Implementing Layer-2 Multicast with IGMP Snooping

Internet Group Management Protocol (IGMP) snooping restricts multicast flows at Layer 2 to only those segments with at least one interested receiver. This module describes how to implement IGMP snooping on Cisco ASR 9000 Series Routers.

Feature History for IGMP Snooping

Release	Modification
Release 3.7.2	This feature was introduced.
Release 3.9.2	Support was added for the following features: • IGMP snooping group limits and access groups.
Release 4.0.0	Support was added for the following features: • Multicast redundancy using Multi-Chassis Link Aggregation (MC-LAG).

Prerequisites for IGMP Snooping

The following prerequisites must be satisfied before implementing IGMP snooping:

- The network must be configured with a Layer 2 VPN (L2VPN).

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

  To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Supported Features and Restrictions for IGMP Snooping

- EVPN dual-homed Active Active (AA) IGMP State Sync using IGMP snooping profile is supported.
- BVI under bridge domain is supported.
- IGMP snooping is supported only under L2VPN bridge domains.
- Explicit host tracking (an IGMPv3 snooping feature) is not supported.
- IPv6 Multicast Listener Discovery (MLD) snooping is not supported.
- IGMPv1 is not supported.
- IGMP snooping with VPLS on bridge domain is not supported.
- IGMP snooping over access and core Pseudo-wire is not supported.
- ISSU is not supported on Layer 2 Multicast.
- IGMPv3-exclude is not supported in EVPN multi-homing or proxy scenarios.
- For EVPN AA, IGMPv2 and IGMPv3 joins for same groups are not supported.
- **router-alert-check disable** configuration command is not supported.
- EVPN configuration must have the **control-word-disable** configuration.
- PIM control packets (join and hello) processing is not supported when snooping is enabled, so a multicast router selection based on PIM packets won't occur.
- In an EVPN dual-home AA scenario:
  - If the multicast source and receiver are in the same bridge domain (BD), the receiver might receive permanent traffic duplication.
  - In an EVPN dual-home receiver AA scenario, transient traffic duplication is expected when the DH node role changes from DF to nDF and vice versa.
  - Source=ESI1=BE-X.A, Receiver=ESI1=BE-X.B under the same BD is not supported (where X.A and X.B represent two AC ports for the bundle interface BE).
  - Source=ESI1=BE-X.A (for NCS 5700 line cards), Receiver=ESI2=BE-Y.A (for NCS 5500 line cards) under the same BD is not supported (where X.A and Y.A represent two AC ports for the bundle interface BE).

Note IPv4 multicast is supported for a multicast source that is behind the BVI interface. For example, the below configuration shows how to configure source behind BVI for IPv4 multicast:

```
l2vpn
bridge group 1
  bridge-domain 1
   multicast-source ipv4
   igmp snooping profile grp1
   !
   interface TenGigE0/0/0/3.32
   !
   routed interface BVI1
```

IGMP snooping for bridge domains without Bridged Virtual Interface (BVI) is supported with the following design consideration: You must configure the multicast-source ipv4 command in the source switch where bridge domain and IGMP snooping are enabled.

Information About IGMP Snooping

IGMP Snooping Overview

Description of Basic Functions

IGMP snooping provides a way to constrain multicast traffic at Layer 2. By snooping the IGMP membership reports sent by hosts in the bridge domain, the IGMP snooping application can set up Layer 2 multicast forwarding tables to deliver traffic only to ports with at least one interested member, significantly reducing the volume of multicast traffic.

Configured at Layer 3, IGMP provides a means for hosts in an IPv4 multicast network to indicate which multicast traffic they are interested in and for routers to control and limit the flow of multicast traffic in the network at Layer 3.

IGMP snooping uses the information in IGMP membership report messages to build corresponding information in the forwarding tables to restrict IP multicast traffic at Layer 2. The forwarding table entries are in the form <Route, OIF List>, where:

- Route is a <*, G> route or <S, G> route, where * is any source, G is group and S is the source.
- OIF List comprises all bridge ports that have sent IGMP membership reports for the specified route plus all multicast router (mrouter) ports in the bridge domain.

Implemented in a multicast network, IGMP snooping has the following attributes:

- In its basic form, it reduces bandwidth consumption by reducing multicast traffic that would otherwise flood an entire VPLS bridge domain.
- With the use of some optional configurations, it provides security between bridge domains by filtering the IGMP reports received from hosts on one bridge port and preventing leakage towards the hosts on other bridge ports.

- Using optional configurations, reduces the traffic impact on upstream IP multicast routers by suppressing IGMP membership reports (IGMPv2) or by acting as an IGMP proxy reporter (IGMPv3) to the upstream IP multicast router.

High Availability Features

All high availability features apply to the IGMP snooping processes with no additional configuration beyond enabling IGMP snooping. The following high availability features are supported:

- Process restarts
- RP Failover
- Stateful Switch-Over (SSO)
- Non-Stop Forwarding (NSF)—Forwarding continues unaffected while the control plane is restored following a process restart or route processor (RP) failover.
- Line card online insertion and removal (OIR)

Bridge Domain Support

IGMP snooping operates at the bridge domain level. When IGMP snooping is enabled on a bridge domain, the snooping functionality applies to all ports under the bridge domain, including:

- Physical ports under the bridge domain.
- Ethernet flow points (EFPs)—An EFP can be a VLAN, VLAN range, list of VLANs, or an entire interface port.
- Ethernet bundles—Ethernet bundles include IEEE 802.3ad link bundles and Cisco EtherChannel bundles. From the perspective of the IGMP snooping application, an Ethernet bundle is just another EFP. The forwarding application in the Cisco ASR 9000 Series Routers randomly nominates a single port from the bundle to carry the multicast traffic.

Note The **efp-visibility** configuration is required when a bridge has attachment circuits as VLAN sub-interfaces from the same bundle-ether or physical interface.

IGMP snooping for bridge domains without Bridged Virtual Interface (BVI) is supported with the following design consideration:

You must configure the **multicast-source ipv4** command in the source switch where IGMP snooping is enabled as seen in the following example:

```
l2vpn
bridge group 1
bridge-domain 1
multicast-source ipv4
igmp snooping profile grp1
!
interface TenGigE0/0/0/3.31 //Source
!
interface TenGigE0/0/0/3.32
!
routed interface BVI1
```

Multicast Router and Host Ports

IGMP snooping classifies each port (for example, EFPs, PWs, physical ports, or EFP bundles) as one of the following:

- Multicast router ports (mrouter ports)—These are ports to which a multicast-enabled router is connected. Mrouter ports are usually dynamically discovered, but may also be statically configured. Multicast traffic is always forwarded to all mrouter ports, except when an mrouter port is the ingress port.
- Host ports—Any port that is not an mrouter port is a host port.

Multicast Router Discovery and Static Configuration

IGMP snooping discovers mrouter ports dynamically. You can also explicitly configure a port as an mrouter port.

- Discovery—IGMP snooping identifies upstream mrouter ports in the bridge domain by snooping IGMP query messages and Protocol Independent Multicast Version 2 (PIMv2) hello messages. Snooping PIMv2 hello messages identifies IGMP nonqueriers in the bridge domain.
- Static configuration—You can statically configure a port as an mrouter port with the **mrouter** command in a profile attached to the port. Static configuration can help in situations when incompatibilities with non-Cisco equipment prevent dynamic discovery.

The **router-guard** command prevents a port from becoming a dynamically discovered mrouter port by filtering out multicast router messages, including IGMP queries and PIM messages. You can configure a port with the **router-guard** command and then configure it as a static mrouter. See the Router Guard and Static Mrouter, on page 16 for more information about configuring router-guard and mrouter commands on the same port.

Multicast Traffic Handling within a Bridge Domain with IGMP Snooping Enabled

The following tables describe traffic handling behaviors by IGMP snooping mrouter and host ports. Table 1: Multicast Traffic Handling for an IGMPv2 Querier, on page 5 describes traffic handling for an IGMPv2 querier. Table 2: Multicast Traffic Handling for an IGMPv3 Querier, on page 6 applies to an IGMPv3 querier.

By default, IGMP snooping supports IGMPv2 and IGMPv3. The version of the IGMP querier discovered in the bridge domain determines the operational version of the snooping processes. If you change the default, configuring IGMP snooping to support a minimum version of IGMPv3, IGMP snooping ignores any IGMPv2 queriers.

Table 1: Multicast Traffic Handling for an IGMPv2 Querier

Traffic Type	Received on MRouter Ports	Received on Host Ports
IP multicast source traffic	Forwards to all mrouter ports and to host ports that indicate interest.	Forwards to all mrouter ports and to host ports that indicate interest.
IGMP general queries	Forwards to all ports.	—
IGMP group-specific queries	Forwards to all other mrouter ports.	Dropped

Traffic Type	Received on MRouter Ports	Received on Host Ports
IGMPv2 joins	Examines (snoops) the reports. • If report suppression is enabled, forwards first join for a new group or first join following a general query for an existing group. • If report suppression is disabled, forwards on all mrouter ports.	Examines (snoops) the reports. • If report suppression is enabled, forwards first join for a new group or first join following a general query for an existing group. • If report suppression is disabled, forwards on all mrouter ports.
IGMPv3 reports	Ignores	Ignores
IGMPv2 leaves	Invokes last member query processing.	Invokes last member query processing.

Table 2: Multicast Traffic Handling for an IGMPv3 Querier

Traffic Type	Received on MRouter Ports	Received on Host Ports
IP multicast source traffic	Forwards to all mrouter ports and to host ports that indicate interest.	Forwards to all mrouter ports and to host ports that indicate interest.
IGMP general queries	Forwards to all ports.	—
IGMP group-specific queries	If received on the querier port floods on all ports.	—
IGMPv2 joins	Handles as IGMPv3 IS_EX{} reports.	Handles as IGMPv3 IS_EX{} reports.
IGMPv3 reports	• If proxy reporting is enabled—For state changes or source-list changes, generates a state change report on all mrouter ports. • If proxy reporting is disabled—Forwards on all mrouter ports.	• If proxy reporting is enabled—For state changes or source-list changes, generates a state change report on all mrouter ports. • If proxy reporting is disabled—Forwards on all mrouter ports.
IGMPv2 leaves	Handles as IGMPv3 IS_IN{} reports.	Handles as IGMPv3 IS_IN{} reports.

