IPv4 Multicast

This feature module describes how to configure IP multicast in an IPv4 network. IP multicast is an efficient way to use network resources, especially for bandwidth-intensive services such as audio and video.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Prerequisites for IPv4 Multicast

- Cisco IOS Release 15.4(1)S or a later release that supports the IPv4 Multicast feature must be installed previously on the Cisco ASR 901 Series Aggregation Services Router.
- You must enable the **asr901-multicast source** command on the SVI interface that is connected to the traffic source for PIM sparse mode.

Restrictions for IPv4 Multicast

- Source Specific Multicast (SSM) mapping takes a group G join from a host and identifies this group with an application associated with one or more sources. The SSM mapping can support only one such application per group G.
- When both SSM mapping and Internet Group Management Protocol Version 3 (IGMPv3) are enabled and the hosts already support IGMPv3 (but source specific information is not present), they start sending IGMPv3 group reports. These IGMPv3 group reports are not supported with SSM mapping and the router does not correctly associate sources with these reports.
- PIM Dense Mode is not supported.
- Only PIM version 2 is supported.
- PIM SM in VRF lite is not supported.
- Time-To-Live (TTL) threshold is not supported.
- Mroute ageing is not supported.
- Bi-Directional PIM (BIDIR-PIM) is not supported.
- Mroute based counter or rate statistics are not supported. Multicast counters are not supported.
- Multicast counters on physical and SVI interfaces are not supported till Cisco IOS Release 15.5(1)S.
- Multicast VPN (MVPN) is not supported.
- Multicast is *not* supported on Serial and MLPPP interfaces.
- PIM SSM IPv4 Multicast routing for VRF lite is supported only from Cisco IOS Release 15.4(3)S.
- Multiple L3 SVI interfaces on PoCH as replication VLAN's for multicast traffic are not supported.
- IP Multicast on loopback interface is not supported.

Information About IPv4 Multicast

IP multicast is a bandwidth-conserving technology that reduces traffic by delivering a single stream of information simultaneously to potentially thousands of businesses and homes. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

IP multicast routing enables a host (source) to send packets to a group of hosts (receivers) anywhere within the IP network by using a special form of IP address called the IP multicast group address. The sending host inserts the multicast group address into the IP destination address field of the packets and IP multicast routers and multilayer switches forward the incoming IP multicast packets out of all interfaces that lead to the members of the multicast group. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

Effective with Cisco IOS Release 15.4(1)S, IPv4 multicast is supported on the Cisco ASR 901 series routers. The router supports up to 500 unique multicast IP address entries, which includes both (*, G) and (S, G)

entries. Multicast support is provided for source and multicast groups using IGMP (IGMPv1 or IGMPv2 or IGMPv3) report messages.

For more information on IP Multicast Technology, see the *IP Multicast Technology Overview* document at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/xe-3s/imc_tech_oview.html.

Supported Protocols

- Basic multicast routing
- IP Multicast Routing for VRF Lite
- IGMP
- PIMv4 SSM
- PIMv4 SSM Mapping
- PIM MIB
- PIM sparse mode
- PIM BFD
- Static Rendezvous Point (RP)
- Auto RP
- Bootstrap router (BSR)

PIM SSM for IPv4

PIM SSM is the routing protocol that supports the implementation of SSM and is derived from the PIM sparse mode (PIM-SM). IGMP is the Internet Engineering Task Force (IETF) standards track protocol used for hosts to signal multicast group membership to routers. IGMPv3 supports source filtering, which is required for SSM. In order for SSM to run with IGMPv3, SSM must be supported in the device (the host where the application is running) and in the application itself.

Source Specific Multicast

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments and is described in RFC 3569 . The following two components together support SSM:

- PIM SSM
- IGMPv3

Protocol Independent Multicast

The PIM protocol maintains the current IP multicast service mode of receiver-initiated membership. PIM is not dependent on a specific unicast routing protocol; it is IP routing protocol independent, and can leverage whichever unicast routing protocols are used to populate the unicast routing table, including Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and static routes. PIM uses unicast routing information to perform the multicast forwarding function.

Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the RPF check function instead of building up a completely independent multicast routing table. Unlike other routing protocols, PIM does not send and receive routing updates between routers.

For more information on SSM and PIM, see the *IP Multicast Technology Overview* document at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/xe-3s/imc_tech_oview.html

PIM SSM Address Range

SSM can coexist with the Internet Standard Multicast (ISM) service by applying the SSM delivery model to a configured subset of the IP multicast group address range. The Cisco IOS software allows SSM configuration for an arbitrary subset of the IP multicast address range 224.0.0.0 through 239.255.255.255. When an SSM range is defined, existing IP multicast receiver applications do not receive any traffic when they try to use addresses in the SSM range (unless the application is modified to use explicit (S, G) channel subscription).

For groups within the SSM range, (S, G) channel subscriptions are accepted through IGMPv3 INCLUDE mode membership reports.

IGMP

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Enabling PIM on an interface also enables IGMP. IGMP provides a means to automatically control and limit the flow of multicast traffic throughout the network with the use of special multicast queriers and hosts.

For more information on IGMP, see the IP Multicast: IGMP Configuration Guide at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_igmp/configuration/xe-3s/imc_customizing_igmp.html

IGMPv1

IGMP version 1 is a simple protocol consisting of two messages. It provides the basic query-response mechanism that allows the multicast device to determine which multicast groups are active and other processes that enable hosts to join a multicast group. RFC 1112 defines the IGMPv1 host extensions for IP multicasting.

IGMPv2

IGMP version 2 extends the functionality of IGMP, allowing such capabilities as the IGMP leave process, group-specific queries, and an explicit maximum response time field. IGMPv2 also adds the capability for devices to elect the IGMP querier without dependence on the multicast protocol to perform this task. RFC 2236 defines IGMPv2.

