Inspur

CN12900 Series

INOS-CN Multicast Routing Configuration Guide

Inspur-Cisco Networking Technology Co.,Ltd. provides customers with comprehensive technical support and services. For any assistance, please contact our local office or company headquarters.
Website: http://www.inspur.com/
Technical Support Tel: 400-691-1766
Technical Support Email:icnt_service@inspur.com
Technical Document Support Email: icnt_service@inspur.com
Address: 1036 Langchao Road, Lixia District, Jinan City, Shandong Province
Postal code: 250101

Notice

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied

Preface

Objectives

This guide describes main functions of the CN12900 Series. To have a quick grasp of the CN12900 Series, please read this manual carefully.

Versions

The following table lists the product versions related to this document.

Product name	Version
CN12900 Series	

Conventions

Symbol conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ Warning	Indicates a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
⚠ Caution	Indicates a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
✎ Note	Provides additional information to emphasize or supplement important points of the main text.
🔍 Tip	Indicates a tip that may help you solve a problem or save time.

General conventions

Convention	Description
Boldface	Names of files, directories, folders, and users are in **boldface**. For example, log in as user **root**.
Italic	Book titles are in *italics*.
`Lucida Console`	Terminal display is in `Lucida Console`.

Command conventions

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	The parameter before the & sign can be repeated 1 to n times.

GUI conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, windows, and dialog titles are in **boldface**. For example, click **OK**.
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose **File** > **Create** > **Folder**.

Keyboard operation

Format	Description
Key	Press the key. For example, press **Enter** and press **Tab**.

Format	Description
Key 1+Key 2	Press the keys concurrently. For example, pressing **Ctrl+C** means the two keys should be pressed concurrently.
Key 1, Key 2	Press the keys in turn. For example, pressing **Alt**, **A** means the two keys should be pressed in turn.

Mouse operation

Action	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

Change history

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Issue 01 (2020-02-24)

Initial commercial release

Contents

Table

Figurel

CHAPTER 1 Overview

This chapter describes the multicast features of Inspur INOS-CN.

·About Multicast

·Licensing Requirements for Multicast

·Guidelines and Limitations for Multicast

·High-Availability Requirements for Multicast

·Virtual Device Contexts

·Technical Assistance

1.1 About Multicast

IP multicast is a method of forwarding the same set of IP packets to a number of hosts within a network. You can use multicast in IPv4 networks to provide efficient delivery of data to multiple destinations.

Multicast involves both a method of delivery and discovery of senders and receivers of multicast data, which is transmitted on IP multicast addresses called groups. A multicast address that includes a group and source IP address is often referred to as a channel. The Internet Assigned Number Authority (IANA) has assigned 224.0.0.0 through 239.255.255.255 as IPv4 multicast addresses.

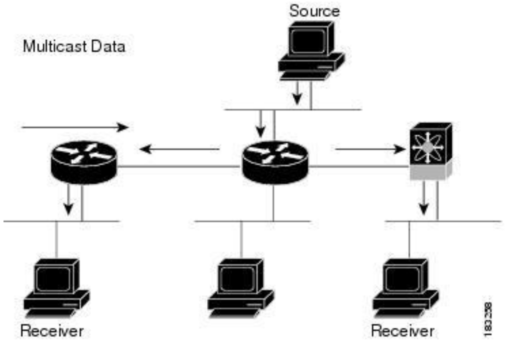
Note

For a complete list of RFCs related to multicast, see Appendix A, IETF RFCs for IP Multicast.

The routers in the network listen for receivers to advertise their interest in receiving multicast data from selected groups. The routers then replicate and forward the data from sources to the interested receivers. Multicast data for a group is transmitted only to those LAN segments with receivers that requested it.

This figure shows one source transmitting multicast data that is delivered to two receivers. In the figure, because the center host is on a LAN segment where no receiver requested multicast data, no data is delivered to that receiver.

Figurel 1 Multicast Traffic from One Source to Two Receivers



1.2Multicast Distribution Trees

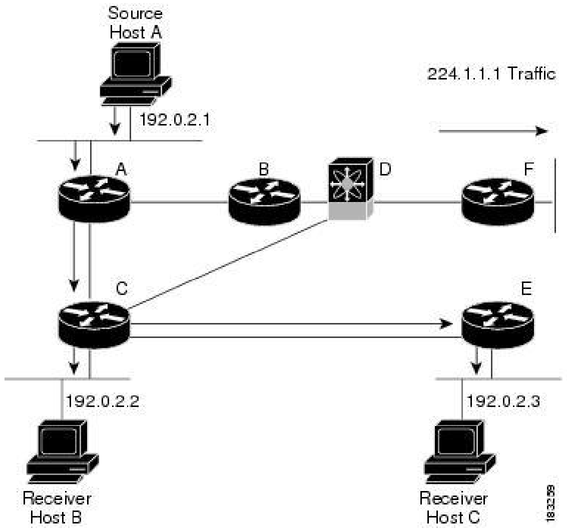
A multicast distribution tree represents the path that multicast data takes between the routers that connect sources and receivers. The multicast software builds different types of trees to support different multicast methods.

1.2.1Source Trees

A source tree represents the shortest path that the multicast traffic takes through the network from the sources that transmit to a particular multicast group to receivers that requested traffic from that same group. Because of the shortest path characteristic of a source tree, this tree is often referred to as a shortest path tree (SPT).

This figure shows a source tree for group 224.1.1.1 that begins at host A and connects to hosts B and C.

Figurel 2 Source Tree

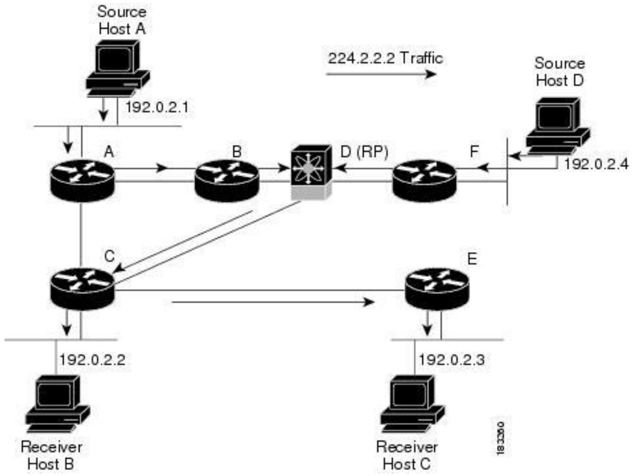


The notation (S, G) represents the multicast traffic from source S on group G. The SPT in this figure is written (192.0.2.1, 224.1.1.1). Multiple sources can be transmitting on the same group.

1.2.2 Shared Trees

A shared tree represents the shared distribution path that the multicast traffic takes through the network from a shared root or rendezvous point (RP) to each receiver. (The RP creates an SPT to each source.) A shared tree is also called an RP tree (RPT). This figure shows a shared tree for group 224.1.1.1 with the RP at router D. Source hosts A and D send their data to router D, the RP, which then forwards the traffic to receiver hosts B and C.

Figurel 3 Shared Tree

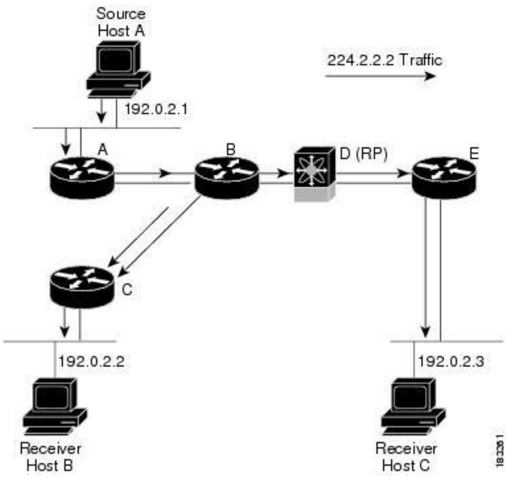


The notation (*, G) represents the multicast traffic from any source on group G. The shared tree in this figure is written (*, 224.2.2.2).

1.2.3 Bidirectional Shared Trees

A bidirectional shared tree represents the shared distribution path that the multicast traffic takes through the network from a shared root, or rendezvous point (RP), to each receiver. Multicast data is forwarded to receivers encountered on the way to the RP. The advantage of the bidirectional shared tree is shown in the figure below. Multicast traffic flows directly from host A to host B through routers B and C. In a shared tree, the data from source host A is first sent to the RP (router D) and then forwarded to router B for delivery to host B.

Figurel 4 Bidirectional Shared Tree



The notation (*, G) represents the multicast traffic from any source on group G. The bidirectional tree in the figure is written as (*, 224.2.2.2).

1.3 Multicast Forwarding

Because multicast traffic is destined for an arbitrary group of hosts, the router uses reverse path forwarding (RPF) to route data to active receivers for the group. When receivers join a group, a path is formed toward the source (SSM mode) or the RP (ASM or Bidir mode). The path from a source to a receiver flows in the reverse direction from the path that was created when the receiver joined the group.

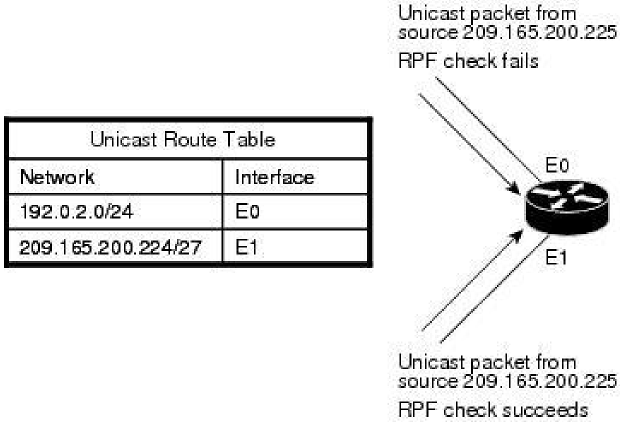
For each incoming multicast packet, the router performs an RPF check. If the packet arrives on the interface leading to the source, the packet is forwarded out each interface in the outgoing interface (OIF) list for the group. Otherwise, the router drops the packet.

Note

In Bidir mode, if a packet arrives on a non-RPF interface and the interface was elected as the designated forwarder (DF), then the packet is also forwarded in the upstream direction toward the RP.

This figure shows an example of RPF checks on packets coming in from different interfaces. The packet that arrives on E0 fails the RPF check because the unicast route table lists the source of the network on interface E1. The packet that arrives on E1 passes the RPF check because the unicast route table lists the source of that network on interface E1.

Figurel 5 RPF Check Example


Unicast Route Table

Network	Interface
192.0.2.0/24	E0
209.165.200.224/27	E1

1.4 Inspur INOS-CN PIM

Inspur INOS-CN supports multicasting with Protocol Independent Multicast (PIM) sparse mode. PIM is IP routing protocol independent and can leverage whichever unicast routing protocols are used to populate the unicast routing table. In PIM sparse mode, multicast traffic is sent only to locations of the network that specifically request it. PIM dense mode is not supported by Inspur INOS-CN.

Note

In this publication, the term "PIM" is used for PIM sparse mode version 2.

To access multicast commands, you must enable the PIM feature. Multicast is enabled only after you enable PIM on an interface of each router in a domain. You can configure PIM for an IPv4 network. By default, IGMP is running on the system.

PIM, which is used between multicast-capable routers, advertises group membership across a routing domain by constructing multicast distribution trees. PIM builds shared distribution trees, on which packets from multiple sources are forwarded, as well as source distribution trees, on which packets from a single source are forwarded.

The distribution trees change automatically to reflect the topology changes due to link or router failures. PIM dynamically tracks both multicast-capable sources and receivers, although the source state is not created in Bidir mode.

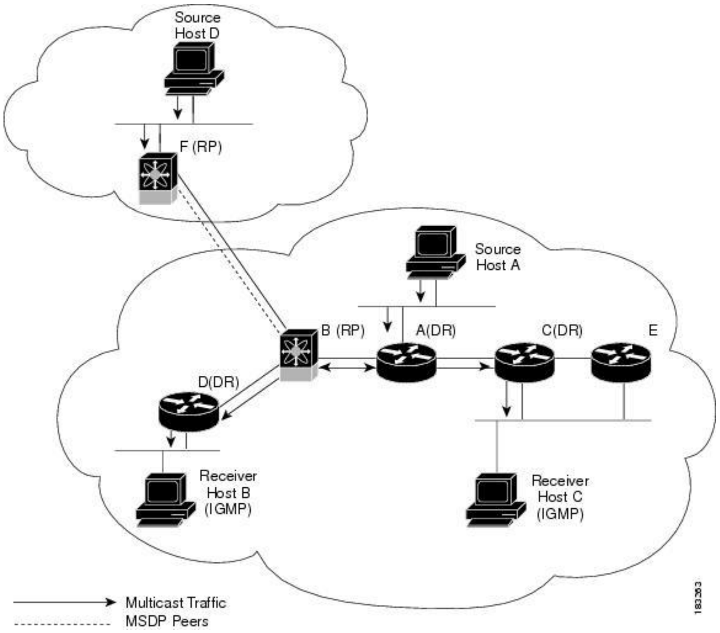
The router uses the unicast routing table and RPF routes for multicast to create multicast routing information. In Bidir mode, additional multicast routing information is created.

Note

In this publication, "PIM for IPv4" refers to the Inspur INOS-CN implementation of PIM sparse mode.

This figure shows two PIM domains in an IPv4 network.

FigureI 6 PIM Domains in an IPv4 Network



• The lines with arrows show the path of the multicast data through the network. The multicast data originates from the sources at hosts A and D.

• The dashed line connects routers B and F, which are Multicast Source Discovery Protocol (MSDP) peers. MSDP supports the discovery of multicast sources in other PIM domains.

- Hosts B and C receive multicast data by using Internet Group Management Protocol (IGMP) to advertise requests to join a multicast group.
- Routers A, C, and D are designated routers (DRs). When more than one router is connected to a LAN segment, such as C and E, the PIM software chooses one router to be the DR so that only one router is responsible for putting multicast data on the segment.

Router B is the rendezvous point (RP) for one PIM domain, and router F is the RP for the other PIM domain. The RP provides a common point for connecting sources and receivers within a PIM domain.

PIM supports these multicast modes for connecting sources and receivers:

- Any source multicast (ASM)
- Source-Specific Multicast (SSM)
- Bidirectional shared trees (Bidir)

Inspur INOS-CN supports a combination of these modes for different ranges of multicast groups. You can also define RPF routes for multicast.

1.4.1 ASM

Any Source Multicast (ASM) is a PIM tree building mode that uses shared trees to discover new sources and receivers as well as source trees to form shortest paths from receivers to sources. The shared tree uses a network node as the root, called the rendezvous point (RP). The source tree is rooted at first-hop routers, directly attached to each source that is an active sender. The ASM mode requires an RP for a group range. An RP can be configured statically or learned dynamically by the Auto-RP or BSR group-to-RP discovery protocols. If an RP is learned and is not known to be a Bidir-RP, the group operates in ASM mode.

The ASM mode is the default mode when you configure RPs.

1.4.2 SSM

Source-Specific Multicast (SSM) is a PIM mode that builds a source tree that originates at the designated router on the LAN segment that receives a request to join a multicast source. Source trees are built by sending PIM join messages in the direction of the source. The SSM mode does not require any RP configuration.

The SSM mode allows receivers to connect to sources outside the PIM domain.

1.4.3 RPF Routes for Multicast

You can configure static multicast RPF routes to override what the unicast routing table uses. This feature is used when the multicast topology is different than the unicast topology.

1.5 IGMP

By default, the Internet Group Management Protocol (IGMP) for PIM is running on the system.

IGMP is used by hosts that want to receive multicast data to request membership in multicast groups. Once the group membership is established, multicast data for the group is directed to the LAN segment of the requesting host.

You can configure IGMPv2 or IGMPv3 on an interface. You have to configure IGMPv3 with (S, G) to support SSM mode. By default, the software enables IGMPv2.

1.6 IGMP Snooping

IGMP snooping is a feature that limits multicast traffic on VLANs to the subset of ports that have known receivers. By examining (snooping) IGMP membership report messages from interested hosts, multicast traffic is sent only to VLAN ports that interested hosts reside on. By default, IGMP snooping is running on the system.

1.7 Interdomain Multicast

Inspur INOS-CN provides several methods that allow multicast traffic to flow between PIM domains.

1.7.1 SSM

The PIM software uses SSM to construct a shortest path tree from the designated router for the receiver to a known source IP address, which may be in another PIM domain. The ASM and Bidir modes mode cannot access sources from another PIM domain without the use of another protocol.

Once you enable PIM in your networks, you can use SSM to reach any multicast source that has an IP address known to the designated router for the receiver.

1.7.2 MRIB

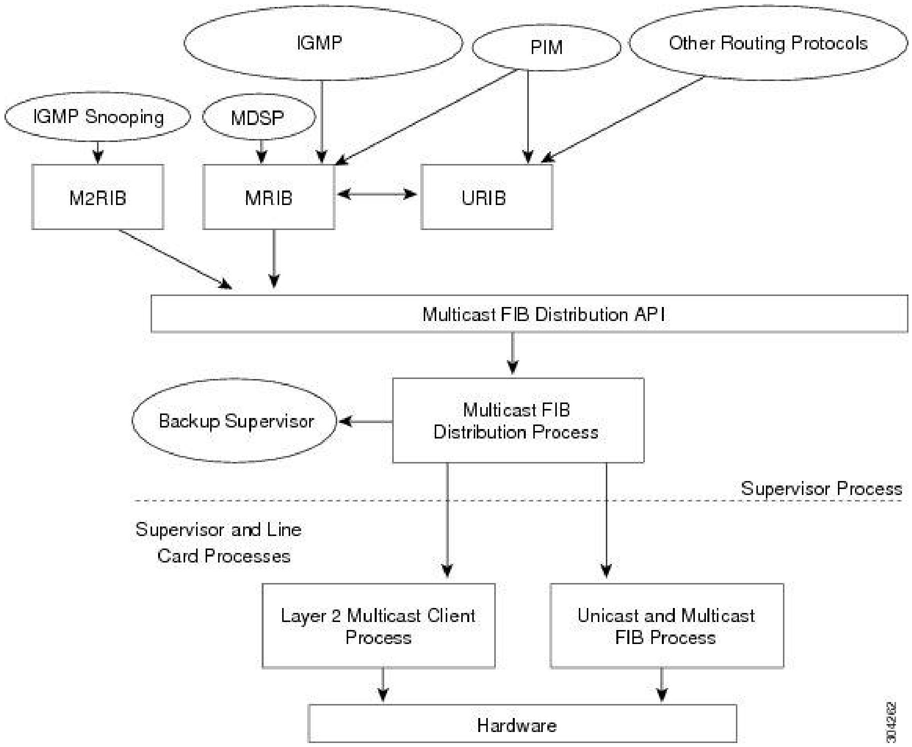
The Inspur INOS-CN IPv4 Multicast Routing Information Base (MRIB) is a repository for route information that is generated by multicast protocols such as PIM and IGMP. The MRIB does not affect the route information itself. The MRIB maintains independent route information for each virtual routing and forwarding (VRF) instance.

The major components of the Inspur INOS-CN multicast software architecture are as follows:

- The Multicast FIB (MFIB) Distribution (MFDM) API defines an interface between the multicast Layer 2 and Layer 3 control plane modules, including the MRIB, and the platform forwarding plane. The control plane modules send the Layer 3 route update using the MFDM API.
- The multicast FIB distribution process distributes the multicast update messages to all the relevant modules and the standby supervisor. It runs only on the supervisor.
- The Layer 2 multicast client process sets up the Layer 2 multicast hardware forwarding path. It runs on both the supervisor and the modules.
- The unicast and multicast FIB process manages the Layer 3 hardware forwarding path. It runs on both the supervisor and the modules.

The following figure shows the Inspur INOS-CN multicast software architecture.

Figurel 7 Inspur INOS-CN Multicast Software Architecture


IGMP
PIM
Other Routing Protocols
IGMP Snooping
MDSP
M2RIB
MRIB
URIB
Multicast FIB Distribution API
Backup Supervisor
Multicast FIB Distribution Process
Supervisor Process
Supervisor and Line Card Processes
Layer 2 Multicast Client Process
Unicast and Multicast FIB Process
Hardware
304262

1.7.3 Virtual Port Channels and Multicast

A virtual port channel (vPC) allows a single device to use a port channel across two upstream switches. When you configure a vPC, the following multicast features might be affected:

- PIM—Inspur INOS-CN software for the Inspur CN12900 Series switches does not support PIM Bidir on a vPC.
- IGMP snooping—You should configure the vPC peers identically.

1.8 Licensing Requirements for Multicast

The multicast features that require a license are as follows:

- PIM

The multicast features that require no license are as follows:

- IGMP
- IGMP snooping

1.9 Guidelines and Limitations for Multicast

- Layer 3 Ethernet port-channel subinterfaces are not supported with multicast routing.
- Layer 2 IPv6 multicast packets will be flooded on the incoming VLAN.
- Traffic storm control is not supported for unknown multicast traffic.

1.10 High-Availability Requirements for Multicast

After a multicast routing protocol is restarted, its state is recovered from the MRIB process. When a supervisor switchover occurs, the MRIB recovers its state from the hardware, and the multicast protocols recover their state from periodic message activity. For more information about high availability, see the *Inspur CN12900 Series INOS-CN High Availability and Redundancy Guide*.

1.11 Virtual Device Contexts

Inspur INOS-CN can segment operating system and hardware resources into virtual device contexts (VDCs) that emulate virtual devices. The Inspur CN12900 Series switches currently do not support multiple VDCs. All switch resources are managed in the default VDC.

CHAPTER 2 Configuring IGMP

This chapter describes how to configure the Internet Group Management Protocol (IGMP) on Inspur INOS-CN devices for IPv4 networks.

- About IGMP
- Licensing Requirements for IGMP
- Prerequisites for IGMP
- Guidelines and Limitations for IGMP
- Default Settings for IGMP
- Configuring IGMP Parameters
- Restarting the IGMP Process
- Verifying the IGMP Configuration
- Configuration Examples for IGMP

2.1 About IGMP

IGMP is an IPv4 protocol that a host uses to request multicast data for a particular group. Using the information obtained through IGMP, the software maintains a list of multicast group or channel memberships on a per-interface basis. The systems that receive these IGMP packets send multicast data that they receive for requested groups or channels out the network segment of the known receivers.

By default, the IGMP process is running. You cannot enable IGMP manually on an interface. IGMP is automatically enabled when you perform one of the following configuration tasks on an interface:

- Enable PIM
- Statically bind a local multicast group
- Enable link-local group reports

2.1.1 IGMP Versions

The device supports IGMPv2 and IGMPv3, and IGMPv1 report reception.

By default, the software enables IGMPv2 when it starts the IGMP process. You can enable IGMPv3 on interfaces where you want its capabilities.

IGMPv3 includes the following key changes from IGMPv2:

- Support for Source-Specific Multicast (SSM), which builds shortest path trees from each receiver to the source, through the following features:
- Host messages that can specify both the group and the source.
- The multicast state that is maintained for groups and sources, not just for groups as in IGMPv2.
- Hosts no longer perform report suppression, which means that hosts always send IGMP membership reports when an IGMP query message is received.

