLAN  Source-BEB
-----
192.0.2.10  233.252.0.1  16300001  10     e12
192.0.2.10  233.252.0.2  16300002  20     e12
192.0.2.10  233.252.0.3  16300003  10     e12
```

IP Multicast over Fabric Connect services configuration

```

192.0.2.10    233.252.0.4    16300004    20    e12
192.0.2.10    233.252.0.5    16300005    10    e12
192.0.2.10    233.252.0.6    16300006    20    e12
192.0.2.10    233.252.0.7    16300007    10    e12
192.0.2.10    233.252.0.8    16300008    20    e12
192.0.2.10    233.252.0.9    16300009    10    e12
192.0.2.10    233.252.0.10   16300010    20    e12

```

```
-----
Total Number of SPBM IP MULTICAST ROUTE Entries: 10
-----
```

```
Switch:1#show isis spbm ip-multicast-route vlan 501
```

```
=====
SPBM IP-multicast ROUTE INFO ALL
=====
```

Type	VrfName	Vlan	Source	Group	VSN-ISID	Data	ISID	BVLAN	Source-BEB
Id									
routed	GRT	501	192.0.2.1	233.252.0.1	5010	16300001	10	e12	
routed	GRT	501	192.0.2.1	233.252.0.2	5010	16300002	20	e12	
routed	GRT	501	192.0.2.1	233.252.0.3	5010	16300003	10	e12	
routed	GRT	501	192.0.2.1	233.252.0.4	5010	16300004	20	e12	
routed	GRT	501	192.0.2.1	233.252.0.5	5010	16300005	10	e12	
routed	GRT	501	192.0.2.1	233.252.0.6	5010	16300006	20	e12	
routed	GRT	501	192.0.2.1	233.252.0.7	5010	16300007	10	e12	
routed	GRT	501	192.0.2.1	233.252.0.8	5010	16300008	20	e12	
routed	GRT	501	192.0.2.1	233.252.0.9	5010	16300009	10	e12	
routed	GRT	501	192.0.2.1	233.252.0.10	5010	16300010	20	e12	

```
-----
Total Number of SPBM IP multicast ROUTE Entries: 10
-----
```

```
Switch:1# show isis spbm ip-multicast-route vsn-isid 5010
```

```
=====
SPBM IP-multicast ROUTE INFO - VLAN ID : 501, VSN-ISID : 5010
=====
```

Source	Group	Data	ISID	BVLAN	Source-BEB
192.0.2.1	233.252.0.2	16300002	20	e12	
192.0.2.1	233.252.0.3	16300003	10	e12	
192.0.2.1	233.252.0.4	16300004	20	e12	
192.0.2.1	233.252.0.5	16300005	10	e12	
192.0.2.1	233.252.0.6	16300006	20	e12	
192.0.2.1	233.252.0.7	16300007	10	e12	
192.0.2.1	233.252.0.8	16300008	20	e12	
192.0.2.1	233.252.0.9	16300009	10	e12	
192.0.2.1	233.252.0.10	16300010	20	e12	

```
-----
Total Number of SPBM IP multicast ROUTE Entries: 10
-----
```

```
Switch:1# show isis spb-mcast-summary
```

```
=====
SPB multicast - Summary
=====
```

SCOPE I-SID	SOURCE ADDRESS	GROUP ADDRESS	DATA I-SID	BVID	LSP FRAG	HOST NAME
5010	192.0.2.1	233.252.0.1	16300001	10	0x0	e12
5010	192.0.2.1	233.252.0.3	16300003	10	0x0	e12
5010	192.0.2.1	233.252.0.5	16300005	10	0x0	e12
5010	192.0.2.1	233.252.0.7	16300007	10	0x0	e12
5010	192.0.2.1	233.252.0.9	16300009	10	0x0	e12
5010	192.0.2.1	233.252.0.2	16300002	20	0x0	e12
5010	192.0.2.1	233.252.0.4	16300004	20	0x0	e12
5010	192.0.2.1	233.252.0.6	16300006	20	0x0	e12
5010	192.0.2.1	233.252.0.8	16300008	20	0x0	e12
5010	192.0.2.1	233.252.0.10	16300010	20	0x0	e12

Variable definitions

Use the data in the following table to use the `show isis spbm ip-multicast-route` command.

Variable	Value
all	Displays all IP Multicast over Fabric Connect route information.
detail	Displays detailed IP Multicast over Fabric Connect route information.
group{A.B.C.D}	Displays information on the group IP address for the IP Multicast over Fabric Connect route.
vlan<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
vrfWORD<1-16>	Displays IP Multicast over Fabric Connect route information by VRF.
vsn-isid<1-16777215>	Displays IP Multicast over Fabric Connect route information by I-SID.

Use the data in the following table to use the `show isis spb-mcast-summary` command.

Variable	Value
host-nameWORD<0-255>	Displays the IP Multicast over Fabric Connect summary information by host-name.
lspid<xxxx.xxxx.xxxx.xx-xx>	Displays the IP Multicast over Fabric Connect summary information by LSP ID.

Job aid

The following table describes the fields for the `show ip vrf mvpn` command.

Parameter	Description
Vrf name	Specifies the VRF name.
mvpn	Specifies if MVPN is enabled.
fwd-cache-timeout	Specifies the forward cache timeout (in seconds) for the VRF.

The following table describes the fields for the `show isis spbm ip-multicast-route` command.

Parameter	Description
Type	Specifies the type for the IP Multicast over Fabric Connect route.
VrfName	Specifies the VRF name.
Vlan Id	Specifies the ID for the C-VLAN.
Source	Specifies the group IP address for the IP Multicast over Fabric Connect route.
Group	Specifies the group IP address for the IP Multicast over Fabric Connect route.
VSN-ISID	Specifies the VSN I-SID. Layer 2 VSN and Layer 3 VSN each require a VSN I-SID. This is the scope I-SID.
Data ISID	Specifies the data I-SID for the IP Multicast over Fabric Connect route. After a BEB receives IP multicast data from a sender, the BEB allocates a data I-SID in the range of 16,000,000 to 16, 512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
BVLAN	Specifies the B-VLAN for the IP Multicast over Fabric Connect route.
Source-BEB	Specifies the source BEB for the IP Multicast over Fabric Connect route.

The following table describes the fields for the `show isis spbm ip-multicast-route all` command.

Parameter	Description
Source	Specifies the group IP address for the IP Multicast over Fabric Connect route.

Table continues...

Parameter	Description
Group	Specifies the group IP address for the IP Multicast over Fabric Connect route.
Data ISID	Specifies the data I-SID for the IP multicast route. After a BEB receives IP multicast data from a sender, the BEB allocates a data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
BVLAN	Specifies the B-VLAN for the IP Multicast over Fabric Connect route.
NNI Rcvrs	Specifies the NNI receivers.
UNI Rcvrs	Specifies the UNI receivers.
Source-BEB	Specifies the source BEB for the IP Multicast over Fabric Connect route.

The following table describes the fields for the `show isis spb-mcast-summary` command.

Parameter	Description
SCOPE I-SID	Specifies the scope I-SID. Layer 2 VSN and Layer 3 VSN each require a scope I-SID.
SOURCE ADDRESS	Specifies the group IP address for the IP Multicast over Fabric Connect route.
GROUP ADDRESS	Specifies the group IP address for the IP Multicast over Fabric Connect route.
DATA I-SID	Specifies the data I-SID for the IP Multicast over Fabric Connect route. After the BEB receives IP multicast data from a sender, the BEB allocates a data I-SID in the range of 16,000,000 to 16,512,000 for the stream. The stream is identified by the source IP address, group IP address, and the local VLAN the stream is received on. The data I-SID is a child of the scope or VSN I-SID.
BVID	Specifies the Backbone VLAN ID associated with the SPBM instance.
LSP FRAG	Specifies the LSP fragment number.
HOST NAME	Specifies the host name listed in the LSP, or the system name if the host is not configured.

Viewing IGMP information for Layer 3 VSN multicast

Use the following commands to check IGMP information.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display information about the interfaces where IGMP is enabled:

```
show ip igmp interface [gigabitethernet {slot/port[/sub-port]}[-slot/
port[/sub-port]][,...]] [vlan <1-4059>[vrf WORD<1-16>][vrfids
WORD<0-512>]
```

Ensure that the output displays `routed-spb` under `MODE`.

3. Display information about the IGMP cache:

```
show ip igmp cache [vrf WORD<1-16>][vrfids WORD<0-512>]
```

4. Display information about the IGMP group:

```
show ip igmp group [count][member-subnet default|{A.B.C.D/X}][vrf
WORD<1-16>][vrfids WORD<0-512>]
```

5. Display information about the IGMP sender:

```
show ip igmp sender [count][member-subnet default|{A.B.C.D/X}][vrf
WORD<1-16>][vrfids WORD<0-512>]
```

Example

Display IGMP information for Layer 3 VSN with IP multicast over Fabric Connect:

```
Switch:#enable
Switch:1#show ip igmp interface vrf green
=====
                        Igmp Interface - GlobalRouter
=====
IF      QUERY      OPER      QUERY      WRONG      LASTMEM
INTVL  STATUS  VERS.  VERS  QUERIER  MAXRSPT  QUERY  JOINS  ROBUST  QUERY  MODE
-----
V100   125     activ  2      2    0.0.0.0  100   0     0     2     10   routed-spb
1 out of 1 entries displayed
Switch:1(config)#show ip igmp interface vlan 501
=====
                        Vlan Ip Igmp
=====
VLAN  QUERY  QUERY  ROBUST  VERSION  LAST  PROXY  SNOOP  SSM    FAST  FAST
ID    INTVL  MAX    RESP    MEMB    SNOOP  SNOOP  SNOOP  SNOOP  LEAVE  LEAVE
      RESP                QUERY  ENABLE  ENABLE  ENABLE  ENABLE  PORTS
-----
501   125    100    2      2      10    false  false  false  false
VLAN  SNOOP    SNOOP                DYNAMIC  COMPATIBILITY  EXPLICIT
ID    QUERIER  QUERIER                DOWNGRADE  MODE          HOST
      ENABLE  ADDRESS                VERSION     TRACKING
-----
501   false   0.0.0.0                enable    disable       disable
```

```
Switch:1# show ip igmp sender vrf green
```

```
=====
IGMP Sender - GlobalRouter
=====
GRPADDR          IFINDEX    MEMBER      MLT          PORT/
STATE
-----
233.252.0.1     Vlan 501   192.2.0.1   9/5         NOTFILTERED
233.252.0.2     Vlan 501   192.2.0.1   9/5         NOTFILTERED
233.252.0.3     Vlan 501   192.2.0.1   9/5         NOTFILTERED
233.252.0.4     Vlan 501   192.2.0.1   9/5         NOTFILTERED
233.252.0.5     Vlan 501   192.2.0.1   9/5         NOTFILTERED
233.252.0.6     Vlan 501   192.2.0.1   9/5         NOTFILTERED
233.252.0.7     Vlan 501   192.2.0.1   9/5         NOTFILTERED
233.252.0.8     Vlan 501   192.2.0.1   9/5         NOTFILTERED
233.252.0.9     Vlan 501   192.2.0.1   9/5         NOTFILTERED
233.252.0.10    Vlan 501   192.2.0.1   9/5         NOTFILTERED
```

```
10 out of 10 entries displayed
```

```
Switch:1# show ip igmp group vrf green
```

```
=====
IGMP Group - GlobalRouter
=====
GRPADDR          INPORT     MEMBER      EXPIRATION  TYPE
-----
233.252.0.1     V501-9/16 192.2.0.1   204         Dynamic
233.252.0.2     V501-9/16 192.2.0.1   206         Dynamic
233.252.0.3     V501-9/16 192.2.0.1   206         Dynamic
233.252.0.4     V501-9/16 192.2.0.1   207         Dynamic
233.252.0.5     V501-9/16 192.2.0.1   204         Dynamic
233.252.0.6     V501-9/16 192.2.0.1   209         Dynamic
233.252.0.7     V501-9/16 192.2.0.1   206         Dynamic
233.252.0.8     V501-9/16 192.2.0.1   206         Dynamic
233.252.0.9     V501-9/16 192.2.0.1   211         Dynamic
233.252.0.10    V501-9/16 192.2.0.1   207         Dynamic
```

```
10 out of 10 group Receivers displayed
```

```
Total number of unique groups 10
```

Variable definitions

Use the data in the following table to use the **show ip igmp interface** command.

Variable	Value
gigabitethernet {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.
vlan <1-4059>	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the

Table continues...

Variable	Value
	system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
vrf <i>WORD</i> <1–16>	Specifies the VRF by name.
vrfids <i>WORD</i> <0–512>	Specifies the VRF by VRF ID.

Use the data in the following table to use the **show ip igmp cache** command.

Variable	Value
vrf <i>WORD</i> <1–16>	Specifies the VRF by name.
vrfids <i>WORD</i> <0–512>	Specifies the VRF by VRF ID.

Use the data in the following table to use the **show ip igmp group** command.

Variable	Value
count	Specifies the number of entries.
group { <i>A.B.C.D</i> }	Specifies the group address.
member-subnet { <i>A.B.C.D/X</i> }	Specifies the IP address and network mask.
vrf <i>WORD</i> <1–16>	Displays the multicast route configuration for a particular VRF by name.
vrfids <i>WORD</i> <0–512>	Displays the multicast route configuration for a particular VRF by VRF ID.

Use the data in the following table to use the **show ip igmp sender** command.

Variable	Value
count	Specifies the number of entries.
group { <i>A.B.C.D</i> }	Specifies the group address.
member-subnet { <i>A.B.C.D/X</i> }	Specifies the IP address and network mask.
vrf <i>WORD</i> <1–16>	Displays the multicast route configuration for a particular VRF by name.
vrfids <i>WORD</i> <0–512>	Displays the multicast route configuration for a particular VRF by VRF ID.

Job aid

The following table describes the fields for the **show ip igmp interface** command.

Parameter	Description
IF	Indicates the interface where IGMP is configured.

Table continues...

Parameter	Description
QUERY INTVL	Indicates the frequency at which IGMP host query packets transmit on this interface.
STATUS	Indicates the activation of a row, which activates IGMP on the interface. The destruction of a row disables IGMP on the interface.
VERS.	Indicates the version of IGMP that runs on this interface. This object configures a router capable of running either version. For IGMP to function correctly, you must configure all routers on a LAN to run the same version of IGMP.
OPER VERS	Indicates the operational version of IGMP.
QUERIER	Indicates the address of the IGMP querier on the IP subnet to which this interface attaches.
QUERY MAXRSPT	Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.
WRONG QUERY	Indicates the number of queries received where the IGMP version does not match the interface version. You must configure all routers on a LAN to run the same version of IGMP. If queries are received with the wrong version, a configuration error occurs.
JOINS	Indicates the number of times this interface added a group membership.
ROBUST	Indicates the robustness variable, which you can configure for the expected packet loss on a subnet. If you expect packet loss on a subnet, increase the robustness variable.
LASTMEM QUERY	Indicates the maximum response time (in tenths of a second) inserted into group specific queries sent in response to leave group messages, and is also the amount of time between group specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This variable does not apply to IGMPv1.
MODE	Indicates the protocol configured on the VLAN added. If routed-spb displays in the MODE column, then IP Multicast over Fabric Connect is enabled on the Layer 3 VSN or for IP Shortcuts. If snoop-spb displays in the MODE column, then IGMP is enabled on a VLAN with an associated I-SID (Layer 2 VSN).

The following table describes the fields for the `show ip igmp interface vlan` command.

Parameter	Description
VLAN ID	Identifies the VLAN where IGMP is configured.
QUERY INTVL	Indicates the frequency at which IGMP host query packets transmit on this interface.
QUERY MAX RESP	Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.
ROBUST	Indicates the robustness variable, which you can configure for the expected packet loss on a subnet. If you expect packet loss on a subnet, increase the robustness variable.
VERSION	Indicates the version of IGMP that runs on this interface. This object configures a router capable of running either version. For IGMP to function correctly, you must configure all routers on a LAN to run the same version of IGMP.
LAST MEMB QUERY	Indicates the maximum response time (in tenths of a second) inserted into group specific queries sent in response to leave group messages, and is also the amount of time between group specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This variable does not apply to IGMPv1.
PROXY SNOOP ENABLE	Indicates if proxy snoop is enabled on the interface.
SNOOP ENABLE	Indicates if snoop is enabled on the interface.
SSM SNOOP ENABLE	Indicates if SSM snoop is enabled on the interface.
FAST LEAVE ENABLE	Indicates if fast leave mode is enabled on the interface.
FAST LEAVE PORTS	Indicates the set of ports that are enabled for fast leave.
VLAN ID	Identifies the VLAN where IGMP is configured.
SNOOP QUERIER ENABLE	Indicates if the IGMP Layer 2 Querier feature is enabled.
SNOOP QUERIER ADDRESS	Indicates the IP address of the IGMP Layer 2 Querier.
DYNAMIC DOWNGRADE VERSION	Indicates if the dynamic downgrade feature is enabled.
COMPATIBILITY MODE	Indicates if compatibility mode is enabled.
EXPLICIT HOST TRACKING	Indicates if explicit host tracking is enabled to track all the source and group members.

The following table describes the fields for the `show ip igmp cache` command.

Parameter	Description
GRPADDR	Indicates the multicast group address (Class D) that others want to join. Many incoming ports can use the same group address.
INTERFACE	Indicates the physical interface or a logical interface (VLAN), which received group reports from various sources.
LASTREPORTER	Indicates the IP address of the source of the last membership report received for this IP multicast group address on this interface. If the interface does not receive a membership report, this object uses the value 0.0.0.0.
EXPIRATION	Indicates the minimum amount of time that remains before this entry ages out.
V1HOSTIMER	Indicates the time that remains until the local router assumes that no IGMPv1 members exist on the IP subnet attached to this interface.
TYPE	Indicates whether the entry is learned dynamically or is added statically.
STATICPORTS	Indicates the list of statically-defined ports.

The following table describes the fields for the `show ip igmp group` command.

Parameter	Description
GRPADDR	Indicates the multicast group address (Class D) that others want to join. Many incoming ports can use the same group address.
INPORT	Indicates the physical interface or a logical interface (VLAN), which received group reports from various sources.
MEMBER	Indicates the IP address of a source that sent a group report to join this group.
EXPIRATION	Indicates the minimum amount of time that remains before this entry ages out.
TYPE	Indicates whether the entry is learned dynamically or is added statically.

The following table describes the fields for the `show ip igmp sender` command.

Parameter	Description
GRPADDR	Indicates the IP multicast address.
IFINDEX	Indicates the interface index number.
MEMBER	Indicates the IP address of the host.
PORT/MLT	Indicates the IGMP sender ports.

Table continues...

Parameter	Description
STATE	Indicates if a sender exists because of an IGMP access filter. Options include filtered and nonfiltered.

Viewing TLV information for a Layer 3 VSN with IP Multicast over Fabric Connect

Use the following commands to check TLV information.

For a Layer 3 VSN multicast, TLV 185 on the BEB where the source is located displays the multicast source and group addresses and have the Tx bit set. Each multicast group should have its own unique data I-SID with a value between 16,000,000 to 16,512,000. TLV 144 on the BEB bridge, where the sender is located, has the Tx bit set. All BEB bridges, where a receiver exists, have the Rx bit set.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display IS-IS Link State Database information by TLV:


