CONFIGURATION GUIDE

RUCKUS FastIron IP Multicast Configuration Guide, 09.0.10

Supporting FastIron Software Release 09.0.10

Part Number: 53-1005721-02
Publication Date: 03 February 2022

Copyright, Trademark and Proprietary Rights Information

© 2022 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.commscope.com/ruckus and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://forums.ruckuswireless.com/
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.commscope.com/ruckus .

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{**x**| **y**| **z**}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x|**y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

About This Document

Supported Hardware

This guide supports the following RUCKUS products:

- RUCKUS ICX 7850 Switch
- RUCKUS ICX 7650 Switch
- RUCKUS ICX 7550 Switch
- RUCKUS ICX 7450 Switch
- RUCKUS ICX 7250 Switch
- RUCKUS ICX 7150 Switch

For information about what models and modules these devices support, refer to the hardware installation guide for the specific product family.

What's New in this Document

The following table describes the changes to this guide for FastIron 09.0.10a.

TABLE 2 Summary of Changes in FastIron 09.0.10a

Feature	Description	Location
Multicast VLAN Registration	Multicast VLAN Registration (MVR) enables more efficient distribution of multicast streams across Layer 2 networks, and the duplication of multicast streams from the same source is eliminated while maintaining isolation between hosts on different VLANs. A number of changes and enhancements have been introduced for MVR. These include the following: • MVR is supported for both tagged and untagged receiver ports. • MVR is supported for router images only. • Query messages are supported for MVR. • Multicast data is supported for MVR.	Multicast VLAN Registration on page 47
Updates to address defects	Minor updates on content throughout to address defects.	All chapters.
Minor editorial updates	Minor editorial updates were made throughout the Configuration Guide.	All chapters.

The following table describes the changes to this guide for FastIron 09.0.10.

TABLE 3 Summary of Changes in FastIron 09.0.10

Feature	Description	Location
Disabling Multicast Static Group Forwarding for a VLAN	Multicast static group forwarding can be disabled at the VLAN level.	Disabling Multicast Static Group Forwarding for a VLAN on page 25
IGMP Filtering and State Limit	An IGMP report filter policy can be configured globally or for an interface. Additionally, the maximum number of IGMP group addresses for the default VRF, or a non-default VRF instance, can be changed globally or at the interface level.	• Configuring the IGMP Report Filter Policy on page 81 • Setting the Maximum Number of IGMP Group Addresses on page 80
IPv4 PIM Join Message Filter	IPv4 PIM devices can be configured to accept or reject Join and Prune messages for all the multicast group addresses and for all source addresses.	IPv4 PIM Join and Prune Policy on page 122
IPv4 PIM Register Message Filter Rule	The register message filter rule for PIM can be configured so that unauthorized multicast sources or groups are blocked.	• IPv4 PIM Register Message Filter Rule on page 82 • Configuring the Register Message Filter Rule for PIM on page 83
IPv4 PIM Register Message Rate Limit	The maximum number of register packets sent or received per second by a device can be configured. The rate limit for the number of register messages can be set to a relatively low value to avoid adverse pressure on the CPU when numerous sources start concurrently.	• IPv4 PIM Register Message Rate Limit on page 81 • Configuring the Register Message Rate Limit for PIM on page 82
IPv6 PIM Join Message Filter	IPv6 PIM devices can be configured to accept or reject Join and Prune messages for all the multicast group addresses and for all source addresses.	IPv6 PIM Join and Prune Policy on page 161
IPv6 PIM Register Message Filter Rule	The register message filter rule for IPv6 PIM can be configured so that unauthorized multicast sources or groups are blocked.	• IPv6 PIM Register Message Filter Rule on page 175 • Configuring the Register Message Filter Rule for PIMv6 on page 175
IPv6 PIM Register Message Rate Limit	The maximum number of register packets sent or received per second by a device can be configured.	• IPv6 PIM Register Message Rate Limit on page 174 • Configuring the Register Message Rate Limit for PIMv6 on page 175
MLD Filtering and State Limit	An MLD report filter policy can be configured globally or for an interface. Additionally, the maximum number of MLD group addresses for the default VRF, or a non-default VRF instance, can be changed globally or at the interface level.	• Configuring the MLD Report Filter Policy on page 173 • Setting the Maximum Number of MLD Group Addresses on page 174

TABLE 3 Summary of Changes in FastIron 09.0.10 (continued)

Feature	Description	Location
Multicast VLAN Registration	Multicast VLAN Registration (MVR) enables more efficient distribution of multicast streams across Layer 2 networks, and the duplication of multicast streams from the same source is eliminated while maintaining isolation between hosts on different VLANs.	Multicast VLAN Registration on page 47
MSDP TCP Authentication Option (AO) Support	MSDP can be configured to use TCP keychain settings. MSDP **show** commands have been updated to include information on TCP AO settings.	Configuring MSDP Globally on page 107 *RUCKUS FastIron Security Configuration Guide* for information on the TCP keychain module and AO configuration *RUCKUS FastIron Command Reference* for details on new and updated commands
Updates to address defects	Minor updates on content throughout to address defects.	All chapters.
Minor editorial updates	Minor editorial updates were made throughout the Configuration Guide.	All chapters.

IPv4 Multicast VLAN Traffic Reduction

IGMP Snooping Overview

When a device processes a multicast packet, by default, it broadcasts the packet to all ports except the incoming port of a VLAN. Packets are flooded by hardware without going to the CPU. This behavior causes some clients to receive unwanted traffic.

IGMP snooping provides multicast containment by forwarding traffic to only the ports that have IGMP receivers for a specific multicast group (destination address). A device maintains the IGMP group membership information by processing the IGMP reports and leave messages, so traffic can be forwarded to ports receiving IGMP reports.

An IPv4 multicast address is a destination address in the range of 224.0.0.0 to 239.255.255.255. Addresses of 224.0.0.X are reserved. Because packets destined for these addresses may require VLAN flooding, devices do not snoop in the reserved range. Data packets destined to addresses in the reserved range are flooded to the entire VLAN by hardware, and mirrored to the CPU. Multicast data packets destined for the non-reserved range of addresses are snooped. A client must send IGMP reports in order to receive traffic.

The responsibility of an IGMP device is to broadcast general queries periodically, and to send group queries when receiving a leave message, to confirm that none of the clients on the port still want specific traffic before removing the traffic from the port. IGMPv2 lets clients specify what group (destination address) receives the traffic, but clients do not specify the source of the traffic. IGMPv3 is for source-specific multicast traffic, adding the capability for clients to include or exclude specific traffic sources. An IGMPv3 device port state could be INCLUDE or EXCLUDE, and there are different types of group records for client reports.

The receivers respond to general or group queries by sending a membership report that contains one or more of the following records associated with a specific group:

- A current-state record that indicates from which sources the interface wants to receive and not receive traffic. This record contains the source address of interfaces and whether traffic will be included (IS_IN) or excluded (IS_EX) from this source.
- A filter-mode-change record. If the interface state changes from IS_IN to IS_EX, a TO_EX record is included in the membership report. Likewise, if the interface state changes from IS_EX to IS_IN, a TO_IN record appears in the membership report.
- An IGMPv2 leave report is equivalent to a TO_IN (empty) record in IGMPv3. This record means that no traffic from this group will be received regardless of the source.
- An IGMPv2 group report is equivalent to an IS_EX (empty) record in IGMPv3. This record means that all traffic from this group will be received regardless of source.
- A source-list-change record. If the interface wants to add or remove traffic sources from its membership report, the report can contain an ALLOW record, which includes a list of new sources from which the interface wants to receive traffic. It can also contain a BLOCK record, which lists the current traffic sources from which the interface wants to stop receiving traffic.

IGMP protocols provide a method for clients and a device to exchange messages, and let the device build a database indicating which port wants what traffic. The protocols do not specify forwarding methods. They require IGMP snooping or multicast protocols such as PIM to handle packet forwarding. PIM can route multicast packets within and outside a VLAN, while IGMP snooping can switch packets only within a VLAN.

If a VLAN is not IGMP snooping-enabled, it floods multicast data and control packets to the entire VLAN in hardware. When snooping is enabled, IGMP packets are trapped to the CPU. Data packets are mirrored to the CPU in addition to being VLAN flooded. The CPU then installs hardware resources, so that subsequent data packets can be switched to desired ports in hardware without going to the CPU. If there is no client report or port to queriers for a data stream, the hardware resource drops it.

Queriers and Non-Queriers

An IGMP snooping-enabled RUCKUS ICX device can be configured as a querier (active) or non-querier (passive). An IGMP querier sends queries; a non-querier listens for IGMP queries and forwards them to the entire VLAN. VLANs can be independently configured to be queriers or non-queriers. If a VLAN has a connection to a PIM-enabled port on another router, the VLAN must be configured as a non-querier. When multiple IGMP snooping devices are connected together, and there is no connection to a PIM-enabled port, one of the devices must be configured as a querier. If multiple devices are configured as queriers, after these devices exchange queries, then all except the selected device stop sending queries. The device with the lowest address becomes the querier. Although the system will work when multiple devices are configured as queriers, RUCKUS recommends that only one device (preferably the one with the traffic source) is configured as a querier.

The non-queriers always forward multicast data traffic and IGMP messages to router ports which receive IGMP queries or PIM hellos. RUCKUS recommends that you configure the device with the data traffic source (server) as a querier. If a server is attached to a non-querier, the non-querier always forwards traffic to the querier regardless of whether there are any clients on the querier.

NOTE
In a topology of one or more connecting devices, at least one device must be configured as active. Otherwise, none of the devices can send out queries, and traffic cannot be forwarded to clients.

VLAN-specific Configuration

IGMP snooping can be enabled on some VLANs or on all VLANs. Each VLAN can be independently configured to be a querier or non-querier and can be configured for IGMPv2 or IGMPv3. In general, the **ip multicast** commands apply globally to all VLANs except those configured with VLAN-specific multicast commands. The VLAN-specific multicast commands supersede the global **ip multicast** commands.

IGMP snooping can be configured for IGMPv2 or IGMPv3 on individual ports of a VLAN. An interface or router sends the queries and reports that include its IGMP version specified on it. The version configuration only applies to sending queries. Earlier versions cannot recognize and process later version reports. Later versions can recognize and process both earlier and later versions.

To avoid version deadlock, an interface retains its version configuration even when it receives a report with an earlier version.

Tracking and Fast Leave

RUCKUS devices support fast leave for IGMPv2, and tracking and fast leave for IGMPv3. Fast leave stops the traffic immediately when the port receives a leave message. Tracking traces all IGMPv3 clients. Refer to Enabling IGMPv3 Membership Tracking and Fast Leave for the VLAN on page 27 and Enabling Fast Leave for IGMPv2 on page 27.

Support for IGMP Snooping and Layer 3 Multicast Routing Together on the Same Device

The RUCKUS device supports global Layer 2 IP multicast traffic reduction (IGMP snoopoing) and Layer 3 multicast routing (PIM-Sparse or PIM-Dense) together on the same device in the full Layer 3 software image.

NOTE
IGMP snooping and Layer 3 multicast are not supported on the same VLAN. They must be configured on separate VLANs.

Hardware Resources for IGMP and PIM-SM Snooping

RUCKUS devices allocate or program FDB or MAC entries to achieve multicast snooping in hardware. If a data packet does not match any of these resources, it might be sent to the CPU, which increases the CPU burden. This can happen if the device runs out of hardware resources, or is unable to install resources for a specific matching address due to a hashing collision.

The hardware hashes addresses into available FDB or MAC entries, with some addresses hashed into the same entry. If the collision number in an entry is more than the hardware chain length, the resource cannot be installed.

Configuration Notes and Feature Limitations for IGMP Snooping and Layer 3 Multicast Routing

- IGMP snooping is supported for the default VLAN for the router image also. Prior to FastIron 09.0.00, IGMP snooping was supported for the default VLAN on the switch image only.
- Layer 2 IGMP multicast is automatically enabled with Layer 3 multicast routing. Layer 2 IGMP snooping and Layer 3 multicast routing cannot be configured on the same VLAN.
- The default IGMP version is IGMPv2.
- A user can configure the maximum numbers of group address entries.
- An IGMP device can be configured to rate-limit the forwarding IGMPv2 membership reports to queriers.
- The device supports static groups. The device acts as a proxy to send IGMP reports for the static groups when receiving queries.
- A user can configure static router ports to force all multicast traffic to these specific ports.
- When there are two or more possible queriers, it is recommended to configure the IP multicast age interval to 20 seconds more than the default calculated age interval on all switches enabled with IGMP snooping. This prevents the aging of groups when the active querier fails.
- If a VLAN has a connection to a PIM-enabled port on another router, the VLAN must be configured as a non-querier (passive). When multiple snooping devices connect together and there is no connection to PIM ports, one device must be configured as a querier (active). If multiple devices are configured as active (queriers), only one will keep sending queries after exchanging queries.
- The querier must configure an IP address to send out queries.
- IGMP snooping requires hardware resource. Hardware resource is installed only when there is data traffic. If resource is inadequate, the data stream without a resource is mirrored to the CPU in addition to being VLAN flooded, which can cause high CPU usage. RUCKUS recommends that you avoid global enabling of snooping unless necessary.
- IGMP snooping requires clients to send membership reports in order to receive data traffic. If a client application does not send reports, you must configure static groups on the snooping VLAN to force traffic to client ports. Note that servers (traffic sources) are not required to send IGMP memberships.
- Support for VSRP together with IGMP snooping on the same interface.
- When VSRP or VSRP-aware is configured on a VLAN, only IGMP version 2 is recommended; IGMP version 3 is not recommended.
- Each VLAN can independently enable or disable IGMP, or configure IGMPv2 or IGMPv3.
- IGMP/PIM-SM snooping over Multi-Chassis Trunking is supported on the following RUCKUS ICX devices:
  - ICX 7650
  - ICX 7850
- IGMP snooping is MAC-based for ICX7150-C08 device, whereas IGMP snooping is IP-based for all other devices..
- For snooping when it is MAC-based, Only *,G entries will be present in multicast mcache output for IPv4 and IPv6. S,G entries will not be present.

- Only one mcache will be created for all multicast groups which share same multicast MAC address. Mcache will be created for the group for which the packets first arrive.

MAC-based Forwarding Implementation on ICX 7150-C08P Devices

With MAC-based implementation, multiple groups point to one Layer 2 entry in the IPv4 multicast hardware table. The user may receive traffic for groups that have not been requested. The source of the group is not programmed in the hardware for the Layer 2 entry. Therefore, the user receives traffic from all sources for a specific group.

IGMP Snooping Configuration

Configuring IGMP snooping on a RUCKUS device consists of the following global, VLAN-specific, and port-specific tasks.

Perform the following global IGMP snooping tasks:

- Configuring the IGMP snooping software resource limits
- Enabling IGMP snooping globally on the device
- Configuring the global IGMP mode
- Configuring the global IGMP version
- Modifying the age interval for group membership entries
- Modifying the query interval (active IGMP snooping mode only)
- Modifying the maximum response time
- Configuring report control (rate limiting)
- Modifying the wait time before stopping traffic when receiving a leave message
- Modifying the multicast cache age time
- Enabling or disabling error and warning messages

Perform the following VLAN-specific IGMP snooping tasks:

- Configuring the IGMP mode for a VLAN (active or passive)
- Disabling IGMP snooping on a VLAN
- Configuring the IGMP version for a VLAN
- Configuring static router ports
- Turning off static group proxy
- Enabling IGMPv3 membership tracking and fast leave for the VLAN
- Enabling fast leave for IGMP
- Enabling fast convergence

Perform the following port-specific IGMP snooping task:

- Configuring the IGMP version for individual ports in a VLAN

IGMP Snooping Software Resource Limits

The IGMP snooping mcache resource limits for RUCKUS devices are shown in the following table.

TABLE 4 IGMP Snooping Software Resource Limits

Platform	Groups		Mcache	
	Default	Maximum	Default	Maximum
RUCKUS ICX 7150	1024	3072	512	3072
RUCKUS ICX 7250	512	8192	512	8192
RUCKUS ICX 7450	512	8192	512	8192
RUCKUS ICX 7550	512	8192	512	8192
RUCKUS ICX 7850	8192	8192	6144	6144

NOTE
For ICX 7850 and ICX 7550 devices, values are used from the forwarding profile. Refer to the **forwarding-profile** command in the *RUCKUS FastIron Command Reference* and the "Configuration Fundamentals" chapter in the *RUCKUS FastIron Management Configuration Guide* for more information.

IGMP Snooping Mcache Entries and Group Addresses

An IGMP snooping group address entry is created when an IGMP join message is received for a group. An IGMP snooping mcache entry is created when data traffic is received for that group. Each mcache entry represents one data stream, and multiple mcache entries (up to 32) can share the same hardware (MAC) address entry. The egress port list for the mcache entry is obtained from the IGMP group address entry. If there is no existing IGMP group address entry when an mcache entry is created, data traffic for that multicast group is dropped in hardware. If there is an existing IGMP group address entry when an mcache is created, data traffic for that multicast group is switched in hardware.

Setting the Maximum Number of IGMP Mcache Entries and Group Addresses

You can change the maximum number of IGMP group addresses and the maximum number of IGMP mcache entries.

NOTE
For ICX 7850 and ICX 7550 devices, values are used from the forwarding profile. Refer to the **forwarding-profile** command in the *RUCKUS FastIron Command Reference* and the *Configuration Fundamentals* chapter in the *RUCKUS FastIron Management Configuration Guide* for more information.

1. Enter global configuration mode.

```
device# configure terminal
```

2. To set the maximum number of IGMP group addresses, use the **system-max igmp-snoop-group-addr** command.

```
device(config)# system-max igmp-snoop-group-addr 1600
```

The configured number of IGMP group addresses is the upper limit of an expandable database. Client memberships exceeding the group limit are not processed.

3. To change the maximum number of IGMP snooping cache entries supported on a device, use the **system-max igmp-snoop-mcache** command.

```
device(config)# system-max igmp-snoop-mcache 2000
```

The following example sets the maximum number of IGMP group addresses to 1600, and the maximum number of IGMP mcache entries to 2000.

```
device# configure terminal
device(config)# system-max igmp-snoop-group-addr 1600
device(config)# system-max igmp-snoop-mcache 2000
```

IGMP Snooping Configuration Notes for Layer 3 Devices

- If Layer 3 multicast routing is enabled on an interface or VLAN, do not attempt to enable Layer 2 IGMP snooping on the same interface or VLAN.
- If the "route-only" feature is enabled on the Layer 3 switch, then IP multicast traffic reduction will not be supported.

IGMP Snooping Modes

You can configure active or passive IGMP modes on the RUCKUS device. The default mode is passive. If you specify an IGMP mode for a VLAN, it overrides the global setting.

- **Active**: When active IGMP mode is enabled, a RUCKUS device actively sends out IGMP queries to identify multicast groups on the network, and makes entries in the IGMP table based on the group membership reports it receives.

  NOTE
  Routers in the network generally handle this operation. Use the active IGMP mode only when the device is in a standalone Layer 2 switched network with no external IP multicast router attachments. In this case, enable the active IGMP mode on only one of the devices and leave the other devices configured for passive IGMP mode.

- **Passive**: When passive IGMP mode is enabled, it forwards reports to the router ports which receive queries. IGMP snooping in the passive mode does not send queries. However, it forwards queries to the entire VLAN.

Configuring the IGMP Snooping Mode and Version Globally

IGMP mode and version can be configured on RUCKUS devices in global configuration mode.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Globally set the IGMP mode to active.

   ```
   device(config)# ip multicast active
   ```

   If you do not specify the **active** keyword, the default mode is passive.

3. Globally set the IGMP version to version 3.

   ```
   device(config)# ip multicast version 3
   ```

   If you do not specify an IGMP version, the default version is IGMPv2.

The following example globally sets the device to run IGMPv3 in active mode.

```
device# configure terminal
device(config)# ip multicast active
device(config)# ip multicast version 3
```

Configuring the IGMP Snooping Mode and Version for a VLAN

IGMP mode and version can be configured on RUCKUS devices for a specific VLAN.

Even if the IGMP mode and version have been configured globally, specifying the mode and version for a VLAN overrides the global settings.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Create a VLAN.

   ```
   device(config)# vlan 20
   ```

3. Set the IGMP mode to active for a VLAN.

   ```
   device(config-vlan-20)# multicast active
   ```

   If you do not specify the **active** keyword, the default mode is passive. If you do not specify a mode for the VLAN, the globally-configured mode is used.

4. Set the IGMP version for VLAN 20 to version 3.

   ```
   device(config-vlan-20)# multicast version 3
   ```

   If no IGMP version is specified, then the globally-configured IGMP version is used. If an IGMP version is specified for individual ports, those ports use that version, instead of the VLAN version.

5. You can specify the IGMP version for individual ports in a VLAN. You can specify a list of ports, a range of ports, or a combination of lists and ranges.

   ```
   device(config-vlan-20)# multicast port-version 3 ethernet 1/2/4 to 1/2/6
   ```

   In this example, the ports 1/2/4, 1/2/5, and 1/2/6 are configured to use IGMPv3. The other ports either use the IGMP version specified with the **multicast version** command, or the globally-configured IGMP version.

6. You can configure static groups to specific ports.

   ```
   device(config-vlan-20)# multicast static-group 224.1.1.1 count 2 ethernet 1/1/3 ethernet 1/1/5 to
   1/1/7
   ```

   A snooping-enabled VLAN cannot forward multicast traffic to ports that do not receive IGMP membership reports. If clients cannot send reports, you can configure a static group which applies to specific ports. The static group allows packets to be forwarded to the static group ports even though they have no client membership reports.

The following example configures VLAN 20 to run IGMPv3 in active mode with some ports configured specifically to use IGMPv3 with a static group to specific ports.

```
device# configure terminal
device(config)# vlan 20
device(config-vlan-20)# multicast active
device(config-vlan-20)# multicast version 3
device(config-vlan-20)# multicast port-version 3 ethernet 1/2/4 to 1/2/6
device(config-vlan-20)# multicast static-group 224.1.1.1 count 2 ethernet 1/1/3 ethernet 1/1/5 to 1/1/7
```

Configuring IGMP Snooping Global Options

A number of IGMP snooping options can be configured on RUCKUS devices in global configuration mode.

You must configure the IGMP mode and version globally before entering these options. Refer to Configuring the IGMP Snooping Mode and Version Globally on page 22.

The following option configurations are outlined in the following steps:

- Modify the age interval for group membership entries: When the device receives a group membership report, it makes an entry for that group in the IGMP group table. The age interval specifies how long the entry can remain in the table before the device receives another group membership report.
- Modify the query interval (only for IGMP active mode): If IP multicast traffic reduction is set to active mode, you can modify the query interval to specify how often the device sends general queries.
- Modify the maximum response time: The maximum response time is the number of seconds that a client can wait before responding to a query sent by the device.
- Configure report control (v2 only): A device in passive mode forwards reports and leave messages from clients to the upstream router ports that are receiving queries. You can configure a report control option to rate-limit report forwarding within the same group to no more than once every 10 seconds. This rate-limiting does not apply to the first report answering a group-specific query.
- Modify the wait time before stopping traffic when receiving a leave message: You can define the wait time before stopping traffic to a port when a leave message is received. The device sends group-specific queries once per second to ask if any client in the same port still needs this group. Due to internal timer granularity, the actual wait time is between n and (n+1) seconds (n is the configured value).
- Modify the multicast cache age time: You can set the time for an mcache to age out when it does not receive traffic. The traffic is hardware switched. One minute before aging out an mcache, the device mirrors a packet of this mcache to CPU to reset the age. If no data traffic arrives within one minute, this mcache is deleted. A lower value quickly removes resources consumed by idle streams, but it mirrors packets to CPU often. A higher value is recommended when data streams are continually arriving.
- Enable or disable error or warning messages: The device prints error or warning messages when it runs out of software resources or when it receives packets with the wrong checksum or groups. These messages are rate-limited. You can turn off these messages.

The following task steps can be configured in any order and are all optional. Commands that are limited to a specific IGMP mode or version are identified in the task step.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Modify the age interval, in seconds, for group membership entries.

   ```
   device(config)# ip multicast age-interval 280
   ```

   When multiple devices are connected together, all devices must have the same age interval configured, which must be at least twice the length of the query interval, so that missing one report will not stop traffic. Non-querier age intervals must be the same as the age interval of the querier.

3. Modify the query interval, in seconds (only for IGMP active mode).

   ```
   device(config)# ip multicast query-interval 120
   ```

   When multiple queriers connect together, they must all be configured with the same query interval.

4. Modify the IPv4 multicast maximum response time, in seconds.

   ```
   device(config)# ip multicast max-response-time 5
   ```

5. Configure report control (IGMPv2 only).

   ```
   device(config)# ip multicast report-control
   ```

   IGMP V2 membership reports of the same group from different clients are considered to be the same and are rate-limited.

   NOTE
   This feature applies to IGMP V2 only. The leave messages are not rate limited.

6. Modify the wait time before stopping traffic when receiving a leave message.

```
device(config)# ip multicast leave-wait-time 5
```

7. Modify the multicast cache age time.

```
device(config)# ip multicast mcache-age 180
```

NOTE
The mcache age value configured may not expire accurately. You may notice a delay of 0 to 60 seconds.

8. Enable or disable error or warning messages.

```
device(config)# ip multicast verbose-off
```

The following example globally sets the device to run IP multicast version 3 in active mode.

```
device# configure terminal
device(config)# ip multicast active
device(config)# ip multicast version 3
device(config)# ip multicast age-interval 280
device(config)# ip multicast query-interval 120
device(config)# ip multicast max-response-time 5
device(config)# ip multicast report-control
device(config)# ip multicast leave-wait-time 5
device(config)# ip multicast mcache-age 180
device(config)# ip multicast verbose-off
```

Disabling IGMP Snooping on a VLAN

When IGMP snooping is enabled globally, you can still disable it for a specific VLAN. For example, the following commands cause IGMP snooping to be disabled for VLAN 20. This setting overrides the global setting.

```
device# configure terminal
device(config)# vlan 20
device(config-vlan-20)# multicast disable-igmp-snoop
```

Disabling Multicast Static Group Forwarding for a VLAN

Multicast static group forwarding can be disabled at the VLAN level.

The following example disables multicast static group forwarding for a VLAN. The addition of static-group-based outbound interfaces to mcache is disabled. These steps can be used in conjunction with proxy configuration to generate proxy reports for static groups and eliminate traffic from the ICX device to reduce join latency. With this configuration, a proxy module pulls traffic for affected static groups from the ICX device, but does not forward the traffic to recipients configured in the static group. The traffic is forwarded only when IGMP report messages are received from the recipients.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Create a VLAN.

```
device(config)# vlan 100
```

3. Disable multicast static group forwarding on VLAN 100.

```
device(config-vlan-100)# multicast static-grp-fwd-disable
```

The following example disables multicast static group forwarding on VLAN 100.

```
device# configure terminal
device(config)# vlan 100
device(config-vlan-100)# multicast static-grp-fwd-disable
device(config-vlan-100)
```

Configuring Static Router Ports

The RUCKUS device forwards all multicast control and data packets to router ports which receive queries. Although router ports are learned, you can force multicast traffic to specified ports even though these ports never receive queries. You can specify a list of ports, a range of ports, or a combination of lists and ranges.

The following configuration example configures static router ports.

```
device# configure terminal
device(config)# vlan 70
device(config-vlan-70)# multicast router-port ethernet 1/1/4 to 1/1/5 ethernet 1/1/8
```

Turning Off Static Group Proxy

If a device has been configured for static groups, it acts as a proxy and sends membership reports for the static groups when it receives general or group-specific queries. When a static group configuration is removed, it is deleted from the active group table immediately. However, leave messages are not sent to the querier, and the querier must age out the group. Proxy activity can be turned off. The default is on.

The following configuration example turns proxy activity off for VLAN 20.

```
device# configure terminal
device(config)# vlan 20
device(config-vlan-20)# multicast proxy-off
```

Configuring the Layer 2 Mode IPv4 Querier Address

You can configure an IPv4 querier address for every VLAN. This functionality is available only for multicast snooping.

In releases before FastIron 08.0.50, you cannot specifically configure a querier address per VLAN. Instead, in an IPv4 environment, the device internally attempts to select an address, either a VE address and a loopback address for a router image, or a management port address for a switch image.

Starting with FastIron 08.0.50, you can configure a Layer 2 mode querier IP address. You can now plan an elected querier location suitable for your network, and use the most suitable querier location. This address can be configured regardless of whether the current multicast snooping mode is set to active or passive. Once the mode changes to active, the configured IP address is used as a querier address. You can configure a different querier IP address for every VLAN.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Enter VLAN configuration mode.

   ```
   device(config)# vlan 100
   ```

3. Enter the **multicast querier-address** command followed by the IPv4 address.

   ```
   device(config-vlan-100)# multicast querier-address 10.2.2.2
   ```

The following example configures an IPv4 address as the multicast querier address for the VLAN.

```
device# configure terminal
device(config)# vlan 100
device(config-vlan-100)# multicast querier-address 10.2.2.2
```

Enabling IGMPv3 Membership Tracking and Fast Leave for the VLAN

IGMPv3 gives clients membership tracking and fast leave capability. In IGMPv2, only one client on an interface needs to respond to a router's queries. This can leave some clients invisible to the router, making it impossible to track the membership of all clients in a group. When a client leaves the group, the device sends group-specific queries to the interface to see if other clients on that interface need the data stream of the client who is leaving. If no client responds, the device waits a few seconds before it stops the traffic. You can configure the wait time using the **ip multicast leave-wait-time** command.

IGMPv3 requires every client to respond to queries, allowing the device to track all clients. When tracking is enabled, and an IGMP v3 client sends a leave message and there is no other client, the device immediately stops forwarding traffic to the interface. This feature requires the entire VLAN be configured for IGMPv3 and IGMPv2 clients. If a client does not send a report during the specified group membership time (the default is 260 seconds), that client is removed from the tracking list.

Every group on a physical port keeps its own tracking record. However, it can only track group membership; it cannot track by (source, group). For example, Client A and Client B belong to group1 but each receives traffic streams from different sources. Client A receives a stream from (source_1, group1) and Client B receives a stream from (source_2, group1). The device still waits for the configured leave-wait-time before it stops the traffic because these two clients are in the same group. If the clients are in different groups, then the waiting period is not applied and traffic is stopped immediately.

The following configuration example enables the tracking and fast leave feature for VLAN 20.

```
device# configure terminal
device(config)# vlan 20
device(config-vlan-20)# multicast tracking
```

The membership tracking and fast leave features are supported for IGMPv3 only. If any port or any client is not configured for IGMPv3, then the **multicast tracking** command is ignored.

Enabling Fast Leave for IGMPv2

When a device receives an IGMPv2 leave message, it sends out multiple group-specific queries. If no other client replies within the waiting period, the device stops forwarding traffic. When fast leave version 2 is configured, and when the device receives a leave message, it immediately stops forwarding to that port. The device does not send group-specific queries. When fast leave version 2 is configured on a VLAN, you must not have multiple clients on any port that is part of the VLAN. In a scenario where two devices connect, the querier device should not be configured for fast leave version 2 because the port might have multiple clients through the non-querier. The number of queries, and the waiting period (in seconds) can be configured.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Configure a VLAN.

   ```
   device(config)# vlan 20
   ```

3. Enable fast leave version 2 for IGMP.

   ```
   device(config-vlan-20)# multicast fast-leave-v2
   ```

The following example enables fast leave for IGMP with a leave message waiting period of 4 seconds.

```
device# configure terminal
device(config)# vlan 20
device(config-vlan-20)# multicast fast-leave-v2
```

Enabling Fast Convergence

In addition to sending periodic general queries, an active device sends general queries when it detects a new port. However, because the device does not recognize the other device's port up event, multicast traffic might still require up to the query-interval time to resume after a topology change. Fast convergence allows the device to listen to topology change events in Layer 2 protocols such as spanning tree, and then send general queries to shorten the convergence time.

If the Layer 2 protocol cannot detect a topology change, fast convergence may not work in some cases. For example, if the direct connection between two devices switches from one interface to another, the rapid spanning tree protocol (802.1w) considers this optimization, rather than a topology change. In this example, other devices will not receive topology change notifications, and will be unable to send queries to speed up the convergence. Fast convergence works well with the regular spanning tree protocol in this case.

The following configuration example enables fast-convergency for VLAN 70.

```
device# configure terminal
device(config)# vlan 70
device(config-vlan-70)# multicast fast-convergence
```

Disabling the Flooding of Unregistered IPv4 Multicast Frames in an IGMP-Snooping-Enabled VLAN

Unregistered IPv4 multicast frames can be enabled in an IGMP-snooping-enabled VLAN. The following task enables the flooding of unregistered IPv4 multicast frames in an IGMP-snooping-enabled VLAN.

Enabling the flooding of unregistered IPv4 multicast frames in an IGMP-snooping-enabled VLAN is supported on the following platforms:

- RUCKUS ICX 7850 (MCT, standalone, and stacking)
- RUCKUS ICX 7650 (MCT, standalone, and stacking)
- RUCKUS ICX 7550 (MCT, standalone, and stacking)
- RUCKUS ICX 7450 (standalone and stacking)
- RUCKUS ICX 7250 (standalone and stacking)
- RUCKUS ICX 7150 (standalone and stacking)

1. Use the **configure terminal** command to enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Use the **ip multicast flood-unregistered** command to enable the flooding of unregistered IPv4 multicast frames.

   ```
   device# ip multicast flood-unregistered
   ```

The following example enables the flooding of unregistered IPv4 multicast frames.

```
device# configure terminal
device(config)# ip multicast flood-unregistered
```

Software Defined Video-over-Ethernet

Software Defined Video-over-Ethernet (SDVoE) is a software-based AV-over-IP platform that provides solutions for point-to-point connectivity and Ethernet-based audio visual (AV) distribution. The technology and solution offer cost effective, flexible hardware and software platforms which can support many AV applications. SDVoE provides standardization and interoperability among the ecosystem partner products to enable great AV user experiences. RUCKUS ICX switches are certified to be part of this solution and allow efficient switching of AV multicast traffic.

SDVoE Configuration Options

You can configure SDVoE using one of the following methods:

- Using the **multicast sdvoe** command.
- Creating edge-ports automatically.

  NOTE
  Only one of the below methods should be used for a network.

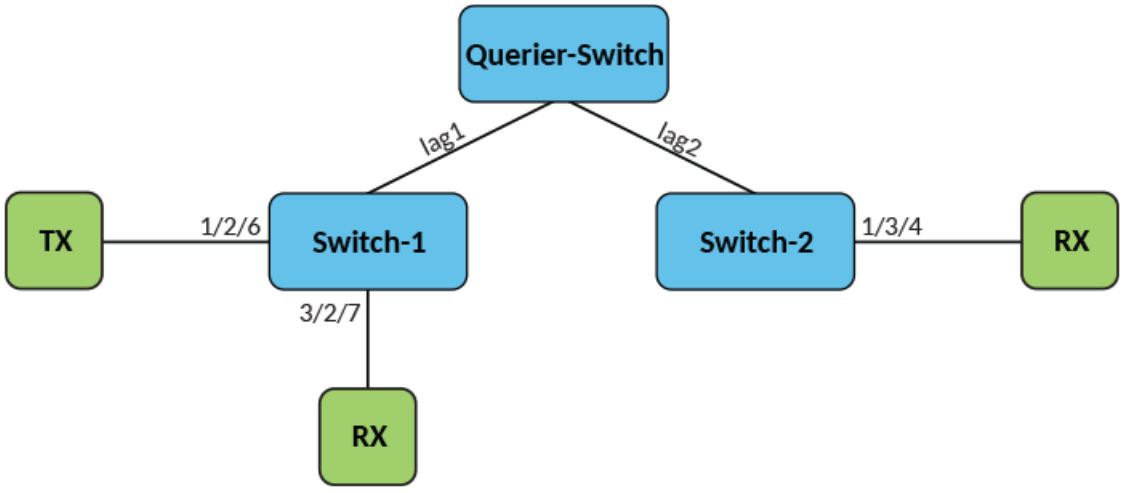
Enabling SDVoE for an IGMP-snooping-enabled VLAN using the multicast sdvoe Command

Consider the following when using this method:

- Edge ports should be manually configured.
- Fast-leave-v2 on edge ports should be manually configured.
- If using IGMPv3, tracking should be manually configured.

The following illustration shows a network topology where edge ports are configured on Switch 1 and Switch 2 so that fast leave can be enabled only on these ports. IGMP snooping is enabled in passive mode for Switch 1 and Switch 2. SDVoE is configured for multicast packets in the VLAN. The Querier switch does not have any edge ports configured. IGMP snooping is enabled in active mode for the Querier switch so that queries are generated.

FIGURE 1 Enabling SDVoE using the multicast sdvoe Command



Configuration Example: Enabling SDVoE using the multicast sdvoe Command

The following example enables IGMP snooping and SDVoE on all switches, and fast-leave on Swtich1 and Switch2.

```
Switch 1:
Switch-1# configure terminal
Switch-1(config)# vlan 11
Switch-1(config-vlan-11)# tagged ethernet 1/2/6 ethernet 3/2/7 lag 1
Switch-1(config-vlan-11)# multicast passive
Switch-1(config-vlan-11)# multicast fast-leave-v2 edge-ports
Switch-1(config-vlan-11)# multicast sdvoe

Querier:
Querier# configure terminal
Querier(config)# vlan 11
Querier(config-vlan-11)# tagged lag 1 lag 2
Querier(config-vlan-11)# multicast active
Querier(config-vlan-11)# multicast querier-address 3.3.3.3
Querier(config-vlan-11)# multicast sdvoe

Switch-2:
Switch-2# configure terminal
Switch-2(config)# vlan 11
Switch-2(config-vlan-11)# tagged ethernet 1/3/4 lag 2
Switch-2(config-vlan-11)# multicast passive
Switch-2(config-vlan-11)# multicast fast-leave-v2 edge-ports
Switch-2(config-vlan-11)# multicast sdvoe
```

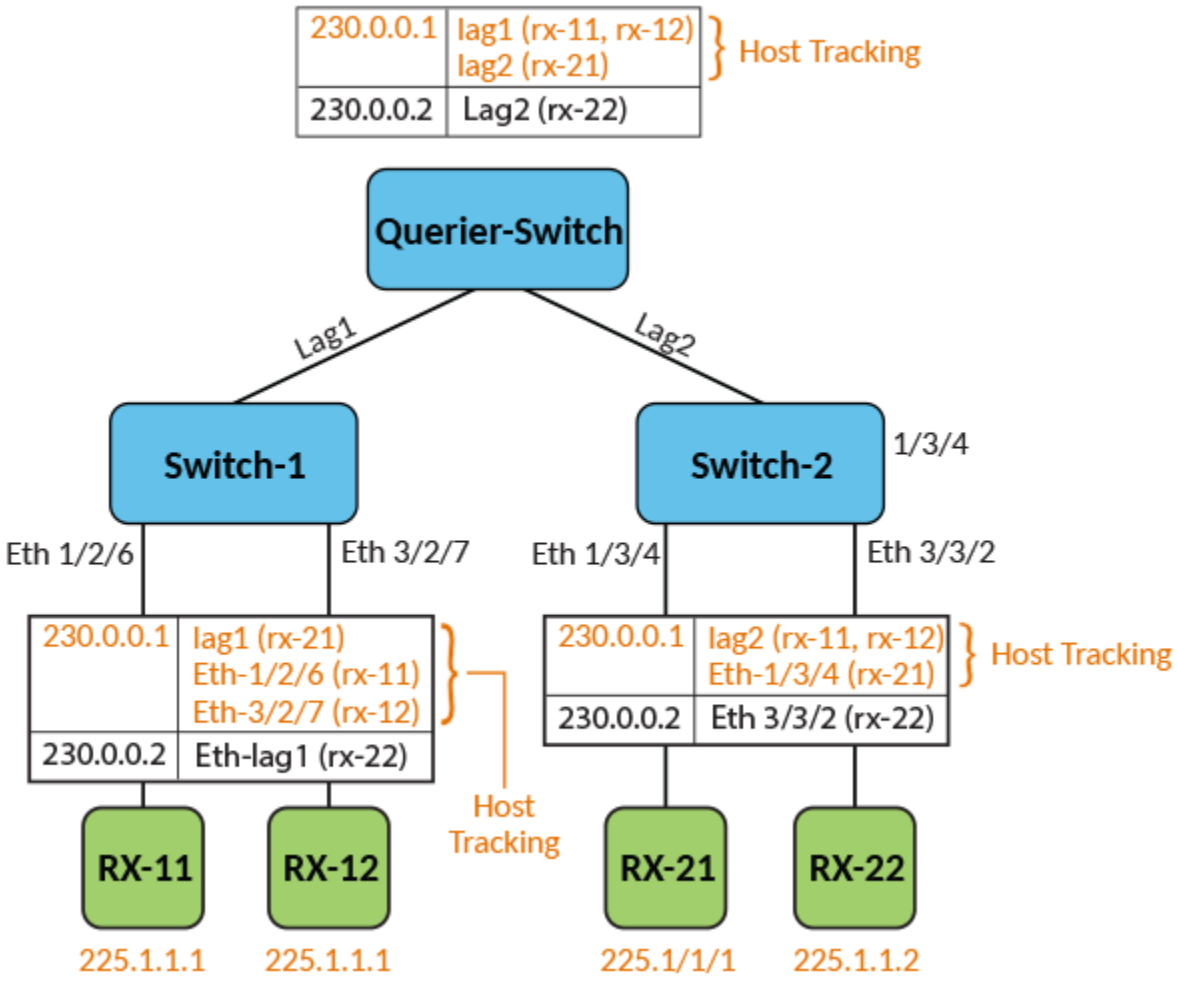
Enabling SDVoE for an IGMP-snooping-enabled VLAN where Edge-ports are Automatically Created

Consider the following when using this method:

- Edge-ports are automatically created.
- Fast leave is not supported.
- Tracking is automatically enabled for both IGMPv2 and IGMPv3.
- This method is not interoperable with other vendor switches.

The following illustration shows a network topology where edge ports are automatically configured on Switch 1 and Switch 2. Tracking for IGMPv2 and IGMPv3 is automatically enabled. Multicast passive, dynamic edge port and IGMPv2 and IGMPv3 client tracking is configured for Switch 1 and Switch 2. Multicast active, dynamic edge port and IGMPv2 and IGMPv3 client tracking is configured for the Querier switch. Passive neighbors can dynamically identify edge and non –edge ports. Receiver client tracking is enabled across the switches for all reports. In this network topology, any VLAN can be configured as the Querier switch.

FIGURE 2 Enabling SDVoE where Edge-ports are Automatically Created



Configuration Example: Enabling SDVoE where Edge-ports are Automatically Created

```
Switch 1:
Switch-1# configure terminal
Switch-1(config)# vlan 11
Switch-1(config-vlan-11)# tagged ethernet 1/2/6 ethernet 3/2/7 lag 1
Switch-1(config-vlan-11)# multicast sdvoe auto-edge-port-track-passive

Querier:

Querier-1# configure terminal
Querier(config)# vlan 11
Querier(config-vlan-11)# tagged lag 1 lag 2
Querier(config-vlan-11)# multicast sdvoe auto-edge-port-track-act
Querier(config-vlan-11)# multicast querier-address 3.3.3.3


Switch-2:
Switch-2# configure terminal
Switch-2(config)# vlan 11
Switch-2(config-vlan-11)# tagged ethernet 1/3/4 ethernet 3/3/2 lag 2
Switch-2(config-vlan-11)# multicast sdvoe auto-edge-port-track-passive
```

Configuring SDVoE using the multicast sdvoe Command

The following task enables SDVoE in a network, as illustrated in the Figure 1 on page 29 figure. Switch 1 and Switch 2 have manually configured edge ports and fast leave is enabled only on these ports. IGMP snooping is enabled in passive mode for Switch 1 and Switch 2. SDVoE is configured for multicast packets in the VLAN. No edge ports are configured for the Querier switch. IGMP snooping is enabled in active mode for the Querier switch so that queries are generated.

NOTE
Edge-ports should be configured so that fast-leave can be enabled only on these ports.

NOTE
Querier switches do not need to have edge-ports configured as querier switches are generally used to connect to other switches.

1. On switch 1, enter global configuration mode.

```
Switch-1# configure terminal
```

2. Configure a VLAN dedicated to the SDVoE application and add ports to it.

```
Switch-1(config)# vlan 11
Switch-1(config-vlan-11)# tagged ethernet 1/2/6 ethernet 3/2/7 lag 1
```

3. Set the IGMP mode to passive for the VLAN.

```
Switch-1(config-vlan-11)# multicast passive
```

4. Enable fast leave on edge-ports only.

```
Switch-1(config-vlan-11)# multicast fast-leave-v2 edge-ports
```

5. Enable SDVoE for multicast packets in the VLAN.

```
Switch-1(config-vlan-11)# multicast sdvoe
```

6. For the Querier switch, enter global configuration mode.

```
Querier# configure terminal
```

7. Configure a VLAN dedicated to the SDVoE application and add ports to it.

```
Querier(config)# vlan 11
Querier(config-vlan-11)# tagged lag 1 lag 2
```

8. Set the IGMP mode to active.

```
Querier(config-vlan-11)# multicast active
```

9. Configure the source IPv4 address to be used in every query.

```
Querier(config-vlan-11)# multicast querier-address 3.3.3.3
```

10. Enable SDVoE for multicast packets.

```
Querier(config-vlan-11)# multicast sdvoe
```

11. On switch 2, enter global configuration mode.

```
Switch-2# configure terminal
```

12. Configure a VLAN dedicated to the SDVoE application and add ports to it.

```
Switch-2(config)# vlan 11
Switch-2(config-vlan-11)# tagged ethernet 1/3/4 ethernet 3/3/2 lag 2
```

13. Set the IGMP mode to passive for the VLAN.

```
Switch-2(config-vlan-11)# multicast passive
```

14. Enable fast leave on edge-ports only.

```
Switch-2(config-vlan-11)# multicast fast-leave-v2 edge-ports
```

15. Enable SDVoE for multicast packets in the VLAN.

```
Switch-2(config-vlan-11)# multicast sdvoe
```

The following example configures SDVoE in a network using the **multicast sdvoe** command.

```
Switch 1:
Switch-1# configure terminal
Switch-1(config)# vlan 11
Switch-1(config-vlan-11)# tagged ethernet 1/2/6 ethernet 3/2/7 lag 1
Switch-1(config-vlan-11)# multicast passive
Switch-1(config-vlan-11)# multicast fast-leave-v2 edge-ports
Switch-1(config-vlan-11)# multicast sdvoe

Querier Switch:
Querier# configure terminal
Querier(config)# vlan 11
Querier(config-vlan-11)# tagged lag 1 lag 2
Querier(config-vlan-11)# multicast active
Querier(config-vlan-11)# multicast querier-address 3.3.3.3
Querier(config-vlan-11)# multicast sdvoe


Switch 2:
Switch-2# configure terminal
Switch-2(config)# vlan 11
Switch-2(config-vlan-11)# tagged ethernet 1/3/4 ethernet 3/3/2 lag 2
Switch-2(config-vlan-11)# multicast passive
Switch-2(config-vlan-11)# multicast fast-leave-v2 edge-ports
Switch-2(config-vlan-11)# multicast sdvoe
```

Enabling SDVoE where Edge-ports are Automatically Created

The following task enables SDVoE in a network, as illustrated in the Figure 2 on page 31 figure. Edge ports are automatically configured for Switch 1 and Switch 2. Tracking for IGMPv2 and IGMPv3 is automatically enabled. Multicast passive, dynamic edge port and IGMPv2 and IGMPv3 client tracking is configured for Switch 1 and Switch 2. Multicast active, dynamic edge port and IGMPv2 and IGMPv3 client tracking is configured for the Querier switch.

NOTE
Fast leave is not supported.

1. On switch 1, enter global configuration mode.

```
Switch-1# configure terminal
```

2. Configure a VLAN dedicated to the SDVoE application and add ports to it.

```
Switch-1(config)# vlan 11
Switch-1(config-vlan-11)# tagged ethernet 1/2/6 ethernet 3/2/7 lag 1
```

3. Configure a multicast passive dynamic edge port and IGMPv2 and IGMPv3 client tracking for the VLAN.

```
Switch-1(config-vlan-11)# multicast sdvoe auto-edge-port-track-passive
```

4. For the querier switch, enter global configuration mode.

```
Querier# configure terminal
```

5. Configure a VLAN dedicated to the SDVoE application and add ports to it.

```
Querier(config)# vlan 11
Querier(config-vlan-11)# tagged lag 1 lag 2
```

6. Configure a multicast active dynamic edge port and IGMPv2 and IGMPv3 client tracking for the VLAN.

```
Querier(config-vlan-11)# multicast sdvoe auto-edge-port-track-active
```

7. Configure the IPv4 querier address per VLAN.

```
Querier(config-vlan-11)# multicast querier-address 3.3.3.3
```

8. On switch 2, enter global configuration mode.

```
Switch-2# configure terminal
```

9. Configure a VLAN dedicated to the SDVoE application and add ports to it.

```
Switch-2(config)# vlan 11
Switch-2(config-vlan-11)# tagged ethernet 1/3/4 ethernet 3/3/2 lag 2
```

10. Configure a multicast passive dynamic edge port and IGMPv2 and IGMPv3 client tracking for the VLAN.

```
Switch-2(config-vlan-11)# multicast sdvoe auto-edge-port-track-passive
```

The following example configures SDVoE in a network using the **multicast sdvoe auto-edge-port-track-act** and **multicast sdvoe auto-edge-port-track-pas** commands.

```
Switch 1:
Switch-1# configure terminal
Switch-1(config)# vlan 11
Switch-1(config-vlan-11)# tagged ethernet 1/2/6 ethernet 3/2/7 lag 1
Switch-1(config-vlan-11)# multicast sdvoe auto-edge-port-track-passive

Querier Switch:
Querier# configure terminal
Querier(config)# vlan 11
Querier(config-vlan-11)# tagged lag 1 lag 2
Querier(config-vlan-11)# multicast sdvoe auto-edge-port-track-active
Querier(config-vlan-11)# multicast querier-address 3.3.3.3

Switch 2:
Switch-2# configure terminal
Switch-2(config)# ip multicast edge-port ethe 1/3/4
Switch-2(config)# vlan 11
Switch-2(config-vlan-11)# tagged ethernet 1/3/4 ethernet 3/3/2 lag 2
Switch-2(config-vlan-11)# multicast sdvoe auto-edge-port-track-passive
```

Configuration Notes and Feature Limitations

- RUCKUS recommends that IGMPv2 configuration should be used for v2 hosts and IGMPv3 for v3 hosts for optimal performance. Using IGMPv3 with tracking with a v2 host does not give the desired result.
- With IGMPv3 tracking, only non-SSM groups using exclude mode for join is supported.

- If a set of group addresses that are flooded have identical MAC addresses with some other multicast streams, these Multicast streams are also flooded.
- When reports and leave messages are flooded in a VLAN for all non-edge ports, the Vlan learns the IGMP membership information for all the respective ports.
- Multicast streams received in a VLAN are not forwarded to mrouter ports.
- The configuring of a set of Multicast addresses to flood or drop in a VLAN is only supported for snooping-enabled VLANs.
- SDVoE cannot be enabled if the **ip multicast flood-unregistered** command is configured.
- Source-specific tracking is not supported.
- If you want packets for some multicast groups to be flooded in the hardware, you can add mcaches statically for those groups, either to flood or drop those packets.
- When SDVoE is enabled for a VLAN, a default profile is added automatically and static mcaches are created for the groups in the default profile.
- When SDVoE is not enabled for a VLAN, you can manually add a static mcache profile for that VLAN.