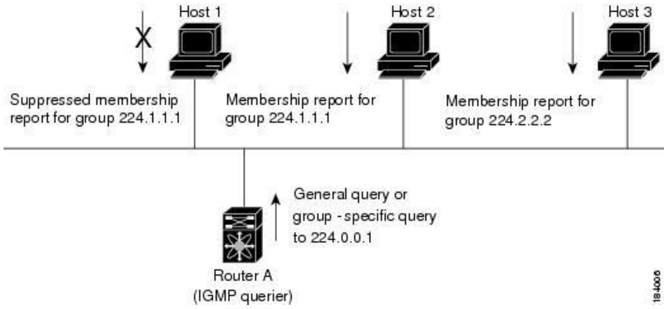
For detailed information about IGMPv2, see RFC 2236.

For detailed information about IGMPv3, see RFC 3376.

2.1.2 IGMP Basics

This figure shows the basic IGMP process of a router that discovers multicast hosts. Hosts 1, 2, and 3 send unsolicited IGMP membership report messages to initiate receiving multicast data for a group or channel.

Figurel 8 IGMPv1 and IGMPv2 Query-Response Process


Host 1
Host 2
Host 3
Suppressed membership report for group 224.1.1.1
Membership report for group 224.1.1.1
Membership report for group 224.2.2.2
General query or group - specific query to 224.0.0.1
Router A (IGMP querier)
184006

In the figure below, router A, which is the IGMP designated querier on the subnet, sends query messages to the all-hosts multicast group at 224.0.0.1 periodically to discover whether any hosts want to receive multicast data. You can configure the group membership timeout value that the router uses to determine that no members of a group or source exist on the subnet.

The software elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes the designated querier. If that router later receives a host query message from a router with a lower IP address, it drops its role as the designated querier and sets its querier timer again.

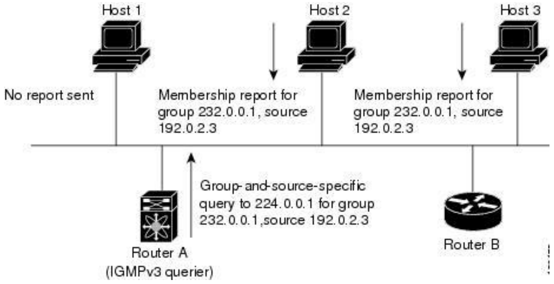
In this figure, host 1's membership report is suppressed, and host 2 sends its membership report for group 224.1.1.1 first. Host 1 receives the report from host 2. Because only one membership report per group needs to be sent to the router, other hosts suppress their reports to reduce network traffic. Each host waits for a random time interval to avoid sending reports at the same time. You can configure the query maximum response time parameter to control the interval in which hosts randomize their responses.

Note

IGMPv1 and IGMPv2 membership report suppression occurs only on hosts that are connected to the same port.

In this figure, router A sends the IGMPv3 group-and-source-specific query to the LAN. Hosts 2 and 3 respond to the query with membership reports that indicate that they want to receive data from the advertised group and source. This IGMPv3 feature supports SSM.

Figurel 9 IGMPv3 Group-and-Source-Specific Query


Host 1
Host 2
Host 3
No report sent
Membership report for group 232.0.0.1, source 192.0.2.3
Membership report for group 232.0.0.1, source 192.0.2.3
Group-and-source-specific query to 224.0.0.1 for group 232.0.0.1,source 192.0.2.3
Router A (IGMPv3 querier)
Router B

Note

IGMPv3 hosts do not perform IGMP membership report suppression.

Messages sent by the designated querier have a time-to-live (TTL) value of 1, which means that the messages are not forwarded by the directly connected routers on the subnet. You can configure the frequency and number of query messages sent specifically for IGMP startup, and you can configure a short query interval at startup so that the group state is established as quickly as possible. Although usually unnecessary, you can tune the query interval used after startup to a value that balances the responsiveness to host group membership messages and the traffic created on the network.

⚠**Caution**

Changing the query interval can severely impact multicast forwarding.

When a multicast host leaves a group, a host that runs IGMPv2 or later sends an IGMP leave message. To check if this host is the last host to leave the group, the software sends an IGMP query message and starts a timer that you can configure called the last member query response interval. If no reports are received before the timer expires, the software removes the group state. The router continues to send multicast traffic for a group until its state is removed.

You can configure a robustness value to compensate for packet loss on a congested network. The robustness value is used by the IGMP software to determine the number of times to send messages.

Link local addresses in the range 224.0.0.0/24 are reserved by the Internet Assigned Numbers Authority (IANA). Network protocols on a local network segment use these addresses; routers do not forward these addresses because they have a TTL of 1. By default, the IGMP process sends membership reports only for nonlink local addresses, but you can configure the software to send reports for link local addresses.

2.2 Licensing Requirements for IGM

Product	License Requirement
Inspur INOS-CN	IGMP requires no license. Any feature not includedin a license package is bundled with the INOS-CN image and is provided at no extra charge to you.

2.3 Prerequisites for IGMP

IGMP has the following prerequisites.

・You are logged onto the device.

・For global configuration commands, you are in the correct virtual routing and forwarding (VRF) mode. The default configuration mode shown in the examples in this chapter applies to the default VRF.

2.4 Guidelines and Limitations for IGMP

IGMP has the following guidelines and limitations: None.

2.5 Default Settings for IGMP

This table lists the default settings for IGMP parameters.

Table 1 Default IGMP Parameters

Parameters	Default
IGMP version	2
Startup query interval	30 seconds
Startup query count	2
Robustness value	2
Querier timeout	255 seconds
Query timeout	255 seconds
Query max response time	10 seconds
Query interval	125 seconds
Last member query response interval	1 second
Last member query count	2
Group membership timeout	260 seconds
Report link local multicast groups	Disabled
Enforce router alert	Disabled
Immediate leave	Disabled

2.6 Configuring IGMP Parameters

You can configure the IGMP global and interface parameters to affect the operation of the IGMP process.

2.6.1 Configuring IGMP Interface Parameters

You can configure the optional IGMP interface parameters described in the table below.

Table 2 IGMP Interface Parameters

Parameter	**Description**
IGMP version	IGMP version that is enabled on the interface. The IGMP version can be 2 or 3. The default is 2.
Static multicast groups	Multicast groups that are statically bound to the interface. You can configure the groups to join the interface with the (*, G) state or specify a source IP to join with the (S, G) state. You can specify a route-map policy name that lists the group prefixes,group ranges, and source prefixes to use with the **match ip multicast** command. **Note** Although you can configure the (S, G)state, the source tree is built only if you enable IGMPv3. You can configure a multicast group on all the multicast-capable routers on the network so that pinging the group causes all the routers to respond.
Static multicast groups on OIF	Multicast groups that are statically bound to the output interface. You can configure the groups to join the output interface with the (*, G) state or specify a source IP to join with the (S, G) state. You can specify a route-map policy name that lists the group prefixes, group ranges, and source prefixes to use with the **match ip multicast** command. **Note** Although you can configure the (S, G)state, the source tree is built only if you enable IGMPv3.
Startup query interval	Startup query interval. By default, this interval is shorter than the query interval so that the software can establish the group state as quickly as possible. Values range from 1 to 18,000 seconds. The default is 31 seconds.
Startup query count	Number of queries sent at startup that are separated by the startup query interval. Values range from 1 to10. The default is 2.
Robustness value	Robustness variable that you can tune to reflect expected packet loss on a congested network. You can increase the robustness variable to increase the number of times that packets are resent. Values range from 1 to 7. The default is 2.
Querier timeout	Number of seconds that the software waits after the previous querier has stopped querying and before it takes over as the querier. Values range from 1 to65,535 seconds. The default is 255 seconds.
Query max response time	Maximum response time advertised in IGMP queries. You can tune the IGMP messages on the network by setting a larger value so that host responses are spread out over a longer time. This value must be less than the query interval. Values range from 1 to 25 seconds. The default is 10 seconds.
Query interval	Frequency at which the software sends IGMP host query messages. You can tune the number of IGMP messages on the network by setting a larger value so that the software sends IGMP queries less often. Values range from 1 to 18,000 seconds. The default is 125 seconds.
Last member query response interval	Interval in which the software sends a response to an IGMP query after receiving a host leave message from the

	last known active host on the subnet. If no reports are received in the interval, the group state is deleted. You can use this value to tune how quickly the software stops transmitting on the subnet. The software can detect the loss of the last member of a group or source more quickly when the values are smaller. Values range from 1 to 25 seconds. The default is 1 second.
Last member query count	Number of times that the software sends an IGMP query, separated by the last member query response interval, in response to a host leave message from the last known active host on the subnet. Values range from 1 to 5. The default is 2. Setting this value to 1 means that a missed packet in either direction causes the software to remove the multicast state from the queried group or channel. The software may wait until the next query interval before the group is added again.
Group membership timeout	Group membership interval that must pass before the router decides that no members of a group or source exist on the network. Values range from 3 to 65,535seconds. The default is 260 seconds.
Report link local multicast groups	Option that enables sending reports for groups in 224.0.0.0/24. Link local addresses are used only by protocols on the local network. Reports are always sent for nonlink local groups. The default is disabled.
Report policy	Access policy for IGMP reports that is based on a route-map policy.
Access groups	Option that configures a route-map policy to control the multicast groups that hosts on the subnet serviced by an interface can join. **Note** Only the **match ip multicast group** command is supported in this route map policy. The **match ip address** command for matching an ACL is not supported.
Immediate leave	Option that minimizes the leave latency of IGMPv2 group memberships on a given IGMP interface because the device does not send group-specific queries. When immediate leave is enabled, the device removes the group entry from the multicast routing table immediately upon receiving a leave message for the group. The default is disabled.
	Note Use this command only when there is one receiver behind the interface for a given group.

To configure route-map policies, see the *Inspur CN12900 Series INOS-CN Unicast Routing Configuration Guide*.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example**: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**interface interface**	Enters interface configuration mode.

	Example: switch(config)# interface ethernet 2/1 switch(config-if)#		
Step 3	Option	Description	These commands are used to configure the IGMP interface parameters.
	ip igmp version *value* **Example:** switch(config-if)# ip igmp verson 3	Sets the IGMP version to the value specified. Values can be 2 or 3. The default is 2. The **no** form of the command sets the version to 2.	
	ip igmp join-group {group [source *source***] | route-map** *policy-name}* **Example:** switch(config-if)# ip igmp join-group 230.0.0.0	Configures an interface on the device to join the specified group or channel. The device accepts the multicast packets for CPU consumption only. **Caution** The device CPU must be able to handle the traffic generated by using this command. Because of CPU load constraints, using this command, especially in any form of scale, is not recommended. Consider using the **ip igmp static-oif** command instead.	
	ip igmp static-oif {*group* **[source** *source***] | route-map** *policy-name*} **Example:** switch(config-if)# ip igmp static-oif 230.0.0.0	Statically binds a multicast group to the **outgoing** interface, which is handled by the device hardware. If you specify the source address, the (S, G) state is created. If you specify the source address, the (S, G) state is created. You can specify a route-map policy name that lists the group prefixes, group ranges, and source prefixes to use with the **match ip multicast** command. **Note** A source tree is built for the (S, G) state only if you enable IGMPv3.	
	ip igmp startup-query-interval *seconds* **Example:** switch(config-if)# ip igmp startup-query-interval 25	Sets the query interval used when the software starts up. Values can range from 1 to 18,000 seconds. The default is 31 seconds	
	ip igmp startup-query-count *count* **Example:** switch(config-if)# ip igmp startup-query-count 3	Sets the query count used when the software starts up. Values can range from 1 to 10. The default is 2.	
	ip igmp robustness-variable *value* **Example:** switch(config-if)# ip igmp robustness-variable 3	Sets the robustness variable. Values can range from 1 to 7. The default is 2.	
	ip igmp querier-timeout *seconds* **Example**:	Sets the querier timeout that the software uses when deciding to take	

	switch(config-if)# ip igmp querier-timeout 300	over as the querier. Values can range from 1 to 65,535 seconds. The default is 255 seconds.	
	ip igmp query-max-response-time *seconds* **Example:** switch(config-if)# ip igmp query-max-response-time 15	Sets the response time advertised in IGMP queries. Values can range from 1 to 25 seconds. The default is 10 seconds.	
	ip igmp query-interval *interval* **Example:** switch(config-if)# ip igmp query-interval 100	Sets the frequency at which the software sends IGMP host query messages. Values can range from 1 to 18,000 seconds. The default is 125 seconds.	
	ip igmp last-member-query-response-time *seconds* **Example:** switch(config-if)# ip igmp last-member-query-response-time 3	Sets the query interval waited after sending membership reports before the software deletes the group state. Values can range from 1 to 25 seconds. The default is 1 second.	
	ip igmp group-timeout *seconds* **Example:** switch(config-if)# ip igmp group-timeout 300	Sets the number of times that the software sends an IGMP query in response to a host leave message. Values can range from 1 to 5. The default is 2.	
	ip igmp group-timeout *seconds* **Example:** switch(config-if)# ip igmp group-timeout 300	Sets the group membership timeout for IGMPv2. Values can range from 3 to 65,535 seconds. The default is 260 seconds.	
	ip igmp report-link-local-groups **Example:** switch(config-if)# ip igmp report-link-local-groups	Enables sending reports for groups in 224.0.0.0/24. Reports are always sent for nonlink local groups. By default, reports are not sent for link local groups.	
	ip igmp report-policy policy **Example:** switch(config-if)# ip igmp report-policy my_report_policy	Configures an access policy for IGMP reports that is based on a report-policy route-map policy.	
	ip igmp access-group policy **Example:** switch(config-if)# ip igmp access-group my_access_policy	Configures a route-map policy to control the ip igmp access-group policy multicast groups that hosts on the subnet serviced by an interface can join. **Note** Only the match ip multicast group command is supported in this route map policy. The match ip address command for matching an ACL is not supported.	
	ip igmp immediate-leave **Example:** switch(config-if)# ip igmp	Enables the device to remove the group entry from the multicast routing table immediately upon receiving a leave message for the group. Use this	

	immediate-leave	command to minimize the leave latency of IGMPv2 group memberships on a given IGMP interface because the device does not send group-specific queries. The default is disabled. **Note** Use this command only when there is one receiver behind the interface for a given group.	
Step 4	(Optional) **show ip igmp interface [***interface***] [vrf** *vrf-name* **| all] [brief]** **Example:** switch(config)# show ip igmp interface	Displays IGMP information about the interface.	
Step 5	(Optional) **show copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.	

2.6.2 Configuring an IGMP SSM Translation

You can configure an SSM translation to provide SSM support when the router receives IGMPv1 or IGMPv2 membership reports. Only IGMPv3 provides the capability to specify group and source addresses in membership reports. By default, the group prefix range is 232.0.0.0/8.

The IGMP SSM translation feature enables an SSM-based multicast core network to be deployed when the multicast host does not support IGMPv3 or is forced to send group joins instead of (S,G) reports to interoperate with Layer 2 switches. The IGMP SSM translation feature provides the functionality to configure multiple sources for the same SSM group. Protocol Independent Multicast (PIM) must be configured on the device before configuring the SSM translation.

This table lists the example SSM translations.

This tabl shows the resulting MRIB routes that the IGMP process creates when it applies an SSM translation to the IGMP membership report. If more than one translation applies, the router creates the (S, G) state for each translation.

Table 3 Example SSM Translations

Group Prefix	**Source Address**
232.0.0.0/8	10.1.1.1
232.0.0.0/8	10.2.2.2
232.1.0.0/16	10.3.3.3
232.1.1.0/24	10.4.4.4

Table 4 Example Result of Applying SSM Translations

IGMPv2 Membership Report	**Resulting MRIB Route**
232.1.1.1	(10.4.4.4, 232.1.1.1)
232.2.2.2	(10.1.1.1, 232.2.2.2) (10.2.2.2, 232.2.2.2)

PROCEDURE

	Command or Action	**Purpose**
Step 1	**configure terminal**	Enters global configuration mode.

	Example: switch# configure terminal switch(config)#	
Step 2	**ip igmp ssm-translate** *group-prefix source-addr* **Example:** switch(config)# ip igmp ssm-translate 232.0.0.0/8 10.1.1.1	Configures the translation of IGMPv1 or IGMPv2membership reports by the IGMP process to create the (S,G) state as if the router had received an IGMPv3 membership report.
Step 3	(Optional) **show running-configuration igmp** **Example:** switch(config)# show running-configuration igmp	Shows the running-configuration information, including **ssm-translate** command lines.
Step 4	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

2.6.3 Configuring the Enforce Router Alert Option Check

You can configure the enforce router alert option check for IGMPv2 and IGMPv3 packets.

PROCEDURE

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	[**no**] **ip igmp enforce-router-alert** **Example:** switch(config)# ip igmp enforce-router-alert	Enables or disables the enforce router alert option check for IGMPv2 and IGMPv3 packets. By default, the enforce router alert option check is enabled.
Step 3	(Optional) **show running-configuration igmp** **Example:** switch(config)# show running-configuration igmp	Shows the running-configuration information.
Step 4	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

2.7 Restarting the IGMP Process

You can restart the IGMP process and optionally flush all routes.

PROCEDURE

	Command or Action	Purpose
Step 1	**restart igmp** **Example:** switch# restart igmp	Restarts the IGMP process.
Step 2	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 3	**ip igmp flush-routes** **Example:** switch(config)# ip igmp flush-routes	Removes routes when the IGMP process is restarted. By default, routes are not flushed.
Step 4	(Optional) **show running-configuration igmp** **Example:** switch(config)# show running-configuration igmp	Shows the running-configuration information.
Step 5	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

2.8 Verifying the IGMP Configuration

To display the IGMP configuration information, perform one of the following tasks:

Command	Description
show ip igmp interface [*interface*] [**vrf** *vrf-name* | **all**] [**brief**]	Displays IGMP information about all interfaces or a selected interface, the default VRF, a selected VRF, or all VRFs. If IGMP is in vPC mode, use this command to display vPC statistics.
show ip igmp groups [{**source** [*group*]}] | {**group** [*source*]}] [**interface**] [**summary**] [**vrf** *vrf-name* | **all**]	Displays the IGMP attached group membership for a group or interface, the default VRF, a selected VRF, or all VRFs.
show ip igmp route [{**source** [*group*]}] | {**group** [*source*]}] [**interface**] [**summary**] [**vrf** *vrf-name* | **all**]	Displays the IGMP attached group membership for a group or interface, the default VRF, a selected VRF, or all VRFs.
show ip igmp local-groups	Displays the IGMP local group membership.
show running-configuration igmp	Displays the IGMP running-configuration information.
show startup-configuration igmp	Displays the IGMP startup-configuration information.

2.9 Configuration Examples for IGMP

The following example shows how to configure the IGMP parameters:

```
configure terminal
ip igmp ssm-translate 232.0.0.0/8 10.1.1.1 interface ethernet 2/1
ip igmp version 3
ip igmp join-group 230.0.0.0
ip igmp startup-query-interval 25 ip igmp startup-query-count 3
ip igmp robustness-variable 3 ip igmp querier-timeout 300 ip igmp query-timeout 300
ip igmp query-max-response-time 15 ip igmp query-interval 100
ip igmp last-member-query-response-time 3 ip igmp last-member-query-count 3
ip igmp group-timeout 300
ip igmp report-link-local-groups
ip igmp report-policy my_report_policy ip igmp access-group my_access_policy
```

CHAPTER 3 Configuring PIM and PIM6

This chapter describes how to configure the Protocol Independent Multicast (PIM) and PIM6 features on Inspur INOS-CN devices in your IPv4 and IPv6 networks.

•About PIM and PIM6
•Licensing Requirements for PIM and PIM6
•Prerequisites for PIM and PIM6
•Guidelines and Limitations for PIM and PIM6
•Default Settings
•Configuring PIM and PIM6
•Verifying the PIM and PIM6 Configuration
•Displaying Statistics
•Configuration Examples for PIM
•Related Documents
•Standards

3.1 About PIM and PIM6

PIM, which is used between multicast-capable routers, advertises group membership across a routing domain by constructing multicast distribution trees. PIM builds shared distribution trees on which packets from multiple sources are forwarded, as well as source distribution trees on which packets from a single source are forwarded.

Inspur INOS-CN supports PIM sparse mode for IPv4 networks (PIM) and for IPv6 networks (PIM6). In PIM sparse mode, multicast traffic is sent only to locations of the network that specifically request it. You can configure PIM and PIM6 to run simultaneously on a router. You can use PIM and PIM6 global parameters to configure rendezvous points (RPs), message packet filtering, and statistics. You can use PIM and PIM6 interface parameters to enable multicast, identify PIM borders, set the PIM hello message interval, and set the designated router (DR) priority.

Note

Inspur INOS-CN does not support PIM dense mode.

In Inspur INOS-CN, multicast is enabled only after you enable the PIM and PIM6 feature on each router and then enable PIM or PIM6 sparse mode on each interface that you want to participate in multicast.

You can configure PIM for an IPv4 network and PIM6 for an IPv6 network. In an IPv4 network, if you have not already enabled IGMP on the router, PIM enables it automatically. In an IPv6 network, MLD is enabled by default.

You use the PIM and PIM6 global configuration parameters to configure the range of multicast group addresses to be handled by these distribution modes:

・Any Source Multicast (ASM) provides discovery of multicast sources. It builds a shared tree between sources and receivers of a multicast group and supports switching over to a source tree when a new receiver is added to a group. ASM mode requires that you configure an RP.

・Source-Specific Multicast (SSM) builds a source tree originating at the designated router on the LAN segment that receives a request to join a multicast source. SSM mode does not require you to configure RPs. Source discovery must be accomplished through other means.

・Bidirectional shared trees (Bidir) build a shared tree between sources and receivers of a multicast group but do not support switching over to a source tree when a new receiver is added to a group. Bidir mode requires that you configure an RP. Bidir forwarding does not require source discovery because only the shared tree is used.

Note

Inspur CN12900 Series switches do not support PIM6 Bidir.

You can combine these modes to cover different ranges of group addresses.

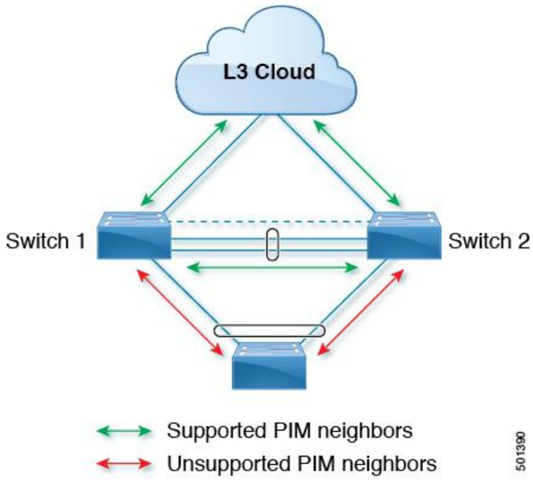
For more information about PIM sparse mode and shared distribution trees used by the ASM and Bidir modes, see RFC 4601.