Multichassis Link Aggregation

The Multichassis Link Aggregation (MC-LAG) feature provides a simple redundancy mechanism for the Digital Subscriber Line Access Multiplexer (DSLAM) to access Cisco ASR 9000 Series Routers. The redundancy is achieved by allowing a dual-homed connection to two or more Cisco ASR 9000 Series Routers.

The DSLAM is known as a Dual-Homed Device (DHD) and the Cisco ASR 9000 Series Router is known as a Point of Attachment (PoA). An MC-LAG is assigned into a Redundancy Group (RG). The Cisco ASR 9000 Series Routers (PoAs) that manage a given MC-LAG are members of this RG. There may be multiple MC-LAGs in the RG. This indicates that the same RG may cover MC-LAG connections to other DSLAMs. Hence, the RG is uniquely identified on the PoAs by an Redundancy Group Identifier (RGID). The MC-LAG is identified

on each PoA by a unique Redundancy Object Identifier, also termed as ROID. If VLAN sub-interfaces are configured on the MC-LAG, then each VLAN sub-interface has a unique ROID.

IGMP Snooping on the Cisco ASR 9000 Series Router supports MC-LAG configurations looking either downstream towards a DSLAM or upstream towards a multicast router.

Note Both the active and standby POAs must have the same configuration for the MC-LAG feature to work.

For more information on configuring link bundling and protocols used, see the Configuring Link Bundling chapter in Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

Bidirectional Internet Group Management Protocol Snoop Synchronization for Satellite Dual-Homed System

In a dual-homed nV Satellite system, the satellites can align to either of the two satellite hosts acting as a Unicast Active Host. So, each host contains a partially-built IGMP snooping protocol table, based on the joins received from the satellite access ports aligned to that specific host. The Unicast Standby Host does not have the same IGMP snooping information.

In the case of a switchover, where the satellites may have to realign to the other host, the Internet Group Management Protocol (IGMP) snooping protocol has to rebuild the protocol tables again, increasing the overall convergence times. This can be improved by synchronizing the IGMP snoop protocol table states across both hosts so that the switchover is faster. Also, in the case of the nV multicast offload feature, both hosts form an active-active system by forwarding a copy of every offloaded flow from either ends of a ring topology. This requires that the replication list per Route (S, G) be same on both hosts via synchronization for faster convergence and independent choice of designated multicast forwarder from unicast active host.

With Bidirectional IGMP Snoop Synchronization feature, the Cisco ASR 9000 Series Router (Satellite Host) acting as Unicast Active host for a given satellite port, processes IGMP messages snooped on that satellite-ether port and distributes state changes to the unicast standby host in a dual-homed system. The standby host is responsible for accepting IGMP state changes from ICCP and updating the local IGMP snooping protocol states so that they are in synchronization with the unicast active host.

The ICCP Client library provides the IGMP snoop application with an interface to the ICCP functionality and also enables the IGMP snoop application between the participating hosts on the same redundancy group to communicate and synchronize using the ICCP protocol.

The IGMP snoop synchronization functionality is available for all the supported satellite hardware types in 5.2.2 release. This is also a prerequisite for faster convergence times in the case of nV multicast offload feature, which is also introduced in 5.2.2 . For more information on nV Multicast Offload feature, see *Cisco ASR 9000 Series Aggregation Services Router nV System Configuration Guide.*

Note IGMP Snoop Synchronization is not supported in the cases, where hosts are of different endian types in dual-homed system topology.

Restrictions

The following are the restrictions of the Bidirectional IGMP Snoop Synchronization feature on Satellite Dual-Homed Systems feature:

- Synchronization is not supported on ASR9K chassis running RSP cards of different endian types.
- IGMP synchronization over BVI requires that the BVI must have a lower IP address than the internal-querier, and the bridge domain is configured with an internal querier with the lowest possible query max response time, that is, "query-max-response-time 1."
- Ambiguous VLAN ports are not supported with IGMP snoop synchronization functionality.
- The IGMP snoop configuration has to be manually synchronized on both the hosts for the synchronization functionality to work as expected on the nV Satellite dual-homed systems.

IGMP Snooping Configuration Profiles

To enable IGMP snooping on a bridge domain, you must attach a profile to the bridge domain. The minimum configuration is an empty profile if BVI is configured. An empty profile enables the default configuration options and settings for IGMP snooping, as listed in the Default IGMP Snooping Configuration Settings, on page 11.

Note The **internal-querier** is a requirement under the IGMP snooping profile if BVI is not configured under L2VPN.

Configuration Example:

```
igmp snooping profile igmpsn
 internal-querier
!
```

You can attach IGMP snooping profiles to bridge domains or to ports under a bridge domain. The following guidelines explain the relationships between profiles attached to ports and bridge domains:

- Any IGMP Snooping profile attached to a bridge domain, even an empty profile, enables IGMP snooping. To disable IGMP snooping, detach the profile from the bridge domain.
- An empty profile configures IGMP snooping on the bridge domain and all ports under the bridge using default configuration settings.
- A bridge domain can have only one IGMP snooping profile attached to it (at the bridge domain level) at any time.
- Port profiles are not in effect if the bridge domain does not have a profile attached to it.
- IGMP snooping must be enabled on the bridge domain for any port-specific configurations to be in effect.
- If a profile attached to a bridge domain contains port-specific configuration options, the values apply to all of the ports under the bridge, including all mrouter and host ports, unless another port-specific profile is attached to a port.
- When a profile is attached to a port, IGMP snooping reconfigures that port, disregarding any port configurations that may exist in the bridge-level profile.

Creating Profiles

To create a profile, use the **igmp snooping profile** command in global configuration mode.

Attaching and Detaching Profiles

To attach a profile to a bridge domain, use the **igmp snooping profile** command in l2vpn bridge group bridge domain configuration mode. To attach a profile to a port, use the **igmp snooping profile** command in the interface configuration mode under the bridge domain. To detach a profile, use the **no** form of the command in the appropriate configuration mode.

When you detach a profile from a bridge domain or a port, the profile still exists and is available for use at a later time. Detaching a profile has the following results:

- If you detach a profile from a bridge domain, IGMP snooping is deactivated in the bridge domain.
- If you detach a profile from a port, IGMP snooping configuration values for the port are instantiated from the bridge domain profile.

Changing Profiles

You cannot make changes to an active profile. An active profile is one that is currently attached.

- If the active profile is configured under the bridge, you must detach it from the bridge, and reattach it.
- If the active profile is configured under a specific bridge port, you must detach it from the bridge port, and reattach it.

Another way to do this is to create a new profile incorporating the desired changes and attach it to the bridges or ports, replacing the existing profile. This deactivates IGMP snooping and then reactivates it with parameters from the new profile.

Configuring Access Control

Access control configuration is the configuration of access groups and weighted group limits.

The role of access groups in IGMP v2/v3 message filteringis to permit or deny host membership requests for multicast groups (*,G) and multicast source groups (S,G). This is required to provide blocked-and-allowed list access to IPTV channel packages.

Weighted group limits restrict the number of IGMP v2/v3 groups, in which the maximum number of concurrently allowed multicast channels can be configured on a per EFP- and per PW-basis.

IGMP Snooping Access Groups

Although Layer-3 IGMP routing also uses the **igmp access-group** command in support of access groups, the support is not the same in Layer-2 IGMP, because the Layer-3 IGMP routing access group feature does not support source groups.

Access groups are specified using an extended IP access list referenced in an IGMP snooping profile that you attach to a bridge domain or a port.

Note A port-level access group overrides any bridge domain-level access group.

The **access-group** command instructs IGMP snooping to apply the specified access list filter to received membership reports. By default, no access list is applied.

Changes made to the access-list referenced in the profile (or a replacement of the access-list referenced in the igmp snooping profile) will immediately result in filtering the incoming igmp group reports and the existing group states accordingly, without the need for a detach-reattach of the igmp snooping profile in the bridge-domain, each time such a change is made.

IGMP Snooping Group Weighting

To limit the number of IGMP v2/v3 groups, in which the maximum number of concurrently allowed multicast channels must be configurable on a per EFP-basis and per PW-basis, configure group weighting.

IGMP snooping limits the membership on a bridge port to a configured maximum, but extends the feature to support IGMPv3 source groups and to allow different weights to be assigned to individual groups or source groups. This enables the IPTV provider, for example, to associate standard and high- definition IPTV streams, as appropriate, to specific subscribers.

This feature does not limit the actual multicast bandwidth that may be transmitted on a port. Rather, it limits the number of IGMP groups and source-groups, of which a port can be a member. It is the responsibility of the IPTV operator to configure subscriber membership requests to the appropriate multicast flows.

The **group policy** command, which is under igmp-snooping-profile configuration mode, instructs IGMP snooping to use the specified route policy to determine the weight contributed by a new <*,G> or <S,G> membership request. The default behavior is for there to be no group weight configured.

The **group limit** command specifies the group limit of the port. No new group or source group is accepted if its contributed weight would cause this limit to be exceeded. If a group limit is configured (without group policy configuration), a <S/*,G> group state will have a default weight of 1 attributed to it.

Note By default, each group or source-group contributes a weight of 1 towards the group limit. Different weights can be assigned to groups or source groups using the group policy command.

The group limit policy configuration is based on these conditions:

- Group weight values for <*,G> and <S,G> membership are configured in a Route Policy, that is included in an igmp snooping profile attached to a BD or port.
- Port level weight policy overrides any bridge domain level policy, if group-limit is set and route-policy is configured.
- If there is no policy configured, each group weight is counted equally and is equal to 1.
- If policy has been configured, all matching groups get weight of 1 and un-matched groups have 0 weight.

