



Implementing Layer 2 Multicast

- [Implementing IGMP Snooping, on page 1](#)
- [Prerequisites for IGMP Snooping, on page 1](#)
- [Supported Features and Restrictions for IGMP Snooping, on page 1](#)
- [Information About IGMP Snooping, on page 3](#)
- [EVPN All-Active Multi-homed Multicast Source Behind a BVI, on page 9](#)
- [How to Configure IGMP Snooping, on page 13](#)
- [Configuration Examples for IGMP Snooping, on page 20](#)
- [Additional References, on page 27](#)

Implementing 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.



Note Multicast traffic without Spanning-Tree protocol is supported at Layer 2 for multicast traffic without snooping enabled.

Prerequisites for IGMP Snooping

Before implementing IGMP snooping, make sure that the network is configured with a Layer 2 VPN (L2VPN).

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.

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 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.

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.
- 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 NCS 5500 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 **multicast-source ipv4** under L2VPN if snooping is enabled and multicast traffic source is located behind the AC port.

Configuration Example:

```
Router(config)# l2vpn
Router(config-l2vpn)# bridge group 1
Router(config-l2vpn-bg)#bridge-domain 1
Router(config-l2vpn-bg-bd)#multicast-source ipv4
Router(config-l2vpn-bg-bd)#efp-visibility
Router(config-l2vpn-bg-bd)#igmp snooping profile igmpsn
Router(config-l2vpn-bg-bd)#exit
Router(config-l2vpn-bg-bd)#interface TenGigE0/0/0/3.31
Router(config-l2vpn-bg-bd-ac)#exit
Router(config-l2vpn-bg-bd)#interface TenGigE0/0/0/3.32
Router(config-l2vpn-bg-bd-ac)#exit
Router(config-l2vpn-bg-bd)#routed interface BVI1
Router(config-l2vpn-bg-bd-bvi)#exit
```

Multicast Router Port

A Multicast router (Mrouter) port is a port that connects to a Multicast router. The device includes the Multicast router port(s) numbers when it forwards the Multicast streams and IGMP registration messages. This is required so that the Multicast routers can, in turn, forward the Multicast streams and propagate the registration messages to other subnets. The reports would be re-injected over mrouter ports.

Multicast Host Ports

IGMP snooping classifies each port (for example, EFPs, physical ports, or EFP bundles) as a host ports, that is, any port that is not an mrouter port is a host port.

Multicast Traffic Handling within a Bridge Domain with IGMP Snooping Enabled

The following tables describe traffic handling behaviors by IGMP snooping 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 5](#) 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 Host Ports
IP multicast source traffic	Forwards to all mrouter ports and to host ports that indicate interest.
IGMP general queries	—
IGMP group-specific queries	Dropped
IGMPv2 joins	Examines (snoops) the reports. <ul style="list-style-type: none"> • 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
IGMPv2 leaves	Invokes last member query processing.

Table 2: Multicast Traffic Handling for an IGMPv3 Querier

Traffic Type	Received on Host Ports
IP multicast source traffic	Forwards to all mrouter ports and to host ports that indicate interest.
IGMP general queries	—
IGMP group-specific queries	—
IGMPv2 joins	Handles as IGMPv3 IS_EX{} reports.
IGMPv3 reports	<ul style="list-style-type: none"> • 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.

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 7](#).



Note You must configure the **system-ip-address** and **internal-querier** when the BVI is not configured, and no other queriers are present in the same domain.