IGMPv3

IGMP version 3 provides for source filtering, which enables a multicast receiver host to signal to a device which groups it wants to receive multicast traffic from, and from which sources this traffic is expected. In addition, IGMPv3 supports the link local address 224.0.0.22, which is the destination IP address for IGMPv3 membership reports; all IGMPv3-capable multicast devices must listen to this address. RFC 3376 defines IGMPv3.

IGMP Snooping

IGMP snooping allows a router to examine IGMP packets and make forwarding decisions based on their content. IGMP, which runs at Layer 3 on a multicast router, generates Layer 3 IGMP queries in subnets where the multicast traffic has to be routed. Using IGMP snooping, the router intercepts IGMP messages from the host and updates its multicast table accordingly.

You can configure the router to use IGMP snooping in subnets that receive IGMP queries from either IGMP or the IGMP snooping querier. IGMP snooping constrains IPv4 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv4 multicast traffic only to those ports that want to receive it.

You can configure the IGMP snooping lookup method for each VLAN. Layer 3 IGMP snooping lookup uses destination IP addresses in the Layer 2 multicast table (This is the default behavior). Layer 2 IGMP snooping lookup uses destination MAC addresses in the Layer 2 multicast table.

For more information on IGMP snooping, see the *IPv4 Multicast IGMP Snooping* document at: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/ipv4_igmp_snooping.html

IGMP Snooping Support

IGMP snooping is supported with the following specifics:

- Source-specific IGMP snooping is not supported.
- When IGMP snooping is configured, unknown multicast packets are flooded to the BD.
- The **ip igmp snooping tcn flood** and **ip igmp snooping tcn query solicit** commands are not supported.

Layer 2 VPN on the Physical Interface

- Default and port-based Xconnet—IGMP packets (control and data) are sent over the L2 VPN session.
- Dot1Q based Xconnect—If Xconnect is configured for a customer VLAN, IGMP packets (control and data) are carried into an L2 VPN. If they are not IGMP control packets, they are handled as reserved multicast packets in the BD VLAN, and data packets are forwarded according to the data in the IGMP snooping tables.

Layer 3 IP Multicast with IP IGMP Snooping

- Flows destined for PIM Sparse Mode-enabled and PIM Source-Specific Multicast-enabled groups are forwarded using Layer 3 IP Multicast logic.
- Flows destined for groups that are populated using IGMP snooping table are forwarded using IGMP snooping forward logic.
- Flows that are common (destined to groups that are populated using PIM-SM or PIM-SSM and IGMP snooping):
  - The accept interface of PIM-SM or PIM-SSM Multicast Forwarding Information Base (MFIB) is the same as the BD VLAN in which IGMP snooping based forwarding takes place.
  - Layer 3 forwarding takes place using output Layer 3 interface of PIM-SM or PIM-SSM MFIB.
  - Layer 2 forwarding takes place using the output ports from the IGMP snooping logic.

REP and MSTP Interworking

- After the Resilient Ethernet Protocol (REP) and Multiple Spanning Tree Protocol (MSTP) topology change, the routers in the ring generate IGMP general queries, and the convergence is based on the host replying to the general queries.

The following are supported as part of IGMP snooping:

- IGMP report and query processing
- IPv4 IGMP snooping

- Packet forwarding at hardware within bridge domain using IP multicast address lookup and IPv4 IGMP information.

PIM SSM Mapping

PIM SSM mapping supports SSM transition in cases where neither the URD nor IGMP v3lite is available, or when supporting SSM on the end system is not feasible. SSM mapping enables you to leverage SSM for video delivery to legacy set-top boxes (STBs) that do not support IGMPv3 or for applications that do not take advantage of the IGMPv3 host stack. URD and IGMPv3lite are applications used on receivers which do not have SSM support.

SSM mapping introduces a means for the last hop router to discover sources sending to groups. When SSM mapping is configured, if a router receives an IGMPv1 or IGMPv2 membership report for a particular group G, the router translates this report into one or more (S, G) channel memberships for the well-known sources associated with this group.

SSM mapping only needs to be configured on the last hop router connected to receivers. No support is needed on any other routers in the network. When the router receives an IGMPv1 or IGMPv2 membership report for a group G, the router uses SSM mapping to determine one or more source IP addresses for the group G. SSM mapping then translates the membership report as an IGMPv3 report INCLUDE (G, [S1, G], [S2, G]...[Sn, G] and continues as if it had received an IGMPv3 report.

Static SSM Mapping

SSM static mapping enables you to configure the last hop router to use a static map to determine the sources sending to groups. Static SSM mapping requires that you configure access lists (ACLs) to define group ranges. The groups permitted by those ACLs then can be mapped to sources using the **ip igmp static ssm-map** command.

For more information on SSM Mapping, see the IP Multicast: IGMP Configuration Guide at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_igmp/configuration/xe-3s/imc_ssm_map.html

Reverse Path Forwarding

Reverse-path forwarding is used for forwarding multicast datagrams. It functions as follows:

- If a router receives a datagram on an interface it uses to send unicast packets to the source, it means the packet has arrived on the RPF interface.
- If the packet arrives on the RPF interface, a router forwards the packet out the interfaces present in the outgoing interface list of a multicast routing table entry.
- If the packet does not arrive on the RPF interface, the packet is silently discarded to prevent loops.

PIM SSM uses source trees to forward datagrams; the RPF check is performed as follows:

- If a PIM router has source-tree state (that is, an [S, G] entry is present in the multicast routing table), the router performs the RPF check against the IPv4 address of the source of the multicast packet.
- Sparse-mode PIM uses the RPF lookup function to determine where it needs to send joins and prunes. (S, G) joins (which are source-tree states) are sent toward the source.