Default IGMP Snooping Configuration Settings

Table 3: IGMP Snooping Default Configuration Values

Scope	Feature	Default Value
Bridge Domain	IGMP snooping	Disabled on a bridge domain until an enabling IGMP snooping profile is attached to the bridge domain.
	internal querier	By default Internal Querier is disabled. To enable Internal Querier, add it to the IGMP snooping profile. Internal Querier is not recommended, when BVI and IGMP snooping is configured under a bridge.
	last-member-query-count	2
	last-member-query-interval	1000 (milliseconds)
	minimum-version	2 (supporting IGMPv2 and IGMPv3)
	querier query-interval	60 (seconds) **Note** This is a nonstandard default value.
	report-suppression	Enabled (enables report suppression for IGMPv2 and proxy-reporting for IGMPv3)
	querier robustness-variable	2
	router alert check	Enabled
	tcn query solicit	Disabled
	tcn flood	Enabled
	ttl-check	Enabled
	unsolicited-report-timer	1000 (milliseconds)
Port	immediate-leave	Disabled
	mrouter	No static mrouters configured; dynamic discovery occurs by default.
	router guard	Disabled
	static group	None configured

IGMP Snooping Configuration at the Bridge Domain Level

IGMP Minimum Version

The **minimum-version** command determines which IGMP versions are supported by IGMP snooping in the bridge domain:

- When minimum-version is 2, IGMP snooping intercepts IGMPv2 and IGMPv3 messages. This is the default value.
- When minimum-version is 3, IGMP snooping intercepts only IGMPv3 messages and drops all IGMPv2 messages.

IGMPv1 is not supported. The scope for this command is the bridge domain. The command is ignored in a profile attached to a port.

System IP Address

The **system-ip-address** command configures an IP address for IGMP snooping use. If not explicitly configured, the default address is 0.0.0.0. The default is adequate except in the following circumstances:

- If you are configuring an internal querier. The internal querier cannot use 0.0.0.0.
- If the bridge needs to communicate with an IGMP router that does not accept the 0.0.0.0 address.

The IGMP snooping system IP address is used in the following ways:

- The internal-querier sends queries from the system IP address. An address other than the default 0.0.0.0 must be configured.
- IGMPv3 sends proxy reports from the systemIP address. The default address 0.0.0.0 is preferred but may not be acceptable to some IGMP routers.
- In response to topology change notifications (TCNs) in the bridge domain, IGMP snooping sends global-leaves from the system IP address. The default address 0.0.0.0 is preferred but may not be acceptable to some IGMP routers.

Group Membership Interval, Robustness Variable, and Query Interval

The group membership interval (GMI) controls when IGMP snooping expires stale group membership states. The **show igmp snooping group** command shows groups with an expiry time of 0 until that stale state is cleaned up following the next query interval.

The GMI is calculated as:

GMI = (robustness-variable * query-interval) + maximum-response-time

where:

- maximum-response-time (MRT) is the amount of time during which receivers are required to report their membership state.
- robustness-variable is an integer used to influence the calculated GMI.
- query-interval is the amount of time between general queries.

Values for the components in the GMI are obtained as follows:

- MRT is advertised in the general query, for both IGMPv2 and IGMPv3.
- If the querier is running IGMPv2, IGMP snooping uses the IGMP-snooping-configured values for the robustness-variable and query-interval. These parameter values must match the configured values for the querier. In most cases, if you are interacting with other Cisco routers, you should not need to explicitly configure these values—the default values for IGMP snooping should match the default values of the

querier. If they do not, use the **querier robustness-variable** and **querier query-interval** commands to configure matching values.

- IGMPv3 general queries convey values for robustness-variable and query-interval (QRV and QQI, respectively). IGMP snooping uses the values from the query, making the IGMP snooping GMI exactly match that of the querier.

Report Suppression (IGMPv2) and Proxy Reporting (IGMPv3)

The following IGMP snooping features reduce multicast traffic in a bridge domain. Both are enabled by default.

- IGMPv2 report suppression—If the bridge domain querier is running IGMPv2, IGMP snooping suppresses joins from a host if it has already forwarded the same join from another host during the current query interval. IGMP snooping forwards the last leave message to all mrouter ports.

  As insurance against lost reports when report suppression is enabled, IGMP snooping forwards IGMPv2 join reports the configured querier robustness-variable times for new groups. Configure the querier robustness-variable using the **querier robustness-variable** command.

- IGMPv3 proxy reporting—If the bridge domain querier is running IGMPv3, IGMP snooping acts as a proxy, generating reports from the proxy reporting address. Configure the proxy reporting address using the **system-ip-address** command. The default value is 0.0.0.0.

  As insurance against lost reports when proxy reporting is enabled, IGMP snooping generates and forwards state change reports robustness-variable times, where the robustness-variable is the QRV value in the querier's general query. The reports are forwarded at random intervals within the timeframe configured with the **unsolicited-report-timer** command.

To disable report suppression and proxy reporting, use the **report-suppression disable** command.

The scope for the commands mentioned in this section is the bridge domain. The commands are ignored in a profile attached to a port.

Group Leave Processing

Group Leave Options

When hosts want to leave a multicast group, they can either ignore the periodic general IGMP queries (called a silent leave), or they can send a group-specific leave message.

IGMP snooping can respond to group leaves in the following ways:

- Last member query processing—This is the default method for processing group leaves.
- Immediate leave—You can optionally configure individual ports for immediate leave.

Note IGMPv3 explicit host tracking, which provides per host immediate leave functionality on a multi-host LAN, is not supported.

Last Member Query Processing for IGMPv2 and IGMPv3

Last member query is the default group leave processing method used by IGMP snooping. With last member query processing, IGMP snooping processes leave messages as follows:

- IGMP snooping sends group-specific queries on the port that receives the leave message to determine if any other devices connected to that interface are interested in traffic for the specified multicast group. Using the following two configuration commands, you can control the latency between the request for a leave and the actual leave:
  - **last-member-query-count** command—Controls the number of group-specific queries IGMP snooping sends in response to a leave message.
  - **last-member-query-interval** command—Controls the amount of time between group-specific queries.
- If IGMP snooping does not receive an IGMP join message in response to group-specific queries, it assumes that no other devices connected to the port are interested in receiving traffic for this multicast group, and it removes the port from its Layer-2 forwarding table entry for that multicast group.
- If the leave message was from the only remaining port, IGMP snooping removes the group entry and generates an IGMP leave to the multicast routers.

Immediate-Leave Configuration

Immediate-leave is an optional port-level configuration parameter. Immediate-leave processing causes IGMP snooping to remove a Layer-2 interface from the forwarding table entry immediately, without first sending IGMP group-specific queries to the interface. After receiving an IGMP leave message, IGMP snooping immediately removes the interface from the Layer-2 forwarding table entry for that multicast group, unless a multicast router was learned on the port.

Immediate-leave processing improves leave latency, but is appropriate only when one receiver is configured on a port. For example, immediate-leave is appropriate in the following situations:

- Point-to-point configurations, such as an IPTV channel receiver
- Downstream DSLAMs with proxy reporting

Do not use immediate-leave on a port when the possibility exists for more than one receiver per port. Doing so could prevent an interested receiver from receiving traffic. For example, immediate-leave is not appropriate in a LAN.

Immediate-leave processing is a port-level option. You can configure this option explicitly per port in port profiles or in the bridge domain profile, in which case, it applies to all ports under the bridge.

Reaction to Topology Change Notifications

In a Spanning Tree Protocol (STP) topology, a Topology Change Notification (TCN) indicates that an STP topology change has occurred. As a result of a topology change, mrouters and hosts reporting group membership may migrate to other STP ports under the bridge domain. Mrouter and membership states must be relearned after a TCN.

IGMP snooping reacts to TCNs in the following ways:

1. IGMP snooping temporarily extends the flood set for all known multicast routes to include all ports participating in STP that are in forwarding state. The short-term flooding ensures that multicast delivery

continues to all mrouters and all member hosts in the bridge domain while mrouter and membership states are relearned.

But, as a result of this TCN flooding, downstream STP links may sometimes become over-subscribed by these extra multicast flows. This feature can in such cases be disabled by use of the **tcn flood disable** command.

2. The STP root bridge issues a global leave (for group 0.0.0.0) on all ports. This action triggers interoperable IGMP queriers to send general queries, expediting the relearning process.

Note Sending global leaves for query solicitation is a Cisco-specific implementation.

3. When the TCN refresh period ends, IGMP snooping withdraws the non-mrouter and non-member STP ports from the multicast route flood sets. You can control the amount of time that flooding occurs with the **tcn flood query count** command. This command sets the number of IGMP general queries for which the multicast traffic is flooded following a TCN, thereby influencing the refresh period.

IGMP snooping default behavior is that the STP root bridge always issues a global leave in response to a TCN, and that the non-root bridges do not issue global leaves.

With the **tcn query solicit** command, you can enable a bridge to always issue a global leave in response to TCNs, even when it is not the root bridge. In that case, the root bridge and the non-root bridge would issue the global leave and both would solicit general queries in response to a TCN. Use the **no** form of the command to turn off soliciting when the bridge is not the root.

Note One use for the **tcn query solicit** command is when Reverse Layer 2 Gateway Protocol (RL2GP) is configured to set up a MSTP Access Gateway. In this scenario, IGMP snooping is unaware of the root or non-root status of the bridge and, therefore, when a TCN occurs, no query is solicited in the domain unless IGMP snooping is explicity configured to do so on at least one bridge.

The root bridge always issues a global leave in response to a TCN. This behavior can not be disabled.

The internal querier has its own set of configuration options that control its reactions to TCNs.

The scope for all tcn related configuration option(s) is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

IGMP Snooping Packet Checks

By default, IGMP snooping performs the following validations. If your network performs these validations elsewhere, you can disable the IGMP snooping validations.