For more information about PIM SSM mode, see RFC 3569.

For more information about PIM Bidir mode, see draft-ietf-pim-bidir-09.txt.

3.2 PIM SSM with vPC

You can enable PIM SSM on Inspur CN12900 Series switches with an upstream Layer 3 cloud along with the vPC feature. If there are no downstream PIM neighbors, you can form a PIM neighbor relationship between two switches over a vPC VLAN through a vPC peer link.



3.3 Hello Messages

The PIM process begins when the router establishes PIM neighbor adjacencies by sending PIM hello messages to the multicast IPv4 address 224.0.0.13 or IPv6 address FF02::d. Hello messages are sent periodically at the interval of 30 seconds. When all neighbors have replied, the PIM software chooses the router with the highest priority in each LAN segment as the designated router (DR). The DR priority is based on a DR priority value in the PIM hello message. If the DR priority value is not supplied by all routers, or the priorities match, the highest IP address is used to elect the DR.

The hello message also contains a hold-time value, which is typically 3.5 times the hello interval. If this hold time expires without a subsequent hello message from its neighbor, the device detects a PIM failure on that link.

Note

PIM6 does not support MD5 authentication.

For added security, you can configure an MD5 hash value that the PIM software uses to authenticate PIM hello messages with PIM neighbors.

3.4 Join-Prune Messages

When the DR receives an IGMP membership report message from a receiver for a new group or source, the DR creates a tree to connect the receiver to the source by sending a PIM join message out the interface toward the rendezvous point (ASM or Bidir mode) or source (SSM mode). The rendezvous point (RP) is the root of a shared tree, which is used by all sources and hosts in the PIM domain in the ASM or Bidir mode. SSM does not use an RP but builds a shortest path tree (SPT) that is the lowest cost path between the source and the receiver.

When the DR determines that the last host has left a group or source, it sends a PIM prune message to remove the path from the distribution tree.

The routers forward the join or prune action hop by hop up the multicast distribution tree to create (join) or tear down (prune) the path.

Note

In this publication, the terms “PIM join message” and “PIM prune message” are used to simplify the action taken when referring to the PIM join-prune message with only a join or prune action.

Join-prune messages are sent as quickly as possible by the software. You can filter the join-prune messages by defining a routing policy.

3.5 State Refreshes

PIM requires that multicast entries are refreshed within a 3.5-minute timeout interval. The state refresh ensures that traffic is delivered only to active listeners, and it keeps routers from using unnecessary resources.

To maintain the PIM state, the last-hop DR sends join-prune messages once per minute. State creation applies to both (*, G) and (S, G) states as follows:

- (*, G) state creation example—An IGMP (*, G) report triggers the DR to send a (*, G) PIM join message toward the RP.
- (S, G) state creation example—An IGMP (S, G) report triggers the DR to send an (S, G) PIM join message toward the source.

If the state is not refreshed, the PIM software tears down the distribution tree by removing the forwarding paths in the multicast outgoing interface list of the upstream routers.

3.6 Rendezvous Points

A rendezvous point (RP) is a router that you select in a multicast network domain that acts as a shared root for a multicast shared tree. You can configure as many RPs as you like, and you can configure them to cover different group ranges.

3.6.1 Static RP

You can statically configure an RP for a multicast group range. You must configure the address of the RP on every router in the domain.

You can define static RPs for the following reasons:

- To configure routers with the Anycast-RP address
- To manually configure an RP on a device

3.6.2 BSRs

The bootstrap router (BSR) ensures that all routers in the PIM domain have the same RP cache as the BSR. You can configure the BSR to help you select an RP set from BSR candidate RPs. The function of the BSR is to broadcast the RP set to all routers in the domain. You select one or more candidate BSRs to manage the RPs in the domain. Only one candidate BSR is elected as the BSR for the domain.

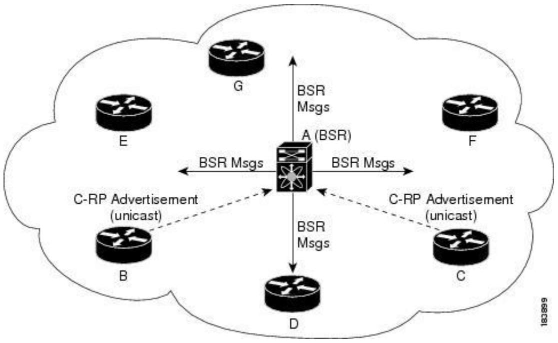
⚠**Caution**

Do not configure both Auto-RP and BSR protocols in the same network.

This figure shows the BSR mechanism. Router A, the software-elected BSR, sends BSR messages out all enabled interfaces (shown by the solid lines in the figure). The messages, which contain the RP set, are flooded hop by hop to all routers in the network. Routers B and C are candidate RPs that send their candidate-RP advertisements directly to the elected BSR (shown by the dashed lines in the figure).

The elected BSR receives candidate-RP messages from all the candidate RPs in the domain. The bootstrap message sent by the BSR includes information about all of the candidate RPs. Each router uses a common algorithm to select the same RP address for a given multicast group.

Figurel 10 BSR Mechanism



In the RP selection process, the RP address with the best priority is determined by the software. If the priorities match for two or more RP addresses, the software might use the RP hash in the selection process. Only one RP address is assigned to a group.

By default, routers are not enabled to listen or forward BSR messages. You must enable the BSR listening and forwarding feature so that the BSR mechanism can dynamically inform all routers in the PIM domain of the RP set assigned to multicast group ranges.

Note

The BSR mechanism is a nonproprietary method of defining RPs that can be used with third-party routers.

Note

BSR is not supported for PIM6.

3.6.3 Auto-RP

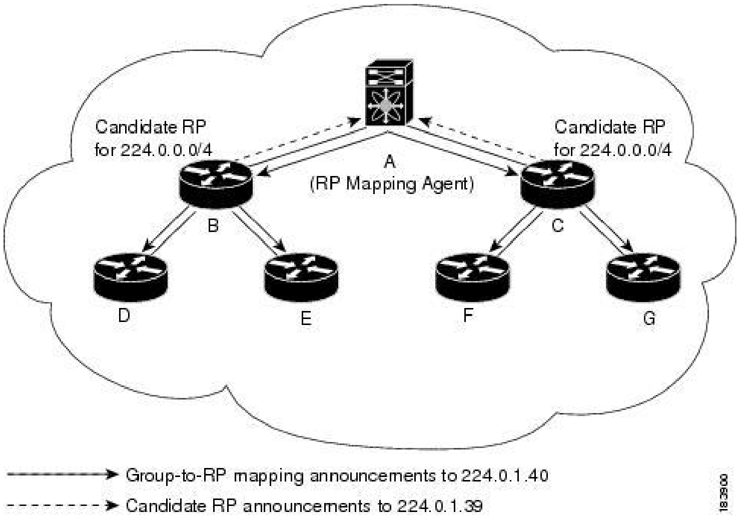
Auto-RP is a Inspur protocol that was introduced prior to the Internet standard bootstrap router mechanism. You configure Auto-RP by selecting candidate mapping agents and RPs. Candidate RPs send their supported group range in RP-Announce messages to the Inspur RP-Announce multicast group 224.0.1.39. An Auto-RP mapping agent listens for RP-Announce messages from candidate RPs and forms a Group-to-RP mapping table. The mapping agent multicasts the Group-to-RP mapping table in RP-Discovery messages to the Inspur RP-Discovery multicast group 224.0.1.40.

⚠ **Caution**

Do not configure both Auto-RP and BSR protocols in the same network.

This figure shows the Auto-RP mechanism. Periodically, the RP mapping agent multicasts the RP information that it receives to the Inspur-RP-Discovery group 224.0.1.40 (shown by the solid lines in the figure).

Figurel 11 Auto-RP Mechanism


Candidate RP
for 224.0.0.0/4
A
(RP Mapping Agent)
Candidate RP
for 224.0.0.0/4
B
C
D
E
F
G
Group-to-RP mapping announcements to 224.0.1.40
Candidate RP announcements to 224.0.1.39
183900

By default, routers are not enabled to listen or forward Auto-RP messages. You must enable the Auto-RP listening and forwarding feature so that the Auto-RP mechanism can dynamically inform routers in the PIM domain of the group-to-RP mapping.

Note

Auto-RP is not supported for PIM6.

3.6.4 Multiple RPs Configured in a PIM Domain

This section describes the election process rules when multiple RPs are configured in a PIM domain.

3.6.5 Anycast-RP

Anycast-RP has two implementations: one uses Multicast Source Discovery Protocol (MSDP) and the other is based on *RFC 4610, Anycast-RP Using Protocol Independent Multicast (PIM)*. This section describes how to configure PIM Anycast-RP.

You can use PIM Anycast-RP to assign a group of routers, called the Anycast-RP set, to a single RP address that is configured on multiple routers. The set of routers that you configure as Anycast-RPs is called the Anycast-RP set. This method is the only RP method that supports more than one RP per multicast group, which allows you to load balance across all RPs in the set. The Anycast RP supports all multicast groups.

PIM register messages are sent to the closest RP, and PIM join-prune messages are sent in the direction of the closest RP as determined by the unicast routing protocols. If one of the RPs goes down, unicast routing ensures these messages will be sent in the direction of the next-closest RP.

You must configure PIM on the loopback interface that is used for the PIM Anycast RP and the PIM Bidir RP.

3.7 PIM Register Messages

PIM register messages are unicast to the RP by designated routers (DRs) that are directly connected to multicast sources. The PIM register message has the following functions:

- To notify the RP that a source is actively sending to a multicast group.
- To deliver multicast packets sent by the source to the RP for delivery down the shared tree.

The DR continues to send PIM register messages to the RP until it receives a Register-Stop message from the RP. The RP sends a Register-Stop message in either of the following cases:

- The RP has no receivers for the multicast group being transmitted.
- The RP has joined the SPT to the source but has not started receiving traffic from the source.

You can use the **ip pim register-source** command to configure the IP source address of register messages when the IP source address of a register message is not a uniquely routed address to which the RP can send packets. This situation might occur if the source address is filtered so that the packets sent to it are not forwarded or if the source address is not unique to the network. In these cases, the replies sent from the RP to the source address will fail to reach the DR, resulting in Protocol Independent Multicast sparse mode (PIM-SM) protocol failures.

The following example shows how to configure the IP source address of the register message to the loopback 3 interface of a DR:

```
ip pim register-source loopback 3
```

Note

In Inspur INOS-CN, PIM register messages are rate limited to avoid overwhelming the RP.

You can filter PIM register messages by defining a routing policy.

3.8 Designated Routers

In PIM ASM and SSM modes, the software chooses a designated router (DR) from the routers on each network segment. The DR is responsible for forwarding multicast data for specified groups and sources on that segment.

The DR for each LAN segment is determined as described in the Hello messages.

In ASM mode, the DR is responsible for unicasting PIM register packets to the RP. When a DR receives an IGMP membership report from a directly connected receiver, the shortest path is formed to the RP, which may or may not go through the DR. The result is a shared tree that connects all sources transmitting on the same multicast group to all receivers of that group.

In SSM mode, the DR triggers (S, G) PIM join or prune messages toward the source. The path from the receiver to the source is determined hop by hop. The source must be known to the receiver or the DR.

3.9 Designated Forwarders

In PIM Bidir mode, the software chooses a designated forwarder (DF) at RP discovery time from the routers on each network segment. The DF is responsible for forwarding multicast data for specified groups on that segment. The DF is elected based on the best metric from the network segment to the RP.

If the router receives a packet on the RPF interface toward the RP, the router forwards the packet out all interfaces in the OIF-list. If a router receives a packet on an interface on which the router is the elected DF for that LAN segment, the packet is forwarded out all interfaces in the OIF-list except the interface that it was received on and also out the RPF interface toward the RP.

Note

Inspur INOS-CN puts the RPF interface into the OIF-list of the MRIB but not in the OIF-list of the MFIB.

3.10 ASM Switchover from Shared Tree to Source Tree

Note

Inspur INOS-CN puts the RPF interface into the OIF-list of the MRIB but not in the OIF-list of the MFIB.

In ASM mode, the DR that is connected to a receiver switches over from the shared tree to the shortest-path tree (SPT) to a source unless you configure the PIM parameter to use shared trees only.

During the switchover, messages on the SPT and shared tree might overlap. These messages are different. The shared tree messages are propagated upstream toward the RP, while SPT messages go toward the source.

For information about SPT switchovers, see the “Last-Hop Switchover to the SPT" section in RFC 4601.

3.11 Administratively Scoped IP Multicast

The administratively scoped IP multicast method allows you to set boundaries on the delivery of multicast data. For more information, see RFC 2365.

You can configure an interface as a PIM boundary so that PIM messages are not sent out on that interface.

You can use the Auto-RP scope parameter to set a time-to-live (TTL) value.

3.12 Multicast Heavy Template

You can enable the multicast heavy template in order to support significantly more multicast routes and to display multicast counters in the output of the **show ip mroute** command.

3.13 Multicast VRF-Lite Route Leaking

Multicast receivers can forward IPv4 traffic across VRFs. In previous releases, multicast traffic can flow only within the same VRF.

With multicast VRF-lite route leaking, Reverse Path Forwarding (RPF) lookup for multicast routes in the receiver VRF can be performed in the source VRF. Therefore, traffic originating from the source VRF can be forwarded to the receiver VRF.

3.14 PIM Graceful Restart

Protocol Independent Multicast (PIM) graceful restart is a multicast high availability (HA) enhancement that improves the convergence of multicast routes (mroutes) after a route processor (RP) switchover. In the event of an RP switchover, the PIM graceful restart feature utilizes the generation ID (GenID) value (defined in RFC 4601) as a mechanism to trigger adjacent PIM neighbors on an interface to send PIM join messages for all (*, G) and (S, G) states that use that interface as a reverse path forwarding (RPF) interface. This mechanism enables PIM neighbors to immediately reestablish those states on the newly active RP.

3.14.1 Generation IDs

A generation ID (GenID) is a randomly generated 32-bit value that is regenerated each time Protocol Independent Multicast (PIM) forwarding is started or restarted on an interface. In order to process the GenID value in PIM hello messages, PIM neighbors must be running Inspur software with an implementation of PIM that is compliant with RFC 4601.

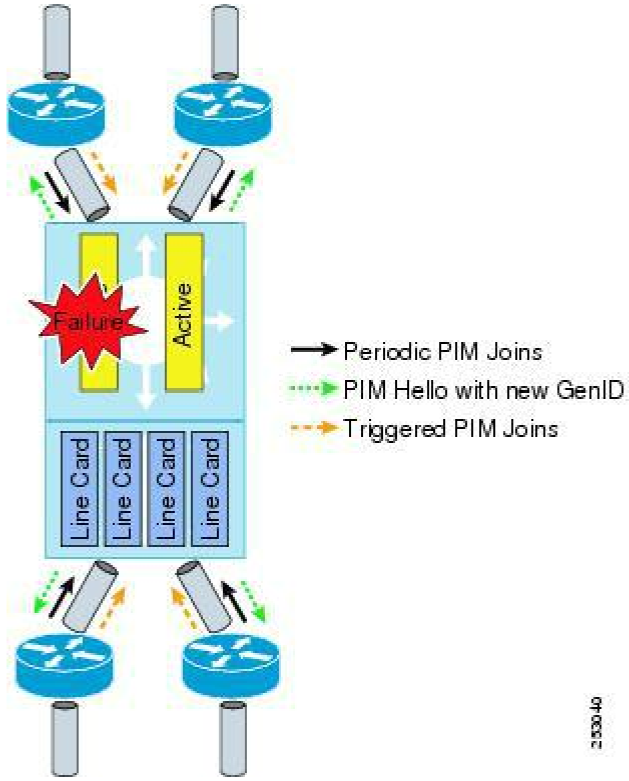
Note

PIM neighbors that are not compliant with RFC 4601 and are unable to process GenID differences in PIM hello messages will ignore the GenIDs.

3.14.2 PIM Graceful Restart Operations

This figure illustrates the operations that occur after a route processor (RP) switchover on devices that support the PIM graceful restart feature.

Figurel 12 PIM Graceful Restart Operations During an RP Switchover



The PIM graceful restart operations are as follows:

- In steady state, PIM neighbors exchange periodic PIM hello messages.
- An active RP receives PIM joins periodically to refresh multicast route (mroute) states.
- When an active RP fails, the standby RP takes over to become the new active RP.
- The new active RP then modifies the generation ID (GenID) value and sends the new GenID in PIM hello messages to adjacent PIM neighbors.
- Adjacent PIM neighbors that receive PIM hello messages on an interface with a new GenID send PIM graceful restart for all (*, G) and (S, G) mroutes that use that interface as an RPF interface.
- Those mroute states are then immediately reestablished on the newly active RP.

3.14.3 PIM Graceful Restart and Multicast Traffic Flow

Multicast traffic flow on PIM neighbors is not affected if the multicast traffic detects support for PIM graceful restart PIM or PIM hello messages from a node with the failing RP within the default PIM hello hold-time interval. Multicast traffic flow on a failing RP is not affected if it is non-stop forwarding (NSF) capable.

⚠**Caution**

The default PIM hello hold-time interval is 3.5 times the PIM hello period. Multicast high availability (HA) operations might not function as per design if you configure the PIM hello interval with a value lower than the default value of 30 seconds.

3.15 High Availability

When a route processor reloads, multicast traffic across VRFs behaves the same as traffic forwarded within the same VRF.

For information about high availability, see the *Inspur CN12900 Series INOS-CN High Availability and Redundancy Guide*.

3.16 Licensing Requirements for PIM and PIM6

Product	License Requirement
Inspur INOS-CN	PIM and PIM6 require an Enterprise Services license.

3.17 Prerequisites for PIM and PIM6

PIM and PIM6 have the following prerequisites:

- You are logged onto the device.
- For global commands, you are in the correct virtual routing and forwarding (VRF) mode. The default configuration mode shown in the examples in this chapter applies to the default VRF.
- For PIM Bidir, you must configure the ACL TCAM region size using the **hardware access-list tcam region mcast-bidir** command. See Configuring ACL TCAM Region Sizes for more information.

Note

By default the mcast-bidir region size is zero. You need to allocate enough entries to this region in order to support PIM Bidir.

3.18 Guidelines and Limitations for PIM and PIM6

PIM and PIM6 have the following guidelines and limitations:

- For most Inspur devices, RPF failure traffic is dropped and sent to the CPU at a very low rate to trigger PIM asserts. For the Inspur CN12900 Series switches, RPF failure traffic is always copied to the CPU in order to learn multicast sources.
- For first-hop source detection in most Inspur devices, traffic coming from the first hop is detected based on the source subnet check, and multicast packets are copied to the CPU only if the source belongs to the local subnet. The Inspur CN12900 Series switches cannot detect the local source, so multicast packets are sent to the supervisor to learn the local multicast source.
- Inspur INOS-CN PIM and PIM6 do not interoperate with any version of PIM dense mode or PIM Sparse Mode version 1.
- Do not configure both Auto-RP and BSR protocols in the same network.
- Configure candidate RP intervals to a minimum of 15 seconds.
- You must configure PIM on the loopback interface that is used for the PIM Anycast RP and the PIM Bidirectional RP.
- The loopback interface that is used to configure RP in multicast must have the **ip**[**v6**] **pim sparse-mode** configuration.
- If a device is configured with a BSR policy that should prevent it from being elected as the BSR, the device ignores the policy. This behavior results in the following undesirable conditions:
- If a device receives a BSM that is permitted by the policy, the device, which incorrectly elected itself as the BSR, drops that BSM so that routers downstream fail to receive it. Downstream devices correctly filter the BSM from the incorrect BSR so that these devices do not receive RP information.
- A BSM received by a BSR from a different device sends a new BSM but ensures that downstream devices do not receive the correct BSM.
- Default values for the PIM hello interval are recommended and should not be modified.
- Inspur CN12900 Series switches support PIM ASM on vPCs.
- Inspur CN12900 Series switches support PIM SSM on vPCs.
- Inspur CN12900 Series switches do not support PIM adjacency with a vPC leg or with a router behind a vPC.
- Inspur CN12900 Series switches support PIM6 ASM and SSM.

Note

Only Inspur 9500 Series switches with CN12904-FM, CN12908-FM, line cards support PIM6 ASM and SSM. Inspur 9500 Series switches with other line cards or fabric modules do not support PIM6.

- PIM6 Bidirectional is not supported.
- PIM6 is not supported on SVIs.

- PIM6 does not support BSRs.
- Inspur CN12900 Series switches do not support PIM Bidir on vPCs or PIM6 ASM, SSM, and Bidirectional on vPCs.
- The following devices support PIM and PIM6 sparse mode on Layer 3 port-channel subinterfaces:
- Inspur 9500 Series switches with CN12904-FM, CN12908-FM, .
- The following guidelines and limitations apply to multicast VRF-lite route leaking:
- Inspur CN12900 Series switches support multicast VRF-lite route leaking.
- PIM Sparse Mode and PIM SSM are supported with multicast VRF-lite route leaking. However, PIM SSM with vPC is not supported with multicast VRF-lite route leaking.
- Only static rendezvous points (RPs) are supported with multicast VRF-lite route leaking.
- The multicast heavy template supports real-time packets and byte statistics but does not support VXLAN and tunnel egress statistics.

3.19 Default Settings

This table lists the default settings for PIM and PIM6 parameters.

Table 5 Default PIM and PIM6 Parameters

Parameters	**Default**
Use shared trees only	Disabled
Flush routes on restart	Disabled
Log neighbor changes	Disabled
Auto-RP message action	Disabled
BSR message action	Disabled
SSM multicast group range or policy	232.0.0.0/8 for IPv4 and FF3x::/96 for IPv6
PIM sparse mode	Disabled
Designated router priority	1
Hello authentication mode	Disabled
Domain border	Disabled
RP address policy	No message filtering
PIM register message policy	No message filtering
BSR candidate RP policy	No message filtering
BSR policy	No message filtering
Auto-RP mapping agent policy	No message filtering
Auto-RP RP candidate policy	No message filtering
Join-prune policy	No message filtering
Neighbor adjacency policy	Become adjacent with all PIM neighbors
BFD	Disabled

3.20 Configuring PIM and PIM6

You can configure both PIM and PIM6 on the same router. You can configure either PIM or PIM6 for each interface, depending on whether that interface is running IPv4 or IPv6.

Note

Inspur INOS-CN supports only PIM sparse mode version 2. In this publication, “PIM” refers to PIM sparse mode version 2.

You can configure separate ranges of addresses in the PIM or PIM6 domain using the multicast distribution modes described in the table below.

Multicast Distribution Mode	**Requires RP Configuration**	**Description**
ASM	Yes	Any source multicast
Bidir	Yes	Bidirectional shared trees
SSM	No	Source-Specific Multicast
RPF routes for multicast	No	RPF routes for multicast

3.21 PIM and PIM6 Configuration Tasks

The following steps configure PIM and PIM6.