```
show isis lsdb tlv <1-236> [sub-tlv <1-3>][detail]
```
3. Display IS-IS Link State Database information by Link State Protocol ID:


```
show isis lsdb lspid <xxxx.xxxx.xxxx.xx-xx> [tlv <1-236>] [sub-tlv <1-3>] [detail]
```

Example

Display TLV information for a Layer 3 VSN with IP Multicast over Fabric Connect:

```
Switch:1# show isis lsdb tlv 185 detail
=====
                ISIS LSDB (DETAIL)
=====
Level-1 LspID: 000c.f803.83df.00-04 SeqNum: 0x000002eb Lifetime: 1113
Chksum: 0x7e3b PDU Length: 556
Host name: e12
Attributes: IS-Type 1
TLV:185 SPBM IPVPN :
  VSN ISID:5010
  BVID :10
    Metric:0
    IP Source Address: 192.0.2.10
    Group Address : 233.252.0.1
    Data ISID : 16300011
    TX : 1
    Metric:0
    IP Source Address: 192.0.2.10
    Group Address : 233.252.0.3
    Data ISID : 16300013
    TX : 1
    Metric:0
    IP Source Address: 192.0.2.10
    Group Address : 233.252.0.5
    Data ISID : 16300015
    TX : 1
```



```

Metric:0
IP Source Address: 192.0.2.10
Group Address : 233.252.0.7
Data ISID : 16300017
TX : 1
Metric:0
IP Source Address: 192.0.2.10
Group Address : 233.252.0.9
Data ISID : 16300019
TX : 1
VSN ISID:5010
BVID :20
Metric:0
IP Source Address: 192.0.2.10
Group Address : 233.252.0.2
Data ISID : 16300012
TX : 1
Metric:0
IP Source Address: 192.0.2.10
Group Address : 233.252.0.4
Data ISID : 16300014
TX : 1
Metric:0
IP Source Address: 192.0.2.10
Group Address : 233.252.0.6
Data ISID : 16300016
TX : 1
Metric:0
IP Source Address: 192.0.2.10
Group Address : 233.252.0.8
Data ISID : 16300018
TX : 1
Metric:0
IP Source Address: 192.0.2.10
Group Address : 233.252.0.10
Data ISID : 16300020
TX : 1

```

Variable definitions

Use the data in the following table to use the `show isis lsdb` command.

Variable	Value
detail	Displays detailed information about the IS-IS Link State database.
level {1, 12, 112}	Displays information on the IS-IS level. The IEEE 802.1aq standard currently only defines the use of one hierarchy, Level 1. Level 2 function is disabled.
local	Displays information on the local LSDB.
lspid <xxxx.xxxx.xxxx.xx-xx>	Specifies information about the IS-IS Link State database by LSP ID.
sub-tlv <1-3>	Specifies information about the IS-IS Link State database by sub-TLV.
sysid <xxxx.xxxx.xxxx>	Specifies information about the IS-IS Link State database by System ID.
tlv <1-236>	Specifies information about the IS-IS Link State database by TLV.

Job aid

The following table describes the fields for the `show isis lsdB tlv` and the `show isis lsdB lspid` commands.

Parameter	Description
LSP ID	Indicates the LSP ID assigned to external IS-IS routing devices.
LEVEL	Indicates the level of the external router: I1, I2, or I12.
LIFETIME	Indicates the maximum age of the LSP. If the max-lsp-gen-interval is set to 900 (default), then the lifetime value begins to count down from 1200 seconds and updates after 300 seconds if connectivity remains. If the timer counts down to zero, the counter adds on an additional 60 seconds, then the LSP for that router is lost. This happens because of the zero age lifetime, which is detailed in the RFC standards.
SEQNUM	Indicates the LSP sequence number. This number changes each time the LSP is updated.
CKSUM	Indicates the LSP checksum. This is an error checking mechanism used to verify the validity of the IP packet.
HOST-NAME	Indicates the host-name.

Layer 3 VSN configuration using EDM

This section provides procedures to configure Layer 3 Virtual Services Networks (VSNs) using Enterprise Device Manager (EDM).

Enabling MVPN for a VRF

Use this procedure to enable MVPN for a particular VRF. IP Multicast over Fabric Connect, constrains multicast streams of senders to all receivers in the same Layer 3 VSN. MVPN functionality is disabled by default.

 **Note:**

VLAN level configuration is also required to turn on the service on each VLAN within the VRF on which this services is required. You can turn it on under the VLAN context or the brouter context.

Before you begin

- You must enable IP Multicast over Fabric Connect globally.

Procedure

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

2. Click **IP-MVPN**.
3. Click the **MVPN** tab.
4. Double-click in the **Enable** field in the table.
5. Select **Enable** from the drop down menu.
6. Double-click in the **FwdCacheTimeout** field in the table, and then type the VRF timeout value.
7. Click **Apply**.

MVPN field descriptions

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

Name	Description
Vrflid	Specifies the VRF ID.
Enable	Enables Layer 3 VSN IP Multicast over Fabric Connect services for a particular VRF. The default is disabled.
FwdCacheTimeout	Specifies the VRF timeout value. The timeout value ages out the sender when there is no multicast stream on the VRF. The default is 210 seconds..

Viewing the IGMP interface table

Use the Interface tab to view the IGMP interface table. When an interface does not use an IP address, it does not appear in the IGMP table.

Procedure

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

Configuring IP Multicast over Fabric Connect on a VLAN for Layer 3

Use this procedure to enable IP Multicast over Fabric Connect for a Layer 3 VSN. The default is disabled.

To configure a VLAN for IP Shortcuts with IP Multicast over Fabric Connect, see [Configuring IP Multicast over Fabric Connect on a VLAN within the GRT](#) on page 79.

* Note:

On DvR Controllers in a DvR domain, you must manually configure IP multicast over Fabric Connect on Layer 3 VSNs (VRFs). This configuration is then automatically pushed to the Leaf nodes in the DvR domain.

For more information on DvR, see *Configuring IPv4 Routing*.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must configure a VRF and an IP VPN instance with an I-SID configured under it on the switch. The IP VPN does not need to be enabled for Layer 3 VSN multicast to function.
- You must enable IP Multicast over Fabric Connect globally.
- If there is no IP interface on the VLAN, then you create one. (The IP interface must be in the same subnet as the IGMP hosts that connect to the VLAN).
- You must enable MVPN for the particular VRF.

About this task

You must configure VLANs to turn on the service on each VLAN with in the VRF on which the service is required. You can turn it on under the VLAN context or the brouter context.

If you only want to use IP Multicast over Fabric Connect, you do not need to enable the Layer 3 VSN or redistribute unicast routes into or out of IS-IS. IP Multicast over Fabric Connect routing does not depend on unicast routing (for Layer 3 VSN). This allows for you to more easily migrate from a PIM environment to IP Multicast over Fabric Connect. You can migrate a PIM environment to IP Multicast over Fabric Connect first and then migrate unicast separately or not at all.

The switch only supports IPv4 address with IP Multicast over Fabric Connect.

Note:

You cannot enable IP PIM when IP Multicast over Fabric Connect is enabled on the VLAN.

Procedure

1. In the navigation pane, expand the **Configuration > VRF Context View** folders.
2. Click **Set VRF Context View**.
3. Choose a VRF name.
4. Click **Launch VRF Context View**.
5. Select an enabled port on the Physical Device View.
6. In the navigation pane, expand the **Configuration > VLAN** folders.
7. Click **VLANs**.
8. Choose a VLAN, and then click the **IP** from under the tab bar.
9. Click the **SPB Multicast** tab.
10. Check the **Enable** box.
11. Click **Apply**.

Configuring IP Multicast over Fabric Connect on a brouter port for a Layer 3 VSN

Use this procedure to enable IP Multicast over Fabric Connect on a brouter port. The default is disabled.

To configure a brouter port for IP Shortcuts with IP Multicast over Fabric Connect, see [Configuring IP Multicast over Fabric Connect on a brouter port within the GRT](#) on page 80.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must configure a VRF and an IP VPN instance with an I-SID configured under it on the switch. The IP VPN does not need to be enabled for Layer 2 VSN multicast to function.
- You must enable IP Multicast over Fabric Connect globally.
- If there is no IP interface on the VLAN, then you create one. (The IP interface must be in the same subnet as the IGMP hosts that connect to the VLAN).
- You must enable MVPN for the particular VRF.

About this task

You must enable IP Multicast over Fabric Connect on each of the VLANs that need to support IP multicast traffic.

If you only want to use IP Multicast over Fabric Connect, you do not need to enable the Layer 3 VSN or redistribute unicast routes into or out of IS-IS. IP Multicast over Fabric Connect routing does not depend on unicast routing, which allows for you to more easily migrate from a PIM environment to Multicast over Fabric Connect. You can migrate a PIM environment to IP Multicast over Fabric Connect first, and then migrate unicast separately or not at all.