- IGMP snooping checks the time-to-live (TTL) field in the IGMP header and drops packets where TTL is not equal to 1. The TTL field should always be set to 1 in the headers of IGMP reports and queries.

  You can disable this check using the **ttl-check disable** command, in which case IGMP snooping processes all packets without examining the TTL field in the IGMP header.

- IGMP snooping checks for the presence of the router alert option in the IP packet header of the IGMP message and drops packets that do not include this option.

You can disable this check using the **router-alert-check disable** command, in which case IGMP snooping does not perform the validation before processing the message.

Startup Query Configuration

The startup query feature is configured using new igmp snooping profile parameters. You can configure the startup query processing in response to the following events:

- MC-LAG Port goes active
- Topology-change
- Port-up
- Process start

The above parameters are specific to MC-LAG feature. These are apart from the existing bridge domain level parameters such as count, MRT, and query interval. For more information about these CLI, refer the *Multicast Command Reference for Cisco ASR 9000 Series Routers*.

Note

- For IGMP snooping to work on MC-LAG properly, the IGMP snooping configuration on both the POAs must be the same.
- In the case of downstream MC-LAG, when MC-LAG is configured and up and running, the MC-LAG port has to be added in IGMP Snooping enabled Bridge-domain.
- In the case of upstream MC-LAG, where POAs are attached to multicast router, the static mrouter port has to be configured on the multicast router that is towards both the POAs so that traffic is drawn to both the POAs.

IGMP Snooping Configuration at the Host Port Level

Router Guard and Static Mrouter

Router guard is a security feature that prevents malicious users from making a host port into an mrouter port. (This undesirable behavior is known as spoofing.) When a port is protected with the **router-guard** command, it cannot be dynamically discovered as an mrouter. When router guard is on a port, IGMP snooping filters protocol packets sent to the port and discards any that are multicast router control packets.

The **mrouter** command configures a port as a static mrouter.

You can use the **router-guard** and the **mrouter** commands on the same port to configure a guarded port as a static mrouter, for example, when:

- A large number of downstream host ports are present and you want to block dynamic mrouter discovery and configure static mrouters. In this case, configure the router guard feature at the domain level. By default, it will be applied to all ports, including the typically large number of downstream host ports. Then, use another profile without router guard configured for the relatively few upstream ports on which you want to permit dynamic mrouter discovery or configure static mrouters.
- Incompatibilities with non-Cisco equipment prevents correct dynamic discovery, you can disable all attempts for dynamic discovery using the router guard feature, and statically configure the mrouter.

If you are using the router guard feature, because there is an incompatible IGMP router on the port, you should also configure the **mrouter** command on the port to ensure that the router receives IGMP reports and multicast flows.

Immediate-Leave

See the Group Leave Processing, on page 13.

Static Groups

IGMP snooping learns Layer-2 multicast groups dynamically. You can also statically configure Layer-2 multicast groups.

You can use the **static group** command in profiles intended for bridge domains or ports. I f you configure this option in a profile attached to a bridge domain, it applies to all ports under the bridge.

A profile can contain multiple static groups. You can define different source addresses for the same group address. Using the **source** keyword, you can configure IGMPv3 source groups.

Static group membership supersedes any dynamic manipulation by IGMP snooping. Multicast group membership lists can contain both static and dynamic group definitions.

When you configure a static group or source groups on a port, IGMP snooping adds the port as an outgoing port to the corresponding <S/*,G> forwarding entry and sends an IGMPv2 join or IGMPv3 report to all mrouter ports. IGMP snooping continues to send the membership report in response to general queries for as long as the static group remains configured on the port.

Internal Querier

When to Use an Internal Querier

In a network where IP multicast routing is configured, the IP multicast router acts as the IGMP querier. In situations when no external querier exists in the bridge domain (because the multicast traffic does not need to be routed), but local multicast sources exist, you must configure an internal querier to implement IGMP snooping. The internal querier solicits membership reports from hosts in the bridge domain so that IGMP snooping can build constrained multicast forwarding tables for the multicast traffic within the bridge domain.

An internal querier might also be useful when interoperability issues with non-Cisco equipment prevent IGMP snooping from working correctly with an external querier. In this case, you can:

1. Prevent the uncooperative external querier from being discovered by placing the **router-guard** command on that port.
2. Configure an internal querier to learn group membership interests from the ports in the bridge domain.
3. Configure static mrouter ports to receive multicast traffic.

Internal Querier Default Configuration

The minimum configuration for an internal querier is:

- Add the **internal-querier** command to a profile attached to the bridge domain. The default configuration is shown in Table 4: Internal Querier Default Configuration Values, on page 18.

- Add the **system-ip-address** command to a profile attached to the bridge domain to configure an address other than the default 0.0.0.0.

Table 4: Internal Querier Default Configuration Values

Configuration Command	Default Value
system-ip-address	0.0.0.0. The default address is invalid for the internal-querier.
internal-querier *max-response-time*	10
internal-querier *query-interval*	60 (seconds) **Note** This is a nonstandard default value.
internal-querier *robustness-variable*	2
internal-querier tcn query *count*	2
internal-querier tcn query *interval*	10 (seconds)
internal-querier timer *expiry* **Note** This is the Other Querier Present Interval as defined in RFC-3376, Section 8.5.	125 (seconds): robustness-variable * query-interval + ½(max-response-time) For example, using the default values for all components: (2 * 60) + ½ (10) = 125
internal-querier *version*	3

You can disable the internal querier (using the **no** form of the **internal-querier** command) without removing any other internal querier commands. The additional internal querier commands are ignored in that case.

The scope for the **internal-querier** command is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

Internal Querier Processing

When the internal querier is the elected querier in the domain, it solicits membership reports by sending IGMP general queries at the interval specified by the **internal-querier query-interval** command on every active port in the bridge domain. The internal querier sends IGMPv3 queries by default. You can configure it to send IGMPv2 messages instead using the **internal-querier version** command.

The local IGMP snooping process responds to the internal querier's general queries. In particular, the IGMPv3 proxy (if enabled) generates a current-state report and forwards it to all mrouters. For IGMPv2 or when the IGMPv3 proxy is disabled, IGMP snooping generates current-state reports for static group state only.

The queries are sent from the address you configure for IGMP snooping using the **system-ip-address** command. The queries include the maximum response time configured with the **internal-querier max-response-time** command.

The **internal-querier robustness-variable** and **internal-querier query-interval** commands configure values for both IGMPv2 and IGMPv3 processing.

Querier Election for One Active Querier

A bridge domain can have only one active querier at a time. If the internal-querier receives queries from another querier in a bridge domain, it performs querier election. The lowest IP address wins. If the internal querier is the election loser, IGMP snooping starts a timer with the value set by the **internal-querier timer expiry** command. If this timer expires before another query is received from the election winner, the internal querier becomes the active querier.

Note The default **internal-querier timer expiry** command value is derived from the values of other configuration options, as described in Table 4: Internal Querier Default Configuration Values, on page 18. You can configure a different value to override the default calculation.

Internal Querier Reaction to TCNs

IGMP snooping generates group leaves in response to topology change notifications. For more information about how IGMP snooping reacts to TCNs, see the Reaction to Topology Change Notifications, on page 14.

If the internal querier receives a group leave while it is the elected querier in the domain, it reacts as follows:

- Generates an IGMP general query immediately.
- Waits the amount of time set by the **internal-querier tcn query interval** command and generates another IGMP general query.
- Continues to wait for the specified interval time and to send general queries until the query count reaches the value set with the **internal querier tcn query count** command.

Note You can configure the internal querier to ignore global leaves by setting the internal querier TCN query count to 0.

Multicast over Integrated Routing Bridging

Multicast over integrated routing bridging active or active multihome feature enables the routers to quickly and safely switch traffic between routers, during failure, without any traffic loss.

During the software upgrade to Cisco IOS XR Release 7.3.2, the BGP session flaps due to the change in the field in the NLRI key. This behavior occurs when you configure EVPN multihoming with the multicast feature. To avoid BGP flapping, you must concurrently upgrade all the nodes to Cisco IOS XR Release 7.3.2.

This feature comprises of the following four sub features that work together as a solution:

- First, IGMPv2 snooping is enabled for the peer routers to know which Layer 2 interface has receiver interested in a particular group.
- After snooping, this information is synced to the peer routers with the Layer 2 EVPN sync feature.

- After both peer routers are synced, they act like a last hop router and send PIM join upstream.
- Once the traffic arrives on both the peer routers, only one peer router forwards the traffic to the receiver with the designated forwarder election feature.

Configuration Example

To configure multicast over integrated routing bridging, you must complete the following configurations:

- Layer 2 Base Configuration
- EVPN Configuration
- IGMPv2 Snoop Configurations

Configurations performed on peer 1:

```
/*1. Layer 2 Base Configuration*\
hostname peer1
!
interface Bundle-Ether2
!
interface Bundle-Ether2.2 l2transport
 encapsulation dot1q 2
 rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/0
 bundle id 2 mode on
 no shutdown
!

/*2. EVPN Configuration*\

hostname peer1
!
router bgp 100
 bgp router-id 10.99.1.1
 bgp graceful-restart
 address-family l2vpn evpn
 !
 neighbor 3.3.3.3
  remote-as 100
  update-source Loopback0
  address-family l2vpn evpn
  !
 !
!
evpn
 evi 2
  advertise-mac
  !
 !
 interface Bundle-Ether2
  ethernet-segment
   identifier type 0 02.02.02.02.02.02.02.02.02
   bgp route-target 0002.0002.0002
  !
 !
!

/*3. IGMPv2 Snoop Configurations*\
```

```
hostname peer1
!
router igmp

  version 2
 !
!
l2vpn
 bridge group VLAN2
  bridge-domain VLAN2
   igmp snooping profile 1
   interface Bundle-Ether2.2
   !

   evi 2
   !
  !
 !
igmp snooping profile 1
!
```

Configurations performed on peer 2:

```
/*1. Layer 2 Base Configuration*\

hostname peer2
!
interface Bundle-Ether2
!
interface Bundle-Ether2.2 l2transport
 encapsulation dot1q 2
 rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/0
 bundle id 2 mode on
 no shut
!
/*2. EVPN Configuration*\

hostname peer2
!
router bgp 100
 bgp router-id 2.2.2.2
 bgp graceful-restart
 address-family l2vpn evpn
 !
 neighbor 3.3.3.3
  remote-as 100
  update-source Loopback0
  address-family l2vpn evpn
  !
 !
!
evpn
 evi 2
  advertise-mac
  !
 !
 interface Bundle-Ether2
  ethernet-segment
   identifier type 0 02.02.02.02.02.02.02.02.02
   bgp route-target 0002.0002.0002
  !
 !
```

```
!
/*3. IGMPv2 Snoop Configurations*\

hostname peer2
!
router igmp

  version 2
 !
!
l2vpn
 bridge group VLAN2
  bridge-domain VLAN2
   igmp snooping profile 1
   interface Bundle-Ether2.2
   !

   evi 2
   !
  !
 !
igmp snooping profile 1
!
```

How to Configure IGMP Snooping

The first two tasks are required to configure basic IGMP snooping configuration.