Displaying SDVoE Information

You can use various **show** commands to view information about Software Defined Video-over-Ethernet (SDVoE) configurations.

Use one of the following commands to view information about SDVoE configurations. The commands do not need to be entered in the specified order. Using these commands is optional and they can be entered in any order. For more information on the full list of **show ip multicast** commands, refer to the *RUCKUS FastIron Command Reference*.

1. Enter the **show ip multicast mcache** command to display information for the multicast forwarding mcache, including static mcache profile information and flooded and dropped packets.

```
device> show ip multicast mcache

Example:
(S G) (MAC ADDR) cnt=: SRC and GRP IPv4/IPv6 address,
Multicast Mac address, cnt is number of SW processed packets
OIF: 1/1/22 TR(1/1/32,1/1/33), TR is trunk, 1/1/32 primary, 1/1/33 output
IPv4 Multicast Forwarding Mode: IP
Total Multicast Cache: 13
vlan 10, 3 caches.
1 (* 225.0.0.2) (0100.5e00.0002) cnt=0
OIF: flood
age=5s up-time=3739s, change=3739s ipmc=2 (ref-cnt=1) static
2 (* 225.1.2.250) (0100.5e01.02fa) cnt=0
OIF: flood
age=20s up-time=3739s, change=3739s ipmc=2 (ref-cnt=1) static
3 (* 225.0.1.10) (0100.5e00.010a) cnt=0
OIF: drop
age=0s up-time=3739s, change=3739s ipmc=0 (ref-cnt=1) static

vlan 20, 7 caches.
1 (* 239.255.255.253) (0100.5e7f.fffd) cnt=0
OIF: flood
age=20s up-time=3739s, change=3739s ipmc=2 (ref-cnt=1) static
2 (* 224.0.1.129) (0100.5e00.0181) cnt=0
OIF: flood
age=5s up-time=3739s, change=3739s ipmc=2 (ref-cnt=1) static
3 (* 224.0.1.130) (0100.5e00.0182) cnt=0
OIF: flood
age=27s up-time=3739s, change=3739s ipmc=2 (ref-cnt=1) static
4 (* 239.255.255.250) (0100.5e7f.fffa) cnt=0
OIF: flood
age=18s up-time=3739s, change=3739s ipmc=2 (ref-cnt=1) static
5 (* 224.0.1.1) (0100.5e00.0101) cnt=0
OIF: flood
age=0s up-time=3739s, change=3739s ipmc=2 (ref-cnt=1) static
6 (* 224.0.1.132) (0100.5e00.0184) cnt=0
OIF: flood
age=11s up-time=3739s, change=3739s ipmc=2 (ref-cnt=1) static
7 (* 224.0.1.131) (0100.5e00.0183) cnt=0
OIF: flood
age=12s up-time=3739s, change=3739s ipmc=2 (ref-cnt=1) static
vlan 30, 3 caches.
1 (* 225.0.0.2) (0100.5e00.0002) cnt=0
OIF: flood
age=5s up-time=3739s, change=3739s ipmc=2 (ref-cnt=1) static
2 (* 225.1.2.250) (0100.5e01.02fa) cnt=0
OIF: flood
age=20s up-time=3739s, change=3739s ipmc=2 (ref-cnt=1) static
3 (* 225.0.1.10) (0100.5e00.010a) cnt=0
OIF: drop
age=0s up-time=3739s, change=3739s ipmc=0 (ref-cnt=1) static
```

2. Enter the **show ip multicast static-mcache-profile** command and specify a profile to view static mcache information for a configured profile.

```
device# show ip multicast static-mcache-profile 10

profile-id: 10, num of groups: 3, vlans: 10,
     Group            Fwd-mode
1    225.0.0.2        Flood
2    225.1.2.250      Flood
3    225.0.1.10       Drop
```

3. Enter the **show ip multicast static-mcache-profile** command with the **default-profile** keyword to view information about the profile of SDVoE groups.

```
device# show ip multicast static-mcache-profile default-profile

profile-id: Default profile, num of groups: 7, vlans: 20,
     Group            Fwd-mode
1    239.255.255.253  Flood
2    239.255.255.250  Flood
3    224.0.1.132      Flood
4    224.0.1.131      Flood
5    224.0.1.130      Flood
6    224.0.1.129      Flood
7    224.0.1.1        Flood
```

4. Enter the **show ip multicast vlan** command to view IGMP snooping information, including SDVoE configurations, for VLAN interfaces. In the below example, the only router port is the non-edge port. All other ports are edge ports.

```
device> show ip multicast vlan 11

Version=2, Intervals: Query=200, Group Age=1020, Max Resp=20, Other Qr=1010,
             Leave Wait=3, Robustness=5

VL11: dft V2, sdvoe-auto-edge-port-track-passive, 1 grp, 8 (*G) cache, (dy-1, st-0) rtr ports
        router ports: lg1(900) 3.3.3.3,
          My Query address: None
          Static Mcache profile id: Default profile
          e1/2/6    has    1 grp, non-QR (passive), default V2
            group: 225.1.1.1, life = 980
           e3/2/7    has    0 grp, non-QR (passive), default V2
            group: 225.1.1.1, life = 960
            lg1       has    1 grp, non-QR (QR=3.3.3.3, age=120, mrt=20), default V2 trunk
            group: 225.1.1.2, life = 1020
            group: 225.1.1.1, life = 1020
```

In the below example, all non-edge ports are automatically detected and listed (lg1 and lg2)..

```
device> show ip multicast vlan 11
    Version=2, Intervals: Query=200, Group Age=1020, Max Resp=20, Other Qr=1010,
               Leave Wait=3, Robustness=5

    VL11: dft V2, sdvoe-auto-edge-port-track-active, 1 grp, 8 (*G) cache, no rtr port
            passive neighbors: lg1(920), lg2(960)
        My Query address: 3.3.3.3 (configured)
        Static Mcache profile id: Default profile
        lg1       has    0 grp, QR, default V2 trunk
        group: 225.1.1.1, life = 1000
        lg2       has    1 grp, QR, default V2 trunk
        group: 225.1.1.2, life = 1000
            group: 225.1.1.1, life = 1020
```

5. Enter the **show ip multicast group tracking** command to display information about IGMP groups including whether or not if tracking has been enabled for IGMPv2 using the **multicast sdvoe auto-edge-port-track-act** or **multicast sdvoe auto-edge-port-track-pas** command.

```
device# show ip multicast group 225.1.1.1 tracking

    Display group 225.1.1.1  for all vlans on all ports with tracking enabled.
    p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
    VL11 : 1 groups, 1 group-port, tracking_enabled
              group           p-port      ST     QR     life  mode    source
    1   225.1.1.1        lg1         no     no     1000  EX      0
           receive reports from 1 clients:
               (11.3.1.3 (0))
```

Displaying IGMP Snooping Information

You can use various **show** commands to view information about IGMP snooping.

Use one of the following commands to view IGMP snooping information. The commands do not need to be entered in the specified order. Using these commands is optional and they can be entered in any order. For more information on the full list of **show ip multicast** commands, refer to the *RUCKUS FastIron Command Reference*.

1. Enter the **show ip multicast** command to display global IGMP snooping configuration.

```
device> show ip multicast

Summary of all vlans. Please use "sh ip mu vlan <vlan-id>" for details
Version=2, Intervals: Query=30, Group Age=80, Max Resp=10, Other Qr=65,
                      Leave Wait=2, Robustness=2

Replication resource sharing: Enabled.
VL20: dft V2, glb cfg active, 0 grp, 0 (*G) cache, no rtr port,
  My Query address: 20.1.1.1 (configured)
VL30: cfg V3, glb cfg active, track, 0 grp, 0 (SG) cache, no rtr port,
  My Query address: 30.1.1.1 (configured)
VL40: dft V2, glb cfg active, 0 grp, 0 (*G) cache, no rtr port,
  My Query address: None
VL100: dft V2, vlan cfg passive, 0 grp, 0 (*G) cache, rtr ports,
    router ports: e2/1/15(80) 10.1.1.1,
  My Query address: None
VL200: dft V2, vlan cfg passive, 0 grp, 0 (*G) cache, rtr ports,
    router ports: e2/1/15(80) 20.2.2.2,
  My Query address: None
```

2. Enter the **show ip multicast** command and specify a VLAN to display IGMP snooping information for the specified VLAN.

```
device> show ip multicast vlan 11

Version=2, Intervals: Query=300, Group Age=620, Max Resp=10, Other Qr=605,
                      Leave Wait=2, Robustness=2

VL11: dft V2, vlan cfg active, 20 grp, 0 (*G) cache, no rtr port,
  My Query address: 1.1.1.1 (ve/loopback)
  e1/2/2    has   20 grp, QR, default V2
    group: 225.1.11.14, life = 520
    group: 225.1.11.6, life = 520
    group: 225.1.11.12, life = 520
    group: 225.1.11.16, life = 520
  lg203     has    0 grp, QR, default V2 trunk
  e31/2/1   has    0 grp, QR, default V2
```

3. Enter the **show ip multicast error** command to display information about possible IGMP errors.

```
device> show ip multicast error

snoop SW processed pkt: 173, up-time 160 sec
```

4. Enter the **show ip multicast group** command to display information about IGMP groups.

```
device> show ip multicast group

p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL70 : 3 groups, 4 group-port, tracking_enabled
      group            p-port   ST     QR     life mode    source
1     224.1.1.2        1/1/33   no     yes    120  EX      0
2     224.1.1.1        1/1/33   no     yes    120  EX      0
3     226.1.1.1        1/1/35   yes    yes    100  EX      0
4     226.1.1.1        1/1/33   yes    yes    100  EX      0
```

5. Enter the **show ip multicast group** command with the **detail** keyword, and specify a group address, to display detailed information about an IGMP group.

```
device> show ip multicast group 226.1.1.1 detail

Display group 226.1.1.1 in all interfaces in details.
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL70 : 1 groups, 2 group-port, tracking_enabled
      group            p-port   ST     QR     life mode    source
1     226.1.1.1        1/1/35   yes    yes    120  EX      0
    group: 226.1.1.1, EX, permit 0 (source, life):
      life=120, deny 0:
      group            p-port   ST     QR     life mode    source
2     226.1.1.1        1/1/33   yes    yes    120  EX      0
    group: 226.1.1.1, EX, permit 0 (source, life):
      life=120, deny 0:
```

6. Enter the **show ip multicast mcache** command to display information in the multicast forwarding mcache.

```
device> show ip multicast mcache

Example:
    (S G) (MAC ADDR) cnt=: SRC and GRP IPv4/IPv6 address,
    Multicast Mac address, cnt is number of SW processed packets
    OIF: 1/1/22 TR(1/1/32,1/1/33), TR is trunk, 1/1/32 primary, 1/1/33 output
IPv4 Multicast Forwarding Mode: MAC
Total Multicast Cache: 10
vlan 4089, 10 caches.
1    (* 225.1.1.1) (0100.5e01.0101) cnt=97
     OIF: tag e1/1/2
     age=3s up-time=4372s, change=448s l2mc=257 (ref-cnt=1)
2    (* 236.1.1.8) (0100.5e01.0108) cnt=4
     OIF: tag e1/1/2
     age=9s up-time=4372s, change=439s l2mc=257 (ref-cnt=1)
```

7. Enter the **show ip multicast cluster mcache** command to display information in the multicast forwarding mcache when data arrives locally.

```
device> show ip multicast cluster mcache

Example:
    (S G) (MAC ADDR) cnt=: SRC and GRP IPv4/IPv6 address,
    Multicast Mac address, cnt is number of SW processed packets
    OIF: 1/1/22 TR(1/1/32,1/1/33), TR is trunk, 1/1/32 primary, 1/1/33 output
         [1,10]: [1 - has local oif, 10 - ICL due to CCEP count]
IPv4 Multicast Forwarding Mode: IP
Total Multicast Cache: 1
vlan 11, 1 caches.
1    (192.85.1.44 225.1.1.1) (0100.5e01.0101) cnt=2
     OIF: tag e1/1/35 [1,0] tag lg130 [0,1] tag e1/1/5 [1,0] tag lg1 [1,0]
     age=28s up-time=28s, change=28s ipmc=361 (ref-cnt=1)
```

8. Enter the **show ip multicast resource** command to display information about the software resources used.

```
device> show ip multicast resource

                      alloc in-use  avail get-fail    limit  get-mem  size init
igmp group              256      1    255        0    32000        1    16  256
igmp phy port          1024      1   1023        0   200000        1    22 1024
.... entries deleted ...
snoop mcache entry      128      2    126        0     8192        3    56  128
total pool memory 109056 bytes
has total 2 forwarding hash
```

9. Enter the **show ip multicast traffic** command to display information about IPv4 PIM traffic statistics.

```
device> show ip multicast traffic

IGMP snooping: Total Recv: 22, Xmit: 26
Q: query, Qry: general Q,  G-Qry: group Q,  GSQry: group-source Q, Mbr: member
Recv      QryV2     QryV3     G-Qry     GSQry     MbrV2     MbrV3     Leave
VL1           0         0         0         0         4         0         0
VL70         18         0         0         0         0         0         0
Recv       IsIN      IsEX      ToIN      ToEX     ALLOW     BLOCK   Pkt-Err
VL1           0         4         0         0         0         0         0
VL70          0         0         0         0         0         0         0
Send      QryV2     QryV3     G-Qry     GSQry     MbrV2     MbrV3
VL1           0         0         8         0         0         0
VL70          0         0         0         0         0        18
VL70   pimsm-snooping, Hello:    12,  Join/Prune:     9
```

Verifying Multicast Mcache for Multicast Groups which Share the Same Multicast MAC Address (IGMP snooping)

If there are two multicast groups (225.1.1.1 and 234.1.1.1) which map to the same multicast MAC address, the **show ip multicast mcache** command output for one of the groups will be empty.

Complete the following steps to check whether the active mcache is present for that group.

NOTE

These steps are to be used when snooping is MAC-based for IPv4. IGMP snooping is MAC-based for the ICX 7150-C08 device, but it is IP-based for all other devices.

1. Get the mapped multicast MAC address for the interested multicast group (use 23 as the bit value for an exact match).

```
device# show ip multicast group 234.1.1.1 match-last-bits 23
Display groups sharing same mac address 0100.5e01.0101 with group 234.1.1.1  for all vlans on all
ports.
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL4089 : 11 groups, 23 group-port
      group           p-port      ST     QR     life  mode    source
1     234.1.1.1       lg1         no     yes    240   EX      0
2     234.1.1.1       e1/1/8      no     yes    260   EX      1
3     225.1.1.1       lg1         no     yes    240   EX      0
4     225.1.1.1       e1/1/8      no     yes    260   EX      1
```

2. Using the multicast MAC address (0100.5e01.0101), get the multicast group address with which the mcache is programmed.

```
device# show ip multicast mac-mcache 0100.5e01.0101
    Example:
     MAC = xxxx.xxxx.xxxx Vlan = #, l2mc = # , ref_cnt = #
     IP Multicast Group :
         Mcast Group, Src Addr
     OIF: 1/1/22 TR(1/1/32,1/1/33), TR is trunk, 1/1/32 primary, 1/1/33 output
Total Multicast Mac Cache: 1
vlan 4089, 10 caches
1      MAC=0100.5e01.0101, vlan=4089, l2mc=257, ref_cnt=1
       IP Multicast Group
           (* 225.1.1.1)
        OIF:  1/1/2 1/1/8 lg1
        Total Multicast Mac Cache: 1
```

3. Verify whether the multicast mcache is present for the multicast group 225.1.1.1.

```
device# show ip multicast mcache 225.1.1.1
Example:
    (S G) (MAC ADDR) cnt=: SRC and GRP IPv4/IPv6 address,
    Multicast Mac address, cnt is number of SW processed packets
    OIF: 1/1/22 TR(1/1/32,1/1/33), TR is trunk, 1/1/32 primary, 1/1/33 output
IPv4 Multicast Forwarding Mode: MAC
Total Multicast Cache: 10
vlan 4089, 10 caches.
1    (* 225.1.1.1) (0100.5e01.0101) cnt=226
     OIF: tag e1/1/2 tag e1/1/8 tag lg1
     age=26s up-time=141s, change=141s l2mc=257 (ref-cnt=1
```

PIM SM Traffic Snooping Overview

When multiple PIM sparse mode (PIM SM) routers connect through a snooping-enabled device, the RUCKUS device always forwards multicast traffic to these routers. For example, PIM sparse routers R1, R2, and R3 connect through a device. Assume R2 needs traffic, and R1 sends it to the device, which forwards it to both R2 and R3, even though R3 does not need it. A PIM SM snooping-enabled device listens to join and prune messages exchanged by PIM sparse routers, and stops traffic to the router that sends prune messages. This allows the device to forward the data stream to R2 only.

PIM SM traffic snooping requires IGMP snooping to be enabled on the device. IGMP snooping configures the device to listen for IGMP messages. PIM SM traffic snooping provides a finer level of multicast traffic control by configuring the device to listen specifically for PIM SM join and prune messages sent from one PIM SM router to another through the device.

Application Examples of PIM SM Traffic Snooping

The following figure shows an example application of the PIM SM traffic snooping feature. In this example, a device is connected through an IP router to a PIM SM group source that is sending traffic for two PIM SM groups. The device also is connected to a receiver for each of the groups.

When PIM SM traffic snooping is enabled, the device starts listening for PIM SM join and prune messages and IGMP group membership reports. Once the device receives a join message or group membership report for a group, the device forwards subsequent traffic for that group only on the ports from which the join messages or IGMP reports were received.

In this example, the router connected to the receiver for group 239.255.162.1 sends a join message toward the group source. Because PIM SM traffic snooping is enabled on the device, the device examines the join message to learn the group ID, then makes a forwarding entry for the group ID and the port connected to the receiver router. The next time the device receives traffic for 239.255.162.1 from the group source, the device forwards the traffic only on port 1/4/1, because that is the only port connected to a receiver for the group.

Notice that the receiver for group 239.255.162.69 is directly connected to the device. As a result, the device does not see a join message on behalf of the client. However, because IGMP snooping also is enabled, the device uses the IGMP group membership report from the client to select the port for forwarding traffic to group 239.255.162.69 receivers.

The IGMP snooping feature and the PIM SM traffic snooping feature together build a list of groups and forwarding ports for the VLAN. The list includes PIM SM groups learned through join messages as well as MAC addresses learned through IGMP group membership reports. In this case, even though the device never sees a join message for the receiver for group 239.255.162.69, the device nonetheless learns about the receiver and forwards group traffic to the receiver.

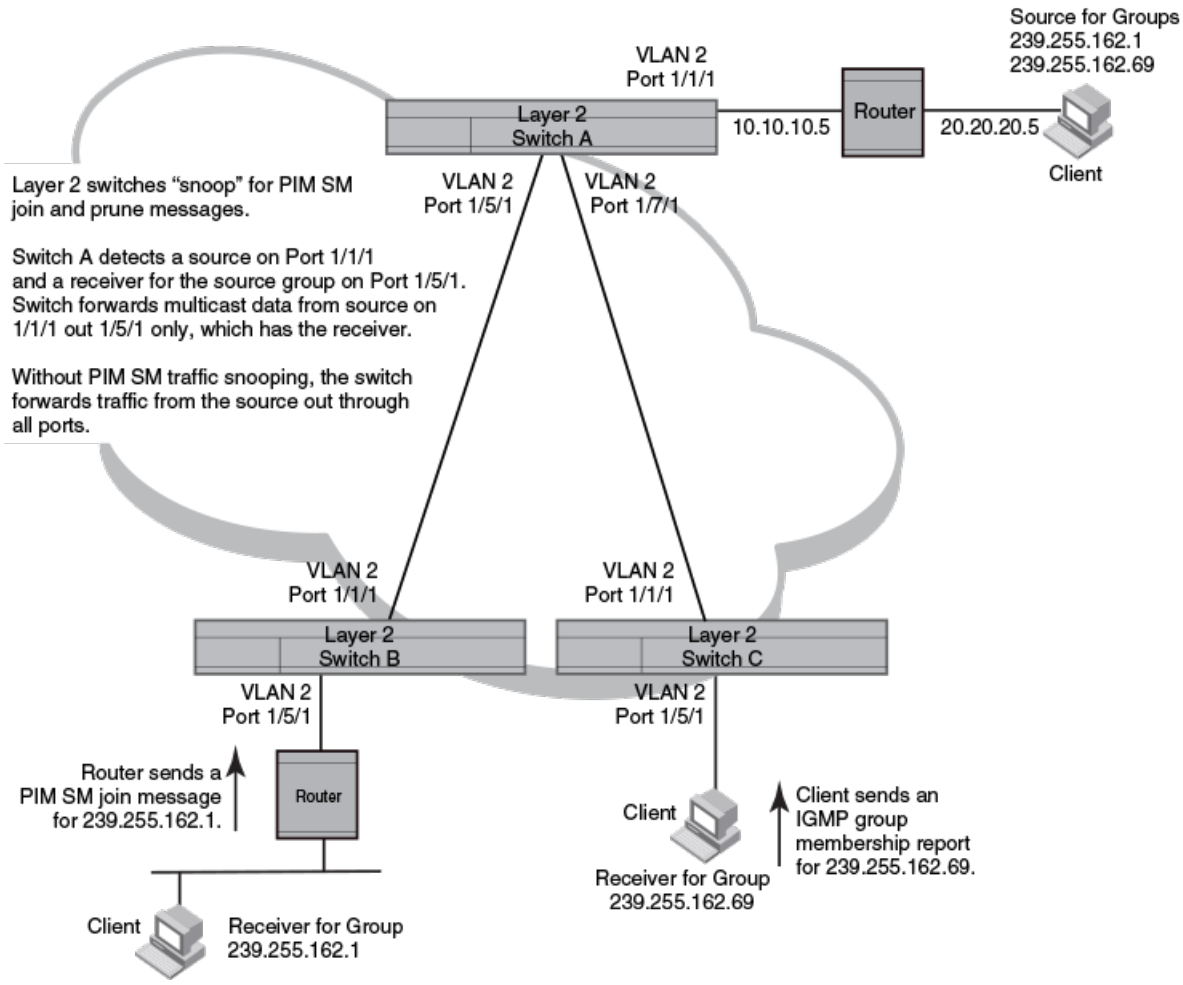
The device stops forwarding IP multicast traffic on a port for a group if the port receives a prune message for the group.

Notice that the ports connected to the source and the receivers are all in the same port-based VLAN on the device. This is required for the PIM SM snooping feature. The devices on the edge of the global Ethernet cloud are configured for IGMP snooping and PIM SM traffic snooping. Although this application uses multiple devices, the feature has the same requirements and works the same way as it does on a single device.

The following figure also shows devices on the edge of a global Ethernet cloud (a Layer 2 packet over SONET cloud). Assume that each device is attached to numerous other devices such as other Layer 2 switches and Layer 3 switches (routers).

NOTE
This example assumes that the devices are actually RUCKUS devices running Layer 2 switch software.

FIGURE 3 PIM SM Traffic Reduction in Global Ethernet Environment



The devices on the edge of the global Ethernet cloud are configured for IGMP snooping and PIM SM traffic snooping. Although this application uses multiple devices, the feature has the same requirements and works the same way as it does on a single device.

Configuration Notes and Limitations for PIM SM Snooping

- PIM SM snooping applies only to PIM SM version 2 (PIM SM V2).
- PIM SM traffic snooping is supported on both the switch and router image.
- IGMP snooping must be enabled on the device that will be running PIM SM snooping. The PIM SM traffic snooping feature requires IGMP snooping.
- On router images, PIM SM traffic snooping is not supported for the default VLAN.

  NOTE
  Use the passive mode of IGMP snooping instead of the active mode. The passive mode assumes that a router is sending group membership queries as well as join and prune messages on behalf of receivers. The active mode configures the device to send group membership queries.

- All the device ports connected to the source and receivers or routers must be in the same port-based VLAN.

- The PIM SM snooping feature assumes that the group source and the device are in different subnets and communicate through a router. The source must be in a different IP subnet than the receivers. A PIM SM router sends PIM join and prune messages on behalf of a multicast group receiver only when the router and the source are in different subnet. When the receiver and source are in the same subnet, they do not need the router in order to find one another. They find one another directly within the subnet.

The device forwards all IP multicast traffic by default. Once you enable IGMP snooping and PIM SM traffic snooping, the device initially blocks all PIM SM traffic instead of forwarding it. The device forwards PIM SM traffic to a receiver only when the device receives a join message from the receiver. Consequently, if the source and the downstream router are in the same subnet, and PIM SM traffic snooping is enabled, the device blocks the PIM SM traffic and never starts forwarding the traffic. This is because the device never receives a join message from the downstream router for the group. The downstream router and group find each other without a join message because they are in the same subnet.

NOTE
If the "route-only" feature is enabled globally on a Layer 3 switch, PIM SM snooping traffic is not supported.

PIM SM Snooping Configuration

Configuring PIM sparse mode (PIM SM) snooping on a RUCKUS device consists of the following global and VLAN-specific tasks.

Perform the following global PIM SM snooping tasks:

- Enabling PIM SM Snooping
- Disabling PIM SM Snooping

Perform the following VLAN-specific PIM SM snooping tasks:

- Enabling PIM SM Snooping on a VLAN
- Disabling PIM SM Snooping on a VLAN

Enabling PIM SM Snooping

Use PIM SM snooping only in topologies where multiple PIM sparse routers connect through a device. PIM SM snooping does not work on a PIM dense mode router which does not send join messages and traffic to PIM dense ports is stopped. A PIM SM snooping-enabled device displays a warning if it receives PIM dense join or prune messages.
The PIM SM traffic snooping feature assumes that the network has routers that are running PIM SM.

1. Enter global configuration mode.

```
device# configure terminal
```

2. To enable PIM sparse snooping globally, enter the **ip pimsm-snooping** command.

```
device(config)# ip pimsm-snooping
```

NOTE
The device must be in passive mode before it can be configured for PIM SM snooping.

Disabling PIM SM Snooping Globally

If PIM SM snooping has been enabled, you can disable it globally. One scenario where PIM SM snooping does not work, is on a PIM dense mode router which does not send join messages. When disabling PIM SM, you may also want to disable IP multicast traffic reduction.

1. Enter global configuration mode.

```
device# configure terminal
```

2. To disable PIM sparse snooping globally, enter the **no ip pimsm-snooping** command.

```
device(config)# no ip pimsm-snooping
```

3. If you also want to disable IP multicast traffic reduction, enter the **no ip multicast** command.

```
device(config)# no ip multicast
```

Enabling PIM SM Snooping on a VLAN

You can enable PIM SM snooping for a specific VLAN. This setting overrides the global setting.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Create VLAN 20.

```
device(config)# vlan 20
```

3. To enable PIM sparse snooping for a specific VLAN, enter the **multicast pimsm-snooping** command.

```
device(config-vlan-20)# multicast pimsm-snooping
```

Disabling PIM SM Snooping on a VLAN

When PIM SM snooping is enabled globally, you can still disable it for a specific VLAN. For example, the following commands disable PIM SM snooping for VLAN 20. This setting overrides the global setting. One scenario where PIM SM snooping does not work, is on a PIM dense mode router which does not send join messages.

1. Enter global configuration mode.

```
device# configure terminal
```

2. To specify the VLAN for which PIM SM snooping is to be disabled.

```
device(config)# vlan 20
```

3. To disable PIM sparse mode snooping, enter the **multicast disable-pimsm-snoop** command.

```
device(config-vlan-20)# multicast disable-pimsm-snoop
```

Displaying PIM SM Snooping Information

You can use various **show** commands to view information about PIM sparse mode (SM) snooping.

Use one of the following commands to view PIM SM snooping information. The commands do not need to be entered in the specified order. Using these commands is optional and they can be entered in any order. For more information on the full list of **show ip multicast** commands, refer to the *RUCKUS FastIron Command Reference*.

1. Enter the **show ip multicast pimsm-snooping** command to display PIM SM snooping information.

```
device> show ip multicast pimsm-snooping
Example: Port: 7/3 (ref_count=1)
         ref_count: no of entries in pimsm snoop cache added this oif)

vlan 503, has 1 caches.
1    (* 225.1.1.1) has 3 pim join ports out of 4 OIF
     4/23 (ref_count=2), 4/13 (ref_count=1), 4/5 (ref_count=3),
```

2. Enter the **show ip pimsm-snooping** command and specify a VLAN to display PIM SM snooping information for the VLAN.

```
device> show ip pimsm-snooping vlan 111

 OIF Info:
 TR - OIF Belongs to Trunk/LAG, Lag Interface is displayed
 SG - (s,g) downstream fsm state:
 G - (*,g) downstream fsm state:
     NI : No Info, J : Join, PP : Prune Pending, CLEAN : cleanup in progress
 RPT - (s,g,rpt) downstream fsm state:
     NI : No Info, P : Pruned, PP : Prune Pending, Px : Temp step in (*,G)
     join processing, PPx : Temp State in (*,G) processing, CLEAN : cleanup
     in progress.

PIMSM Snoop cache for vlan 111, has 240 cache
1      (* 225.1.51.1) Up Time: 00:40:48
        OIF: 1
        lg1 G : J(163) ET: 210, Up Time: 00:40:48
```

Multicast VLAN Registration

MVR Overview

Internet Group Management Protocol (IGMP), which is used for IPv4 network multicasting, uses the resources inefficiently in Layer 2 networks. For example, a multicast stream received on one VLAN in a Layer 2 network is distributed to interfaces only within that VLAN, which could be a problem when receivers are in different VLANs. This inefficiency also poses the issue of duplication of multicast streams when hosts in multiple VLANs request the same multicast stream, which wastes the bandwidth. Multicast VLAN Registration (MVR) enables more efficient distribution of Internet Protocol Television (IPTV) multicast streams across a Layer 2 network. The duplication of multicast streams from the same source is eliminated while maintaining isolation between hosts on different VLANs.

MVR configuration involves creation of a dedicated multicast VLAN (MVLAN) specifically for multicast traffic distribution. This multicast VLAN becomes the MVR source VLAN to which a range of multicast group addresses is assigned. You can configure other VLANs to be MVR receiver VLANs that receive multicast streams from the MVLAN. It is through the single dedicated MVLAN that multicast traffic from the source flows throughout the Layer 2 network while subscribers remain in separate VLANs. When deployed, each device that receives a multicast stream from the MVLAN checks each multicast group address assigned to it and forwards the multicast VLAN traffic to a particular receiver VLAN. You can configure multiple MVLANs on a device, but they must have disjointed multicast groups. An MVR receiver VLAN gets associated dynamically to more than one MVLAN according to the multicast group address.

There are two types of MVR ports:

- MVR Source Port (SP): The port to which the multicast traffic flows using the MVLAN. The source port must be in the MVLAN.
- MVR Receiver Port (RP): The port where a listening host is connected to the switch. Receiver ports can be in different VLANs except the MVLAN.

MVR-enabled devices selectively forward IPTV multicast traffic from interfaces on the MVLAN (source ports) to host interfaces in other VLANs designated as MVR receiver ports. MVR receiver ports can receive traffic from source ports on the MVLAN but cannot send traffic to the MVLAN. The receiver ports remain in their own VLANs for bandwidth and security reasons.

MVR assumes that subscriber ports subscribe and unsubscribe (join and leave) these multicast streams by sending out IGMP join and leave messages.

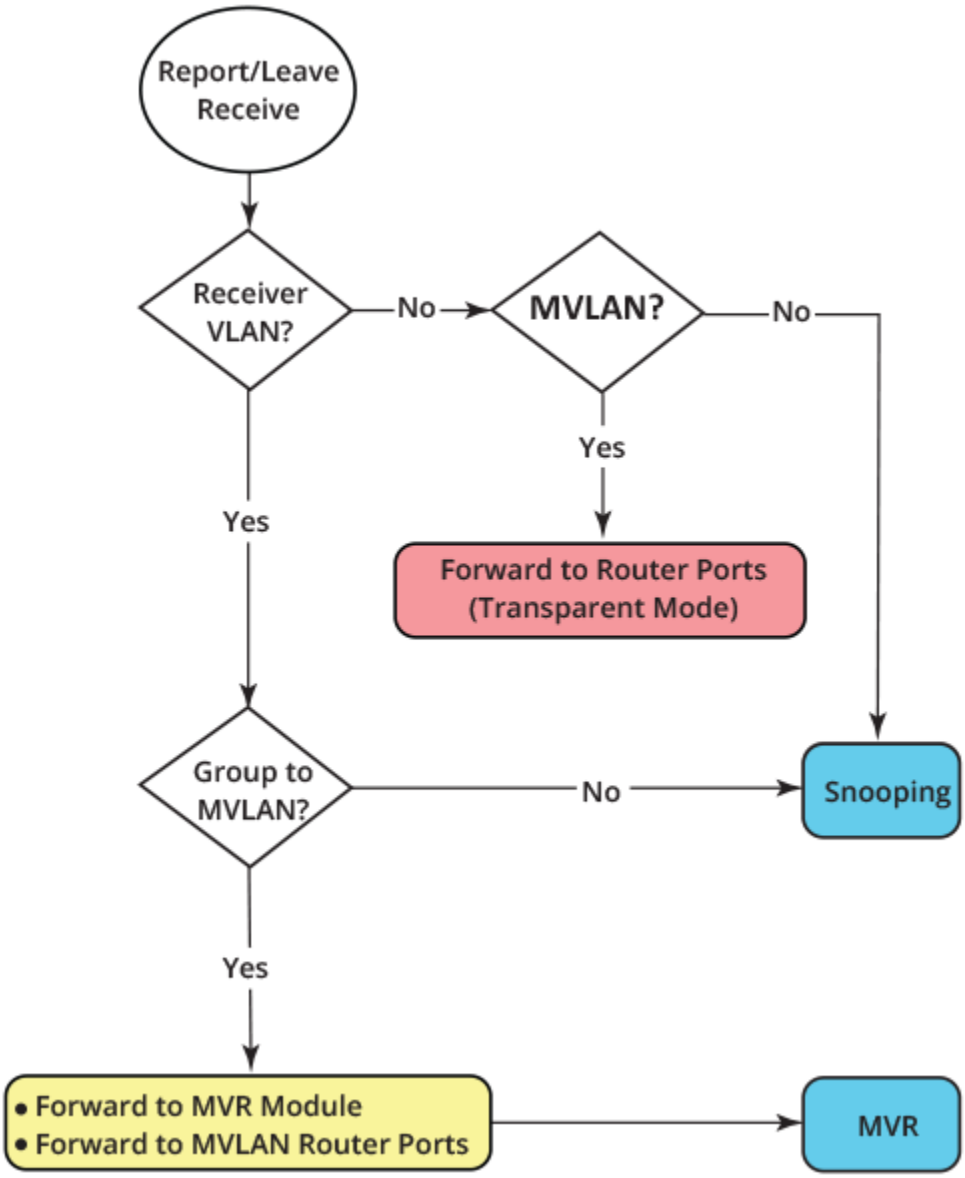
VLAN enabled MVR handles IGMP messages for the following processes:

- Reports/Leaves

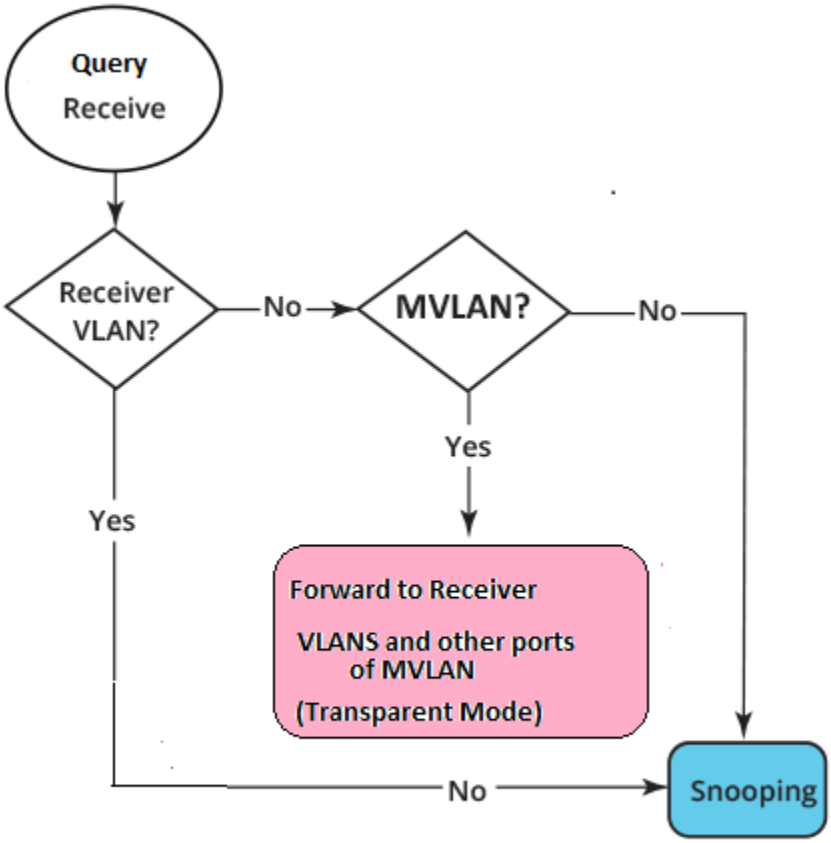
  The following flowchart captures modification in Reports/Leaves processing for MVR-enabled VLANs. Groups that belong to the MVLAN are processed in the MVLAN context only if received from receiver ports.

  NOTE
  The MVLAN is in transparent mode. Reports are transparently forwarded, and are not used to learn group membership in the source VLAN.

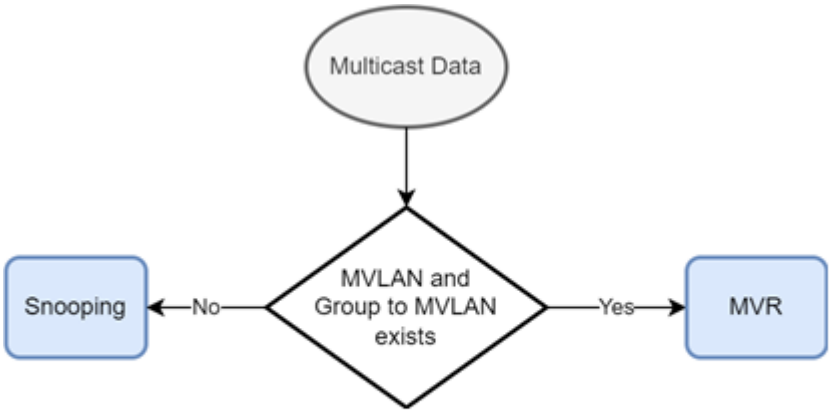
FIGURE 4 MVR: Report/Leave Processing



- Query



- Multicast Data

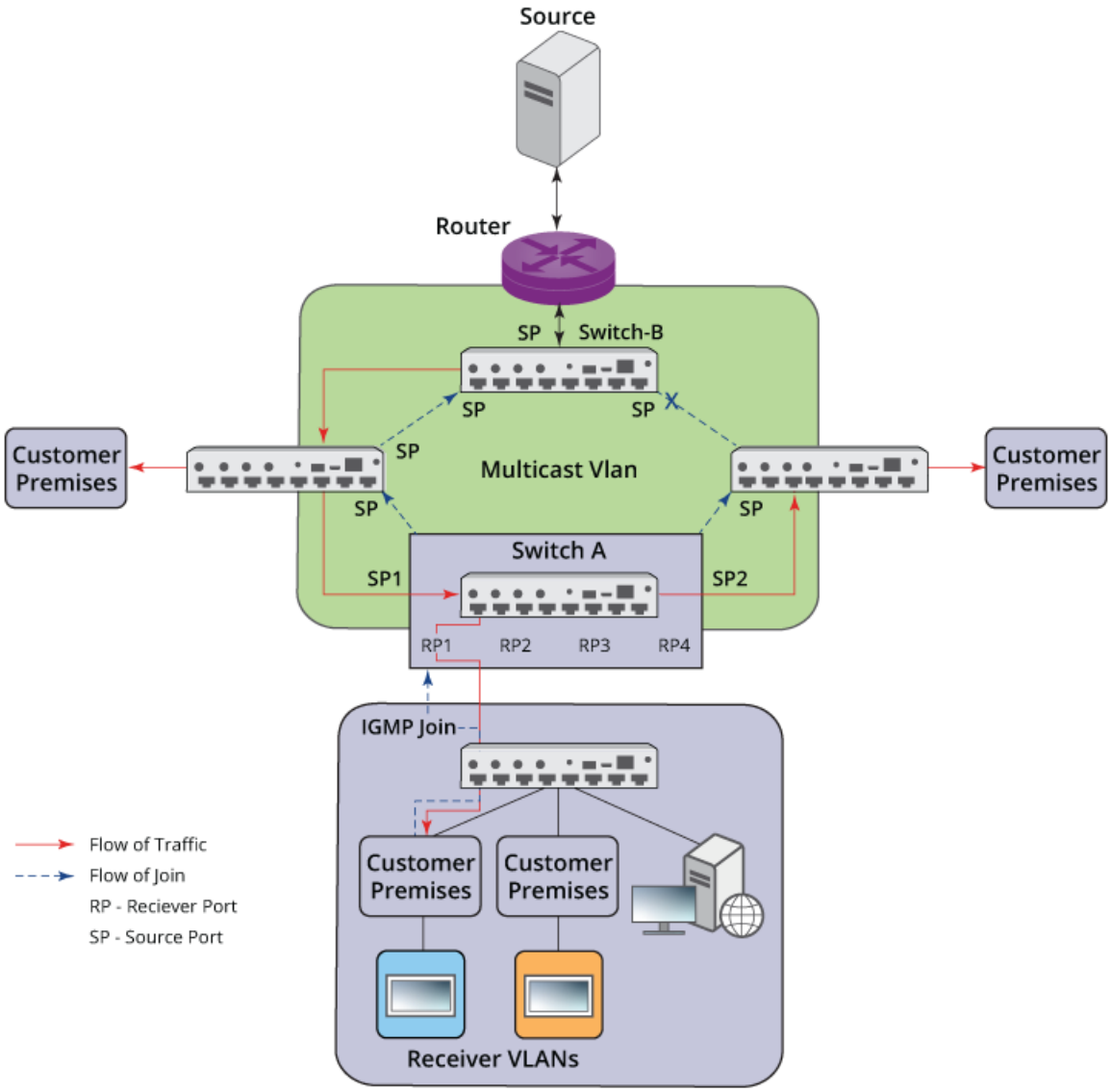


NOTE
By default, multicast data is only forwarded to router ports. Source ports that are not router ports must be manually configured as router ports to be included in the forwarding of multicast data.

Using MVR in a Multicast Television Application

In a multicast television application, a PC or television with a set-top box can receive multicast streams. Multiple PCs or set-top boxes can be connected to one subscriber port, which is a switch port configured as an MVR receiver port (RP). When a subscriber selects a channel, the set-top box or PC sends an IGMP report to Switch A to join the appropriate multicast group. The switch modifies the forwarding table to include this receiver port as a forwarding destination in the MVLAN. An uplink port that sends and receives multicast data to and from within the MVLAN is called an MVR source port (SP).

FIGURE 5 MVR: Ethernet-Based Ring Topology

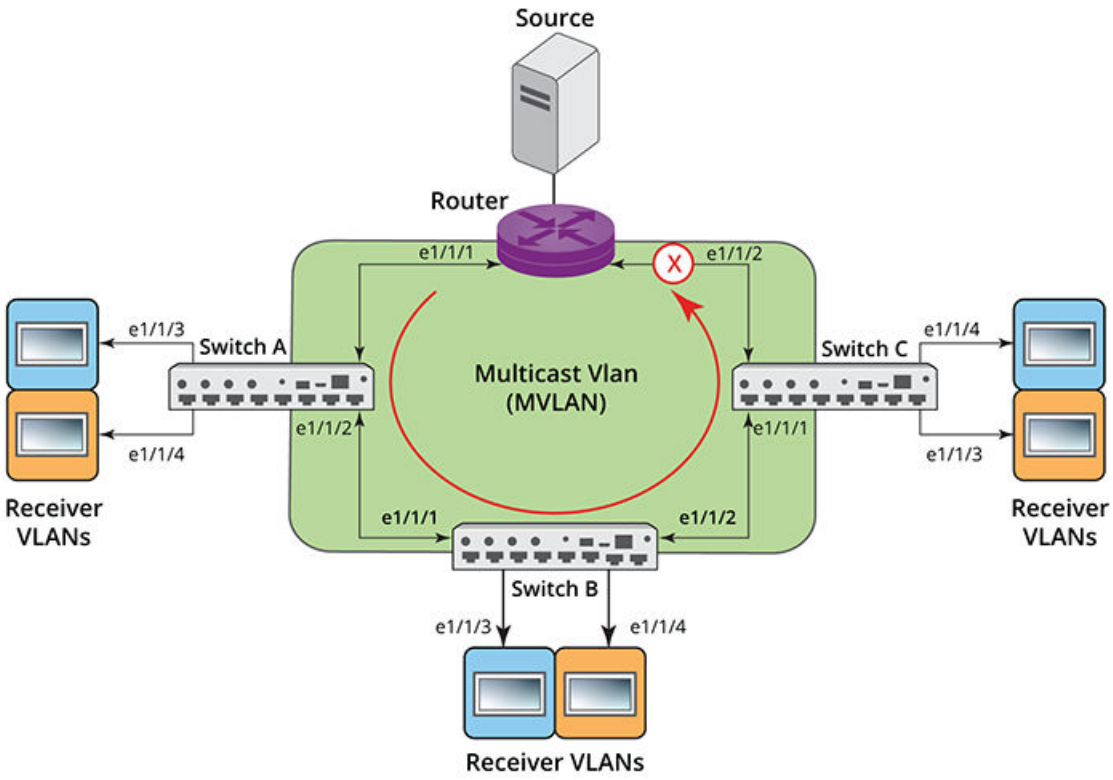


MVR eliminates the need to duplicate television-channel multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent around the MVLAN only once. The receivers in the Receiver VLANs request multicast traffic in the MVLAN using IGMP Report/Leave messages on an on-demand basis. The access layer switch, Switch A in this example, modifies the forwarding behavior to allow the traffice to be forwarded from the MVLAN to the subscriber port in a different VLAN, selectively allowing traffic to cross between two VLANs.

Configuring Multicast VLAN Registration

Complete the following steps to configure Multicast VLAN Registration (MVR) on the device as displayed in the sample configuration topology.

FIGURE 6 MVR Sample Configuration Topology



1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Enable MVR globally.

   ```
   device(config)# ip multicast mvr
   ```

   The global MVR configuration does not enable MVR on the VLAN. To enable MVR on the VLAN, you must use the **multicast mvr** command in VLAN configuration mode.

3. Configure group-to-MVLAN mapping.

```
device(config)# ip multicast mvr mvlan 1 group 225.0.0.1
device(config)# ip multicast mvr mvlan 1 group 226.0.0.1 count 100
```

A

receiver VLAN receiving IGMP group joins gets associated to the MVLAN configured via MVLAN to the group mapping command. This command allows you to selectively associate sets of groups to the MVLAN. Moreover, you can associate unique group sets to different MVLANs, and therefore create multiple MVLANs in the system.

NOTE
A group, in the absence of such mapping, is processed in the snooping module.

NOTE
While changing group-map configs (adding or removing), you must clear the mcache manually to switch between the snooping and the MVR module.

4. Create a receiver VLAN on all switches A, B, and C and add receiver ports as tagged. Enable the MVR receiver.

```
device(config)# vlan 11
device(config-vlan-11)# tagged ethernet 1/1/3 ethernet 1/1/4
device(config-vlan-11)# multicast mvr receiver
device(config-vlan-11)# multicast passive
```

Tagged and untagged interfaces are supported.

5. Configure the source VLAN (MVLAN) on all switches (A, B, and C). Add source ports to the VLAN. Enable the MVR source.

```
device(config)# vlan 1
device(config-vlan-1)# tagged ethernete 1/1/1 ethernet 1/1/2
device(config-vlan-1)# multicast mvr source
device(config-vlan-1)# multicast passive
```

MVR Configuration Considerations and Limitations

- MVR is not supported on a private VLAN (PVLAN).
- The maximum number of MVR interfaces supported is bound by the total number of VE interfaces supported on the platform.
- The maximum number of MVLANs supported is 10 and 100 MVLANs to group configurations.
- The maximum number of flows and outgoing interfaces (OIFs) supported is similar to the PIM module scale numbers for that platform.
- MVR is supported for router images only.
- PIM is not supported with MVR, and vice versa.

Displaying MVR Information

Use the **show ip multicast mvr mvlan group-map** command to display group-to-MVLAN mapping details.

```
device#show ip multicast mvr mvlan group-map

MVLAN      count/             Start Group        End Group
           Range               Address           Address
---------+------------+-------------------+-----------------
10         1           225.0.0.1                225.0.0.1
11         10          226.0.0.1                226.0.0.10
11         range       228.0.0.1                228.0.0.10
12         1           229.0.0.2                229.0.0.2
```

Use the **show ip multicast mvr mvlan** *mvlan-id* **group-map** command to display information about mapping of a specific MVLAN to group.

```
device#show ip multicast mvr mvlan 11 group-map

MVLAN      count/           Start Group           End Group
           Range             Address               Address
---------+------------+-------------------+------------------
11          10            226.0.0.1             226.0.0.10
11          range         228.0.0.1             228.0.0.10
```

Use the **show ip multicast mvr mvlan group-map** *grp-addr* command to display information about MVR based on the multicast group address assigned to the MVLAN.

```
device#show ip multicast mvr mvlan group-map 226.0.0.1

MVLAN      count/           Start Group      End Group
           Range             Address         Address
---------+------------+-------------------+------------------
11         10           226.0.0.1           226.0.0.10
```

Use the **show ip multicast vlan** command to display MVR-related information in IGMP snooping configurations.

```
device# show ip multicast vlan
Summary of all vlans. Please use "sh ip mu vlan <vlan-id>" for details
Version=2, Intervals: Query=11, Group Age=40, Max Resp=10, Other Qr=27,
Leave Wait=2, Robustness=2

Replication resource sharing: Enabled
Unregistered IPv4 Multicast Packets Flooding: Disabled
MVR: Enabled

VL1: dft V2, vlan cfg passive, mvr-s, 0 grp, 0 (SG) cache, no rtr port
VL10: dft V2, vlan cfg passive, mvr-r, 1 grp, 1 (*G) cache, (dy-1, st-0) rtr ports
```

When MVR is disabled, the **show ip multicast vlan** command displays the following output.

```
device#show ip multicast vlan
Summary of all vlans. Please use "sh ip mu vlan <vlan-id>" for details
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=255,
                      Leave Wait=2, Robustness=2

Replication resource sharing: Enabled
Unregistered IPv4 Multicast Packets Flooding: Disabled
MVR: Disabled
```

Use the **show ip multicast vlan** command with a specific *vlan-id* to display MVR details for a specific VLAN.

```
device#show ip multicast vlan 1
Version=2, Intervals: Query=11, Group Age=40, Max Resp=10, Other Qr=27,
Leave Wait=2, Robustness=2

VL1: dft V2, vlan cfg passive, mvr-s, 0 grp, 0 (SG) cache, no rtr port
My Query address: 1.0.0.24 (ve/loopback)
Edge ports: ALL
Non-Edge ports: NONE

e1/1/1 has 0 grp, non-QR (passive), mvr-s, default V2
e1/1/2 has 0 grp, non-QR (passive), mvr-s, default V2
```

Use the **show ip mvr interface** command to display MVR interface information.

```
device> show ip mvr interface

Flags    : MV-R - MVR Receiver, MV-S - MVR Source

---------+---------------+----+---+
Interface|Local          |Mode|St |
         |Address        |    |   |
---------+---------------+----+---+
```

```
      v1 *               MV-S Ena
      v2 *               MV-S Ena
     v10 *               MV-R Ena
     v11 *               MV-R Ena
Total Number of Interfaces : 4
```

Use the **show ip mvr mcache** command to display informataion about the MVR forwarding database.

```
device> show ip mvr mcache

IP Multicast MVR Mcache Table
Entry Flags    : MVR  - Multicast VLAN Registration Mode
                 LSRC - Local Source, LRCV - Local Receiver
                 HW - HW Forwarding Enabled, FAST - Resource Allocated, TAG - Need For Replication Entry
Interface Flags: MJ - Membership Join, MI - Membership Include, ME - Membership Exclude
                 MS - MVR Srouce Port

Total entries in mcache: 1

1     (53.0.0.10, 225.0.0.1) in v1 (tag e1/1/1), Uptime 14:08:27 (MVR) <-------- shows v1 is source vlan
      Source is MVR MVlan
      Flags (0x600400e1) MVR LRCV HW FAST TAG
      fast ports: ethe 1/1/1 eth 1/1/2 eth 1/1/3 eth 1/1/4
      AgeSltMsk: 1, IPMC:   293
      Forwarding_oif: 4
      L3 (HW) 2:
          e1/1/3(VL10), 14:08:27/0, Flags: MJ         <--- Member joined on receiver VLANS
          e1/1/4(VL11), 14:08:27/0, Flags: MJ
      L2 (HW) 2:
          e1/1/1,  14:08:27/0, Flags: MS              <------- Note: source vlan ports are added by default
          e1/1/2,  14:08:18/0, Flags: MS
      Src-Vlan:   1
Number of matching entries: 1
```

Enter the **show ip mvr setting** command to display MVR global settings.

```
device> show ip mvr settings

Global MVR Mode Settings
  MVR: Global               : Yes             Mode                  : Transparent
  Mcache: Total In-Use      : 1               Curr Max limit(HW)    : 1024
  Mcache: Current Count     : 1               Inactivity interval   : 180
```

IPv6 Multicast VLAN Traffic Reduction

MLD Snooping Overview

The default method a device uses to process an IPv6 multicast packet is to broadcast it to all ports except the incoming port of a VLAN. Packets are flooded by hardware without going to the CPU, which may result in some clients receiving unwanted traffic.