For more information on Reverse Path Forwarding, see the *Configuring Unicast Reverse Path Forwarding* document at: http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html

IP Multicast VRF Lite

The IP Multicast VRF Lite feature provides IPv4 multicast support for multiple virtual routing and forwarding (VRF) contexts. The scope of these VRFs is limited to the router in which the VRFs are defined.

This feature enables separation between routing and forwarding, providing an additional level of security because no communication between devices belonging to different VRFs is allowed unless explicitly configured. The IPv4 Multicast VRF Lite feature simplifies the management and troubleshooting of traffic belonging to a specific VRF.

PIM BFD

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols and independent of the higher layer protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning is easier and reconvergence time is consistent and predictable.

Protocol Independent Multicast (PIM) uses a hello mechanism for discovering new neighbors and for detecting failures between adjacent nodes. The minimum failure detection time in PIM is 3 times the PIM Query-Interval. To enable faster failure detection, the rate at which a PIM Hello message is transmitted on an interface is configurable. However, lower intervals increase the load on the protocol and can increase CPU and memory utilization and cause a system-wide negative impact on performance. Lower intervals can also cause PIM neighbors to expire frequently as the neighbor expiry can occur before the hello messages received from those neighbors are processed.

The BFD Support for Multicast (PIM) feature, also known as PIM BFD, registers PIM as a client of BFD. PIM can then utilize BFD to initiate a session with an adjacent PIM node to support BFD's fast adjacency failure detection in the protocol layer. PIM registers just once for both PIM and IPv6 PIM.

At PIMs request (as a BFD client), BFD establishes and maintains a session with an adjacent node for maintaining liveness and detecting forwarding path failure to the adjacent node. PIM hellos will continue to be exchanged between the neighbors even after BFD establishes and maintains a BFD session with the neighbor. The behavior of the PIM hello mechanism is not altered due to the introduction of this feature.

Although PIM depends on the Interior Gateway Protocol (IGP) and BFD is supported in IGP, PIM BFD is independent of IGP's BFD.

Configuring IPv4 Multicast

Enabling IPv4 Multicast Routing

To configure IPv4 multicast on the Cisco ASR 901 series routers, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables the privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**ip multicast-routing** **Example:** `Router(config)# ip multicast-routing`	Enables multicast routing.
Step 4	**asr901-platf-multicast enable** **Example:** `Router(config)# asr901-platf-multicast enable`	Enables multicast on the Cisco ASR 901 series routers.
Step 5	**ip pim rp-address** *rp-address* **Example:** `Router(config)# ip pim rp-address 192.168.0.1`	Configures the address of a PIM RP for multicast groups.
Step 6	**interface** *type number* **Example:** `Router(config)# interface vlan 5`	Configures the interface type and enters interface configuration mode.
Step 7	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables the PIM sparse mode.
Step 8	**asr901-multicast source** **Example:** `Router(config-if)# asr901-multicast source`	Configures the router to send multicast packets to the CPU enabling it to transmit register packets to the RP. **Note** This command should be enabled on the SVI which is facing the source and is applicable only for PIM SM.

Configuring PIM SSM

To configure PIM SSM, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip pim ssm [default | range** *access-list***]** **Example:** `Router(config-if)# ip pim ssm default`	Configures SSM service. The **default** keyword defines the SSM range access list. The **range** keyword specifies the standard IP access list number or name that defines the SSM range.
Step 4	**interface** *type number* **Example:** `Router(config)# interface vlan 5`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables PIM on an interface.
Step 6	**ip igmp version 3** **Example:** `Router(config-if)# ip igmp version 3`	Enables IGMPv3 on an interface.

Configuring PIM SSM Mapping

To configure PIM SSM mapping, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**no ip igmp ssm-map query dns** **Example:** `Router(config)# no ip igmp ssm-map query dns`	Disables DNS-based SSM mapping.
Step 4	**ip igmp ssm-map enable** **Example:** `Router(config)# ip igmp ssm-map enable`	Enables SSM mapping for groups in the configured SSM range.
Step 5	**ip igmp ssm-map static** *access-list source-address* **Example:** `Router(config)# ip igmp ssm-map static 11 172.16.8.11`	Configures static SSM mapping.

Configuring Multicast Receivers in VRF Interface

The Cisco ASR 901 router supports multicast receivers in VRF interface, if source and RP are present in the global routing table. To configure multicast receivers in VRF interface, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip mroute vrf** *vrf-name source-address mask* **fallback-lookup global** **Example:** `Router(config)# ip mroute vrf ABC 100.0.0.2 255.255.255.255 fallback-lookup global`	Configures the RPF lookup originating in Multicast Receiver VRF interface to continue and to be resolved in global routing table using static mroute. • **vrf**—Configures a static mroute in the MVRF instance specified for the *vrf-name* argument.

	Command or Action	Purpose
		• *source-address*—IP route prefix or explicit IP address of the source. • *mask*—Mask associated with the IP address or IP route prefix. • **global**—Specifies that the Multicast Source is in the global routing table.
Step 4	**end** **Example:** `Router(config)# end`	Exits the global configuration mode.

Configuring IGMP Snooping

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content.

Restrictions

Cisco ASR 901 routers support only the following encapsulations for IGMP snooping.