Creating an IGMP Snooping Profile

SUMMARY STEPS

1. **configure**
2. **igmp snooping profile** *profile-name*
3. Optionally, add commands to override default configuration values.
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**igmp snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config)# igmp snooping profile default-bd-profile`	Enters IGMP snooping profile configuration mode and creates a named profile. The default profile enables IGMP snooping. You can commit the new profile without any additional configurations, or you can include additional configuration options to the profile. You can also return to the profile later to add configurations, as described in other tasks in this module.

	Command or Action	Purpose
Step 3	Optionally, add commands to override default configuration values.	If you are creating a bridge domain profile, consider the following: • An empty profile is appropriate for attaching to a bridge domain. An empty profile enables IGMP snooping with default configuration values. • You can optionally add more commands to the profile to override default configuration values. • If you include port-specific configurations in a bridge domain profile, the configurations apply to all ports under the bridge, unless another profile is attached to a port. If you are creating a port-specific profile, consider the following: • While an empty profile could be attached to a port, it would have no effect on the port configuration. • When you attach a profile to a port, IGMP snooping reconfigures that port, overriding any inheritance of configuration values from the bridge-domain profile. You must repeat the commands in the port profile if you want to retain those configurations. You can detach a profile, change it, and reattach it to add commands to a profile at a later time.
Step 4	**commit**	

Where to Go Next

You must attach a profile to a bridge domain or to a port to have it take effect. See one of the following tasks:

Attaching a Profile and Activating IGMP Snooping on a Bridge Domain

To activate IGMP snooping on a bridge domain, attach an IGMP snooping profile to the bridge domain, as described in the following steps.

SUMMARY STEPS

1. **configure**
2. **l2vpn**
3. **bridge group** *bridge-group-name*
4. **bridge-domain** *bridge-domain-name*
5. **multicast-source ipv4**
6. **igmp snooping profile** *profile-name*
7. **commit**

8. **show igmp snooping bridge-domain detail**
9. **show l2vpn bridge-domain detail**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**l2vpn** **Example:** `RP/0/RSP0/CPU0:router(config)# l2vpn`	Enters Layer 2 VPN configuration mode.
Step 3	**bridge group** *bridge-group-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1`	Enters Layer 2 VPN VPLS bridge group configuration mode for the named bridge group.
Step 4	**bridge-domain** *bridge-domain-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1`	Enters Layer 2 VPN VPLS bridge group bridge domain configuration mode for the named bridge domain.
Step 5	**multicast-source ipv4** **Example:** `RP/0/RSP0/CPU0:router(config)# multicast-source ipv4`	Configures Layer 2 multicast routes with IGMP snooping.
Step 6	**igmp snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# igmp snooping profile default-bd-profile`	Attaches the named IGMP snooping profile to the bridge domain, enabling IGMP snooping on the bridge domain.
Step 7	**commit**	
Step 8	**show igmp snooping bridge-domain detail** **Example:** `RP/0/RSP0/CPU0:router# show igmp snooping`	(Optional) Verifies that IGMP snooping is enabled on a bridge domain and shows the IGMP snooping profile names attached to bridge domains and ports.

	Command or Action	Purpose
	`bridge-domain detail`	
Step 9	**show l2vpn bridge-domain detail** **Example:** `RP/0/RSP0/CPU0:router# show l2vpn bridge-domain`	(Optional) Verifies that IGMP snooping is implemented in the forwarding plane (Layer 2) on a bridge domain.

Detaching a Profile and Deactivating IGMP Snooping on a Bridge Domain

To deactivate IGMP snooping on a bridge domain, remove the profile from the bridge domain using the following steps.

Note A bridge domain can have only one profile attached to it at a time.

SUMMARY STEPS

1. **configure**
2. **l2vpn**
3. **bridge group** *bridge-group-name*
4. **bridge-domain** *bridge-domain-name*
5. **no igmp snooping disable**
6. **commit**
7. **show igmp snooping bridge-domain detail**
8. **show l2vpn bridge-domain detail**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**l2vpn** **Example:** `RP/0/RSP0/CPU0:router(config)# l2vpn`	Enters Layer 2 VPN configuration mode.
Step 3	**bridge group** *bridge-group-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group`	Enters Layer 2 VPN VPLS bridge group configuration mode for the named bridge group.

	Command or Action	Purpose
	GRP1	
Step 4	**bridge-domain** *bridge-domain-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1`	Enters Layer 2 VPN VPLS bridge group bridge domain configuration mode for the named bridge domain.
Step 5	**no igmp snooping disable** **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# no igmp snooping disable`	Detaches the IGMP snooping profile from the bridge domain, disabling IGMP snooping on that bridge domain. **Note** Only one profile can be attached to a bridge domain at a time. If a profile is attached, IGMP snooping is enabled. If a profile is not attached, IGMP snooping is disabled.
Step 6	**commit**	
Step 7	**show igmp snooping bridge-domain detail** **Example:** `RP/0/RSP0/CPU0:router# show igmp snooping bridge-domain detail`	(Optional) Verifies that IGMP snooping is disabled on a bridge domain.
Step 8	**show l2vpn bridge-domain detail** **Example:** `RP/0/RSP0/CPU0:router# show l2vpn bridge-domain`	(Optional) Verifies that IGMP snooping is disabled in the forwarding plane (Layer 2) on a bridge domain.

Attaching and Detaching Profiles to Ports Under a Bridge

Before you begin

IGMP snooping must be enabled on the bridge domain for port-specific profiles to affect IGMP snooping behavior.

SUMMARY STEPS

1. **configure**
2. **l2vpn**
3. **bridge group** *bridge-group-name*
4. **bridge-domain** *bridge-domain-name*
5. **interface** *interface-type interface-number*
6. **multicast-source ipv4**
7. Do one of the following:

- **igmp snooping profile** *profile-name*
- **no igmp snooping**

8. **commit**
9. **show igmp snooping bridge-domain detail**
10. **show l2vpn bridge-domain detail**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**l2vpn** **Example:** `RP/0/RSP0/CPU0:router(config)# l2vpn`	Enters Layer 2 VPN configuration mode.
Step 3	**bridge group** *bridge-group-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1`	Enters Layer 2 VPN bridge group configuration mode for the named bridge group.
Step 4	**bridge-domain** *bridge-domain-name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1`	Enters Layer 2 VPN bridge group bridge domain configuration mode for the named bridge domain.
Step 5	**interface** *interface-type interface-number* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface gig 1/1/1/1`	Enters Layer 2 VPN VPLS bridge group bridge domain interface configuration mode for the named interface or PW.
Step 6	**multicast-source ipv4** **Example:** `RP/0/RSP0/CPU0:router(config)# multicast-source ipv4`	Configures L2 multicast routes in L2 multicast with IGMP Snooping.
Step 7	Do one of the following: • **igmp snooping profile** *profile-name*	Attaches the named IGMP snooping profile to the port. **Note**

	Command or Action	Purpose
	• **no igmp snooping** **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-if)# igmp snooping profile mrouter-port-profile`	A profile on a port has no effect unless there is also a profile attached to the bridge. The **no** form of the command detaches a profile from the port. Only one profile can be attached to a port.
Step 8	**commit**	
Step 9	**show igmp snooping bridge-domain detail** **Example:** `RP/0/RSP0/CPU0:router# show igmp snooping bridge-domain detail`	(Optional) Verifies that IGMP snooping is enabled on a bridge domain and shows the IGMP snooping profile names attached to bridge domains and ports.
Step 10	**show l2vpn bridge-domain detail** **Example:** `RP/0/RSP0/CPU0:router# show l2vpn bridge-domain`	(Optional) Verifies that IGMP snooping is implemented in the forwarding plane (Layer 2) on a bridge domain.

Adding Static Mrouter Configuration to a Profile

Before you begin

IGMP snooping must be enabled on the bridge domain for port-specific profiles to affect IGMP snooping behavior.

Note Static mrouter port configuration is a port-level option and should be added to profiles intended for ports. It is not recommended to add mrouter port configuration to a profile intended for bridge domains.

SUMMARY STEPS

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **mrouter**
4. **commit**
5. **show igmp snooping profile** *profile-name* **detail**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**igmp snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config)# igmp snooping profile mrouter-port-profile`	Enters IGMP snooping profile configuration mode and creates a new profile or accesses an existing profile.
Step 3	**mrouter** **Example:** `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# mrouter`	Configures a port as a static mrouter port.
Step 4	**commit**	
Step 5	**show igmp snooping profile** *profile-name* **detail** **Example:** `RP/0/RSP0/CPU0:router# show igmp snooping profile mrouter-port-profile detail`	(Optional) Displays the configuration settings in the named profile.

Where to Go Next

Attach the profile to ports to complete static mrouter configuration. See the Attaching and Detaching Profiles to Ports Under a Bridge, on page 26.