If a VLAN is not Multicast Listening Discovery (MLD) snooping-enabled, it floods IPv6 multicast data and control packets to the entire VLAN in hardware. When snooping is enabled, MLD packets are trapped to the CPU. Data packets are mirrored to the CPU and flooded to the entire VLAN. The CPU then installs hardware resources so subsequent data packets can be hardware-switched to desired ports without going through the CPU. If there is no client report, the hardware resource drops the data stream.

MLD protocols provide a way for clients and a device to exchange messages, and allow the device to build a database indicating which port wants what traffic. Since the MLD protocols do not specify forwarding methods, MLD snooping or multicast protocols such as IPv6 PIM-Sparse Mode (PIM6 SM) are required to handle packet forwarding. PIM6 SM can route multicast packets within and outside a VLAN, while MLD snooping can switch packets only within a VLAN.

MLD snooping provides multicast containment by forwarding traffic only to those clients that have MLD receivers for a specific multicast group (destination address). The device maintains the MLD group membership information by processing MLD reports and generating messages so traffic can be forwarded to ports receiving MLD reports. This is analogous to IGMP Snooping on RUCKUS Layer 3 switches.

An IPv6 multicast address is a destination address in the range of FF00::/8. A limited number of multicast addresses are reserved. Because packets destined for the reserved addresses may require VLAN flooding, Data packets destined to these addresses are flooded to the entire VLAN by hardware and mirrored to the CPU. Multicast data packets destined to addresses outside the FF0X::00X range and FFXX:XXXX:XXXX:XXXX:XXXX:XXXX:1:2 are snooped. A client must send MLD reports in order to receive traffic.

An MLD device periodically sends general queries and sends group queries upon receiving a leave message, to ensure no other clients at the same port still want this specific traffic before removing it. MLDv1 allows clients to specify which group (destination IPv6 address) will receive traffic. (MLDv1 cannot choose the source of the traffic.) MLDv2 deals with source-specific multicasts, adding the capability for clients to INCLUDE or EXCLUDE specific traffic sources. An MLDv2 device's port state can either be in include or exclude mode.

There are different types of group records for client reports. Clients respond to general queries by sending a membership report containing one or more of the following records associated with a specific group:

- Current-state record: Indicates the sources from which the client wants to receive or not receive traffic. This record contains the addresses of the multicast sources and indicates whether or not traffic will be included (IS_IN) or excluded (IS_EX) from that source address.
- Filter-mode-change record: If the client changes its current state from IS_IN to IS_EX, a TO_EX record is included in the membership report. Likewise, if a client current state changes from IS_EX to IS_IN, a TO_IN record appears in the membership report.
- MLDv1 leave report: Equivalent to a TO_IN (empty) record in MLDv2. This record means that no traffic from this group will be received, regardless of the source.

- An MLDv1 group report: Equivalent to an IS_EX (empty) record in MLDv2. This record means that all traffic from this group will be received, regardless of the source.
- Source-list-change record: If the client wants to add or remove traffic sources from its membership report, the report can include an ALLOW record, which contains a list of new sources from which the client wishes to receive traffic. The report can also contain a BLOCK record, which lists current traffic sources from which the client wants to stop receiving traffic.

Support for MLD Snooping and Layer 3 IPv6 Multicast Routing Together on the Same Device

The RUCKUS device supports global Layer 2 IPv6 multicast traffic reduction (MLD snooping) and Layer 3 IPv6 multicast routing (PIM-Sparse) together on the same device in the full Layer 3 software image, as long as the Layer 2 feature configuration is at the VLAN level.

NOTE
MLD snooping and Layer 3 IPv6 multicast routing are not supported on the same VLAN.

For full details on MLD snooping resource limits, refer to Hardware and Software Resource Limits on page 61

IP-based Forwarding Implementation on ICX Devices

When an IPv6 multicast data packet is received, the packet destination IP address is matched with the IP address entries in the IPv6 multicast table. If a match is found, packets are sent to the ports associated with the IP address. If a match is not found, packets are flooded to the VLAN and copied to the CPU.

For two multicast traffic streams, Source_1 and Group1 (S1,G1) and Source_2 and Group2 (S2,G2), with the same or different source addresses, if the lowest 32 bits of the 128-bit IPv6 group address are the same, they would map to the same destination address.

Hardware Resources for MLD and PIMv6 SM Snooping

RUCKUS devices allocate or program FDB or MAC entries and application VLAN (vidx) to achieve multicast snooping in hardware. If a data packet does not match any of these resources, it might be sent to the CPU, which increases the CPU burden. This can happen if the device runs out of hardware resource, or is unable to install resources for a specific matching address due to hashing collision. The hardware hashes addresses into available entries, with some addresses hashed into the same entry. If the collision number in an entry is more than the hardware chain length, the resource cannot be installed.

MLD Snooping Configuration Notes and Feature Limitations

- Servers (traffic sources) are not required to send Multicast Listening Discovery (MLD) memberships.
- The default MLD version is V1, where the source address is not sensitive. In this version, (S1,G1) and (S2,G1) would be considered the same group as (*,G1).
- If MLDv2 is configured on any port of a VLAN, you can check the source information, but because MLD snooping is MAC-based, (S,G) switching is not feasible.
- Hardware resources are installed only when there is data traffic.
- You can configure the maximum number of groups and the multicast cache (mcache) number.
- The device supports static groups applying to specific ports. The device acts as a proxy to send MLD reports for the static groups when receiving queries.

- When there are two or more possible queriers, it is recommended to configure the IPv6 multicast age interval to 20 seconds more than the default calculated age interval on all switches enabled with MLD snooping. This prevents the aging of groups when the active querier fails.
- A user can configure static router ports, forcing all multicast traffic to be sent to these ports.
- RUCKUS devices support fast leave for MLDv1, which stops traffic immediately to any port that has received a leave message.
- RUCKUS devices support tracking and fast leave for MLDv2, which tracks all MLDv2 clients. If the only client on a port leaves, traffic is stopped immediately.
- An MLD device can be configured as a querier (active) or non-querier (passive). Queriers send queries. Non-queriers listen for queries and forward them to the entire VLAN.
- Every VLAN can be independently configured as a querier or a non-querier.
- A VLAN that has a connection to an IPv6 PIM-enabled port on another router should be configured as a non-querier. When multiple snooping devices connect together and there is no connection to IPv6 PIM ports, only one device should be configured as the querier. If multiple devices are configured as active, only one will continue to send queries after the devices have exchanged queries. Refer to MLD Snooping-enabled Queriers and Non-Queriers on page 60 for more information.
- An MLD device can be configured to rate-limit the forwarding of MLDv1 membership reports to queriers.
- Because an IPv6 link-local address as the source address when sending queries, a global address is not required.
- The MLD implementation allows snooping on some VLANs or on all VLANs. MLD can be enabled or disabled independently for each VLAN. In addition, individual ports of a VLAN can be configured as MLDv1 and MLDv2. In general, global configuration commands such as **ipv6 multicast...**. apply to all VLANs except those with a local **multicast...** configuration, which supersedes the global configuration. Configuring the version on a port or a VLAN only affects the device sent query version. If the lower version is configured, higher version reports cannot be processed. However, if the higher version is configured lower versions can also be processed.
- MLD snooping requires hardware resources. If the device has insufficient resources, the data stream without a resource is mirrored to the CPU in addition to being VLAN flooded, which can cause high CPU usage. To avoid this situation, RUCKUS recommends that you avoid enabling snooping globally unless necessary.
- To receive data traffic, MLD snooping requires clients to send membership reports. If a client does not send reports, you must configure a static group to force traffic to client ports.
- Multicast Router Discovery (MRD) messages are useful for determining which nodes attached to a switch have multicast routing enabled. This capability is useful in a Layer 2 bridge domain with snooping switches. By utilizing MRD messages, Layer 2 switches can determine where to send multicast source data and group membership messages. Multicast source data and group membership reports must be received by all multicast routers on a segment. Using the group membership protocol Query messages to discover multicast routers is insufficient due to query suppression.

Because RUCKUS does not support MRD, this can lead to stream loss when non-Querier router ports age out on the Querier after the initial Query election. To avoid such stream loss, configure a static router port on the querier on each interface that connects to a non-querier snooping device.

On the ICX devices, if MLDv2 is configured on any port of a VLAN, you can check the source information, but because MLD snooping is MAC-based, (S,G) switching is not feasible.

MLD/PIMv6 SM snooping over Multi-Chasis Trunking (MCT) is only supported on RUCKUSICX 7650 and ICX 7850 devices.

MLD Snooping-enabled Queriers and Non-Queriers

An MLD snooping-enabled device can be configured as a querier (active) or non-querier (passive). An MLD querier sends queries; a non-querier listens for MLD queries and forwards them to the entire VLAN. When multiple MLD snooping devices are connected together, and there is no connection to an IPv6 PIM-enabled port, one of the devices should be configured as a querier. If multiple devices are configured as queriers, after multiple devices exchange queries, then all devices except the winner (the device with the lowest address) stop sending queries. Although the system works when multiple devices are configured as queriers, RUCKUS recommends that only one device, preferably the one with the traffic source, is configured as the querier.

VLANs can also be independently configured as queriers or non-queriers. If a VLAN has a connection to an IPv6 PIM-enabled port on another router, the VLAN should be configured as a non-querier.

Because non-queriers always forward multicast data traffic and MLD messages to router ports which receive MLD queries or IPv6 PIM hellos, RUCKUS recommends that you configure the devices with the data traffic source (server) as queriers. If a server is attached to a non-querier, the non-querier always forwards traffic to the querier regardless of whether or not there are clients on the querier.

> **NOTE**
> In a topology with one or more connected devices, at least one device must be running PIM, or configured as active. Otherwise, no devices can send queries, and traffic cannot be forwarded to clients.

To configure the MLD mode (querier or non-querier) on an MLD snooping-enabled device, refer to Configuring the MLD Snooping Mode and Version Globally on page 62. To configure the MLD mode on a VLAN, refer to Configuring MLD Snooping Options for a VLAN on page 64.

MLD and VLAN Configuration

You can configure MLD snooping on some VLANs or all VLANs. Each VLAN can be independently enabled or disabled for MLD snooping, or can be configured with MLDv1 or MLDv2. In general, the IPv6 MLD snooping commands apply globally to all VLANs except those configured with VLAN-specific MLD snooping commands. VLAN-specific MLD snooping commands supersede global IPv6 MLD snooping commands.

MLDv1 with MLDv2

MLD snooping can be configured as MLDv1 or MLDv2 on individual ports on a VLAN. An interface or router sends queries and reports that include the MLD version with which it has been configured. The version configuration applies only to the sending of queries. If the lower version is configured, higher version reports cannot be processed. However, if the higher version is configured lower versions can also be processed.

> **NOTE**
> To avoid version deadlock, when an interface receives a report with a lower version than that for which it has been configured, the interface does not automatically downgrade the running MLD version.

MLD Snooping Configuration

Configuring Multicast Listening Discovery (MLD) snooping on an IPv6 device consists of the following global and VLAN-specific tasks.

MLD snooping global tasks:

- Configuring hardware and software resource limits
- Disabling transmission and receipt of MLD packets on a port
- Configuring the MLD mode: active or passive (must be enabled for MLD snooping)
- Modifying the age interval
- Modifying the interval for query messages (active MLD mode only)

- Specifying the global MLD version
- Enabling and disabling report control (rate limiting)
- Modifying the leave wait time
- Modifying the mcache age interval
- Disabling error and warning messages

MLD snooping VLAN-specific tasks:

- Configuring the MLD mode for the VLAN: active or passive
- Enabling or disabling MLD snooping for the VLAN
- Configuring the MLD version for the VLAN
- Configuring the MLD version for individual ports
- Configuring static groups
- Configuring static router ports
- Disabling proxy activity for a static group
- Enabling client tracking and the fast leave feature for MLDv2
- Configuring fast leave for MLDv1
- Configuring fast-convergence

Hardware and Software Resource Limits

The system supports up to 8,000 hardware-switched multicast streams. The following table shows the MLD snooping resource limits.

TABLE 5 MLD Snooping Limits

Platform	Groups		Mcache	
	Default	Maximum	Default	Maximum
RUCKUS ICX 7150	1024	3072	512	1024
RUCKUS ICX 7250	4096	8192	512	4096
RUCKUS ICX 7450	4096	8192	512	4096
RUCKUS ICX 7650	8192	8192	512	8192

NOTE
For ICX 7550 and ICX 7850 devices, MLD snooping cache entries and MLD snooping group addresses values are used from the forwarding profile. Refer to the **forwarding-profile** command in the *RUCKUS FastIron Command Reference Guide* and the "Configuration Fundamentals" chapter in the *RUCKUS FastIron Management Configuration Guide* for more information.

Configuring the Hardware and Software Resource Limits

The following task defines the maximum number of MLD snooping mc mcache entries and the maximum number of multicast group addresses supported.

1. Use the **configure terminal** command to enter global configuration mode.

```
device# configure terminal
```

2. Use the **system-max mld-snoop-mcache** command, specifying a value, to define the maximum number of MLD snooping mcache entries.

```
device(config)# system-max mld-snoop-mcache 8000
```

3. Use the **system-max mld-snoop-group-addr** command, specifying a value, to define the maximum number of multicast group addresses supported.

```
device(config)# system-max mld-snoop-group-addr 4000
```

The following example sets the maximum number of MLD snooping mcache entries to 8000 and the maximum number of multicast group addresses supported to 4000.

```
device# configure terminal
device(config)# system-max mld-snoop-mcache 8000
device(config)# system-max mld-snoop-group-addr 4000
```

NOTE
For ICX 7550 and ICX 7850 devices, MLD snooping mcache entries and the number of multicast group addresses values are used from the forwarding profile. Refer to the **forwarding-profile** command in the *RUCKUS FastIron Command Reference* and the *Configuration Fundamentals* chapter in the *RUCKUS FastIron Management Configuration Guide* for more information.

MLD Snooping Modes

You can configure a RUCKUS device for either active or passive (default) MLD mode. If you specify an MLD mode for a VLAN, the MLD mode overrides the global setting.

- Active: In active MLD mode, a device actively sends out MLD queries to identify IPv6 multicast groups on the network, and makes entries in the MLD table based on the group membership reports it receives from the network.
- Passive: In passive MLD mode, the device forwards reports to the router ports which receive queries. MLD snooping in passive mode does not send queries, but does forward queries to the entire VLAN.

To globally set the MLD mode to active, enter the **ipv6 multicast active** command. Refer to the Configuring the MLD Snooping Mode and Version Globally on page 62 task.

NOTE
The **ipv6 mld-snooping** command is replaced by the **ipv6 multicast** command; the **mld-snooping** command is replaced by the **multicast6** command.

Configuring the MLD Snooping Mode and Version Globally

MLD mode and version can be configured on RUCKUS devices in global configuration mode.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Globally set the MLD mode to active.

```
device(config)# ipv6 multicast active
```

If you do not specify the **active** keyword, the default mode is passive.

3. Globally set the MLD version to version 2.

```
device(config)# ipv6 multicast version 2
```

If you do not specify an MLD version, the default version is MLDv1.

The following example globally sets the device to run IPv6 multicast version 2 in active mode.

```
device# configure terminal
device(config)# ipv6 multicast active
device(config)# ipv6 multicast version 2
```

Configuring MLD Snooping Global Options

A number of MLD snooping options can be configured on Ruckus devices in global configuration mode.

You must configure the MLD mode and version globally before entering these options. Refer to Configuring the MLD Snooping Mode and Version Globally on page 62.

The following option configurations are outlined in the following steps:

- Modify the age interval for group membership entries: When the device receives a group membership report, it makes an entry for that group in the MLD group table. The age interval specifies how long the entry can remain in the table before the device receives another group membership report.
- Modify the query interval (only for MLD active mode): If IP multicast traffic reduction is set to active mode, you can modify the query interval to specify how often the device sends general queries.
- Configure report control (MLD v1 only): A device in passive mode forwards reports and leave messages from clients to the upstream router ports that are receiving queries. You can configure a report control option to rate-limit report forwarding within the same group to no more than once every 10 seconds. This rate-limiting does not apply to the first report answering a group-specific query.
- Modify the wait time before stopping traffic when receiving a leave message: You can define the wait time before stopping traffic to a port when a leave message is received. The device sends group-specific queries once per second to ask if any client in the same port still needs this group. Due to internal timer granularity, the actual wait time is between n and (n+1) seconds (n is the configured value).
- Modify the multicast cache age time: You can set the time for an mcache to age out when it does not receive traffic. The traffic is hardware switched. Two seconds before aging out an mcache, the device mirrors a packet of this mcache to CPU to reset the age. If no data traffic arrives within two seconds, this mcache is deleted. Be aware when using ICX devices and MAC-based MLD snooping is supported, more than one mcache can be mapped to the same destination MAC address. As a result, when an mcache entry is deleted, the MAC entry may not be deleted. If you configure a lower value, the resource consumed by idle streams is quickly removed, but packets are mirrored to the CPU more frequently. Configure a higher value only when data streams are arriving consistently.
- Enable or disable error or warning messages: The device prints error or warning messages when it runs out of software resources or when it receives packets with the wrong checksum or groups. These messages are rate-limited. You can turn off these messages.

The following task steps can be configured in any order and are all optional. Commands that are limited to a specific MLD mode or version are identified in the task step.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Globally set the MLD snooping mode to active.

   ```
   device(config)# ipv6 multicast activate
   ```

3. Modify the age interval, in seconds, for group membership entries.

   ```
   device(config)# ipv6 multicast age-interval 280
   ```

   When multiple devices are connected together, all devices must have the same age interval configured, which must be at least twice the length of the query interval, so that missing one report will not stop traffic. Non-querier age intervals must be the same as the age interval of the querier.

4. Modify the query interval, in seconds (only for MLD active mode).

```
device(config)# ipv6 multicast query-interval 120
```

   When multiple queriers connect together, they must all be configured with the same query interval.

5. Configure report control (MLDv1 only).

```
device(config)# ipv6 multicast report-control
```

   MLDv1 membership reports of the same group from different clients are considered to be the same and are rate-limited. This alleviates the report storm caused by multiple clients answering the upstream router query.

   NOTE
   This feature applies to MLDv1 only. The leave messages are not rate limited.

6. Modify the wait time before stopping traffic when receiving a leave message.

```
device(config)# ipv6 multicast leave-wait-time 5
```

7. Modify the multicast cache age time.

```
device(config)# ipv6 multicast mcache-age 150
```

   NOTE
   The mcache age value configured may not expire accurately. You may notice a delay of 0 to 60 seconds.

8. Enable or disable error or warning messages.

```
device(config)# ipv6 multicast verbose-off
```

The following example configures the IPv6 multicast options.

```
device# configure terminal
device(config)# ipv6 multicast active
device(config)# ipv6 multicast age-interval 280
device(config)# ipv6 multicast query-interval 120
device(config)# ipv6 multicast max-response-time 5
device(config)# ipv6 multicast report-control
device(config)# ipv6 multicast leave-wait-time 5
device(config)# ipv6 multicast mcache-age 150
device(config)# ipv6 multicast verbose-off
```

Configuring MLD Snooping Options for a VLAN

MLD snooping mode and version can be configured on RUCKUS devices for a specific VLAN.

Even if the MLD mode and version have been configured globally, specifying the mode and version for a VLAN overrides the global settings. Other MLD Snooping options are described in the task steps and are optional.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Create a VLAN.

```
device(config)# vlan 22
```

3. Set the MLD mode to active for a VLAN.

```
device(config-vlan-22)# multicast6 active
```

   If you do not specify the **active** keyword, the default mode is passive. If you do not specify a mode for the VLAN, the globally-configured mode is used.

4. Set the MLD version for VLAN 22 to version 2.

```
device(config-vlan-22)# multicast6 version 2
```

   If no MLD version is specified, the globally-configured MLD version is used. If an MLD version is specified for individual ports, those ports use that version, instead of the VLAN version.

5. You can specify the MLD version for individual ports in a VLAN. You can specify a list of ports, a range of ports, or a combination of lists and ranges.

```
device(config-vlan-22)# multicast6 port-version 2 ethernet 1/2/4 to 1/2/6
```

   In this example, the ports 1/2/4, 1/2/5, and 1/2/6 are configured to use MLDv2. The other ports either use the MLD version specified with the **multicast6 version** command, or the globally-configured MLD version.

6. You can configure static groups to specific ports using the **multicast6 static-group** command.

```
device(config-vlan-22)# multicast6 static-group 224.1.1.1 count 2 ethernet 1/1/3 ethernet 1/1/5 to
1/1/7
```

   A snooping-enabled VLAN cannot forward multicast traffic to ports that do not receive MLD membership reports. If clients cannot receive multicast traffic, you can configure a static group which applies to specific ports. The static group allows packets to be forwarded to the static group ports even though they have no client membership reports.

7. A device with statically configured groups acts as a proxy and sends membership reports for its static groups when it receives general or group-specific queries. When a static group configuration is removed, the group is immediately deleted from the active group table. However, the device does not send leave messages to the querier. The querier should age out the group. The proxy activity can be disabled using the **multicast6 proxy-off** command.

```
device(config-vlan-22)# multicast6 proxy-off
```

   The proxy activity is enabled by default.

8. To configure static router ports, enter the **multicast6 router-port** command.

```
device(config-vlan-22)# multicast6 router-port ethernet 1/2/1 to 1/2/3 ethernet 1/2/8
```

   All multicast control and data packets are forwarded to router ports that receive queries. Although router ports are learned, you can configure static router ports to force multicast traffic to specific ports, even though these ports never receive queries.

The following example configures VLAN 22 to run IPv6 multicast version 2 in active mode with some ports configured specifically to use MLD version 2 with a static group that applies to specific ports, the static group proxy activity is disabled, and static router ports are configured.

```
device# configure terminal
device(config)# vlan 22
device(config-vlan-22)# multicast6 active
device(config-vlan-22)# multicast6 version 2
device(config-vlan-22)# multicast6 port-version 2 ethernet 1/2/4 to 1/2/6
device(config-vlan-22)# multicast6 static-group 224.1.1.1 count 2 ethernet 1/1/3 ethernet 1/1/5 to 1/1/7
device(config-vlan-22)# multicast6 proxy-off
device(config-vlan-22)# multicast6 router-port ethernet 1/2/1 to 1/2/3 ethernet 1/2/8
```

Disabling MLD Snooping for the VLAN

When MLD snooping is enabled globally, you can disable it for a specific VLAN. In the following configuration example, MLD snooping is disabled for VLAN 22. This setting overrides the global setting for VLAN 22.

```
device(config)# vlan 22
device(config-vlan-22)# multicast6 disable-mld-snoop
```

Configuring the Layer 2 Mode IPv6 Querier Address

You can configure an IPv6 querier address for every VLAN. This functionality is available only for multicast snooping.

In releases prior to FastIron 08.0.50, you could not specifically configure a querier address per VLAN. Instead, in an IPv6 environment, a system MAC-dependent link local address was used as a querier address.

Starting with FastIron 08.0.50, you can configure a Layer 2 mode querier IP address. You can now plan an elected querier location suitable for your network and use the most suitable querier location. This address can be configured regardless of whether the current multicast snooping mode is set to active or passive. Once the mode changes to active, the configured IP address is used as a querier address. You can configure a different querier IP address for every VLAN.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Enter VLAN configuration mode.

   ```
   device(config)# vlan 100
   ```

3. Enter the **multicast6 querier-address** command followed by the IPv6 address.

   ```
   device(config-vlan-100)# multicast6 querier-address FE80::44
   ```

The following example configures an IPv6 address as the multicast querier address for the VLAN.

```
device# configure terminal
device(config)# vlan 100
device(config-vlan-100)# multicast6 querier-address FE80::44
```

Enabling MLDv2 Membership Tracking and Fast Leave for the VLAN

MLDv2 provides membership tracking and fast leave services to clients. In MLDv1, only one client per interface must respond to a router queries; leaving some clients invisible to the router, which makes it impossible for the device to track the membership of all clients in a group. In addition, when a client leaves the group, the device sends group-specific queries to the interface to see if other clients on that interface need the data stream of the client who is leaving. If no client responds, the device waits a few seconds before stopping the traffic.

MLDv2 requires that every client respond to queries, allowing the device to track every client. When the tracking feature is enabled, the device immediately stops forwarding traffic to the interface if an MLDv2 client sends a leave message, and there is no other client. This feature requires the entire VLAN to be configured for MLDv2 and have no MLDv1 clients. If a client does not send a report during the specified group membership time (the default is 140 seconds), that client is removed from the tracking list.

Every group on a physical port keeps its own tracking record. However, it can track group membership only; it cannot track by (source, group). For example, Client A and Client B belong to group1 but each is receiving traffic from different sources. Client A receives a traffic stream from (source_1, group1) and Client B receives a traffic stream from (source_2, group1). The device waits for the configured *leave-wait-time* before it stops the traffic because the two clients are in the same group. If the clients are in different groups, the waiting period is ignored and traffic is stopped immediately.

The following configuration example enables tracking and fast leave for VLAN 22.

```
device# configure terminal
device(config)# vlan 22
device(config-vlan-22)# multicast6 tracking
```

NOTE
The membership tracking feature is supported for MLDv2 only.

If a port or client is not configured for MLDv2, the **multicast6 tracking** command is ignored.

Configuring Fast Leave for MLDv1

When a device receives an MLDv1 leave message, it sends out multiple group-specific queries. If no other client replies within the waiting period, the device stops forwarding traffic to this port. Configuring fast-leave-v1 allows the device to stop forwarding traffic to a port immediately upon receiving a leave message. The device does not send group-specific queries. When fast-leave-v1 is configured on a VLAN, make sure you do not have multiple clients on any port that is part of the VLAN. In a scenario where two devices connect, the querier device should not be configured for fast-leave-v1, because the port might have multiple clients through the non-querier.

The following configuration example configures fast leave for MLDv1, use the following commands.

```
device(config)# vlan 22
device(config-vlan-22)# multicast6 fast-leave-v1
```

Enabling Fast Convergence

In addition to periodically sending general queries, an active (querier) device sends out general queries when it detects a new port. However, since it does not recognize the other device port-up event, the multicast traffic might still use the query-interval time to resume after a topology change. Configuring fast convergence allows the device to listen to topology change events in Layer 2 protocols, such as spanning tree, and send general queries to shorten the convergence time.

If the Layer 2 protocol is unable to detect a topology change, the fast convergence feature may not work. For example, if the direct connection between two devices switches from one interface to another, the rapid spanning tree protocol (802.1w) considers this an optimization action, rather than a topology change. In this case, other devices will not receive topology change notifications and will be unable to send queries to speed up the convergence. The original spanning tree protocol does not recognize optimization actions, and fast convergence works in all cases.

The following configuration example enables fast convergence.

```
device(config)# vlan 70
device(config-vlan-70)# multicast6 fast-convergence
```

Enabling the Flooding of Unregistered IPv6 Multicast Frames Globally

The following task enables the flooding of initial packets for unregistered IPv6 multicast groups until hardware entries are programmed. Once the hardware entries are programmed, packets are dropped for unregistered multicast groups. .

1. **NOTE**
   If SDVoE is enabled for a VLAN, it must be disabled before attemting to enable the flooding of unregistered IPv4 Multicast frames.

   Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Enable the flooding of unregistered IPv6 Frames.

```
device(config)# ipv6 multicast flood-unregistered
```

The following example enables the flooding of unregistered IPv6 mulitcast frames globally.

```
device# configure terminal
device(config)# ipv6 multicast flood-unregistered
```

The following example disables the flooding of unregistered IPv6 mulitcast frames globally.

```
device# configure terminal
device(config)# no ipv6 multicast flood-unregistered
```

Displaying MLD Snooping Information

You can use various **show** commands to view information about MLD snooping.

Use one of the following commands to view MLD snooping information. The commands do not need to be entered in the specified order. Using these commands is optional and they can be entered in any order. For more information on the full list of **show ipv6 multicast** commands, refer to the *RUCKUS FastIron Command Reference Guide}*.

1. Enter the **show ipv6 multicast traffic** command to display status information about MLD snooping traffic.

```
device> show ipv6 multicast traffic

MLD snooping: Total Recv: 32208, Xmit: 166
Q: query, Qry: general Q, G-Qry: group Q, GSQry: group-source Q, Mbr: member
Recv    QryV1    QryV2    G-Qry    GSQry    MbrV1    MbrV2     Leave
VL1         0        0        0        0    31744      208       256
VL70        0        0        0        0        0        0         0
Recv     IsIN     IsEX     ToIN     ToEX    ALLOW    BLOCK   Pkt-Err
VL1      1473    31784        0        1        1        7         0
VL70        0        0        0        0        0        0         0
Send    QryV1    QryV2    G-Qry    GSQry    MbrV1    MbrV2
VL1         0        0      166        0        0        0
VL70        0        0        0        0        0        0
```

2. Enter the **show ipv6 multicast vlan** command and specify a VLAN to display MLD snooping information for the specified VLAN.

```
device> show ipv6 multicast vlan 11

Version=1, Intervals: Query=300, Group Age=620, Max Resp=10, Other Qr=605,
Leave Wait=2, Robustness=2
    router ports: 1/36(120) 2001:DB8::2e0:52ff:fe00:9900,
  My Query address: fe80::ce4e:24ff:fe6f:980 (link-local)
  1/26 has 2 grp, non-QR (passive), cfg V1
  1/26 has 2 grp, non-QR (passive), cfg V1
    group: ff10:1234::5679, life = 100
    group: ff10:1234::5678, life = 100
  1/35 has 0 grp, non-QR (QR=2001:DB8::2e0:52ff:fe00:9900, age=20), dft V2 trunk
```

3. Enter the **show ipv6 multicast error** command to display information about possible MLD snooping errors.

```
device> show ipv6 multicast  error

MLD Snoop Resource infromation
Packet Drop:-
   DMAC Error:          0
snoop SW processed pkt: 39, up-time 23:49:40
```

4. Enter the **show default values**command to display default, maximum, current, and configured values for system maximum parameters. The following output example does not show complete output; it shows only MLD snooping group values.

```
device> show default values

System Parameters     Default    Maximum    Current    Configured
MLD-snoop-group-addr  4096       8192       5000       5000
```

5. Enter the **show ipv6 multicast group** command to display information about MLD snooping groups.

```
device> show ipv6 multicast group

p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL1 : 263 grp, 263 grp-port, tracking_enabled
      group                                  p-port ST QR life mode source
1     ff0e::ef00:a0e3                        1/1/7  N  Y  120  EX   0
2     ff01::1:f123:f567                      1/1/9  N  Y       IN   1
```

In this example, an MLD 1 group is in EXCLUDE mode with a source of 0. The group excludes traffic from the 0 (zero) source list, which means that all traffic sources are included.

6. Enter the **show ipv6 multicast group** command with the **detail** keyword, and specify a group address, to display detailed information about an MLD snooping group.

```
device> show ipv6 multicast group ff0e::ef00:a096 detail

Display group ff0e::ef00:a096 in all interfaces in details.
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL1 : 1 grp, 1 grp-port, tracking_enabled
      group                                  p-port ST QR life mode source
1     ff0e::ef00:a096                        1/1/7  N  Y  100  EX   0
    group: ff0e::ef00:a096, EX, permit 0 (source, life):
      life=100, deny 0:
```

7. Enter the **show ipv6 multicast group**command with the **tracking** keyword and specify a group address, to display the list of clients for a particular group if tracking and fast leave are enabled.

```
device> show ipv6 multicast group ff0e::ef00:a096 tracking

Display group ff0e::ef00:a096 in all interfaces with tracking enabled.
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL1 : 1 grp, 1 grp-port, tracking_enabled
      group                                  p-port ST QR life mode source
1     ff0e::ef00:a096                        1/1/7  N  Y  80   EX   0
    receive reports from 1 clients: (age)
      (2001:DB8::1011:1213:1415 60)
```

8. The MLD snooping mcache contains multicast forwarding information for VLANs. Enter the **show ipv6 multicast mcache** command to display information in the multicast forwarding mcache.

```
device> show ipv6 multicast mcache
(Example:
(S G) (MAC ADDR) cnt=: SRC and GRP IPv4/IPv6 address,
Multicast Mac address, cnt is number of SW processed packets
OIF: 1/1/22 TR(1/1/32,1/1/33), TR is trunk, 1/1/32 primary, 1/1/33 output
IPv6 Multicast Forwarding Mode: IP
Total Multicast Cache: 2
vlan 300, 2 caches.
1 (2001:300::2 ff1e::3337) (3333.0000.3337) cnt=135
OIF: tag lg1
age=16s up-time=143s, change=143s ipmc=360 (ref-cnt=1)
2 (2001:300::2 ff1e::3333) (3333.0000.3333) cnt=129
OIF: tag lg1
age=28s up-time=143s, change=143s ipmc=360 (ref-cnt=1)
```

9. Enter the **show ipv6 multicast resource** command to display information about the software resources used.

```
device> show ipv6 multicast resource

                      alloc in-use  avail get-fail    limit  get-mem  size init
mld group               512      9    503        0    32000      272    28  256
mld phy port           1024     16   1008        0   200000      279    21 1024
snoop group hash        512      9    503        0    59392      272    20  256
.... Entries deleted
total pool memory 194432 bytes
has total 1 forwarding hash
Available ipmc: 4061
```

Verifying Multicast Mcache for Multicast Groups which Share Same Multicast MAC Address (MLD snooping)

If there are two multicast groups (ff1e::10:1:1 and ff1e::11:1:1) which map to the same multicast MAC address, the **show ipv6 multicast mcache** command output for one of the groups will be empty.

Complete the following steps to check whether active mcache is present for that group.

1. Get the mapped multicast MAC address for the interested multicast group (use 32 as bit value for exact match).

```
device#show ipv6 multicast group ff1e::11:1:1 match-last-bits 32
Display groups sharing same mac address 3333.0001.0001 with group ff1e::11:1:1  for all vlans on all
ports.
p-:physical, ST:static, QR:querier, EX:exclude, IN:include, Y:yes, N:no
VL4089 : 15 grp, 25 grp-port
      group                                   p-port     ST QR life  mode source
1     ff1e::10:1:1                            lg1        N  Y  180   EX   0
2     ff1e::10:1:1                            e1/1/8     N  Y  180   EX   0
3     ff1e::11:1:1                            lg1        N  Y  180   EX   0
4     ff1e::11:1:1                            e1/1/8     N  Y  180   EX   1
```

2. Using the multicast MAC address (3333.0001.0001), get the multicast group address with which the mcache is programmed.

```
device#show ipv6 multicast mac-mcache 3333.0001.0001
       Example:
               MAC = xxxx.xxxx.xxxx Vlan = #, l2mc = # , ref_cnt = #
               IP Multicast Group :
               Mcast Group, Src Addr
               OIF: 1/1/22 TR(1/1/32,1/1/33), TR is trunk, 1/1/32 primary, 1/1/33 output
               Total Multicast Mac Cache: 11
               vlan 4089, 11 caches
               1      MAC=3333.0001.0001, vlan=4089, l2mc=259, ref_cnt=1
                       IP Multicast Group
                                (* ff1e::10:1:1)
                        OIF:  1/1/8 lg1
```

3. Verify whether the multicast mcache is present for the multicast group ff1e::10:1:1.

```
device#show ipv6 multicast mcache ff1e::10:1:1
Example:
     (S G) (MAC ADDR) cnt=: SRC and GRP IPv4/IPv6 address,
    Multicast Mac address, cnt is number of SW processed packets
    OIF: 1/1/22 TR(1/1/32,1/1/33), TR is trunk, 1/1/32 primary, 1/1/33 output
IPv6 Multicast Forwarding Mode: MAC
Total Multicast Cache: 11
vlan 4089, 11 caches.
1     (* ff1e::10:1:1)  (3333.0001.0001) cnt=19
      OIF: tag e1/1/8 tag lg1
      age=4s up-time=63s, change=63s l2mc=259 (ref-cnt=1)
```

Clearing MLD Counters and Mcache on All VLANs

The **clear** commands for MLD snooping should only be used in troubleshooting situations or when recovering from error conditions.

The following steps are optional and can be used in any order.

1. To clear MLD snooping error and traffic counters on all VLANs, enter the **clear ipv6 multicast counters** command.

```
device# clear  ipv6 multicast counters
```

2. To clear the mcache on all VLANs, enter the **clear ipv6 multicast mcache** command.

```
device# clear ipv6 multicast mcache
```

Disabling the Flooding of Unregistered IPv6 Multicast Frames in an MLD-Snooping-Enabled VLAN

Unregistered IPv6 multicast frames can be disabled in an MLD-snooping-enabled VLAN. The following task disables the flooding of unregistered IPv6 multicast frames in an MLD-snooping-enabled VLAN.

NOTE
Disabling the flooding of unregistered IPv6 multicast frames in an MLD-snooping-enabled VLAN is supported on RUCKUSICX 7550, ICX 7650, and ICX 7850 platforms.

1. Use the **configure terminal** command to enter global configuration mode.

```
device# configure terminal
```

2. Use the **ipv6 multicast disable-flooding** command to disable the flooding of unregistered IPv6 multicast frames.

```
device# ipv6 multicast disable-flooding
```

The following example disables the flooding of unregistered IPv6 multicast frames in an MLD-snooping-enabled VLAN.

```
device# configure terminal
device(config)# ipv6 multicast disable-flooding
```

PIM6 SM Traffic Snooping Overview

When multiple PIM sparse routers connect through a snooping-enabled device, the RUCKUS device always forwards multicast traffic to these routers. For example, PIM sparse routers R1, R2, and R3 connect through a device. Assume R2 needs traffic, and R1 sends it to the device, which forwards it to both R2 and R3, even though R3 does not need it. A PIM6 SM snooping-enabled device listens to join and prune messages exchanged by PIM sparse routers, and stops traffic to the router that sends prune messages. This allows the device to forward the data stream to R2 only.

PIM6 SM traffic snooping requires MLD snooping to be enabled on the device. MLD snooping configures the device to listen for MLD messages. PIM6 SM traffic snooping provides a finer level of multicast traffic control by configuring the device to listen specifically for PIM6 SM join and prune messages sent from one PIM6 SM router to another through the device.

Application Examples of PIM6 SM Traffic Snooping

The following figure shows an example application of the PIM6 SM traffic snooping feature. In this example, a device is connected through an IP router to a PIM6 SM group source that is sending traffic for two PIM6 SM groups. The device also is connected to a receiver for each of the groups.

When PIM6 SM traffic snooping is enabled, the device starts listening for PIM6 SM join and prune messages and MLD group membership reports. Once the device receives a join message or group membership report for a group, the device forwards subsequent traffic for that group only on the ports from which the join messages or MLD reports were received.

In this example, the router connected to the receiver for group ff1e::1:2 sends a join message toward the group source. Because PIM6 SM traffic snooping is enabled on the device, the device examines the join message to learn the group ID, then makes a forwarding entry for the group ID and the port connected to the receiver router. The next time the device receives traffic for ff1e::1:2 from the group source, the device forwards the traffic only on port 1/5/1, because that is the only port connected to a receiver for the group.

Notice that the receiver for group ff1e::3:4 is directly connected to the device. As a result, the device does not see a join message on behalf of the client. However, because MLD snooping also is enabled, the device uses the MLD group membership report from the client to select the port for forwarding traffic to group ff1e::3:4 receivers.

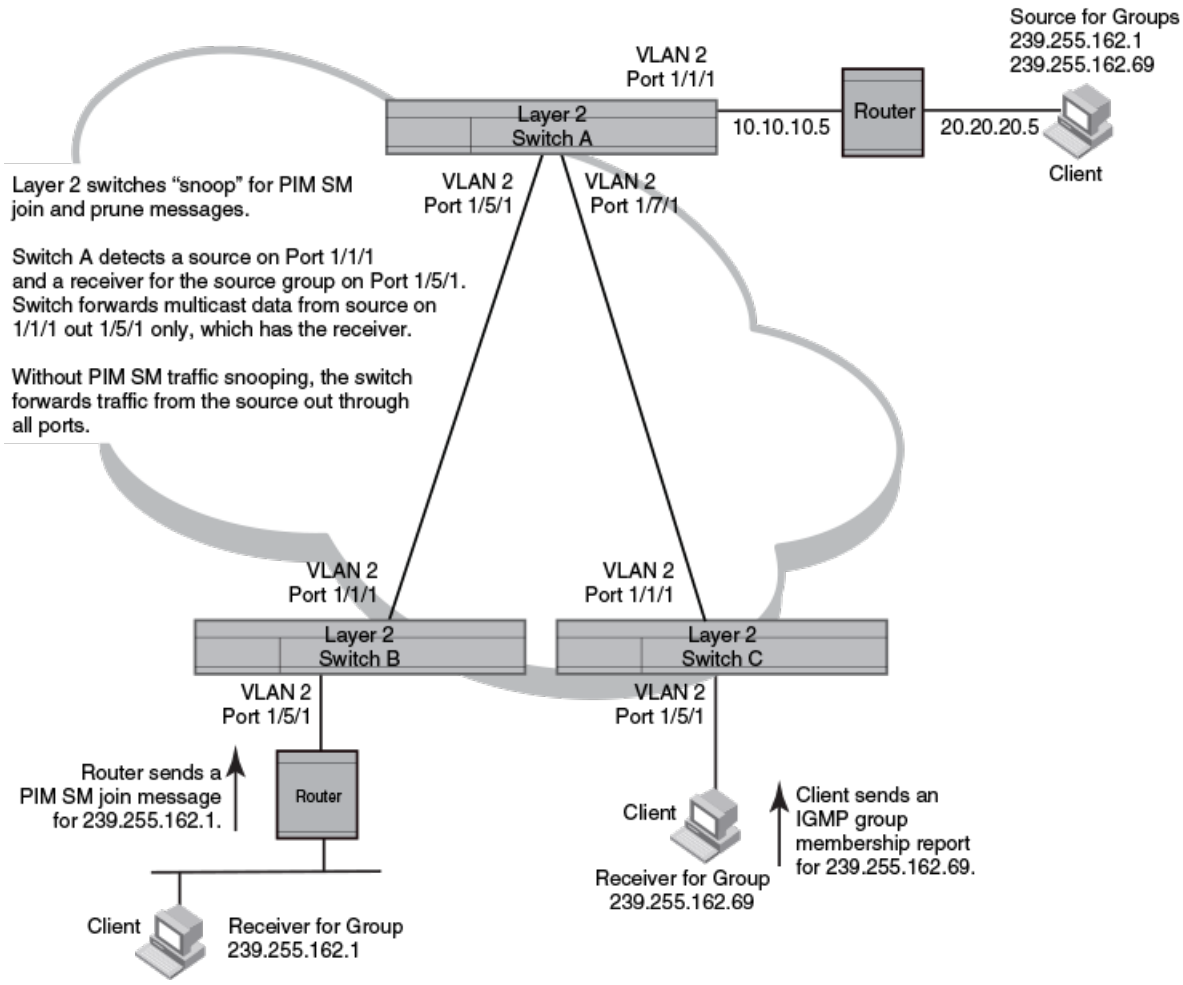
The MLD snooping feature and the PIM6 SM traffic snooping feature together build a list of groups and forwarding ports for the VLAN. The list includes PIM6 SM groups learned through join messages as well as MAC addresses learned through MLD group membership reports. In this case, even though the device never sees a join message for the receiver for group ff1e::3:4, the device nonetheless learns about the receiver and forwards group traffic to the receiver.

The device stops forwarding IP multicast traffic on a port for a group if the port receives a prune message for the group.

Notice that the ports connected to the source and the receivers are all in the same port-based VLAN on the device. This is required for the PIM6 SM snooping feature. The devices on the edge of the global Ethernet cloud are configured for MLD snooping and PIM6 SM traffic snooping. Although this application uses multiple devices, the feature has the same requirements and works the same way as it does on a single device.

NOTE
This example assumes that the devices are actually RUCKUS devices running Layer 2 switch software.

FIGURE 7 PIM6 SM Traffic Reduction in Global Ethernet Environment



The devices on the edge of the global Ethernet cloud are configured for MLD snooping and PIM6 SM traffic snooping. Although this application uses multiple devices, the feature has the same requirements and works the same way as it does on a single device.

Configuration Notes and Limitations for PIM6 SM Snooping

- PIM6 SM snooping applies only to PIM6 SM.
- PIM6 SM traffic snooping is supported for both switch and router images.
- MLD snooping must be enabled on the device that will be running PIM6 SM snooping. The PIM6 SM traffic snooping feature requires MLD snooping.
- PIMv6 snooping is not supported on default VLANs on router images.

  NOTE
  Use the passive mode of MLD snooping instead of the active mode. The passive mode assumes that a router is sending group membership queries as well as join and prune messages on behalf of receivers. The active mode configures the device to send group membership queries.

- All the device ports connected to the source and receivers or routers must be in the same port-based VLAN.

- The PIM6 SM snooping feature assumes that the group source and the device are in different subnets and communicate through a router. The source must be in a different IP subnet than the receivers. A PIM6 SM router sends PIM join and prune messages on behalf of a multicast group receiver only when the router and the source are in different subnet. When the receiver and source are in the same subnet, they do not need the router in order to find one another. They find one another directly within the subnet.

The device forwards all IP multicast traffic by default. Once you enable MLD snooping and PIM6 SM traffic snooping, the device initially blocks all PIM6 SM traffic instead of forwarding it. The device forwards PIM6 SM traffic to a receiver only when the device receives a join message from the receiver. Consequently, if the source and the downstream router are in the same subnet, and PIM6 SM traffic snooping is enabled, the device blocks the PIM6 SM traffic and never starts forwarding the traffic. This is because the device never receives a join message from the downstream router for the group. The downstream router and group find each other without a join message because they are in the same subnet.

NOTE
If the "route-only" feature is enabled on a Layer 3 switch, PIM6 SM traffic snooping will not be supported.

PIM6 SM Snooping Configuration

Configuring PIM6 SM snooping on a RUCKUS device consists of the following global and VLAN-specific tasks.

Perform the following global PIM6 SM snooping tasks:

- Enabling PIM6 SM snooping
- Disabling PIM6 SM snooping

Perform the following VLAN-specific PIM6 SM snooping tasks:

- Enabling PIM6 SM snooping on a VLAN
- Disabling PIM6 SM snooping on a VLAN

Enabling PIM6 SM Snooping

Use IPv6 PIM-Sparse Mode (PIM6 SM) snooping only in topologies where multiple PIM sparse routers connect through a device. PIM6 SM snooping does not work on a PIM dense mode router which does not send join messages and traffic to PIM dense ports is stopped. A PIM6 SM snooping-enabled device displays a warning if it receives PIM dense join or prune messages.
The PIM6 SM traffic snooping feature assumes that the network has routers that are running PIM6 SM.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable MLD snooping passive globally.

```
device(config)# ipv6 multicast passive
```

   The device must be in passive mode before it can be configured for PIM SM snooping.

3. Enable PIM6 SM snooping globally.

```
device(config)# ipv6 pimsm-snooping
```

Disabling PIM6 SM Snooping Globally

If PIM6 SM snooping has been enabled, you can disable it globally. One scenario where PIM6 SM snooping does not work, is on a PIM6 dense mode router which does not send join messages. When disabling PIM6 SM, you may also want to disable IPv6 multicast traffic reduction.

1. Enter global configuration mode.

```
device# configure terminal
```

2. To disable PIM6 SM snooping, enter the **no ipv6 pimsm-snooping** command.

```
device(config)# no ipv6 pimsm-snooping
```

3. If you also want to disable IPv6 multicast traffic reduction, enter the **no ipv6 multicast** command.

```
device(config)# no ipv6 multicast
```

Enabling PIM6 SM Snooping on a VLAN

You can enable PIM6 SM snooping for a specific VLAN. This setting overrides the global setting.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Configure a VLAN.

```
device(config)# vlan 20
```

3. Add the ports that are connected to the device and host in the same port-based VLAN.

```
device(config-vlan-20)# untagged ethernet 1/1/5 ethernet 1/1/7 ethernet 1/1/11
```

4. Enable PIM6 SM snooping on the VLAN.

```
device(config-vlan-20)# multicast6 pimsm-snooping
```

The following example enables PIM6 SM snooping for VLAN 20 for the ethernet ports 1/1/5, 1/1/7, and 1/1/11.

```
device# configure terminal
device(config)# vlan 20
device(config-vlan-20)# untagged ethernet 1/1/5 ethernet 1/1/7 ethernet 1/1/11
device(config-vlan-20)# multicast6 pimsm-snooping
```

Disabling PIM6 SM Snooping on a VLAN

When PIM6 SM snooping is enabled globally, you can still disable it for a specific VLAN. For example, the following commands disable PIM6 SM snooping for VLAN 20. This setting overrides the global setting.