1.Select the range of multicast groups that you want to configure in each multicast distribution mode.

2.Enable PIM and PIM6.

3.Follow the configuration steps for the multicast distribution modes that you selected in Step 1.

- For ASM or Bidir mode, see Configuring ASM and Bidir.
- For SSM mode, see Configuring SSM (PIM).
- For RPF routes for multicast, see Configuring RPF Routes for Multicast.

4.Configure message filtering.

Note

The CLI commands used to configure PIM are as follows:

•Configuration commands begin with **ip pim** for PIM and with **ipv6 pim** for PIM6.

•Show commands begin with show **ip pim** for PIM and with show **ipv6 pim** for PIM6.

3.22 Enabling the PIM and PIM6 Feature

Before you can access the PIM or PIM6 commands, you must enable the PIM or PIM6 feature.

Note

You do not need to enable at least one interface with IP PIM sparse mode in order to enable PIM or PIM6.

Before you begin

Ensure that you have installed the Enterprise Services license.

PROCEDURE

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**feature pim** **Example:** switch(config)# feature pim	Enables PIM. By default, PIM is disabled.
Step 3	**feature pim6** **Example:** switch(config)# feature pim6	Enables PIM6. By default, PIM6 is disabled.
Step 4	(Optional) **show running-configuration pim** **Example:** switch(config)# show running-configuration pim	Shows the running-configuration information for PIM.
Step 5	(Optional) **show running-configuration pim6** **Example:** switch(config)# show running-configuration pim6	Shows the running-configuration information for PIM6.
Step 6	**(Optional) copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.23 Configuring PIM or PIM6 Sparse Mode Parameters

You configure PIM or PIM6 sparse mode on every device interface that you want to participate in a sparse mode domain. You can configure the sparse mode parameters described in the table below.

Table 6 PIM and PIM6 Sparse Mode Parameters

Parameter	**Description**
Global to the device	
Auto-RP message action	Enables listening for and forwarding of Auto-RP messages.The default is disabled, which means that the router does not listen for or forward Auto-RP messages unless it is configured as a candidate RP or mapping agent.
	Note PIM6 does not support the Auto-RP method.
BSR message action	Enables listening for and forwarding of BSR messages. The default is disabled, which means that the router does not listen for or forward BSR messages unless it is configured as a candidate RP or BSR candidate.
	Note PIM6 does not support BSR.
Bidir RP limit	Configures the number of Bidir RPs that you can configure for IPv4. The maximum number of Bidir RPs supported per VRF for PIM cannot exceed 8.Values range from 0 to 8. The default is 6.
	Note PIM6 does not support Bidir.
Register rate limit	Configures the IPv4 or IPv6 register rate limit in packets per second. The range is from 1 to 65,535.The default is no limit.
Initial holddown period	Configures the IPv4 or IPv6 initial holddown period in seconds. This holddown period is the time it takes for the MRIB to come up initially. If you want faster convergence, enter a lower value. The range is from90 to 210. Specify 0 to disable the holddown period.The default is 210.
Per device interface	
PIM sparse mode	Enables PIM or PIM6 on an interface.
Designated router priority	Sets the designated router (DR) priority that is advertised in PIM hello messages on this interface.On a multi-access network with multiple PIM-enabled routers, the router with the highest DR priority is elected as the DR router. If the priorities match, the software elects the DR with the highest IP address.The DR originates PIM register messages for the directly connected multicast sources and sends PIM join messages toward the rendezvous point (RP) for directly connected receivers. Values range from 1 to 4294967295. The default is 1.
Designated router delay	Delays participation in the designated router (DR) election by setting the DR priority that is advertised in PIM hello messages to 0 for a specified period.During this delay, no DR changes occur, and the current switch is given time to learn all of the multicast states on that interface. After the delay period expires, the correct DR priority is sent in the hello packets, which retriggers the DR election.Values range from 3 to 0xffff seconds.
Hello authentication mode	Enables an MD5 hash authentication key, or password, in PIM hello messages on the interface so that directly connected neighbors can authenticate each other. The PIM hello messages are IPsec encoded using the Authentication Header (AH) option. You can enter an unencrypted (cleartext) key or one of these values

	followed by a space and the MD5 authentication key: • 0—Specifies an unencrypted (cleartext) key • 3—Specifies a 3-DES encrypted key • 7—Specifies a Inspur Type 7 encrypted key The authentication key can be up to 16 characters. The default is disabled.	
	Note	PIM6 does not support MD5 authentication.
Hello interval	Configures the interval at which hello messages are sent in milliseconds. The range is from 1000 to 18724286. The default is 30000.	
	Note	See the *Inspur CN12900 Series INOS-CN Verified Scalability Guide* for the verified range of this parameter and associated PIM neighbor scale.
Domain border	Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled.	
	Note	PIM6 does not support the Auto-RP method.
Neighbor policy	Configures which PIM neighbors to become adjacent to based on a prefix-list policy.[3] If the policy name does not exist or no prefix lists are configured in a policy, adjacency is established with all neighbors. The default is to become adjacent with all PIM neighbors.	
	Note	We recommend that you should configure this feature only if you are an experienced network administrator.
	Note	The PIM neighbor policy supports only prefix lists. It does not support ACLs used inside a route map.

[3] To configure prefix-list policies, see the *Inspur CN12900 Series INOS-CN Unicast Routing Configuration Guide*.

3.23.1Configuring PIM Sparse Mode Parameters

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	(Optional) **ip pim auto-rp {listen [forward] | forward[listen]}** **Example:** switch(config)# ip pim auto-rp listen	Enables listening for or forwarding of Auto-RP messages. The default is disabled, which means that the software does not listen for or forward Auto-RP messages.
Step 3	(Optional) **ip pim bsr {listen [forward] | forward[listen]}** **Example:** switch(config)# ip pim bsr forward	Enables listening for or forwarding of BSR messages. The default is disabled, which means that the software does not listen for or forward BSR messages.
Step 4	(Optional) **ip pim bidir-rp-limit limit** **Example:** switch(config)# ip pim bidir-rp-limit 4	Specifies the number of Bidir RPs that you can configure for IPv4. The maximum number of Bidir RPs supported per VRF for PIM cannot exceed 8. Values range from 0to 8. The default value is 6.
Step 5	(Optional) **ip pim register-rate-limit rate** **Example:**	Configures the rate limit in packets per second. The rangeis from 1 to 65,535. The default is no limit.

	switch(config)# ip pim register-rate-limit 1000	
Step 6	(Optional) **ip pim spt-threshold infinity group-list route-map-name** **Example:** switch(config)# ip pim spt-threshold infinity group-list my_route-map-name	Creates the IPv4 PIM (*, G) state only, for the group prefixes defined in the specified route map. Inspur INOS-CN Supports up to 1000 route-map entries. This command is not supported for virtual port channels(vPC/vPC+). **Note** The **ip pim use-shared-tree-only group-list** command performs the same function as the **ip pim spt-threshold infinity group-list** command. You can choose to use either command to implement this step.
Step 7	(Optional) **[ip | ipv4] routing multicast holddown**holddown-period **Example:** switch(config)# ip routing multicast holddown 100	Configures the initial holddown period in seconds. The range is from 90 to 210. Specify 0 to disable the holddown period. The default is 210.
Step 8	(Optional) **show running-configuration pim** **Example:** switch(config)# show running-configuration pim	Displays PIM running-configuration information, including the Bidir RP limit and register rate limit.
Step 9	**interface** interface **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode.
Step 10	**ip pim sparse-mode** **Example:** switch(config-if)# ip pim sparse-mode	Enables PIM sparse mode on this interface. The default is disabled.
Step 11	(Optional) **ip pim dr-priority** priority **Example:** switch(config-if)# ip pim dr-priority 192	Sets the designated router (DR) priority that is advertised in PIM hello messages. Values range from 1 to4294967295. The default is 1.
Step 12	(Optional) **ip pim dr-delay** delay **Example:** switch(config-if)# ip pim dr-delay 3	Delays participation in the designated router (DR) election by setting the DR priority that is advertised in PIM hello messages to 0 for a specified period. During this delay, no DR changes occur, and the current switch is given time to learn all of the multicast states on that interface. After the delay period expires, the correct DR priority is sent in the hello packets, which retriggers the DR election.Values range from 3 to 0xffff seconds. **Note** This command delays participation in the DR election only upon bootup or following an IP address or interface state change. It is intended for use with multicast-access non-vPC Layer 3 interfaces only.
Step 13	(Optional) **ip pim hello-authentication ah-md5** auth-key **Example:** switch(config-if)# ip pim hello-authentication ah-md5 my_key	Enables an MD5 hash authentication key in PIM hello messages. You can enter an unencrypted (cleartext) key or one of these values followed by a space and the MD5authentication key: • 0—Specifies an unencrypted (cleartext) key • 3—Specifies a 3-DES encrypted key • 7—Specifies a Inspur Type 7 encrypted key The key can be up to 16 characters. The default is disabled.
Step 14	(Optional) **ip pim hello-interval** interval	Configures the interval at which hello messages are

	Example: switch(config-if)# ip pim hello-interval 25000	sent in milliseconds. The range is from 1000 to 18724286. The default is 30000. **Note** The minimum value is 1 millisecond.
Step 15	(Optional) **ip pim border** **Example:** switch(config-if)# ip pim border	Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled.
Step 16	(Optional) **ip pim neighbor-policy prefix-list** prefix-list **Example:** switch(config-if)# ip pim neighbor-policy prefix-list AllowPrefix	Enables the interface to be on the border of a PIM domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is disabled. Also configures which PIM neighbors to become adjacent to based on a prefix-list policy with the **ip prefix-list** prefix-list command. The prefix list can be up to 63 characters. The default is to become adjacent with all PIM neighbors. **Note** We recommend that you configure this feature only if you are an experienced network administrator.
Step 17	(Optional) **show ip pim interface** [interface | **brief] [vrf**vrf-name | **all]** **Example:** switch(config-if)# show ip pim interface	Displays PIM interface information.
Step 18	(Optional) **copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.23.2Configuring PIM6 Sparse Mode Parameters

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	(Optional) **ipv6 pim register-rate-limit rate** **Example:** switch(config)# ipv6 pim register-rate-limit 1000	Configures the rate limit in packets per second. The range is from 1 to 65,535. The default is no limit.
Step 3	(Optional) **ipv6 routing multicast holddown***holddown-period* **Example:** switch(config)# ipv6 routing multicast holddown 100	Configures the initial holddown period in seconds.The range is from 90 to 210. Specify 0 to disable the holddown period. The default is 210.
Step 4	(Optional) **show running-configuration pim6** **Example:** switch(config)# show running-configuration pim6	Displays PIM6 running-configuration information, including the register rate limit.
Step 5	**interface** *interface* **Example:**	Enters interface configuration mode on the specified interface.

	switch(config)# interface ethernet 2/1 switch(config-if)#	
Step 6	**ipv6 pim sparse-mode** **Example:** switch(config-if)# ipv6 pim sparse-mode	Enables PIM sparse mode on this interface. The default is disabled.
Step 7	(Optional) **ipv6 pim dr-priority priority** **Example:** switch(config-if)# ipv6 pim dr-priority 192	Sets the designated router (DR) priority that is advertised in PIM6 hello messages. Values range from 1 to4294967295. The default is 1.
Step 8	(Optional) **ipv6 pim hello-interval interval** **Example:** switch(config-if)# ipv6 pim hello-interval 25000	Configures the interval at which hello messages are sent in milliseconds. The range is from 1000 to 18724286. The default is 30000.
Step 9	(Optional) **ipv6 pim border** **Example:** switch(config-if)# ipv6 pim border	Enables the interface to be on the border of a PIM6 domain so that no bootstrap, candidate-RP, or Auto-RP messages are sent or received on the interface. The default is
Step 10	(Optional) **ipv6 pim neighbor-policy** *prefix-list prefix-list* **Example:** switch(config-if)# ipv6 pim neighbor-policy prefix-list AllowPrefix	Configures which PIM6 neighbors to become adjacent to based on a prefix-list policy with the **ipv6 prefix-list** prefix-list command. The prefix list can be up to 63 characters. The default is to become adjacent with all PIM6 neighbors. **Note** We recommend that you configure this feature only if you are an experienced network administrator.
Step 11	show **ipv6 pim interfac**e [*interface* | brief] [*vrf vrf-name* | all] **Example:** switch(config-if)# show ipv6 pim interface	Displays PIM6 interface information.
Step 12	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	(Optional) Saves configuration changes.

3.24 Configuring ASM and Bidir

Any Source Multicast (ASM) and bidirectional shared trees (Bidir) are multicast distribution modes that require the use of RPs to act as a shared root between sources and receivers of multicast data.

To configure ASM or Bidir mode, you configure sparse mode and the RP selection method, where you indicate the distribution mode and assign the range of multicast groups.

3.24.1Configuring Static RPs

You can configure an RP statically by configuring the RP address on every router that will participate in the PIM domain.

Note

We recommend that the RP address uses the loopback interface.

You can specify a route-map policy name that lists the group prefixes to use with the **match ip multicast** command or specify a prefix-list method of configuration.

Note

Inspur INOS-CN always uses the longest-match prefix to find the RP, so the behavior is the same irrespective of the position of the group prefix in the route map or in the prefix list.

The following example configuration produces the same output using Inspur INOS-CN (231.1.1.0/24 is always denied irrespective of the sequence number):

```
ip prefix-list
ip prefix-list
ip prefix-list
ip prefix-list
plist seq 10 deny
231.1.1.0/24
plist seq 20 permit
231.1.0.0/16
plist seq 10 permit
231.1.0.0/16
plist seq 20 deny
231.1.1.0/24
```

Configuring Static RPs (PIM)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal	Enters global configuration mode.
Step 2	**ip pim rp-address** *rp-address* [**group-list** *ip-prefix* | **prefix-list** *name* | **route-map** *policy-name*] [**bidir**] **Example:** switch(config)# ip pim rp-address 192.0.2.33group-list 224.0.0.0/9	Configures a PIM static RP address for a multicast group range. You can specify a prefix-list policy name for the static RP address or a route-map policy name that lists the group prefixes to use with the **match ip multicast** command. The mode is ASM unless you specify the **bidir** keyword. The example configures PIM ASM mode for the specified group range.
Step 3	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf***vrf-name*] **Example:** switch(config)# show ip pim group-range	Displays PIM RP information, including BSR listen and forward states.
Step 4	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Configuring Static RPs (PIM6)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM6.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**ipv6 pim rp-address** *rp-address* [**group-list** *ipv6-prefix* |**route-map** *policy-nsmr*] **Example:** switch(config)# ipv6 pim rp-address 2001:0db8:0:abcd::1 group-list ff1e:abcd:def1::0/24	Configures a PIM6 static RP address for a multicast group range. You can specify a route-map policy name that lists the group prefixes to use with the **match ip multicast** command. The mode is ASM. The default group range is ff00::0/8. The example configures PIM6 ASM mode for the specified group range.

Step 3	(Optional) **show ipv6 pim group-range** [*ipv6-prefix* | **vrf***vrf-name*] **Example:** switch(config)# show ipv6 pim group-range	Displays PIM6 modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.24.2 Configuring BSRs

You configure BSRs by selecting candidate BSRs and RPs.

⚠ **Caution**

Do not configure both Auto-RP and BSR protocols in the same network.

You can configure a candidate BSR with the arguments described in the table below.

Note

PIM6 does not support BSRs.

Table 7 Candidate BSR Arguments

Argument	Description
interface	Interface type and number used to derive the BSR source IP address used in bootstrap messages.
hash-length	Number of high order 1s used to form a mask that is ANDed with group address ranges of candidate RPs to form a hash value. The mask determines the number of consecutive addresses to assign across RPs with the same group range. For PIM, this value ranges from 0 to 32 and has a default of 30. For PIM6, this value ranges from 0 to 128 and has a default of 126.
priority	Priority assigned to this BSR. The software elects the BSR with the highest priority, or if the BSR priorities match, the software elects the BSR with the highest IP address. This value ranges from 0, the lowest priority, to 255 and has a default of 64.

Configuring BSRs Candidate RP Arguments and Keywords

You can configure a candidate RP with the arguments and keywords described in this table.

Table 8 BSR Candidate RP Arguments and Keywords

Argument or Keyword	Description
interface	Interface type and number used to derive the BSR source IP address used in bootstrap messages.
group-list *ip-prefix*	Multicast groups handled by this RP specified in a prefix format.
interval	Number of seconds between sending candidate-RP messages. This value ranges from 1 to 65,535 and has a default of 60 seconds. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds.
priority	Priority assigned to this RP. The software elects the RP with the highest priority for a range of groups or,if the priorities match, the highest IP address. (The highest priority is the lowest numerical value.) This value ranges from 0, the highest priority, to 255 and

	Note This priority differs from the BSR BSR-candidate priority, which prefers the highest value between 0 and 255.
bidir	Unless you specify bidir, this RP will be in ASM mode. If you specify bidir, the RP will be in Bidir mode.
route-map *policy-name*	Route-map policy name that defines the group prefixes where this feature is applied.

Tip

You should choose the candidate BSRs and candidate RPs that have good connectivity to all parts of the PIM domain.

You can configure the same router to be both a BSR and a candidate RP. In a domain with many routers, you can select multiple candidate BSRs and RPs to automatically fail over to alternates if a BSR or an RP fails.

To configure candidate BSRs and RPs, follow these steps:

1.Configure whether each router in the PIM domain should listen for and forward BSR messages. A router configured as either a candidate RP or a candidate BSR will automatically listen for and forward all bootstrap router protocol messages, unless an interface is configured with the domain border feature.

2.Select the routers to act as candidate BSRs and RPs.

3.Configure each candidate BSR and candidate RP as described in this section.

4.Configure BSR message filtering.

Configuring BSRs (PIM)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**ip pim bsr {forward [listen] | listen [forward]}** **Example:** switch(config)# ip pim bsr listen forward	Configures listen and forward. Ensure that you have entered this command in each VRF on the remote PE.
Step 3	**ip pim [bsr] bsr-candidate** *interface* [**hash-len***hash-length*] [**priority** *priority*] **Example:** switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 24	Configures a candidate bootstrap router (BSR). The source IP address used in a bootstrap message is the IP address of the interface. The hash length ranges from 0 to 32 and has a default of 30. The priority ranges from 0 to 255 and has a default of 64.
Step 4	(Optional) **ip pim [bsr] rp-candidate** interface **group-list** ip-prefix **route-map** policy-name **priority** priority **interval**interval [**bidir**] **Example:** switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24	Configures a candidate RP for BSR. The priority ranges from 0, the highest priority, to 65,535 and has a default of 192. The interval ranges from 1 to 65,535 seconds and has a default of 60. Use the **bidir** option to create a Bidir candidate RP. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds. The example configures an ASM candidate RP.
Step 5	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf***vrf-name*] **Example:** switch(config)# show ip pim group-range	Displays PIM modes and group ranges.

Step 6	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.24.3 Configuring Auto-RP

You can configure Auto-RP by selecting candidate mapping agents and RPs. You can configure the same router to be both a mapping agent and a candidate RP.

Note

Auto-RP is not supported by PIM6.

Caution

Do not configure both Auto-RP and BSR protocols in the same network.

You can configure an Auto-RP mapping agent with the arguments described in this table.

Table 9 Auto-RP Mapping Agent Arguments

Argument	Description
interface	Interface type and number used to derive the IP address of the Auto-RP mapping agent used in bootstrap messages.
scope *ttl*	Time-to-Live (TTL) value that represents the maximum number of hops that RP-Discovery messages are forwarded. This value can range from1 to 255 and has a default of 32.

If you configure multiple Auto-RP mapping agents, only one is elected as the mapping agent for the domain. The elected mapping agent ensures that all candidate RP messages are sent out. All mapping agents receive the candidate RP messages and advertise the same RP cache in their RP-discovery messages.

You can configure a candidate RP with the arguments and keywords described in this table.

Table 10 Auto-RP Candidate RP Arguments and Keywords

Argument or Keyword	Description
interface	Interface type and number used to derive the IP address of the candidate RP used in bootstrap messages.
group-list *ip-prefix*	Multicast groups handled by this RP. It is specified in a prefix format.
scope *ttl*	Time-to-Live (TTL) value that represents the maximum number of hops that RP-Discovery messages are forwarded. This value can range from 1 to 255 and has a default of 32.
interval	Number of seconds between sending RP-Announce messages. This value can range from 1 to 65,535 and has a default of 60. **Note** We recommend that you configure the candidate RP interval to a minimum of 15
bidir	If not specified, this RP will be in ASM mode. If specified, this RP will be in Bidir mode.
route-map *policy-name*	Route-map policy name that defines the group prefixes where this feature is applied.

Tip

You should choose mapping agents and candidate RPs that have good connectivity to all parts of the PIM domain.

To configure Auto-RP mapping agents and candidate RPs, follow these steps:

1.For each router in the PIM domain, configure whether that router should listen for and forward Auto-RP messages. A router configured as either a candidate RP or an Auto-RP mapping agent will automatically listen for and forward all Auto-RP protocol messages, unless an interface is configured with the domain border feature.

2.Select the routers to act as mapping agents and candidate RPs.

3.Configure each mapping agent and candidate RP as described in this section.

4.Configure Auto-RP message filtering.

Ensure that you have installed the Enterprise Services license and enabled PIM.

Configuring Auto RP (PIM)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**ip pim {send-rp-discovery | auto-rp mapping-agent}** *interface* [**scope** *ttl*] **Example:** switch(config)# ip pim auto-rp mapping-agent ethernet 2/1	Configures an Auto-RP mapping agent. The source IP address used in Auto-RP Discovery messages is the IP address of the interface. The default scope is 32.
Step 3	**ip pim {send-rp-announce | auto-rp rp-candidate}** *interface* {**group-list** *ip-prefix* | **prefix-list** *name* |**route-map** *policy-name*} [**scope** *ttl*] **interval** *interval*][**bidir**] **Example:** switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24	Configures an Auto-RP candidate RP. The default scope is 32. The default interval is 60 seconds. By default, the command creates an ASM candidate RP. Use the bidir option to create a Bidir candidate RP. **Note** We recommend that you configure the candidate RP interval to a minimum of 15 seconds. The example configures an ASM candidate RP.
Step 4	(Optional) **show ip pim group-range** [*ip-prefi*x | **vrf***vrf-name*] **Example:** switch(config)# show ip pim group-range	Displays PIM modes and group ranges.
Step 5	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.24.4 Configuring a PIM Anycast-RP Set

To configure a PIM Anycast-RP set, follow these steps:

1.Select the routers in the PIM Anycast-RP set.

2.Select an IP address for the PIM Anycast-RP set.

3.Configure each peer RP in the PIM Anycast-RP set as described in this section.