Adding Router Guard to a Profile

To prevent multicast routing protocol messages from being received on a port and, therefore, prevent a port from being a dynamic mrouter port, follow these steps. Note that both router guard and static mrouter commands may be configured on the same port. See the Router Guard and Static Mrouter, on page 16 for information.

Before you begin

IGMP snooping must be enabled on the bridge domain for port-specific profiles to affect IGMP snooping behavior.

Note Router guard configuration is a port-level option and should be added to profiles intended for ports. It is not recommended to add router guard configuration to a profile intended for bridge domains. To do so would prevent all mrouters, including IGMP queriers, from being discovered in the bridge domain.

SUMMARY STEPS

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **router-guard**
4. **commit**
5. **show igmp snooping profile** *profile-name* **detail**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**igmp snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config)# igmp snooping profile host-port-profile`	Enters IGMP snooping profile configuration mode and creates a new profile or accesses an existing profile.
Step 3	**router-guard** **Example:** `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# router-guard`	Protects the port from dynamic discovery.
Step 4	**commit**	
Step 5	**show igmp snooping profile** *profile-name* **detail** **Example:** `RP/0/RSP0/CPU0:router# show igmp snooping profile host-port-profile detail`	(Optional) Displays the configuration settings in the named profile.

Where to Go Next

Attach the profile to ports to complete router guard configuration. See the Attaching and Detaching Profiles to Ports Under a Bridge, on page 26.

Configuring Immediate-Leave

To add the IGMP snooping immediate-leave option to an IGMP snooping profile, follow these steps.

Before you begin

IGMP snooping must be enabled on the bridge domain for port-specific profiles to affect IGMP snooping behavior.

SUMMARY STEPS

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **immediate-leave**
4. **commit**
5. **show igmp snooping profile** *profile-name* **detail**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**igmp snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config)# igmp snooping profile host-port-profile`	Enters IGMP snooping profile configuration mode and creates a new profile or accesses an existing profile.
Step 3	**immediate-leave** **Example:** `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# immediate-leave`	Enables the immediate-leave option. • If you add this option to a profile attached to a bridge domain, it applies to all ports under the bridge. • If you add this option to a profile attached to a port, it applies to the port.
Step 4	**commit**	
Step 5	**show igmp snooping profile** *profile-name* **detail** **Example:** `RP/0/RSP0/CPU0:router# show igmp snooping profile host-port-profile detail`	(Optional) Displays the configuration settings in the named profile.

Where to Go Next

Attach the profile to bridge domains or ports to complete immediate-leave configuration. See one of the following sections:

Configuring Static Groups

To add one or more static groups or IGMPv3 source groups to an IGMP snooping profile, follow these steps.

Before you begin

IGMP snooping must be enabled on the bridge domain for port-specific profiles to affect IGMP snooping behavior.

SUMMARY STEPS

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **static-group** *group-addr* [**source** *source-addr*]
4. Repeat the previous step, as needed, to add more static groups.
5. **commit**
6. **show igmp snooping profile** *profile-name* **detail**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**igmp snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config)# igmp snooping profile host-port-profile`	Enters IGMP snooping profile configuration mode and creates a new profile or accesses an existing profile.
Step 3	**static-group** *group-addr* [**source** *source-addr*] **Example:** `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# static-group 239.1.1.1 source 10.0.1.1`	Configures a static group. • If you add this option to a profile attached to a bridge domain, it applies to all ports under the bridge. • If you add this option to a profile attached to a port, it applies to the port.
Step 4	Repeat the previous step, as needed, to add more static groups.	(Optional) Adds additional static groups.
Step 5	**commit**	
Step 6	**show igmp snooping profile** *profile-name* **detail** **Example:** `RP/0/RSP0/CPU0:router# show igmp snooping profile host-port-profile detail`	(Optional) Displays the configuration settings in the named profile.

Where to Go Next

Attach the profile to bridge domains or ports to complete static-group configuration. See one of the following sections:

Configuring an Internal Querier

Before you begin

IGMP snooping must be enabled on the bridge domain for this procedure to take effect.

SUMMARY STEPS

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **system-ip-address** *ip-addr*
4. **internal-querier**
5. **commit**
6. **show igmp snooping profile** *profile-name* **detail**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**igmp snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config)# igmp snooping profile internal-querier-profile`	Enters IGMP snooping profile configuration mode and creates a new profile or accesses an existing profile.
Step 3	**system-ip-address** *ip-addr* **Example:** `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# system-ip-address 10.1.1.1`	Configures an IP address for internal querier use. The default system-ip-address value (0.0.0.0) is not valid for the internal querier. You must explicitly configure an IP address.
Step 4	**internal-querier** **Example:** `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# internal-querier`	Enables an internal querier with default values for all options.
Step 5	**commit**	

	Command or Action	Purpose
Step 6	**show igmp snooping profile** *profile-name* **detail** **Example:** `RP/0/RSP0/CPU0:router# show igmp snooping profile internal-querier-profile detail`	(Optional) Displays the configuration settings in the named profile.

Where to Go Next

Attach the profile to a bridge domain to complete internal querier configuration.

See Attaching a Profile and Activating IGMP Snooping on a Bridge Domain, on page 23.

Verifying Multicast Forwarding

SUMMARY STEPS

1. **configure**
2. **show l2vpn forwarding bridge-domain** [*bridge-group-name*:*bridge-domain-name*] **mroute ipv4** [**group** *group_IPaddress*] [**hardware** {**ingress** | **egress**}] [**detail**]**location** *node-id*
3. **show l2vpn forwarding bridge-domain** [*bridge-group-name*:*bridge-domain-name*] **mroute ipv4 summary location** *node-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**show l2vpn forwarding bridge-domain** [*bridge-group-name*:*bridge-domain-name*] **mroute ipv4** [**group** *group_IPaddress*] [**hardware** {**ingress**	**egress**}] [**detail**]**location** *node-id* **Example:** `RP/0/RSP0/CPU0:routershow l2vpn forwarding bridge-domain bg1:bd1 mroute ipv4 group 234.192.4.1 hardware ingress detail location 0/1/cPU0`	Displays multicast routes as they are converted into the forwarding plane forwarding tables. Use optional arguments to limit the display to specific bridge groups or bridge domains. If these routes are not as expected, check the control plane configuration and correct the corresponding IGMP snooping profiles.
Step 3	**show l2vpn forwarding bridge-domain** [*bridge-group-name*:*bridge-domain-name*] **mroute ipv4 summary location** *node-id* **Example:** `RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain bg1:bd1 mroute ipv4 summary location`	Displays summary-level information about multicast routes as stored in the forwarding plane forwarding tables. Use optional arguments to limit the display to specific bridge domains.

	Command or Action	Purpose
	0/3/CPU0	

Configuring Group Limits

This procedure consists the following tasks:

Configuring route-policy

SUMMARY STEPS

1. **configure**
2. **route-policy** *policy-name*
3. **end-policy**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**route-policy** *policy-name* **Example:** `RP/0/RSP0/CPU0:router(config)# route-policy sky`	Configures route policy with the defined name.
Step 3	**end-policy** **Example:** `RP/0/RSP0/CPU0:router(config-rpl)# end-policy`	Ends the route-policy configuration.
Step 4	**commit**	

Configuring group limit

SUMMARY STEPS

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **group policy** *policy-name*
4. **group limit** *range*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**igmp snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config)# igmp snooping profile name1`	Enters IGMP snooping profile configuration mode and creates a new profile or accesses an existing profile.
Step 3	**group policy** *policy-name* **Example:** `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# group policy policy1`	Specifies the configured route-policy to set the group weight.
Step 4	**group limit** *range* **Example:** `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# group limit 100`	Limits the number of groups (or source-groups) allowed on a port.
Step 5	**commit**	

Configuring access-groups

This task instructs IGMP Snoop to apply the specified access-list filter(s) to receive membership reports.

The user needs to create and configure access-lists before configuring the access-groups. For detailed configuration procedures, for creating and configuring standard and extended access-lists, refer to the Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide.

SUMMARY STEPS

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **access-group** *acl-name*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**igmp snooping profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config)# igmp snooping profile name1`	Enters IGMP snooping profile configuration mode and creates a new profile or accesses an existing profile.
Step 3	**access-group** *acl-name* **Example:** `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# access-group acl1`	Configures group membership filter(s).
Step 4	**commit**	

Configuration Examples for IGMP Snooping

The following examples show how to enable IGMP snooping on Layer 2 VPLS bridge domains on Cisco ASR 9000 Series Routers:

Configuring IGMP Snooping on Physical Interfaces Under a Bridge: Example

1. Create two profiles.

```
igmp snooping profile bridge_profile
!
igmp snooping profile port_profile
   mrouter
!
```

2. Configure two physical interfaces for L2 transport.

```
interface GigabitEthernet0/8/0/38
   negotiation auto
   l2transport
   no shut
   !
!
interface GigabitEthernet0/8/0/39
   negotiation auto
   l2transport
   no shut
```

```
   !
!
```

3. Add interfaces to the bridge domain. Attach bridge_profile to the bridge domain and port_profile to one of the Ethernet interfaces. The second Ethernet interface inherits IGMP snooping configuration attributes from the bridge domain profile.

```
l2vpn
  bridge group bg1
     bridge-domain bd1
     igmp snooping profile bridge_profile
     interface GigabitEthernet0/8/0/38
       igmp snooping profile port_profile
     interface GigabitEthernet0/8/0/39

!
  !
!
```

4. Verify the configured bridge ports.

```
show igmp snooping port
```

Configuring IGMP Snooping on VLAN Interfaces Under a Bridge: Example

1. Configure two profiles.

```
multicast-source ipv4
igmp snooping profile bridge_profile

igmp snooping profile port_profile
   mrouter
!
```