- Untagged
- Dot1q (with or without rewrite)
- Routed QinQ (with rewrite pop 2)

These sections describe how to configure IGMP snooping:

Enabling IGMP Snooping Globally

IGMP snooping is enabled by default. If IGMP snooping is disabled, to globally enable IGMP snooping on the router, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip igmp snooping** **Example:** `Router(config)# ip igmp snooping`	Enables IGMP snooping globally.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Enabling IGMP Snooping on a VLAN

To enable IGMP snooping on a VLAN, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip igmp snooping** **Example:** `Router(config)# ip igmp snooping`	Enables IGMP snooping globally.
Step 4	**ip igmp snooping vlan** *vlan-id* **Example:** `Router(config)# ip igmp snooping vlan 102`	Enables IGMP snooping on the VLAN. The VLAN ID ranges from 1 to 1001 and 1006 to 4094.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configuring an IGMP Snooping Query

To configure IGMP snooping query characteristics for a router or for a VLAN, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**asr901-platf-multicast enable** **Example:** `Router(config)# asr901-platf-multicast enable`	Enables multicast on the Cisco ASR 901 Router.
Step 4	**ip igmp snooping vlan** *vlan-id* **Example:** `Router(config)# ip igmp snooping vlan 5`	Enables IGMP snooping on a VLAN. • *vlan-id*—Multicast group VLAN ID. The VLAN ID ranges from 1 to 1001 and 1006 to 4094.
Step 5	**ip igmp snooping vlan** *vlan-id* **check rtr-alert-option** **Example:** `Router(config)# ip igmp snooping vlan 5 check rtr-alert-option`	Enforces IGMP snooping check and enables a device or interface to intercept packets only if the Router Alert (rtr-alert) option is enabled.
Step 6	**ip igmp snooping vlan** *vlan-id* **check ttl** **Example:** `Router(config)# ip igmp snooping vlan 5 check ttl`	Accepts IGMP packets with TTL=1.
Step 7	**ip igmp snooping vlan** *vlan-id* **immediate-leave** **Example:** `Router(config)# ip igmp snooping vlan 5 immediate-leave`	Minimizes the leave latency of IGMP memberships when IGMP Version 2 is used and only one receiver host is connected to each interface.
Step 8	**ip igmp snooping vlan** *vlan-id* **last-member-query-count** *interval* **Example:** `Router(config)# ip igmp snooping vlan 5 last-member-query-count-count 3`	Configures how often IGMP snooping sends query messages when an IGMP leave message is received. • *interval*—The interval at which query messages are sent, in milliseconds. The range is from 1 to 7. The default is 2.

	Command or Action	Purpose

Step 9	**ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *interval*
	Example:
	`Router(config)# ip igmp snooping vlan 5`
	`last-member-query-interval 100`
		Sets the last member query interval of the bridge domain.
		• *interval*—Length of time, in milliseconds, after which the group record is deleted if no reports are received. The default is 1000.

Step 10	**ip igmp snooping vlan** *vlan-id* **report-suppression**
	Example:
	`Router(config)# ip igmp snooping vlan 5`
	`report-suppression`
		Enables report suppression on the bridge domain.

Step 11	**ip igmp snooping vlan** *vlan-id* **robustness-variable** *variable*
	Example:
	`Router(config)# ip igmp snooping vlan 5`
	`robustness-variable 2`
		Sets the robust variable for the bridge domain.
		• *variable*—Robustness variable number. The range is from 1 to 3. The default is 2.

Step 12	**ip igmp snooping vlan** *vlan-id* **static** *ip-address* **interface** *interface-name interface-number*
	Example:
	`Router(config)# ip igmp snooping vlan 106`
	`static 226.1.1.2 interface gigabitEthernet 0/10`
		Configures static group membership entries on an interface.
		• *ip-address*—IP address of the IGMP snooping group.
		• **interface**—Specifies that one or more interfaces configured to a static router port are to be added to the group being configured.

Step 13	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Disabling IGMP Snooping

To disable IGMP snooping, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no ip igmp snooping** **Example:** `Router(config)# no ip igmp snooping`	Disables IGMP snooping.
Step 4	**no ip igmp snooping vlan** *vlan-id* **Example:** `Router(config)# no ip igmp snooping vlan 10`	Disables IGMP snooping from a VLAN.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configuring IPv4 Multicast Routing for VRF Lite

To configure IPv4 multicast routing for VRF Lite, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing vrf** *vrf-name* **Example:** `Router(config)# ip vrf vpe_1`	Names the VRF and enters VRF configuration mode. The *vrf-name*is the name assigned to a VRF. **Note** Configure the **ip pim vrf** *vrf-name* **ssm default** command on the Last Hop Router (LHR).
Step 4	**vrf definition** *vrf-name* **Example:** `Router(config-vrf)# vrf definition vpe_1`	Configures a VRF routing table instance and enters VRF configuration mode.

	Command or Action	Purpose
Step 5	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 1.1.1.1:100`	Specifies a route distinguisher (RD) for a VRF instance. The *route-distinguisher*is an 8-byte value to be added to an IPv4 prefix to create a VPN IPv4 prefix.
Step 6	**address-family ipv4** **Example:** `Router(config-vrf)# address-family ipv4`	Specifies the address family submode for configuring routing protocols.
Step 7	**exit address-family** **Example:** `Router(config-router-af)# exit address-family`	Exits the address family submode.

Enabling a VRF Under the VLAN Interface

To configure a VRF under the VLAN interface, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface VLAN 80`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Router(config-if)# vrf forwarding vpe_1`	Associates a VRF instance or a virtual network with an interface or subinterface. The *vrf-name* is the name assigned to a VRF.
Step 5	**ip address** *ip-address* **Example:** `Router(config-if)# ip address 192.108.1.27 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 6	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables PIM on an interface. The **sparse-mode** keyword enables sparse mode of operation.

	Command or Action	Purpose
Step 7	**ip ospf** *process-id* **area** *area-id* **Example:** `Router(config-if)# ip ospf 1 area 0`	Enables OSPFv2 on an interface . • *process-id*—A decimal value in the range 1 to 65535 that identifies the process ID. • *area-id*—A decimal value in the range 0 to 4294967295, or an IP address.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 9	**ip pim vrf** *vrf-name* **ssm default** **Example:** `Router(config)# ip pim vrf vpe-1 ssm default`	Defines the Source Specific Multicast (SSM) range of IP multicast addresses. • *vrf-name*—Name assigned to the VRF. • **default**—Defines the SSM range access list to 232/8.. **Note** This command should be configured on the Last Hop Router (LHR).