Configuring a PIM Anycast RP Set (PIM)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**interface loopback** *number* **Example:** switch(config)# interface loopback 0 switch(config-if)#	Configures an interface loopback. This example configures interface loopback 0.
Step 3	**ip address** *ip-prefix*	Configures an IP address for this interface. It

	Example: switch(config-if)# ip address 192.168.1.1/32	should be a unique IP address that helps to identify this router.
Step 4	**ip pim sparse-mode** **Example:** switch(config-if)# ip pim sparse-mode	Enables PIM sparse mode.
Step 5	**ip router** *routing-protocol-configuration* **Example:** switch(config-if)# ip router ospf 1 area 0.0.0.0	Enables the interface to be reachable by other routers in the Anycast RP set.
Step 6	**exit** **Example:** switch(config-if)# exit switch(config)#	Exits interface configuration mode.
Step 7	**interface loopback** *number* **Example:** switch(config)# interface loopback 1 switch(config-if)#	Configures an interface loopback. This example configures interface loopback 1.
Step 8	**ip address** *ip-prefix* **Example:** switch(config-if)# ip address 10.1.1.1/32	Configures an IP address for this interface. It should be a common IP address that acts as the Anycast RP address.
Step 9	**ip pim sparse-mode** **Example:** switch(config-if)# ip pim sparse-mode	Enables PIM sparse mode.
Step 10	**ip router** *routing-protocol-configuration* **Example:** switch(config-if)# ip router ospf 1 area 0.0.0.0	Enables the interface to be reachable by other routers in the Anycast RP set.
Step 11	**exit** **Example:** switch(config-if)# exit switch(config)#	Exits interface configuration mode.
Step 12	**ip pim rp-address** *anycast-rp-addres*s [**group-list***ip-address*] **Example:** switch(config)# ip pim rp-address 10.1.1.1 group-list 224.0.0.0/4	Configures the PIM Anycast RP address.
Step 13	**ip pim anycast-rp** *anycast-rp-addressanycast-rp-set-router-address* **Example:** switch(config)# ip pim anycast-rp 10.1.1.1 192.168.1.1	Configures a PIM Anycast-RP peer address for the specified Anycast-RP address. Each command with the same Anycast-RP address forms an Anycast-RP set. The IP addresses of RPs are used for communication with RPs in the set.
Step 14	Repeat Step 13 using the same Anycast-RP address for each peer router in the RP set (including the local router).	
Step 15	(Optional) **show ip pim rp** **Example:** switch(config)# show ip pim rp	Displays the PIM RP mapping.
Step 16	(Optional) **show ip mroute** *ip-address* **Example:** switch(config)# show ip mroute 239.1.1.1	Displays the mroute entries.
Step 17	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf***vrf-name*] **Example:** switch(config)# show ip pim group-range	Displays PIM modes and group ranges.
Step 18	(Optional) **copy running-config startup-config**	Copies the running configuration to the startup

	Example: switch(config)# copy running-config startup-config	configuration.

Configuring a PIM Anycast RP Set (PIM6)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM6.

Procedure

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**interface loopback** *number* **Example:** switch(config)# interface loopback 0 switch(config-if)#	Configures an interface loopback. This example configures interface loopback 0.
Step 3	**ipv6 address** *ipv6-prefix* **Example:** switch(config-if)# ipv6 address 2001:0db8:0:abcd::5/32	Configures an IP address for this interface. It should be a unique IP address that helps to identify this router.
Step 4	**ipv6 pim sparse-mode** **Example:** switch(config-if)# ipv6 pim sparse-mode	Enable PIM6 sparse mode.
Step 5	**ipv6 router** *routing-protocol-configuration* **Example:** switch(config-if)# ipv6 router ospfv3 1 area 0.0.0.0	Enables the interface to be reachable by other routers in the Anycast RP set.
Step 6	**exit** **Example:** switch(config-if)# exit switch(config)#	Exits interface configuration mode.
Step 7	**interface loopback** *number* **Example:** switch(config)# interface loopback 1 switch(config-if)#	Configures an interface loopback. This example configures interface loopback 1.
Step 8	**ipv6 address** *ipv6-prefix* **Example:** switch(config-if)# ipv6 address 2001:0db8:0:abcd::1111/32	Configures an IP address for this interface. It should be a common IP address that acts as the Anycast RP address.
Step 9	**ipv6 pim sparse-mode** **Example:** switch(config-if)# ipv6 pim sparse-mode	Enable PIM6 sparse mode.
Step 10	**ipv6 router** *routing-protocol-configuration* **Example:** switch(config-if)# ipv6 router ospfv3 1 area 0.0.0.0	Enables the interface to be reachable by other routers in the Anycast RP set.
Step 11	**exit** **Example:** switch(config-if)# exit switch(config)#	Exits interface configuration mode.
Step 12	**ipv6 pim rp-address** anycast-rp-address [**group-li**st ip-address] **Example:**	Configures the PIM6 Anycast RP address.

	switch(config)# ipv6 pim rp-address2001:0db8:0:abcd::1111 group-listff1e:abcd:def1::0/24	
Step 13	**ipv6 pim anycast-rp** *anycast-rp-addressanycast-rp-set-router-address* **Example:** switch(config)# ipv6 pim anycast-rp 2001:0db8:0:abcd::5 2001:0db8:0:abcd::1111	Configures a PIM6 Anycast-RP peer address for the specified Anycast-RP address. Each command with the same Anycast-RP address forms an Anycast-RP set. The IP addresses of RPs are used for communication with RPs in the set.
Step 14	Repeat Step 13 using the same Anycast-RP address for each peer router in the RP set (including the local router).	
Step 15	(Optional) **show ipv6 pim rp** **Example:** switch(config)# show ipv6 pim rp	Displays the PIM RP mapping.
Step 16	(Optional) **show ipv6 mroute** *ipv6-address* **Example:** switch(config)# show ipv6 mrouteff1e:2222::1:1:1:1	Displays the mroute entries.
Step 17	(Optional) **show ipv6 pim group-range** [*ipv6-prefix*] [**vrf** *vrf-name* | **all**] **Example:** switch(config)# show ipv6 pim group-range	Displays PIM6 modes and group ranges.
Step 18	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.24.5 Configuring Shared Trees Only for ASM

You can configure shared trees only on the last-hop router for Any Source Multicast (ASM) groups, which means that the router never switches over from the shared tree to the SPT when a receiver joins an active group. You can specify a group range where the use of shared trees is to be enforced with the **match ip**[**v6**]**multicast** command. This option does not affect the normal operation of the router when a source tree join-prune message is received.

Note

The Inspur INOS-CN software does not support the shared-tree feature on vPCs. For more information about vPCs, see *Inspur CN12900 Series INOS-CN Interfaces Configuration Guide.*

The default is disabled, which means that the software can switch over to source trees.

Note

In ASM mode, only the last-hop router switches from the shared tree to the SPT.

Configuring Shared Trees Only for ASM (PIM)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**ip pim use-shared-tree-only group-list** *policy-name* **Example:** switch(config)# ip pim use-shared-tree-onlygroup-list	Builds only shared trees, which means that the software never switches over from the shared tree to the SPT. You specify a route-map policy

	my_group_policy	name that lists the groups to use with the **match ip multicast** command. By default, the software triggers a PIM (S, G) join toward the source when it receives multicast packets for a source for which it has the (*, G) state.
Step 3	(Optional) **show ip pim group-range** [*ip-prefix* | **vrf***vrf-name*] **Example:** switch(config)# show ip pim group-range	Displays PIM modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Configuring Shared Trees Only for ASM (PIM6)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM6.

Procedure

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**ipv6 pim use-shared-tree-only group-list** *policy-name* **Example:** switch(config)# ipv6 pim use-shared-tree-only group-list my_group_policy	Builds only shared trees, which means that the software never switches over from the shared tree to the SPT. You specify a route-map policy name that lists the groups to use with the **match ipv6 multica**st command. By default, the software triggers a PIM (S, G) join toward the source when it receives multicast packets for a source for which it has the (*, G) state.
Step 3	(Optional) show ipv6 pim group-range [*ipv6-prefix* | **vrf** *vrf-name*] Example: switch(config)# show ipv6 pim group-range	Displays PIM6 modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.25 Configuring SSM (PIM)

SSM is a multicast distribution mode where the software on the DR connected to a receiver that is requesting data for a multicast source builds a shortest path tree (SPT) to that source.

On an IPv4 network, a host can request multicast data for a specific source only if it is running IGMPv3 and the DR for that host is running IGMPv3. You will usually enable IGMPv3 when you configure an interface for PIM in the SSM mode. For hosts running IGMPv1 or IGMPv2, you can configure group-to-source mapping using SSM translation.

You can configure the group range that is used by SSM.

Note

If you want to use the default SSM group range, you do not need to configure the SSM group range.

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	[no] **ip pim ssm {prefix-list** *name* | **range** {*ip-prefix* | none}| route-map *policy-name*} **Example:** switch(config)# ip pim ssm range 239.128.1.0/24 Example: switch(config)# no ip pim ssm range none	The following options are available: • **prefix-list**—Specifies a prefix-list policy name for the SSM range. • **range**—Configures a group range for SSM. The default range is 232.0.0.0/8. If the keyword **none** is specified, all group ranges are removed. • **route-map**—Specifies a route-map policy name that lists the group prefixes to use with the **match ip multicast** command. The **no** option removes the specified prefix from the SSM range or removes the prefix-list or route-map policy. If the keyword **none** is specified, the **no** command resets the SSM range to the default value of 232.0.0.0/8. **Note** You can configure a maximum of four ranges for SSM multicast, using the **prefix-list, range**,or **route-map** commands.
Step 3	(Optional) **show ip pim group-rang**e [*ip-prefix* | **vrf***vrf-name*] **Example:** switch(config)# show ip pim group-range	Displays PIM modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.26 Configuring SSM (PIM6)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM6.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal	Enters global configuration mode.
Step 2	**[no] ipv6 pim ssm {prefix-list** *name* | **range** {*ivp6-prefix*| none} | route-map *policy-nam*e} **Example:** switch(config)# ipv6 pim ssm range FF30::0/32 **Example:** switch(config)# no ipv6 pim ssm range none	The following options are available: • **prefix-list**—Specifies a prefix-list policy name for the SSM range. • **range**—Configures a group range for SSM. The default range is FF3x/96. If the keyword **none** is specified, all group ranges are removed. • **route-map**—Specifies a route-map policy name that lists the group prefixes to use with the **match ipv6 multicast** command. The **no** option removes the specified prefix from the SSM range or removes the prefix-list or route-map policy. If the keyword **none** is specified, the **no** command resets the SSM range

		to the default value of FF3x/96. **Note** You can configure a maximum of four ranges for SSM multicast, using the **prefix-list**, **range**,or **route-map** commands.
Step 3	(Optional) **show ipv6 pim group-range** [*ipv6-prefix* | **vrf***vrf-name*]	Displays PIM6 modes and group ranges.
Step 4	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.27 Configuring PIM SSM Over a vPC

Configuring PIM SSM over a vPC enables support for IGMPv3 joins and PIM S,G joins over vPC peers in the SSM range. This configuration is supported for orphan sources or receivers in the Layer 2 or Layer 3 domain. When you configure PIM SSM over a vPC, no rendezvous point (RP) configuration is required.

(S,G) entries will have the RPF as the interface toward the source, and no *,G states will be maintained in the MRIB.

Before you begin

Ensure that you have the PIM and vPC features enabled.

Ensure that you have installed the Enterprise Services license and enabled PIM.

PROCEDURE

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**vrf context** *name* **Example:** switch(config)# vrf context Enterprise switch(config-vrf)#	Creates a new VRF and enters VRF configuration mode.The name can be any case-sensitive, alphanumeric string up to 32 characters.
Step 3	(Optional) **[no] ip pim ssm {prefix-list** *name* | **range**{*ip-prefix* | **none}** | **route-map** *policy-name*} **Example:** switch(config-vrf)# ip pim ssm range 234.0.0.0/24	The following options are available: • **prefix-list**—Specifies a prefix-list policy name for the SSM range. • **range**—Configures a group range for SSM. The default range is 232.0.0.0/8. If the keyword **none** is specified, all group ranges are removed. • **route-map**—Specifies a route-map policy name that lists the group prefixes to use with the **match ip multicast** command. By default, the SSM range is 232.0.0.0/8. PIM SSM over vPC works as long as S,G joins are received in this range. If you want to override the default with some other range,you must specify that range using this command. The command in the example overrides the default range to234.0.0.0/24. The **no** option removes the specified prefix from the SSM range or removes the prefix-list or route-map policy. If the keyword **none** is specified, the **no** command resets the SSM range to the default value of 232.0.0.0/8.
Step 4	(Optional) **show ip pim group-range** [*ip-prefix*] [**vrf***vrf-name* | **all]**	Displays PIM modes and group ranges.

	Example: switch(config-vrf)# show ip pim group-range	
Step 5	(Optional) **copy running-config startup-config** **Example:** switch(config-vrf)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.28 Configuring RPF Routes for Multicast

You can define reverse path forwarding (RPF) routes for multicast when you want multicast data to diverge from the unicast traffic path. You can define RPF routes for multicast on border routers to enable RPF to an external network.

Multicast routes are used not to directly forward traffic but to make RPF checks. RPF routes for multicast cannot be redistributed.

Note

IPv6 static multicast routes are not supported.

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

PROCEDURE

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** switch# configure terminal	Enters global configuration mode.
Step 2	**ip mroute** {*ip-addr mask* | *ip-prefix*} {*next-hop* | *nh-prefix*| *interface}* [*route-preference*] [**vrf** vrf-name] **Example:** switch(config)# ip mroute 192.0.2.33/1 224.0.0.0/1	Configures an RPF route for multicast for use in RPF calculations. Route preference values range from 1 to 255. The default preference is 1.
Step 3	(Optional) **show ip static-route [multicast] [vrf** *vrf-name*] **Example:** switch(config)# show ip static-route multicast	Displays configured static routes.
Step 4	(Optional) **copy running-config startup-config**	Copies the running configuration to the startup configuration.

3.28.1Configuring Multicast Multipath

By default, the RPF interface for multicast is chosen automatically when multiple ECMP paths are available.

PROCEDURE

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** switch# configure terminal	Enters global configuration mode.
Step 2	**ip multicast multipath {none | s-g-hash next-hop-based| resilient}** **Example:** switch(config)# ip multicast multipath none	Configures multicast multipath using the following options: • **none**—Disables multicast multipath by suppressing hashing across multiple ECMPs in the URIB RPF lookup. With this option, the highest RPF neighbor (next-hop) address is used for the RPF interface. • **s-g-hash next-hop-based**—Initiates S, G, nexthop hashing (rather than the default of S/RP, G-based hashing) to select the RPF interface.

		• **resilient**—If the ECMP path list changes and the old RPF information is still part of the ECMP, this option uses the old RPF information instead of performing a rehash and potentially changing the RPF information.
		Note For Inspur CN12908 switches with the X9636C-R or X9636Q-R line card or the C9508-FM-R fabric module, if you want to change from the **resilient** option to the **none** option, first enter the **no ip multicast multipath resilient** command and then enter the **ip multicast multipath none** command.
Step 3	**clear ip mroute *** **Example:** switch(config)# clear ip mroute *	Clears multipath routes and activates multicast multipath suppression.

3.29 Configuring Multicast VRF-Lite Route Leaking

You can configure multicast VRF-lite route leaking, which allows IPv4 multicast traffic across VRFs.

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**ip multicast rpf select vrf** *src-vrf-name* **group-list***group-list* **Example:** switch(config)# ip multicast rpf select vrf blue group-list 236.1.0.0/16	Specifies which VRF to use for RPF lookup for a particular multicast group.src-vrf-name is the name of the source VRF. It can be a maximum of 32 alphanumeric characters and is case sensitive.group-list is the group range for the RPF. The format is A.B.C.D/LEN with a maximum length of 32.
Step 3	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.30 Configuring Route Maps to Control RP Information Distribution

You can configure route maps to help protect against some RP configuration errors and malicious attacks.

By configuring route maps, you can control distribution of RP information that is distributed throughout the network. You specify the BSRs or mapping agents to be listened to on each client router and the list of candidate RPs to be advertised (listened to) on each BSR and mapping agent to ensure that what is advertised is what you expect.

Note

Only the match ipv6 multicast command has an effect in the route map.

Ensure that you have installed the Enterprise Services license and enabled PIM or PIM6.

3.30.1 Configuring Route Maps to Control RP Information Distribution (PIM)

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**route-map** *map-name* **[permit | deny**] [*sequence-number*] **Example:** switch(config)# route-map ASM_only permit 10 switch(config-route-map)# **Example:** switch(config)# route-map Bidir_only permit 10 switch(config-route-map)#	Enters route-map configuration mode.
Step 3	**match ip multicast {rp** *ip-address* [**rp-type** *rp-type*]}{**group** *ip-prefix*} {**source** *source-ip-address*} **Example:** switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type ASM **Example:** switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type Bidir	Matches the group, RP, and RP type specified. You can specify the RP type (ASM or Bidir). This configuration method requires the group and RP specified as shown in the example.
Step 4	(Optional) **show route-map** **Example:** switch(config-route-map)# show route-map	Displays configured route maps.
Step 5	(Optional) **copy running-config startup-config** **Example:** switch(config-route-map)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.30.2 Configuring Route Maps to Control RP Information Distribution (PIM6)

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**route-map** m*ap-name* **[permit | deny**] [*sequence-number*] **Example:** switch(config)# route-map ASM_only permit 10 switch(config-route-map)#	Enters route-map configuration mode.
Step 3	**match ipv6 multicast {rp** *ip-address* [**rp-type** *rp-type*]}{**group** *ipv6-prefix*} {**source** *source-ip-address*} **Example:** switch(config-route-map)# match ipv6 multicast group ff1e:abcd:def1::0/24 rp 2001:0db8:0:abcd::1	Matches the group, RP, and RP type specified. You can specify the RP type (ASM). This configuration method requires the group and RP specified as shown in the example.

	rp-type ASM	
Step 4	(Optional) **show route-map** **Example:** switch(config-route-map)# show route-map	Displays configured route maps.
Step 5	(Optional) **copy running-config startup-config** **Example:** switch(config-route-map)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.31 Configuring Message Filtering

Note

Prefix matches in the rp-candidate-policy must be exact relative to what the c-rp is advertising. Subset matches are not possible.

You can configure filtering of the PIM and PIM6 messages described in the table below.

Table 11 PIM and PIM6 Message Filtering

Message Type	**Description**
Global to the Device	
Log Neighbor changes	Enables syslog messages that list the neighbor state changes to be generated. The default is disabled.
PIM register policy	Enables PIM register messages to be filtered based on a route-map policy[4] where you can specify group or group and source addresses with the **match ip**[**v6**] **multicast** command. This policy applies to routers that act as an RP. The default is disabled, which means that the software does not filter PIM register messages.
BSR candidate RP policy	Enables BSR candidate RP messages to be filtered by the router based on a route-map policy where you can specify the RP and group addresses and whether the type is Bidir or ASM with the **match ip multicast** command. This command can be used on routers that are eligible for BSR election. The default is no filtering of BSR messages **Note** PIM6 does not support BSRs.
Auto-RP candidate RP policy	Enables Auto-RP announce messages to be filtered by the Auto-RP mapping agents based on a route-map policy where you can specify the RP and group addresses and whether the type is Bidir or ASM with the **match ip multicast** command. This command can be used on a mapping agent. The default is no filtering of Auto-RP messages. **Note** PIM6 does not support the Auto-RP method.
Auto-RP mapping agent policy	Enables Auto-RP discover messages to be filtered by client routers based on a route-map policy where you can specify mapping agent source addresses with the **match ip multicast** command. This command can be used on client routers that listen to discover messages. The default is no filtering of Auto-RP messages **Note** PIM6 does not support the Auto-RP method
Join-prune policy	Enables join-prune messages to be filtered based on a route-map policy where you can specify group,group and source, or group and RP addresses with the **match ip[v6] multic**ast command. The default is no filtering of join-prune messages.

[4]For information about configuring route-map policies, see the *Inspur CN12900 Series INOS-CN Unicast Routing Configuration Guide*.

Route maps as a filtering policy can be used (either **permit** or **deny** for each statement) for the following commands:

- The **jp-policy** command can use (S,G), (*,G), or (RP,G).
- The **register-policy** command can use (S,G) or (*,G).
- The **igmp report-policy** command can use (*,G) or (S,G).
- The **state-limit reserver-policy** command can use (*,G) or (S,G).
- The **auto-rp rp-candidate-policy** command can use (RP,G).
- The **bsr rp-candidate-policy** command can use (RP,G).
- The **autorp mapping-agent policy** command can use (S).
- The **bsr bsr-policy** command can use (S).

Route maps as containers can be used for the following commands, where the route-map action (**permit** or **deny**) is ignored:

- The **ip pim rp-address route map** command can use only G.
- The **ip pim ssm-range route map** can use only G.
- The **ip igmp static-oif route map** command can use (S,G), (*,G), (S,G-range), (*,G-range).
- The **ip igmp join-group route map** command can use (S,G), (*,G), (S,G-range, (*, G-range).

3.31.1 Configuring Message Filtering (PIM)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	(Optional) **ip pim log-neighbor-changes** **Example:** switch(config)# ip pim log-neighbor-changes	Enables syslog messages that list the neighbor state changes to be generated. The default is disabled.
Step 3	(Optional) **ip pim register-policy** *policy-name* **Example:** switch(config)# ip pim register-policy my_register_policy	Enables PIM register messages to be filtered based on a route-map policy. You can specify group or group and source addresses with the **match ip multicast** command.
Step 4	(Optional) **ip pim bsr rp-candidate-policy** *policy-name* **Example:** switch(config)# ip pim bsr rp-candidate-policy my_bsr_rp_candidate_policy	Enables BSR candidate RP messages to be filtered by the router based on a route-map policy where you can specify the RP and group addresses and whether the type is ASM or Bidir with the **match ip multicast** command. This command can be used on routers that are eligible for BSR election.The default is no filtering of BSR messages.
Step 5	(Optional) **ip pim bsr bsr-policy** *policy-name* **Example:** switch(config)# ip pim bsr bsr-policy my_bsr_policy	Enables BSR messages to be filtered by the BSR client routers based on a route-map policy where you can specify BSR source addresses with the **match ip multicast** command. This command can be used on client routers that listen to BSR messages. The default is no filtering of BSR messages.
Step 6	(Optional) **ip pim auto-rp rp-candidate-policy** *policy-name*	Enables Auto-RP announce messages to be filtered by the Auto-RP mapping agents based

	Example: switch(config)# ip pim auto-rp rp-candidate-policy my_auto_rp_candidate_policy	on a route-map policy where you can specify the RP and group addresses and whether the type is ASM or Bidir with the **match ip multicas**t command. This command can be used on a mapping agent. The default is no filtering of Auto-RP messages.
Step 7	(Optional) **ip pim auto-rp mapping-agent-polic**y *policy-name* **Example:** switch(config)# ip pim auto-rp mapping-agent-policy my_auto_rp_mapping_policy	Enables Auto-RP discover messages to be filtered by client routers based on a route-map policy where you can specify mapping agent source addresses with the **match ip multicast** command. This command can be used on client routers that listen to discover messages. The default is no filtering of Auto-RP messages.
Step 8	**interface interface** **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface mode on the specified interface.
Step 9	(Optional) **ip pim jp-policy** *policy-name* [**in** | **out**] **Example:** switch(config-if)# ip pim jp-policy my_jp_policy	Enables join-prune messages to be filtered based on a route-map policy where you can specify group, group and source, or group and RP addresses with the **match ip multicast** command. The default is no filtering of join-prune messages.
Step 10	(Optional) **show run pim** **Example:** switch(config-if)# show run pim	Displays PIM configuration commands.
Step 11	(Optional) **copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.31.2 Configuring Message Filtering (PIM6)

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM6.