2. Configure VLAN interfaces for L2 transport.

```
interface GigabitEthernet0/8/0/8
   negotiation auto
   no shut
   !
!
interface GigabitEthernet0/8/0/8.1 l2transport
   encapsulation dot1q 1001
   rewrite ingress tag pop 1 symmetric
   !
!
interface GigabitEthernet0/8/0/8.2 l2transport
   encapsulation dot1q 1002
   rewrite ingress tag pop 1 symmetric
   !
!
```

3. Attach a profile and add interfaces to the bridge domain. Attach a profile to one of the interfaces. The other interface inherits IGMP snooping configuration attributes from the bridge domain profile.

```
l2vpn
  bridge group bg1
     bridge-domain bd1
     multicast-source ipv4
     igmp snooping profile bridge_profile
     interface GigabitEthernet0/8/0/8.1
       igmp snooping profile port_profile
     interface GigabitEthernet0/8/0/8.2

     !
  !
!
```

4. Verify the configured bridge ports.

```
show igmp snooping port
```

Configuring IGMP Snooping on Ethernet Bundles Under a Bridge: Example

1. This example assumes that the front-ends of the bundles are preconfigured. For example, a bundle configuration might consist of three switch interfaces, as follows:

```
    interface Port-channel1Bundle-Ether121
    !
interface GigabitEthernet0/0/0/0
    !
interface GigabitEthernet0/0/0/1
!
    interface GigabitEthernet0/0/0/2
       channel-group 1 mode on
    !
    interface GigabitEthernet0/0/0/3
       channel-group 1 mode on
    !
```

2. Configure two IGMP snooping profiles.

```
multicast-source ipv4
       igmp snooping profile bridge_profile
       !
       multicast-source ipv4
       igmp snooping profile port_profile
          mrouter
       !
```

3. Configure interfaces as bundle member links.

```
       interface GigabitEthernet0/0/0/0
         bundle id 1 mode on
         negotiation auto
       !
       interface GigabitEthernet0/0/0/1
         bundle id 1 mode on
         negotiation auto
       !
```

```
interface GigabitEthernet0/0/0/2
  bundle id 2 mode on
  negotiation auto
!
interface GigabitEthernet0/0/0/3
  bundle id 2 mode on
  negotiation auto
!
```

4. Configure the bundle interfaces for L2 transport.

```
interface Bundle-Ether 1
          l2transport
          !
       !
       interface Bundle-Ether 2
          l2transport
          !
       !
```

5. Add the interfaces to the bridge domain and attach IGMP snooping profiles.

```
l2vpn
  bridge group bg1
     bridge-domain bd1
     multicast-source ipv4
     igmp snooping profile bridge_profile
     interface bundle-Ether 1
       multicast-source ipv4
       igmp snooping profile port_profile
     interface bundle-Ether 2

     !
   !
!
```

6. Verify the configured bridge ports.

```
show igmp snooping port
```

Configuring IGMP Snooping on VFIs Under a Bridge: Example

This example configures IGMP snooping on a virtual forwarding instance (VFI) under a bridge domain. The topology consists of two routers, PE1 and PE2, each with an access circuit (AC) and pseudowire (PW) as bridge ports.

PE1 Configuration

1. Configure IGMP snooping profiles.

```
igmp snooping profile prof1
!
igmp snooping profile prof2
```

```
    mrouter
!
```

2. Configure interfaces.

```
interface Loopback0
  ipv4 address 10.1.1.1 255.255.255.255
!
interface GigabitEthernet0/2/0/9
   ipv4 address 10.10.10.1 255.255.255.0
   negotiation auto
!
interface GigabitEthernet0/2/0/39
   negotiation auto
   l2transport
!
```

3. Configure Open Shortest Path First (OSPF).

```
router ospf 1
  log adjacency changes
  router-id 10.1.1.1
  area 0
    interface Loopback0
    !
    interface GigabitEthernet0/2/0/9
    !
  !
!
```

4. Configure Label Distribution Protocol (LDP).

```
mpls ldp
   router-id 10.1.1.1
   log neighbor
   !
   interface GigabitEthernet0/2/0/9
   !
!
```

5. Configure a bridge domain, enable IGMP snooping on the bridge, and add the interfaces to the bridge domain.

```
    l2vpn
      pw-class atom-dyn
      encapsulation mpls
         protocol ldp
      !
    !

    bridge group bg1
        bridge-domain bd1
        igmp snooping profile prof1
        interface GigabitEthernet0/2/0/39
           igmp snooping profile prof2
        vfi mplscore
           neighbor 10.2.2.2 pw-id 101
```

```
            pw-class atom-dyn
            !
          !
        !
      !
```

6. Verify the configured bridge ports.

```
show igmp snooping port
```

PE2 Configuration

1. Configure the IGMP profiles.

```
igmp snooping profile bridge_profile
!
igmp snooping profile port_profile
   mrouter
!
```

2. Configure interfaces.

```
interface Loopback0
  ipv4 address 10.2.2.2 255.255.255.255
!
interface GigabitEthernet0/2/0/9
   ipv4 address 10.10.10.1 255.255.255.0
   negotiation auto
!
interface GigabitEthernet0/2/0/39
   negotiation auto
   l2transport
!
```

3. Configure OSPF.

```
router ospf 1
  log adjacency changes
  router-id 10.2.2.2
  area 0
    interface Loopback0
    !
    interface GigabitEthernet0/2/0/9
    !
  !
!
```

4. Configure LDP.

```
mpls ldp
   router-id 10.2.2.2
   log neighbor
   !
   interface GigabitEthernet0/2/0/9
   !
```

```
    !
```

5. Add interfaces to the bridge domain and attach IGMP snooping profiles.

```
l2vpn
   pw-class atom-dyn
   encapsulation mpls
      protocol ldp
   !
 !

 bridge group bg1
     bridge-domain bd1
     igmp snooping profile bridge_profile
     interface GigabitEthernet0/2/0/39
        igmp snooping profile port_profile
     vfi mplscore
        neighbor 10.1.1.1 pw-id 101
        pw-class atom-dyn
        !
     !
   !
 !
```

6. Verify the configured bridge ports.

```
show igmp snooping port
```

Configuring IGMP access-groups

In the example below, a list is configured and attached to an L2VPN bridge port that allows user membership of <*,G> groups 225.0.0.0/24 and 228.0.0.0/24, only. A second access-list is defined that permits <S,G> membership. This access-list is attached to a bridge-port.

```
interface gig 0/2/0/1.1 l2transport
...
!
ipv4 access-list iptv-basic-white-list
 10 permit ipv4 any 225.0.0.0/24
 20 permit ipv4 any 228.0.0.0/24
!
ipv4 access-list iptv-premium-white-list
 10 permit ipv4 192.168.0.1 232.0.1.0/24
 20 permit ipv4 192.168.0.1 232.0.2.0/24
!
igmp snooping profile iptv
 access-group iptv-white-list
!
igmp snooping profile iptv2
 access-group iptv-premium-white-list
!
l2vpn
 bridge group vz
bridge domain vz-iptv
 igmp snooping profile iptv
 interface gig 0/2/0/1.1
```

```
 interface gig 0/2/0/1.2
  igmp snooping profile iptv2
 interface gig 0/2/0/1.3
 ...
!
```

IGMP routing also supports access-groups using the igmp **access-group** command. It uses simple IP access-groups to specify group address filters. In order to support source-group filters as well as group filters, IGMP Snooping requires extended IP access-lists.

Note Access-groups are not applied to static groups and source-groups.

Configuring IGMP Snooping over MCLAG: Example

Case 1: Downstream MCLAG

Topology : DHD connected to 2 POAs which in turn is connected to PE.

DHD:

1. Configure a bundle towards POA1 and POA2. This device will be masked from the existence of 2 POAs. The bundle considers that it is connected to a single POA.

```
interface Bundle-Ether10
 description interface towards POAs
 lacp switchover suppress-flaps 100
 bundle maximum-active links 1
l2transport
 !

!

interface GigabitEthernet0/0/0/28
 description interface towards POA1
 bundle id 10 mode active
!

interface GigabitEthernet0/0/0/29
 description interface towards POA2
 bundle id 10 mode active
!
```

2. Joins coming to this must be forwarded to POAs over bundle. So, configuring the incoming port (host port) and bundle in L2VPN BD (without snooping).

```
RP/0/RSP0/CPU0:router:DHD# show running-config l2vpn

l2vpn
 bridge group bg1
  bridge-domain bg1_bd1
   interface Bundle-Ether10
   !
interface GigabitEthernet0/0/0/10
```

```
   !

  !

 !

!
```

POA1:

1. Configure interfaces (for OSPF and MPLS LDP)

```
interface Loopback0

ipv4 address 20.20.20.20 255.255.255.255

!

interface GigabitEthernet0/2/0/1
description interface towards POA2
ipv4 address 10.0.0.1 255.255.255.0

 negotiation auto

!

interface GigabitEthernet0/2/0/8

 description interface towards PE

 ipv4 address 10.0.1.1 255.255.255.0

 negotiation auto

!
```

2. Configure OSPF and MPLS LDP:

```
router ospf 1
router-id 20.20.20.20
nsf cisco
area 0
interface Loopback0

  !
interface GigabitEthernet0/2/0/1
  !
interface GigabitEthernet0/2/0/8

  !

 !

!
mpls ldp
router-id 20.20.20.20
graceful-restart
interface GigabitEthernet0/2/0/1
 !
interface GigabitEthernet0/2/0/8
```

```
 !

!
```

3. Configure an MCLAG bundle towards DHD:

```
interface Bundle-Ether10
description interface towards DHD
lacp switchover suppress-flaps 100
mlacp iccp-group 1
mlacp switchover recovery-delay 60
mlacp port-priority 1
mac-address 0.aaaa.1111
bundle wait-while 0
l2transport

 !

!
interface GigabitEthernet0/2/0/29
bundle id 10 mode active
!
```

4. Configure redundancy group for MCLAG:

```
redundancy

 iccp
group 1
mlacp node 1
mlacp system mac 0000.aaaa.0000
mlacp system priority 1
member
neighbor 30.30.30.30
!
backbone
interface GigabitEthernet0/2/0/8
  !

  !

 !

!
```