Configuring PIM BFD on an IPv4 Interface

To configure PIM BFD on an IPv4 interface, perform this task:

Restriction

- This feature is supported only on switch virtual interfaces on which both PIM and BFD are supported.
- For ECMP, PIM BFD is used to detect quick neighbor failure.
- For non-ECMP, BFD for IGP should be configured for faster convergence.
- Timers that are less than 50 ms for 3 sessions are not supported.

Before you begin

- IP multicast must be enabled and Protocol Independent Multicast (PIM) must be configured on the interface.
- Ensure that Bidirectional Forwarding Detection (BFD) for IGP is always configured along with PIM.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface VLAN 80`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**ip pim bfd** **Example:** `Router(config-if)# ip pim bfd`	Enables PIM BFD on an interface.

Verifying IPv4 Multicast Routing

Use the following **show** command to verify the IPv4 multicast routing.

```
Router# show asr901 multicast-support

Platform support for IPv4(v6) Multicast: ENABLED
```

Verifying PIM SSM

Use the **show** commands listed below to verify the PIM SSM configuration.

To display the multicast groups with receivers that are directly connected to the router and that were learned through IGMP, use the **show ip igmp groups** command described in the following example.

```
Router# show ip igmp groups

IGMP Connected Group Membership
Group Address    Interface              Uptime    Expires   Last Reporter   Group Accounted
232.1.1.1        Vlan70                   04:10:01  stopped   70.1.1.10
224.0.1.40       Vlan16                   04:17:35  00:02:58  16.1.1.3
224.0.1.40       Vlan23                   05:08:03  00:02:54  23.1.1.1
```

To display the contents of the IP multicast routing table, use the **show** command described in the following example.

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
```

```
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(9.1.1.1, 232.1.1.1), 00:00:03/00:02:57, flags: sTI
  Incoming interface: Vlan16, RPF nbr 16.1.1.1
  Outgoing interface list:
    Vlan70, Forward/Sparse, 00:00:04/00:02:56
(5.1.1.1, 232.1.1.1), 00:00:04/00:02:56, flags: sTI
  Incoming interface: Vlan16, RPF nbr 16.1.1.1
  Outgoing interface list:
    Vlan70, Forward/Sparse, 00:00:04/00:02:56
(*, 224.0.1.40), 00:00:12/00:02:47, RP 6.6.6.6, flags: SJCL
  Incoming interface: Vlan16, RPF nbr 16.1.1.1
  Outgoing interface list:
    Vlan23, Forward/Sparse, 00:00:12/00:02:47
```

Verifying PIM SSM Mapping

Use the **show** commands listed below to verify the PIM SSM Mapping configuration.

To display information about SSM mapping, use the **show** command described in the following example.

```
Router# show ip igmp ssm-mapping

SSM Mapping  : Enabled
DNS Lookup   : Disabled
Cast domain : ssm-map.cisco.com
Name servers : 255.255.255.255
```

To display the sources that SSM mapping uses for a particular group, use the show command described in the following example.

```
Router# show ip igmp ssm-mapping 232.1.1.1

Group address: 232.1.1.1
Database     : Static
Source list  : 5.1.1.1
               9.1.1.1
```

To display the multicast groups with receivers that are directly connected to the router and that were learned through IGMP, use the show command described in the following examples.

- **show ip igmp groups group-address**

```
Router# show ip igmp groups 232.1.1.1

IGMP Connected Group Membership
Group Address    Interface              Uptime    Expires   Last Reporter   Group Accounted
232.1.1.1        Vlan70                   04:14:26  stopped   70.1.1.10
```

- **show ip igmp groups interface-type** *interface-number*

```
Router# show ip igmp groups vlan70

IGMP Connected Group Membership
Group Address    Interface              Uptime    Expires   Last Reporter   Group Accounted
232.1.1.1        Vlan70                   04:15:33  stopped   70.1.1.10
```

- **show ip igmp groups interface-type detail**

```
Router# show ip igmp groups vlan70 detail

Flags: L - Local, U - User, SG - Static Group, VG - Virtual Group,
       SS - Static Source, VS - Virtual Source,
       Ac - Group accounted towards access control limit
Interface:      Vlan70
Group:          232.1.1.1
Flags:          SSM
Uptime:         04:15:37
Group mode:     INCLUDE
Last reporter:  70.1.1.10
CSR Grp Exp:    00:02:04
Group source list: (C - Cisco Src Report, U - URD, R - Remote, S - Static,
                    V - Virtual, M - SSM Mapping, L - Local,
                    Ac - Channel accounted towards access control limit)
  Source Address   Uptime    v3 Exp   CSR Exp   Fwd  Flags
  5.1.1.1          04:15:37  stopped   00:02:04  Yes  CM
  9.1.1.1          04:15:37  stopped   00:02:04  Yes  CM
```

Verifying Static Mroute

To display information about static mroute, use the **show ip mroute [vrf** *vrf-name*] *group-address* command described in the following examples.