The switch only supports IPv4 address with IP Multicast over Fabric Connect.

Procedure

1. In the navigation pane, expand the **Configuration > VRF Context View** folders.
2. Click **Set VRF Context View**.
3. Choose a VRF name.
4. Click **Launch VRF Context View**.
5. Select an enabled port on the Physical Device View.
6. In the navigation pane, expand the **Configuration > Edit > Port** folders.
7. Click **IP**.
8. Click the **SPB Multicast** tab.
9. Click **Enable**.
10. Click **Apply**.

Configuring IGMP on a VLAN interface for a Layer 3 VRF

Use this procedure to configure IGMP for each VLAN interface to enable the interface to perform multicast operations.

IGMPv2 at the VLAN level is the default setting, with no other configuration required. You only need to enable IGMPv3. You must enable SSM snoop before you configure IGMP version 3, and you must enable both ssm-snoop and snooping for IGMPv3.

For IGMP Snooping, ensure that the IGMP version used by multicast hosts and other devices in the network is the same as the IGMP version configured on the IGMP Snooping VLAN, or that you enable compatibility mode.

*** Note:**

You cannot enable IP PIM when IP Multicast over Fabric Connect is enabled on the VLAN.

Before you begin

- You must configure the required SPBM IS-IS infrastructure.
- You must configure a VRF and IP VPN instance with an I-SID on the switch.
- You must create the C-VLANs and add slots/ports.
- You must enable IP Multicast over Fabric Connect for a Layer 3 VSN.

About this task

For IGMP Snooping, ensure that the IGMP version used by multicast hosts and other devices in the network is the same as the IGMP version configured on the IGMP Snooping VLAN, or that you enable compatibility mode.

Procedure

1. In the navigation pane, expand the **Configuration > VRF Context View** folders.
2. Click **Set VRF Context View**.
3. Choose a VRF name.
4. Click **Launch VRF Context View**.
5. In the navigation pane, expand the **Configuration > VLAN** folders.
6. Click **VLANs**.
7. Select the desired VLAN from the listing.
8. Click the **IP** button.
9. Click the **IGMP** tab.
10. **(Optional)** If you want to enable SsmSnoopEnable, select the **SsmSnoopEnable** box.
11. **(Optional)** If you want to enable Snoop, select the **SnoopEnable** box.
12. **(Optional)** In the **Version** box, select the correct IGMP version.

You must enable SSM snoop before you configure IGMP version 3, and you must enable both ssm-snoop and snooping for IGMPv3.

13. **(Optional)** Select **SnoopQuerierEnable**, to enable Snoop Querier. Only select this option, if you want to configure an address for the IGMP queries.
14. **(Optional)** In the **SnoopQuerierAddr** box, type an IP address, if you want to configure a snoop querier address.

*** Note:**

If the SPBM bridge connects to an edge switch, it can be necessary to add an IGMP query address. If you omit adding a query address, the SPB bridge sends IGMP queries with a source address of 0.0.0.0. Some edge switch models do not accept a query with a source address of 0.0.0.0.

IGMP field descriptions

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

Name	Description
QueryInterval	Configures the frequency (in seconds) at which the IGMP host query packets transmit on the interface. The range is from 1–65535 and the default is 125.
QueryMaxResponseTime	<p>Configures the maximum response time (in tenths of a second) advertised in IGMPv2 general queries on this interface. You cannot configure this value for IGMPv1.</p> <p>Smaller values allow a router to prune groups faster. The range is from 0–255 and the default is 100 tenths of a second (equal to 10 seconds.)</p> <p>! Important: You must configure this value lower than the QueryInterval.</p>
Robustness	<p>Configure this parameter to tune for the expected packet loss of a network. This value is equal to the number of expected query packet losses for each serial query interval, plus 1. If you expect the network to lose query packets, increase the robustness value.</p> <p>The range is from 2–255 and the default is 2. The default value of 2 means that the switch drops one query for each query interval without the querier aging out.</p>
LastMembQueryIntvl	<p>Configures the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages. This value is also the time between group-specific query messages. You cannot configure this value for IGMPv1.</p> <p>Decreasing the value reduces the time to detect the loss of the last member of a group. The range is from 0–255 and the default is 10 tenths of a second.</p> <p>Configure this parameter to values greater than 3. If you do not require a fast leave process, use values greater than 10. (The value 3 is equal to 0.3 seconds, and 10 is equal to 1 second.)</p>
SnoopEnable	Enables or disables snoop.
SsmSnoopEnable	Enables or disables support for SSM on the snoop interface.
ProxySnoopEnable	Enables or disables proxy snoop.

Table continues...

Name	Description
Version	Configures the version of IGMP (1, 2, or 3) that you want to use on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. The default is version 2. For IGMP Snooping, ensure that the IGMP version used by multicast hosts and other devices in the network is the same as the IGMP version configured on the IGMP Snooping VLAN, or that you enable compatibility mode.
FastLeaveEnable	Enables or disables fast leave on the interface.
StreamLimitEnable	Enables or disables stream limitation on this VLAN.
Maximum Number Of Stream	Configures the maximum number of streams allowed on this VLAN. The range is from 0–65535 and the default is 4.
Current Number Of Stream	Displays the current number of streams. This value is a read-only value.
FastLeavePortMembers	Selects the ports that are enabled for fast leave.
SnoopMRouterPorts	Selects the ports in this interface that provide connectivity to an IP multicast router.
DynamicDowngradeEnable	Configures if the switch downgrades the version of IGMP to handle older query messages. If the switch downgrades, the host with IGMPv3 only capability does not work. If you do not configure the switch to downgrade the version of IGMP, the switch logs a warning. The default value is selected (enabled), which means the switch downgrades to the oldest version of IGMP on the network.
CompatibilityModeEnable	Enables or disables v2-v3 compatibility mode. The default value is clear (disabled), which means IGMPv3 is not compatible with IGMPv2.
ExplicitHostTrackingEnable	Enables or disables IGMPv3 to track hosts per channel or group. The default is disabled. You must select this field if you want to use fast leave for IGMPv3.
SnoopQuerierEnable	Enables Snoop Querier. The default is disabled. When you enable IGMP Layer 2 Querier, Layer 2 switches in your network can snoop IGMP control packets exchanged with downstream hosts and upstream routers. The Layer 2 switches then generate the Layer 2 MAC forwarding table, used for switching sessions and multicast traffic regulation, and provide the recurring queries required to maintain IGMP groups. Enable Layer 2 Querier on only one node in the VLAN.
SnoopQuerierAddr	Specifies the pseudo IP address of the IGMP Snoop Querier. The default IP address is 0.0.0.0. If the SPBM bridge connects to an edge switch, it can be necessary to add an IGMP query address. If you omit adding a query address, the SPBM bridge sends IGMP queries with a source address of

Table continues...

Name	Description
	0.0.0.0. Some edge switch models do not accept a query with a source address of 0.0.0.0.

Configuring the Global Routing Table timeout value

Use this procedure to configure the timeout value in the GRT. The timeout value ages out the sender when there are no multicast streams coming from the sender for a specified period of time. The default timeout value is 210 seconds.

Before you begin

- You must configure the required SPBM and IS-IS infrastructure, which includes the creation of SPBM B-VLANs.
- You must create the C-VLANs and add slots/ports.
- You must enable IP Multicast over Fabric Connect globally.

Procedure

1. In the navigation pane, expand the **Configuration > IS-IS > SPBM** folders.
2. Click the **SPBM** tab.
3. Modify the **McastFwdCacheTimeout** value.
4. Click **Apply**.

Layer 3 VSN configuration example

Layer 3 VSN with IP Multicast over Fabric Connect configuration example

The example below shows the configuration to enable IP Multicast over Fabric Connect support on VLANs 500 and 501 that are part of VRF Green:

```

ISIS SPBM CONFIGURATION

router isis
spbm 1 multicast enable

VRF CONFIGURATION

ip vrf green vrfid 2

VLAN CONFIGURATION - PHASE 1

vlan 110 i-sid 100
interface vlan 500
vrf green
ip address 192.0.2.1 255.255.255.0 1
ip spb-multicast enable
exit

vlan 111 i-sid 100
interface vlan 501

```

IP Multicast over Fabric Connect services configuration

```
vrf green
ip address 192.0.2.2 255.255.0 0
ip spb-multicast enable
exit
```

ISIS SPBM IPVPN CONFIGURATION

```
router vrf green
ipvpn
i-sid 100
mvpn enable
exit
```

When using IGMPv3, the configuration is:

ISIS SPBM CONFIGURATION

```
router isis
spbm 1 multicast enable
```

VRF CONFIGURATION

```
ip vrf green vrfid 2
```

VLAN CONFIGURATION - PHASE 1

```
vlan 110 i-sid 100
interface vlan 500
vrf green
ip address 192.0.2.1 255.255.255.0 1
ip spb-multicast enable
ip igmp version 3
exit
```

```
vlan 111 i-sid 100
interface vlan 501
vrf green
ip address 192.0.2.2 255.255.0 0
ip spb-multicast enable
ip igmp version 3
exit
```

ISIS SPBM IPVPN CONFIGURATION

```
router vrf green
ipvpn
i-sid 100
mvpn enable
exit
```

Chapter 6: SPB-PIM Gateway configuration

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.

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.

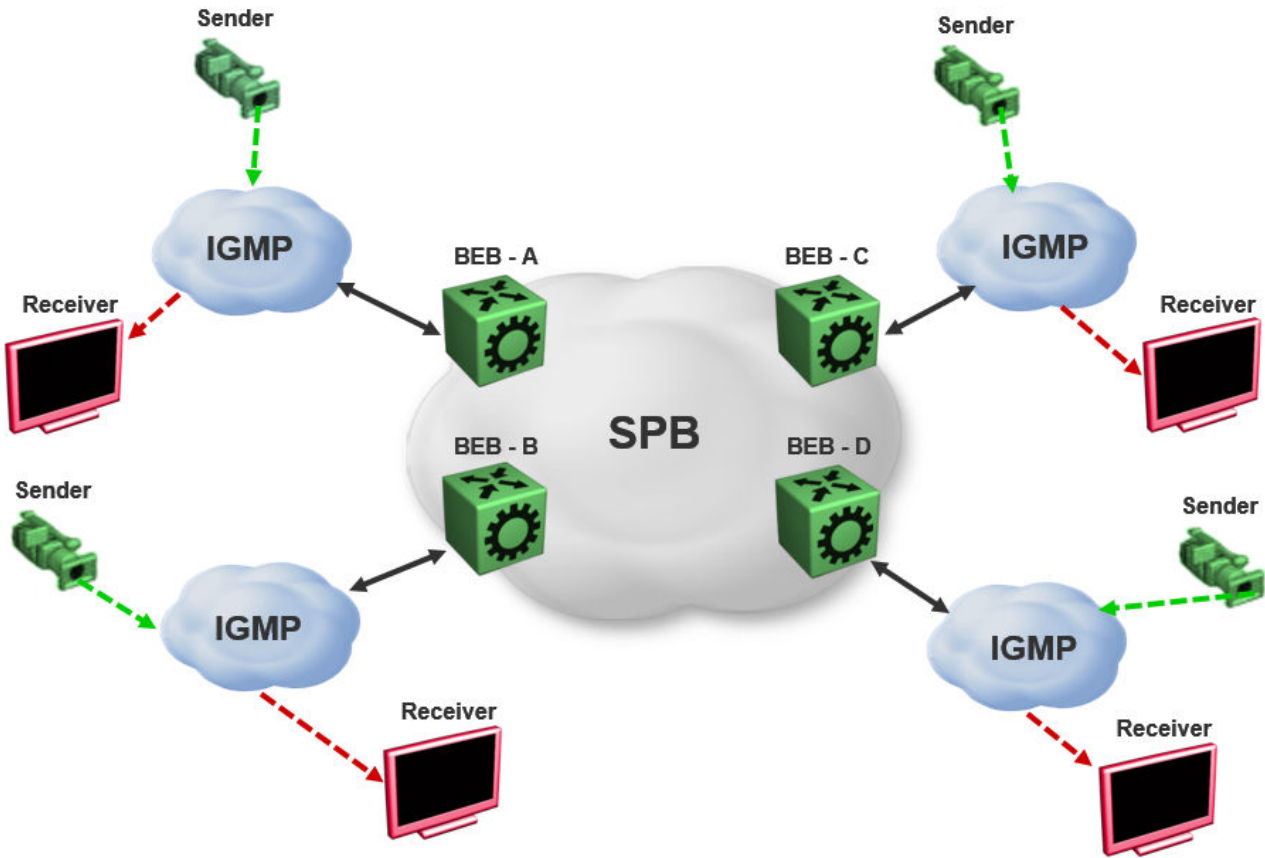


Figure 3: IP Multicast over Fabric Connect streams

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.

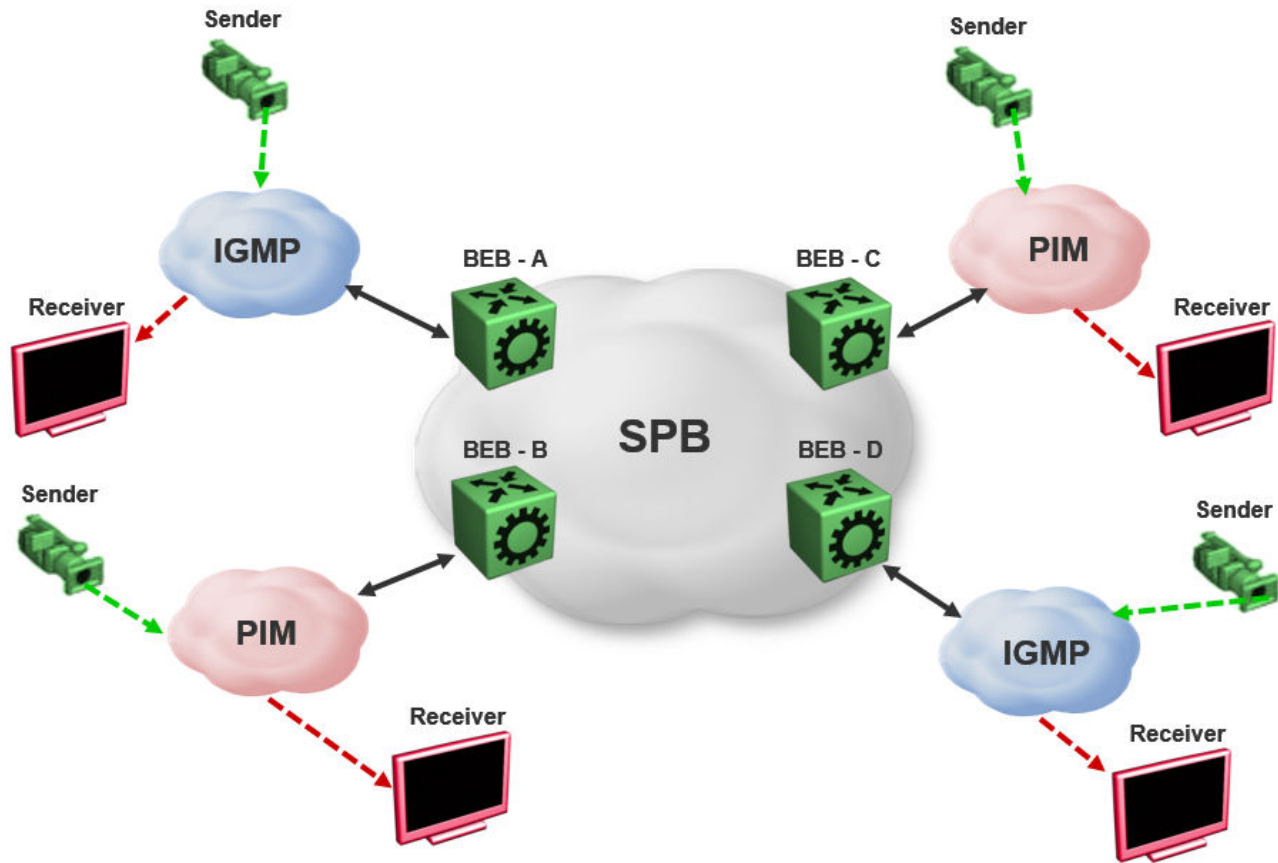


Figure 4: IP Multicast over Fabric Connect Streams

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.

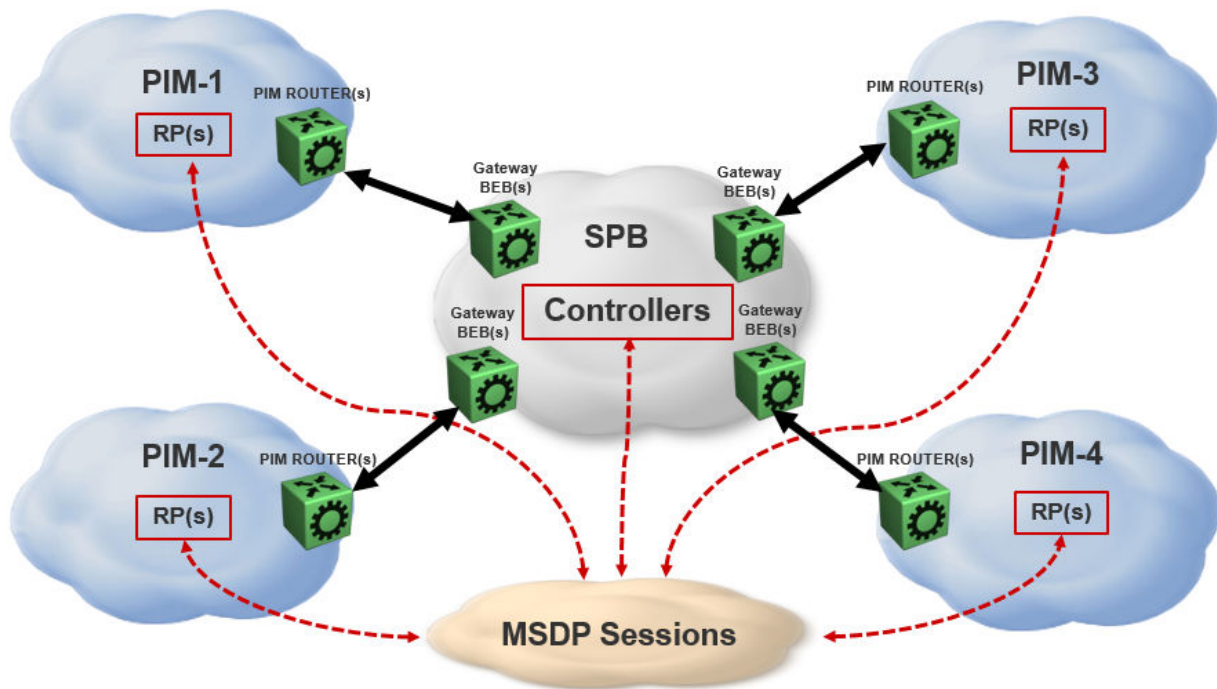


Figure 5: Multicast over Fabric Connect with SPB-PIM GW

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.

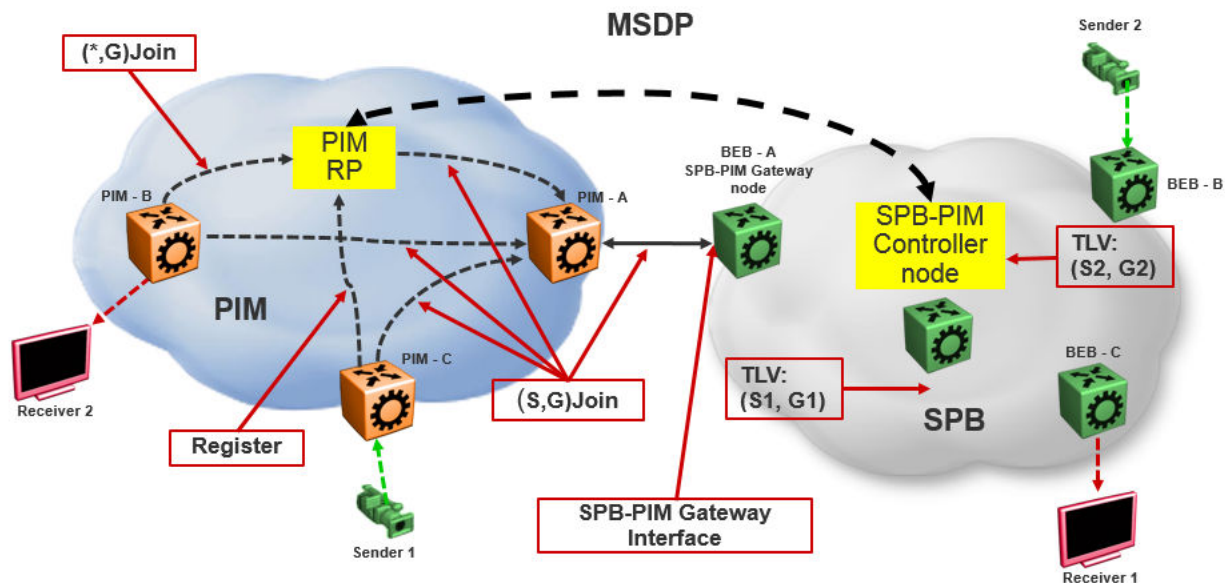


Figure 6: SPB-PIM GW components

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 124.

* 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 127.

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.

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. Default value is 1.

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.

Table continues...

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

SPB-PIM Gateway configuration