5. Configure IGMP Snooping profile:

```
igmp snooping profile p1
ttl-check disable
router-alert-check disable

!
```

6. Enable IGMP Snooping in the L2VPN BD which includes MCLAG bundle towards DHD and PW towards PE:

```
l2vpn
```

```
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface Bundle-Ether10
!
vfi bg1_bd1_vfi
neighbor 40.40.40.40 pw-id 1

    !

   !

  !

 !

!
```

POA2:

1. Configure interfaces (for OSPF and MPLS LDP)

```
interface Loopback0

ipv4 address 30.30.30.30 255.255.255.255
!
interface GigabitEthernet0/0/0/1
description interface towards POA1
ipv4 address 10.0.0.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/8
description interface towards PE
ipv4 address 10.0.2.1 255.255.255.0
negotiation auto
!
```

2. Configure OSPF and MPLS LDP:

```
router ospf 1
router-id 30.30.30.30
nsf cisco
area 0
interface Loopback0
!
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/8
!
!

!
mpls ldp
router-id 30.30.30.30
graceful-restart
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/8

 !
```

```
!
```

3. Configure an MCLAG bundle towards DHD:

```
interface Bundle-Ether10
description interface towards DHD
lacp switchover suppress-flaps 100
mlacp iccp-group 1
mlacp switchover recovery-delay 60
mlacp port-priority 2
mac-address 0.aaaa.1111
bundle wait-while 0
l2transport

 !

!
interface GigabitEthernet0/0/0/28
bundle id 10 mode active

!
```

4. Configure redundancy group for MCLAG:

```
redundancy
iccp
group 1
mlacp node 2
mlacp system mac 0000.aaaa.0000
mlacp system priority 1
member
neighbor 20.20.20.20
!
backbone
interface GigabitEthernet0/0/0/8
   !
  !
 !
!
```

5. Configure IGMP Snooping profile:

```
igmp snooping profile p1
ttl-check disable
router-alert-check disable
!
```

6. Enable IGMP Snooping in the L2VPN BD which includes MCLAG bundle towards DHD and PW towards PE:

```
l2vpn
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface Bundle-Ether10
!
```

```
vfi bg1_bd1_vfi
neighbor 40.40.40.40 pw-id 1

    !

   !

  !

 !

!
```

PE:

1. Configure Interfaces :

```
interface Loopback0
ipv4 address 40.40.40.40 255.255.255.255
!
interface GigabitEthernet0/0/0/8
description interface towards POA1
ipv4 address 10.0.1.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/9
description interface towards POA2
ipv4 address 10.0.2.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/20
description interface towards Multicast Router
l2transport
!
!
```

2. Configure OSPF and MPLS LDP:

```
router ospf 1
router-id 40.40.40.40
nsf cisco
area 0
interface Loopback0
!
interface GigabitEthernet0/0/0/8
!
interface GigabitEthernet0/0/0/9
!
!
!
mpls ldp
router-id 40.40.40.40
graceful-restart

interface GigabitEthernet0/0/0/8
!
interface GigabitEthernet0/0/0/9
!
!
```

3. Configure IGMP Snooping profile:

```
igmp snooping profile p1
ttl-check disable
router-alert-check disable
!
```

4. Enable IGMP Snooping in the L2VPN BD which includes PWs towards both the POAs and a port towards Multicast Router:

```
l2vpn
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface GigabitEthernet0/0/0/20
!
vfi bg1_bd1_vfi
neighbor 20.20.20.20 pw-id 1
!
neighbor 30.30.30.30 pw-id 1
!
!
!
```

Case 2 : Upstream MCLAG

Topology: The multicast router is connected to 2 POAs and which is in turn connected to PE multicast Router.

1. Configure bundle towards POAs.

```
interface Bundle-Ether10
description interface towards POAs
ipv4 address 100.0.0.1 255.255.255.0
lacp switchover suppress-flaps 100
bundle maximum-active links 1
!
interface GigabitEthernet0/0/0/28
description interface towards POA1
bundle id 10 mode active
!
interface GigabitEthernet0/0/0/29
description interface towards POA2
bundle id 10 mode active
!
```

2. Enable multicast routing on the bundle interface:

```
multicast-routing
address-family ipv4
interface Bundle-Ether10
enable
!
!
!
```

POA1:

1. Configure interfaces (for OSPF and MPLS LDP).

```
interface Loopback0
ipv4 address 20.20.20.20 255.255.255.255
!
interface GigabitEthernet0/2/0/1
description interface towards POA2
ipv4 address 10.0.0.1 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/2/0/8
description interface towards PE
ipv4 address 10.0.1.1 255.255.255.0
negotiation auto
!
```

2. Configure OSPF and MPLS LDP:

```
router ospf 1
router-id 20.20.20.20
nsf cisco
area 0
interface Loopback0
!
interface GigabitEthernet0/2/0/1
!
interface GigabitEthernet0/2/0/8
!
!
!
mpls ldp
router-id 20.20.20.20
graceful-restart
interface GigabitEthernet0/2/0/1
!
interface GigabitEthernet0/2/0/8
!
!
```

3. Configure an MCLAG bundle towards DHD:

```
interface Bundle-Ether10
description interface towards DHD
lacp switchover suppress-flaps 100
mlacp iccp-group 1
mlacp switchover recovery-delay 60
mlacp port-priority 1
mac-address 0.aaaa.1111
bundle wait-while 0
l2transport
!
!
interface GigabitEthernet0/2/0/29
bundle id 10 mode active
!
```

4. Configure redundancy group for MCLAG:

```
redundancy
iccp
group 1
mlacp node 1
mlacp system mac 0000.aaaa.0000
mlacp system priority 1
member
neighbor 30.30.30.30
!
backbone
interface GigabitEthernet0/2/0/8
!
!
!
!
```

5. Configure IGMP Snooping profile:

```
igmp snooping profile p1
ttl-check disable
router-alert-check disable
!
```

6. Enable IGMP Snooping in the L2VPN BD which includes MCLAG bundle towards DHD and PW towards PE:

```
l2vpn
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface Bundle-Ether10
!
vfi bg1_bd1_vfi
neighbor 40.40.40.40 pw-id 1
!
!
!
!
!
```

POA2:

1. Configure interfaces (for OSPF and MPLS LDP).

```
interface Loopback0
ipv4 address 30.30.30.30 255.255.255.255
!
interface GigabitEthernet0/0/0/1
description interface towards POA1
ipv4 address 10.0.0.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/8
description interface towards PE
ipv4 address 10.0.2.1 255.255.255.0
negotiation auto
!
```

2. Configure OSPF and MPLS LDP:

```
router ospf 1
router-id 30.30.30.30
nsf cisco
area 0
interface Loopback0
!
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/8
!
!
!
mpls ldp
router-id 30.30.30.30
graceful-restart
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/8
!
!
```

3. Configure an MCLAG bundle towards DHD:

```
interface Bundle-Ether10
description interface towards DHD
lacp switchover suppress-flaps 100
mlacp iccp-group 1
mlacp switchover recovery-delay 60
mlacp port-priority 2
mac-address 0.aaaa.1111
bundle wait-while 0
l2transport
!
!
interface GigabitEthernet0/0/0/28
bundle id 10 mode active
!
```

4. Configure redundancy group for MCLAG:

```
redundancy
iccp
group 1
mlacp node 2
mlacp system mac 0000.aaaa.0000
mlacp system priority 1
member
neighbor 20.20.20.20
!
backbone
interface GigabitEthernet0/0/0/8
!
!
!
```

5. Configure IGMP Snooping profile:

```
igmp snooping profile p1
ttl-check disable
router-alert-check disable
!
```

6. Enable IGMP Snooping in the L2VPN BD which includes MCLAG bundle towards DHD and PW towards PE:

```
l2vpn
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface Bundle-Ether10
!
vfi bg1_bd1_vfi
neighbor 40.40.40.40 pw-id 1
!
!
!
!
```

PE:

1. Configure interfaces:

```
interface Loopback0
ipv4 address 40.40.40.40 255.255.255.255
!
interface GigabitEthernet0/0/0/8
description interface towards POA1
ipv4 address 10.0.1.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/9
description interface towards POA2
ipv4 address 10.0.2.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/20
description interface towards Host
l2transport
!
!
```

2. Configure OSPF and MPLS LDP:

```
router ospf 1
router-id 40.40.40.40
nsf cisco
area 0
interface Loopback0
!
interface GigabitEthernet0/0/0/8
!
interface GigabitEthernet0/0/0/9
!
!
!
```

```
mpls ldp
router-id 40.40.40.40
graceful-restart
interface GigabitEthernet0/0/0/8
!
interface GigabitEthernet0/0/0/9
!
!
```

3. Configure IGMP Snooping profile:

```
igmp snooping profile p1
ttl-check disable
router-alert-check disable
!
igmp snooping profile p2
mrouter
!
```

4. Enable IGMP Snooping in the L2VPN BD which includes PWs towards both the POAs and a port towards the Host. Configure static mrouter port on the PWs towards both the POAs.

```
l2vpn
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface GigabitEthernet0/0/0/20
!
vfi bg1_bd1_vfi
neighbor 20.20.20.20 pw-id 1
igmp snooping profile p2
!
neighbor 30.30.30.30 pw-id 1
igmp snooping profile p2
!
!
!
!
```

Additional References

Related Documents

Related Topic	Document Title
Configuring MPLS VPLS bridges	Implementing Virtual Private LAN Services on Cisco IOS XR Software module in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*
Getting started information	*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*
Configuring EFPs and EFP bundles	*Interface and Hardware Component Configuration Guide for Cisco ASR 9000 Series Routers*

Standards

Standards[1]	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

[1] Not all supported standards are listed.

MIBs

MIBs	MIBs Link
No MIBs support IGMP snooping.	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
RFC-4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

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