```
Router# show ip mroute

mroute vrf VPN_A 239.1.1.1
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.1.1.1), 00:03:57/stopped, RP 4.4.4.4, flags: SJCL
  Incoming interface: Vlan21, RPF nbr 21.1.1.1, using vrf IPv4 default
  Outgoing interface list:
    Vlan72, Forward/Sparse, 00:03:56/00:02:10

(70.1.1.10, 239.1.1.1), 00:00:49/stopped, flags: LT
```

```
  Incoming interface: Vlan22, RPF nbr 22.1.1.2, using vrf IPv4 default
  Outgoing interface list:
    Vlan72, Forward/Sparse, 00:00:49/00:02:10
```

Verifying IGMP Snooping

Use the show commands listed below to verify the IGMP snooping configuration.

To display the IGMP snooping configuration of a device, use the **show ip igmp snooping** command, as shown in the following example:

```
Router# show ip igmp snooping

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping Oper State     : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000
Check TTL=1                  : No
Check Router-Alert-Option    : No

Vlan 101:
--------
IGMP snooping Admin State           : Enabled
IGMP snooping Oper State            : Enabled
IGMPv2 immediate leave              : Disabled
Report suppression                  : Enabled
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
Check TTL=1                         : Yes
Check Router-Alert-Option           : Yes

Vlan 102:
--------
IGMP snooping Admin State           : Enabled
IGMP snooping Oper State            : Enabled
IGMPv2 immediate leave              : Disabled
Report suppression                  : Enabled
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
Check TTL=1                         : Yes
Check Router-Alert-Option           : Yes

Vlan 105:
--------
IGMP snooping Admin State           : Enabled
IGMP snooping Oper State            : Enabled
IGMPv2 immediate leave              : Disabled
Report suppression                  : Enabled
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
Check TTL=1                         : Yes
Check Router-Alert-Option           : Yes
```

To display the IGMP snooping configuration, use the **show ip igmp snooping vlan** *bridge-domain* command, as shown in the following example:

```
Router# show ip igmp snooping vlan 105

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping Oper State     : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000
Check TTL=1                  : No
Check Router-Alert-Option    : No

Vlan 105:
--------
IGMP snooping Admin State           : Enabled
IGMP snooping Oper State            : Enabled
IGMPv2 immediate leave              : Disabled
Report suppression                  : Enabled
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
Check TTL=1                         : Yes
Check Router-Alert-Option           : Yes
Query Interval                      : 0
Max Response Time                   : 10000
```

To display the IGMP snooping configuration, use the **show ip igmp snooping groups** command, as shown in the following examples:

```
Router# show ip igmp snooping groups

Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode

Vlan Group/source Type Version Port List
------------------------------------------------------------------------
104 232.0.0.5 I v3 Gi0/0
104 232.0.0.6 I v3 Gi0/0
104 232.0.0.7 I v3 Gi0/0
104 232.0.0.8 I v3 Gi0/0
104 232.0.0.9 I v3 Gi0/0


Router# show ip igmp snooping groups vlan 104

Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode

Vlan Group/source Type Version Port List
------------------------------------------------------------------------
104 232.0.0.5 I v3 Gi0/0
104 232.0.0.6 I v3 Gi0/0
104 232.0.0.7 I v3 Gi0/0
104 232.0.0.8 I v3 Gi0/0
104 232.0.0.9 I v3 Gi0/0


Router# show ip igmp snooping groups count
```

```
Total number of groups: 6
Total number of (S,G): 0

------------------------------------------------------------------------
```

Verifying IP Multicast Routing for VRF Lite

Use the **show** commands listed below to verify IPv4 multicast routing for VRF Lite configuration.

To view information about the interfaces configured for Protocol Independent Multicast (PIM), use the **show ip pim interface detail** command:

```
Router# show ip pim vrf vpe_2 interface detail

Vlan80 is administratively down, line protocol is down
  Internet address is 192.108.1.27/24
  Multicast switching: fast
  Multicast packets in/out: 0/0
  Multicast TTL threshold: 0
  PIM: enabled
    PIM version: 2, mode: sparse
    PIM DR: 0.0.0.0
    PIM neighbor count: 0
    PIM Hello/Query interval: 30 seconds
    PIM Hello packets in/out: 0/0
    PIM J/P interval: 60 seconds
    PIM State-Refresh processing: enabled
    PIM State-Refresh origination: disabled
    PIM NBMA mode: disabled
    PIM ATM multipoint signalling: disabled
    PIM domain border: disabled
    PIM neighbors rpf proxy capable: FALSE
    PIM BFD: disabled
    PIM Non-DR-Join: FALSE
  Multicast Tagswitching: disabled
```

To view the information in a PIM topology table, use the **show ip mroute vrf** command:

```
Router# show ip mroute vrf vpe_2

IP Multicast Forwarding is not enabled.
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
```

To view the forwarding entries and interfaces in the IP Multicast Forwarding Information Base (MFIB), use the **show ip mfib vrf** command:

```
Router# show ip mfib vrf

Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
                ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
                MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
                MS  - MoFRR  Entry in Sync, MC - MoFRR entry in MoFRR Client.
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
Default
 (*,224.0.0.0/4) Flags: C
   SW Forwarding: 0/0/0/0, Other: 8/8/0
 (*,224.0.1.39) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   4106200/12/60/5, Other: NA/NA/NA
   Vlan24 Flags: F NS
     Pkts: 0/0
   Vlan21 Flags: F NS
     Pkts: 0/0
   Loopback0 Flags: NS
 (4.4.4.4,224.0.1.39) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   876500/12/60/5, Other: NA/NA/NA
   Loopback0 Flags: A
   Vlan24 Flags: F NS
     Pkts: 0/0
   Vlan21 Flags: F NS
     Pkts: 0/0
 (*,224.0.1.40) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   5369900/12/60/5, Other: NA/NA/NA
   Vlan24 Flags: F NS
     Pkts: 0/0
   Vlan21 Flags: F NS
     Pkts: 0/0
   Loopback0 Flags: F IC NS
     Pkts: 0/0
 (2.2.2.2,224.0.1.40) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   200/0/60/0, Other: NA/NA/NA
   Vlan24 Flags: A
   Loopback0 Flags: F IC NS
     Pkts: 0/0
 (*,232.0.0.1) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: NA/NA/NA
   Tunnel4 Flags: A
 (70.1.1.10,232.0.0.1) Flags:
   SW Forwarding: 0/0/0/0, Other: 2/0/2
   HW Forwarding:   0/0/0/0, Other: NA/NA/NA
   Tunnel4 Flags: A
   Vlan24 Flags: NS
```