1. Enter global configuration mode.

```
device# configure terminal
```

2. To specify the VLAN for which PIM6 SM snooping is to be disabled.

```
device(config)# vlan 20
```

3. To disable PIM6 sparse mode snooping, enter the **multicast6 disable-pimsm-snoop** command.

```
device(config-vlan-20)# multicast6 disable-pimsm-snoop
```

Displaying PIM6 SM Snooping Information

To display information related to the PIM6 SM snooping outgoing interface (OIF) in the mcache, enter the **show ipv6 multicast pimsm-snooping** command.

```
device# show ipv6 multicast pimsm-snooping

Example: Port: 1/7/3 (ref_count=1)
         ref_count: no of entries in pimsm snoop cache added this oif)

vlan 503, has 1 caches.
1    (* 2:3) has 1 pim join ports out of 1 OIF
     1/1/4 (ref_count=2),
```

You can display PIM6 SM snooping information for VLANs. The **show ipv6 multicast pimsm-snooping** command can be entered at any level of the CLI.

```
device# show ipv6 multicast pimsm-snooping vlan 25

vlan 25, has 2 caches.
1    (0:11 1:3) has 2 pim join ports out of 2 OIF
     1/1/2 (age=30), 2/1/3 (age=30),
     1/1/2 has 1 src: 15::11(30),
     2/1/3 has 1 src: 15::11(30),
2    (0:16 1:3) has 2 pim join ports out of 2 OIF
     2/1/3 (age=90), 1/1/2 (age=10),
     1/1/2 has 1 src: 15::16(10),
```

Refer to the *RUCKUS FastIron Command Reference* for more information on PIM SM commands.

IPv4 Multicast Protocols

Overview of IP Multicasting

Multicast protocols allow a group or channel to be accessed over different networks by multiple stations (clients) for the receipt and transmission of multicast data.

Distribution of stock quotes, video transmissions such as news services and remote classrooms, and video conferencing are all examples of applications that use multicast routing.

RUCKUS devices support the Protocol-Independent Multicast (PIM) protocol, along with the Internet Group Membership Protocol (IGMP).

PIM is a broadcast and pruning multicast protocol that delivers IP multicast datagrams. This protocol employs reverse path lookup check and pruning to allow source-specific multicast delivery trees to reach all group members. PIM builds a different multicast tree for each source and destination host group.

Security Enhancement for IGMP

A security enhancement was made to IGMPv2 to comply with the following recommendation of RFC 2236: “Ignore the Report if you cannot identify the source address of the packet as belonging to a subnet assigned to the interface on which the packet was received.”

> **NOTE**
> When used in applications such as IP-TV (or any multicast application in general), the administrator should ensure that the set-top box (or multicast client) is configured on the same subnet as the virtual Ethernet interface configured on the device. This is typically the case, but is emphasized here to ensure correct operation. Without this configuration, IGMP messages received by the device are ignored, which causes an interruption in any multicast traffic directed towards the set-top box (multicast client).

Multicast Terms

The following terms are commonly used in discussing multicast-capable devices. These terms are used throughout this chapter:

Node: A device.

Root Node: The node that initiates the tree building process. It is also the device that sends the multicast packets down the multicast delivery tree.

Upstream: The direction from which a device receives multicast data packets. An upstream device is a node that sends multicast packets.

Downstream: The direction to which a device forwards multicast data packets. A downstream device is a node that receives multicast packets from upstream transmissions.

Group Presence: A multicast group has been learned from one of the directly connected interfaces. Members of the multicast group are present on the device.

Intermediate nodes: Devices that are in the path between source devices and leaf devices.

Leaf nodes: Devices that do not have any downstream devices.

Multicast Tree: A unique tree is built for each source group (S,G) pair. A multicast tree is comprised of a root node and one or more nodes that are leaf or intermediate nodes.

Support for Multicast Multi-VRF

PIM sparse mode (PIM-SM) and PIM dense mode (PIM-DM) are supported by the Multicast Multi-VRF feature on RUCKUS devices.

The procedure for configuring PIM within a VRF instance is described in the following sections:

- Enabling PIM Sparse on page 99
- Enabling PIM Sparse on a Specific VRF on page 100

Changes to system-max Commands

Several changes have been made to the **system-max** commands in support of Multicast Multi-VRF. The **system-max pim-mcache** command has been deprecated and replaced by the **system-max pim-hw-mcache** command.

The following new runtime commands have been introduced:

- **max-mcache**: The maximum number of PIM(S,G) (S- Source G-Groups) that can be created in the mcache table from PIM traffic or PIM(S,G) join received from the neighbor. For each new entry, the source of the PIM(S,G) should be a unique entry..
- **ip igmp max-group-address**: Configures the maximum number of IGMP addresses for the default virtual routing and forwarding (VRF) instance or for a specified VRF. The **ip igmp max-group-address** command replaces the **system-max igmp-max-group-address** command.

  NOTE
  For ICX 7850 and ICX 7550 devices, values are used from the forwarding profile. Refer to the **forwarding-profile** command in the *RUCKUS FastIron Command Reference* and the *Configuration Fundamentals* chapter in the *RUCKUS FastIron Management Configuration Guide* for more information.

Support for show and clear Commands

The following **show** and **clear** commands have been updated to support the Multicast Multi-VRF feature:

- **clear ip igmp [** *vrf vrf-name* **]cache**
- **clear ip igmp [** *vrf vrf-name* **]traffic**
- **show ip igmp [** *vrf vrf-name* **]group**
- **show ip igmp [** *vrf vrf-name* **]interface**
- **show ip igmp [** *vrf vrf-name* **]settings**
- **show ip igmp [** *vrf vrf-name* **]traffic**

For full syntax details, refer to the *RUCKUS FastIron Command Reference*.

Changing Global IP Multicast Parameters

The following sections apply to PIM-DM, PIM-SM, and IGMP.

Concurrent Support for Multicast Routing and Snooping

Multicast routing and multicast snooping instances work concurrently on the same device. For example, you can configure PIM routing on certain virtual Ethernet (VE) interfaces and snooping on other VLANs. The limitation is that either multicast snooping or routing can be enabled on a VE interface or a VLAN, but not both. This is because all of the multicast data and control packets (IGMP, PIM) received on the snooping VLAN are handled by multicast snooping and do not reach the multicast routing component. Similarly, any multicast data or control packets received on a VE interface enabled with PIM routing are handled by the PIM routing component and are not seen by the IGMP or PIM snooping component.

The following considerations apply when configuring concurrent operation of Multicast Routing and Snooping.

1. Either multicast snooping or routing can be enabled on a VE or VLAN, but not both.
2. Snooping can be enabled globally by configuring the **ip multicast** command with either the **active** or **passive** keyword.
3. The global snooping configuration is inherited by all current VLANs that are not enabled for multicast routing.
4. The global snooping configuration is also inherited by all new VLANs. Enabling multicast routing on a newly created VLAN or VE automatically disables snooping on the VLAN or VE.
5. When a VLAN-level snooping is configured, it is displayed.

Defining the Maximum Number of PIM Cache Entries

You can define the maximum number of multicast cache entries.

To define the maximum number of PIM (S,G) mcache entries for the default VRF, use the following steps. You can also define this number for a specific VRF when you add the VRF name to the **router pim** command in step 2.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable PIM globally.

```
device(config)# router pim
```

3. Define the maximum number of PIM cache entries.

```
device(config-router-pim)# max-mcache 999
```

The following example defines the maximum number of PIM cache entries as 999.

```
device# configure terminal
device(config)# router pim
device(config-router-pim)# max-mcache 999
```

Setting the Maximum Number of IGMP Group Addresses

You can change the maximum number of IGMP group addresses for the default virtual routing and forwarding (VRF) instance or a specific VRF, globally or at the interface level.

Complete the following steps to set the maximum number of IGMP addresses for a specific VRF.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Specify the VRF.

```
device(config)# vrf vpn1
```

3. Enter IPv4 address family mode.

```
device(config-vrf-vpn1)# address-family ipv4
```

4. Set the maximum number of IGMP group addresses.

```
device(config-vrf-vpn1-ipv4)# ip igmp max-group-address 1000
```

The following example sets the maximum number of IGMP group addresses for VRF VPN1 to 1000.

```
device# configure terminal
device(config)# vrf vpn1
device(config-vrf-vpn1)# address-family ipv4
device(config-vrf-vpn1-ipv4)# ip igmp max-group-address 1000
```

The following example configures a maximum of 1000 IGMP group addresses for a VE interface.

```
device# configure terminal
device(config)# interface ve 10
device(config-vif-10)# ip igmp max-group-address 1000
```

Configuring the IGMP Report Filter Policy

The IGMP report filter policy can be configured globally, for a non-default VRF instance, or for an interface. The following task configures the IGMP report filter policy globally.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Configure the IGMP report filter policy globally, specifying an ACL.

```
device(config)# ip igmp access-group test1-v4
```

NOTE
ACL rules are used to configure which multicast group addresses, source addresses, or report and leave messages are to be dropped or allowed. For standard ACLs, only multicast group addresses and prefixes are configured, because this ACL is used for group filtering only. For extended ACLs, multicast group addresses or prefixes are configured as destination IP prefixes and the source addresses and prefixes are configured as the source IP address and prefix.

NOTE
If the specified ACL is not configured, the IGMP report messages for all multicast group addresses and source addresses are dropped.

NOTE
If an IGMP report filter policy is configured both globally and at the interface level, only the interface filter is applied.

The following example configures the IGMP report filter policy for a VE interface.

```
device# configure terminal
device(config)# interface ve 10
device(config-vif-10)# ip igmp access-group test1-v4
```

IPv4 PIM Register Message Rate Limit

When a new source begins transmitting within a Protocol Independent Multicast (PIM) network, the designated router (DR) encapsulates multicast packets into register messages and forwards them to the rendezvous point (RP). If the source is running at a high data rate with many new sources starting concurrently, pressure can be put on the CPU due to the large number of multicast packet streams being sent to the network. This situation can occur after a network or power failure. To avoid this scenario, the rate limit for the number of register messages should be set to a relatively low value. This value is based on the known number of multicast sources present.

The following values apply when configuring register message rate limiting usable in both DR and RP switches:

- For a DR, the default rate limit is set to one message per second.
- For an RP, the default rate limit is set to one message per second. The maximum supported rate can be set to 50 packets per second (pps) for all (S, G) pairs counted per VRF.

  NOTE
  In an RP, where both the PIM register message filter rule and the PIM register message rate limit are configured, filtering functionality takes precedence over rate limiting.

When PIM register message rate limit is not configured, a RUCKUS ICX network stack allows a maximum of 1000 register messages for software forwarding. When PIM register message rate limit is configured, the maximum number of supported register messages is 50 per device or VRF.

Configuring the Register Message Rate Limit for PIM

The maximum number of register packets sent or received per second by a device can be configured.

Complete the following steps to configure the register message rate limit to 20 packets per second, changing it from the default of 1 packet per second. This rate is applicable to register messages from all sources. This rate is applied to all sources that are permitted by the accept-register filter that is used to block unauthorized sources or groups.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable PIM globally.

```
device(config)# router pim
```

3. Set the register rate limit to 20 packets per second.

```
device(config-pim-router)# register-rate-limit 20
```

The following example sets the register message rate limit to 20 packets per second.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# register-rate-limit 20
```

The following example restores the register message rate limit to the default of 1 packet per second..

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# no register-rate-limit
```

IPv4 PIM Register Message Filter Rule

Protocol Independent Multicast (PIM) register messages received from a downstream multicast designated router (DR) should be filtered for reserved or any other undesirable multicast groups.

The IPv4 PIM register message filter rule interacts with configured extended IP access control lists (ACLs) at software level to either permit or deny register messages for matching (S, G) IP address rules in the RP. When a deny ACL action matches, the RP sends a register stop message to the DR to further limit new register messages.

Networks that do not maintain a multicast domain and require only the IP multicast service are required to stand up a PIM-SM router that will be incorporated into the JIE shared tree structure by establishing a peering session with an RP router. This helps to provide a secured IP core network. All RP devices that are peering with customer PIM-SM routers implement a PIM import policy that blocks multicast registration requests for reserved or any other undesirable multicast groups.

NOTE
In an RP, where both the PIM register message filter rule and the PIM register message rate limit are configured, filtering functionality takes precedence over rate limiting.

NOTE
Register message filtering depends on the availability of ACL resources in the network.

Configuring the Register Message Filter Rule for PIM

Complete the following steps to configure the register message filter rule for PIM so that unauthorized multicast sources or groups are blocked.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable PIM globally.

```
device(config)# router pim
```

3. Configure the register message filter rule for PIM, specifying an ACL.

```
device(config-pim-router)# accept-register pim_reg_filter
```

The following example configures the register message filter rule for PIM with a specified ACL.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# accept-register pim_reg_filter
```

The following example removes the register message filter rule for PIM with a specific configured ACL..

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# no accept-register pim_reg_filter
```

The following example displays PIM Sparse configuration information, including information about the register message filter rules.

```
device> show ip pim sparse
Global PIM Sparse Mode Settings
Maximum Mcache             : 2048            Current Count                : 0
Hello interval             : 30              Neighbor timeout             : 105
Join/Prune interval        : 60              Inactivity interval          : 180
Hardware Drop Enabled      : Yes              Prune Wait Interval         : 3
Bootstrap Msg interval     : 60               Candidate-RP Msg interval   : 60
Register Suppress Time     : 60               Register Probe Time         : 10
Register Stop Delay        : 10               SPT Threshold               : 1
SSM Enabled                : No
Route Precedence           : uc-non-default uc-default mc-non-default mc-default
Embedded RP Enabled        : Yes
Slow Path Disable All      : No               Slow Path Enable SSM        : No
Slow Path Filter Acl       : None
Register Rate Limit        : 20 pps        Register Filter                :  pim_reg_filter
```

Modifying IGMPv1 and IGMPv2 Parameters

Various IGMP parameters can be modified from their default values.

IGMP allows RUCKUS devices to limit the multicast of IGMP packets to only those ports on the device that are identified as IP Multicast members. The device actively sends out host queries to identify IP Multicast groups on the network, inserts the group information in an IGMP packet, and forwards the packet to IP Multicast neighbors.

The following IGMP version 1 (v1) and version 2 (v2) parameters apply to PIM:

- IGMP query interval: Specifies how often the RUCKUS device queries an interface for group membership. Possible values are from 2 through 3600. The default is 125.
- IGMP group membership time: Specifies how many seconds an IP Multicast group can remain on a RUCKUS device interface in the absence of a group report. Possible values are from 5 through 26000. The default is 260.

- IGMP maximum response time: Specifies how many seconds the RUCKUS device will wait for an IGMP response from an interface before concluding that the group member on that interface is down and removing the interface from the group. Valid values range from 1 through 50 seconds. The default is 10 seconds.

1. Enter global configuration mode.

```
device# configure terminal
```

2. To modify the default value for the IGMP query interval, use the **ip igmp query-interval** command.

```
device(config)# ip igmp query-interval 120
```

3. To modify the IGMP group membership time, use the **ip igmp group-membership-time** command.

```
device(config)# ip igmp group-membership-time 240
```

4. To change the IGMP maximum response time, use the **ip igmp max-response-time** command.

```
device(config)# ip igmp max-response-time 8
```

The following example modifies the IGMP query interval to 120 seconds, the IGMP group membership time to 240 seconds, and the IGMP maximum response time to 8 seconds.

```
device# configure terminal
device(config)# ip igmp query-interval 120
device(config)# ip igmp group-membership-time 240
device(config)# ip igmp max-response-time 8
```

Adding an Interface to a Multicast Group

You can manually add an interface to a multicast group. This is useful in the following cases:

- Hosts attached to the interface are unable to add themselves as members of the group using IGMP.
- There are no members for the group attached to the interface.

When you manually add an interface to a multicast group, the device forwards multicast packets for the group but does not itself accept packets for the group.

You can manually add a multicast group to individual ports only. If the port is a member of a virtual routing and forwarding (VRF) interface, you must add the ports to the group individually.

To manually add a port port 1/1/1 to multicast group 224.2.2.2:

```
device# configure terminal
device(config)# interface ethernet 1/1/1
device(config-if-e10000-1/1/1)# ip igmp static-group 224.2.2.2
```

To add a port 1/4/2 in VRF interface 1 to multicast group 224.2.2.2:

```
device# configure terminal
device(config)# interface ve 1
device(config-vif-1)# ip igmp static-group 224.2.2.2 ethernet 1/4/2
```

You can display information about manually added group using the following commands:

- **show ip igmp group**
- **show ip pim group**

To display static multicast groups in the default VRF, use the **show ip igmp static** command.

```
device# show ip igmp static

Group Address  Interface Port List
---------------------------------
    224.2.2.2  v1 ethe   1/4/2
```

To display information for IP PIM groups, use the **show ip pim group** command.

```
device> show ip pim group

Total number of groups for VRF default-vrf: 1
1    Group 224.2.2.2
     Group member at  e1/4/2
```

Multicast Non-Stop Routing

Multicast non-stop routing (NSR) provides hitless-failover support on all platforms for IPv4 multicast features (default and non-default VRFs): PIM-DM, PIM-SM, and PIM-SSM.

If multicast NSR is enabled, the software state is kept in sync between the active and standby modules. The standby module is NSR ready when the software state of the standby and active modules are in sync. When the standby module is NSR ready, a hitless-failover does not result in a disruption to the multicast forwarding state or traffic

If Multicast NSR is not enabled, or if the standby module is not NSR ready, the software state of the standby and active modules are not in sync. In this case, after a switchover or failover occurs, the new active module enters protocol learning phase for a duration of 55 seconds. During this phase, it learns the protocol state information from its PIM neighbors and local clients. During this period, new multicast flows will not be forwarded, but the existing mutlicast flows (which existed prior to switchover or failover) are forwarded in hardware without any disruption. At the end of the period, all the existing flows are deleted from hardware and they are reprogrammed as per the newly learned state information. Multicast traffic will incur a slight disturbance until the new active module reprograms the hardware with new forwarding state information.

The following message is displayed on the console of the active and standby modules to indicate that the standby module is NSR ready:

```
Mcastv4 is NSR ready
```

Configuring Multicast Non-Stop Routing

Multicast non-stop routing (NSR) provides hitless-failover support on all platforms for IPv4 multicast features.

- Multicast NSR is not supported for IPv6 multicast.
- When multicast NSR is turned on, unicast routing must be protected by NSR or graceful restart on all multicast VRFs.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Globally enable multicast non-stop routing for all VRFs, using the **ip multicast-nonstop-routing** command.

```
device(config)# ip multicast-nonstop-routing
```

During a hitless upgrade and switchover, the following syslog message is generated on the CLI. The message displayed depends on which version of PIM is configured.

```
MCASTv4 protocol receives switchover event
Mcastv4 protocol switchover done
```

In this example, PIM v4 is configured.

Passive Multicast Route Insertion

To prevent unwanted multicast traffic from being sent to the CPU, PIM routing and passive multicast route insertion (PMRI) can be used together to ensure that multicast streams are forwarded out only ports with interested receivers and unwanted traffic is dropped in hardware on Layer 3 switches.

PMRI enables a Layer 3 switch running PIM Sparse to create an entry for a multicast route (for example, (S,G), with no directly attached clients or when connected to another PIM device (transit network).

When a multicast stream has no output interfaces (OIF), the Layer 3 switch can drop packets in hardware if the multicast traffic meets either of the following conditions.

In PIM-SM:

- The route has no OIF *and*
- If directly connected source passed source reverse-path forwarding (RPF) check *and* completed data registration with reverse path (RP) *or*
- If a non-directly connected source passed source RPF check.

In PIM-DM:

- The route has no OIF *and*
- Passed source RPF check *and*
- Device has no downstream PIM neighbor.

If the OIF is inserted after the hardware-drop entries are installed, the hardware entries will be updated to include the OIFs.

NOTE
Disabling hardware-drop does not immediately take away existing hardware-drop entries. They will go through the normal route aging processing when the traffic stops.

Viewing PMRI Status and Disabling PMRI

Passive multicast route insertion (PMRI) is enabled by default. In some situations you may need to view the PMRI status and use the hardware-drop feature to disable PMRI.

After determining that PMRI is enabled, you must enable PIM routing and then disable PMRI using the hardware-drop feature syntax.

1. Use the **show ip pim sparse** command to display the status of PMRI.

```
device> show ip pim sparse

Global PIM Sparse Mode Settings
  Maximum Mcache         : 16384       Current Count              : 3
  Hello interval         : 30          Neighbor timeout           : 105
  Join/Prune interval    : 60          Inactivity interval        : 180
  Hardware Drop Enabled  : Yes         Prune Wait Interval        : 3
  Bootstrap Msg interval : 60          Candidate-RP Msg interval  : 60
  Register Suppress Time : 60          Register Probe Time        : 10
  Register Stop Delay    : 10
  SSM Enabled            : Yes         SPT Threshold              : 1
  SSM Group Range        : 232.0.0.0/8
  Route Precedence       : uc-non-default uc-default mc-non-default mc-default
  Slow Path Disable All        : Yes                                  Slow Path Enable
SSM                          :Yes
        Slow Path Filter Acl : acl
```

   In the output, you can see that the hardware-drop is enabled meaning that PMRI is enabled.

2. Enter global configuration mode.

```
device# configure terminal
```

3. Configure PIM.

```
device(config)# router pim
```

4. Disable PMRI, using the **hardware-drop-disable** command.

```
device(config-pim-router)# hardware-drop-disable
```

The following example displays the status of PMRI and then disables PMRI using the hardware-drop feature.

```
device# show ip pim sparse
device# configure terminal
device(config)# router pim
device(config-pim-router)# hardware-drop-disable
```

IP Multicast Boundaries

The IP multicast boundary feature is designed to selectively allow or disallow multicast flows to configured interfaces.

The **ip multicast-boundary** command allows you to configure a boundary on a PIM enabled interface by defining which multicast groups may not forward packets over a specified interface. This includes incoming and outgoing packets. By default, all interfaces that are enabled for multicast are eligible to participate in a multicast flow provided they meet the multicast routing protocol's criteria for participating in a flow.

Configuration Considerations

- Only one ACL can be bound to any interface.

- Normal ACL restrictions apply as to how many software ACLs can be created, but there is no hardware restrictions on ACLs with this feature.
- Creation of a static IGMP client is allowed for a group on a port that may be prevented from participation in the group on account of an ACL bound to the port's interface. In such a situation, the ACL would prevail and the port will not be added to the relevant entries.
- Either standard or extended ACLs can be used with the multicast boundary feature. When a standard ACL is used, the address specified is treated as a group address and NOT a source address.
- When a boundary is applied to an ingress interface, all packets destined to a multicast group that is filtered out will be dropped by software. Currently, there is no support to drop such packets in hardware.
- The **ip multicast-boundary** command may not stop clients from receiving multicast traffic if the filter is applied on the egress interface up-stream from RP.

Configuring Multicast Boundaries

An access list is used to define boundaries for PIM enabled interfaces.

This task requires a standard or extended access list to be created to filter multicast traffic. A standard access list is defined in the steps. Other access list example configurations follow this task.

This task assumes that PIM routing is enabled for the interface used in this task.

1. Enter global configuration mode.

```
device# configure terminal
```

2. To permit multicast traffic for group 225.1.0.2, enter the following command.

```
device(config)# ip access-list standard 10
device(config-std-ipacl-10)# permit host 225.1.0.2
```

3. To deny all other traffic, enter the following command.

```
device(config-std-ipacl-10)# deny any
device(config-std-ipacl-10)# exit
```

4. Enter virtual Ethernet interface mode.

```
device(config)# interface ve 40
```

5. Configure multicast boundaries for VE 40 using access list 10.

```
device(config-vif-40)# ip multicast-boundary 10
```

The following example creates standard access list 10 to permit multicast traffic for group 225.1.0.2 and deny all other traffic. Access list 10 is used to define multicast boundaries for PIM-enabled interfaces.

```
device# configure terminal
device(config)# ip access-list standard 10
device(config-std-ipacl-10)# permit host 225.1.0.2
device(config-std-ipacl-10)#  deny any
device(config-std-ipacl-10)# exit
device(config)# interface ve 40
device(config-vif-40)# ip multicast-boundary 10
```

Extended ACL to Permit Multicast Traffic

To permit multicast data traffic from source 97.1.1.50 for group 225.1.0.1 and deny all other traffic, enter the following commands.

```
device# configure terminal
device(config)# ip access-list extended 102
device(config-ext-ipacl-102)# permit ip host 97.1.1.50 host 225.1.0.1
device(config-ext-ipacl-102)# deny ip any any
```

Extended ACL to Deny Multicast Traffic

To deny multicast data traffic from group 225.1.0.1 and permit all other traffic, enter the following commands.

```
device# configure terminal
device(config)# ip access-list extended 101
device(config-ext-ipacl-101)# deny ip any host 225.1.0.1
device(config-ext-ipacl-101)# permit ip any any
```

PIM Dense

NOTE
This section describes the "dense" mode of PIM, described in RFC 3973. Refer to PIM Sparse on page 97 for information about PIM Sparse.

PIM was introduced to simplify some of the complexity of the routing protocol at the cost of additional overhead tied with a greater replication of forwarded multicast packets. PIM builds source-routed multicast delivery trees and employs reverse path check when forwarding multicast packets.

There are two modes in which PIM operates: Dense and Sparse. The Dense Mode is suitable for densely populated multicast receivers, primarily in the LAN environment. The Sparse Mode is suitable for sparsely populated multicast receivers with the focus on WAN.

PIM uses the IP routing table instead of maintaining its own, thereby being routing protocol dependent.

Initiating PIM Multicasts on a Network

Once PIM is enabled on each device, a network user can begin a video conference multicast from the server on R1 as shown in Figure 8 on page 90. When a multicast packet is received on a PIM-capable device interface, the interface checks its IP routing table to determine whether the interface that received the packet provides the shortest path back to the source. If the interface does provide the shortest path back to the source, the multicast packet is then forwarded to all neighboring PIM devices. Otherwise, the multicast packet is discarded and a prune message is sent back upstream.

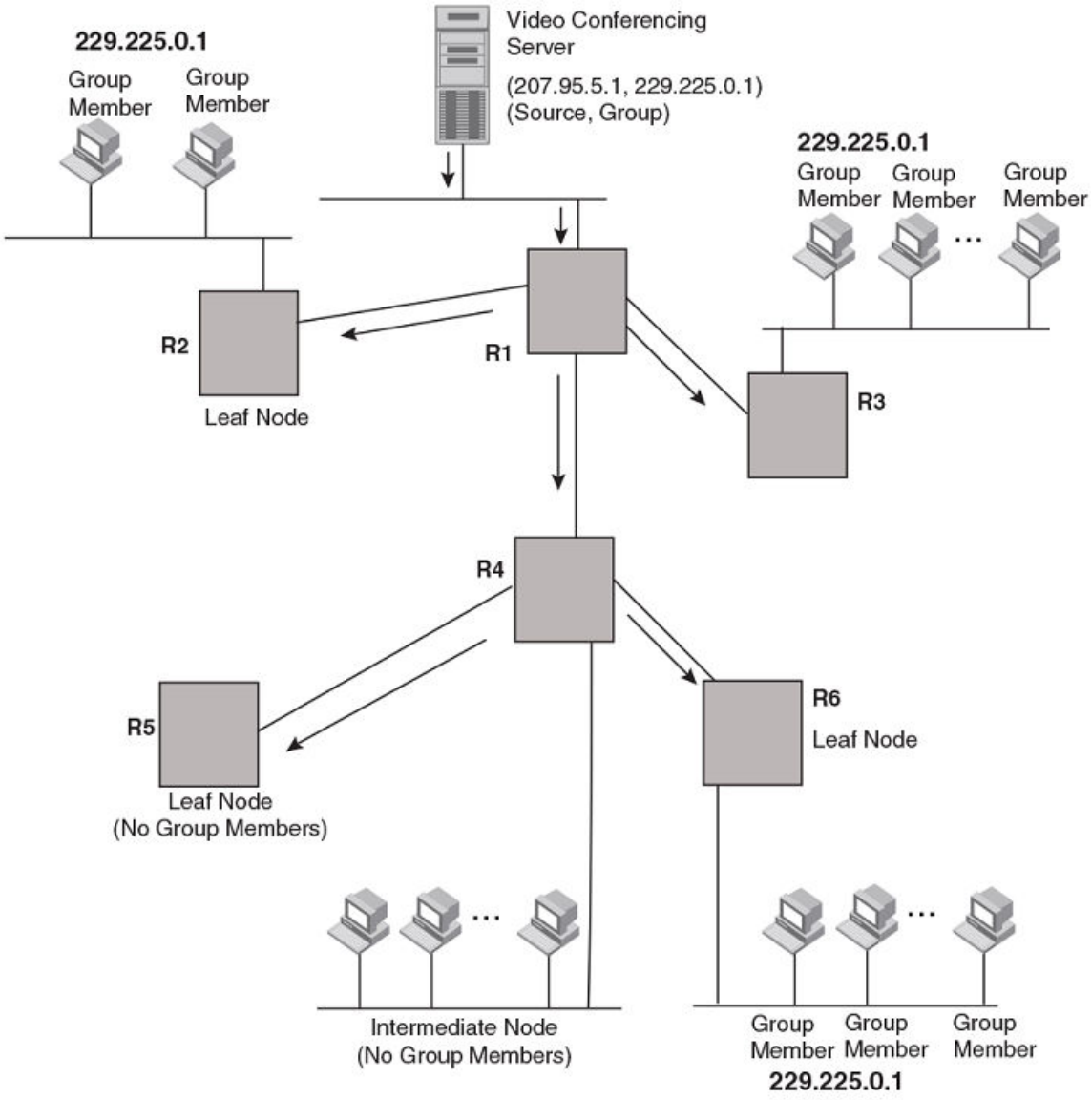
In Figure 8 on page 90, the root node (R1) is forwarding multicast packets for group 229.225.0.1, which it receives from the server, to its downstream nodes, R2, R3, and R4. Device R4 is an intermediate device with R5 and R6 as its downstream devices. Because R5 and R6 have no downstream interfaces, they are leaf nodes. The receivers in this example are those workstations that are resident on devices R2, R3, and R6.

Pruning a Multicast Tree

As multicast packets reach these leaf devices, the devices check their IGMP databases for the group. If the group is not in the IGMP database of the device, the device discards the packet and sends a prune message to the upstream device. The device that discarded the packet also maintains the prune state for the source, group (S,G) pair. The branch is then pruned (removed) from the multicast tree. No further multicast packets for that specific (S,G) pair will be received from that upstream device until the prune state expires. You can configure the PIM Prune Timer (the length of time that a prune state is considered valid).

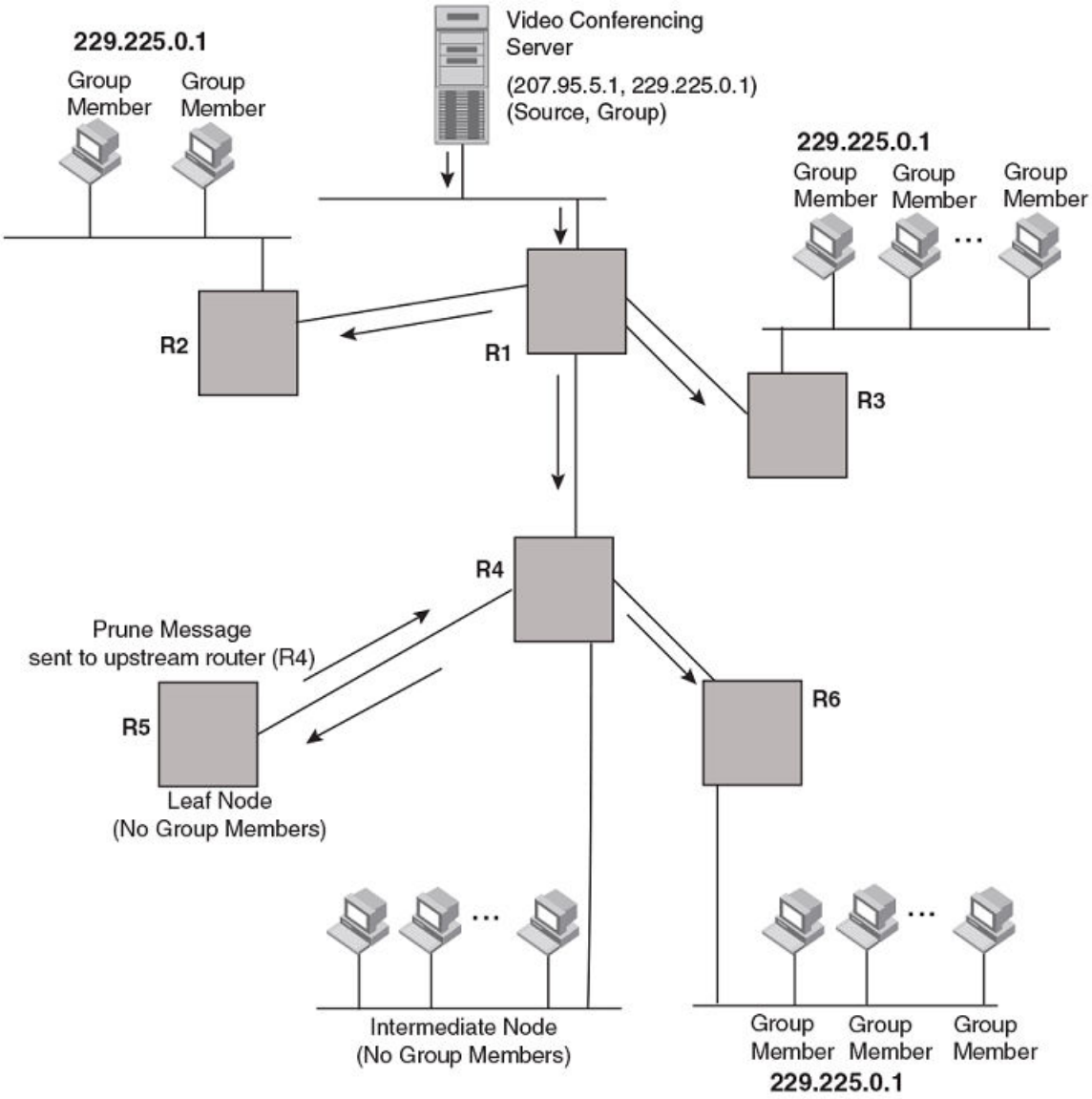
For example, in the figure below, the sender with address 207.95.5.1 is sending multicast packets to the group 229.225.0.1. If a PIM device receives any groups other than that group, the device discards the group and sends a prune message to the upstream PIM device.

FIGURE 8 Transmission of Multicast Packets from the Source to Host Group Members



In the figure below, device R5 is a leaf node with no group members in its IGMP database. Therefore, the device must be pruned from the multicast tree. R5 sends a prune message upstream to its neighbor device R4 to remove itself from the multicast delivery tree and install a prune state, as seen in the “Pruning leaf nodes from a multicast tree” figure. Device 5 will not receive any further multicast traffic until the prune age interval expires.

FIGURE 9 Pruning Leaf Nodes from a Multicast Tree



When a node on the multicast delivery tree has all of its downstream branches (downstream interfaces) in the prune state, a prune message is sent upstream. In the case of R4, if both R5 and R6 are in a prune state at the same time, R4 becomes a leaf node with no downstream interfaces and sends a prune message to R1. With R4 in a prune state, the resulting multicast delivery tree would consist only of leaf nodes R2 and R3.

Grafts to a Multicast Tree

A PIM device restores pruned branches to a multicast tree by sending graft messages towards the upstream device. Graft messages start at the leaf node and travel up the tree, first sending the message to its neighbor upstream device.

In the preceding example, if a new 229.255.0.1 group member joins on device R6, which was previously pruned, a graft is sent upstream to R4. Since the forwarding state for this entry is in a prune state, R4 sends a graft to R1. Once R4 has joined the tree, R4 along with R6 once again receive multicast packets.

Prune and graft messages are continuously used to maintain the multicast delivery tree. You do not need to configure anything.

PIM DM Versions

The RUCKUS device supports only PIM V2. PIM DM V2 sends messages to the multicast address 224.0.0.13 (ALL-PIM-ROUTERS) with protocol number 103.

Configuring PIM DM

NOTE
This section describes how to configure the "dense" mode of PIM, described in RFC 1075. Refer to Configuring PIM Sparse on page 98 for information about configuring PIM Sparse.

Enabling PIM Dense

PIM must be enabled globally and PIM Dense Mode (PIM DM) enabled locally on specific interfaces.

By default, PIM is disabled. To enable PIM:

- Enable the feature globally.
- Configure the IP interfaces that will use PIM.
- Enable PIM DM locally on the ports that have the IP interfaces you configured for PIM.

A use case for PIM DM can be to initiate the use of desktop video for fellow users on a sprawling campus network. All destination workstations have the appropriate hardware and software but the devices that connect the various buildings need to be configured to support PIM multicasts from the designated video conference server, as illustrated in the Pruning a Multicast Tree on page 89 section. In this section, PIM is enabled on each of the devices on which multicasts are expected. You can enable PIM on each device independently, or remotely from one of the devices with a Telnet connection. Follow the same steps for each device. All changes are dynamic.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Globally enable PIM.

```
device(config)# router pim
```

3. Exit to global configuration mode.

```
device(config-pim-router)# exit
```

4. Enter interface configuration mode.

```
device(config)# interface ethernet 1/1/3
```

This step configures Ethernet interface 1/1/3 and this interface is to run PIM DM.

5. Enter the IP address for the interface.

```
device(config-if-e10000-1/1/3)# ip address 10.9.9.9/32
```

6. Configure PIM DM on the interface.

```
device(config-if-e10000-1/1/3)# ip pim
```

The following example enables PIM globally and PIM DM on Ethernet interface 1/1/3.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# interface ethernet 1/1/3
device(config-if-e10000-1/1/3)# ip address 207.95.5.1/24
device(config-if-e10000-1/1/3)# ip pim
```

Enabling PIM Dense on a Specific VRF

PIM must be enabled globally and PIM Dense Mode (PIM DM) can be enabled for a specific virtual routing and forwarding instance (VRF).

By default, PIM is disabled. To enable PIM:

- Enable the feature globally.
- Configure the IP interfaces that will use PIM.
- Enable PIM DM locally on the ports that have the IP interfaces you configured for PIM.

A use case for PIM DM can be to initiate the use of desktop video for fellow users on a sprawling campus network. All destination workstations have the appropriate hardware and software but the devices that connect the various buildings need to be configured to support PIM multicasts from the designated video conference server, as illustrated in the Pruning a Multicast Tree on page 89 section. In this section, PIM is enabled on each of the devices shown in the “Pruning leaf nodes from a multicast tree” figure, on which multicasts are expected. You can enable PIM on each device independently or remotely from one of the devices with a Telnet connection. Follow the same steps for each device. All changes are dynamic.

All PIM parameters available for the default device instance are configurable for a VRF-based PIM instance.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Enable PIM for a specific VRF.

   ```
   device(config)# router pim vrf blue
   ```

   In this example, PIM is enabled for the VRF named blue. The VRF must be created before you specify it in this task step or you will receive an error message stating that the VRF does not exist.

The following example enables PIM for the VRF named blue.

```
device# configure terminal
device(config)# router pim vrf blue
```

Modifying PIM Global Options

Many PIM options can be modified from their default values in gloabl configuration mode.

PIM global parameters come with preset values. The defaults work well in most networks, but you can modify the following parameters if necessary:

- Neighbor timeout: Neighbor timeout is the interval after which a PIM device will consider a neighbor to be absent. Absence of PIM hello messages from a neighboring device indicates that a neighbor is not present.
- Hello timer: The hello timer defines the interval at which periodic hellos are sent out PIM interfaces. Devices use hello messages to inform neighboring devices of their presence.
- Prune timer: The prune timer defines how long a PIM device will maintain a prune state for a forwarding entry. The first received multicast packet is forwarded to all other PIM interfaces on the device. If there is no presence of groups on that interface, the leaf node sends a prune message upstream and stores a prune state. This prune state travels up the tree and installs a prune state. A prune state is maintained until the prune timer expires or a graft message is received for the forwarding entry.

- Prune wait timer: The prune wait timer allows you to configure the amount of time a PIM device will wait before stopping traffic to neighbor devices that do not want the traffic. A prune wait value of zero causes the PIM device to stop traffic immediately upon receiving a prune message. If there are two or more neighbors on the physical port, then the prune wait timer must not be used because one neighbor may send a prune message while the other sends a join message at the same time, or within less than three seconds.
- Graft retransmit timer: The graft retransmit timer defines the interval between the transmission of graft messages. A graft message is sent by a device to cancel a prune state. When a device receives a graft message, the device responds with a Graft Ack (acknowledge) message. If this Graft Ack message is lost, the device that sent the graft message will resend it.
- Inactivity timer: The device deletes a forwarding entry if the entry is not used to send multicast packets. The PIM inactivity timer defines how long a forwarding entry can remain unused before the device deletes it.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable PIM globally.

```
device(config)# router pim
```

3. Apply a PIM neighbor timeout value of 360 seconds to all ports on the device operating with PIM.

```
device(config-pim-router)# nbr-timeout 360
```

   The timeout interval can be set from 3 through 65535 seconds, and it must not be less than 3.5 times the hello timer value. The default value is 105.

4. Apply a PIM hello timer of 120 seconds to all ports on the device operating with PIM.

```
device(config-pim-router)# hello-timer 120
```

   The hello timer interval can be set from 10 through 3600 seconds, and the default is 30.

5. Set the PIM prune timer to 90.

```
device(config-pim-router)# prune-timer 90
```

   The prune timer range is from 60 through 3600 seconds. The default is 180.

6. Set the prune wait time to zero.

```
device(config-pim-router)# prune-wait 0
```

   The prune wait value can be set from 0 through 30 seconds. A smaller prune wait value reduces flooding of unwanted traffic. The default is 3. To view the currently configured prune wait time, enter the **show ip pim dense** command.

7. Set the graft retransmit timer to 90 seconds.

```
device(config-pim-router)# graft retransmit-timer 90
```

   The graft retransmit timer range is from 60 through 3600 second. The default is 180.

8. Apply a PIM inactivity timer of 90 seconds to all PIM interfaces.

```
device(config-pim-router)# inactivity-timer 90
```

   The value of the inactivity timer can be set from 60 through 3600 seconds. The default is 180.

9. Configure the register probe time.

```
device(config-pim-router)# register-probe-time 15
```

10. Configure the register suppression time.

```
device(config-pim-router)# register-suppress-time 90
```

11. Configure the message interval.

```
device(config-pim-router)# message-interval 120
```

12. Configure the SPT threshold.

```
device(config-pim-router)# spt-threshold 10
```

The following example shows how to configure the various PIM global options.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# nbr-timeout 360
device(config-pim-router)# hello-timer 120
device(config-pim-router)# prune-timer 90
device(config-pim-router)# prune-wait 0
device(config-pim-router)# graft retransmit-timer 90
device(config-pim-router)# inactivity-timer 90
device(config-pim-router)# register-probe-time 15
device(config-pim-router)# register-suppress-time 90
device(config-pim-router)# message-interval 120
device(config-pim-router)# spt-threshold 10
```

Configuring the Slow Path Forwarding of IPv4 Multicast Data Packets

The slow path forwarding of IPv4 multicast data packets is enabled by default for PIM-SM groups and disabled by default for PIM-SSM groups. Various commands can be used to change the default settings for the slow path forwarding of IPv4 multicast data packets.

The following task enables slow path forwarding for SSM groups.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable PIM globally.

```
device(config)# router pim
```

3. Enable slow path forwarding for Source-Specific Multicast (SSM) groups.

```
device(config-pim-router)# slow-path-forwarding enable-ssm
```

   Slow path forwarding for SSM groups is disabled by default.

The following example disables the slow path forwarding for all IP multicast data packets.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# slow-path-forwarding disable-all
```

The following example enables the slow path forwarding of IP multicast data packets for SSM groups.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# slow-path-forwarding enable-ssm
```

Selection of Shortest Path Back to Source

By default, when a multicast packet is received on a PIM-capable interface in a multi-path topology, the interface checks its IP routing table to determine the shortest path back to the source.

If the alternate paths have the same cost, the first alternate path in the table is picked as the path back to the source. For example, in the following example of output from the **show ip route** command, the first four routes have the same cost back to the source. However, 137.80.127.3 is chosen as the path to the source since it is the first one on the list. The device rejects traffic from any port other than Port v11 on which 137.80.127.3 resides

```
device> show ip route

Total number of IP routes: 19
Type Codes - B:BGP D:Connected I:ISIS S:Static R:RIP O:OSPF Cost - Dist/Metric
     Destination     Gateway         Port       Cost       Type
       ..
     172.17.41.4     137.80.127.3    v11        2          O
     172.17.41.4     137.80.126.3    v10        2          O
     172.17.41.4     137.80.129.1    v13        2          O
     172.17.41.4     137.80.128.3    v12        2          O
     172.17.41.8     0.0.0.0         1/2        1          D
```

Failover time in a Multi-Path Topology

When a port in a multi-path topology fails, multicast devices, depending on the routing protocol being used, take a few seconds to establish a new path, if the failed port is the input port of the downstream device.

Configuring a DR Priority

The DR priority option lets you give preference to a particular device in the DR election process by assigning it a numerically higher DR priority. This value can be set for IPv4 interfaces. To set a DR priority higher than the default value of 1, use the **ip pim dr-priority** command as shown in the following configuration example:

```
device# configure terminal
device(config)# interface ethernet 1/3/24
device(config-if-e10000-1/3/24)# ip pim dr-priority 50
```

The following information may be useful for troubleshooting.

- If more than one device has the same DR priority on a subnet (as in the case of default DR priority on all), the device with the numerically highest IP address on that subnet is elected as the DR.
- The DR priority information is used in the DR election ONLY IF ALL the PIM devices connected to the subnet support the DR priority option. If there is at least one PIM device on the subnet that does not support this option, then the DR election falls back to the backwards compatibility mode in which the device with the numerically highest IP address on the subnet is declared the DR regardless of the DR priority values.

PIM Convergence on MAC Address Movement

PIM convergence occurs when the PIM module is notified of a topology change.

The notification is triggered upon a change in port status, Reverse Path Forwarding (RPF) failure in the hardware, or by the unicast routing module if there is a change in the Layer 3 topology. If the topology change occurs without setting off any of the two events or if the Layer 3 topology change is not notified by the unicast routing module, PIM convergence does not take place.

If there is a change in the source traffic at the Layer 2 interface level, the RPF check fails because only loose RPF check is supported (loose RPF check detects the change in the source traffic only at the Layer 3 interface level). A notification for a change in the source traffic at the Layer 2 interface level can be triggered by establishing a signaling process for MAC address movement. The MAC address movement notification triggers RPF check on MAC address movement for directly connected sources. The MAC address movement notification can be triggered by configuring the **ip multicast-routing rpf-check mac-movement** command. The MAC address movement notification triggers a notification to the PIM module which results in convergence. PIM convergence is supported in both PIM Sparse and PIM Dense modes.

PIM convergence on MAC address movement is supported on the RUCKUS ICX 7xxx switches.

NOTE
PIM convergence on MAC address movement is applicable only in a topology where the multicast source port and PIM routers are in the same Layer 2 domain.

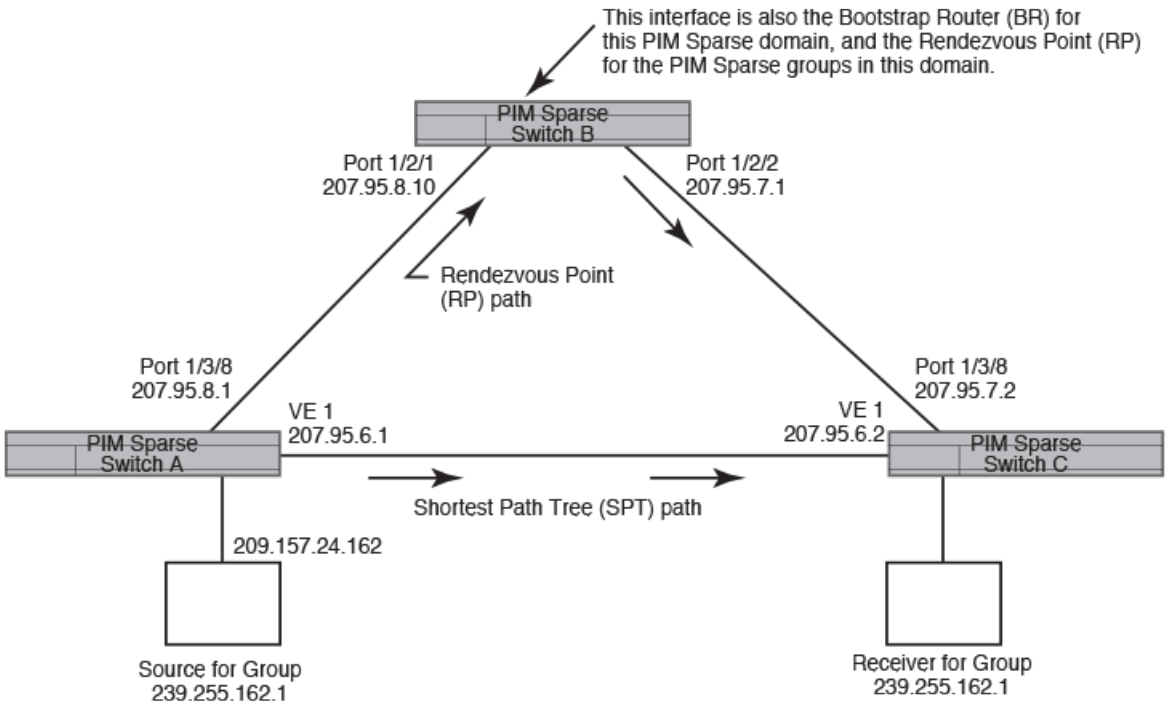
PIM Sparse

RUCKUS devices support Protocol Independent Multicast (PIM) Sparse version 2. PIM Sparse provides multicasting that is especially suitable for widely distributed multicast environments. The RUCKUS implementation is based on RFC 2362.

In a PIM Sparse network, a PIM Sparse device that is connected to a host that wants to receive information for a multicast group must explicitly send a join request on behalf of the receiver (host).

PIM Sparse devices are organized into domains. A PIM Sparse domain is a contiguous set of devices that all implement PIM and are configured to operate within a common boundary. The following figure shows a simple example of a PIM Sparse domain. This example shows three devices configured as PIM Sparse devices. The configuration is described in detail following the figure.

FIGURE 10 Example PIM Sparse Domain



PIM Sparse Device Types

Devices that are configured with PIM Sparse interfaces also can be configured to fill one or more of the following roles:

- PMBR: A PIM device that has some interfaces within the PIM domain and other interface outside the PIM domain. PMBRs connect the PIM domain to the Internet.
- BSR: The Bootstrap Router (BSR) distributes RP information to the other PIM Sparse devices within the domain. Each PIM Sparse domain has one active BSR. For redundancy, you can configure ports on multiple devices as candidate BSRs. The PIM Sparse protocol uses an election process to select one of the candidate BSRs as the BSR for the domain. The BSR with the highest BSR priority (a user-configurable parameter) is elected. If the priorities result in a tie, then the candidate BSR interface with the highest IP address is elected. In the example in the preceding figure, PIM Sparse device B is the BSR. Port 1/2/2 is configured as a candidate BSR.
- RP: The RP is the meeting point for PIM Sparse sources and receivers. A PIM Sparse domain can have multiple RPs, but each PIM Sparse multicast group address can have only one active RP. PIM Sparse devices learn the addresses of RPs and the groups for which they are responsible from messages that the BSR sends to each of the PIM Sparse devices. In the example in the preceding figure, PIM Sparse device B is the RP. Port 1/2/2 is configured as a candidate Rendezvous Point (RP). To enhance overall network performance, the RUCKUS device uses the RP to forward the packets from a group source to the group's receivers. Later, the RUCKUS device calculates the shortest path between the receiver and source (the Shortest Path Tree, or SPT) and uses the SPT for subsequent packets from the source to the receiver. The RUCKUS device calculates a separate SPT for each source-receiver pair.