```
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
<code>group{A.B.C.D}</code>	Displays all SA cache entries that match the group IP address.
<code>local</code>	Displays the local SA cache.
<code>rp{A.B.C.D}</code>	Displays all SA cache entries that match the RP IP address.
<code>source{A.B.C.D}</code>	Displays all SA cache entries that match the source IP address.
<code>vrf WORD<0-16></code>	Displays configuration information for a particular VRF.
<code>vrfids WORD<0-512></code>	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/ Downtime	Established Count	SA 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 <i>WORD<0-16></i>	Displays configuration information for a particular VRF.
vrfids <i>WORD<0-512></i>	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
{ <i>A.B.C.D</i> }	Specifies the RP IP address.
vrf <i>WORD<0-16></i>	Displays configuration information for a particular VRF.
vrfids <i>WORD<0-512></i>	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 WORD<0-16>	Displays configuration information for a particular VRF.
vrfids WORD<0-512>	Displays configuration information for a particular VRF ID.
WORD<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
=====
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:
  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/ Downtime	Established Count	SA 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.
RPAAddress	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.

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).
ClearPeer	Clears the TCP connection to the specified MSDP peer and resets all MSDP message counters. 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 1–255. The default value is 1, 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.

Table continues...

Name	Description
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.
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

Table continues...

Name	Description
	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 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.

Table continues...

Name	Description
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 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).
ClearPeer	Clears the TCP connection to the specified MSDP peer and resets all MSDP message counters. The default value is disabled (false).

Table continues...

Name	Description
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 1–255. The default value is 1, 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.

Table continues...

Name	Description
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 in the value of this counter can occur at reinitialization of the management system.

Table continues...

Name	Description
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 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).
ClearPeer	Clears the TCP connection to the specified MSDP peer and resets all MSDP message counters. 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 1–255. The default value is 1, 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.

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.
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).
ClearPeer	Clears the TCP connection to the specified MSDP peer and resets all MSDP message counters. 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 1–255. The default value is 1, 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

Table continues...

Name	Description
	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.
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.

Table continues...

Name	Description
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 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.

Table continues...

Name	Description
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 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).
ClearPeer	Clears the TCP connection to the specified MSDP peer and resets all MSDP message counters. 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 1–255. The default value is 1, 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

Table continues...

Name	Description
	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.
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.

Table continues...

Name	Description
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 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.

Table continues...

Name	Description
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 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).
ClearPeer	Clears the TCP connection to the specified MSDP peer and resets all MSDP message counters. 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 1–255. The default value is 1, 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.

Table continues...

Name	Description
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.
InDataPackets	Shows the total number of encapsulated packets received on this TCP connection. Discontinuities in

Table continues...

Name	Description
	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.
SAsAdvertisedToThisPeer	Shows the total number of SAs advertised from this peer.

Table continues...

Name	Description
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).
ClearPeer	Clears the TCP connection to the specified MSDP peer and resets all MSDP message counters. 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 1–255. The default value is 1, 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.

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).
ClearPeer	Clears the TCP connection to the specified MSDP peer and resets all MSDP message counters. 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 1–255. The default value is 1, 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.

Table continues...

Name	Description
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.
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.

Table continues...

Name	Description
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 appears as the autonomous system number of the peer.
TooShortMessages	Shows the number of short messages received from this peer.