PROCEDURE

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	(Optional) **ipv6 pim log-neighbor-changes** **Example:** switch(config)# ipv6 pim log-neighbor-changes	Enables syslog messages that list the neighbor state changes to be generated. The default is disabled.
Step 3	(Optional) **ipv6 pim register-policy** *policy-name* **Example:** switch(config)# ipv6 pim register-policy my_register_policy	Enables PIM register messages to be filtered based on a route-map policy. You can specify group or group and source addresses with the **match ipv6 multicast** command. The default is disabled.
Step 4	**interface interface** **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface mode on the specified interface.

Step 5	(Optional) **ipv6 pim jp-policy** *policy-name* [**in** | **out**] **Example:** switch(config-if)# ipv6 pim jp-policy my_jp_policy	Enables join-prune messages to be filtered based on a route-map policy where you can specify group, group and source, or group and RP addresses with the **match ipv6 multicast** command. The default is no filtering of join-prune messages. This command filters messages in both incoming and outgoing directions.
Step 6	(Optional) **show run pim6** **Example:** switch(config-if)# show run pim6	Displays PIM6 configuration commands.
Step 7	(Optional) **copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.32 Restarting the PIM and PIM6 Processes

When routes are flushed, they are removed from the Multicast Routing Information Base (MRIB and M6RIB) and the Multicast Forwarding Information Base (MFIB and M6FIB).

When you restart PIM or PIM6, the following tasks are performed:

- The PIM database is deleted.
- The MRIB and MFIB are unaffected and forwarding of traffic continues.
- The multicast route ownership is verified through the MRIB.
- Periodic PIM join and prune messages from neighbors are used to repopulate the database.

3.32.1 Restarting the PIM Process

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

PROCEDURE

	Command or Action	Purpose
Step 1	restart pim **Example:** switch# restart pim	Restarts the PIM process. **Note** Traffic loss might occur during the restartprocess.
Step 2	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 3	**ip pim flush-routes** **Example:** switch(config)# ip pim flush-routes	Removes routes when the PIM process is restarted. By default, routes are not flushed.
Step 4	(Optional) **show running-configuration pim** **Example:** switch(config)# show running-configuration pim	Displays the PIM running-configuration information,including the **flush-routes** command.
Step 5	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.32.2 Restarting the PIM6 Process

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM6.

PROCEDURE

	Command or Action	Purpose
Step 1	**restart pim6** **Example:** switch# restart pim6	Restarts the PIM6 process.
Step 2	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 3	**ipv6 pim flush-routes** **Example:** switch(config)# ipv6 pim flush-routes	Removes routes when the PIM6 process is restarted. By default, routes are not flushed.
Step 4	(Optional) **show running-configuration pim6** **Example:** switch(config)# show running-configuration pim6	Displays the PIM6 running-configuration information, including the **flush-routes** command.
Step 5	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.33 Configuring BFD for PIM in VRF Mode

Note

You can configure Bidirectional Forwarding Detection (BFD) for PIM by either VRF or interface.

Note

BFD is not supported for PIM6.

Before you begin

Ensure that you have installed the Enterprise Services license, enabled PIM, and enabled BFD.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**vrf context** *vrf-name* **Example:** switch# vrf context test switch(config-vrf)#	Enters VRF configuration mode.
Step 3	**ip pim bfd** **Example:** switch(config-vrf)# ip pim bfd	Enables BFD on the specified VRF. **Note** You can also enter the **ip pim bfd** command in global configuration mode, which enables BFD on the VRF instance.

3.33.1 Configuring BFD for PIM in Interface Mode

Before you begin

Ensure that you have installed the Enterprise Services license, enabled PIM, and enabled BFD.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	switch# configure terminal switch(config)#	
Step 2	**interface interface-type** **Example:** switch(config)# interface ethernet 7/40 switch(config-if)#	Enters interface configuration mode.
Step 3	**ip pim bfd instance** **Example:** switch(config-if)# ip pim bfd instance	Enables BFD on the specified interfaces. You can enable or disable BFD on PIM interfaces irrespective of whether BFD is enabled on the VRF.
Step 4	(Optional) **show running-configuration pim** **Example:** switch(config-if)# show running-configuration pim	Displays the PIM running-configuration information.
Step 5	(Optional) **copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.34 Enabling the Multicast Heavy Template

You can enable the multicast heavy template in order to support significantly more multicast routes and to display multicast counters in the output of the **show ip mroute** command.

Before you begin

Ensure that you have installed the Enterprise Services license and enabled PIM.

PROCEDURE

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**system routing template-multicast-heavy** **Example:** switch(config)# system routing template-multicast-heavy	Enables the multicast heavy template.
Step 3	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.35 Verifying the PIM and PIM6 Configuration

To display the PIM and PIM6 configuration information, perform one of the following tasks. Use the **show ip** form of the command for PIM and the **show ipv6** form of the command for PIM6.

Command	**Description**
show ip[**v6**] **mroute** [*ip-address*] [**detail** | **summary**]	Displays the IP or IPv6 multicast routing table.The **detail** option displays detailed route attributes.The **summary** option displays route counts and packet rates.
show ip[**v6**] **pim df** [**vrf** *vrf-name* | **all**]	Displays the designated forwarder (DF) information for each RP by interface.
show ip[**v6**] **pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**]	Displays the learned or configured group ranges and modes. For similar information, see the **show ip**[**v6**]**pim rp** command.
show ip[**v6**] **pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**]	Displays information by the interface.
show ip[**v6**] **pim neighbor** [**interface** *interface* |*ip-prefix*] [**vrf** *vrf-name* | **all**]	Displays neighbors by the interface.

show ip[**v6**] **pim oif-list** *group* [*source*] [**vrf** *vrf-name*| **all**]	Displays all the interfaces in the outgoing interface(OIF) list.
show ip[**v6**] **pim route** [*source* | *group* [*source*]] [**vrf** *vrf-name* | **all**]	Displays information for each multicast route, including interfaces on which a PIM join for that (S, G) has been received.
show ip[**v6**] **pim rp** [*ip-prefix*] [**vrf** *vrf-name* | **all**]	Displays rendezvous points (RPs) known to the software, how they were learned, and their group ranges. For similar information, see the **show ip[v6] pim group-rang**e command.
show ip pim rp-hash *group* [**vrf** *vrf-name* | **all**]	Displays the bootstrap router (BSR) RP hash information.
show ip[**v6**] **pim config-sanity**	Displays the following messages if any PIM configuration errors are detected: For Static RPs: • interface_name should be PIM enabled • interface_name should be UP For Anycast RPs: • Anycast-RP rp_address should be configured on local interface • For Anycast-RP rp_address, interface_name should be PIM enabled • Anycast-RP rp_address is not configured as RP for any group-range • interface_name should be PIM enabled • interface_name should be UP • None of the members in Anycast-RP set for rp_address is local For BSR RPs: • BSR RP Candidate interface interface_name is not PIM/IP enabled • BSR RP Candidate interface interface_name is not IP enabled • BSR RP Candidate interface interface_name is not PIM enabled • interface_name should be UP • BSR Candidate interface interface_name is not PIM/IP enabled • BSR Candidate interface interface_name is not IP enabled • BSR Candidate interface interface_name is not PIM enabled • interface_name should be UP For Auto-RPs: • Auto-RP RP Candidate interface interface_name is not PIM/IP enabled • Auto-RP RP Candidate interface interface_name is not IP enabled • Auto-RP RP Candidate interface interface_name is not PIM enabled • interface_name should be UP • Auto-RP Candidate interface interface_name is not PIM/IP enabled • Auto-RP Candidate interface interface_name is not IP enabled • Auto-RP Candidate interface interface_name is not

	PIM enabled • interface_name should be UP
show running-config pim[**6**]	Displays the running-configuration information.
show startup-config pim[**6**]	Displays the startup-configuration information.
show ip[**v6**] **pim vrf** [*vrf-name* | **all**] [**detail**]	Displays per-VRF information.

This example shows sample output, including multicast counters, for the **show ip mroute summary** command:

```
switch# show ip mroute summary
IP Multicast Routing Table for VRF "default"
Route Statistics unavailable - only liveness    detected
Total number of routes: 701
Total number of (*,G) routes: 0
Total number of (S,G) routes: 700
Total number of (*,G-prefix) routes: 1
Group count: 700, rough average sources per group:     1.0
Group: 224.1.24.0/32, Source count: 1                                 oifs
Source    packets bytes  aps     pps    bit-rate
192.205.38.2      3110   158610  51     0       27.200 bps     5
Group: 224.1.24.1/32, Source            count: 1                                     oifs
Source    packets bytes  aps     pps    bit-rate
192.205.38.2      3106   158406  51     0       27.200 bps     5
```

This example shows sample output, including multicast counters, for the **show ip mroute** *ip-address* **summary** command:

```
switch# show ip mroute 224.1.24.1 summary
IP Multicast Routing Table for VRF "default"
Route Statistics unavailable - only liveness detected
Total number of routes: 701
Total number of (*,G) routes: 0
Total number of (S,G) routes: 700
Total number of (*,G-prefix) routes: 1
Group count: 700, rough average sources per group:     1.0
Group: 224.1.24.1/32, Source count: 1                                 oifs
Source    packets bytes  aps     pps    bit-rate
192.205.38.2      3114   158814  51     0       27.200 bps     5
```

This example shows sample output, including multicast counters, for the **show ip mroute detail** command:

```
switch# show ip mroute detai
IP Multicast Routing Table for VRF "default
Total number of routes: 70
Total number of (*,G) routes:
Total number of (S,G) routes: 700
Total number of (*,G-prefix) routes: 1
(192.205.38.2/32, 224.1.24.0/32), uptime: 13:03:24, nbm(5) pim(0) ip(0) Data Created: No
Stats: 3122/159222 [Packets/Bytes], 27.200      bps
Stats: Active Flow
Incoming interface: Ethernet1/51,
uptime: 13:03:24, internal
Outgoing interface list: (count: 5) Ethernet1/39,
uptime: 13:03:24, nbm Ethernet1/40,
uptime: 13:03:24, nbm Ethernet1/38,
uptime: 13:03:24, nbm Ethernet1/37,
uptime: 13:03:24, nbm Ethernet1/36,
uptime: 13:03:24, nbm
```

This example shows sample output, including multicast counters, for the **show ip mroute** *ip-address* **detail** command:

```
switch# show ip mroute 224.1.24.1 detail
IP Multicast Routing Table for VRF "default"
Total number of routes: 701
Total number of (*,G) routes: 0
Total number of (S,G) routes: 700
Total number of (*,G-prefix) routes: 1
(192.205.38.2/32, 224.1.24.1/32), uptime: 13:00:32, nbm(5) ip(0) pim(0) Data Created: No
Stats: 3110/158610 [Packets/Bytes], 27.200      bps
Stats: Active Flow
Incoming interface: Ethernet1/50,
uptime: 12:59:04, internal
Outgoing interface list: (count: 5) Ethernet1/39,
uptime: 12:59:04, nbm Ethernet1/40,
uptime: 12:59:04, nbm Ethernet1/38,
uptime: 12:59:04, nbm Ethernet1/37,
uptime: 12:59:04, nbm Ethernet1/36,
uptime: 13:00:32, nbm
```

3.36 Displaying Statistics

You can display and clear PIM and PIM6 statistics by using the commands in this section.

3.36.1 Displaying PIM and PIM6 Statistics

You can display the PIM and PIM6 statistics and memory usage using these commands.

Note

Use the show ip form of the command for PIM and the show ipv6 form of the command for PIM6.

Command	**Description**
show ip[**v6**] **pim policy statistics**	Displays policy statistics for register, RP, and join-prune message policies.
show ip[**v6**] **pim statistics** [**vrf** *vrf-name*]	Displays global statistics.

3.37 Clearing PIM and PIM6 Statistics

You can clear the PIM and PIM6 statistics using these commands. Use the **show ip** form of the command for PIM and the **show ipv6** form of the command for PIM6.

Command	**Description**
clear ip[**v6**] **pim interface statistics** *interface*	Clears counters for the specified interface.
clear ip[**v6**] **pim policy statistics**	Clears policy counters for register, RP, and join-prune message policies.
clear ip[**v6**] **pim statistics** [**vrf** *vrf-name*]	Clears global counters handled by the PIM process.

3.38 Configuration Examples for PIM

This section describes how to configure PIM using different data distribution modes and RP selection methods.

3.39 SSM Configuration Example

To configure PIM in SSM mode, follow these steps for each router in the PIM domain:

1.Configure PIM sparse mode parameters on the interfaces that you want to participate in the domain. We recommend that you enable PIM on all interfaces.

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim sparse-mode
```

2.Configure the parameters for IGMP that support SSM. Usually, you configure IGMPv3 on PIM interfaces to support SSM.

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip igmp version 3
```

3.Configure the SSM range if you do not want to use the default range.

```
switch# configure terminal
switch(config)# ip pim ssm range 239.128.1.0/24
```

4.Configure message filtering.

```
switch# configure terminal
switch(config)# ip pim log-neighbor-changes
```

The following example shows how to configure PIM SSM mode:

```
configure terminal interface ethernet 2/1
ip pim sparse-mode
ip igmp version 3 exit
ip pim ssm range 239.128.1.0/24
ip pim log-neighbor-changes
```

3.40 PIM SSM Over vPC Configuration Example

This example shows how to override the default SSM range of 232.0.0.0/8 to 225.1.1.0/24. PIM SSM over vPC will work as long as S,G joins are received in this range.

```
switch# configure terminal switch(config)#vrf context Enterprise
switch(config-vrf)# ip pim ssm range 225.1.1.0/24
switch(config-vrf)# show ip pim group-range --> Shows the configured SSM group range.
PIM Group-Range Configuration for VRF "Enterprise"
Group-range       Mode    RP-address     Shared-tree-only range
225.1.1.0/24      SSM     -              -
switch1# show vpc (primary vPC) --> Shows vPC-related information.
Legend:(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                                :10
Peer status                                  :peer adjacency formed ok
vPC keep-alive status                        :peer is alive
Configuration consistency status             :success
Per-vlan consistency status                  :success
Type-2 consistency status                    :success
vPC role                                     : primary
Number of vPCs                               : 2
configured Peer Gateway                      : Disabled
Dual-active excluded VLANs                   : -
Graceful Consistency Check                   : Enabled
Auto-recovery status                         : Disabled
Delay-restore status                         : Timer is off.(timeout = 30s)
Delay-restore SVI status                     :Timer is off.(timeout = 10s)
vPC Peer-link status
---------------------------------------------------------------------
id Port    Status Active vlans
------   ------ --------------------------------------------------
1  Po1000 up      101-102
vPC status
----------------------------------------------------------------------
id Port    Status  Consistency    Reason  Active vlans
-- ----    ------  -----------    ------  ------------
1  Po1     up      success success 102
2  Po2     up      success success 101
switch2# show vpc (secondary vPC) Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                                :10
Peer status                                  :peer adjacency formed ok
vPC keep-alive status                        :peer is alive
Configuration consistency status             :success
Per-vlan consistency status                  :success
Type-2 consistency status                    :success
vPC role                                     : primary
Number of vPCs                               : 2
configured Peer Gateway                      : Disabled
Dual-active excluded VLANs                   : -
Graceful Consistency Check                   : Enabled
Auto-recovery status                         : Disabled
Delay-restore status                         : Timer is off.(timeout = 30s)
Delay-restore SVI status                     :Timer is off.(timeout = 10s)
vPC Peer-link status
---------------------------------------------------------------------
id Port    Status Active vlans
------   ------ --------------------------------------------------
1  Po1000 up      101-102
vPC status
----------------------------------------------------------------------
id Port    Status  Consistency Reason     Active vlans
-- ----    ------  ----------- ------     ------------
1  Po1     up      success success 102
2  Po2     up      success success 101
switch1# show ip igmp snooping group vlan 101 (primary vPC IGMP snooping states) --> Shows
if S,G v3 joins are received     and on which VLAN. The same VLAN should be OIF in the MRIBoutput.
Type: S    - Static, D - Dynamic, R - Router port, F - Fabricpath core port
Vlan       Group Address  Ver     Type    Port list
101        */*     -      R       Po1000 Vlan101
```

```
101       225.1.1.1      v3      D       Po2
          100.6.160.20
switch2# show ip igmp snooping group vlan 101 (secondary vPC IGMP snooping states)
Type: S - Static, D - Dynamic, R - Router port, F - Fabricpath core port
Vlan      Group Address  Ver     Type    Port list
101       */*    -       R       Po1000 Vlan101
101       225.1.1.1      v3
         100.6.160.20    D       Po2
switch1# show ip pim route (primary vPC  PIM route) --> Shows the route information in the entries
PIM       protocol.
PIM       Routing Table for VRF "default" - 3
(10.6.159.20/32, 225.1.1.1/32), expires 00:02:37 Incoming
interface: Ethernet1/19, RPF nbr 10.6.159.20
Oif-list:  (1) 00000000, timeout-list: (0) 00000000
Immediate-list: (1) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 2, JP-holdtime round-up: 3

(100.6.160.20/32, 225.1.1.1/32), expires 00:01:19 Incoming
interface: Vlan102, RPF nbr 100.6.160.20
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 2, JP-holdtime round-up: 3

(*, 232.0.0.0/8), expires 00:01:19
Incoming interface:      Null0, RPF nbr 0.0.0.0 00000000
Oif-list:                   (0)00000000, timeout-list: (0)
Immediate-list:              (0)00000000, timeout-list: (0)    00000000
Sgr-prune-list:             (0)00000000
Timeout-interval: 2, JP-holdtime round-up: 3

switch2# show ip pim route (secondary vPC PIM route)
PIM Routing Table for VRF "default" - 3 entries
(10.6.159.20/32, 225.1.1.1/32), expires 00:02:51
Incoming interface: Vlan102, RPF nbr 100.6.160.100
Oif-list:  (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holdtime round-up: 3

(100.6.160.20/32, 225.1.1.1/32), expires 00:02:51
Incoming interface: Vlan102, RPF nbr 100.6.160.20
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holdtime round-up: 3

(*, 232.0.0.0/8), expires 00:02:51

Incoming interface:      Null0, RPF nbr 0.0.0.0 00000000
Oif-list:  (0)    00000000, timeout-list: (0)
Immediate-list: (0)      00000000, timeout-list: (0)   00000000
Sgr-prune-list: (0)      00000000
Timeout-interval: 3, JP-holdtime round-up: 3

switch2# show ip pim route (secondary vPC PIM route)
PIM Routing Table for VRF "default" - 3 entries
(10.6.159.20/32, 225.1.1.1/32), expires 00:02:29
Incoming interface: Vlan102, RPF nbr 100.6.160.100
Oif-list:  (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holdtime round-up: 3

(100.6.160.20/32, 225.1.1.1/32), expires 00:02:29
Incoming interface: Vlan102, RPF nbr 100.6.160.20
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holdtime round-up: 3

(*, 232.0.0.0/8), expires 00:02:29
Incoming interface: Null0, RPF nbr 0.0.0.0
```

```
Oif-list:  (0)     00000000, timeout-list: (0)   00000000
Immediate-list: (0)      00000000, timeout-list: (0)   00000000
Sgr-prune-list: (0)      00000000
Timeout-interval: 3, JP-holdtime round-up: 3

switch1# show ip mroute (primary vPC MRIB route) --> Shows the IP multicast routing table.
IP Multicast Routing Table for VRF "default"
(10.6.159.20/32, 225.1.1.1/32), uptime: 03:16:40, pim ip
Incoming interface: Ethernet1/19, RPF nbr: 10.6.159.20
Outgoing interface list: (count: 1)
Vlan102, uptime: 03:16:40, pim

(100.6.160.20/32, 225.1.1.1/32), uptime: 03:48:57, igmp ip pim
Incoming interface: Vlan102, RPF nbr: 100.6.160.20
Outgoing interface list: (count: 1)
Vlan101, uptime: 03:48:57, igmp

(*, 232.0.0.0/8), uptime: 6d06h, pim ip
Incoming interface: Null, RPF nbr: 0.0.0.0
Outgoing interface list: (count: 0)

switch1# show ip mroute detail (primary vPC MRIB route) --> Shows if the (S,G) entries have the RPF
as the interface toward the source and no *,G states are maintained for the SSM group range in the
MRIB.
IP Multicast Routing Table for VRF "default"
Total number of routes: 3
Total number of (*,G) routes: 0
Total number of (S,G) routes: 2
Total number of (*,G-prefix) routes: 1

(10.6.159.20/32, 225.1.1.1/32), uptime: 03:24:28, pim(1) ip(0)
Data Created: Yes
VPC Flags
RPF-Source Forwarder
Stats: 1/51 [Packets/Bytes], 0.000      bps
Stats: Inactive Flow
Incoming interface: Ethernet1/19, RPF nbr: 10.6.159.20
Outgoing interface list: (count: 1) Vlan102, uptime: 03:24:28, pim

(100.6.160.20/32, 225.1.1.1/32), uptime: 03:56:45, igmp(1) ip(0) pim(0)
Data Created: Yes
VPC Flags
RPF-Source Forwarder
Stats: 1/51 [Packets/Bytes], 0.000      bps
Stats: Inactive Flow
Incoming interface: Vlan102, RPF nbr: 100.6.160.20
Outgoing interface list: (count: 1) Vlan101, uptime: 03:56:45, igmp (vpc-svi)

(*, 232.0.0.0/8), uptime: 6d06h, pim(0) ip(0)
Data Created: No
Stats: 0/0 [Packets/Bytes], 0.000       bps
Stats: Inactive Flow
Incoming interface: Null, RPF nbr: 0.0.0.0
Outgoing interface list: (count: 0)

switch2# show ip mroute detail (secondary vPC MRIB route)
IP Multicast Routing Table for VRF "default"
Configuring PIM and PIM6
BSR Configuration Example
Total number of routes: 3
Total number of (*,G) routes: 0
Total number of (S,G) routes: 2
Total number of (*,G-prefix) routes: 1

(10.6.159.20/32, 225.1.1.1/32), uptime: 03:26:24, igmp(1) pim(0) ip(0)
Data Created: Yes bps
Stats: 1/51 [Packets/Bytes], 0.000
Stats: Inactive Flow
Incoming interface: Vlan102, RPF nbr: 100.6.160.100
Outgoing interface list: (count: 1)
Ethernet1/17, uptime: 03:26:24, igmp

(100.6.160.20/32, 225.1.1.1/32), uptime: 04:06:32, igmp(1) ip(0) pim(0)
Data Created: Yes
```

```
VPC Flags
RPF-Source Forwarder     bps
Stats: 1/51 [Packets/Bytes], 0.000
Stats: Inactive Flow
Incoming interface: Vlan102, RPF nbr: 100.6.160.20
Outgoing interface list: (count: 1)
Vlan101, uptime: 04:03:24, igmp (vpc-svi)

(*, 232.0.0.0/8), uptime: 6d06h, pim(0) ip(0)
Data Created: No
Stats: 0/0 [Packets/Bytes], 0.000       bps
Stats: Inactive Flow
Incoming interface: Null, RPF nbr: 0.0.0.0
Outgoing interface list: (count: 0)
```

3.41 BSR Configuration Example

To configure PIM in ASM mode using the BSR mechanism, follow these steps for each router in the PIM domain:

1.Configure PIM sparse mode parameters on the interfaces that you want to participate in the domain. We recommend that you enable PIM on all interfaces.