  NOTE
  It is recommended that you configure the same ports as candidate BSRs and RPs.

RP Paths and SPT Paths

The preceding figure shows two paths for packets from the source for group 239.255.162.1 and a receiver for the group. The source is attached to PIM Sparse device A and the recipient is attached to PIM Sparse device C. PIM Sparse device B in is the RP for this multicast group. As a result, the default path for packets from the source to the receiver is through the RP. However, the path through the RP sometimes is not the shortest path. In this case, the shortest path between the source and the receiver is over the direct link between device A and device C, which bypasses the RP (device B).

To optimize PIM traffic, the protocol contains a mechanism for calculating the Shortest Path Tree (SPT) between a given source and receiver. PIM Sparse devices can use the SPT as an alternative to using the RP for forwarding traffic from a source to a receiver. By default, the RUCKUS device forwards the packets they receive from a given source to a given receiver using the RP path, but forward subsequent packets from that source to that receiver through the SPT. In the preceding figure, device A forwards the packets from group 239.255.162.1's source to the destination by sending the packet to device B, which is the RP. Device B then sends the packet to device C. Later, all packets that device A receives from the source for the receiver, device A forwards them directly to device C using the SPT path.

Configuring PIM Sparse

To configure a RUCKUS device for PIM Sparse, perform the following tasks:

- Configure the following global parameter:
  - Enable the PIM Sparse mode of multicast routing.
- Configure the following interface parameters:
  - Configure an IP address on the interface.
  - Enable PIM Sparse.
  - Identify the interface as a PIM Sparse border, if applicable.
- Configure the following PIM Sparse global parameters:
  - Identify the RUCKUS device as a candidate PIM Sparse Bootstrap Router (BSR), if applicable.

- Identify the RUCKUS device as a candidate PIM Sparse Rendezvous Point (RP), if applicable.
- Specify the IP address of the RP (if you want to statically select the RP).

NOTE
It is recommended that you configure the same RUCKUS device as both the BSR and the RP.

RP Configuration Considerations

When configuring a device as a candidate RP using the **rp-candidate** command, pay attention to the following considerations:

- When the candidate RP (c-RP) is configured, before explicitly specifying the groups that it serves, the c-RP does, by default, serve all the groups in the PIM SM multicast range, but this includes all groups beginning with 224.x.x.x all the way up to 239.x.x.x. This is reflected in the "rp-candidate add 224.0.0.0 4" line displayed as part of the runtime configuration. This entry will be referred to as the default prefix.
- When any group prefix is explicitly added (and the 224.0.0.0/4 prefix itself can also be explicitly added through the CLI), the default prefix is implicitly removed. Now, the only groups served by the candidate RP, are the groups that have been explicitly added.
- All explicitly added groups can be removed using the "delete" option or "no ... add" option. However, once all the explicitly added groups are deleted from the candidate RP group prefix list, the default prefix becomes active once more.

  NOTE
  This default group prefix cannot be removed.

- It is not possible to punch holes in the group prefix range. For example, running **rp-candidate add 228.0.0.0/16** and then **rp-candidate delete 228.0.1.0/24** is not allowed. This syntax cannot be used to ensure that the rp-candidate will serve all group prefixes in the 228.0.0.0/16 range except those in the 228.0.1.0/24 range.

Current Limitations

The implementation of PIM Sparse in the current software release has the following limitations:

- PIM Sparse and regular PIM (dense mode) cannot be used on the same interface.
- You cannot configure or display PIM Sparse information using the Web Management Interface. (You can display some general PIM information, but not specific PIM Sparse information.)

Enabling PIM Sparse

PIM must be enabled globally and PIM Sparse Mode (PIM SM) enabled locally on specific interfaces.

By default, PIM SM is disabled. To enable PIM SM:

- Enable PIM globally.
- Configure the IP interfaces that will use PIM SM.
- Enable PIM SM locally on the individual interfaces connected to the PIM Sparse network.

The steps in this task do not configure the device as a candidate PIM Sparse Bootstrap Router (BSR) and candidate Rendezvous Point (RP). You can configure a device as a PIM Sparse device without configuring the device as a candidate BSR and RP. If you do configure the device as a candidate BSR or RP, it is recommended that you configure the device as both a BSR and an RP. Refer to Configuring BSRs and RPs for PIM Sparse on page 101.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Globally enable PIM.

```
device(config)# router pim
```

3. Exit to global configuration mode to enter the interface.

```
device(config-router-pim)# exit
```

4. Enter interface configuration mode.

```
device(config)# interface ethernet 1/2/2
```

   This step configures Ethernet interface 1/2/2 and this interface is to run PIM SM.

5. Enter the IP address for the interface.

```
device(config-if-e10000-1/2/2)# ip address 207.95.7.1 255.255.255.0
```

6. Configure PIM SM on the interface.

```
device(config-if-e10000-1/2/2)# ip pim-sparse
```

7. (Optional) Specify that the interface is on the border of the PIM Sparse domain.

```
device(config-if-e10000-1/2/2)# ip pim border
```

The following example enables PIM globally and PIM SM on Ethernet interface 1/2/2 which is on the border of the PIM Sparse domain.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# exit
device(config)# interface ethernet 1/2/2
device(config-if-e10000-1/2/2)# ip address 207.95.7.1 255.255.255.0
device(config-if-e10000-1/2/2)# ip pim-sparse
device(config-if-e10000-1/2/2)# ip pim border
```

Enabling PIM Sparse on a Specific VRF

PIM must be enabled globally and PIM Sparse Mode (PIM SM) can be enabled for a specific virtual routing and forwarding instance (VRF).

By default, PIM is disabled. To enable PIM:

- Enable the feature globally.
- Configure the IP interfaces that will use PIM.
- Enable PIM DM locally on the ports that have the IP interfaces you configured for PIM.

To configure PIM SM on a virtual routing instance (VRF), the **vrf** option and *vrf-name* variable are added to the **router pim** command. All PIM parameters available for the default router instance are configurable for a VRF-based PIM instance.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable PIM for a specific VRF.

```
device(config)# router pim vrf blue
```

   In this example, PIM is enabled for the VRF named blue. The VRF must be created before you specify it in this task step or you will receive an error message stating that the VRF does not exist.

The following example enables PIM for the VRF named blue.

```
device# configure terminal
device(config)# router pim vrf blue
```

Configuring BSRs and RPs for PIM Sparse

After enabling PIM SM globally and locally, you need to identify an interface on at least one device as a candidate PIM Sparse Bootstrap router (BSR) and candidate PIM Sparse rendezvous point (RP).

This task assumes that you have configured PIM SM globally and on local interfaces.

NOTE
It is possible to configure the device as a candidate for either BSR or RP, but it is recommended that you configure the same interface on the same device as both a BSR and an RP.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Globally enable PIM.

   ```
   device(config)# router pim
   ```

3. Configure an interface as a candidate for BSR.

   ```
   device(config-pim-router)# bsr-candidate ethernet 1/2/2 30 255
   ```

   The hash number after the interface configuration specifies the number of bits in a group address that are significant when calculating the group-to-RP mapping. The hash value is from 1 through 32. It is recommended that you specify a value of 30 for IP version 4 (IPv4) networks. BSR priority can be configured as a value from 0 through 255. When the election process for BSR takes place, the candidate BSR with the highest priority becomes the BSR.

4. Configure the device as a candidate RP.

   ```
   device(config-pim-router)# rp-candidate ethernet 1/2/2
   ```

   By default, this command configures the device as a candidate RP for all group numbers beginning with 224. As a result, the device is a candidate RP for all valid PIM Sparse group numbers. You can change this by adding or deleting specific address ranges.

5. (Optional) To add a group number range for which the device is a candidate RP, use the **add** option to explicitly add a range.

   ```
   device(config-pim-router)# rp-candidate add 224.126.0.0 16
   ```

   In this example, the device is a candidate RP for all groups that begin with 224.126. When you add a range, you override the default. The device then becomes a candidate RP only for the group address ranges you add.

6. (Optional) To delete a group number range for which the device is a candidate RP, use the **delete** option to explicitly remove a range that was previously added.

   ```
   device(config-pim-router)# rp-candidate delete 224.126.22.0 24
   ```

   This example deletes an address group from the devices for which it is a candidate RP.

The following example configures the PIM Sparse interface on port 1/2/2 as a BSR candidate, with a hash mask length of 30 and a priority of 255. The same interface is also configured as an RP candidate. An explicit group address range is configured and the device is now a candidate RP for prefixes starting with 224.126.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# bsr-candidate ethernet 1/2/2 30 255
device(config-pim-router)# rp-candidate ethernet 1/2/2
device(config-pim-router)# rp-candidate add 224.126.0.0 16
```

Updating PIM-Sparse Forwarding Entries with New RP Static Configuration

You can define a static RP instead of using the PIM Sparse RP election process. After defining a static RP, you must clear out the old RP configuration.

It is recommended that you use the PIM Sparse protocol's RP election process so that a backup RP can automatically take over if the active RP router becomes unavailable. However, if you do not want the RP to be selected by the RP election process but instead you want to explicitly identify the RP by IP address, use the **rp-address** command.

If you explicitly specify the RP, the device uses the specified RP for all group-to-RP mappings and overrides the set of candidate RPs supplied by the BSR.

> **NOTE**
> Specify the same IP address as the RP on all PIM Sparse devices within the PIM Sparse domain. Make sure the device is on the backbone or is otherwise well connected to the rest of the network.

If you make changes to your static RP configuration, the entries in the PIM-Sparse multicast forwarding table continue to use the old RP configuration until they are aged out.

The **clear pim rp-map** command allows you to update the entries in the static multicast forwarding table immediately after making RP configuration changes. This command is meant to be used with the **rp-address** command.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Globally enable PIM.

   ```
   device(config)# router pim
   ```

3. Create a static RP IP address.

   ```
   device(config-pim-router)# rp-address 207.95.7.1
   ```

   The command in this example identifies the device interface at IP address 207.95.7.1 as the RP for the PIM Sparse domain. The device uses the specified RP and ignore group-to-RP mappings received from the BSR.

4. Exit to privileged EXEC configuration mode.

   ```
   device(config-pim-router)# end
   ```

5. To update the entries in a PIM sparse static multicast forwarding table with new RP configuration, you must clear out the old RP entries.

   ```
   device# clear ip pim rp-map
   ```

The following example configures a static RP for the PIM Sparse domain and clears out existing RP entries.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# rp-address 207.95.7.1
device(config-pim-router)# end
device# clear ip pim rp-map
```

ACL-based RP Assignment

Multiple static rendezvous point (RP) assignments can be configured. For each static RP, an ACL can be given as an option to define the multicast address ranges that the static RP permit or deny to serve.

A static RP by default serves the range of 224.0.0.0/4 if the RP is configured without an ACL name. If an ACL name is given but the ACL is not defined, the static RP is set to inactive mode and it will not cover any multicast group ranges.

The optional static RP ACL can be configured as a standard ACL or as an extended ACL. For an extended ACL, the destination filter will be used to derive the multicast group range and all other filters are ignored. The content of the ACL needs to be defined in the order of prefix length; the longest prefix must be placed at the top of the ACL definition.

If there are overlapping group ranges among the static RPs, the static RP with the longest prefix match is selected. If more than one static RP covers the exact same group range, the highest IP static RP will be used.

Configuration Considerations:

- The Static RP has higher precedence over RP learned from the BSR.
- There is a limit of 64 static RPs in the systems.

Configuring an ACL-based RP Assignment

The following configuration example configures an ACL based RP assignment.

```
device(config)# router pim
device(config-pim-router)# rp-address 130.1.1.1 acl1
```

The IP address specifies the device you want to designate as an RP device. The ACL name or ID number specifies which multicast groups use the RP.

IP multicast PIM Neighbor Filter

The IP multicast PIM neighbor filter feature allows you to control which devices can be PIM neighbors.

When two PIM-enabled neighbor devices exchange Hello packets at regular intervals they become PIM neighbors by default. The IP multicast PIM neighbor filter feature gives you more control over which devices can be PIM neighbors by configuring the **ip pim neighbor-filter** command or **ipv6 pim neighbor-filter** command. You can configure the ACL to filter PIM Hello packets from sources you want to deny or allow, thereby controlling those devices' eligibility to become PIM neighbors.

FIGURE 11 Multicast PIM Filter Topology

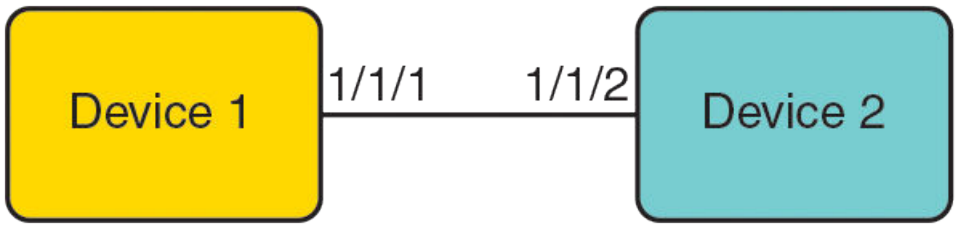


TABLE 6 Configurations for Devices Running IP multicast PIM Filters

Device 1	Device 2
ip access-list standard 10	interface ethernet 1/1/2
deny host 10.0.0.2	enable
permit any	ip address 10.0.0.2/24
interface ethernet 1/1/1	ip pim-sparse
enable	
ip address 10.0.0.1/24	
ip pim-sparse	
ip pim neighbor-filter 10	

Limitations

ACLs deny all access by default, and you must configure the **permit** command to permit access to one or more devices. You can configure the **permit any** command (or the **permit any any** command for an IPv4 extended ACL) on an interface to permit traffic on the interface to pass through without filtering.

An interface can have only one ACL configured on it.

There are no checks to validate whether an ACL applies to an interface. If the interface has no ACL, a warning that no filtering can occur is displayed.

The IP multicast PIM neighbor filter feature supports a maximum of 128 PIM neighbor filters for both IPv4 and IPv6.

Precedence-value matching in extended ACL configurations is not supported. Refer to the RUCKUS*FastIron Security Configuration Guide* for information on ACLs.

Configuring IPv4 PIM Neighbor Filtering

Configure an ACL and apply it to an interface to control neighbor access.

1. Configure an ACL named 10 to deny access to the device 10.10. 102.

```
device(config)# ip access-list standard 10
device(config-std-ipacl-10)# deny host 10.10.10.2
```

   You can identify the ACL by name as an ASCII string, by a number in the range 1 to 99 (for a standard ACL), or by a number in the range 100 to 199 (for an extended ACL).

2. Configure ACL 10 to permit access to all other devices.

```
device(config-std-ipacl-10)# permit any
device(config-std-ipacl-10)# exit
```

3. Configure an Ethernet interface.

```
device(config)# interface ethernet 1/3/2
```

4. Configure a filter that applies ACL 10 to the interface.

```
device(config-if-e1000-1/3/2)# ip pim neighbor-filter 10
```

   The host that is specified in ACL 10, 10.10.10.2 is prevented from becoming a PIM neighbor on the interface.

PIM Passive

PIM Passive is used to reduce and minimize unnecessary PIM Hello and other PIM control messages.

PIM Passive allows you to specify that the interface is "passive" in regards to PIM. No PIM control packets are sent or processed (if received), but hosts can still send and receive multicast traffic and IGMP control traffic on the interface. Also, PIM Passive prevents any malicious router from taking over as the designated router (DR), which can prevent all hosts on the LAN from joining multicast traffic outside the LAN.

The following guidelines apply to PIM Passive:

- PIM Passive is a Layer 3 interface [Ethernet, VE] level feature.
- Because the loopback interfaces are never used to form PIM neighbors, PIM Passive is not supported on loopback interfaces.
- Both PIM SM and PIM DM modes support PIM Passive.
- Applying PIM Passive on an interface requires PIM to be enabled on the interface.
- The sent and received statistics of a PIM Hello message are not changed for an interface while it is configured as PIM passive.

To enable PIM Passive on an interface, enter the following commands:

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# exit
device(config)# interface ethernet 2
device(config-if-e1000-2)# ip pim
device(config-if-e1000-2)# ip pim passive
device(config-if-e1000-2)# exit
device(config)# interface ve 2
device(config-vif-2)# ip pim-sparse
device(config-vif-2)# ip pim passive
device(config-vif-2)# exit
```

Multicast Outgoing Interface (OIF) List Optimization

Each multicast route entry maintains a list of outgoing interfaces (OIF List) to which an incoming multicast data packet matching the route is replicated. In hardware-forwarded route entries, these OIF lists are stored inside the hardware in replication tables which are limited in size. In many deployment scenarios, more than one multicast route can have identical OIF lists and can optimize usage of the replication table entries by sharing them across multiple multicast routes.

Multicast OIF list optimization keeps track of all the OIF lists in the system. It manages the hardware replication resources optimally, in real time, by dynamically assigning or re-assigning resources to multicast route entries to suit their current OIF list requirements, while maximizing resource sharing.

NOTE
IPv4 multicast routes do not share hardware replication table entries with IPv6 multicast routes even if they share the same OIF lists.

Clearing the PIM Forwarding Cache

You can clear the PIM forwarding cache using the following command.

```
device# clear ip pim cache
```

Use the **vrf** option to clear the PIM forwarding cache for a VRF instance specified by the *vrf-name* variable.

Clearing the PIM Message Counters

You can clear the PIM message counters using the following command.

```
device# clear ip pim traffic
```

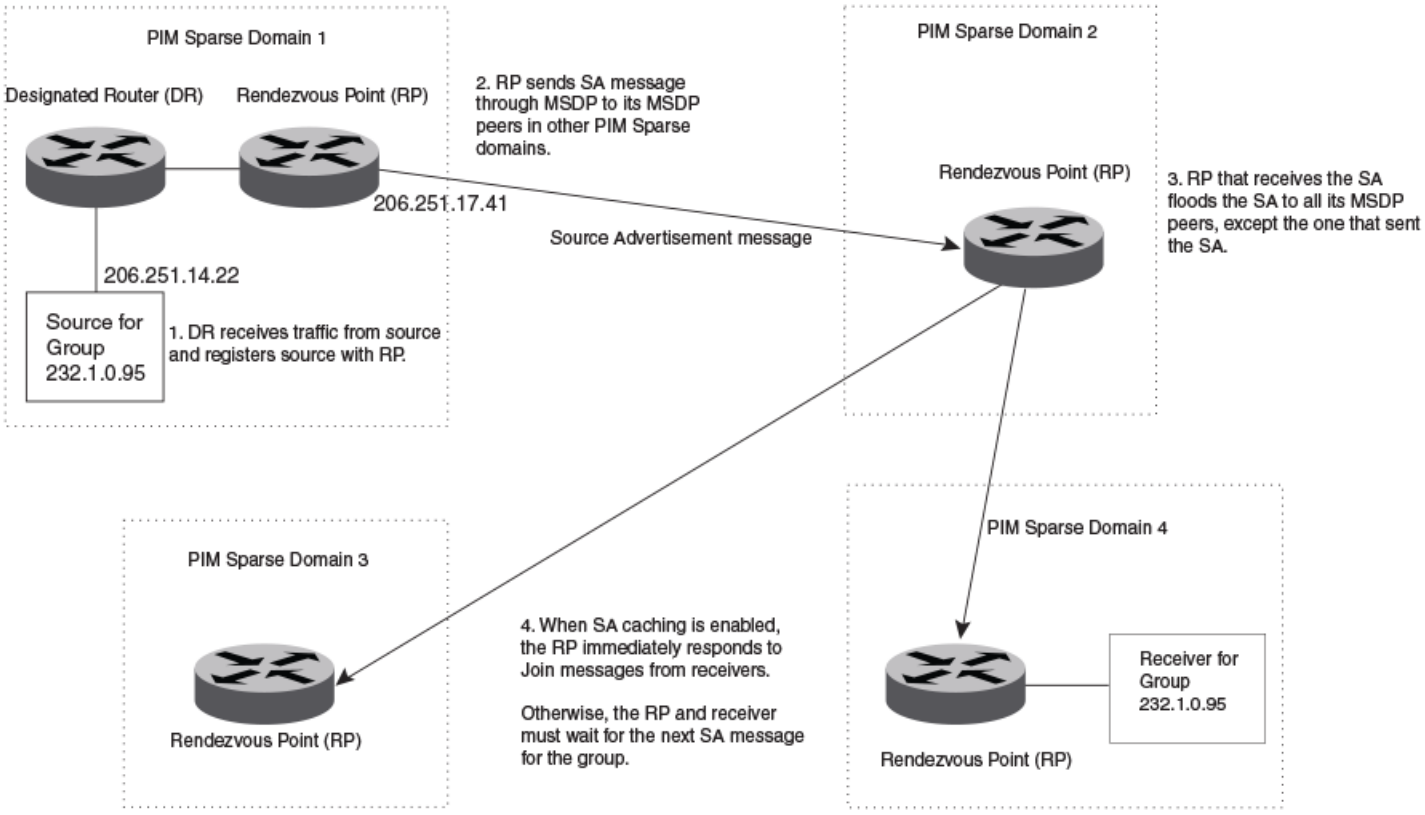
Use the **vrf** option to clear the PIM message counters for a VRF instance specified by the *vrf-name* variable.

Configuring Multicast Source Discovery Protocol

The Multicast Source Discovery Protocol (MSDP) is used by Protocol Independent Multicast (PIM) Sparse devices to exchange source information across PIM Sparse domains. Devices running MSDP can discover PIM Sparse sources in other PIM Sparse domains.

The following figure shows an example of some PIM Sparse domains. For simplicity, this example shows one Designated Router (DR), one group source, and one receiver for the group. Only one PIM Sparse device within each domain needs to run MSDP.

FIGURE 12 PIM Sparse Domains Joined by MSDP Devices



In this example, the source for PIM Sparse multicast group 232.0.1.95 is in PIM Sparse domain 1. The source sends a packet for the group to its directly attached DR. The DR sends a PIM register message for this flow to the RPDR. The RP is configured for MSDP, which enables the RP to exchange source information with other PIM Sparse domains by communicating with RPs in other domains that are running MSDP.

The RP sends the source information to each peer through a Source Active message. The message contains the IP address of the source, the group address to which the source is sending, and the IP address of the RP.

In this example, the Source Active message contains the following information:

- Source address: 206.251.14.22
- Group address: 232.1.0.95
- RP address: 206.251.17.41

Figure 12 shows only one peer for the MSDP device (which is also the RP here) in domain 1, so the Source Active message goes to only that peer. When an MSDP device has multiple peers, it sends a Source Active message to each of those peers. Each peer sends the Source Advertisement to other MSDP peers. The RP that receives the Source Active message also sends a Join message to the source if the RP that received the message has receivers for the group and source.

Peer Reverse Path Forwarding Flooding

When the MSDP device (also the RP) in domain 2 receives the Source Active message from the peer in domain 1, the MSDP device in domain 2 forwards the message to all other peers. This propagation process is sometimes called "peer Reverse Path Forwarding (RPF) flooding". In Figure 12 on page 106, the MSDP device floods the Source Active message it receives from the peer in domain 1 to peers in domains 3 and 4.

The MSDP device in domain 2 does not forward the Source Active back to the peer in domain 1, because that is the peer from which the device received the message. An MSDP device never sends a Source Active message back to the peer that sent it. The peer that sent the message is sometimes called the "RPF peer". The MSDP device uses the unicast routing table for its Exterior Gateway Protocol (EGP) to identify the RPF peer by looking for the route entry that is the next hop toward the source. Often, the EGP protocol is Border Gateway Protocol (BGP) version 4.

NOTE
MSDP depends on BGP for inter-domain operations.

The MSDP routers in domains 3 and 4 also forward the Source Active message to all peers except the ones that sent them the message. Figure 12 on page 106 does not show additional peers.

Source Active Caching

When an MSDP device that is also an RP receives a Source Active message, it checks the PIM sparse multicast group table for receivers for that group. If there are receivers for that group being advertised in the Source Active message, the RP sends a Join message towards the source.

In Figure 12 on page 106, if the MSDP device and RP in domain 4 has a table entry for the receiver, the RP sends a Join message on behalf of the receiver back through the RPF tree to the source, in this case the source in domain 1.

Source Active caching is enabled in MSDP on RUCKUS devices. The RP caches the Source Active messages it receives even if the RP does not have a receiver for the group. Once a receiver arrives, the RP can then send a Join to the cached source immediately.

The size of the cache used to store MSDP Source Active messages is 4K. MSDP SA cache size can be configured using the **system-max msdp-sa-cache** command.

Configuring MSDP Globally

To configure Multicast Source Discovery Protocol (MSDP) you must enable MSDP and configure the MSDP peers.

NOTE
The PIM Sparse Rendezvous Point (RP) can also be an MSDP peer.

It is strongly recommended that you use the **connect-source loopback** command when configuring the MSDP peers. If you do not use the **connect-source loopback** command, the device uses the IP address of the outgoing interface. You should also make sure the IP address of the connect-source loopback is the source IP address used by the PIM-RP, and the BGP device. Devices that run MSDP usually also run BGP.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Enter loopback interface configuration mode.

   ```
   device(config)# interface loopback 1
   ```

   The loopback interface is used as the source interface for sessions with the peer.

3. Enter the IP address to be used as the source address for peer sessions.

   ```
   device(config-lbif-1)# ip address 10.9.9.9/32
   ```

4. Exit to global configuration mode.

   ```
   device(config-lbif-1)# exit
   ```

5. Enable MSDP.

   ```
   device(config)# router msdp
   ```

6. Configure MSDP peers.

   ```
   device(config-msdp-router)# msdp-peer 205.216.162.1 connect-source loopback 1
   ```

   By default, the device uses the subnet address configured on the physical interface where you configure the neighbor as the source address for sessions with the neighbor.

7. Configure MSDP peer and specify that the interface loopback 1 and the TCP AO keychain chain1 are to be used for sessions with the peer.

   NOTE
   Change in TCP-AO keychain used by MSDP neighbor may cause the existing sessions to flap. Similarly, by removing or replacing the existing keychain configured in MSDP neighbor can also cause the sessions to flap.

   ```
   device(config-msdp-router)# msdp-peer 205.216.162.1 connect-source loopback 1 ao chain1
   ```

   Clear the MSDP peer session for the keychain configuration to take effect.

The following example configures a loopback interface, enables MSDP, and configures a neighbor as an MSDP peer using the loopback interface as the source interface and address.

```
device# configure terminal
device(config)# interface loopback 1
device(config-lbif-1)# ip address 10.9.9.9/32
device(config-lbif-1)# exit
device(config)# router msdp
device(config-msdp-router)# msdp-peer 205.216.162.1 connect-source loopback 1
```

Configuring MSDP for a Specific VRF

You can configure Multicast Source Discovery Protocol (MSDP) for a specific virtual routing forwarding (VRF) instance.

You must configure the VRF before starting this task.

All MSDP parameters available for the default router instance are configurable for a VRF-based MSDP instance.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable MSDP for a VRF named blue.

```
device(config)# router msdp vrf blue
```

3. Configure an MSDP peer on the VRF.

```
device(config-msdp-router-vrf-blue)# msdp-peer 205.216.162.1
```

The following example enables MSDP on VRF blue and configures a neighbor as an MSDP peer on the VRF.

```
device# configure terminal
device(config)# router msdp vrf blue
device(config-msdp-router-vrf-blue)# msdp-peer 205.216.162.1
```

Disabling an MSDP Peer

The following configuration example disables an MSDP peer.

```
device# configure terminal
device(config)# router msdp
device(config-msdp-router)# msdp-peer 205.216.162.1 shutdown
```

The following configuration example disables an MSDP peer for a specific VRF named blue.

NOTE

The syntax for disabling an MSDP peer is different in VRF configuration mode.

```
device# configure terminal
device(config)# router msdp vrf blue
device(config-msdp-router-vrf-blue)# no msdp-peer 205.216.162.1
```

Designating the Interface IP Address as the RP IP Address

When an RP receives a Source Active message, it checks its PIM Sparse multicast group table for receivers for the group. If a receiver exists the RP sends a Join to the source.

By default, the IP address included in the RP address field of the SA message is the IP address of the originating RP. An SA message can use the IP address of any interface on the originating RP. (The interface is usually a loopback interface.)

To designate an interface IP address to be the IP address of the RP, enter commands such as the following.

```
device(config)# interface loopback 2
device(config-lbif-2)# ip address 2.2.1.99/32
device(config)# router msdp
device(config-msdp-router)# originator-id loopback 2
device(config-msdp-router)# exit
```

To specify VRF information, enter the following commands at the MSDP VRF configuration level.

```
device(config)# interface loopback 2
device(config-lbif-2)# ip address 2.2.1.99/32
device(config)# router msdp vrf blue
device(config-msdp-router-vrf blue)# originator-id loopback 2
device(config-msdp-router-vrf blue)# exit
```

The **originator-id** command instructs MSDP to use the specified interface IP address as the IP address of the RP in an SA message. This address must be the address of the interface used to connect the RP to the source. The default address used is the RP IP address.

Filtering MSDP Source-Group Pairs

You can filter individual source-group pairs in MSDP Source-Active messages:

- **sa-filter in**: Filters source-group pairs received in Source-Active messages from an MSDP neighbor.
- **sa-filter originate**: Filters self-originated source-group pairs in outbound Source-Active messages sent to an MSDP neighbor
- **sa-filter out**: Filters self-originated and forwarded source-group pairs in outbound Source-Active messages sent to an MSDP neighbor

Filtering Incoming and Outgoing Source-Active Messages

The following example configures filters for incoming Source-Active messages from three MSDP neighbors:

- For peer 2.2.2.99, all source-group pairs in Source-Active messages from the neighbor are filtered (dropped).
- For peer 2.2.2.97, all source-group pairs except those with source address matching 10.x.x.x and group address of 235.10.10.1 are permitted.
- For peer 2.2.2.96, all source-group pairs except those associated with RP 2.2.42.3 are permitted.

To configure filters for incoming Source-Active messages, enter commands at the MSDP VRF configuration level.

To configure filters for outbound Source-Active messages, enter the optional **out** keyword.

The following commands configure extended ACLs. The ACLs will be used in route maps, which will be used by the Source-Active filters.

```
device(config)# ip access-list extended 123
device(config-ext-ipacl-123)# permit ip 10.0.0.0 0.255.255.255 host 235.10.10.1
device(config-ext-ipacl-123)# exit
device(config)# ip access-list extended 124
device(config-ext-ipacl-124)# permit ip host 2.2.42.3 any
device(config-ext-ipacl-124)# exit
device(config)# ip access-list extended 125
device(config-ext-ipacl-125)# permit ip any any
device(config-ext-ipacl-125)# exit
```

The following commands configure the route maps.

```
device(config)# route-map msdp_map deny 1
device(config-routemap msdp_map)# match ip address 123
device(config-routemap msdp_map)# exit
device(config)# route-map msdp_map permit 2
device(config-routemap msdp_map)# match ip address 125
device(config-routemap msdp_map)# exit
device(config)# route-map msdp2_map permit 1
device(config-routemap msdp2_map)# match ip address 125
device(config-routemap msdp2_map)# exit
device(config)# route-map msdp2_rp_map deny 1
device(config-routemap msdp2_rp_map)# match ip route-source 124
device(config-routemap msdp2_rp_map)# exit
device(config)# route-map msdp2_rp_map permit 2
device(config-routemap msdp2_rp_map)# match ip route-source 125
device(config-routemap msdp2_rp_map)# exit
```

To specify VRF information, enter the following commands at the MSDP VRF configuration level.

```
device(config)# router msdp vrf blue
device(config-msdp-router-vrf blue)# sa-filter in 2.2.2.99
device(config-msdp-router-vrf blue)# sa-filter in 2.2.2.97 route-map msdp_map
device(config-msdp-router-vrf blue)# sa-filter in 2.2.2.96 route-map msdp2_map rp-route-map msdp2_rp_map
```

The **sa-filter** commands configure the following filters:

- The first line of the **sa-filter** command drops all source-group pairs received from neighbor 2.2.2.99.

  NOTE
  The default action is to deny all source-group pairs from the specified neighbor. If you want to permit some pairs, use route maps.

- The second line of the **sa-filter** command drops source-group pairs received from neighbor 2.2.2.97 if the pairs have source addresses matching 10.x.x.x and group address 235.10.10.1.
- The third line of the **sa-filter** command accepts all source-group pairs except those associated with RP 2.2.42.3.

Filtering Advertised Source-Active Messages

The following example configures the device to advertise all source-group pairs except the ones that have source address 10.x.x.x.

The following commands configure extended ACLs to be used in the route map definition.

```
device(config)# ip access-list extended 123
device(config-ext-ipacl-123)# permit ip 10.0.0.0 0.255.255.255 any
device(config-ext-ipacl-123)# ip access-list extended 125
device(config-ext-ipacl-125)# permit ip any any
device(config-ext-ipacl-125)# exit
```

The following commands use the previously configured ACLs to configure a route map that denies source-group with source address 10.x.x.x and any group address, while permitting everything else.

```
device(config)# route-map msdp_map deny 1
device(config-routemap msdp_map)# match ip address 123
device(config-routemap msdp_map)# exit
device(config)# route-map msdp_map permit 2
device(config-routemap msdp_map)# match ip address 125
device(config-routemap msdp_map)# exit
```

The following commands configure the Source-Active filter.

```
device(config)# router msdp
device(config-msdp-router)# sa-filter originate route-map msdp_map
```

To specify VRF information, enter the following commands at the MSDP VRF configuration level.

```
device(config)# router msdp vrf blue
device(config-msdp-router-vrf blue)# sa-filter originate route-map msdp_map
```

This example specifies a route map. The router applies the filter to source-group pairs that match the route map.

NOTE
The default filter action is deny. If you want to permit some source-group pairs, use a route map. A permit action in the route map allows the device to advertise the matching source-group pairs. A deny action in the route map drops the source-group pairs from advertisements.

Displaying MSDP Information

You can use various **show** commands to view information about Multicast Source Discovery Protocol (MSDP).

Use one of the following commands to view MSDP information. The commands do not need to be entered in the specified order. Using these commands is optional and they can be entered in any order. For more information on the full list of **show ip msdp** commands, refer to the *RUCKUS FastIron Command Reference*.

1. Enter the **show ip msdp** command to display MSDP peer information including TCP keychain (AO) options..

```
device# show ip msdp  peer
        IP Address           State       Mesh-group-name
1       10.10.10.1           ESTABLISH
        Keep Alive Time  Hold Time   Age
        60               75          9
                             Message Sent         Message Received
        Keep Alive           18639                18634
        Notifications        0                    0
        Source-Active        0                    0
        Lack of Resource     0
        Last Connection Reset Reason:Reason Unknown
        Notification Message Error Code Received:Unspecified
        Notification Message Error SubCode Received:Not Applicable
        Notification Message Error Code Transmitted:Unspecified
        Notification Message Error SubCode Transmitted:Not Applicable
        Local IP Address:  10.10.10.2
        AO Keychain name:  chain4new
        TCP Connection state: ESTABLISHED

      TCP Keychain name      : chain4new
      TCP-AO Enabled         : YES
      TCP-AO in use          : YES
      Keychain valid         : YES
      No of segments dropped : 0
      Send-Active-Key
      ---------------
        Key-id               : 1
        Crypto Algorithm     : HMAC-SHA1
        Send-id              : 255
        Recv-id              : 255
        Include-tcp-options  : YES
        Accept-ao-mismatch   : YES
      Recv-Active-Key
      ---------------
        Key-id               : 1
        Crypto Algorithm     : HMAC-SHA1
        Send-id              : 255
        Recv-id              : 255
        Include-tcp-options  : YES
        Accept-ao-mismatch   : YES
           Local host:  10.10.10.2, Local  Port: 639
           Remote host: 10.10.10.1, Remote Port: 8746
           ISentSeq: 4196729273  SendNext: 4196785191  TotUnAck:          0
           SendWnd:       16384  TotSent:       55918  ReTrans:        264
           IRcvSeq:  1236641563  RcvNext:  1236697466  RcvWnd:       16384
           TotalRcv:      55903  RcvQue:            0  SendQue:          0
         Input SA Filter:Not Applicable
         Input (S,G) route-map:None
         Input RP route-map:None
         Output SA Filter:Not Applicable
         Output (S,G) route-map:None
         Output RP route-map:None
        SA message Drops:
                 Bad_length        : 0
                 Invalid_VrfIdx    : 0
                 Rpf_Failure_Drop  : 0
                 Wrong_group_Drop  : 0
                 Inbound_sg_Drop   : 0
                 Inbound_rp_Drop   : 0
                 Outbound_sg_Drop  : 0
                 Outbound_rp_Drop  : 0
```

2. Enter the **show ip msdp rpf-peer** command, and enter an IP address, to display MSDP peer information for a reverse-path forwarding (RPF) peer.

```
device> show ip msdp rpf-peer 10.1.1.1

MSDP Peer Status Summary
KA: Keepalive SA:Source-Active NOT: Notification
Peer Address Peer As State KA SA NOT Age
In Out In Out In Out
40.40.40.3 1001 ESTABLISH 62 62 0 0 0 0 7
```

3. Enter the **show ip msdp** command, specifying a VRF, to display information for the source actives in the MSDP cache for a non-default VRF instance.

```
device> show ip msdp vrf my_vrf sa-cache

Total of 10 SA cache entries
Index RP address (Source, Group) Orig Peer Age
1 2.2.2.2 (192.6.1.10, 227.1.1.1) 192.1.1.2 0
2 2.2.2.2 (192.6.1.10, 227.1.1.2) 192.1.1.2 0
3 2.2.2.2 (192.6.1.10, 227.1.1.3) 192.1.1.2 0
4 2.2.2.2 (192.6.1.10, 227.1.1.4) 192.1.1.2 0
5 2.2.2.2 (192.6.1.10, 227.1.1.5) 192.1.1.2 0
6 2.2.2.2 (192.6.1.10, 227.1.1.6) 192.1.1.2 0
7 2.2.2.2 (192.6.1.10, 227.1.1.7) 192.1.1.2 0
8 2.2.2.2 (192.6.1.10, 227.1.1.8) 192.1.1.2 0
9 2.2.2.2 (192.6.1.10, 227.1.1.9) 192.1.1.2 0
10 2.2.2.2 (192.6.1.10, 227.1.1.10) 192.1.1.2 0
```

Clearing MSDP Information

You can clear the following MSDP information:

- Peer information
- Source active cache
- MSDP statistics

Clearing Peer Information

To clear MSDP peer information, enter the following command at the privileged EXEC level of the CLI.

```
device# clear ip msdp peer 205.216.162.1
```

The command in this example clears the MSDP peer connection with MSDP router 205.216.162.1. The CLI displays a message to indicate when the connection has been successfully closed. To clear all the peers, omit the *ip-addr* variable from the command.

Clearing Peer Information on a VRF

To clear the MSDP VRF peers, enter the following command at the MSDP VRF configuration level.

```
device# clear ip msdp vrf blue peer 207.207.162.5
```

Clearing the Source Active Cache

To clear the source active cache, enter the following command at the privileged EXEC level of the CLI.

```
device# clear ip msdp sa-cache
```

The command in this example clears all the cache entries. Use the *ip-addr* variable to clear only the entries matching either a source or a group.

Clearing the Source Active Cache for a VRF

To clear the MSDP VRF source active cache by entering the following command at the MSDP VRF configuration level.

```
device# clear ip msdp sa-cache
 vrf blue
```

Clearing MSDP Statistics

To clear MSDP statistics, enter the following command at the privileged EXEC level of the CLI.

```
device# clear ip msdp statistics
```

The command in this example clears statistics for all the peers. To clear statistics for only a specific peer, enter the IP address of the peer.

Clearing MSDP VRF Statistics

To clear the MSDP VRF statistics by entering the following command.

```
device# clear ip msdp vrf blue sa-cache
```

The command in this example clears all statistics for all the peers in the VRF named blue.

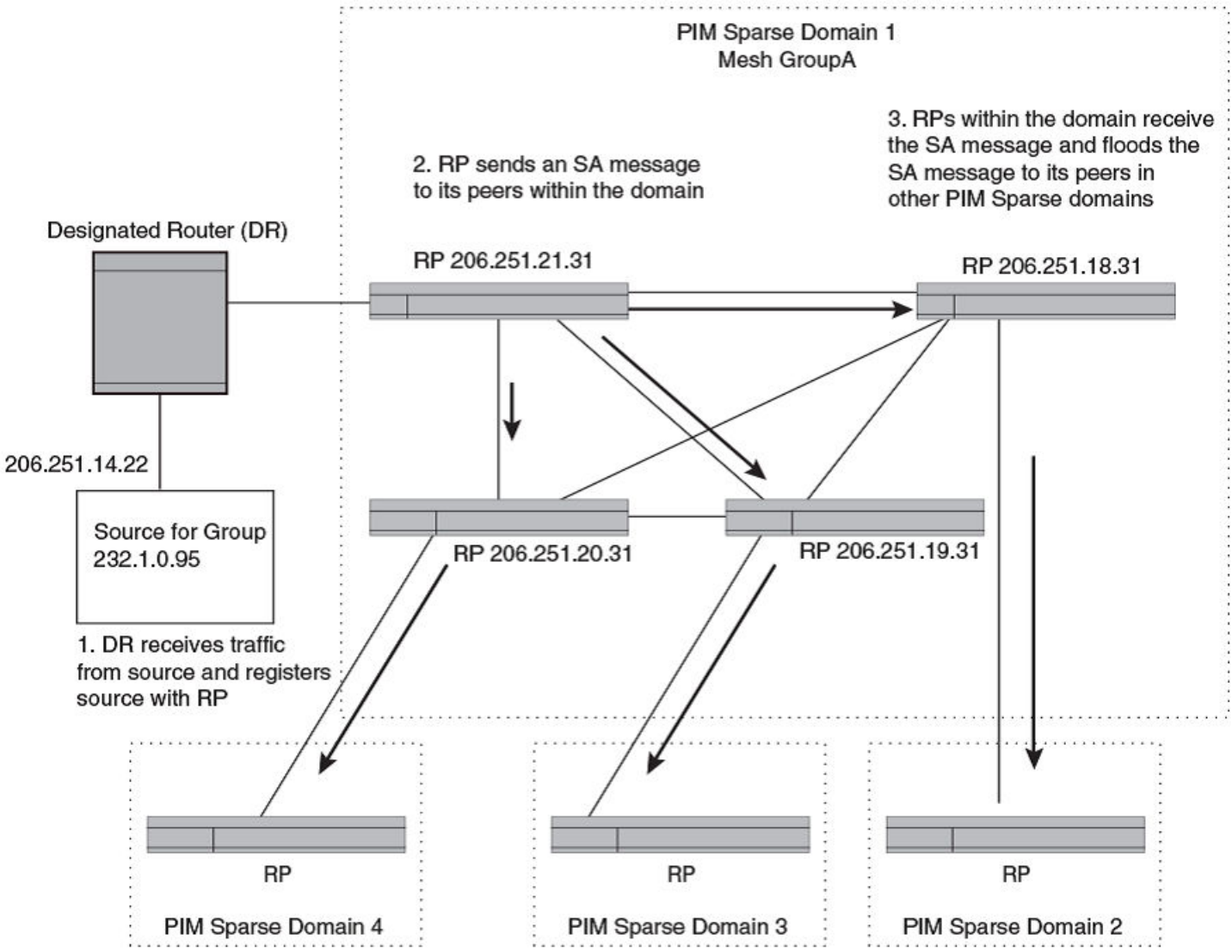
Configuring MSDP Mesh Groups

A PIM Sparse domain can have several RPs that are connected to each other to form an MSDP mesh group. To qualify as a mesh group, the RPs have to be fully meshed; that is, each RP must be connected to all peer RPs in a domain. (Refer to Figure 13.)

A mesh group reduces the forwarding of SA messages within a domain. Instead of having every RP in a domain forward SA messages to all the RPs within that domain, only one RP forwards the SA message. Since an MSDP mesh group is fully meshed, peers do not forward SA messages received in a domain from one member to any member of the group. The RP that originated the SA or the first RP in a domain that receives the SA message is the only one that forwards the message to the members of a mesh group. An RP can forward an SA message to any MSDP router as long as that peer is farther away from the originating RP than the current MSDP router.

The following figure shows an example of an MSDP mesh group. In a PIM-SM mesh group the RPs are configured to be peers of each other. They can also be peers of RPs in other domains.

FIGURE 13 Example of MSDP Mesh Group



PIM Sparse Domain 1 in Figure 13 contains a mesh group with four RPs. When the first RP, for example, RP 206.251.21.31 originates or receives an SA message from a peer in another domain, it sends the SA message to its peers within the mesh group. However, the peers do not send the message back to the originator RP or to each other. The RPs then send the SA message farther away to their peers in other domains. The process continues until all RPs within the network receive the SA message.

Configuring MSDP Mesh Group Example

To configure an MSDP mesh group, you must define MSDP peers and then add the MSDP pers into a mesh group. The configuration must be added on each device in the mesh group.

You first configure the MSDP peers using the **msdp-peer** command to assign their IP addresses and the loopback interfaces.

Next, place the MSDP peers within a domain into a mesh group. Use the **mesh-group** command. There are no default mesh groups. You can have up to 4 mesh groups within a multicast network. A maximum of 32 MSDP peers can be configured per mesh group.

NOTE
On each device that will be part of the mesh group, there must be a mesh group definition for all the peers in the mesh group.

The following sample configuration reflects the configuration in Figure 13 on page 116. On RP 206.251.21.31, you specify its peers within the same domain (206.251.18.31, 206.251.19.31, and 206.251.20.31).

```
device(config)# router msdp
device(config-msdp-router)# msdp-peer 206.251.18.31 connect-source loopback 2
device(config-msdp-router)# msdp-peer 206.251.19.31 connect-source loopback 2
device(config-msdp-router)# msdp-peer 206.251.20.31 connect-source loopback 2
device(config-msdp-router)# mesh-group GroupA 206.251.18.31
device(config-msdp-router)# mesh-group GroupA 206.251.19.31
device(config-msdp-router)# mesh-group GroupA 206.251.20.31
device(config-msdp-router)# exit
```

You can use the **show ip msdp mesh-group** command to view the details of a specific mesh group or the mesh group details for the VRF instance specified by the *vrf-name* variable.

MSDP Anycast RP

MSDP Anycast RP is a method of providing intra-domain redundancy and load-balancing between multiple Rendezvous Points (RP) in a Protocol Independent Multicast Sparse mode (PIM-SM) network. It is accomplished by configuring all RPs within a domain with the same anycast RP address which is typically a loopback IP address. Multicast Source Discovery Protocol (MSDP) is used between all of the RPs in a mesh configuration to keep all RPs in sync regarding the active sources.

PIM-SM routers are configured to register (statically or dynamically) with the RP using the same anycast RP address. Since multiple RPs have the same anycast address, an Interior Gateway Protocol (IGP) such as OSPF routes the PIM-SM router to the RP with the best route. If the PIM-SM routers are distributed evenly throughout the domain, the loads on RPs within the domain will be distributed. If the RP with the best route goes out of service, the PIM-SM router's IGP changes the route to the closest operating RP that has the same anycast address.

This configuration works because MSDP is configured between all of the RPs in the domain. Consequently, all of the RPs share information about active sources.

This feature uses functionality that is already available on the RUCKUS device but repurposes it to provide the benefits desired as described in RFC 3446.

MSDP Anycast RP Configuration

To configure MSDP Anycast RP, you must perform the following tasks:

- Configure a loopback interface with the anycast RP address on each of the RPs within the domain and enable PIM-SM on these interfaces.
- Ensure that the anycast RP address is leaked into the IGP domain. This is typically done by enabling the IGP on the loopback interface (in passive mode) or redistributing the connected loopback IP address into the IGP.

  NOTE
  The anycast RP address must not be the IGP router ID.

- Enable PIM-SM on all interfaces on which multicast routing is desired.
- Enable an IGP on each of the loopback interfaces and physical interfaces configured for PIM-SM.
- Configure loopback interfaces with unique IP addresses on each of the RPs for MSDP peering. This loopback interface is also used as the MSDP originator-id.
- The non-RP PIM-SM routers may be configured to use the anycast RP address statically or dynamically (by the PIMv2 bootstrap mechanism).

Configuring MSDP Anycast RP Example

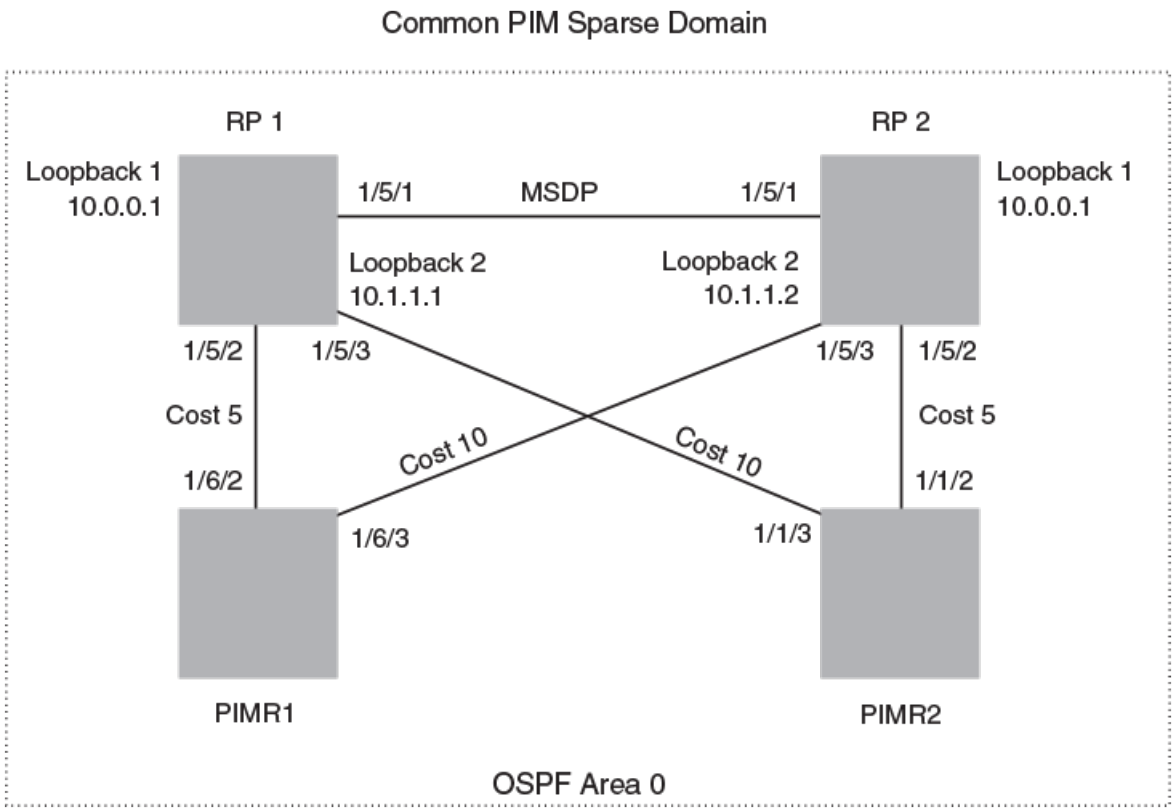
The example shown in Figure 14 is a simple MSDP Anycast-enabled network with two RPs and two PIM-SM routers. Loopback 1 in RP 1 and RP 2 have the same IP address. Loopback 2 in RP1 and Loopback 2 in RP2 have different IP addresses and are configured as MSDP peering IP addresses in a mesh configuration.