Table continues...

Name	Description
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.

Clearing the MSDP peer connection

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

The default is disabled (false).

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 **ClearPeer** 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).

Table continues...

Name	Description
ClearPeer	Clears the TCP connection to the specified MSDP peer and resets all MSDP message counters. 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 1–255. The default value is 1, 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.

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).
ClearPeer	Clears the TCP connection to the specified MSDP peer and resets all MSDP message counters. 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 1–255. The default value is 1, 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

Table continues...

Name	Description
	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.
OutSARquests	Shows the number of MSDP SA-Request messages sent on this connection. Discontinuities in the value

Table continues...

Name	Description
	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.
AsNumber	Specifies the autonomous system number of the MSDP peer. A peer can appear to be in another

Table continues...

Name	Description
	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).
ClearPeer	Clears the TCP connection to the specified MSDP peer and resets all MSDP message counters. 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 1–255. The default value is 1, 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.

Table continues...

Name	Description
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.
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.

Table continues...

Name	Description
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 appears as the autonomous system number of the peer.
TooShortMessages	Shows the number of short messages received from this peer.

Table continues...

Name	Description
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.
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).
ClearPeer	Clears the TCP connection to the specified MSDP peer and resets all MSDP message counters. 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 1–255. The default value is 1, 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

Table continues...

Name	Description
	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.
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.

Table continues...

Name	Description
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 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.

Table continues...

Name	Description
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.

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  VLAN        VLAN      NAME      TRAP
-----
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
-----
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>] [vrffids 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</i> <0-16>	Displays information from the Controller foreign source database for a specific VRF name.
vrfids <i>WORD</i> <0-512>	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.

Table continues...

Variable	Value
<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 <i>WORD</i> <0-16>	Displays SPB originated sources for a specific VRF.
vrfids <i>WORD</i> <0-512>	Displays SPB originated sources 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 a specific source IP address from SPB originated sources database.
group { <i>A.B.C.D</i> }	Displays information for a specific multicast group IP address from SPB originated sources database.
originator <i>WORD</i> <0-32>	Displays information for a specific originator host name from SPB originated sources database.
<i>spb-node-as-mac</i>	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 198

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.

Node field descriptions

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

Name	Description
MacAddress	Shows the MAC address of the active node.
HostName	Shows the host name of the active node.
RoleType	Shows the role of the active node: either gateway, controller, or both.

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 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.
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.

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 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.

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 218.

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:

```
spbm <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)#spbm 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'.
<i>source {A.B.C.D}</i>	Displays information for the specific source IP address from the Gateway foreign source database.
<i>group {A.B.C.D}</i>	Displays information for the specific multicast group IP address from the Gateway foreign source database.
<i>from-controller 0x00:0x00:0x00:0x00:0x00:0x00</i>	Displays information filtering on a specific Controllers assignments, where the Controller is specified as a mac address.
<i>from-controller preferred</i>	Displays information from Gateway source database filtering on a preferred Controller or chosen by the Gateway.
<i>static</i>	Displays information from the Gateway foreign source database that is configured statically at the assigning Controller.

Table continues...

Variable	Value
<i>msdp</i>	Displays information from the Gateway foreign source database that is learned through MSDP.
<i>spb-node-as-mac</i>	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.

Table continues...

Name	Description
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.
OwnerType	Displays if the owner is MSDP or static.

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.

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 brouter port optional parameters

Configure the SPB-PIM Gateway interface parameters 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. 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 `spbm <spbm-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
<code>{slot/port[/sub-port]} [-slot/port[/sub-port]] [,...]</code>	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.
<code>vrf WORD<0-16></code>	Displays SPB-PIM Gateway interface information for a specific VRF.
<code>vrfids WORD<0-512></code>	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 WORD<0-16>	Displays the SPB-PIM Gateway interface neighbor information for a specific VRF name.

Table continues...

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

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
=====
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. <p>* Note: Enter a single VRF ID or multiple VRF IDs separated by ',' or enter a range of VRF IDs 'x-y'.</p>

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
Enable	Enables SPB-PIM Gateway on the interface. The default is disabled.
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.

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 optional parameters

Perform this procedure to configure the optional parameters on existing SPB-PIM Gateway interfaces.

Procedure

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

Interfaces field descriptions

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

Name	Description
IfIndex	Shows the interface index.
OperState	Shows the operational state of the interface.
AddressType	Shows the address type of the interface.
Address	Shows the address assigned to the interface.
AddressMask	Shows the address mask associated with the interface address.
HelloInterval	Configures the PIM HELLO transmission interval. The default is 30 seconds.
JoinPruneInterval	Configures the PIM JOIN PRUNE transmission interval. The default 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. 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 brouter 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.

Table continues...

Name	Description
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.

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.
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)

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 234, 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).

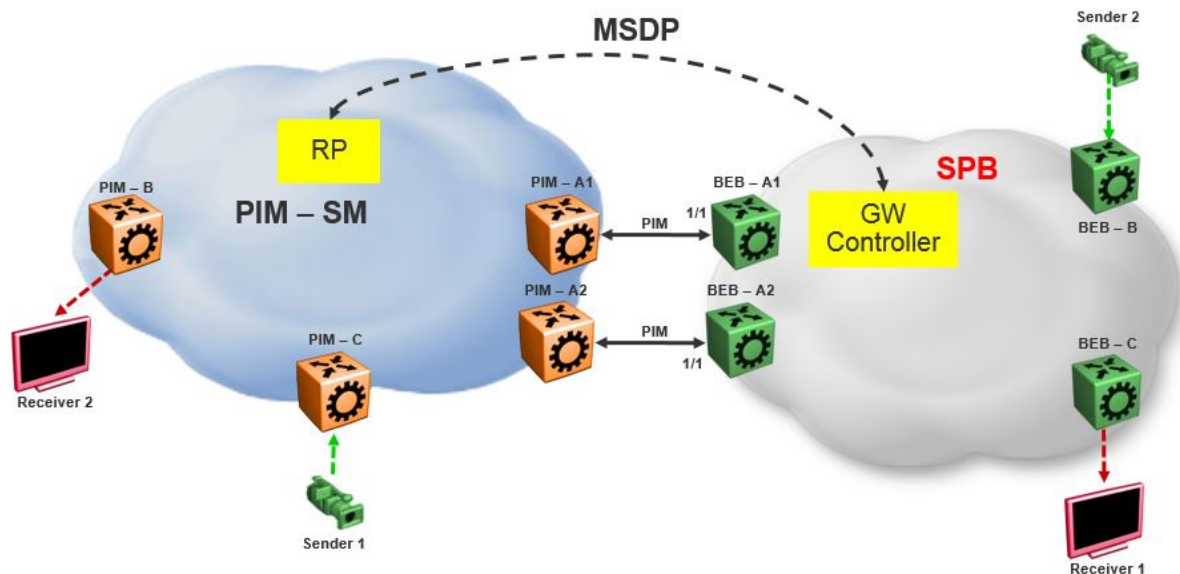


Figure 7: SPB-PIM Gateway base case configuration

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 0
Switch:1(config)#vlan members add 2100 1/3 portmember
```