```
VRF VPN_C
 (*,224.0.0.0/4) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,224.0.1.40) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: NA/NA/NA
   Vlan131 Flags: IC
 (*,232.0.0.1) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: NA/NA/NA
 (171.1.1.10,232.0.0.1) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   923200/12/60/5, Other: NA/NA/NA
   Vlan134 Flags: A
   Vlan131 Flags: F NS
     Pkts: 0/0

VRF VPN_B
 (*,224.0.0.0/4) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
 (*,224.0.1.40) Flags: C
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   5369300/12/60/5, Other: NA/NA/NA
   Vlan121 Flags: IC
```

Verifying PIM BFD Support

Use the **show** commands listed below to verify PIM BFD support.

To display a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies for an IPv4 neighbor, use the **show bfd neighbors ipv4** command:

```
Router# show bfd neighbors ipv4

IPv4 Sessions
NeighAddr LD/RD RH/RS State Int
24.24.24.1 3/3 Up Up Vl24
101.101.101.1 1/3 Up Up Vl101
```

To display BFD's registered clients such as PIM, OSPF, and so on, use the **show bfd neighbors ipv4 details** command:

```
Router# show bfd neighbors ipv4 details

IPv4 Sessions
NeighAddr LD/RD RH/RS State Int
24.24.24.1 3/3 Up Up Vl24
Session state is UP and not using echo function.
Session Host: Software
OurAddr: 24.24.24.2
Handle: 3
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 126(0), Hello (hits): 50(36644)
Rx Count: 36656, Rx Interval (ms) min/max/avg: 1/56/45 last: 24 ms ago
```

```
Tx Count: 36647, Tx Interval (ms) min/max/avg: 1/56/46 last: 8 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: PIM CEF OSPF
Template: abc
Authentication(Type/Keychain): md5/chain1
last_tx_auth_seq: 5 last_rx_auth_seq 4
Uptime: 00:27:47
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
C bit: 0
Multiplier: 3 - Length: 48
My Discr.: 3 - Your Discr.: 3
Min tx interval: 50000 - Min rx interval: 50000
Min Echo interval: 0

IPv4 Sessions
NeighAddr LD/RD RH/RS State Int
101.101.101.1 1/3 Up Up Vl101
Session state is UP and not using echo function.
Session Host: Software
OurAddr: 101.101.101.2
Handle: 1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 126(0), Hello (hits): 50(37036)
Rx Count: 37014, Rx Interval (ms) min/max/avg: 1/56/46 last: 24 ms ago
Tx Count: 37037, Tx Interval (ms) min/max/avg: 1/60/46 last: 0 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: PIM CEF OSPF
Template: abc
Authentication(Type/Keychain): md5/chain1
last_tx_auth_seq: 4 last_rx_auth_seq 6
Uptime: 00:28:03
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
C bit: 0
Multiplier: 3 - Length: 48
My Discr.: 3 - Your Discr.: 1
Min tx interval: 50000 - Min rx interval: 50000
Min Echo interval: 0
```

Configuration Examples for IPv4 Multicast

Example: IPv4 Multicast Routing

The following is a sample configuration of IPv4 Multicast routing feature on the Cisco ASR 901 Router:

```
!
Building configuration...
Current configuration : 120 bytes
!
ip multicast-routing
asr901-platf-multicast enable
!
interface Vlan5
```

```
 asr901-multicast source
 ip address 22.1.1.2 255.255.255.0
 ip pim sparse-mode
!
end
```

Example: Configuring PIM SSM

The following is a sample configuration of PIM SSM on the Cisco ASR 901 Router:

```
!
Building configuration...
Current configuration : 116 bytes
!
ip multicast-routing
asr901-platf-multicast enable
!
ip pim ssm default
interface Vlan70
ip address 70.1.1.2 255.255.255.0
ip pim sparse-mode
ip igmp version 3
ip ospf 1 area 0
end
```

Example: Configuring PIM SSM Mapping

The following is a sample configuration of PIM SSM Mapping on the Cisco ASR 901 Router:

```
!
no ip domain lookup
ip domain multicast ssm.map.cisco.com
ip name-server 10.48.81.21
!
ip multicast-routing
ip igmp ssm-map enable
ip igmp ssm-map static 10 172.16.8.10
ip igmp ssm-map static 11 172.16.8.11
!
.
.
.
!
interface vlan10
 description Sample IGMP Interface Configuration for SSM-Mapping Example
 ip address 10.20.1.2 255.0.0.0
 ip pim sparse-mode
 ip igmp static-group 232.1.2.1 source ssm-map
 ip igmp version 3
!
.
.
.
!
ip pim ssm default
!
access-list 10 permit 232.1.2.10
access-list 11 permit 232.1.2.0 0.0.0.255
```

```
!
```

Example: Configuring Rendezvous Point

For a sample configuration of RP, see the *Configuring a Rendezvous Point* document at: http://www.cisco.com/en/US/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

Example: Configuring Multicast Receivers in the VRF Interface

The following is a sample configuration multicast receivers in the VRF interface on the Cisco ASR 901 Router:

```
ip mroute vrf ABC 100.0.0.2 255.255.255.255 fallback-lookup global
```

Example: Configuring IGMP Snooping

The following is a sample IGMP snooping configuration:

```
Building configuration...