In the PIM configuration for PIM-SM routers PIMR1 and PIMR2 the RP address is configured to be the anycast RP address that was configured on the Loopback 1 interfaces on RP1 and RP2. OSPF is configured as the IGP for the network and all of the devices are in OSPF area 0.

Since PIMR1 has a lower cost path to RP1 and PIMR2 has a lower cost path to RP2 they will register with the respective RPs when both are up and running. This shares the load between the two RPs. If one of the RPs fails, the higher-cost path to the IP address of Loopback 1 on the RPs is used to route to the still-active RP.

The configuration examples demonstrate the commands required to enable this application.

FIGURE 14 Example of an MDSP Anycast RP Network



RP 1 Configuration

The following commands provide the configuration for the RP 1 router in Figure 14.

```
RP1(config)# router ospf
RP1(config-ospf-router)# area 0
RP1(config-ospf-router)# exit
RP1(config)# interface loopback 1
RP1(config-lbif-1)# ip ospf area 0
RP1(config-lbif-1)# ip ospf passive
RP1(config-lbif-1)# ip address 10.0.0.1/32
RP1(config-lbif-1)# ip pim-sparse
```

```
RP1(config-lbif-1)# exit
RP1(config)# interface loopback 2
RP1(config-lbif-2)# ip ospf area 0
RP1(config-lbif-2)# ip ospf passive
RP1(config-lbif-2)# ip address 10.1.1.1/32
RP1(config-lbif-2)# exit
RP1(config)# interface ethernet 1/5/1
RP1(config-if-e1000-1/5/1)# ip ospf area 0
RP1(config-if-e1000-1/5/1)# ip address 192.1.1.1/24
RP1(config-if-e1000-1/5/1)# ip pim-sparse
RP1(config)# interface ethernet 1/5/2
RP1(config-if-e1000-1/5/2)# ip ospf area 0
RP1(config-if-e1000-1/5/2)# ip ospf cost 5
RP1(config-if-e1000-1/5/2)# ip address 192.2.1.1/24
RP1(config-if-e1000-1/5/2)# ip pim-sparse
RP1(config)# interface ethernet 1/5/3
RP1(config-if-e1000-1/5/3)# ip ospf area 0
RP1(config-if-e1000-1/5/3)# ip ospf cost 10
RP1(config-if-e1000-1/5/3)# ip address 192.3.1.1/24
RP1(config-if-e1000-1/5/3)# ip pim-sparse
RP1(config-if-e1000-1/5/3)# exit
RP1(config)# router pim
RP1(config-pim-router)# rp-candidate loopback 1
RP1(config-pim-router)# exit
RP1(config)# router msdp
RP1(config-msdp-router)# msdp-peer 10.1.1.2 connect-source loopback 2
RP1(config-msdp-router)# originator-id loopback 2
```

RP 2 Configuration

The following commands provide the configuration for the RP 2 router in Figure 14.

```
RP2(config)# router ospf
RP2(config-ospf-router)# area 0
RP2(config-ospf-router)# exit
RP2(config)# interface loopback 1
RP2(config-lbif-1)# ip ospf area 0
RP2(config-lbif-1)# ip ospf passive
RP2(config-lbif-1)# ip address 10.0.0.1/32
RP2(config-lbif-1)# ip pim-sparse
RP2(config-lbif-1)# exit
RP2(config)# interface loopback 2
RP2(config-lbif-2)# ip ospf area 0
RP2(config-lbif-2)# ip ospf passive
RP2(config-lbif-2)# ip address 10.1.1.2/32
RP2(config-lbif-2)# exit
RP2(config)# interface ethernet 1/5/1
RP2(config-if-e1000-1/5/1)# ip ospf area 0
RP2(config-if-e1000-1/5/1)# ip address 192.1.1.2/24
RP2(config-if-e1000-1/5/1)# ip pim-sparse
RP2(config)# interface ethernet 1/5/2
RP2(config-if-e1000-1/5/2)# ip ospf area 0
RP2(config-if-e1000-1/5/2)# ip ospf cost 5
RP2(config-if-e1000-1/5/2)# ip address 192.5.2.1/24
RP2(config-if-e1000-1/5/2)# ip pim-sparse
RP2(config)# interface ethernet 1/5/3
RP2(config-if-e1000-1/5/3)# ip ospf area 0
RP2(config-if-e1000-1/5/3)# ip ospf cost 10
RP2(config-if-e1000-1/5/3)# ip address 192.6.1.2/24
RP2(config-if-e1000-1/5/3)# ip pim-sparse
RP2(config-if-e1000-1/5/3)# exit
RP2(config)# router pim
RP2(config-pim-router)# rp-candidate loopback 1
RP2(config-pim-router)# exit
RP2(config)# router msdp
RP2(config-msdp-router)# msdp-peer 10.1.1.1 connect-source loopback 2
RP2(config-msdp-router)# originator-id loopback 2
```

PIMR1 Configuration

The following commands provide the configuration for the PIMR1 router in Figure 14.

```
PIMR1(config)# router ospf
PIMR1(config-ospf-router)# area 0
PIMR1(config-ospf-router)# exit
PIMR1(config)# interface ethernet 1/6/2
PIMR1(config-if-e1000-1/6/2)# ip ospf area 0
PIMR1(config-if-e1000-1/6/2)# ip ospf cost 5
PIMR1(config-if-e1000-1/6/2)# ip address 192.2.1.2/24
PIMR1(config-if-e1000-1/6/2)# ip pim-sparse
PIMR1(config)# interface ethernet 1/6/3
PIMR1(config-if-e1000-1/6/3)# ip ospf area 0
PIMR1(config-if-e1000-1/6/3)# ip ospf cost 10
PIMR1(config-if-e1000-1/6/3)# ip address 192.6.1.1/24
PIMR1(config-if-e1000-1/6/3)# ip pim-sparse
PIMR1(config-if-e1000-1/6/3)# exit
PIMR1(config)# router pim
PIMR1(config-pim-router)# rp-address 10.0.0.1
PIMR1(config-pim-router)# exit
```

PIMR2 Configuration

The following commands provide the configuration for the PIMR2 router in Figure 14.

```
PIMR2(config)# router ospf
PIMR2(config-ospf-router)# area 0
PIMR2(config-ospf-router)# exit
PIMR2(config)# interface ethernet 1/1/2
PIMR2(config-if-e1000-1/1/2)# ip ospf area 0
PIMR2(config-if-e1000-1/1/2)# ip ospf cost 5
PIMR2(config-if-e1000-1/1/2)# ip address 192.5.2.2/24
PIMR2(config-if-e1000-1/1/2)# ip pim-sparse
PIMR2(config)# interface ethernet 1/1/3
PIMR2(config-if-e1000-1/1/3)# ip ospf area 0
PIMR2(config-if-e1000-1/1/3)# ip ospf cost 10
PIMR2(config-if-e1000-1/1/3)# ip address 192.3.1.2/24
PIMR2(config-if-e1000-1/1/3)# ip pim-sparse
PIMR2(config-if-e1000-1/1/3)# exit
PIMR2(config)# router pim
PIMR2(config-pim-router)# rp-address 10.0.0.1
PIMR2(config-pim-router)# exit
```

PIM Anycast RP

PIM Anycast RP is a method of providing load balancing and fast convergence to PIM RPs in an IPv4 multicast domain. The RP address of the Anycast RP is a shared address used among multiple PIM routers, known as PIM RP. The PIM RP routers create an Anycast RP set. Each router in the Anycast RP set is configured using two IP addresses; a shared RP address in their loopback address and a separate, unique ip address. The loopback address must be reachable by all PIM routers in the multicast domain. The separate, unique ip address is configured to establish static peering with other PIM routers and communication with the peers.

When the source is activated in a PIM Anycast RP domain, the PIM First Hop (FH) will register the source to the closet PIM RP. The PIM RP follows the same MSDP Anycast RP operation by decapsulating the packet and creating the (S,G) state. If there are external peers in the Anycast RP set, the router will re-encapsulate the packet with the local peering address as the source address of the encapsulation. The router will unicast the packet to all Anycast RP peers. The re-encapsulation of the data register packet to Anycast RP peers ensures source state distribution to all RPs in a multicast domain.

Configuring PIM Anycast RP

PIM Anycast RP can be configured to map RP and Anycast RPs.

NOTE
MSDP and Anycast RP do not interoperate. If transitioning from MSDP to Anycast RP or vice versa, all RPs in the network must be configured for the same method of RP peering; either Anycast RP or MSDP.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable PIM

```
device(config)# router pim
```

3. Configure an RP address.

```
device(config-pim-router)# rp-address 100.1.1.1
```

The RP address is shared among multiple PIM routers.

4. Configure PIM Anycast RP.

```
device(config-pim-router)# anycast-rp 100.1.1.1 my-anycast-rp-set-acl
```

The **anycast-rp** command defines the mapping of the RP and the Anycast RP peers using a host-based simple ACL to specify the address of the Anycast RP set.

5. Exit to privileged EXEC mode.

```
device(config-pim-router)# end
```

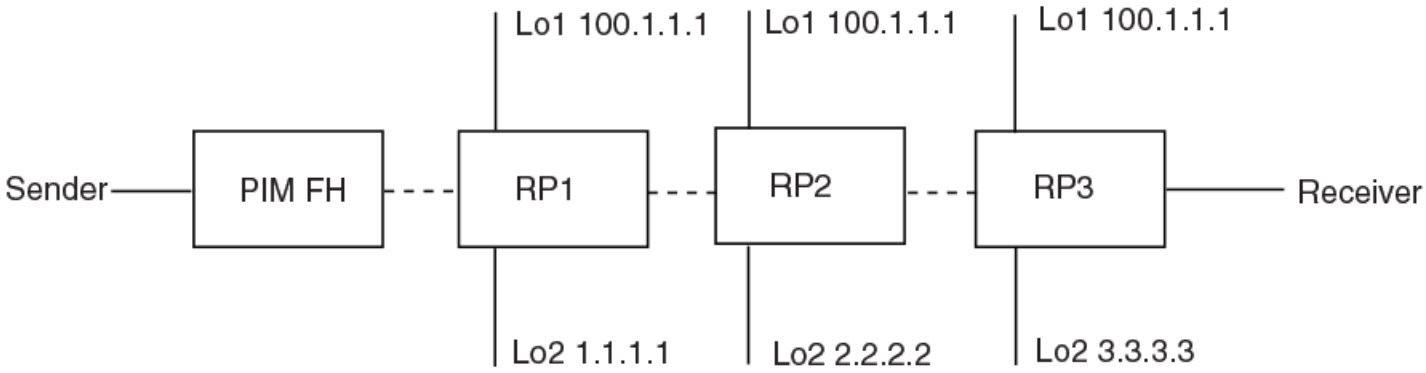
6. Display information for a PIM Anycast RP interface.

```
device> show ip pim anycast-rp

Number of Anycast RP: 1
Anycast RP: 100.1.1.1
  ACL Name: 200
  Peer List:
    1.1.1.1
    2.2.2.2
    3.3.3.3
```

The example shown in the following figure is a PIM Anycast-enabled network with 3 RPs, 1 PIM-FH router connecting to its active source and local receiver. Loopback 2 in RP1, RP2, and RP3 have the same IP addresses 100.1.1.1. Loopback 3 in RP1, RP2, and RP3 each have separate IP addresses configured to communicate with their peers in the Anycast RP set.

FIGURE 15 Example of a PIM Anycast RP Network



The following example is a configuration of PIM Anycast RP 100.1.1.1.The example avoids using loopback 1 interface when configuring PIM Anycast RP because the loopback 1 address could be used as a router-id. A PIM First Hop router will register the source with the closest RP. The first RP that receives the register will re-encapsulate the register to all other Anycast RP peers.

The RP shared address 100.1.1.1 is used in the PIM domain. IP addresses 1.1.1.1, 2.2.2.2, and 3.3.3.3 are listed in the ACL that forms the self inclusive Anycast RP set. Multiple anycast-rp instances can be configured on a system; each peer with the same or different Anycast RP set.

> **NOTE**
> The PIM software supports up to eight PIM Anycast-RP routers. All deny statements in the anycast_rp_set ACL and additional routers more than eight listed in an access list are ignored.

```
device# configure terminal
device(config)# interface loopback 2
device(config-lbif-2)# ip address 100.1.1.1/24
device(config-lbif-2)# ip pim-sparse
device(config-lbif-2)# interface loopback 3
device(config-lbif-3)# ip address 1.1.1.1/24
device(config-lbif-3)# ip pim-sparse
device(config-lbif-3)# router pim
device(config-pim-router)# rp-address 100.1.1.1
device(config-pim-router)# anycast-rp 100.1.1.1 my-anycast-rp-set
device(config-pim-router)# ip access-list standard my-anycast-rp-set
device(config-std-ipacl-my-anycast-rp-set)# permit host 1.1.1.1
device(config-std-ipacl-my-anycast-rp-set)# permit host 2.2.2.2
device(config-std-ipacl-my-anycast-rp-set)# permit host 3.3.3.3
```

IPv4 PIM Join and Prune Policy

The IPv4 PIM Join and Prune Policy provides the capability for the following options to be configured:.

- (RP, G) J/P filtering: Permit or deny PIM (*, G) J/P messages for IP multicast group addresses with a given RP.
- (*, G) J/P filtering: Permit or deny PIM (*, G) J/P messages for IP multicast group addresses independent of RP.
- (S, G) J/P filtering: Permit or deny PIM (S, G) J/P messages for IP multicast sources and group addresses.

Access control lists (ACLs) are used to define the policy.

By default, all PIM devices accept Join and Prune messages for all the multicast group addresses and for all source addresses. When the IPv4 PIM Join and Prune policy is configured, a PIM network is prevented from forwarding multicast traffic for reserved or unauthorized groups, which could lead to the overuse of available bandwidth of the links and the overuse of software or hardware resources on PIM routers.

With the IPv4 PIM Join and Prune policy, a PIM-SM device can be configued to drop PIM J/P messages of the following types::

- (*, G) sent to a given RP for unauthorized groups.
- (*, G) for unauthorized groups independent of RP.
- (S, G) for unauthorized groups and sources.

Configuration Notes and Feature Limiations

- A (RP, G) configuration is limited to 64 IPv4 RPs and 64 IPv6 RPs per VRF. Though ICX can support more than 64 RPs (learned dynamically through Bootstrap Protocol), there is a limited number of RPs generally in a given network.
- Standard and extended ACLs are supported for IPv4 (RP, G). Group addresses and prefixes can be configured as the the source IP addresses in the standard ACL rules.
- ACL rules are used to configure which multicast group addresses (*, G) are sent to the RP, and which are to be dropped or allowed. Multicast group address and prefixes are configured as destination IP addresses and prefixes in the extended ACL rules. Because this ACL is used for (RP, G) filtering, the source IP addresses and prefixes in the case of extended ACL rules are ignored.
- Only one ACL can be applied to an RP address.
- If the specified ACL is not configured, then the (*, G) Join and Prune messages sent to that RP for all multicast group addresses are dropped.
- Only one ACL can be applied to both (*, G) and (S, G) Join and Prune filtering at a time.

Configuring IPv4 PIM Join and Prune Policy

IPv4 PIM Join and Prune policies can be configured.

The following task configures the PIM (RP, G) jp-policy.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable PIM globally.

```
device(config)# router pim
```

3. Configure the IPv4 PIM Join and Prune policy, specifying an RP address and an ACL list.

```
device(config-router-pim)# jp-policy 10.9.9.9 1
```

4. Configure the IPv4 PIM Join and Prune policy, specifying another RP address and an ACL list.

```
device(config-router-pim)#  jp-policy 22.9.9.9 22
```

5. Configure the IPv4 PIM Join and Prune policy, specifying another RP address and an ACL list.

```
device(config-router-pim)# jp-policy 100.9.9.9 1
```

The following example configures the PIM (RP, G) Join and Prune policy. An ACL number is specified.

```
device# configure terminal
device(config)# router pim
device(config-router-pim)# jp-policy 10.9.9.9 1
device(config-router-pim)# jp-policy 22.9.9.9 22
device(config-router-pim)# jp-policy 100.9.9.9 1
```

The following example configures the PIM (RP, G) Join and Prune policy for a non-default VRF instance. An ACL number is specified.

```
device# configure terminal
device# router pim vrf blue
device# (config-pim-router-vrf-blue)# jp-policy 10.9.9.9 1
device(config-pim-router-vrf-blue)# jp-policy 22.9.9.9 22
device(config-pim-router-vrf-blue)# jp-policy 100.9.9.9 1
```

The following example configures the PIM (*, G) and (S, G) Join and Prune policy for the default VRF. An ACL name is specified.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# jp-policy wg-sg-acl
```

The following example unconfigures a previously configured PIM (RP, G) Join and Prune policy for a non-default VRF instance.

```
device(config)# router pim vrf blue
device(config-pim-router-vrf-blue)# no jp-policy 10.9.9.9    1
device(config-pim-router-vrf-blue)# no jp-policy 22.9.9.9    22
device(config-pim-router-vrf-blue)# no jp-policy 100.9.9.9   1
```

The following example unconfigures a previously configured PIM (*, G) and (S, G) Join and Prune policy.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# no jp-policy wg-sg-acl
```

Displaying PIM Information

You can use various **show** commands to view information about PIM.

Use one of the following commands to view PIM information. The commands do not need to be entered in the specified order. Using these commands is optional and they can be entered in any order. For more information on the full list of **show ip pim** commands, refer to the *RUCKUS FastIron Command Reference*.

1. Enter the **show ip pim counter nsr** command to display multicast non-stop routing (NSR) counter and statistics information.

```
device> show ip pim counter nsr

Mcache sync (entity id: 203)
  pack: 0
  unpack: 0
  ack: 0
RPset sync (entity id: 201)
  pack: 0
  unpack: 0
  ack: 0
BSR status (entity id: 202)
  pack: 1
  unpack: 0
  ack: 1
```

2. Enter the **show ip pim nsr** command to display the multicast non-stop routing (NSR) status.

```
device> show ip pim nsr

Global Mcast NSR Status
  NSR: ON
  Switchover In Progress Mode: FALSE
```

3. Enter the **show ip pim interface** command to display information for PIM interfaces.

```
device> show ip pim interface

Flags    : SM  - Sparse Mode v2, DM - Dense Mode v2, P - Passive Mode

--------+---------------+-----+---+-------+---+-----+-------+-------+----+--------+

Int'face|Local          |Mode |St |Des Rtr|TTL|Mcast| Filter| VRF   |DR  |Override
        |Address        |     |   |AddPort|Thr|Bndry|  ACL  |       |Prio|Interval
--------+---------------+-----+---+-------+---+-----+-------+-------+----+--------+
e1/1/1   5.5.5.5         SM   Ena  Itself   1  None   None   default  1   3000ms
e1/1/9   15.1.1.5        SM   Ena  Itself   1  None   10     default  1   3000ms
e1/1/12  12.12.12.1      SM   Dis  Itself   1  None   None   default  1   3000ms
v20      21.21.21.22     SM   Ena  Itself   1  None   None   default  1   3000ms
v60      60.60.60.1      SM   Ena  Itself   1  None   None   default  1   3000ms
v310     110.110.110.2   SM   Dis  Itself   1  None   None   default  1   3000ms
v360     160.160.160.1   SM   Dis  Itself   1  None   None   default  1   3000ms
l2       4.4.4.4         SM   Ena  Itself   1  None   None   default  1   3000ms
l3       10.10.10.10     SM   Ena  Itself   1  None   None   default  1   3000ms
Total Number of Interfaces : 9
```

4. Enter the **show ip pim sparse** command to display PIM Sparse configuration information.

```
device> show ip pim sparse
Global PIM Sparse Mode Settings
Maximum Mcache         : 12288       Current Count             : 0
Hello interval         : 30          Neighbor timeout          : 105
Join/Prune interval    : 60          Inactivity interval       : 180
Hardware Drop Enabled  : Yes         Prune Wait Interval       : 3
Bootstrap Msg interval : 60          Candidate-RP Msg interval : 60
Register Suppress Time : 60          Register Probe Time       : 10
Register Stop Delay    : 10          SPT Threshold             : 1
Join/Prune Policy     : Yes
SSM Enabled            : No
Route Precedence       : mc-non-default mc-default uc-non-default uc-default
Slow Path Disable All  : No          Slow Path Enable SSM      : No
Slow Path Filter Acl   : None
```

5. Enter the **show ip pim bsr** command to display bootstrap router (BSR) information. The following example shows information for a device that has been elected as the BSR.

```
device> show ip pim bsr

PIMv2 Bootstrap information for Vrf Instance : default-vrf
------------------------------------------------------------------------------
  This system is the Elected BSR
  BSR address: 1.51.51.1. Hash Mask Length 32. Priority 255.
  Next bootstrap message in 00:01:00
  Configuration:
    Candidate loopback 2 (Address 1.51.51.1). Hash Mask Length 32. Priority 255.
Next Candidate-RP-advertisment in 00:01:00
  RP: 1.51.51.1
    group prefixes:
    224.0.0.0 / 4
  Candidate-RP-advertisement period: 60
```

6. Enter the **show ip pim neighbor** command to display information about PIM neighbors.

```
device> show ip pim neighbor

--------+--------+---------------+--------+---+---------+---------+-----+------------+-----------
+----
Port    |PhyPort |Neighbor       |Holdtime|T  |PropDelay|Override |Age  |UpTime      |VRF        |
Prio
        |        |               |sec     |Bit|msec     |msec     |sec  |            |
|
--------+--------+---------------+--------+---+---------+---------+-----+------------+-----------
+----
v2       e1/1/1     2.1.1.2         105      1   500       3000      0     00:44:10  default-vrf
1
v4       e1/2/2     4.1.1.2         105      1   500       3000      10    00:42:50  default-vrf
1
v5       e1/1/4     5.1.1.2         105      1   500       3000      0     00:44:00  default-vrf
1
v22      e1/1/1     22.1.1.1        105      1   500       3000      0     00:44:10  default-vrf
1
Total Number of Neighbors : 4
```

7. Enter the **show ip pim traffic** command to display information about IPv4 PIM traffic statistics.

```
device> show ip pim traffic

Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Rx        Rx          Rx        Rx        Rx        Rx        Rx        Rx
------+---------+-----------+---------+---------+---------+---------+---------+---
v30     0         0           0         0         0         0         0         0
v50     2526      1260        0         0         0         1263      0         0
v150    2531      0           0         0         0         1263      0         0
v200    2531      0           0         0         0         1         0         0
Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Tx        Tx          Tx        Tx        Tx        Tx        Tx
------+---------+-----------+---------+---------+---------+---------+---------+---
v30     2528      0           0         0         0         0         0
v50     2540      1263        0         0         0         2         0
v150    2529      0           0         0         0         1262      0
v200    2529      0           0         0         0         1262      0
```

8. Enter the **show ip pim dense** command to display PIM Dense configuration information.

```
device> show ip pim dense

Global PIM Dense Mode Settings
  Maximum Mcache            : 12992    Current Count                     : 2
  Hello interval            : 30       Neighbor timeout                  : 105
  Join/Prune interval       : 60       Inactivity interval               : 180
  Hardware Drop Enabled     : Yes      Prune Wait Interval               : 3
  Graft Retransmit interval : 180      Prune Age                         : 180
  Route Precedence          : mc-non-default mc-default uc-non-default uc-default
```

9. Enter the **show ip pim prune** command to display multicast cache entries that are currently in a pruned state and have not yet aged out.

```
device> show ip pim prune

    1 (104.1.1.2 231.0.1.1):
   e1/2/2,1/2/2(150)
    2 (108.1.1.100 231.0.1.1):
   e1/2/2,1/2/2(150)
    3 (104.1.1.2 231.0.1.2):
   e1/2/2,1/2/2(150)
    4 (108.1.1.100 231.0.1.2):
   e1/2/2,1/2/2(150)
    5 (108.1.1.100 231.0.1.3):
   e1/2/2,1/2/2(150)
    6 (104.1.1.2 231.0.1.4):
   e1/2/2,1/2/2(150)
    7 (108.1.1.100 231.0.1.4):
   e1/2/2,1/2/2(150)
    8 (104.1.1.2 231.0.1.5):
   e1/2/2,1/2/2(150)
    9 (108.1.1.100 231.0.1.5):
   e1/2/2,1/2/2(150)
Total Prune entries: 9
```

10. Enter the **show ip pim mcache** command to display the PIM multicast cache.

```
device> show ip pim mcache

IP Multicast Mcache Table
Entry Flags : SM - Sparse Mode, SSM - Source Specific Multicast, DM - Dense Mode
       RPT - RPT Bit, SPT - SPT Bit, LSRC - Local Source, LRCV - Local Receiver
       HW - HW Forwarding Enabled, FAST - Resource Allocated, TAG - Need For
        Replication Entry
       REGPROB - Register In Progress, REGSUPP - Register Suppression Timer
       MSDPADV - Advertise MSDP, NEEDRTE - Route Required for Src/RP, PRUN - DM
        Prune Upstream
Interface Flags: IM - Immediate, IH - Inherited, WA - Won Assert
       MJ - Membership Join, MI - Membership Include, ME - Membership Exclude
       BR - Blocked RPT, BA - Blocked Assert, BF - Blocked Filter, BI - Blocked IIF
Total entries in mcache: 20
1  (140.140.140.3, 225.0.0.1) in v340 (tag e1/8/1), Uptime 00:00:02
  Source is directly connected
  Flags (0x200004e1) DM HW FAST TAG
  fast ports: ethe 1/4/6 ethe 1/8/26
  AgeSltMsk: 1, L2 FID: 8188, DIT: 3
  Forwarding_oif: 2
  L3 (HW) 2:
    TR(e1/4/6,e1/4/6)(VL330), 00:00:02/0, Flags: IM
    e1/8/26(VL310), 00:00:02/0, Flags: IM
  Src-Vlan: 340
```

11. Enter the **show ip pim mcache** command with the **dit-dx** keyword, and specify a value, to display the PIM multicast cache for the specified DIT.

```
device> show ip pim mcache dit-idx 414

IP Multicast Mcache Table
Entry Flags    : SM  - Sparse Mode, SSM - Source Specific Multicast, DM - Dense Mode
                 RPT    - RPT Bit, SPT - SPT Bit, LSRC - Local Source, LRCV - Local Receiver
                 HW - HW Forwarding Enabled, FAST - Resource Allocated, TAG - Need For Replication
Entry
                 REGPROB - Register In Progress, REGSUPP - Register Suppression Timer
                 MSDPADV - Advertise MSDP, NEEDRTE - Route Required for Src/RP,  PRUN - DM Prune
Upstream
Interface Flags: IM - Immediate, IH - Inherited, WA - Won Assert
                 MJ - Membership Join, MI - Membership Include, ME - Membership Exclude
                 BR - Blocked RPT, BA - Blocked Assert, BF - Blocked Filter, BI - Blocked IIF
Total entries in mcache: 30
1     (20.20.20.100, 225.1.1.1) in v220 (tag e1/1/13), Uptime 07:12:07
      upstream neighbor 220.220.220.1
      Flags (0x200680e1) SM SPT LRCV HW FAST TAG
      fast ports: ethe 1/1/11
      AgeSltMsk: 1,  IPMC:   414 , RegPkt: 0
      Forwarding_oif: 1, Immediate_oif: 0, Blocked_oif: 0
      L3 (HW) 1:
          e1/1/11(VL40), 07:12:07/0, Flags: MJ
      Src-Vlan: 220
2     (20.20.20.100, 225.1.1.2) in v220 (tag e1/1/13), Uptime 00:01:00
      upstream neighbor 220.220.220.1
      Flags (0x200680e1) SM SPT LRCV HW FAST TAG
      fast ports: ethe 1/1/11
      AgeSltMsk: 1, IPMC:   414 , RegPkt: 0
      Forwarding_oif: 1, Immediate_oif: 0, Blocked_oif: 0
      L3 (HW) 1:
          e1/1/11(VL40), 00:01:00/0, Flags: MJ
      Src-Vlan: 220
3     (20.20.20.100, 225.1.1.3) in v220 (tag e1/1/13), Uptime 00:01:00
      upstream neighbor 220.220.220.1
      Flags (0x200680e1) SM SPT LRCV HW FAST TAG
      fast ports: ethe 1/1/11
      AgeSltMsk: 1, IPMC:   414 , RegPkt: 0
      Forwarding_oif: 1, Immediate_oif: 0, Blocked_oif: 0
      L3 (HW) 1:
          e1/1/11(VL40), 00:01:00/0, Flags: MJ
      Src-Vlan: 220
```

12. Enter the **show ip pim jp-policy** command to display PIM (RP, G), (*, G), and (S, G) Join and Prune policy configuration information and the number of Join and Prune drops for each such policy.

```
device> show ip pim jp-policy

Vrf Instance : default-vrf
---------------------------

(RP, G) JP policy
---------

(RP, G) JP policy count: 3

RP-Address       ACL Name (RP, G)       Join Drops (RP, G)         Prune Drops
10.9.9.9           rp-wg-acl                 1500                      499
22.9.9.9              22                     1888                      1000
100.9.9.9            122                     921                        300
---------------------------

(*, G) and (S, G) JP policy
---------

ACL Name (*, G)        Join Drops (*, G)        Prune Drops (S, G)           Join Drops (S,
G)          Prune Drops
wg-sg-acl                   1500                     499
385                      139
```

13. Enter the **show ip pim rp-set** command to display RP-set list for the device elected as the bootstrap router (BSR).

```
device> show ip pim rp-set

Static RP and associated group ranges
-------------------------------------
Static RP count: 4
130.1.1.1
120.1.1.1
120.2.1.1
124.1.1.1
Number of group prefixes Learnt from BSR: 0
No RP-Set present.
```

14. Enter the **show ip pim rp-map** command to display RP-to-group mapping.

```
device> show ip pim rp-map

Number of group-to-RP mappings: 5
-----------------------------------------
S.No  Group address                      RP address
-----------------------------------------
1     225.1.1.1                          25.0.0.25
2     225.1.1.2                          25.0.0.25
3     225.1.1.3                          25.0.0.25
4     225.1.1.4                          25.0.0.25
5     225.1.1.5                          25.0.0.25
```

15. Enter the **show ip pim anycast-rp** command to display information for a PIM Anycast RP interface.

```
device> device> show ip pim anycast-rp

Number of Anycast RP: 1
Anycast RP: 100.1.1.1
  ACL Name: 200
  Peer List:
    1.1.1.1
    2.2.2.2
    3.3.3.3
```

16. Enter the **show ip pim error** command to display information for PIM error counters.

```
device> show ip pim error
Vrf Instance : default-vrf
-----------------------------------
Protocol errors:
PIM_PKT_DRP    : 0  PIM_PKT_DRP(Glb)        : 0
MCGRP_PKT_DRP : 0  MCGRP_PKT_DRP(Glb)      : 0
PIM_THR_DRP    : 0  PIM_THR_DRP(Glb)        : 0
MCGRP_THR_DRP : 0  MCGRP_THR_DRP(Gl)       : 0
RPSET_MAXED    : 0  Join/Prune Drops       : 1999

Forwarding Errors (Packet Drops):
RPF-Fail: 0 No-RP    : 0 IfMsmtch: 0
OIFEmpty: 0 InvldIf  : 0 TTLXpire: 0
NoFwEntr: 0 TrkMove  : 0 PortMove: 0
NoCause : 0 FwEntrFl: 0 ResFail : 0
SSMNoEnt: 0 InvldGrp: 0 Bidir    : 0
WrongIf : 0 IPCError: 0 IPCBufEr: 0
DMACErr : 0
```

Static Multicast Routes

Configure static multicast routes to control the network paths, administrative distance, and precedence for multicast routes.

Static multicast routes allow you to control the network path used by multicast traffic. Static multicast routes are especially useful when the unicast and multicast topologies of a network are different. By configuring static multicast routes you do not have to make the topologies similar.

> **NOTE**
> In IP multicasting, source IP addresses are unicast addresses while destination IP addresses are multicast (group) addresses. Therefore, in IP multicasting, a route lookup is done for source IP address, rather than its destination IP address.

You can configure more than one static multicast route. The device always uses the most specific route that matches a multicast source address. Thus, if you want to configure a multicast static route for a specific multicast source and also configure another multicast static route for all other sources, you can configure two static routes

Configure the **distance** keyword in the **ip mroute** command to specify the administrative distance, which the device uses to determine the best path for a route. When comparing multiple paths for a route, the device prefers the path with the lower administrative distance. To ensure that the default static route is used, configure a low administrative distance value. However, the device prefers directly connected routes over other routes, no matter what the administrative distance.

Configure the **route-precedence** command to specify a precedence table that dictates how routes are selected for multicast.

IGMP Proxy

IGMP Proxy provides a means for routers to receive any or all multicast traffic from an upstream device if the router is not able to run PIM and runs only IGMP. IGMP Proxy supports IGMPv1, IGMPv2, and IGMPv3.

IGMP Proxy enables the router to issue IGMP host messages on behalf of hosts that the router discovered through standard PIM interfaces. The router acts as a proxy for its hosts and performs the host portion of the IGMP task on the upstream interface in the following situations:

- When queried, the router sends group membership reports for the groups learned.
- When one of its hosts joins a multicast address group to which none of its other hosts belong, the router sends unsolicited membership reports to that group.

- When the last of its hosts in a particular multicast group leaves the group, the router sends an unsolicited leave group membership report to group (multicast IP address 224.0.0.2).

IGMP Proxy Configuration Notes

When using IGMP Proxy, you must note the following considerations:.

- Configure PIM on all multicast client ports to build the group membership table. The group membership table will be reported by the proxy interface. Refer to the **ip pim passive** command in the *RUCKUS FastIron Command Reference* for more information on configuring PIM.
- Enable IP multicast on an interface to an upstream router that will be the IGMP proxy interface and configure IGMP Proxy on that interface. Refer to Configuring IGMP Proxy on page 131 for more information.

IGMP Proxy Limitations

- IGMP Proxy cannot be enabled on the same interface on which PIM SM or PIM DM is enabled.
- IGMP Proxy is only supported in a PIM Dense environment where there are IGMP clients connected to the RUCKUS device. The RUCKUS device does not send IGMP reports on an IGMP proxy interface for remote clients connected to a PIM neighbor,because it is not aware of groups that the remote clients are interested in. Static groups on the other PIM interfaces are included in proxy reports.
- PIM DM must be enabled in passive mode. This is a change from the previous implementation; to be backward compatible, PIM-DM passive mode is enabled in passive mode indirectly if PIM-DM is not enabled explicitly.

Configuring IGMP Proxy

Perform the following steps to configure IGMP Proxy from global configuration mode.

1. Configure PIM globally on the router device.

```
device(config)# router pim
```

2. Configure an interface (physical, virtual routing, or tunnel interface) that will serve as the IGMP proxy for an upstream device.

```
device(config)# interface ethernet 1/1/3
```

3. Configure an IP address on Ethernet interface 1/1/3.

```
device(config-if-e1000-1/1/3)# ip address 10.95.5.1/24
```

4. Enable PIM in passive mode on the interface.

```
device(config-if-e1000-1/1/3)# ip pim passive
```

5. Enable IGMP Proxy on the interface.

```
device(config-if-e1000-1/1/3)# ip igmp proxy
```

Filtering Groups in Proxy Report Messages

Once IGMP Proxy is configured and the router receives a query on an IGMP proxy interface, the router sends a report in response to the query before the IGMP maximum response time expires.

You can filter out groups in proxy report messages by specifying an access list name or number. This task assumes that an access list has been created to filter out one or more groups.

1. Configure PIM globally on the router device.

```
device(config)# router pim
```

2. Configure an interface (physical, virtual routing, or tunnel interface) that will serve as the IGMP proxy for an upstream device.

```
device(config)# interface ethernet 1/1/3
```

3. Configure an IP address on Ethernet interface 1/1/3.

```
device(config-if-e1000-1/1/3)# ip address 10.95.5.1/24
```

4. Enable PIM in passive mode on the interface.

```
device(config-if-e1000-1/1/3)# ip pim passive
```

5. Filter out groups in proxy report messages using an access list.

```
device(config-if-e1000-1/1/3)# ip igmp proxy group-filter ACL1
```

The following example configures IGMP Proxy and filters out groups in proxy report messages using the ACL1 access list.

```
device(config)# router pim
device(config)# interface ethernet 1/1/3
device(config-if-e1000-1/1/3)# ip address 10.95.5.1/24
device(config-if-e1000-1/1/3)# ip pim passive
device(config-if-e1000-1/1/3)# ip igmp proxy group-filter ACL1
```

Displaying IGMP Proxy Information

You can use various **show** commands to view information about proxy groups and interfaces .

Use one of the following commands to view information about the proxy groups and interfaces on the default VRF. The commands do not need to be entered in the specified order. Using these commands is optional and they can be entered in any order. For other VRF instances, use the same command with the **vrf** option. For more information on the full list of **show ip igmp proxy** commands, for both default and non-default VRFs, refer to the *RUCKUS FastIron Command Reference*.

1. Enter the **show ip igmp proxy** command to display information about the proxy groups and interfaces for the default VRF.

```
device> show ip igmp proxy

Proxy instance name: default-vrf
Total proxy groups: 4
Address             Mode      Source    ref       flags
                              count     count
-----------------------------------------------------
225.1.1.1           exclude   0         0         0
225.1.1.2           exclude   0         0         0
225.1.1.3           exclude   0         0         0
225.1.1.4           exclude   0         0         0
Proxy interfaces
----------------
Name      Oper     Cfg       Unsoli    Filter    Filter
          Version  Robust    Interval  Acl Id    Name
-----------------------------------------------------
e1/1/3       2         2         1         0
```

2. Enter the **show ip igmp proxy summary** command display summarized information about the proxy groups and interfaces for the default VRF.

```
device> show ip igmp proxy summary

Proxy instances:
----------------------------------
Inst-Name      Total Grps
----------------------------------
default-vrf    4
```

3. Enter the **show ip igmp proxy stats** command to display informationabout queries and reports on a specific interface.

```
device> show ip igmp proxy stats

Intf      genQv1   genQv2   genQv3   GrpQ     SrcQ     Rprtv1   Rprtv2   Rprtv3   leave
           RX       RX       RX       RX       RX       TX       TX       TX       TX
-------------------------------------------------------------------------------------------
v3000      0        0        0        0        0        0        0        0        0
```

IGMPv3

The Internet Group Management Protocol (IGMP) allows an IPV4 system to communicate IP Multicast group membership information to its neighboring routers. The routers in turn limit the multicast of IP packets with multicast destination addresses to only those interfaces on the router that are identified as IP Multicast group members.

In IGMPv2, when a router sent a query to the interfaces, the clients on the interfaces respond with a membership report of multicast groups to the router. The router can then send traffic to these groups, regardless of the traffic source. When an interface no longer needs to receive traffic from a group, it sends a leave message to the router which in turn sends a group-specific query to that interface to see if any other clients on the same interface is still active.

In contrast, IGMPv3 provides selective filtering of traffic based on traffic source. A router running IGMPv3 sends queries to every multicast enabled interface at the specified interval. These general queries determine if any interface wants to receive traffic from the router. The following are the three variants of the Query message:

- A "General Query" is sent by a multicast router to learn the complete multicast reception state of the neighboring interfaces. In a General Query, both the Group Address field and the Number of Sources (N) field are zero.
- A "Group-Specific Query" is sent by a multicast router to learn the reception state, with respect to a *single* multicast address, of the neighboring interfaces. In a Group-Specific Query, the Group Address field contains the multicast address of interest, and the Number of Sources (N) field contains zero.
- A "Group-and-Source-Specific Query" is sent by a multicast router to learn if any neighboring interface desires reception of packets sent to a specified multicast address, from any of a specified list of sources. In a Group-and-Source-Specific Query, the Group Address field contains the multicast address of interest, and the Source Address [i] fields contain the source address(es) of interest.

The hosts respond to these queries by sending a membership report that contains one or more of the following records that are associated with a specific group:

- Current-State Record that indicates from which sources the interface wants to receive and not receive traffic. The record contains source address of packets and whether or not traffic will be received or included (IS_IN) or not received or excluded (IS_EX) from that source.

The following messages are generated by hosts. These messages are generated when there is a change in the group member state.

- Filter-mode-change record:. If the interface changes its current state from IS_IN to IS_EX, a TO_EX record is included in the membership report. Likewise, if an interface's current state changes from IS_EX to IS_IN, a TO_IN record appears in the membership report.

An IGMPv2 Leave report is equivalent to a TO_IN (empty) record in IGMPv3. This record means that no traffic from this group will be received regardless of the source.

An IGMPv2 group report is equivalent to an IS_EX (empty) record in IGMPv3. This record means that all traffic for this group will be received regardless of source.

- Source-List-Change Record:. If the interface wants to add or remove traffic sources from its membership report, the membership report can have an ALLOW record, which contains a list of new sources from which the interface wishes to receive traffic. It can also contains a BLOCK record, which lists current traffic sources from which the interfaces wants to stop receiving traffic.

In response to membership reports from the interfaces, the router sends a Group-Specific or a Group-and-Source Specific query to the multicast interfaces. For example, a router receives a membership report with a Source-List-Change record to block old sources from an interface. The router sends Group-and-Source Specific Queries to the source and group (S,G) identified in the record. If none of the interfaces is interested in the (S,G), it is removed from (S,G) list for that interface on the router.

Each IGMPv3-enabled router maintains a record of the state of each group and each physical port within a virtual routing interface. This record contains the group, group-timer, filter mode, and source records information for the group or interface. Source records contain information on the source address of the packet and source timer. If the source timer expires when the state of the group or interface is in Include mode, the record is removed.

Default IGMP Version

IGMPv3 is available for RUCKUS devices; however, these routers are shipped with IGMPv2-enabled. You must enable IGMPv3 globally or per interface.

Also, you can specify what version of IGMP you want to run on a device globally, on each interface (physical port or virtual routing interface), and on each physical port within a virtual routing interface. If you do not specify an IGMP version, IGMPv2 will be used.

Compatibility with IGMPv1 and IGMPv2

Different multicast groups, interfaces, and routers can run their own version of IGMP. Their version of IGMP is reflected in the membership reports that the interfaces send to the router. Routers and interfaces must be configured to recognized the version of IGMP you want them to process.

An interface or router sends the queries and reports that include its IGMP version specified on it. It may recognize a query or report that has a different version. For example, an interface running IGMPv2 can recognize IGMPv3 packets, but cannot process them. Also, a router running IGMPv3 can recognize and process IGMPv2 packets, but when that router sends queries to an IGMPv2 interface, the downgraded version is supported, no the upgraded version.

If an interface continuously receives queries from routers that are running versions of IGMP that are different from what is on the interface, the interface logs warning messages in the syslog every five minutes. Reports sent by interfaces to routers that contain different versions of IGMP do not trigger warning messages; however, you can see the versions of the packets using the **show ip igmp traffic** command.

The version of IGMP can be specified globally, per interface (physical port or virtual routing interface), and per physical port within a virtual routing interface. The IGMP version set on a physical port within a virtual routing interface supersedes the version set on a physical or virtual routing interface. Likewise, the version on a physical or virtual routing interface supersedes the version set globally on the device. The following sections present how to set the version of IGMP.

Enabling the IGMP Version Globally

The IGMP version can be configured on RUCKUS devices in global configuration mode.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Globally set the IGMP version.

```
device(config)# ip igmp version 3
```

   This example enables IGMP version 3. If you do not specify an IGMP version, the default version is IGMPv2.

The following example globally sets the device to run IGMPv3.

```
device# configure terminal
device(config)# ip igmp version 3
```

Enabling the IGMP Version for a Specific Interface

The IGMP version can be configured on RUCKUS devices for a specific interface.

When the IGMP version is configured for a specific interface, the setting overrides the globally-configured version. The following task steps show how to configure the IGMP version on either a physical interface or a virtual interface.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Configure a physical or virtual interface.
   - Configure a physical interface.

```
device(config)# interface ethernet 1/1/5
```

   - Configure a virtual interface.

```
device(config)# interface ve 3
```

   This example enables IGMP version 3. If you do not specify an IGMP version, the default version is IGMPv2.

3. Enable the IGMP version.
   - Enable IGMPv3 for a physical port, Ethernet interface 1/1/5

```
device(config-if-1/1/5)# ip igmp version 3
```

   - Enable IGMPv3 for a physical port on a virtual interface.

```
device(config-vif-3)# ip igmp version 3
```

The following example enables IGMPv3 on a specific physical interface.

```
device# configure terminal
device(config)# interface ethernet 1/1/5
device(config-if-1/1/5)# ip igmp version 3
```

The following example enables IGMPv3 on a specific virtual interface.

```
device# configure terminal
device(config)# interface ve 3
device(config-vif-3)# ip igmp version 3
```

Enabling the IGMP Version for Specific Ports Within a Virtual Routing Interface

The IGMP version can be configured on RUCKUS devices for a specific port which is a member of a virtual Ethernet interface, even when the virtual interface is configured with a different IGMP version.

When the IGMP version is configured for a specific port or range of ports, the setting overrides the IGMP version configured for the virtual interface. The following task steps show how to configure the IGMP version on a virtual interface and then configure a different IGMP version for a range of ports that are members of that virtual interface.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Configure a virtual interface.

   ```
   device(config)# interface ve 3
   ```

   This example enables IGMP version 3. If you do not specify an IGMP version, the default version is IGMPv2.

3. Enable IGMP version 2 for the virtual interface.

   ```
   device(config-vif-3)# ip igmp version 2
   ```

4. Enable IGMP version 3 for specific ports within the virtual Ethernet interface.

   ```
   device(config-vif-3)# ip igmp port-version 3 ethernet 1/1/3 to ethernet 1/1/7 ethernet 1/2/9
   ```

   In this example, IGMPv3 is enabled on Ethernet ports 1/1/3 through 1/1/7 and 1/2/9. All other ports in this virtual Ethernet interface are configured with IGMPv2.

The following example enables IGMPv2 on a virtual Ethernet interface and enables IGMPv3 on specific Ethernet ports.

```
device# configure terminal
device(config)# interface ve 3
device(config-vif-3)# ip igmp version 2
device(config-vif-3)# ip igmp port-version 3 ethernet 1/1/3 to ethernet 1/1/7 ethernet 1/2/9
```

Enabling Membership Tracking and Fast Leave

NOTE
The IGMPv3 fast leave feature is supported in include mode, but does not work in the exclude mode.

IGMPv3 provides membership tracking and fast leave of clients. In IGMPv2, only one client on an interface needs to respond to a router's queries; therefore, some of the clients may be invisible to the router, making it impossible for the switch to track the membership of all clients in a group. Also, when a client leaves the group, the switch sends group specific queries to the interface to see if other clients on that interface need the data stream of the client who is leaving. If no client responds, the switch waits three seconds before it stops the traffic.

IGMPv3 contains the tracking and fast leave feature that you enable on virtual Ethernet interfaces. Once enabled, all physical ports on that virtual Ethernet interface will have the feature enabled. IGMPv3 requires all clients to respond to general and group specific queries so that all clients on an interface can be tracked. Fast leave allows clients to leave the group without the three second waiting period, if the following conditions are met:

- If the interface, to which the client belongs, has IGMPv3 clients only. Therefore, all physical ports on a virtual Ethernet interface must have IGMPv3 enabled and no IGMPv1 or IGMPv2 clients can be on the interface. (Although IGMPv3 can handle IGMPv1 and IGMPv2 clients, these two clients cannot be on the interface in order for fast leave to take effect.)
- No other client on the interface is receiving traffic from the group to which the client belongs.

Every group on the physical interface of a virtual Ethernet interface keeps its own tracking record. It can track by (source, group).

For example, two clients (Client A and Client B) belong to group1 but each is receiving traffic streams from different sources. Client A receives a stream from (source_1, group1) and Client B receives it from (source_2, group1). If Client B leaves, the traffic stream (source_2, group1) will be stopped immediately. The **show ip igmp group tracking** command displays that clients in a group that are being tracked.

If a client sends a leave message, the client is immediately removed from the group. If a client does not send a report during the specified group membership time (the default is 140 seconds), that client is removed from the tracking list.

The following configuration example enables the tracking and fast leave feature.

```
device# configure terminal
device(config)# interface ve 13
device(config-vif-13)# ip igmp tracking
```

Creating a Static IGMP Group

You can configure one or more physical ports to be a permanent (static) member of an IGMP group based on the range or count. You can specify a **count** from 2 through 256 and up to 255 IP addresses in the range.

The following example configures two static groups starting from 226.0.0.1 using the **count** option.

```
device(config)# interface ethernet 1/1/5
device(config-if-e1000-1/1/5)# ip igmp static-group 226.0.0.1 count 2
```

The following example configures two static groups starting from 226.0.0.1 using the range of IP addresses option.

```
device(config)# interface ethernet 1/1/5
device(config-if-e1000-1/1/5)# ip igmp static-group 226.0.0.1 to 226.0.0.2
```

The following example configures two static groups on virtual ports starting from 226.0.0.1 using the **count** option.

```
device(config)# interface ethernet 1/1/5
device(config-if-e1000-1/1/5)# ip igmp static-group 226.0.0.1 count 2 ethernet 1/1/5
```

The following example configures two static groups on virtual ports starting from 226.0.0.1 using the range of IP addresses option.

```
device(config)# interface ve 10
device(config-vif-10)# ip igmp static-group 226.0.0.1 to 226.0.0.2 ethernet 1/1/5
```

NOTE
Static groups are supported on an interface enabled for IGMPv3, but the source address cannot be specified. Only the group address can be specified.

NOTE
The total number of static IGMP groups that can be configured is 256 per VLAN.

The following example displays the existing static IGMP groups, use the **show ip igmp static** command. The **vrf** keyword and *vrf-name* variable are inserted after the **igmp** part of the command.

```
device# show ip igmp vrf eng static

Group Address    Interface Port List
-----------------+---------+---------
   229.1.0.12       1/4/1 ethe 1/4/1
   229.1.0.13       1/4/1 ethe 1/4/1
   229.1.0.14       1/4/1 ethe 1/4/1
   229.1.0.92       1/4/1 ethe 1/4/1
```

Configuring IGMP Routing Global Options

A number of IGMP routing options can be configured on RUCKUS devices in global configuration mode.

You must configure the IGMP version globally before entering these options.

The following option configurations are outlined in the following steps:

- Modify the group membership time: Group membership time defines how long a group will remain active on an interface in the absence of a group report. Values range from 5 through 26000 seconds; the default value is 260.
- Modify the query interval: The IGMP query interval period defines how often a device will query an interface for group membership. Values range from 2 through 3600 seconds; the default value is 125. The query interval value you enter must be a little more than twice the group membership time.
- Modify the maximum response time: The maximum response time defines the maximum number of seconds that a client can wait before it replies to the query sent by the router. Values range from 1 through 50 seconds; the default is 10.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Modify the group membership time, in seconds.

```
device(config)# ip igmp group-membership-time 240
```

   When multiple devices are connected together, all devices must have the same group membership time configured, which must be at least twice the length of the query interval, so that missing one report will not stop traffic.