SPB-PIM Gateway configuration

```
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 0
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:

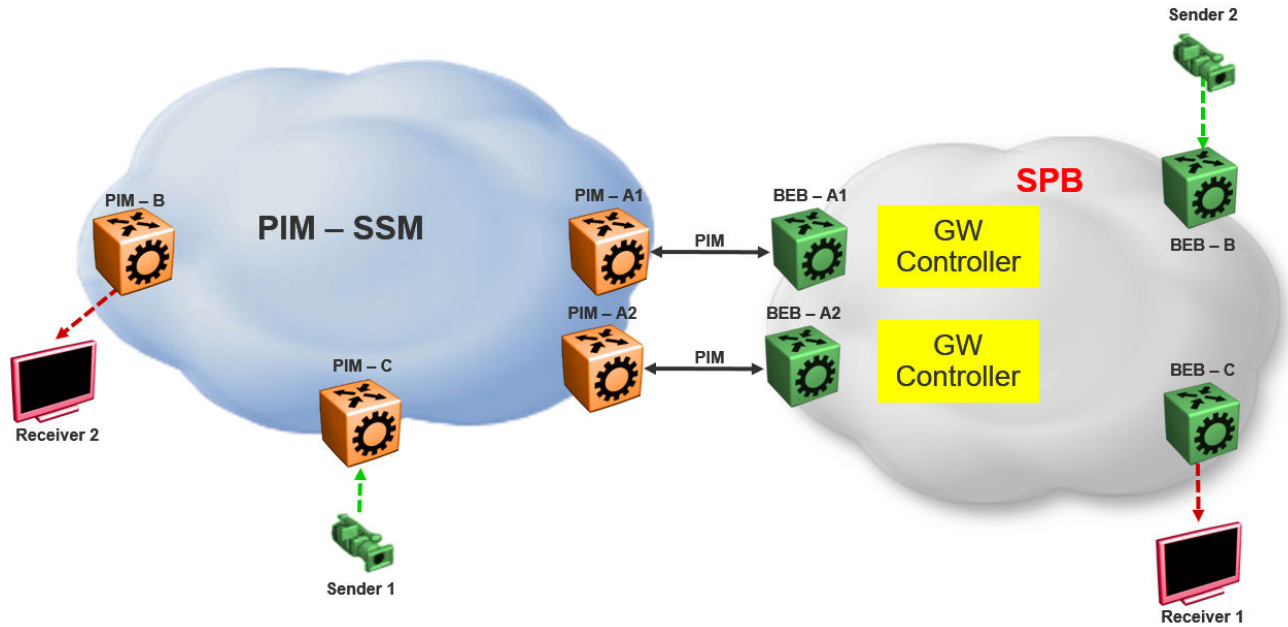


Figure 8: Static configuration of SSM groups in Controllers

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.

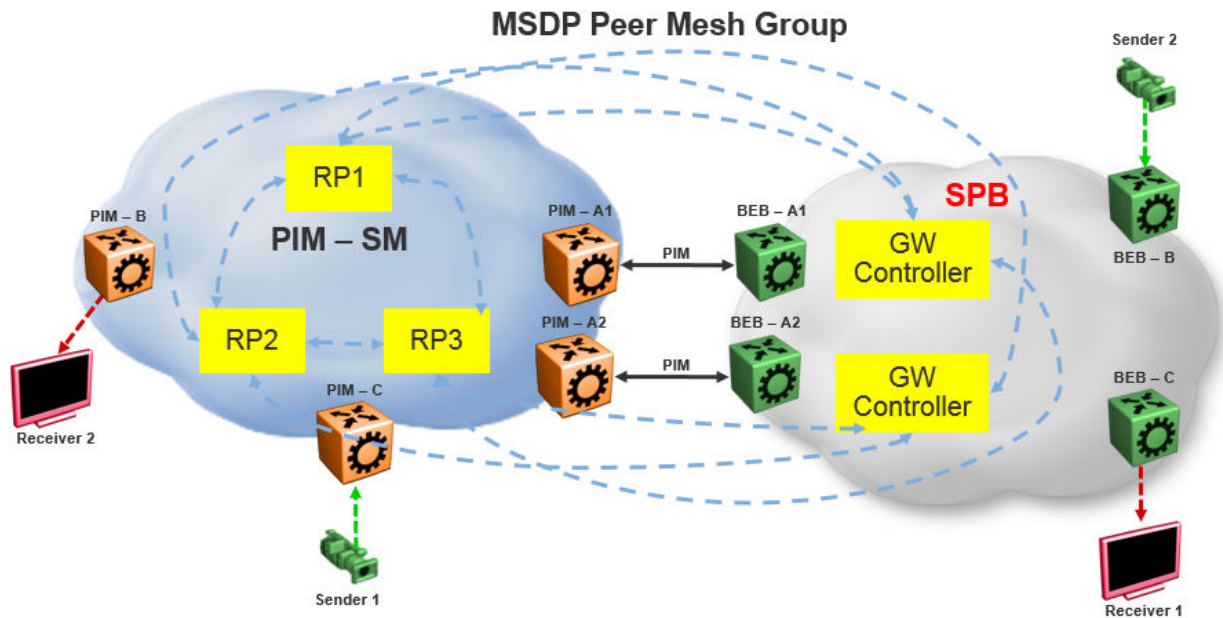


Figure 9: Peer Mesh Group

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:

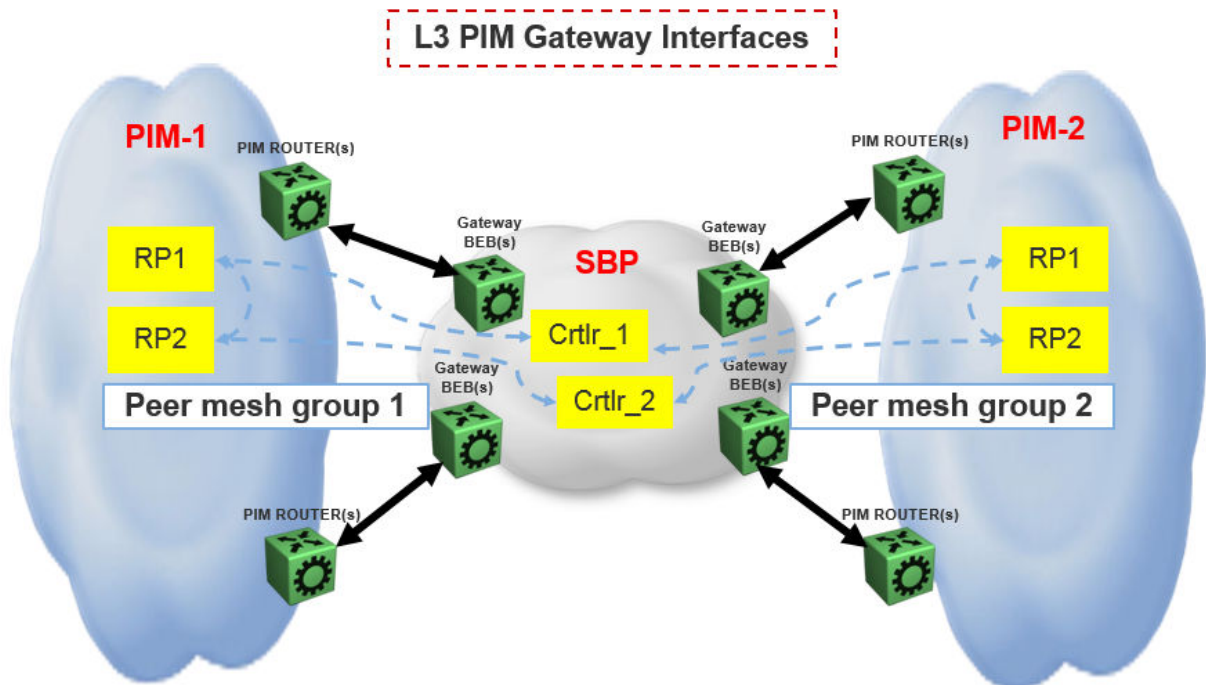


Figure 10: Multi domain configuration

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.

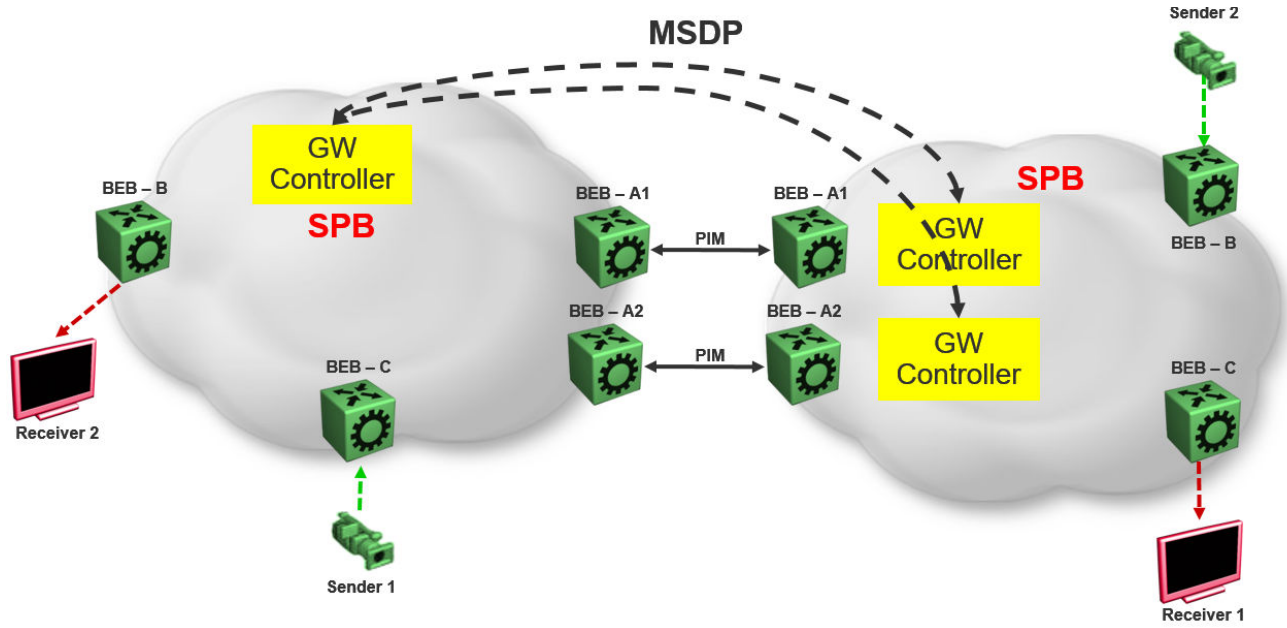


Figure 11: SPB domain interconnect

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.