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim sparse-mode
```

2.Configure whether that router should listen and forward BSR messages.

```
switch# configure terminal
switch(config)# ip pim bsr forward listen
```

3.Configure the BSR parameters for each router that you want to act as a BSR.

```
switch# configure terminal
switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 30
```

4.Configure the RP parameters for each router that you want to act as a candidate RP.

```
switch# configure terminal
switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24
```

5.Configure message filtering.

```
switch# configure terminal
switch(config)# ip pim log-neighbor-changes
```

The following example shows how to configure PIM ASM mode using the BSR mechanism and how to configure the BSR and RP on the same router:

```
configure terminal interface ethernet 2/1
ip pim sparse-mode exit
ip pim bsr forward listen
ip pim bsr-candidate ethernet 2/1 hash-len 30
ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24
ip pim log-neighbor-changes
Auto-RP Configuration Example
```

To configure PIM in Bidir mode using the Auto-RP mechanism, follow these steps for each router in the PIM domain:

1.Configure PIM sparse mode parameters on the interfaces that you want to participate in the domain. We recommend that you enable PIM on all interfaces.

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim sparse-mode
```

2.Configure whether that router should listen and forward Auto-RP messages.

```
switch# configure terminal
switch(config)# ip pim auto-rp forward listen
```

3.Configure the mapping agent parameters for each router that you want to act as a mapping agent.

```
switch# configure terminal
switch(config)# ip pim auto-rp mapping-agent ethernet 2/1
```

4.Configure the RP parameters for each router that you want to act as a candidate RP.

```
switch# configure terminal
switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24 bidir
```

5.Configure message filtering.

```
switch# configure terminal
switch(config)# ip pim log-neighbor-changes
```

This example shows how to configure PIM Bidir mode using the Auto-RP mechanism and how to configure the mapping agent and RP on the same router:

```
configure terminal interface ethernet 2/1
ip pim sparse-mode exit
ip pim auto-rp listen ip pim auto-rp forward
ip pim auto-rp mapping-agent ethernet 2/1
ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24 bidir
ip pim log-neighbor-changes
```

3.42 PIM Anycast RP Configuration Example

To configure ASM mode using the PIM Anycast-RP method, follow these steps for each router in the PIM domain:

1.Configure PIM sparse mode parameters on the interfaces that you want to participate in the domain. We recommend that you enable PIM on all interfaces.

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim sparse-mode
```

2.Configure the RP address that you configure on all routers in the Anycast-RP set.

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# ip address 192.0.2.3/32
switch(config-if)# ip pim sparse-mode
```

3.Configure a loopback with an address to use in communication between routers in the Anycast-RP set for each router that you want to be in the Anycast-RP set.

```
switch# configure terminal
switch(config)# interface loopback 1
switch(config-if)# ip address 192.0.2.31/32
switch(config-if)# ip pim sparse-mode
```

4.Configure the Anycast-RP parameters and repeat with the IP address of each Anycast-RP for each router that you want to be in the Anycast-RP set. This example shows two Anycast-RPs.

```
switch# configure terminal
switch(config)# ip pim anycast-rp 192.0.2.3 193.0.2.31
switch(config)# ip pim anycast-rp 192.0.2.3 193.0.2.32
```

5.Configure message filtering.

```
switch# configure terminal
switch(config)# ip pim log-neighbor-changes
```

The following example shows how to configure PIM ASM mode using two Anycast-RPs:

```
configure terminal interface ethernet 2/1
ip pim sparse-mode exit
interface loopback 0 ip address 192.0.2.3/32
ip pim sparse-mode exit
interface loopback 1
ip address 192.0.2.31/32
ip pim sparse-mode exit
ip pim anycast-rp 192.0.2.3 192.0.2.31
ip pim anycast-rp 192.0.2.3 192.0.2.32
ip pim log-neighbor-changes
```

3.43 Prefix-Based and Route-Map-Based Configurations

```
ip prefix-list plist11 seq 10 deny 231.129.128.0/17
ip prefix-list plist11 seq 20 deny 231.129.0.0/16
ip prefix-list plist11 seq 30 deny 231.128.0.0/9
ip prefix-list plist11 seq 40 permit 231.0.0.0/8
ip prefix-list plist22 seq 10 deny 231.129.128.0/17
ip prefix-list plist22 seq 20 deny 231.129.0.0/16
ip prefix-list plist22 seq 30 permit 231.128.0.0/9
ip prefix-list plist22 seq 40 deny 231.0.0.0/8
ip prefix-list plist33 seq 10 deny 231.129.128.0/17
ip prefix-list plist33 seq 20 permit 231.129.0.0/16
ip prefix-list plist33 seq 30 deny 231.128.0.0/9
ip prefix-list plist33 seq 40 deny 231.0.0.0/8
ip pim    rp-address 172.21.0.11 prefix-list plist11
ip pim    rp-address 172.21.0.22 prefix-list plist22
ip pim    rp-address 172.21.0.33 prefix-list plist33
route-map  rmap11 deny 10
match     ip      multicast group 231.129.128.0/17
route-map  rmap11 deny 20
match     ip      multicast group 231.129.0.0/16
route-map  rmap11 deny 30
match     ip      multicast group 231.128.0.0/9
route-map  rmap11 permit 40
match     ip      multicast group 231.0.0.0/8
route-map  rmap22 deny 10
match     ip      multicast group 231.129.128.0/17
route-map  rmap22 deny 20
match     ip      multicast group 231.129.0.0/16
route-map  rmap22 permit 30
match     ip      multicast group 231.128.0.0/9
route-map  rmap22 deny 40
match     ip      multicast group 231.0.0.0/8
route-map  rmap33 deny 10
match     ip      multicast group 231.129.128.0/17
route-map  rmap33 permit 20
match     ip      multicast group 231.129.0.0/16
route-map  rmap33 deny 30
match     ip      multicast group 231.128.0.0/9
route-map  rmap33 deny 40
match     ip      multicast group 231.0.0.0/8
ip pim    rp-address 172.21.0.11 route-map rmap11
ip pim    rp-address 172.21.0.22 route-map rmap22
ip pim    rp-address 172.21.0.33 route-map rmap33
```

3.43.1 Output

```
dc3rtg-d2(config-if)# show ip pim rp
PIM RP Status Information for VRF "default" BSR disabled
Auto-RP disabled
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None
RP: 172.21.0.11, (0), uptime: 00:12:36, expires: never,
  priority: 0, RP-source: (local), group-map: rmap11, group ranges:
    231.0.0.0/8 231.128.0.0/9 (deny)
    231.129.0.0/16 (deny) 231.129.128.0/17 (deny)
RP: 172.21.0.22, (0), uptime: 00:12:36, expires: never,
  priority: 0, RP-source: (local), group-map: rmap22, group ranges:
    231.0.0.0/8 (deny) 231.128.0.0/9
    231.129.0.0/16 (deny) 231.129.128.0/17 (deny)
RP: 172.21.0.33, (0), uptime: 00:12:36, expires: never,
  priority: 0, RP-source: (local), group-map: rmap33, group ranges:
    231.0.0.0/8 (deny) 231.128.0.0/9 (deny)
    231.129.0.0/16 231.129.128.0/17 (deny)
dc3rtg-d2(config-if)# show ip mroute
IP Multicast Routing Table for VRF "default"
(*, 231.1.1.1/32), uptime: 00:07:20, igmp pim ip
  Incoming interface: Ethernet2/1, RPF nbr: 10.165.20.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:07:20, igmp
(*, 231.128.1.1/32), uptime: 00:14:27, igmp pim ip
  Incoming interface: Ethernet2/1, RPF nbr: 10.165.20.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:14:27, igmp
(*, 231.129.1.1/32), uptime: 00:14:25, igmp pim ip
```

```
  Incoming interface: Ethernet2/1, RPF nbr: 10.165.20.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:14:25, igmp
(*, 231.129.128.1/32), uptime: 00:14:26, igmp pim ip
  Incoming interface: Null, RPF nbr: 10.0.0.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:14:26, igmp
(*, 232.0.0.0/8), uptime: 1d20h, pim ip
  Incoming interface: Null, RPF nbr: 10.0.0.1
  Outgoing interface list: (count: 0)
dc3rtg-d2(config-if)# show ip pim group-range
PIM Group-Range Configuration for VRF "default"
Group-range       Mode    RP-address     Shared-tree-only range
232.0.0.0/8       ASM     -       -
231.0.0.0/8       ASM     172.21.0.11    -
231.128.0.0/9     ASM     172.21.0.22    -
231.129.0.0/16    ASM     172.21.0.33    -
231.129.128.0/17  Unknown -       -
```

3.44 Related Documents

Related Topic	Document Title
ACL TCAM regions	*Inspur CN12900 Series INOS-CN Security Configuration Guide*
Configuring VRFs	*Inspur CN12900 Series INOS-CN Unicast Routing Configuration Guide*

3.45 Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature	

CHAPTER 4 Configuring IGMP Snooping

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on a Inspur INOS-CN device.

·About IGMP Snooping
·Licensing Requirements for IGMP Snooping
·Prerequisites for IGMP Snooping
·Guidelines and Limitations for IGMP Snooping
·Default Settings
·Configuring IGMP Snooping Parameters
·Verifying the IGMP Snooping Configuration
·Displaying IGMP Snooping Statistics
·Clearing IGMP Snooping Statistics
·Configuration Examples for IGMP Snooping

4.1 About IGMP Snooping

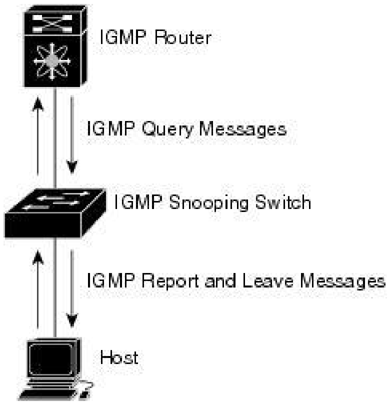
Note

We recommend that you do not disable IGMP snooping on the device. If you disable IGMP snooping, you might see reduced multicast performance because of excessive false flooding within the device.

IGMP snooping software examines Layer 2 IP multicast traffic within a VLAN to discover the ports where interested receivers reside. Using the port information, IGMP snooping can reduce bandwidth consumption in a multi-access LAN environment to avoid flooding the entire VLAN. IGMP snooping tracks which ports are attached to multicast-capable routers to help the routers forward IGMP membership reports. The IGMP snooping software responds to topology change notifications. By default, IGMP snooping is enabled on the device.

This figure shows an IGMP snooping switch that sits between the host and the IGMP router. The IGMP snooping switch snoops the IGMP membership reports and Leave messages and forwards them only when necessary to the connected IGMP routers.

Figurel 13 IGMP Snooping Switch



The IGMP snooping software operates upon IGMPv1, IGMPv2, and IGMPv3 control plane packets where Layer 3 control plane packets are intercepted and influence the Layer 2 forwarding behavior.

The Inspur INOS-CN IGMP snooping software has the following proprietary features:

- Source filtering that allows forwarding of multicast packets based on destination and source IP addresses
- Multicast forwarding based on IP addresses rather than the MAC address
- Multicast forwarding alternately based on the MAC address

4.1.1 IGMPv1 and IGMPv2

Both IGMPv1 and IGMPv2 support membership report suppression, which means that if two hosts on the same subnet want to receive multicast data for the same group, the host that receives a member report from the other host suppresses sending its report. Membership report suppression occurs for hosts that share a port.

If no more than one host is attached to each VLAN switch port, you can configure the fast leave feature in IGMPv2. The fast leave feature does not send last member query messages to hosts. As soon as the software receives an IGMP leave message, the software stops forwarding multicast data to that port.

IGMPv1 does not provide an explicit IGMP leave message, so the software must rely on the membership message timeout to indicate that no hosts remain that want to receive multicast data for a particular group.

Note

The software ignores the configuration of the last member query interval when you enable the fast leave feature because it does not check for remaining hosts.

4.1.2 IGMPv3

The IGMPv3 snooping implementation on Inspur INOS-CN supports full IGMPv3 snooping, which provides constrained flooding based on the (S, G) information in the IGMPv3 reports. This source-based filtering enables the device to constrain multicast traffic to a set of ports based on the source that sends traffic to the multicast group.

By default, the software tracks hosts on each VLAN port. The explicit tracking feature provides a fast leave mechanism. Because every IGMPv3 host sends membership reports, report suppression limits the amount of traffic that the device sends to other multicast-capable routers. When report suppression is enabled, and no IGMPv1 or IGMPv2 hosts requested the same group, the software provides proxy reporting. The proxy feature builds the group state from membership reports from the downstream hosts and generates membership reports in response to queries from upstream queriers.

Even though the IGMPv3 membership reports provide a full accounting of group members on a LAN segment, when the last host leaves, the software sends a membership query. You can configure the parameter last member query interval. If no host responds before the timeout, the software removes the group state.

4.1.3 IGMP Snooping Querier

When PIM is not enabled on an interface because the multicast traffic does not need to be routed, you must configure an IGMP snooping querier to send membership queries. You define the querier in a VLAN that contains multicast sources and receivers but no other active querier.

The querier can be configured to use any IP address in the VLAN.

As a best practice, a unique IP address, one that is not already used by the switch interface or the Hot Standby Router Protocol (HSRP) virtual IP address, should be configured so as to easily reference the querier.

Note

The IP address for the querier should not be a broadcast IP address, multicast IP address, or 0 (0.0.0.0)

When an IGMP snooping querier is enabled, it sends out periodic IGMP queries that trigger IGMP report messages from hosts that want to receive IP multicast traffic. IGMP snooping listens to these IGMP reports to establish appropriate forwarding.

The IGMP snooping querier performs querier election as described in RFC 2236. Querier election occurs in the following configurations:

- When there are multiple switch queriers configured with the same subnet on the same VLAN on different switches.
- When the configured switch querier is in the same subnet as with other Layer 3 SVI queriers.

4.1.4 Virtualization Support

You can define multiple virtual routing and forwarding (VRF) instances for IGMP snooping.

You can use the **show** commands with a VRF argument to provide a context for the information displayed. The default VRF is used if no VRF argument is supplied.

For information about configuring VRFs, see the *Inspur CN12900 Series INOS-CN Unicast Routing Configuration Guide*.

4.2 Licensing Requirements for IGMP Snooping

Product	**License Requirement**
Inspur INOS-CN	IGMP snooping requires no license. Any feature not included in a license package is bundled with the INOS-CN image and is provided at no extra charge to you.

4.3 Prerequisites for IGMP Snooping

IGMP snooping has the following prerequisites:

- You are logged onto the device.
- For global commands, you are in the correct virtual routing and forwarding (VRF) mode. The default configuration mode shown in the examples in this chapter applies to the default VRF.

4.4 Guidelines and Limitations for IGMP Snooping

IGMP snooping has the following guidelines and limitations:

- Inspur CN12900 Series switches support IGMP snooping for IPv4 but do not support MLD snooping for IPv6.
- IGMP snooping is not supported with PVLAN.
- Layer 3 IPv6 multicast routing is not supported.
- Layer 2 IPv6 multicast packets will be flooded on the incoming VLAN.
- Inspur CN12908 and CN12904 platform switches with CN129-X636C-R, CN129-X636Q-R, and CN129-X636C-RX line cards support IGMP snooping with vPCs.
- IGMP snooping configuration must be identical on both vPC peers in a vPC pair. Either enable or disable IGMP snooping on both vPC peers.

Note

Enabling or disabling IGMP snooping on both vPC peers also enables the forwarding of IGMP queries from different MVR source VLANs into the same MVR receiver VLAN. The resulting IGMP queries may send out queries with different versions and query interval..

- You must enable the **ip igmp snooping group-timeout** command when you use the **ip igmp snooping proxy general-queries** command. We recommend that you set it to "never". Otherwise, you might experience multicast packet loss.
- All external multicast router ports (either statically configured or dynamically learned) use the global ltl index. As a result, traffic in VLAN X goes out on the multicast router ports in both VLAN X and VLAN Y, in case both multicast router ports (Layer 2 trunks) carry both VLAN X and VLAN Y.

4.5 Default Settings

Parameters	Default
IGMP snooping	Enabled
Explicit tracking	Enabled
Fast leave	Disabled
Last member query interval	1 second
Snooping querier	Disabled
Report suppression	Enabled
Link-local groups suppression	Enabled
IGMPv3 report suppression for the entire device	Disabled
IGMPv3 report suppression per VLAN	Enabled

4.6 Configuring IGMP Snooping Parameters

Note

You must enable IGMP snooping globally before any other commands take effect.

4.6.1Configuring Global IGMP Snooping Parameters

To affect the operation of the IGMP snooping process globally, you can configure various optional IGMP snooping parameters.

Notes for IGMP Snooping Parameters

- IGMP Snooping Proxy parameter

To decrease the burden placed on the snooping switch during each IGMP general query (GQ) interval, the Inspur INOS-CN software provides a way to decouple the periodic general query behavior of the IGMP snooping switch from the query interval configured on the multicast routers.

You can configure the device to consume IGMP general queries from the multicast router, rather than flooding the general queries to all the switchports. When the device receives a general query, it produces proxy reports for all currently active groups and distributes the proxy reports over the period specified by the MRT that is specified in the router query. At the same time, independent of the periodic general query activity of the multicast router, the device sends an IGMP general query on each port in the VLAN in a round-robin fashion. It cycles through all the interfaces in the VLAN at the rate given by the following formula.

Rate = {number of interfaces in VLAN} * {configured MRT} * {number of VLANs}

When queries are run in this mode, the default MRT value is 5,000 milliseconds (5 seconds). For a device that has 500 switchports in a VLAN, it would take 2,500 seconds (40 minutes) to cycle through all the interfaces in the system. This is also true when the device itself is the querier.

This behavior ensures that only one host responds to a general query at a given time, and it keeps the simultaneous reporting rate below the packet-per-second IGMP capability of the device (approximately 3,000 to 4,000 pps).

Note

When you use this option, you must change the **ip igmp snooping group-timeout** parameter to a high value or to never time out.

The **ip igmp snooping proxy general-queries** [**mrt**] command causes the snooping function to proxy reply to general queries from the multicast router while also sending round-robin general queries on each switchport with the specified MRT value. (The default MRT value is 5 seconds.)

- IGMP Snooping Group-timeout parameter

Configuring the group-timeout parameter disables the behavior of an expiring membership based on three missed general queries. Group membership remains on a given switchport until the device receives an explicit IGMP leave on that port.

The **ip igmp snooping group-timeout** {*timeout* | **never**} command modifies or disables the behavior of an expiring IGMP snooping group membership after three missed general queries.