3. Modify the query interval, in seconds.

```
device(config)# ip igmp query-interval 120
```

4. Modify the IGMP maximum response time, in seconds.

```
device(config)# ip igmp max-response-time 8
```

The following example globally configures various IGMP options.

```
device# configure terminal
device(config)# ip igmp group-membership-time 240
device(config)# ip igmp query-interval 120
device(config)# ip igmp max-response-time 8
```

Displaying IGMPv3 Information

The following examples present the **show** commands available for IGMPv3.

To display the IGMP traffic status on each virtual routing interface.

```
device> show ip igmp traffic

RECEIVE COUNTERS
Port QryV1 QryV2 QryV3 G-Qry GSQry MbrV1 MbrV2 MbrV3 Leave IsIN IsEX ToIN ToEX ALLO BLK
--------+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----+----+----
*** total: V1 Reports 0, Errors: xsum 0, group 0, Invalid intf 0, router alert err 0, subnet miss 0, ttl
err 0,
Filter: Report 10, Leave 5
TRANSMIT COUNTERS
Port QryV1 QryV2 QryV3 G-Qry GSQry
--------+-----+-----+-----+-----+-----
v200 0 0 9 40 0
Note: All Counter are reset, if anyone reaches 100000 and above
```

You can display the status of all IGMP multicast groups on a device.

```
device# show ip igmp group

Total 2 entries
------------------------------------------------------
Idx Group Address    Port   Intf   Mode      Timer Srcs
---+----------------+------+------+---------+-----+----
  1 232.0.0.1        e1/6/2   v30    include     0   7
  2 226.0.0.1        e1/6/2   v30    exclude   240   2
                     e1/6/3   e1/6/3 include     0   3
Total number of groups 2
```

To display the status of one IGMP multicast group in detail.

```
device# show ip igmp group 239.0.0.1 detail

Total 2 entries
------------------------------------------------------
Idx Group Address    Port   Intf   Mode     Timer Srcs
---+----------------+------+------+-------+-----+----
  1 226.0.0.1        e1/6/2 v30    exclude   218   2
     S: 40.40.40.12
     S: 40.40.40.11
     S: 40.40.40.10
     S: 40.40.40.2          (Age: 218)
     S: 40.40.40.3          (Age: 218)
        226.0.0.1    e1/6/3 e1/6/3 include     0   3
     S: 30.30.30.3          (Age: 165)
     S: 30.30.30.2          (Age: 165)
     S: 30.30.30.1          (Age: 165)
```

If the tracking and fast leave feature is enabled, you can display the list of clients that belong to a particular IGMP group.

```
device# show ip igmp group 224.1.10.1 tracking

Total 2 entries
------------------------------------------------------
Idx Group Address    Port   Intf   Mode    Timer Srcs
---+----------------+------+------+-------+-----+----
  1 226.0.0.1        e1/6/2 v30    exclude   253   3
     S: 40.40.40.12
     S: 40.40.40.11
     S: 40.40.40.10
     S: 40.40.40.2          (Age: 253)
                    C: 10.10.10.1       (Age: 253)
     S: 40.40.40.3          (Age: 253)
                    C: 10.10.10.1       (Age: 253)
        226.0.0.1    e1/6/3 e1/6/3 include     0   3
     S: 30.30.30.3          (Age: 196)
                    C: 10.2.0.1         (Age: 196)
     S: 30.30.30.2          (Age: 196)
                    C: 10.2.0.1         (Age: 196)
     S: 30.30.30.1          (Age: 196)
                    C: 10.2.0.1         (Age: 196)
```

If you want a report for a specific multicast group, enter that group's address for the *group-address* option. Omit the *group-address* if you want a report for all multicast groups.

You can display the status of a multicast-enabled port.

```
device# show ip igmp interface

---------+------+---------+---------------+---------+-----+-----+---------
Intf/Port|Groups| Version |Querier        |  Timer  |V1Rtr|V2Rtr|Tracking
         |      |Oper  Cfg|               |OQrr GenQ|     |     |
---------+------+----+----+---------------+----+----+-----+-----+---------
e1/6/3       1    3    3                Self          0   94     No    No     Disabled
e1/6/4       0    2    -                Self          0   94     No    No     Disabled
v30          1    3    3                                          Disabled
```

```
e1/6/2            3    -                 Self           0   20     No    No
v40          0    3    3                                            Disabled
e1/6/2            3    -                 Self           0   20     No    No
v50          0    2    -                                            Disabled
e1/2/1            2    -                 Self           0   29     No    No
e1/6/8            2    -                 50.1.1.10     46    0     No    Yes
e1/6/1            2    -                 Self           0  115     No    Yes
```

The following command displays static IGMP groups for the "eng" VRF.

```
device# show ip igmp vrf eng static

Group Address    Interface Port List
---------------+---------+---------
      229.1.0.12       1/4/1 ethe 1/4/1
      229.1.0.13       1/4/1 ethe 1/4/1
      229.1.0.14       1/4/1 ethe 1/4/1
      229.1.0.92       1/4/1 ethe 1/4/1
```

Clearing IGMP Traffic Statistics and the IGMP Group Membership Table

To clear statistics for IGMP traffic, enter the **clear ip igmp traffic** command. This command clears all the multicast traffic information on all interfaces on the device.

```
device# clear ip igmp traffic
```

Use the **vrf** option to clear the traffic information for a VRF instance specified by the *vrf* variable.

To clear the IGMP group membership table from all interfaces on the device, use the **clear ip igmp cache** command.

```
device# clear ip igmp cache
```

Use the **vrf** option to clear the IGMP group membership table from a VRF instance specified by the *vrf* variable.

Source-Specific Multicast

Using the Any-Source Multicast (ASM) service model, sources and receivers register with a multicast address. The protocol uses regular messages to maintain a correctly configured broadcast network where all sources can send data to all receivers and all receivers get broadcasts from all sources.

With Source-Specific Multicast (SSM), the "channel" concept is introduced where a "channel" consists of a single source and multiple receivers who specifically register to get broadcasts from that source. Consequently, receivers are not burdened with receiving data they have no interest in, and network bandwidth requirements are reduced because the broadcast need only go to a sub-set of users. The address range 232/8 has been assigned by the Internet Assigned Numbers Authority (IANA) for use with SSM.

IGMPv3 and Source-Specific Multicast Protocols

When IGMPv3 and PIM Sparse (PIM-SM) are enabled, the source specific multicast service (SSM) can be configured. SSM simplifies PIM-SM by eliminating the RP and all protocols related to the RP. IGMPv3 and PIM-SM must be enabled on any ports where you want SSM to operate.

PIM Source-Specific Multicast (SSM) is a subset of the PIM SM protocol. In PIM SSM mode, the shortest path tree (SPT) is created at the source. The SPT is created between the receiver and source, but the SPT is built without the help of the RP. The router closest to the interested receiver host is notified of the unicast IP address of the source for the multicast traffic. PIM SSM goes directly to the source-based distribution tree without the need of the RP connection. PIM SSM is different from PIM SM because it forms its own SPT, without forming a shared tree.

You can configure a single SSM group address, the default multicast address group range is 232.0.0.0/8.

You can configure multiple SSM group ranges using an ACL. When you are using an ACL, the following configuration considerations apply:

- The existing **ssm-enable range** command with the *group-address address-mask* options are used to identify a single SSM group address.

- The ACL must be configured with the SSM group address in the permit clause of the **ssm-enable range** command using the ACL ID or ACL name. If the **ssm-enable range** command with the *group-address address-mask* options permits a clause, then that group will also operate in the PIM-SM mode.
- If the **ssm-enable range** command with an ACL ID or ACL name is configured with a non-existent or empty ACL, then the SSM group will operate in PIM-SM mode (non PIM-SSM mode). However when an ACL is added or updated, then the group will exist in a PIM-SSM mode. By default, an empty ACL will deny all.
- By default, the group address mentioned in the IGMPv2 ssm-mapping ACL will decide if the group address is a PIM-SSM group or non PIM-SSM group. Therefore, if a user wants to prevent a group from operating in PIM-SSM mode, then the user's configuration must consistently deny the group in all configuration options for PIM-SSM range.
- ACL of any type (named or unnamed, standard or extended) can be used to specify the SSM group range. If an extended ACL is used, then the destination ip address should be used to specify the group address. Any configuration in the source address of an extended ACL is ignored. Only permit statements are considered in the ACL configuration. Any deny statements in the ACL clause are also ignored.

Configuring PIM SSM Group Ranges

The source specific multicast service (SSM) simplifies PIM-SM by eliminating the RP and all protocols related to the RP. Single or multiple PIM SSM group address ranges can be configured.

IGMPv3 and PIM-SM must be enabled on any ports on which you want SSM to operate. When configuring a single SSM group range, the IP address and address mask are used. When configuring multiple SSM group ranges, an ACL is used.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable PIM

```
device(config)# router pim
```

3. To configure SSM group ranges, use one of the following choices.
   - Configure a single SSM group address. The IP address specifies the multicast address for the SSM address range. If this is not configured, the range will default to 232/8 as assigned by the Internet Assigned Numbers Authority (IANA) for use with SSM.

```
device(config-router-pim)# ssm-enable range 232.1.1.1/8
```

   - Configure multiple SSM group ranges using an ACL. In this example, PIM uses the group addresses allowed by the ACL range, as its PIM SSM range. You must configure the ACL before this step.

```
device(config-router-pim)# ssm-enable range acl-range
```

4. To display information for PIM SSM group ranges including the ACL, use the **show ip pim sparse** command.

```
device(config-router-pim)# show ip pim sparse

Global PIM Sparse Mode Settings
  Maximum Mcache          : 16384       Current Count              : 3
  Hello interval          : 30          Neighbor timeout           : 105
  Join/Prune interval     : 60          Inactivity interval        : 180
  Hardware Drop Enabled   : Yes         Prune Wait Interval        : 3
  Bootstrap Msg interval  : 60          Candidate-RP Msg interval  : 60
  Register Suppress Time  : 60          Register Probe Time        : 10
  Register Stop Delay     : 10
  SSM Enabled             : Yes         SPT Threshold              : 1
  SSM Group Range         : 232.0.0.0/8
  Route Precedence        : uc-non-default uc-default mc-non-default mc-default
  Slow Path Disable All        : Yes                                    Slow Path Enable
SSM                          :Yes
        Slow Path Filter Acl : acl
```

IGMPv2 SSM Mapping

The PIM-SSM feature requires all IGMP hosts to send IGMPv3 reports. Where you have an IGMPv2 host, this can create a compatibility problem. In particular, the reports from an IGMPv2 host contain a group multicast address but do not contain source addresses. The IGMPv3 reports contain both the group multicast address and one or more source addresses. This feature converts IGMPv2 reports into IGMPv3 reports through use of the **ip igmp ssm-map** command and a properly configured ACL.

The ACL used with this feature filters for the group multicast address. The ACL is then associated with one or more source addresses using the **ip igmp ssm-map** command. When the **ip igmp ssm-map enable** command is configured, IGMPv3 reports are sent for IGMPv2 hosts.

The following sections describe how to configure the ACL and the **ip igmp ssm-map** command to use the IGMPv2 SSM mapping feature:

- Configuring an ACL for IGMPv2 SSM mapping
- Configuring the IGMPv2 SSM mapping commands

  NOTE
  IGMPv2 SSM mapping is not supported for IGMP static groups.

Configuring an ACL for IGMPv2 SSM Mapping

You can use either a standard or extended ACL to identify the group multicast address(es) that you want to add source addresses to when creating an IGMPv2 SSM mapping.

For standard ACLs, you must create an ACL with a permit clause, and the *ip-source-address* variable must contain the group multicast address. This can be configured directly with a subnet mask or with the **host** keyword, in which case a subnet mask of all zeros (0.0.0.0) is implied.

For extended ACLs, the *ip-source-address* variable must contain either 0.0.0.0 or the **any** keyword. Additionally, the extended ACL must be configured with a **permit** clause and the host keyword. This can be configured directly with a subnet mask or with the **host** keyword, in which case a subnet mask of all zeros (0.0.0.0) is implied.

1. Enter global configuration mode.

```
device# configure terminal
```

2. In the following example, IPv4 standard access-list 20 is configured for the group multicast address: 239.1.1.1 by including the **host** keyword.

```
device(config)# ip access-list standard 20
device(config-std-ipacl-20)# permit host 239.1.1.1
```

3. In the following example, a permit statemnet is added to standard access-list 20 for the group multicast address: 224.1.1.0 with a subnet mask of 0.0.0.255.

```
device(config)# ip access-list standard 20
device(config-std-ipacl-20)# permit 224.1.1.0 0.0.0.225
```

4. In the following example, extended access-list 100 is configured for the group multicast address: 232.1.1.1 with a subnet mask of 0.0.0.255.

```
device(config)# ip access-list extended 100
device(config-ext-ipacl-100)# permit ip any host 232.1.1.1
```

The following example configures two access lists, one standard and one extended, that can be used for SSM mapping.

```
device(config)# ip access-list standard 20
device(config-std-ipacl-20)# permit host 239.1.1.1
device(config-std-ipacl-20)# permit 224.1.1.0 0.0.0.225
device(config-std-ipacl-20)# exit
device(config)# ip access-list extended 100
device(config-ext-ipacl-100)# permit ip any host 232.1.1.1
```

Configuring IGMPv2 SSM Mapping

The **ip ssm-map** command is used to enable the IGMPv2 mapping feature and to define the maps between IGMPv2 group addresses and multicast source addresses.

For standard ACLs, you must create an ACL with a permit clause and the *ip-source-address* variable must contain the group multicast address. This can be configured directly with a subnet mask or with the **host** keyword in which case a subnet mask of all zeros (0.0.0.0) is implied.

For extended ACLs, the *ip-source-address* variable must contain either 0.0.0.0 or the **any** keyword. Additionally, the extended ACL must be configured with a **permit** clause and the host keyword. This can be configured directly with a subnet mask or with the **host** keyword in which case a subnet mask of all zeros (0.0.0.0) is implied.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Create a standard access-list with a permit statement for the group multicast address: 239.1.1.1 by including the **host** keyword.

```
device(config)# ip access-list standard 20
device(config-std-ipacl-20)# permit host 239.1.1.1
```

3. Create a permit statement in the same standard access-list for the group multicast address: 224.1.1.0 with a subnet mask of 0.0.0.255.

```
device(config-std-ipacl-20)# permit 224.1.1.0 0.0.0.225
device(config-std-ipacl-20)# exit
```

4. Create an extended access-list for the group multicast address: 232.1.1.1 with a subnet mask of 0.0.0.255.

```
device(config)# ip access-list extended 100
device(config-ext-ipacl-100)# permit ip any host 232.1.1.1 0.0.0.255
```

5. Enable the IGMPv2 mapping feature, using the **ip igmp ssm-map** command.

```
device(config)# ip igmp ssm-map enable
```

6. Configure a map between an IGMPv2 group address and a multicast source address using the **ip igmp ssm-map static** command.

```
device(config)# ip igmp ssm-map 20 1.1.1.1
```

   Repeat this step to map all the IGMPv2 group addresses and a multicast source address. The configuration example that follows this task displays other SSM mapping examples.

In the following example configuration, an extended ACL and a standard ACLs are defined with group multicast addresses. The **ip igmp ssm-map** commands are configured to map the ACLs to source addresses and to enable the feature on the router.

```
device# configure terminal
device(config)# ip access-list standard 20
device(config-std-ipacl-20)# permit host 239.1.1.1
device(config-std-ipacl-20)# permit 224.1.1.0 0.0.0.225
device(config-std-ipacl-20)# exit
device(config)# ip access-list extended 100
device(config-ext-ipacl-100)# permit ip any host 232.1.1.1 0.0.0.255
device(config)# ip igmp ssm-map 20 1.1.1.1
device(config)# ip igmp ssm-map 20 2.2.2.2
device(config)# ip igmp ssm-map 100 1.1.1.1
device(config)# ip igmp ssm-map enable
```

Displaying an IGMP SSM Mapping Information

Use the **show ip igmp ssm-map** command to display the association between a configured ACL and the source address mapped to it.

```
device# show ip igmp ssm-map

+---------+-----------------+
| Acl id  | Source Address  |
+---------+-----------------+
        20          1.1.1.1
       100          1.1.1.1
        20          2.2.2.2
        20          2.2.2.3
        20          2.2.2.4
        20          2.2.2.5
        20          2.2.2.6
```

Use the **show ip igmp ssm-map** command with the *group-address* variable to display the ACL ID that has the specified multicast group address in its permit list and lists the source addresses mapped to the specified multicast group address.

```
device# show ip igmp ssm-map 232.1.1.1

+---------+-----------------+
| Acl id  | Source Address  |
+---------+-----------------+
        20          1.1.1.1
       100          1.1.1.1
        20          2.2.2.2
        20          2.2.2.3
        20          2.2.2.4
        20          2.2.2.5
        20          2.2.2.6
```

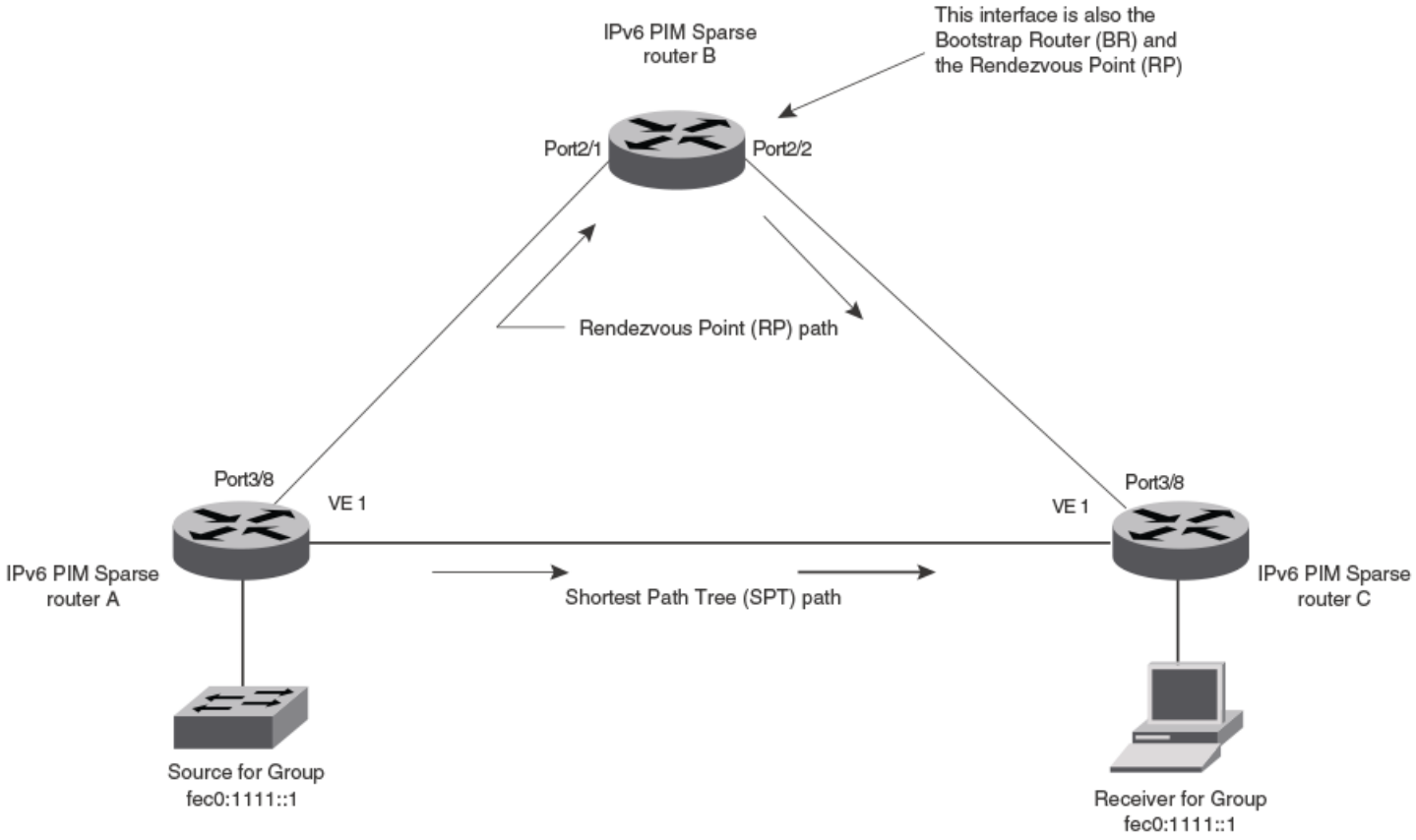
IPv6 Multicast Protocols

IPv6 PIM Sparse

IPv6 Protocol Independent Multicast (PIM) Sparse is supported. IPv6 PIM Sparse provides multicasting that is especially suitable for widely distributed multicast environments.

In an IPv6 PIM Sparse network, an IPv6 PIM Sparse router that is connected to a host that wants to receive information for a multicast group must explicitly send a join request on behalf of the receiver (host).

FIGURE 16 Example IPv6 PIM Sparse Domain



IPv6 PIM Sparse Router Types

Routers that are configured with IPv6 PIM Sparse interfaces also can be configured to fill one or more of the following roles:

- BSR: The Bootstrap Router (BSR) distributes RP information to the other IPv6 PIM Sparse routers within the domain. Each IPv6 PIM Sparse domain has one active BSR. For redundancy, you can configure ports on multiple routers as candidate BSRs. The IPv6 PIM Sparse protocol uses an election process to select one of the candidate BSRs as the BSR for the domain. The BSR with the highest BSR priority (a user-configurable parameter) is elected. If the priorities result in a tie, then the candidate BSR interface with the highest IP address is elected. In the example in Figure 16 on page 145, IPv6 PIM Sparse router B is the BSR. Port 1/2/2 is configured as a candidate BSR.
- RP: The Rendezvous Point (RP) is the meeting point for IPv6 PIM Sparse sources and receivers. A IPv6 PIM Sparse domain can have multiple RPs, but each PIM Sparse multicast group address can have only one active RP. IPv6 PIM Sparse routers learn the addresses of RPs and the groups for which they are responsible from messages that the BSR sends to each of the IPv6 PIM Sparse routers. In the example in Figure 16 on page 145, IPv6 PIM Sparse router B is the RP. Port 1/2/2 is configured as a candidate Rendezvous Point (RP).

To enhance overall network performance, the device uses the RP to forward the packets from a group source to the group receivers. Later, the receiver calculates the shortest path between the receiver and the source (the Shortest Path Tree, or SPT) and uses the SPT for subsequent packets from the source to the receiver. The device calculates a separate SPT for each source-receiver pair.

NOTE
It is recommended that you configure the same ports as candidate BSRs and RPs.

RP Paths and SPT Paths

In a typical IPv6 PIM Sparse domain, there may be two or more paths from a designated router (DR) for a multicast source to an IPv6 PIM group receiver.

- Path through the RP: This is the path the device uses the first time it receives traffic for an IPv6 PIM group. However, the path through the RP may not be the shortest path from the device to the receiver.
- Shortest Path: Each IPv6 PIM Sparse router that is a DR for an IPv6 receiver calculates a short path tree (SPT) towards the source of the IPv6 multicast traffic. The first time the device configured as an IPv6 PIM router receives a packet for an IPv6 group, it sends the packet to the RP for that group, which in turn will forward it to all the intended DRs that have registered with the RP. The first time the device is a recipient, it receives a packet for an IPv6 group and evaluates the shortest path to the source and initiates a switchover to the SPT. Once the device starts receiving data on the SPT, the device proceeds to prune itself from the RPT.

To optimize PIM traffic, the protocol contains a mechanism for calculating the Shortest Path Tree (SPT) between a given source and a receiver. PIM Sparse routers can use the SPT as an alternative to using the RP for forwarding traffic from a source to a receiver. By default, the device forwards the packets it receives from a given source to a given receiver using the RP path, but subsequent packets from that source to that receiver through the SPT. You can change the number of packets the device receives using the RP before switching to using the SPT.

The following examples demonstrate the use of SPT:

Figure 16 on page 145 shows two paths for packets from the source for group fec0:1111::1 and a receiver for the group. The source is attached to an IPv6 PIM Sparse router A and the recipient is attached to an IPv6 PIM Sparse router C. IPv6 PIM Sparse router B is the RP for this multicast group. As a result, the default path for packets from the source to the receiver is through the RP. However, the path through the RP sometimes is not the shortest path. In this case, the shortest path between the source and the receiver is over the direct link between router A and router C, which bypasses the RP (router B).

In Figure 16 on page 145, router A forwards the packets from group fec0:1111::1 source to the destination by sending the packet to router B, which is the RP. Router B then sends the packet to router C. Later packets that router A receives from the source for the receiver, router A forwards them directly to router C using the SPT path.

RFC 3513 and RFC 4007 Compliance for IPv6 Multicast Scope-based Forwarding

The IPv6 multicast implementation recognizes scopes and conforms to the scope definitions in RFC 3513. Per RFC 3513, scopes 0 and 3 are reserved and packets are not forwarded with an IPv6 destination multicast address of scopes 0 and 3. Additionally, scopes 1 and 2 are defined as Node-Local and Link-Local and are not forwarded. Thus, the implementation forwards only those packets with an IPv6 multicast destination address with scope 4 or higher.

RFC 4007 defines "scope zones" and requires that the forwarding of packets received on any interface of a particular scope zone be restricted to that scope zone. Currently, the device supports one zone for each scope, and the default zone for scope 4 and higher consists of all interfaces in the system. Thus, the default zones for scope 4 and higher are the same size.

IPv6 PIM Sparse Configuration

To configure the device for IPv6 PIM Sparse, perform the following tasks:

- Enable the IPv6 PIM Sparse of multicast routing.
- Configure VRF then enable IPv6 Protocol Independent Multicast Sparse mode (PIM-SM) for a specified VRF, if applicable.
- Configure an IPv6 address on the interface.
- Enable IPv6 PIM Sparse.
- Identify the interface as an IPv6 PIM Sparse border, if applicable.
- Identify the device as a candidate PIM Sparse Bootstrap Router (BSR), if applicable.
- Identify the device as a candidate PIM Sparse Rendezvous Point (RP), if applicable.
- Specify the IP address of the RP (if you want to statically select the RP).

  NOTE
  It is recommended that you configure the same device as both the BSR and the RP.

Enabling IPv6 PIM Sparse

IPv6 PIM must be enabled globally and IPv6 PIM Sparse Mode (PIM SM) enabled locally on specific interfaces.

By default, IPv6 PIM SM is disabled. Complete the following steps to enable IPv6 PIM SM:

- Enable IPv6 PIM globally.
- Configure the IPv6 interfaces that will use IPv6 PIM SM.
- Enable IPv6 PIM SM locally on the individual interfaces connected to the IPv6 PIM Sparse network.

The steps in this task do not configure the device as a candidate IPv6 PIM Sparse Bootstrap Router (BSR) and candidate Rendezvous Point (RP). You can configure a device as a PIM Sparse device without configuring the device as a candidate BSR and RP. If you do configure the device as a candidate BSR or RP, it is recommended that you configure the device as both a BSR and an RP.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Globally enables IPv6 PIM.

   ```
   device(config)# ipv6 router pim
   ```

3. Exit to global configuration mode to enter the interface.

   ```
   device(config-ipv6-pim-router)# exit
   ```

4. Enter interface configuration mode.

```
device(config)# interface ethernet 1/2/2
```

   This step configures Ethernet interface 1/2/2 and this interface is to run IPv6 PIM SM.

5. Enter the IPv6 address for the interface.

```
device(config-if-e10000-1/2/2)# ipv6 address a000:1111::1/64
```

6. Configure IPv6 PIM SM on the interface.

```
device(config-if-e10000-1/2/2)# ipv6 pim-sparse
```

7. (Optional) Specify that the interface is on the border of the IPv6PIM Sparse domain.

```
device(config-if-e10000-1/2/2)# ipv6 pim border
```

The following example enables IPv6 PIM globally and IPv6 PIM SM on Ethernet interface 1/2/2 which is on the border of the IPv6 PIM Sparse domain.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# exit
device(config)# interface ethernet 1/2/2
device(config-if-e10000-1/2/2)# ipv6 address a000:1111::1/64
device(config-if-e10000-1/2/2)# ipv6 pim-sparse
device(config-if-e10000-1/2/2)# ipv6 pim border
```

Enabling IPv6 PIM Sparse on a Virtual Ethernet Interface

IPv6 PIM must be enabled globally and IPv6 PIM Sparse Mode (PIM SM) enabled locally on specific interfaces.

By default, IPv6 PIM SM is disabled. Complete the following steps to enable IPv6 PIM SM on a virtual Ethernet interface:

- Enable IPv6 PIM globally.
- Configure the IPv6 virtual Ethernet interfaces that will use IPv6 PIM SM.
- Enable IPv6 PIM SM locally on the individual interfaces connected to the IPv6 PIM Sparse network.

The steps in this task do not configure the device as a candidate PIM Sparse Bootstrap Router (BSR) and candidate Rendezvous Point (RP). You can configure a device as an IPv6 PIM Sparse device without configuring the device as a candidate BSR and RP. If you do configure the device as a candidate BSR or RP, it is recommended that you configure the device as both a BSR and an RP.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Globally enable IPv6 PIM.

```
device(config)# ipv6 router pim
```

3. Exit to global configuration mode to enter the interface.

```
device(config-ipv6-pim-router)# exit
```

4. Enter interface configuration mode.

```
device(config)# interface ve 15
```

   This step configures virtual Ethernet interface 15 and this interface is to run IPv6 PIM SM.

5. Enter the IPv6 address for the interface.

```
device(config-vif-15)# ipv6 address a000:1111::1/64
```

6. Configure IPv6 PIM SM on the interface.

```
device(config-vif-15)# ipv6 pim-sparse
```

7. (Optional) Specify that the interface is on the border of the IPv6 PIM Sparse domain.

```
device(config-vif-15)# ipv6 pim border
```

The following example enables IPv6 PIM globally and IPv6 PIM SM on virtual Ethernet interface 15 which is on the border of the IPv6 PIM Sparse domain.

```
device# configure terminal
device(config)# router pim
device(config-ipv6-pim-router)# exit
device(config)# interface ve 15
device(config-vif-15)# ipv6 address a000:1111::1/64
device(config-vif-15)# ipv6 pim-sparse
device(config-vif-15)# ipv6 pim border
```

Enabling IPv6 PIM Sparse on a Specific VRF

IPv6 PIM must be enabled globally and IPv6 PIM Sparse Mode (PIM SM) can be enabled for a specific virtual routing and forwarding instance (VRF).

By default, IPv6 PIM is disabled. Complete the following steps to enable IPv6 PIM:

- Enable the feature globally.
- Configure the IPv6 interfaces that will use IPv6 PIM.
- Enable IPv6 PIM DM locally on the ports that have the IPv6 interfaces you configured for IPv6 PIM.

To configure IPv6 PIM SM on a virtual routing instance (VRF), the **VRF** option and *vrf-name* variable are added to the **ipv6 router pim** command. All IPv6 PIM parameters available for the default router instance are configurable for a VRF-based IPv6 PIM instance.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable IPv6 PIM for a specific VRF.

```
device(config)# ipv6 router pim vrf blue
```

   In this example, IPv6 PIM is enabled for the VRF named blue. The VRF must be created before you specify it in this task step or you will receive an error message stating that the VRF does not exist. The following configuration example provides example VRF configuration.

The following example creates a VRF named blue and enables IPv6 PIM for VRF blue.

```
device# configure terminal
device(config)# vrf blue
device(config-vrf-blue)# rd 11:1
device(config-vrf-blue)# exit
device(config)# ipv6 router pim vrf blue
device(config-ipv6-pim-router-vrf-blue)
```

Modifying IPv6 PIM Options

Many IPv6 PIM options can be modified from their default values in IPv6 PIM router configuration mode.

IPv6 PIM parameters come with preset values. The defaults work well in most networks, but you can modify the following parameters if necessary:

- Neighbor timeout: Neighbor timeout is the interval after which an IPv6 PIM router will consider a neighbor to be absent. If the timer expires before receiving a new hello message, the IPv6 PIM router will time out the neighbor.
- Hello timer: The hello timer defines the interval at which periodic hellos are sent out IPv6 PIM interfaces. Devices use hello messages to inform neighboring devices of their presence.
- Join and Prune message timer: By default, an IPv6 PIM device sends IPv6 PIM Sparse Join or Prune messages every 60 seconds. These messages inform other IPv6 PIM Sparse routers about clients who want to become receivers (Join) or stop being receivers (Prune) for IPv6 PIM Sparse groups.
- Prune wait timer: The prune wait timer allows you to set the amount of time the IPv6 PIM router should wait for a join override before pruning an Outgoing Interface List Optimization (OIF) from the entry and this stops traffic to neighbor devices that do not want the traffic. A prune wait value of zero causes the IPv6 PIM device to stop traffic immediately upon receiving a prune message. If there are two or more neighbors on the physical port, then the prune wait timer must not be used because one neighbor may send a prune message while the other sends a join message at the same time, or within less than three seconds.
- Shortest Path Tree threshold: To optimize IPv6 PIM traffic, the protocol contains a mechanism for calculating the Shortest Path Tree (SPT) between a given source and a receiver. You can configure a threshold of the number of packets the device receives using the RP before switching to using the SPT.
- Inactivity timer: The device deletes a forwarding entry if the entry is not used to send multicast packets. The IPv6 PIM inactivity timer defines how long a forwarding entry can remain unused before the device deletes it.
- Register suppress interval: The amount of time the IPv6 PIM router uses to periodically trigger the NULL register message.
- Register probe time: The amount of time the IPv6 PIM router waits for a register-stop from an RP before it generates another NULL register to the IPv6 PIM RP. The register probe time configuration applies only to the first hop IPv6 PIM router.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Enable IPv6 PIM globally and enter IPv6 PIM router configuration mode.

   ```
   device(config)# ipv6 router pim
   ```

3. Apply an IPv6 PIM neighbor timeout value to all ports on the router operating with IPv6 PIM.

   ```
   device(config-ipv6-pim-router)# nbr-timeout 50
   ```

   The timeout interval is set to 50 seconds.

4. Apply a IPv6 PIM hello timer to all ports on the device operating with IPv6 PIM.

   ```
   device(config-ipv6-pim-router)# hello-timer 62
   ```

   The hello timer interval is set to 62 seconds.

5. Set the Join or Prune message interval to 30 seconds.

```
device(config-ipv6-pim-router)# message-interval 30
```

   The Join or Prune interval timer is set to 30 seconds.

   NOTE
   Use the same Join or Prune message interval on all the IPv6 PIM Sparse routers in the IPv6 PIM Sparse domain. If the routers do not all use the same timer interval, the performance of IPv6 PIM Sparse can be adversely affected.

6. Set the prune wait time.

```
device(config-ipv6-pim-router)# prune-wait 2
```

   The prune wait value is set to 2 seconds. To view the currently configured prune wait time, enter the **show ipv6 pim dense** command.

7. Change the number of packets the device receives using the RP before switching to the SPT.

```
device(config-ipv6-pim-router)# spt-threshold 1000
```

   In this example, the device does not switch over to using the SPT until it has sent 1000 packets using the RP.

8. Apply an IPv6 PIM inactivity timer to all IPv6 PIM interfaces.

```
device(config-ipv6-pim-router)# inactivity-timer 160
```

   The value of the inactivity timer is set to 160 seconds.

9. Change the default register suppress time.

```
device(config-ipv6-pim-router)# register-suppress-time 90
```

   The register suppress time is set to 90 seconds.

   NOTE
   The register suppress time configuration applies only to the first hop IPv6 PIM router.

10. Change the default register probe time.

```
device(config-ipv6-pim-router)# register-probe-time 20
```

   The value of the register probe is set to 20 seconds.

   NOTE
   Once an IPv6 PIM first hop router successfully registers with a IPv6 PIM RP, the IPv6 PIM first hop router will not default back to the data registration. All subsequent registers will be in the form of the NULL registration.

The following example shows how to configure the various IPv6 PIM options.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# nbr-timeout 50
device(config-ipv6-pim-router)# hello-timer 62
device(config-ipv6-pim-router)# message-interval 30
device(config-ipv6-pim-router)# prune-wait 2
device(config-ipv6-pim-router)# spt-threshold 1000
device(config-ipv6-pim-router)# inactivity-timer 160
device(config-ipv6-pim-router)# register-suppress-time 90
device(config-ipv6-pim-router)# register-probe-time 20
```

Configuring the Slow Path Forwarding of IPv6 Multicast Data Packets

The slow path forwarding of IPv6 multicast data packets is enabled by default. Various commands can be used to change the default settings for the slow path forwarding of IPv6 multicast data packets.

The following task enables slow path forwarding for SSM groups.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Enable IPv6 PIM globally.

   ```
   device(config)# ipv6 router pim
   ```

3. Enable slow path forwarding for Source-Specific Multicast (SSM) groups.

   ```
   device(config-ipv6-pim-router)# slow-path-forwarding enable-ssm
   ```

   Slow path forwarding for SSM groups is disabled by default.

The following example disables the slow path forwarding for all IPv6 multicast data packets.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# slow-path-forwarding disable-all
```

The following example enables the slow path forwarding of IP multicast data packets for SSM groups.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# slow-path-forwarding enable-ssm
```

Configuring BSRs and RPs for IPv6 PIM Sparse

After enabling IPv6 PIM SM globally and locally, you need to identify an interface on at least one device as a candidate IPv6 PIM Sparse Bootstrap Router (BSR) and candidate IPv6 PIM Sparse rendezvous point (RP).

This task assumes that you have configured IPv6 PIM SM globally and on local interfaces.

NOTE
It is possible to configure the device as a candidate for either BSR or RP, but it is recommended that you configure the same interface on the same device as both a BSR and an RP.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Globally enable IPv6 PIM.

   ```
   device(config)# ipv6 router pim
   ```

3. Configure Ethernet interface 1/1/3 as the BSR candidate with a mask length of 32 and a priority of 64.

   ```
   device(config-ipv6-pim-router)# bsr-candidate ethernet 1/1/3 32 64
   ```

4. Set the IPv6 PIM BSR message interval timer.

   ```
   device(config-ipv6-pim-router)# bsr-msg-interval 16
   ```

   The BSR message interval timer is set to 16 seconds.

5. Configure the device as a candidate RP.

```
device(config-ipv6-pim-router)# rp-candidate ethernet 1/1/3
```

6. (Optional) To add a group number range for which the device is a candidate RP, use the **add** option to explicitly add a range.

```
device(config-ipv6-pim-router)# rp-candidate add ff02::200:2 64
```

7. (Optional) To delete a group number range for which the device is a candidate RP, use the **delete** option to explicitly remove a range that was previously added.

```
device(config-ipv6-pim-router)# rp-candidate delete ff02::200:1 128
```

   An address group is deleted from the devices for which it is a candidate RP.

8. Specify how frequently the candidate RP configured on the device sends candidate RP advertisement messages to the BSR.

```
device(config-ipv6-pim-router)# rp-adv-interval 180
```

   The RP advertisement interval of is set to180.

The following example configures the IPv6 PIM Sparse interface on port 1/1/3 as a BSR candidate, with a hash mask length of 32 and a priority of 64. The same interface is also configured as an RP candidate. An explicit group address range is configured and the device is now a candidate RP for prefixes starting with ff02::200:2. The RP advertisement interval is set to 180 seconds.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# bsr-candidate ethernet 1/1/3 32 64
device(config-ipv6-pim-router)# bsr-msg-interval 16
device(config-ipv6=pim-router)# rp-candidate ethernet 1/1/3
device(config-ipv6-pim-router)# rp-candidate add ff02::200:2 64
device(config-ipv6-pim-router)# rp-adv-interval 180
```

Configuring BSRs and RPs for IPv6 PIM Sparse for a Specified VRF

After enabling IPv6 PIM SM globally and locally, you need to identify an interface on at least one device as a candidate IPv6 PIM Sparse Bootstrap Router (BSR) and candidate IPv6 PIM Sparse rendezvous point (RP). You can configure BSRs and RPs for a virtual routing and forwarding (VRF) instance.

This task assumes that you have configured the VRF.

NOTE
It is possible to configure the device as a candidate for either BSR or RP for a specified VRF, but it is recommended that you configure the same interface on the same device as both a BSR and an RP.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Globally enable IPv6 PIM for a VRF.

```
device(config)# ipv6 router pim vrf blue
```

3. Configure Ethernet interface 1/1/3 as the BSR candidate for the specified VRF with a mask length of 32 and a priority of 64.

```
device(config-ipv6-pim-router-vrf-blue)# bsr-candidate ethernet 1/1/3 32 64
```

4. Set the IPv6 PIM BSR message interval timer.

```
device(config-ipv6-pim-router-vrf-blue)# bsr-msg-interval 16
```

   The BSR message interval timer is set to 16 seconds.

5. Configure the device as a candidate RP for the specified VRF.

```
device(config-ipv6-pim-router-vrf-blue)# rp-candidate ethernet 1/1/3
```

6. (Optional) To add a group number range for the configured RP candidate for a specified VRF, use the **add** option to explicitly add a range.

```
device(config-ipv6-pim-router-vrf-blue)# rp-candidate add ff02::200:2 64
```

7. (Optional) To delete the configured RP candidate group ranges for a specified VRF, use the **delete** option to explicitly remove a range that was previously added.

```
device(config-ipv6-pim-router-vrf-blue)# rp-candidate delete ff02::200:1 128
```

   This example deletes an address group from the VRF for which it is a candidate RP.

The following example configures the IPv6 PIM Sparse interface on port 1/1/3 as a BSR candidate for VRF blue, with a hash mask length of 32 and a priority of 64. The same interface is also configured as an RP candidate for VRF blue. An explicit group address range is added.

```
device# configure terminal
device(config)# ipv6 router pim vrf blue
device(config-ipv6-pim-router-vrf-blue)# bsr-candidate ethernet 1/1/3 32 64
device(config-ipv6-pim-router-vrf-blue)# bsr-msg-interval 16
device(config-ipv6=pim-router-vrf-blue)# rp-candidate ethernet 1/1/3
device(config-ipv6-pim-router-vrf-blue)# rp-candidate add ff02::200:2 64
```

Updating IPv6 PIM-Sparse Forwarding Entries with New RP Static Configuration

You can define a static RP instead of using the IPv6 PIM Sparse RP election process. After defining a static RP, you must clear out the old RP configuration.

It is recommended that you use the IPv6 PIM Sparse protocol's RP election process so that a backup RP can automatically take over if the active RP router becomes unavailable. However, if you do not want the RP to be selected by the RP election process but instead you want to explicitly identify the RP by IPv6 address, use the **rp-address** command.

If you explicitly specify the RP, the device uses the specified RP for all group-to-RP mappings and overrides the set of candidate RPs supplied by the BSR.

> **NOTE**
> Specify the same IPv6 address as the RP on all IPv6 PIM Sparse devices within the IPv6 PIM Sparse domain. Make sure the device is on the backbone or is otherwise well connected to the rest of the network.

If you make changes to your static RP configuration, the entries in the IPv6 PIM-Sparse multicast forwarding table continue to use the old RP configuration until they are aged out.

The **clear pim rp-map** command allows you to update the entries in the static multicast forwarding table immediately after making RP configuration changes. This command is meant to be used with the **rp-address** command.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Globally enable IPv6 PIM.

```
device(config)# ipv6 router pim
```

3. Create a static RP IPv6 address.

```
device(config-ipv6-pim-router)# rp-address 31::207
```

   The command in this example identifies the device interface at IPv6 address 31::207 as the RP for the IPv6 PIM Sparse domain. The device uses the specified RP and ignores group-to-RP mappings received from the BSR.

4. Exit to privileged EXEC configuration mode.

```
device(config-ipv6-pim-router)# end
```

5. To update the entries in a IPv6 PIM sparse static multicast forwarding table with new RP configuration, you must clear out the old RP entries.

```
device# clear ipv6 pim rp-map
```

The following example configures a static RP for the IPv6 PIM Sparse domain and clears out existing RP entries.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# rp-address 207.95.7.1
device(config-ipv6-pim-router)# end
device# clear ipv6 pim rp-map
```

Embedded Rendezvous Point

Global deployment of IPv4 multicast relies on Multicast Source Discovery Protocol (MSDP) to convey information about the active sources. Because IPv6 provides more address space, the RP address can be included in the multicast group address.

NOTE
The IPv6 group address must be part of the FF70:/12 prefix.

Embedded RP support is enabled by default. The following configuration examples disable embedded RP support.

To disable embedded RP support.

```
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# no rp-embedded
```

To disable embedded RP support for a specified VRF.

```
device(config)# ipv6 router pim vrf blue
device(config-ipv6-pim-router-vrf-blue)# no rp-embedded
```

Source-Specific Multicast with IPv6 PIM

Using the Any-Source Multicast (ASM) service model, sources and receivers register with a multicast address. The protocol uses regular messages to maintain a correctly configured broadcast network where all sources can send data to all receivers and all receivers get broadcasts from all sources.

With Source-Specific Multicast (SSM), the "channel" concept is introduced where a "channel" consists of a single source and multiple receivers that specifically register to get broadcasts from that source. Consequently, receivers are not burdened with receiving data they have no interest in, and network bandwidth requirements are reduced because the broadcast need only go to a subset of users. The address range ff30:/12 has been assigned by the Internet Assigned Numbers Authority (IANA) for use with SSM.

SSM simplifies IPv6 PIM-SM by eliminating the RP and all protocols related to the RP.

Configuring IPv6 PIM Source-Specific Multicast

You can configure Source-Specific Multicast (SSM) on any interface that is IPv6 PIM SM enabled.

IPv6 PIM-SM must be enabled on any ports on which you want SSM to operate. Use the **ssm-enable** command under the IPv6 router PIM level to globally enable SSM filtering.

To enable SSM for a specified VRF, refer to the example after the task steps.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable IPv6 PIM.

```
device(config)# ipv6 router pim
```

3. Configure an SSM group range. The IPv6 address and mask specifies the multicast address for the SSM address range.

```
device(config-ipv6-pim-router)# ssm-enable range ff30::/12
```

4. To display information for PIM SSM group ranges, use the **show ipv6 pim sparse** command.

```
device> show ipv6 pim sparse

Global PIM Sparse Mode Settings
  Maximum Mcache          : 4096        Current Count              : 7
  Hello interval          : 30          Neighbor timeout           : 105
  Join/Prune interval     : 60          Inactivity interval        : 180
  Hardware Drop Enabled   : Yes         Prune Wait Interval        : 3
  Bootstrap Msg interval  : 60          Candidate-RP Msg interval  : 60
  Register Suppress Time  : 60          Register Probe Time        : 10
  Register Stop Delay     : 10          Register Suppress interval : 60
  SSM Enabled             : Yes         SPT Threshold              : 1
  SSM Group Range         : ff30::/12
  Route Precedence        : mc-non-default mc-default uc-non-default uc-default
  Embedded RP Enabled     : Yes
```

The following example enables SSM for a specified VRF and a user-defined address range.

```
device# configure terminal
device(config)# ipv6 router pim vrf blue
device(config-ipv6-pim-router-vrf-blue)# ssm-enable range ff30:/12
```

Configuring a DR Priority

This task assumes that IPv6 PIM is configured on your network.

The DR priority option lets a network administrator give preference to a particular router in the DR election process by giving it a numerically higher DR priority. To set a DR priority higher than the default value of 1, use the **ipv6 pim dr-priority** command as shown in the following configuration example.

```
device# configure terminal
device(config)# interface ethernet 3/2/4
device(config-if-e10000-3/2/4)# ipv6 pim dr-priority 50
```

To set a DR priority higher than the default value of 1 on a virtual Ethernet interface 10.

```
device# configure terminal
device(config)# interface ve 10
device(config-vif-10)# ipv6 pim dr-priority 50
```

The following information may be useful for troubleshooting when setting the DR priority:

- If more than one router has the same DR priority on a subnet (as in the case of default DR priority on all), the router with the numerically highest IPv6 address on that subnet will get elected as the DR.
- The DR priority information is used in the DR election only if all the IPv6 PIM routers connected to the subnet support the DR priority option. If there is at least one IPv6 PIM router on the subnet that does not support this option, then the DR election falls back to the backwards compatibility mode in which the router with the numerically highest IPv6 address on the subnet is declared the DR regardless of the DR priority values.

Passive Multicast Route Insertion

To prevent unwanted multicast traffic from being sent to the CPU, IPv6 PIM routing and Passive Multicast Route Insertion (PMRI) can be used together to ensure that multicast streams are only forwarded out ports with interested receivers and unwanted traffic is dropped in hardware on Layer 3 routers.

PMRI enables a Layer 3 switch running IPv6 PIM Sparse to create an entry for a multicast route, for example, (S,G), with no directly attached clients or when connected to another PIM router (transit network).

When a multicast stream has no output interfaces, the Layer 3 switch can drop packets in hardware if the multicast traffic meets the following conditions in IPv6 PIM-SM.

- The route has no OIF.
- The directly connected source passes source RPF check and completes data registration with the RP, or the non-directly connected source passes source RPF check.

If the OIF is inserted after the hardware-drop entries are installed, the hardware entries will be updated to include the OIFs.

NOTE
Disabling hardware-drop does not immediately take away existing hardware-drop entries, they will go through the normal route aging processing when the traffic stops.

Viewing PMRI Status and Disabling PMRI

Passive multicast route insertion (PMRI) is enabled by default. In some situations you may need to view the PMRI status and use the hardware-drop feature to disable PMRI.

After determining that PMRI is enabled, you must enable IPv6 PIM routing and then disable PMRI using the hardware-drop feature syntax.

You can disable PMRI for a specified VRF if you specify the VRF when enabling IPv6 PIM.

1. Use the **show ipv6 pim sparse** command to display the status of PMRI.

```
device> show ipv6 pim sparse

Global PIM Sparse Mode Settings
  Maximum Mcache         : 4096        Current Count              : 7
  Hello interval         : 30          Neighbor timeout           : 105
  Join/Prune interval    : 60          Inactivity interval        : 180
  Hardware Drop Enabled  : Yes         Prune Wait Interval        : 3
  Bootstrap Msg interval : 60          Candidate-RP Msg interval  : 60
  Register Suppress Time : 60          Register Probe Time        : 10
  Register Stop Delay    : 10          Register Suppress interval : 60
  SSM Enabled            : Yes         SPT Threshold              : 1
  SSM Group Range        : ff30::/32
  Route Precedence       : mc-non-default mc-default uc-non-default uc-default
  Embedded RP Enabled    : Yes
```

   In the output, you can see that the hardware-drop is enabled meaning that PMRI is enabled.

2. Enter global configuration mode.

```
device# configure terminal
```

3. Configure IPv6 PIM.

```
device(config)# ipv6 router pim
```

4. To disable PMRI, use the **hardware-drop-disable** command.

```
device(config-ipv6-pim-router)# hardware-drop-disable
```

The following example displays the status of PMRI and then disables PMRI using the hardware-drop feature.

```
device# show ipv6 pim sparse
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# hardware-drop-disable
```

Clearing the IPv6 PIM Traffic Counters and Forwarding Cache

You can clear IPv6 PIM traffic counters, IPv6 PIM message counters and the IPv6 PIM forwarding cache. For each of the following options, you can clear the counters or cache for a VRF instance using the **vrf** keyword for the VRF specified by the *vrf-name* variable.

To clear IPv6 PIM traffic counters, enter the **clear ipv6 pim traffic** command.

```
device# clear ipv6 pim traffic
```

To clear the IPv6 PIM message counters, use the **clear ipv6 pim counters** command.

```
device# clear ipv6 pim counters
```

To clear the IPv6 PIM forwarding cache, use the **clear ipv6 pim cache** command.

```
device# clear ipv6 pim cache
```

Use the **vrf** parameter to clear the IPv6 PIM forwarding cache for a VRF instance specified by the *vrf-name* variable.