Current configuration : 3509 bytes
!
.
.
.
asr901-platf-multicast enable
ip multicast-routing
ip igmp snooping explicit-tracking limit 1000
ip igmp snooping vlan 106 immediate-leave
ip igmp snooping vlan 106 robustness-variable 3
ip igmp snooping vlan 106 last-member-query-count 6
ip igmp snooping vlan 106 last-member-query-interval 1000
ipv6 unicast-routing
ipv6 cef
!
.
.
.
```

Example: Configuring IPv4 Multicast Routing for VRF Lite

The following is a sample configuration of IPv4 multicast routing for VRF Lite:

```
!Building configuration...
!
!
!
!
vrf definition vpe_2
 rd 1.1.1.1:100
 !
 address-family ipv4
 exit-address-family
!
!
```

```
!

ip multicast-routing
asr901-platf-multicast enable
license boot level AdvancedMetroIPAccess
!
ip multicast-routing vrf vpe_2
ip pim vrf vpe_2 ssm default
!
interface Vlan80
 vrf forwarding vpe_2
 ip address 192.108.1.27 255.255.255.0
 ip pim sparse-mode
 ip ospf 1 area 0
 shutdown
!
end
```

Example: Configuring PIM BFD on an IPv4 Interface

The following is a sample configuration of PIMv4 BFD on an interface:

```
Building configuration...

Current configuration : 6735 bytes
!
! Last configuration change at 17:19:42 IST Wed May 21 2014
!
version 15.4
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone IST 5 30
ip cef
!
!
!
!
no ip domain lookup

ip multicast-routing



asr901-platf-multicast enable


interface Loopback1
ip address 3.3.3.3 255.255.255.255
ip ospf 1 area 0
!

!
interface GigabitEthernet0/0
no ip address
negotiation auto
service instance 24 ethernet
```

```
encapsulation dot1q 24
rewrite ingress tag pop 1 symmetric
bridge-domain 24


!
interface Vlan24
ip address 24.24.24.2 255.255.255.0
ip pim sparse-mode
ip pim bfd
ip igmp version 3
bfd interval 50 min_rx 50 multiplier 3

!
router ospf 1
router-id 3.3.3.3
timers throttle spf 50 50 5000
timers throttle lsa 10 20 5000
timers lsa arrival 10
timers pacing flood 5
network 24.24.24.0 0.0.0.255 area 0
network 25.25.25.0 0.0.0.255 area 0
network 55.55.55.0 0.0.0.255 area 0
network 101.101.101.0 0.0.0.255 area 0
bfd all-interfaces

ip pim ssm default



end
```

Troubleshooting Tips

To display IGMP packets received and sent, use the following **debug** command:

```
Router# debug ip igmp
```

To display debugging messages about IGMP snooping, use the following **debug** command:

```
Router# debug ip igmp snooping
```

To display debugging messages about IP PIM, use the following **debug** command:

```
Router# debug ip pim hello
```

To display PIM packets received and sent, and to display PIM-related events for BFD, use the following **debug** command:

```
Router# debug ip pim bfd
```

To display debugging messages about BFD, use the following **debug** command:

```
Router# debug bfd event
```

Note We recommend that you do not use these **debug** commands without TAC supervision.

Additional References

The following sections provide references related to IPv4 Multicast feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Router Commands	Cisco ASR 901 Series Aggregation Services Router Command Reference
IP Multicast Technology Overview	IP Multicast: PIM Configuration Guide
Customizing IGMP	IP Multicast: IGMP Configuration Guide
Configuring Unicast Reverse Path Forwarding	Cisco IOS Security Configuration Guide

Standards and RFCs

Standards/RFCs	Title
RFC 1112	Host Extensions for IP Multicasting
RFC 2236	Internet Group Management Protocol, Version 2
RFC 3376	Internet Group Management Protocol, Version 3
RFC 3569	Source-Specific Multicast

MIBs

MIB	MIBs Link
PIM-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for IPv4 Multicast

The following table lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Note The following table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1: Feature Information for IPv4 Multicast

Feature Name	Releases	Feature Information
Source Specific Multicast	15.4(1)S	This feature was introduced on the Cisco ASR 901 Routers. The following section provides information about this feature: **Platform-Independent Cisco IOS Software Documentation** • See the " Configuring Source Specific Multicast " chapter of the *IP Multicast: IGMP Configuration Guide*.
Source Specific Multicast Mapping	15.4(1)S	This feature was introduced on the Cisco ASR 901 Routers. The following section provides information about this feature: **Platform-Independent Cisco IOS Software Documentation** See the " SSM Mapping " chapter of the *IP Multicast: IGMP Configuration Guide*.
IGMP Version 1	15.4(1)S	This feature was introduced on the Cisco ASR 901 Routers. The following section provides information about this feature: **Platform-Independent Cisco IOS Software Documentation** See the " Customizing IGMP " chapter of the *IP Multicast: IGMP Configuration Guide*.

Feature Name	Releases	Feature Information
IGMP Version 2	15.4(1)S	This feature was introduced on the Cisco ASR 901 Routers. The following section provides information about this feature: **Platform-Independent Cisco IOS Software Documentation** See the " Customizing IGMP " chapter of the *IP Multicast: IGMP Configuration Guide*.
IGMP Version 3	15.4(1)S	This feature was introduced on the Cisco ASR 901 Routers. The following section provides information about this feature: **Platform-Independent Cisco IOS Software Documentation** See the " Customizing IGMP " chapter of the *IP Multicast: IGMP Configuration Guide*.
IGMP Snooping	15.4(2)S	This feature was introduced on the Cisco ASR 901 Routers. The following sections provide information about this feature: • IGMP Snooping, on page 4 • Configuring IGMP Snooping, on page 11
IP Multicast VRF Lite	15.4(3)S	This feature was introduced on the Cisco ASR 901 Routers. The following sections provide information about this feature: • IP Multicast VRF Lite, on page 7 • Configuring IPv4 Multicast Routing for VRF Lite, on page 15
BFD Support for Multicast (PIM)	15.4(3)S	This feature was introduced on the Cisco ASR 901 Routers. The following sections provide information about this feature: • PIM BFD, on page 7 • Configuring PIM BFD on an IPv4 Interface, on page 17