Step 1 **configure terminal**

Example:

```
switch# configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 Use the following commands to configure global IGMP snooping parameters.

Option	Description
ip igmp snooping switch(config)# ip igmp snooping	Enables IGMP snooping for the device. The default is enabled. **Note** If the global setting is disabled with the no form of this command, IGMP snooping on all VLANs is disabled, whether IGMP snooping is enabled on a VLAN or not. If you disable IGMP snooping, Layer 2 multicast frames flood to all modules.
ip igmp snooping event-history switch(config)# ip igmp snooping event-history	Configures the size of the event history buffer. The default is small.
ip igmp snooping group-timeout {*minutes* | **never**}switch(config)# ip igmp snooping group-timeoutnever	Configures the group membership timeout value for all VLANson the device.
ip igmp snooping	Configures link-local groups suppression for the entire device.
link-local-groups-suppression switch(config)# ip igmp snooping link-local-groups-suppression	The default is enabled.
ip igmp snooping proxy general-inquiries [**mrt** *seconds*]switch(config)# ip igmp	Configures the IGMP snooping proxy for the device. The default is 5 seconds.

snooping proxy general-inquiries	
ip igmp snooping **v3-report-suppression** switch(config)# ip igmp snooping v3-report-suppression	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as-is to multicast-capable routers. The default is enabled.
ip igmp snooping report-suppression switch(config)# ip igmp snooping report-suppression `switch(config)# ip igmp snooping report-suppression`	Configures IGMPv3 report suppression and proxy reporting. The default is disabled.

Step 3 **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

(Optional) Copies the running configuration to the startup configuration.

4.6.2 Configuring IGMP Snooping Parameters per VLAN

To affect the operation of the IGMP snooping process per VLAN, you can configure various optional IGMP snooping parameters.

Note

You configure the IGMP snooping parameters that you want by using this configuration mode; however, the configurations apply only after you specifically create the specified VLAN. See the *Inspur CN12900 Series INOS-CN Layer 2 Switching Configuration Guide* for information on creating VLANs.

Step 1 **configure terminal**

Example:

switch# configure terminal
switch(config)#

Enters global configuration mode.

Step 2 **ip igmp snooping**

Example:

switch(config)# ip igmp snooping

Enables IGMP snooping. The default is enabled.

Note If the global setting is disabled with the **no** form of this command, IGMP snooping on all VLANs is disabled, whether IGMP snooping is enabled on a VLAN or not. If you disable IGMP snooping, Layer 2 multicast frames flood to all modules.

Step 3 **vlan configuration** *vlan-id*

Example:

switch(config)# vlan configuration 2
switch(config-vlan-config)#

Configures the IGMP snooping parameters you want for the VLAN. These configurations do not apply until you create the specified VLAN.

Step 4 Use the following commands to configure IGMP snooping parameters per VLAN.

Option	**Description**
ip igmp snooping switch(config-vlan-config)# ip igmp snooping	Enables IGMP snooping for the current VLAN. The default is enabled.
ip igmp snooping access-group {**prefix-list** | **route-map**} *policy-name* **interface** *interface slot/port switch(config-vlan-config)# ip igmp snooping access-group prefix-list plist interface ethernet 2/2*	Configures a filter for IGMP snooping reports that is based on a prefix-list or route-map policy. The default is disabled. **Note** Inspur CN12908 switches with the CN129-X636C-R,CN129-X636C-RX, and CN129-X636Q-R line cards support this command beginning with Inspur INOS-CN

ip igmp snooping explicit-tracking switch(config-vlan-config)# ip igmp snooping explicit-tracking	Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled on all VLANs.
ip igmp snooping fast-leave switch(config-vlan-config)# ip igmp snooping fast-leave	Supports IGMPv2 hosts that cannot be explicitly tracked because of the host report suppression mechanism of the IGMPv2 protocol. When you enable fast leave, the IGMP software assumes that no more than one host is present on each VLAN port. The default is disabled for all VLANs.
ip igmp snooping group-timeout {*minutes* | **never**} switch(config-vlan-config)# ip igmp snooping group-timeout never	Configures the group membership timeout for the specified VLANs.
ip igmp snooping last-member-query-interval *seconds* *switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3*	Removes the group from the associated VLAN port if no hosts respond to an IGMP query message before the last member query interval expires. Values range from 1 to 25 seconds. The default is 1 second.
ip igmp snooping proxy general-queries [**mrt** *seconds*] switch(config-vlan-config)# ip igmp snooping proxy general-queries	Configures an IGMP snooping proxy for specified VLANs. The default is 5 seconds.
[**no**] **ip igmp snooping proxy-leave use-group-address** switch(config-vlan-config)# ip igmp snooping proxy-leave use-group-address	Changes the destination address of proxy leave messages to the address of the group that is leaving.Normally, IGMP proxy leave messages generated by the IGMP snooping module use the 224.0.0.2 multicast router address when all hosts leave the group. You should implement this configuration if your multicast applications rely on receiving reports and leave messages to start or stop multicast traffic based on the destination address of the packet.
ip igmp snooping querier *ip-address* switch(config-vlan-config)# ip igmp snooping querier 172.20.52.106	Configures a snooping querier when you do not enable PIM because multicast traffic does not need to be routed. The IP address is used as the source in messages.
ip igmp snooping querier-timeout *seconds* switch(config-vlan-config)# ip igmp snooping querier-timeout 300	Configures a snooping querier timeout value for IGMPv2 when you do not enable PIM because multicast traffic does not need to be routed. The default is 255 seconds.
ip igmp snooping query-interval *seconds* switch(config-vlan-config)# ip igmp snooping query-interval 120	Configures a snooping query interval when you do not enable PIM because multicast traffic does not need to be routed. The default value is 125 seconds.
ip igmp snooping query-max-response-time *seconds* switch(config-vlan-config)# ip igmp snooping query-max-response-time 12	Configures a snooping MRT for query messages when you do not enable PIM because multicast traffic does not need to be routed. The default value is 10 seconds.
[**no**] **ip igmp snooping report-flood** {**all** | **interface ethernet** *slot/port*} switch(config-vlan-config)# ip igmp snooping report-flood interface ethernet 1/2ip igmp snooping report-flood interface ethernet 1/3	Floods IGMP reports on all active interfaces of the VLAN or only on specific interfaces. IGMP reports typically are forwarded to multicast router ports as detected by the IGMP snooping module and are not flooded in the VLAN. However, this command forces the switch to send IGMP reports to custom ports belonging to the VLAN in addition to the multicast router ports. You should implement this configuration if your multicast applications require the ability to view IGMP reports in order to transmit traffic.
ip igmp snooping report-policy {**prefix-list** | **route-map**} *policy-name* **interface** *interface slot/port* switch(config-vlan-config)# ip igmp snooping report-policy route-map rmap	Configures a filter for IGMP snooping reports that is based on a prefix-list or route-map policy. The default is disabled.

interface ethernet 2/4	
ip igmp snooping startup-query-count *value* switch(config-vlan-config)# ip igmp snooping startup-query-count 5	Configures snooping for a number of queries sent at startup when you do not enable PIM because multicast traffic does not need to be routed.
ip igmp snooping startup-query-interval *seconds* switch(config-vlan-config)# ip igmp snooping startup-query-interval 15000	Configures a snooping query interval at startup when you do not enable PIM because multicast traffic does not need to be routed.
ip igmp snooping robustness-variable *value* switch(config-vlan-config)# ip igmp snooping robustness-variable 5	Configures the robustness value for the specified VLANs. The default value is 2.
ip igmp snooping report-suppression switch(config-vlan-config)# ip igmp snooping report-suppression	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as-is to multicast-capable routers. The default is enabled.
ip igmp snooping mrouter interface *interface* switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 2/1	Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN. You can specify the interface by the type and the number, such as **ethernet** slot/port.
ip igmp snooping static-group *group-ip-addr* [**source** *source-ip-addr*] **interface** *interface* switch(config-vlan-config)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1	Configures the Layer 2 port of a VLAN as a static member of a multicast group. You can specify the interface by the type and the number, such as **ethernet** slot/port.
ip igmp snooping link-local-groups-suppression switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression	Configures link-local groups suppression for the specified VLANs. The default is enabled.
ip igmp snooping v3-report-suppression switch(config-vlan-config)# ip igmp snooping v3-report-suppression	Configures IGMPv3 report suppression and proxy reporting for the specified VLANs. The default is enabled per VLAN.
ip igmp snooping version *value* switch(config-vlan-config)# ip igmp snooping version 2	Configures the IGMP version number for the specified VLANs.

Step 5 **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

(Optional) Copies the running configuration to the startup configuration.

4.7 Verifying the IGMP Snooping Configuration

Command	Description
show ip igmp snooping [**vlan** *vlan-id*]	Displays the IGMP snooping configuration by VLAN.
show ip igmp snooping groups [*source* [*group*] |*group* [*source*]] [**vlan** *vlan-id*] [**detail**]	Displays IGMP snooping information about groups by VLAN.
show ip igmp snooping querier [**vlan** *vlan-id*]	Displays IGMP snooping queriers by VLAN.
show ip igmp snooping mroute [**vlan** *vlan-id*]	Displays multicast router ports by VLAN.
show ip igmp snooping explicit-tracking [**vlan** *vlan-id*] [**detail**]	Displays IGMP snooping explicit tracking information by VLAN.

	Note	For vPC VLANs, you must enter the **detail** keyword to display this command on both vPC peer switches, If you do not enter the **detail** keyword, this command displays only on the vPC switch that received the native report.

4.8 Displaying IGMP Snooping Statistics

You can display the IGMP snooping statistics using these commands.

Command	**Description**
show ip igmp snooping statistics vlan	Displays IGMP snooping statistics. You can see the virtual port channel (vPC) statistics in this output.
show ip igmp snooping {**report-policy** |**access-group**} **statistics** [**vlan** *vlan*]	Displays detailed statistics per VLAN when IGMP snooping filters are configured.

4.9 Clearing IGMP Snooping Statistics

You can clear the IGMP snooping statistics using these commands.

Command	**Description**
clear ip igmp snooping statistics vlan	Clears the IGMP snooping statistics.
clear ip igmp snooping {**report-policy** |**access-group**} **statistics** [**vlan** *vlan*]	Clears the IGMP snooping filter statistics.

4.10 Configuration Examples for IGMP Snooping

Note

The configurations in this section apply only after you create the specified VLAN. See the *Inspur CN12900 Series INOS-CN Layer 2 Switching Configuration Guide* for information on creating VLANs.

The following example shows how to configure the IGMP snooping parameters:

```
config t
ip igmp snooping vlan configuration 2
ip igmp snooping
ip igmp snooping explicit-tracking
ip igmp snooping fast-leave
ip igmp snooping last-member-query-interval 3
ip igmp snooping querier 172.20.52.106
ip igmp snooping report-suppression
ip igmp snooping mrouter interface ethernet 2/1
ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
ip igmp snooping link-local-groups-suppression
ip igmp snooping v3-report-suppression
```

The following example shows how to configure prefix lists and use them to filter IGMP snooping reports:

```
ip prefix-list plist seq 5 permit 224.1.1.1/32
ip prefix-list plist seq 10 permit 224.1.1.2/32
ip prefix-list plist seq 15 deny 224.1.1.3/32
ip prefix-list plist seq 20 deny 225.0.0.0/8 eq 32
vlan configuration 2
ip igmp snooping report-policy prefix-list plist interface Ethernet 2/2
ip igmp snooping report-policy prefix-list plist interface Ethernet 2/3
```

In the above example, the prefix-list permits 224.1.1.1 and 224.1.1.2 but rejects 224.1.1.3 and all the groups in the 225.0.0.0/8 range. The prefix-list is an implicit "deny" if there is no match. If you wish to permit everything else, add **ip prefix-list plist seq 30 permit 224.0.0.0/4 eq 32**.

The following example shows how to configure route maps and use them to filter IGMP snooping reports:

```
route-map rmap permit 10
match ip multicast group 224.1.1.1/32 route-map rmap permit 2
match ip multicast group 224.1.1.2/32 route-map rmap deny 3
match ip multicast group 224.1.1.3/32 route-map rmap deny 4
match ip multicast group 225.0.0.0/8
vlan configuration 2
ip igmp snooping report-policy route-map rmap interface Ethernet 2/4
ip igmp snooping report-policy route-map rmap interface Ethernet 2/5
```

In the above example, the route-map permits 224.1.1.1 and 224.1.1.2 but rejects 224.1.1.3 and all the groups in the 225.0.0.0/8 range. The route-map is an implicit "deny" if there is no match. If you wish to permit everything else, add **route-map rmap permit 50 match ip multicast group 224.0.0.0/4**.

CHAPTER 5 Configuring MVR

This chapter describes how to configure the MVR feature on Inspur INOS-CN devices.

This chapter contains the following sections:

5.1 About MVR

In a typical Layer 2 multi-VLAN network, subscribers to a multicast group can be on multiple VLANs. To maintain data isolation between these VLANs, the multicast stream on the source VLAN must be passed to a router, which replicates the stream on all subscriber VLANs, wasting upstream bandwidth.

Multicast VLAN registration (MVR) allows a Layer 2 switch to forward the multicast data from a source on a common assigned VLAN to the subscriber VLANs, conserving upstream bandwidth by bypassing the router. The switch forwards multicast data for MVR IP multicast streams only to MVR ports on which hosts have joined, either by IGMP reports or by MVR static configuration. The switch forwards IGMP reports received from MVR hosts only to the source port. For other traffic, VLAN isolation is preserved.

MVR requires at least one VLAN to be designated as the common VLAN to carry the multicast stream from the source. More than one such multicast VLAN (MVR VLAN) can be configured in the system, and you can configure a global default MVR VLAN as well as interface-specific default MVR VLANs. Each multicast group using MVR is assigned to an MVR VLAN.

MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the MVR VLAN by sending IGMP join and leave messages. IGMP leave messages from an MVR group are handled according to the IGMP configuration of the VLAN on which the leave message is received. If IGMP fast leave is enabled on the VLAN, the port is removed immediately; otherwise, an IGMP query is sent to the group to determine whether other hosts are present on the port.

5.2 MVR Interoperation with Other Features

MVR and IGMP Snooping

Although MVR operates on the underlying mechanism of IGMP snooping, the two features operate independently of each other. One feature can be enabled or disabled without affecting the operation of the other feature. If IGMP snooping is disabled globally or on a VLAN and MVR is enabled on the VLAN, IGMP snooping is internally enabled on the VLAN. Joins received for MVR groups on non-MVR receiver ports or joins received for non-MVR groups on MVR receiver ports are processed by IGMP snooping.

MVR and vPCs

- As with IGMP snooping, IGMP control messages received by virtual port channel (vPC) peer switches are exchanged between the peers, allowing synchronization of MVR group information.
- MVR configuration must be consistent between the peers.
- The **no ip igmp snooping mrouter vpc-peer-link** command applies to MVR. With this command, multicast traffic is not sent to a peer link for the source VLAN and receiver VLAN unless an orphan port is in the VLAN.
- The **show mvr member** command shows the multicast group on the vPC peer switch. However, the vPC peer switch does not show the multicast groups if it does not receive the IGMP membership report of the groups.

5.3 Licensing Requirements for MVR

The following table shows the licensing requirements for this feature:

Product	License Requirement
Inspur INOS-CN	This feature does not require a license. Any feature not included in a license package is bundled with the INOS-CN image and is provided at no extra charge to you.

5.4 Guidelines and Limitations for MVR

MVR has the following guidelines and limitations:

- MVR is supported only for Inspur CN12908 switches with CN129-X636C-R, CN129-X636C-RX, or CN129-X636Q-R line cards.
- MVR is supported only on Layer 2 Ethernet ports, such as individual ports, port channels, and virtual Ethernet (vEth) ports.
- MVR receiver ports can only be access ports; they cannot be trunk ports. MVR source ports can be either access or trunk ports.
- MVR configuration on Flex Link ports is not supported.
- Priority tagging is not supported on MVR receiver ports.
- The total number of MVR VLANs cannot exceed 250.

5.5 Default MVR Settings

This table lists the default settings for MVR parameters.

Table 12 Default MVR Parameters

Parameter	Default
MVR	Disabled globally and per interface
Global MVR VLAN	None configured
Interface (per port)	Neither a receiver nor a source port

5.6 Configuring MVR

5.6.1Configuring MVR Global Parameters

You can globally enable MVR and various configuration parameters.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**[no]mvr** **Example:** switch(config)# mvr switch(config-mvr)#	Globally enables MVR. The default is disabled. Use the **no** form of the command to disable MVR.
Step 3	[**no**] **mvr-vlan** *vlan-id* **Example:** switch(config-mvr)# mvr-vlan 7	Specifies the global default MVR VLAN. The MVR VLAN is the source of the multicast message that subsequent receivers subscribe to. The range is from 1 to 4094. Use the **no** form of the command to clear the MVR VLAN.
Step 4	[**no**] **mvr-group** *addr* [*/mask*] [**count** *groups*] [**vlan** *vlan-id*] **Example:** switch(config-mvr)# mvr-group 230.1.1.1 count 4	Adds a multicast group at the specified IPv4 address (and optional netmask length) to the global default MVR VLAN. You can repeat this command to add additional

		groups to the MVR VLAN. The IP address is entered in the format a.b.c.d/m, where m is the number of bits in the netmask, from 1 to 31. You can optionally specify a number of MVR groups using contiguous multicast IP addresses starting with the specified IP address. Use the **count** keyword followed by a number from 1 to 64. You can optionally specify an MVR VLAN for the group by using the **vlan** keyword. Otherwise, the group is assigned to the default MVR VLAN. Use the **no** form of the command to clear the group configuration.
Step 5	(Optional) **clear mvr counters [source-ports |receiver-ports]** **Example:** switch(config-mvr)# clear mvr counters	Clears MVR IGMP packet counters.
Step 6	(Optional) **show mvr** **Example:** switch(config-mvr)# show mvr	Displays the global MVR configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** switch(config-mvr)# copy running-config startup-config	Copies the running configuration to the startup configuration.

5.6.2 Configuring MVR Interfaces

You can configure MVR interfaces on your Inspur INOS-CN device.

PROCEDURE

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**mvr** **Example:** switch(config)# mvr switch(config-mvr)#	Globally enables MVR. The default is disabled. **Note** If MVR is enabled globally, this command is not required.
Step 3	**interface** {**ethernet** *slot/port* |**port-channel** *channel-number* | **vethernet** *number*} **Example:** switch(config-mvr)# interface ethernet 2/2 switch(config-mvr-if)#	Specifies the Layer 2 port to configure and enters interface configuration mode.
Step 4	[**no**] **mvr-type** {**source** | **receiver**} **Example:** switch(config-mvr-if)# mvr-type source	Configures an MVR port as one of these types of ports: • **source**—An uplink port that sends and receives multicast data is configured as an MVR source. The port automatically becomes a static receiver of MVR multicast groups. A source port should be a member of the MVR VLAN. • **receiver**—An access port that is connected to a host that wants to subscribe to an MVR multicast group is configured as an MVR receiver. A

		receiver port receives data only when it becomes a member of the multicast group by using IGMP leave and join messages. If you attempt to configure a non-MVR port with MVR characteristics, the configuration is cached and does not take effect until the port becomes an MVR port. The default port mode is non-MVR.
Step 5	(Optional) [**no**] **mvr-vlan** *vlan-id* **Example:** switch(config-mvr-if)# mvr-vlan 7	Specifies an interface default MVR VLAN that overrides the global default MVR VLAN for joins received on the interface. The MVR VLAN is the source of the multicast message that subsequent receivers subscribe to. The range is from 1 to 4094.
Step 6	(Optional) [**no**] **mvr-group** *addr* [/*mask*] [**vlan** *vlan-id*] **Example:** switch(config-mvr-if)# mvr-group 225.1.3.1 vlan 100	Adds a multicast group at the specified IPv4 address (and optional netmask length) to the interface MVR VLAN,overriding the global MVR group configuration. You can repeat this command to add additional groups to the MVR. The IP address is entered in the format a.b.c.d/m, where m is the number of bits in the netmask, from 1 to 31. You can optionally specify an MVR VLAN for the group by using the **vlan** keyword; otherwise, the group is assigned to the interface default (if specified) or the global default MVR VLAN. Use the **no** form of the command to clear the IPv4 address and netmask.
Step 7	(Optional) **copy running-config startup-config** **Example:** switch(config-mvr-if)# copy running-config startup-config	Copies the running configuration to the startup configuration.

5.6.3 Suppressing IGMP Query Forwarding from VLANs

To suppress the IGMP general query from the source VLAN to the receiver VLAN perform the following steps.

PROCEDURE

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**mvr-config** **Example:** switch# mvr-config switch(config-mvr)#	Enters global MVR configuration mode.
Step 3	**mvr-suppress-query vlan** *vlan-ID*	Displays the MVR ID or source VLAN range from where the general queries need to be suppressed. The

	Example: switch(config-mvr)# mvr-suppress-query vlan 1-5 switch(config-mvr)#	VLAN IDvalue is 1 to 3967. The VLAN ID may also be expressed as a range 1-5, 10 or 2-5, 7-19.

5.7 Verifying the MVR Configuration

To display the MVR configuration information, perform one of the following tasks:

Command	**Description**
show mvr	Displays the MVR subsystem configuration and status.
show mvr groups	Displays the MVR group configuration.
show ip igmp snooping [**vlan** *vlan-id*]	Displays information about IGMP snooping on the specified VLAN.
show mvr interface {**ethernet** *slot/port* |**port-channel** *number*}	Displays the MVR configuration on the specified interface.
show mvr members [**count**]	Displays the number and details of all MVR receiver members.
show mvr members interface {**ethernet** *slot/port* |**port-channel** *number*}	Displays details of MVR members on the specified interface.
show mvr members vlan *vlan-id*	Displays details of MVR members on the specified VLAN.
show mvr receiver-ports [**ethernet** *slot/port* |**port-channel** *number*]	Displays all MVR receiver ports on all interfaces or on the specified interface.
show mvr source-ports [**ethernet** *slot/port* |**port-channel** *number*]	Displays all MVR source ports on all interfaces or on the specified interface.

This example shows how to verify the MVR parameters:

```
switch# show mvr  : enabled
MVR Status VLAN
Global MVR        : 100
Number of MVR VLANs : 4
```

This example shows how to verify the MVR group configuration:

```
switch# show mvr groups
* - Global default MVR VLAN.
Group start       Group end      CountMask      MVR-VLAN Interface
--------------------------- ------ -------- -----------
228.1.2.240       228.1.2.255    /28     101
230.1.1.1 230.1.1.4      4      *100
235.1.1.6 235.1.1.6      1      340
225.1.3.1  225.1.3.1         1     100
```

This example shows how to verify the MVR interface configuration and status:

```
switch# show      mvr interface  Status  MVR-VLAN
Port      VLAN    Type
----      ----    ----   ------  --------
Po10      100     SOURCE ACTIVE  100-101
Po201     201     RECEIVER       ACTIVE  100-101,340
Po202     202     RECEIVER       ACTIVE  100-101,340
Po203     203     RECEIVER       ACTIVE  100-101,340
Po204     204     RECEIVER       INACTIVE       100-101,340
Po205     205     RECEIVER       ACTIVE  100-101,340
Po206     206     RECEIVER       ACTIVE  100-101,340
Po207     207     RECEIVER       ACTIVE  100-101,340
Po208     208     RECEIVER       ACTIVE  2000-2001
Eth1/9    340     SOURCE ACTIVE  340
Eth1/10   20      RECEIVER       ACTIVE  100-101,340
Eth2/2    20      RECEIVER       ACTIVE  100-101,340
```

```
Eth102/1/1 102     RECEIVER       ACTIVE  100-101,340
Eth102/1/2 102     RECEIVER       INACTIVE       100-101,340
Eth103/1/1 103     RECEIVER       ACTIVE  100-101,340
Eth103/1/2 103     RECEIVER       ACTIVE  100-101,340
Status INVALID indicates one of the following misconfiguration:
a)Interface is not a switchport.
b)MVR receiver is not in access mode.
```

This example shows how to display all MVR members:

```
switch# show mvr members  Status  Members
MVR-VLAN   Group Address
--------   -------------  ------- -------
100        230.1.1.1      ACTIVE  Po201 Po202 Po203 Po205 Po206
100        230.1.1.2      ACTIVE  Po205 Po206 Po207 Po208
340        235.1.1.6      ACTIVE  Eth102/1/1
101        225.1.3.1      ACTIVE  Eth1/10 Eth2/2
101        228.1.2.241    ACTIVE  Eth103/1/1 Eth103/1/2
```

This example shows how to display all MVR receiver ports on all interfaces:

```
switch# show mvr receiver-ports
Port    MVR-VLAN    Status    Joins(v1,v2,v3)      Leaves
------------       --------       ------------------- ------------
Po201      100     ACTIVE         8                 2
Po202      100     ACTIVE         8                 2
Po203      100     ACTIVE         8                 2
Po204      100     INACTIVE      0                  0
Po205      100     ACTIVE        10                 6
Po206      100     ACTIVE        10                 6
Po207      100     ACTIVE        5                 0
Po208      100     ACTIVE        6                  0
Eth1/10    101     ACTIVE        12                 2
Eth2/2     101     ACTIVE        12                 2
Eth102/1/1 340     ACTIVE        16                 15
Eth102/1/2 340     INACTIVE       16                16
Eth103/1/1 101     ACTIVE        33                 0
Eth103/1/2 101     ACTIVE        33                 0
```

This example shows how to display all MVR source ports on all interfaces:

This example shows how to display all MVR source ports on all interfaces:

```
switch# show mvr source-ports
Port         MVR-VLAN    Status
          --------       --------
Po10------     100       ACTIVE
Eth1/9         340       ACTIVE
```

5.8 Configuration Examples for MVR

The following example shows how to globally enable MVR and configure the global parameters:

```
switch# configure terminal

switch(config)# mvr
switch(config-mvr)# mvr-vlan 100
switch(config-mvr)# mvr-group 230.1.1.1 count 4
switch(config-mvr)# mvr-group 228.1.2.240/28 vlan 101
switch(config-mvr)# mvr-group 235.1.1.6 vlan 340
switch# show mvr  : enabled
MVR Status
Global     MVR VLAN       :       100
Number     of MVR VLANs   :       3
```

The following example shows how to configure an Ethernet port as an MVR receiver port:

```
switch# configure terminal
switch(config)# mvr
switch(config-mvr)# interface ethernet 1/10
switch(config-mvr-if)# mvr-group 225.1.3.1 vlan 100
switch(config-mvr-if)# mvr-type receiver
switch(config-mvr-if)## copy running-config startup-config
```