Defining the Maximum Number of IPv6 PIM Cache Entries

You can define the maximum number of IPv6 PIM multicast cache entries.

You can use the **max-mcache** command to define the maximum number of repeated IPv6 PIM traffic packets being sent from the same source address and being received by the same destination address. To define the maximum number of IPv6 PIM cache entries for the default VRF, use the following steps. You can also define this number for a specific VRF when you add the VRF name to the **ipv6 router pim** command in step 2.

If the maximum number of IPv6 PIM multicast cache entries is not defined by the user, the maximum value is determined by the **system max pim6-hw-mcache** command, or by available system resources.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable IPv6 PIM globally.

```
device(config)# ipv6 router pim
```

3. Define the maximum number of IPv6 PIM cache entries.

```
device(config-ipv6-pim-router)# max-mcache 999
```

The following example defines the maximum number of IPv6 PIM cache entries as 999.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# max-mcache 999
```

Configuring a Static Multicast Route Within a VRF

You can configure a static multicast route within a virtual routing instance (VRF).

1. Configure a VRF.

```
device(config)# vrf vpn1
```

2. Configure the VRF address family for IPv6 and enter IPv6 address family configuration mode.

```
device(config-vrf-vpn1)# address-family ipv6
```

3. Configure the destination IPv6 address.

```
device(config-vrf-vpn1-ipv6)# ipv6 mroute 2001:0DB8:0:1::1/120 5100::192:1:1:1
```

Configuring the Route Precedence by Specifying the Route Types

Precedence tables specify how routes are selected for multicast.

IPv6 PIM must be enabled at the global level.

Configure the **none** keyword to fill up the precedence table and ignore certain types of routes.

1. Enable IPv6 PIM at the global level.

```
device(config)# ipv6 router pim
```

2. Configure a precedence table.

```
device(config-ipv6-pim-router)# route-precedence mc-non-default uc-non-default mc-default uc-default
```

The command configures a precedence table for multicast route selection that first looks for a non-default route from the mRTM, then a non-default route from the uRTM, then a default route from the mRTM, and then a default route from the uRTM.

3. Configure the **none** keyword to fill up the precedence table in order to ignore certain types of route.

```
device(config-ipv6-pim-router)# route-precedence mc-non-default mc-default uc-non-default none
```

The command configures a precedence table for multicast route selection that ignores the default route from uRTM .

4. Return to global configuration mode.

```
device(config-ipv6-pim-router)# exit
```

5. Enable IPv6 PIM for a VRF.

```
device(config)# ipv6 router pim vrf blue
```

6. Configure a precedence table for the VRF.

```
device (config-ipv6-pim-router-vrf-blue)# route-precedence mc-non-default uc-non-default mc-default
uc-default
```

   The command configures a precedence table that specifies a non-default route from the mRTM, then a non-default route from the uRTM, then a default route from the mRTM, and then a default route from the uRTM for the specified VRF,.

7. Configure the **none** keyword to fill up the precedence table.

```
device(config-ipv6-pim-router-vrf-blue)# route-precedence mc-non-default mc-default uc-non-default
none
```

   The command configures a precedence table that specifies the unicast default route for multicast for the specified VRF.

The following examples show how to configure the route precedence and display the route-precedence setting.

```
device(config-ipv6-pim-router)# route-precedence mc-non-default mc-default uc-non-default uc-default
device(config-ipv6-pim-router)# show ipv6 pim sparse

Global PIM Sparse Mode Settings
  Maximum Mcache           : 12992      Current Count                 : 2
  Hello interval           : 30         Neighbor timeout              : 105
  Join/Prune interval      : 60         Inactivity interval           : 180
  Hardware Drop Enabled    : Yes        Prune Wait Interval           : 3
  Bootstrap Msg interval   : 60         Candidate-RP Msg interval     : 60
  Register Suppress Time   : 60         Register Probe Time           : 10
  Register Stop Delay      : 10         Register Suppress interval    : 60
  SSM Enabled              : No         SPT Threshold                 : 1
  Route Precedence         : mc-non-default mc-default uc-non-default uc-default
  Embedded RP Enabled      : Yes

device(config-ipv6-pim-router)# route-precedence admin-distance
device(config-ipv6-pim-router)# show ipv6 pim sparse

Global PIM Sparse Mode Settings
  Maximum Mcache           : 12992      Current Count                 : 2
  Hello interval           : 30         Neighbor timeout              : 105
  Join/Prune interval      : 60         Inactivity interval           : 180
  Hardware Drop Enabled    : Yes        Prune Wait Interval           : 3
  Bootstrap Msg interval   : 60         Candidate-RP Msg interval     : 60
  Register Suppress Time   : 60         Register Probe Time           : 10
  Register Stop Delay      : 10         Register Suppress interval    : 60
  SSM Enabled              : No         SPT Threshold                 : 1
  Route Precedence         : admin-distance
  Embedded RP Enabled      : Yes
device(config-ipv6-pim-router)
```

Configuring IPv6 PIM Neighbor Filtering

You can configure an ACL and apply it to an interface to control neighbor access.

1. Configure an ACL named f10.

```
device(config)# ipv6 access-list f10
```

2. Configure ACL f10 to deny access to the device fe80::102.

```
device(config-ipv6-access-list f10)# deny ipv6 host fe80::102 any
```

   NOTE
   In this case, fe80::102 is is the link-local address of the interface.

3. Configure ACL f10 to permit access to all other devices.

```
device(config-ipv6-access-list f10)# permit ipv6 any any
```

4. Return to global configuration mode.

```
device(config-ipv6-access-list f10)# exit
```

5. Configure an Ethernet interface.

```
device(config)# interface ethernet 1/3/2
```

   This command configures an interface and enters interface configuration mode.

6. Configure a filter that applies ACL f10 to the interface.

```
device(config-if-e1000-1/3/2)# ipv6 pim neighbor-filter f10
```

   This command prevents the host that is specified in ACL f10, fe80::102, from becoming an IPv6 PIM neighbor on the interface.

IPv6 PIM Join and Prune Policy

The IPv6 PIM Join and Prune Policy provides the capability for the following options to be configured:

- (RP, G) J/P filtering: Permit or deny PIM (*, G) J/P messages for IP multicast group addresses with a given RP.
- (*, G) J/P filtering: Permit or deny PIM (*, G) J/P messages for IP multicast group addresses independent of RP.
- (S, G) J/P filtering: Permit or deny PIM (S, G) J/P messages for IP multicast sources and group addresses.

Access control lists (ACLs) are used to define the policy.

By default, all PIM routers accept Join and Prune messages for all the multicast group addresses and for all source addresses. When the IPv6 PIM Join and Prune policy is configured, a PIMv6 network is prevented from forwarding multicast traffic for reserved or unauthorized groups, which could lead to the overuse of available bandwidth of the links and the overuse of software or hardware resources on PIM routers.

With the IPv6 PIM Join and Prune policy, a device can be configued to drop PIM J/P messages of: the following types:

- (*, G) sent to a given RP for unauthorized groups.
- (*, G) for unauthorized groups independent of RP.
- (S, G) for unauthorized groups and sources.

Configuration Notes and Feature Limiations

- A (RP, G) configuration is limited to 64 IPv4 RPs and 64 IPv6 RPs per VRF. Although ICX can support more than 64 RPs (learned dynamically through Bootstrap Protocol), there is a limited number of RPs generally in a given network..
- ACL rules are used to configure which multicast group addresses (*, G) are sent to the RP, and which are to be dropped or allowed. Multicast group address and prefixes are configured as destination IP addresses and prefixes in the extended ACL rules. Because this ACL is used for (RP, G) filtering, the source IP address and prefixes in the case of extended ACL rules are ignored.
- Only one ACL can be applied to an RP address.
- If the specified ACL is not configured, then the (*, G) Join and Prune messages sent to that RP for all multicast group addresses are dropped.
- Only one ACL can be applied to both (*, G) and (S, G) Join and Prune filtering at a time.

Configuring IPv6 PIM Join and Prune Policy

IPv6 PIM Join and Prune policies can be configured.

Complete the following steps to configure the PIMv6 (RP, G) jp-policy. An ACL list is specified

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable PIMv6 globally.

```
device(config)# ipv6 router pim
```

3. Configure the IPv6 PIM Join and Prune policy, specifying an RP address and an ACL list.

```
device(config-ipv6-pim-router)# jp-policy 10:10::10:10 testacl
```

4. Configure the IPv6 PIM Join and Prune policy, specifying another RP address and an ACL list.

```
device(config-ipv6-pim-router)# jp-policy 22:9::9:9 testacl
```

5. Configure the IPv6 PIM Join and Prune policy, specifying another RP address and an ACL list.

```
device(config-ipv6-pim-router)# jp-policy 100:9::9:9 testacl
```

The following example configures the PIM (RP, G) Join and Prune policy. An ACL number is specified.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# jp-policy 10:10::10:10 testacl
device(config-ipv6-pim-router)# jp-policy 22:9::9:9 testacl
device(config-ipv6-pim-router)# jp-policy 100:9::9:9 testacl
```

The following example unconfigures a previously configured PIMv6 (RP, G) Join and Prune policy for a non-default VRF instance.

```
ddevice# configure terminal
device(config)# ipv6 router pim vrf blue
device(config-ipv6-pim-router-vrf-blue)# no jp-policy 10:10::10:10 testacl
device(config-ipv6-pim-router-vrf-blue)# no jp-policy 22:9::9:9 testacl
device(config-ipv6-pim-router-vrf-blue)# no jp-policy 100:9::9:9testacl
```

The following example configures the PIMv6 (*, G) and (S, G) Join and Prune policy for the default VRF. An ACL name is specified.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# jp-policy wg-sg-acl
```

The following example unconfigures a previously configured PIM (*, G) and (S, G) Join and Prune policy.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# no jp-policy wg-sg-acl
```

IPv6 PIM Convergence on MAC Address Movement

IPv6 PIM convergence occurs when the IPv6 PIM module is notified of a topology change.

The notification is triggered upon a change in port status, Reverse Path Forwarding (RPF) failure in the hardware, or by the unicast routing module if there is a change in the Layer 3 topology. If the topology change occurs without a change in port status or RPF failure, or if the Layer 3 topology change is not notified by the unicast routing module, IPv6 PIM convergence does not take place.

If there is a change in the source traffic at Layer 2 interface, the RPF check fails because only loose RPF check is supported (loose RPF check detects the change in the source traffic only at the Layer 3 interface level). A notification for a change in the source traffic at the Layer 2 interface can be triggered by MAC address movement. The MAC address movement notification triggers RPF check on MAC address movement for directly connected sources. The MAC address movement notification can be triggered by configuring the **ipv6 multicast-routing rpf-check mac-movement** command. The MAC address movement notification triggers a notification to the IPv6 PIM module which results in convergence. IPv6 PIM convergence is supported only in IPv6 PIM Sparse mode and is not supported in IPv6 PIM Dense mode.

PIM convergence on MAC address movement is supported on RUCKUSICX 7150, ICX 7250, ICX 7450, ICX 7550, ICX 7650, and ICX 7850 devices.

NOTE
IPv6 PIM convergence on MAC address movement is applicable only when the multicast source and IPv6 PIM routers are in the same Layer 2 domain.

IPv6 PIM Anycast RP

IPv6 PIM Anycast RP is a method of providing load balancing and fast convergence to IPv6 PIM RPs in an IPv6 multicast domain. The RP address of the Anycast RP is a shared address used among multiple IPv6 PIM routers, known as IPv6 PIM RP. The IPv6 PIM RP routers create an Anycast RP set. Each router in the Anycast RP set is configured using two IPv6 addresses: a shared RP address in their loopback address and a separate, unique IPv6 address. The loopback address must be reachable by all IPv6 PIM routers in the multicast domain. The separate, unique IPv6 address is configured to establish static peering with other IPv6 PIM routers and communication with the peers.

When the source is activated in an IPv6 PIM Anycast RP domain, the IPv6 PIM First Hop (FH) will register the source to the closest IPv6 PIM RP. The IPv6 PIM RP follows the same MSDP Anycast RP operation by decapsulating the packet and creating the (S,G) state. If there are external peers in the Anycast RP set, the router will re-encapsulate the packet with the local peering address as the source address of the encapsulation. The router will unicast the packet to all Anycast RP peers. The re-encapsulation of the data register packet to Anycast RP peers ensures source state distribution to all RPs in a multicast domain.

Configuring IPv6 PIM Anycast RP

IPv6 PIM Anycast RP can be configured to map RP and Anycast RPs.

NOTE
MSDP and Anycast RP do not interoperate. If transitioning from MSDP to Anycast RP or vice versa, all RPs in the network must be configured for the same method of RP peering; either Anycast RP or MSDP.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable IPv6 PIM.

```
device(config)# ipv6 router pim
```

3. Configure an RP address.

```
device(config-ipv6-pim-router)# rp-address 1001::1
```

The RP address is shared among multiple IPv6 PIM routers.

4. Configure IPv6 PIM Anycast RP.

```
device(config-ipv6-pim-router)# anycast-rp 1001::1 my-anycast-rp-set-acl
```

   The **anycast-rp** command defines the mapping of the RP and the Anycast RP peers using a host-based simple ACL to specify the address of the Anycast RP set.

5. Exit to privileged EXEC mode.

```
device(config-ipv6-pim-router)# end
```

6. Display information for an IPv6 PIM Anycast RP interface.

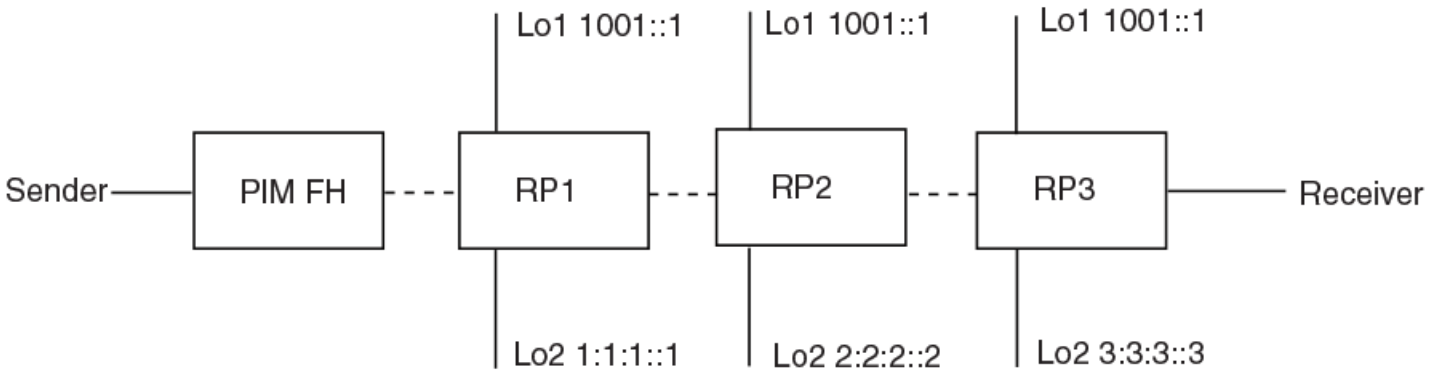
```
device> show ipv6 pim anycast-rp

    Number of Anycast RP: 1
    Anycast RP: 1001::1
      ACL ID: 200
      ACL Name: my-anycast-rp-set
      ACL Filter: SET
      Peer List:
       1:1:1::1
       2:2:2::2
       3:3:3::3
```

The example shown in the following figure is an IPv6 PIM Anycast-enabled network with three RPs and one PIM-FH router connecting to its active source and local receiver. Loopback 2 in RP1, RP2, and RP3 each have the same IPv6 addresses 1001:1. Loopback 3 in RP1, RP2, and RP3 each have separate IPv6 address configured to communicate with their peers in the Anycast RP set.

The RP shared address 1001:1 is used in the PIM domain. IPv6 addresses 1:1:1::1, 2:2:2::2, and 3:3:3::3 are listed in the ACL that forms the self-inclusive Anycast RP set. Multiple Anycast RP instances can be configured on a system; each peer with the same or different Anycast RP set.

FIGURE 17 Example of an IPv6 PIM Anycast RP Network



NOTE
The IPv6 PIM Anycast CLI applies to only IPv6 PIM routers running RP. All deny statements in the my-anycast-rp-set ACL are ignored.

The following example is a configuration of IPv6 PIM Anycast RP 1001::1.The example avoids using the loopback 1 interface when configuring IPv6 PIM Anycast RP because the loopback 1 address could be used as a router-id. An IPv6 PIM First Hop router will register the source with the closest RP. The first RP that receives the register will re-encapsulate the register to all other Anycast RP peers. Refer to the preceding figure for a view of the IPv6 PIM Anycast RP Network.

The RP shared address 1001:1 is used in the IPv6 PIM domain. IPv6 addresses 1:1:1::1, 2:2:2::2, and 3:3:3::3 are listed in the ACL that forms the self-inclusive Anycast RP set. Multiple Anycast RP instances can be configured on a system; each peer with the same or different Anycast RP set.

```
device(config)# interface loopback 2
device(config-lbif-2)# ipv6 address 1001::1/96
device(config-lbif-2)# ipv6 pim-sparse
device(config-lbif-2)# interface loopback 3
device(config-lbif-3)# ipv6 address 1:1:1::1/96
device(config-lbif-3)# ipv6 pim-sparse
device(config-lbif-3)# ipv6 router pim
device(config-ipv6-pim-router)# rp-address 1001::1
device(config-ipv6-pim-router)# anycast-rp 1001::1 my-anycast-rp-set
device(config-ipv6-pim-router)# ipv6 access-list my-anycast-rp-set
device(config-ipv6-access-list my-anycast-rp-set)# permit ipv6 host 1:1:1::1 any
device(config-ipv6-access-list my-anycast-rp-set)# permit ipv6 host 2:2:2::2 any
device(config-ipv6-access-list my-anycast-rp-set)# permit ipv6 host 3:3:3::3 any
```

Displaying IPv6 PIM Information

You can use various **show** commands to view information about IPv6 PIM.

Use one of the following commands to view IPv6 PIM information. The commands do not need to be entered in the specified order. Using these commands is optional and they can be entered in any order. For more information on the full list of **show ipv6 pim** commands, refer to the *RUCKUS FastIron Command Reference*.

1. Enter the **show ipv6 pim sparse** command to display IPv6 PIM sparse configuration information.

```
device> show ipv6 pim sparse

Global PIM Sparse Mode Settings
Maximum Mcache             : 2048             Current Count                 : 0
Hello interval             : 30               Neighbor timeout              : 105
Join/Prune interval        : 60               Inactivity interval           : 180
Hardware Drop Enabled      : Yes              Prune Wait Interval           : 3
Bootstrap Msg interval     : 60               Candidate-RP Msg interval     : 60
Register Suppress Time     : 60               Register Probe Time           : 10
Register Stop Delay        : 10               SPT Threshold                 : 1
SSM Enabled                : No
Route Precedence           : uc-non-default uc-default mc-non-default mc-default
Embedded RP Enabled        : Yes
Slow Path Disable All      : No               Slow Path Enable SSM          : No
Slow Path Filter Acl       : None             Register Rate Limit           : 15 pps
                                              Register Filter               :  pim_reg_acl
```

2. Enter the **show ipv6 pim interface** command, and specify an interface, to display IPv6 PIM multicast information for the interface.

```
device> show ipv6 pim interface ethernet 1/1/7

Flags     : SM  - Sparse Mode v2
---------+-----------------------------------------------------+----+---+---+---------+-------
+----------------
Interface|Global Address                                        |Mode|St |TTL|Multicast|  VRF   | DR    |
Override
         |  + Designated Router                          Port |    |   |Thr|Boundary |        | Prio |
Interval
---------+-----------------------------------------------------+----+---+---+---------+-------
+----------------
   e1/1/1 a141::1                                             SM   Ena   1 None      default 1
3000ms
            + Itself
Total Number of Interfaces : 1
```

3. Enter the **show ipv6 pim group** command to display IPv6 PIM group information.

```
device> show ipv6 pim group

Total number of groups: 1
1    Group ff7e:a40:2001:3e8:27:0:1:2
     Group member at  e1/3/1: v31
```

4. Enter the **show ipv6 pim bsr** command to display bootstrap router (BSR) information. The following example shows information for a device that has been elected as the BSR.

```
device> show ipv6 pim bsr

PIMv2 Bootstrap information for Vrf Instance : default-vrf
------------------------------------------------------------------
This system is the Elected BSR
BSR address: 2006:1001::1. Hash Mask Length 64. Priority 32.
Next bootstrap message in 00:01:00
Configuration:
 Candidate loopback 1 (Address 2006:1001::1). Hash Mask Length 64. Priority 32.
Next Candidate-RP-advertisment in 00:00:50
 RP: 2006:1001::1
  group prefixes:
  ff00:: / 8
 Candidate-RP-advertisement period: 60
 Candidate-RP-advertisement period: 60

 Candidate-RP-advertisement period: 60
```

5. Enter the **show ipv6 rp-candidate** command to display candidate RP information.

```
device> show ipv6 pim rp-candidate

Next Candidate-RP-advertisement in 00:00:10
  RP: 1be::11:21
    group prefixes:
    ff00:: / 8
  Candidate-RP-advertisement period: 60
```

6. Enter the **show ipv6 pim rp-map** command to display RP-to-group-mappings.

```
device> show ipv6 pim rp-map

Number of group-to-RP mappings: 3
--------------------------------------------------------------------------------
S.No  Group address   RP address
--------------------------------------------------------------------------------
1     ff07::c:1       3200:12::32
2     ff07::c:2       3200:12::32
3     ff07::c:3       3200:12::32
Number of group-to-RP mappings: 3
```

7. Enter the **show ipv6 pim rp-set** command to display the RP set list.

```
device> show ipv6 pim rp-set

Static RP
---------
Static RP count: 1
100::1
Number of group prefixes Learnt from BSR: 0
No RP-Set present
```

8. Enter the **show ipv6 pim neighbor** command to display information about IPv6 PIM neighbors.

```
device> show ipv6 pim neighbor

-------+--------+--------------------------+--------+---+
PPort  |PhyPort |Neighbor                  |Holdtime|T  |
       |        |                          |sec     |Bit|
-------+--------+--------------------------+--------+---+-
vv503   e2/1/11  fe80::204:ff:fe05:6         105      1
                + 2006:503::1001
vv503    2/1/11  fe80::768e:f8ff:fe2c:cb80   105      1
                 + 2006:503::1004
Total Number of Neighbors : 2
```

9. Enter the **show ipv6 pim mcache** command to display the IPv6 PIM multicast cache.

```
device> show ipv6 pim mcache

IP Multicast Mcache Table
Entry Flags    : SM  - Sparse Mode, SSM - Source Specific Multicast, DM - Dense Mode
                 RPT    - RPT Bit, SPT - SPT Bit, LSRC - Local Source, LRCV - Local Receiver
                 HW - HW Forwarding Enabled, FAST - Resource Allocated, TAG - Need For Replication
Entry
                 REGPROB - Register In Progress, REGSUPP - Register Suppression Timer
                 MSDPADV - Advertise MSDP, NEEDRTE - Route Required for Src/RP,  PRUN - DM Prune
Upstream
Interface Flags: IM - Immediate, IH - Inherited, WA - Won Assert
                 MJ - Membership Join, MI - Membership Include, ME - Membership Exclude
                 BR - Blocked RPT, BA - Blocked Assert, BF - Blocked Filter, BI - Blocked IIF
Total entries in mcache: 4
1    (*, ff05::4422) RP 2006:1001::1, in v503 (tag e2/1/11), Uptime 1d 00:27:26 (SM)
     upstream neighbor fe80::204:ff:fe05:6 (2006:503::1001)
     Flags (0x002604a2) SM RPT LRCV TAG
     slow ports: ethe 3/1/1
     AgeSltMsk: 0,  IPMC:   417 , RegPkt: 0
     Forwarding_oif: 1, Immediate_oif: 1, Blocked_oif: 0
     L3 (SW) 1:
       e3/1/1(VL170), 1d 00:27:26/0, Flags: MJ
2    (2006:170::1010, ff34::500) in v170 (tag e3/1/1), Uptime 00:37:51, Rate 0 (SM)
     Source is directly connected. RP 2006:1001::1
     Flags (0x20429ce1) SM SPT REG L2REG LSRC HW FAST TAG
     fast ports: ethe 2/1/11
     AgeSltMsk: 1,  IPMC:   417 , RegPkt: 0
     Forwarding_oif: 1, Immediate_oif: 1, Blocked_oif: 0
     L3 (HW) 1:
       TR(e2/1/11,e2/1/11)(VL503), 00:37:26/183, Flags: IM
    Src-Vlan: 170
```

10. Enter the **show ipv6 pim traffic** command to display IPv6 PIM traffic statistics.

```
device> show ipv6 pim traffic

Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Rx        Rx          Rx        Rx        Rx        Rx        Rx        Rx
------+---------+-----------+---------+---------+---------+---------+---------+---
v170    0         0           0         0         0         0         0         0
v501    0         0           0         0         0         0         0         0
v503    3302      2524        0         0         0         0         0         0
Port    HELLO     JOIN-PRUNE  ASSERT    REGISTER  REGISTER  BOOTSTRAP CAND. RP  Err
                                        GRAFT(DM) STOP(SM)  MSGS (SM) ADV. (SM)
-------+---------+-----------+---------+---------+---------+---------+---------+---
       Tx        Tx          Tx        Tx        Tx        Tx        Tx
------+---------+-----------+---------+---------+---------+---------+---------+---
v170    3576      0           0         0         0         0         0
v501    1456      0           0         0         0         0         0
v503    1456      1314        0         0         0         2         0
```

11. Enter the **show ipv6 pim anycast-rp** command to display information for an IPv6 PIM Anycast RP interface.

```
device> show ipv6 pim anycast-rp

    Number of Anycast RP: 1
    Anycast RP: 1001::1
      ACL ID: 200
      ACL Name: my-anycast-rp-set
      ACL Filter: SET
      Peer List:
       1:1:1::1
       2:2:2::2
       3:3:3::3
```

12. Enter the **show ipv6 pim jp-policy** command to display IPv6 PIM (RP, G), (*, G), and (S, G) Join and Prune policy configuration information and the number of Join and Prune drops for each such policy.

```
device> show ipv6 pim jp-policy

Vrf Instance : default-vrf
---------------------------
(RP, G) JP policy
---------

(RP, G) JP policy count: 3

RP-Address     ACL Name (RP, G)     Join Drops (RP, G)     Prune Drops
10:9::9:9         test-acl              1500                   499
22:9::9:9           122                 1888                   1000
100:9::9:9        test-acl              921                    300
---------------------------
(*, G) and (S, G) JP policy
---------

ACL Name (*, G)   Join Drops (*, G)   Prune Drops (S, G)    Join Drops (S, G)   Prune Drops
wg-sg-acl           1500                    499                  385              139
```

13. Enter the **show ipv6 pim error** command to display information for IPv6 PIM error counters.

```
device> show ipv6 pim error

Vrf Instance : default-vrf
-------------------------------------
Protocol errors:
PIM_PKT_DRP   : 0    PIM_PKT_DRP(Glb)       : 0
MCGRP_PKT_DRP : 0    MCGRP_PKT_DRP(Gl)      : 0
PIM_THR_DRP   : 0    PIM_THR_DRP(Glb)       : 0
MCGRP_THR_DRP : 0    MCGRP_THR_DRP(Gl)      : 0
RPSET_MAXED   : 0    Join/Prune Drops      : 1999
Forwarding Errors (Packets Drops):
RPF-Fail: 0 No-RP   : 0 IfMsmtch: 0
OIFEmpty: 0 InvldIf : 0 TTLXpire: 0
NoFwEntr: 0 TrkMove : 0 PortMove: 0
NoCause : 0 FwEntrFl: 0 ResFail : 0
SSMNoEnt: 0 InvldGrp: 0 BidirSW : 0
WrongIf : 0 IPCError: 0 IPCBufEr: 0
DMACErr : 0
```

Multicast Listener Discovery and Source-specific Multicast Protocols

Multicast Listener Discovery Version 2 (MLDv2) protocol is supported. IPv6 routers use the MLDv2 protocol to discover multicast listeners, or nodes that wish to receive multicast packets on directly attached links. MLDv2 supports source filtering, the ability of a node to send reports on traffic that is from a specific source address or from all multicast addresses except the specified source addresses. The information is then provided to the source-specific multicast (SSM) routing protocols such as PIM-SSM.

The IPv6 router stores a list of multicast addresses for each attached link. For each multicast address, the IPv6 router stores a filter mode and a source list. The filter mode is set to INCLUDE if all nodes in the source list for a multicast address are in the INCLUDE state. If the filter mode is INCLUDE, then only traffic from the addresses in the source list is allowed. The filter mode is set to EXCLUDE if at least one of the nodes in the source list is in an EXCLUDE state. If the filter mode is EXCLUDE, traffic from nodes in the source list is denied and traffic from other sources is allowed.

The source list and filter mode are created when the IPv6 querier router sends a query. The querier router is the one with the lowest source IPv6 address. It sends out any of the following queries:

- General query: The querier sends this query to learn all multicast addresses that need to be listened to on an interface.
- Address specific query: The querier sends this query to determine if a specific multicast address has any listeners.
- Address specific and source specific query: The querier sends this query to determine if specified sources of a specific multicast address have any listeners.

In response to these queries, multicast listeners send the following reports:

- Current state: This report specifies the source list for a multicast address and whether the filter mode for that source list is INCLUDE or EXCLUDE.
- Filter-mode change: This report specifies if there has been a change to the filter mode for the source list and provides a new source list.
- Source list change: This report specifies the changes to the source list.

Enabling MLDv2

The default MLD version when IPv6 PIM is enabled is MLDv1. You must configure the **ipv6 mld version 2** command to enable MLDv2.

You can configure MLDv2 globally, on an interface, or for a specified VRF. Refer to the **ipv6 mld version** command in the *RUCKUS FastIron Command Reference*. To enable MLDv2 for a specified VRF, use the following steps.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable IPv6 PIM SM for a VRF named blue.

```
device(config)# ipv6 router pim vrf blue
```

3. Enable MLDv2 for VRF blue.

```
device(config-ipv6-pim-router-vrf-blue)# ipv6 mld version 2
```

The following example enables IPv6 PIM for the VRF named blue and enables MLDv2.

```
device# configure terminal
device(config)# ipv6 router pim vrf blue
device(config-ipv6-pim-router-vrf-blue)# ipv6 mld version 2
```

After enabling MLDv2, you can set MLD options for the default or a specified VRF. Refer to Configuring MLD Options for Default and Non-Default VRFs on page 171.

Configuring MLD Options for Default and Non-Default VRFs

Multicast Listener Discovery Version 2 (MLDv2) allows you to configure options on default and non-default virtual routing instances (VRFs).

MLDv1 is the default MLD version when IPv6 PIM Sparse Mode (PIM-SM) is enabled on an interface. You must configure MLDv2 on an interface to enable MLDv2.

The following option configurations are outlined in the following steps:

- Modify the group membership time: Group membership time defines how long a group will remain active on an interface in the absence of a group report. Values range from 5 through 26000 seconds; the default is 260.
- Modify the MLD query interval: Frequency at which multicast listening discovery (MLD) query messages are sent. Values range from 2 through 3600 seconds; the default is 125. The MLD query interval value you enter must be greater than the interval configured for the maximum response time.
- Last Listener Query Interval: The maximum response delay inserted into Multicast-Address-Specific Queries sent in response to done messages, and is also the amount of time between Multicast-Address-Specific Query messages. When the device receives an MLDv1 leave message or an MLDv2 state change report, it sends out a query and expects a response within the time specified by this value.
- Modify the maximum response time: The maximum amount of time a multicast listener has to respond to queries. Values range from 1 through 50 seconds; the default is 10 seconds.
- Modify the maximum number of MLD group addresses: Any MLD group memberships exceeding the group limit are not processed. Values range from 1 through 8192; the default is 4096.
- Robustness: The number of times that the switch sends each MLD message from an interface. Use a higher value to ensure high reliability from MLD. Values range from 2 through 7; the default is 2.

The following steps show how to configure these options for a specific VRF named blue. You can enable IPv6 PIM using the **ipv6 router pim** command without specifying a VRF to make these options apply to the default VRF.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Enable IPv6 PIM-SM for a VRF named blue.

   ```
   device(config)# ipv6 router pim vrf blue
   ```

3. Modify the group membership time to 2000 seconds.

   ```
   device(config-ipv6-pim-router-vrf-blue)# ipv6 mld group-membership-time 2000
   ```

   When multiple devices are connected together, all devices must have the same group membership time configured, which must be at least twice the length of the query interval, so that missing one report does not stop traffic.

4. Modify the frequency at which MLD query messages are sent for a specified VRF, in seconds.

   ```
   device(config-ipv6-pim-router-vrf-blue)# ipv6 mld query-interval 50
   ```

5. Modify the last listener query interval sent for a specified VRF, in seconds.

   ```
   device(config-ipv6-pim-router-vrf-blue)# ipv6 mld llqi 5
   ```

   The range of values is from 1 through 25; the default is 1. Using a lower value allows members to leave groups more quickly.

6. Modify the IGMP maximum response time, in seconds.

```
device(config-ipv6-pim-router-vrf-blue)# ipv6 mld max-response-time 5
```

7. Modify the maximum number of MLD group addresses.

```
device(config-ipv6-pim-router-vrf-blue)# ipv6 mld max-group-address 1000
```

8. Modify the MLD robustness for a specified VRF.

```
device(config-ipv6-pim-router-vrf-blue)# ipv6 mld robustness 3
```

The following example configures various MLD options for a non-default VRF instance.

```
device# configure terminal
device(config)# ipv6 router pim vrf blue
(config-ipv6-pim-router-vrf-blue)# ipv6 mld group-membership-time 2000
device(config-ipv6-pim-router-vrf-blue)# ipv6 mld query-interval 50
device(config-ipv6-pim-router-vrf-blue)# ipv6 mld llqi 5
device(config-ipv6-pim-router-vrf-blue)# ipv6 mld max-response-time 5
device(config-ipv6-pim-router-vrf-blue)# ipv6 mld max-group-address 1000
device(config-ipv6-pim-router-vrf-blue)# ipv6 mld robustness 3
```

Configuring MLD Options on Interfaces

Multicast Listener Discovery (MLD) has options that are configured on interfaces.

The following MLD parameters can be configured at the interface level:

- Version: The default MLD version when IPv6 PIM Sparse Mode (PIM-SM) is enabled is MLDv1. You must configure MLDv2 on an interface to enable MLDv2.
- Port version: The MLD version can be set on a virtual Ethernet (VE) interface.
- MLD tracking: When MLD tracking is enabled, a Layer 3 device tracks all clients that send membership reports. When a leave message is received from the last client, the device immediately stops forwarding to the physical port (without waiting 3 seconds to confirm that no other clients still want the traffic).
- MLD group addresses: The maximum number of MLD group addresses available, either for the default VRF or for a specified non-default VRF instance.

The following steps show how to configure these options for various interfaces.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable IPv6 PIM-SM globally.

```
device(config)# ipv6 router pim
```

3. Return to global configuration mode to configure MLD on an interface.

```
device(config-ipv6-pim-router)# exit
```

4. Configure virtual Ethernet interface 10.

```
device(config)# interface ve 10
```

5. Enable MLDv2 on the virtual interface using one of the two following methods:
   - Set the MLD version on an interface.

     ```
     device(config-vif-10)# ipv6 mld version 2
     ```

   - Set the MLD port version on an interface.

     ```
     device(config-vif-10)# ipv6 mld port-version 2
     ```

   In both these examples, MLDv2 is enabled. MLDv1 is enabled by default when IPv6 PIM-SM is configured.
6. Configure the maximum number of MLD group addresses for the virtual interface.

   ```
   device(config-vif-10)# ipv6 mld max-group-address 1000
   ```

The following example configures IPv6 PIM-SM, enables MLDv2 for virtual Ethernet interface 10, and enables MLD tracking on the interface. It also configures a maximum of 1000 MLD group addresses for the VE interface.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# exit
device(config)# interface ve 10
device(config-vif-10)# ipv6 mld version 2
device(config-vif-10)# ipv6 mld tracking
device(config-vif-10)# ipv6 mld max-group-address 1000
```

Configuring the MLD Report Filter Policy

The MLD report filter policy can be configured globally, for a non-default VRF instance, or for an Interface. The following task configures the MLD report filter policy globally.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Configure the MLD report filter policy globally, specifying an ACL.

   ```
   device(config)# ipv6 mld access-group test1-v6
   ```

   NOTE
   ACL rules are used to configure which multicast group addresses, source addresses, or report and leave messages are to be dropped or allowed. Multicast group addresses and prefixes are configured as destination IP addresses or prefixes, and the source addresses and prefixes are configured as source IP addresses and prefixes in the extended ACL rules.

   NOTE
   If the specified ACL is not configured, the MLD report messages for all multicast group addresses and source addresses are dropped.

   NOTE
   If an MLD report filter policy is configured both globally and at the interface level, only the interface filter is applied.

The following example configures the MLD report filter policy for a VE interface.

```
device# configure terminal
device(config)# interface ve 10
device(config-vif-10)# ipv6 mld access-group test1-v6
```

Setting the Maximum Number of MLD Group Addresses

You can change the maximum number of MLD group addresses for the default virtual routing and forwarding (VRF) instance or a specific VRF, globally or at the interface level.

Complete the following steps to set the maximum number of MLD addresses for a specific VRF.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Specify the VRF.

```
device(config)# vrf vpn1
```

3. Enter IPv6 address family mode.

```
device(config-vrf-vpn1)# address-family ipv6
```

4. Set the maximum number of IGMP group addresses.

```
device(config-vrf-vpn1-ipv6)# ipv6 mld max-group-address 1000
```

The following example sets the maximum number of MLD group addresses for VRF VPN1 to 1000.

```
device# configure terminal
device(config)# vrf vpn1
device(config-vrf-vpn1)# address-family ipv6
device(config-vrf-vpn1-ipv4)# ipv6 mld max-group-address 1000
```

The following example configures a maximum of 1000 MLD group addresses for a VE interface.

```
device# configure terminal
device(config)# interface ve 10
device(config-vif-10)# ipv6 mld max-group-address 1000
```

IPv6 PIM Register Message Rate Limit

When a new source begins transmitting within a IPv6 Protocol Independent Multicast (PIMv6) network, the designated router (DR) encapsulates multicast packets into register messages and forwards them to the rendezvous point (RP). If the source is running at a high data rate with many new sources starting concurrently, pressure can be put on the CPU due to the large number of multicast packet streams being sent to the network. This situation can occur after a network or power failure. To avoid this scenario, the rate limit for the number of register messages should be set to a relatively low value. The rate limit for the number of register messages can be set to a relatively low value to avoid adverse pressure on the CPU when numerous sources start concurrently. This value is based on the known number of multicast sources present.

The following values apply when configuring register message rate limiting usable in both DR and RP switches:

- For a DR, the default rate limit is set to one message per second.
- For an RP, the default rate limit is set to one message per second. The maximum supported rate can be set to 50 packets per second (pps) for all (S, G) pairs counted per VRF.

  NOTE
  In an RP, where both the PIM register message filter rule and the PIM register message rate limit are configured, filtering functionality takes precedence over rate limiting.

When PIM register message rate limit is not configured, a RUCKUS ICX network stack allows a maximum of 1000 register messages for software forwarding. When PIM register message rate limit is configured, the maximum number of supported register messages is 50 per device or VRF.

Configuring the Register Message Rate Limit for PIMv6

The maximum number of register packets sent or received per second by the router can be configured.

Complete the following steps to configure the register message rate limit to 15 packets per second, changing it from the default of 1 packet per second. This rate is applicable to register messages from all sources. This rate is applied to all sources that are permitted by the accept-register filter that is used to block unauthorized sources or groups.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable PIMv6 globally.

```
device(config)# ipv6 router pim
```

3. Set the register rate limit to 15 packets per second.

```
device(config-ipv6-pim-router)# register-rate-limit 15
```

The following example sets the register message rate limit to 15 packets per second for PIMv6.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# register-rate-limit 15
```

IPv6 PIM Register Message Filter Rule

PIMv6 register messages received from a downstream multicast designated router (DR) should be filtered for reserved or any other undesirable multicast groups.

The IPv6 PIM register message filter rule interacts with configured extended IP access control lists (ACLs) at software level to take action to either permit or deny register messages for matching (S, G) IP address rules in the RP. When a deny ACL action matches, the RP sends a register stop message to the DR to further limit new register messages.

Networks that do not maintain a multicast domain and require only the IP multicast service will be required to stand up a PIM-SM router that will be incorporated into the JIE shared tree structure by establishing a peering session with an RP router. This helps to mitigate against risks in order to provide a secured IP core network. All RP devices that are peering with customer PIM-SM routers implement a PIM import policy to block multicast registration requests for reserved or any other undesirable multicast groups.

NOTE
In an RP, where both the PIM register message filter rule and the PIM register message rate limit are configured, filtering functionality takes precedence over rate limiting.

NOTE
Register message filtering depends on the availability of ACL resources in the network.

Configuring the Register Message Filter Rule for PIMv6

Complete the following steps to configure the register message filter rule for PIMv6 so that unauthorized multicast sources or groups are blocked.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable PIMv6 globally.

```
device(config)# ipv6 router pim
```

3. Configure the register message filter rule for PIMv6, specifying an ACL.

```
device(config-ipv6-pim-router)# accept-register pim_reg_acl
```

The following example configures the register message filter rule for PIMv6 with a specified ACL.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-pim-router)# accept-register pim_reg_acl
```

The following example displays PIMv6 Sparse configuration information, including information about the register message filter rule.

```
device> show ipv6 pim sparse

Global PIM Sparse Mode Settings
Maximum Mcache             : 2048             Current Count                : 0
Hello interval             : 30               Neighbor timeout             : 105
Join/Prune interval        : 60               Inactivity interval          : 180
Hardware Drop Enabled      : Yes              Prune Wait Interval          : 3
Bootstrap Msg interval     : 60               Candidate-RP Msg interval    : 60
Register Suppress Time     : 60               Register Probe Time          : 10
Register Stop Delay        : 10               SPT Threshold                : 1
SSM Enabled                : No
Route Precedence           : uc-non-default uc-default mc-non-default mc-default
Embedded RP Enabled        : Yes
Slow Path Disable All      : No               Slow Path Enable SSM         : No
Slow Path Filter Acl       : None             Register Rate Limit          : 15 pps
                                              Register Filter              :  pim_reg_acl
```

Specifying Mulitple Static Multicast Groups

A multicast group is usually learned when an MLDv1 report is received. You can manually configure one or more static groups without having to receive an MLDv1 report. To manually configure more than one static group, there are two syntax options:

- The **count** keyword followed by a number.
- The **to** keyword in between two addresses

The following configuration examples demonstrate how to manually configure multiple static multicast groups.

Configure two static groups on physical interfaces, using the **count** option and starting from ff0d::1.

```
device# configure terminal
device(config) interface ethernet 1/1/5
device(config-if-e1000-1/1/5)# ipv6 mld static-group ff0d::1 count 2
```

Configure two static groups on physical interfaces, using the **to** option and starting from ff0d::1.

```
device# configure terminal
device(config) interface ethernet 1/1/5
device(config-if-e1000-1/1/5)# ipv6 mld static-group ff0d::1 to ff0d::2
```

Configure two static groups on virtual ports, using the **count** option and starting from ff0d::1. When using a virtual Ethernet interface (VE), you must specify the physical Ethernet port on which to add the group address.

```
device# configure terminal
device(config)# interface ve 10
device(config-vif-10)# ipv6 mld static-group ff0d::1 count 2 ethernet 1/1/5
```

Configure two static groups on virtual ports, using the **to** option and starting from ff0d::1. When using a virtual Ethernet interface (VE), you must specify the physical Ethernet port on which to add the group address.

```
device# configure terminal
device(config)# interface ve 10
device(config-vif-10)# ipv6 mld static-group ff0d::1 to ff0d::2 ethernet 1/1/5
```

Clearing MLD Traffic Counters and IPv6 PIM Group Membership Table Cache

You can clear IPv6 MLD traffic counters and the IPv6 PIM group membership table cache. The **clear** commands for IPv6 MLD should only be used in troubleshooting situations or when recovering from error conditions.

The following steps are optional and can be used in any order. To clear IPv6 MLD traffic counters and the IPv6 PIM group membership table cache for a VRF instance, specify the **vrf** keyword and *vrf-name* variable.

1. Clear the IPv6 MLD traffic counters.

   ```
   device# clear ipv6 mld traffic
   ```

2. Clear the IPv6 PIM group membership table cache.

   ```
   device# clear ipv6 pim cache
   ```

Displaying IPv6 MLD Information

You can use various **show** commands to view information about IPv6 Multicast Listener Discovery (MLD).

Use one of the following commands to view IPv6 MLD information. The commands do not need to be entered in the specified order. Using these commands is optional and they can be entered in any order. For more information on the full list of **show ipv6 mld** commands, refer to the *RUCKUS FastIron Command Reference*.

1. Enter the **show ipv6 mld group** command to display the list of multicast groups.

   ```
   device> show ipv6 mld group

   Total 2 groups
   ------------------------------------------------------------------------------------------
   Idx  Group Address                          Port    Intf    GrpCmpV Mode    Timer Srcs
   ----+---------------------------------------+-------+-------+-------+-------+-----+----
      1 ff05::4422                             e3/1/1  v170      Ver1 exclude   221   0
      2 ff3f::300                              e3/1/1  v170      Ver2 include     0   1
   Total number of groups 2
   ```

2. Enter the **show ipv6 mld settings** command, specifying a VRF, to display MLD settings for a non-default VRF instance.

   ```
   device> show ipv6 mld vrf my_vrf settings

   MLD Global Configuration
   Query Interval : 125s Configured Interval : 125s
   Max Response Time : 10s
   Group Membership Time : 260s
   Operating Version : 2 Configured Version : 0
   Robustness Variable : 2
   Last Member Query Interval: 1s Last Member Query Count: 2
   Older Host Present Timer : 260s
   ```

3. Enter the **show ipv6 mld interface** command to display MLD statistics for an interface.

```
device> show ipv6 mld interface

---------+------+---------+-----------------------------------------+--
Intf/Port|Groups| Version | Querier | Timer |V1Rtr| Tracking
|Oper Cfg | Qrr GenQ | |
---------+------+----+----+-----------------------------------------+--
e1/1/1 0 2 - Self 0 0 No Disabled
v40 0 2 - Disabled
e3/1/1 1 2 - Self 0 0 No
e2/1/1 1 2 - Self 0 0 No
e1/1/1 1 2 - Self 0 0 No
v50 0 2 - Disabled
e1/1/2 0 2 - Self 0 0 No
v220 0 2 - Disabled
e1/1/1 3 2 - Self 0 12 No
```

4. Enter the **show ipv6 mld traffic** command to display information on MLD traffic.

```
device> show ipv6 mld traffic

RECEIVE COUNTERS
Port QryV1 QryV2 G-Qry GSQry MbrV1 MbrV2 Leave IsIN IsEX ToIN ToEX ALLO BLK
--------+-----+-----+-----+-----+-----+-----+-----+-----+----+----+----+----+----
Filter: Report 10, Leave 5
TRANSMIT COUNTERS
Port QryV1 QryV2 G-Qry GSQry
--------+-----+-----+-----+-----
e1/1/1 39 0 0 0
Note: All Counter are reset, if anyone reaches 100000 and above
```

IPv6 Multicast Boundaries

The Multicast Boundary feature is designed to selectively allow or disallow multicast flows to configured interfaces.

The **ipv6 multicast-boundary** command allows you to configure a boundary on an IPv6 PIM enabled interface by defining which multicast groups may not forward packets over a specified interface. This includes incoming and outgoing packets. By default, all interfaces that are enabled for multicast are eligible to participate in a multicast flow provided they meet the multicast routing protocol's criteria for participating in a flow.

Configuration Considerations for IPv6 Multicast Boundaries

- Only one ACL can be bound to any interface.
- Normal ACL restrictions apply as to how many software ACLs can be created, but there is no hardware restrictions on ACLs with this feature.
- Creation of a static MLD client is allowed for a group on a port that may be prevented from participation in the group on account of an ACL bound to the port's interface. In such a situation, the ACL would prevail and the port will not be added to the relevant entries.
- Either standard or extended ACLs can be used with the multicast boundary feature. When a standard ACL is used, the address specified is treated as a group address and NOT a source address.
- When a boundary is applied to an ingress interface, all packets destined to a multicast group that is filtered out will be dropped by software. Currently, there is no support to drop such packets in hardware.
- The **ipv6 multicast-boundary** command may not stop clients from receiving multicast traffic if the filter is applied on the egress interface up-stream from RP.

Configuring IPv6 Multicast Boundaries

An IPv6 access list is used to define boundaries for IPv6 PIM enabled interfaces.

This task requires an IPv6 standard or extended access list to be created to filter IPv6 multicast traffic. An IPv6 standard access list is defined in the steps. Other IPv6 access list example configurations follow this task.

This task assumes that IPv6 PIM routing is enabled for the interface used in this task.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Create a standard IPv6 access and permit multicast traffic for group ff1e::300.

```
device(config)# ipv6 access-list acl10
device(config-ipv6-access-list acl10)# permit ipv6 any host ff1e::300
```

3. Deny all other traffic.

```
device(config-ipv6-access-list acl10)# deny ipv6 any any
```

4. Exit to global configuration mode.

```
device(config-ipv6-access-list acl10)# exit
```

5. Enter virtual Ethernet (VE) interface mode.

```
device(config)# interface ve 40
```

6. Configure multicast boundaries for VE 40 using access list 10.

```
device(config-vif-40)# ipv6 multicast-boundary acl10
```

The following example creates IPv6 access list acl10 to permit multicast traffic for group ff1e::300 and deny all other traffic. Access list acl10 is used to define multicast boundaries for IPv6 PIM-enabled interfaces.

```
device# configure terminal
device(config)# ipv6 access-list acl10
device(config-ipv6-access-list acl10)# permit ipv6 any host ff1e::300
device(config-ipv6-access-list acl10)# deny ipv6 any any
device(config-ipv6-access-list acl10)# exit
device(config)# interface ve 40
device(config-vif-40)# ipv6 multicast-boundary acl10
```

ACL to Permit IPv6 Multicast Traffic

To permit IPv6 multicast traffic for group ff1e::300 and deny all other traffic, enter the syntax shown in the following configuration example.

```
device(config)# ipv6 access-list abc
device(config-ipv6-access-list abc)# permit ipv6 any host ff1e::300
device(config-ipv6-access-list abc)# deny ipv6 any any
```

To permit IPv6 multicast data traffic from source 5555::14 for group ff55::5514 and deny all other traffic, enter the syntax shown in the following configuration example.

```
device(config)# ipv6 access-list ex2
device(config-ipv6-access-list ex2)# permit ipv6 host 5555::14 host ff55::5514
device(config-ipv6-access-list ex2)# deny  ipv6 any any
```

ACL to Deny IPv6 Multicast Traffic

To deny IPv6 multicast data traffic for group ff55::55 and permit all other traffic, enter the syntax shown in the following configuration example.

```
device(config)# ipv6 access-list ex1
device(config-ipv6-access-list ex1)# deny ipv6 any host ff55::55
device(config-ipv6-access-list ex1)# permit ipv6 any any
```

COMMSCOPE®
RUCKUS®

© 2022 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com