Configuration Example:

```
Router(config)#igmp snooping profile igmpsn
Router(config-igmp-snooping-profile)#system-ip-address 192.0.2.1
Router(config-igmp-snooping-profile)#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.

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)

Scope	Feature	Default Value
Port	immediate-leave	Disabled
	mrouter	No static mrouter 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.

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:

$$\text{GMI} = (\text{robustness-variable} * \text{query-interval}) + \text{maximum-response-time}$$

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.

EVPN All-Active Multi-homed Multicast Source Behind a BVI

EVPN AA multi-homed refers to a specific deployment model within the EVPN technology. In the multi-homed setup, a customer site or device (CE) is connected to multiple provider edge (PE) routers or attachment circuits (ACs). Multi-homing provides redundancy and load balancing by allowing a CE to connect to multiple PE routers, enabling traffic to be distributed across different paths. In case of a link (CE to PE and local PE to remote PE) or router failure, traffic can be quickly redirected to an alternate path.

In multi-homing, an AA mode means that all the links or paths between the EVPN sites are active and forwarding traffic simultaneously. This is in contrast to other deployment models, such as Single-Active or Port-Active Load-balancing mode, where only a subset of the links is active at any given time.

Placing the CE device behind the BVI interface has the following advantages:

- It allows for a simplified configuration on the CE side. The CE only needs to be configured with a single default gateway, which is the BVI interface. The CE doesn't have to manage multiple interfaces or deal with complex routing protocols.
- The BVI interface also enables efficient replication and forwarding of multicast traffic to the appropriate multicast distribution trees within the service provider network. This eliminates the need for the CE to handle multicast replication, reducing its processing load and potentially improving overall multicast performance.
- Placing the CE behind the BVI accept interface allows for greater flexibility in multi-homing scenarios. The CE can connect to multiple provider edge (PE) routers through the BVI accept interface, enabling seamless failover and load balancing between the PE routers during link or router failures.

Prerequisites

The network must support the following topology, protocols, and features to use the EVPN AA multi-homed multicast source feature:

- EVPN Control Plane with BGP
- BVI
- IGMP Snooping and MLD Snooping
- MLDP, MPLS, and OSPF (for L3 multicast receivers at core)
- Native multicast, MVPN GRE, or mVPN Profile 14 (core)

For more information related to EVPN technology and supported protocols, refer *EVPN Features* chapter in *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers*.

For more information related to IGMP Snooping and MLD Snooping features, refer *Implementing Layer 2 Multicast* chapter in *Multicast Configuration Guide for Cisco NCS 5500 Series Routers*.

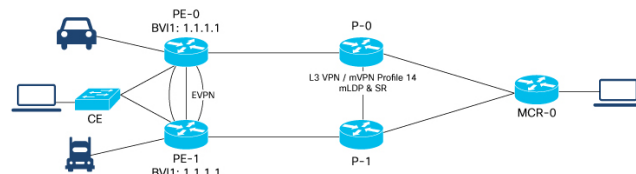
The EVPN AA multi-homed multicast source feature enables multicast data packet support for multi-homed sources in an EVPN AA (All-Active) topology.

In this setup, the multicast traffic is forwarded to the core by EVPN with BVI as the accept interface.

This deployment model combines the benefits of AA forwarding and multi-homing. It's particularly useful in scenarios where high availability, fault tolerance, and optimized bandwidth utilization are essential requirements.

The following illustration shows the multicast data traffic route between a multi-homed source and the multi-homed receivers.

Figure 1: EVPN All-Active Multi-homed Multicast Source behind a BVI Topology



In this illustration, the multicast data sources are connected behind a CE, which is multi-homed to PE-0 and PE-1. PE-1 is configured with a BVI that has an anycast IP address. The image displays an example where the BVI has the IP address 1.1.1.1. The receiver that is behind the MCR-0 has a PIM connection toward the multicast data source.

The data packet flow between the multicast data source and receiver occurs in the following manner:

1. The receiver, located behind Multicast Receiver (MCR-0), initiates an Internet Group Management Protocol (IGMP) join, which triggers a Protocol Independent Multicast (PIM) join towards the source.
2. The PIM join message reaches one of the PE routers (either PE-0 or PE-1) with the incoming or accept interface being the BVI and the outgoing interface leading towards the core network.
3. When the source sends traffic, it reaches one of the PE routers (PE-0 or PE-1). The next path for the traffic depends on the following IGMP snooping configurations:
 - If IGMP snooping is enabled and the multicast source is configured for both IPv4 and IPv6 traffic, the traffic is forwarded to either a route with a BVI interface or the default IGMP snooping route.
 - If IGMP snooping is disabled, the traffic floods the multicast ID (MCID) on the bridge. As part of the flood MCID logic, the packet is recycled for the BVI and flooded to all the ACs, including the EVPN Optimized Local Egress (OLE). The recycled packets for the BVI undergo Layer 3 lookup. If there is a route with the BVI as an accepted interface, the packet is forwarded to the Olist for Layer 3 forwarding.



Note The same packet is not sent back to the CE device due to SHL (Split Horizon Label) filtering for EVPN traffic.

Usage Guidelines and Limitations

The supported scenarios for AA MH multicast are as follows:

- IPv4 SSM with BVI as accept interface is supported.
- IPv4 SM with BVI as accept interface is supported.
- IPv6 SSM with BVI as accept interface is supported.

- IPv4 SSM without BVI (only layer 2 multicast) and multicast source behind L2 is supported.
- IPv4 SM without BVI as accept interface (only layer 2 multicast) is supported.
- IPv6 SSM without BVI as accept interface (only layer 2 multicast) is supported.
- IPv6 SM without BVI as accept interface (only layer 2 multicast) is supported.

This feature has the following limitations:

- IPv6 SM with BVI as accept interface is not supported.
- Dual-homed source and Dual-homed receiver over MLDP profile on the same BD is not supported. It is recommended to disable MVPN peering between the MH nodes to prevent redundant traffic path formation in the core.
- Layer 2 IPv6 traffic is only supported on NCS 5700 fixed port routers and NCS 5500 modular routers (NCS 5700 line cards [Mode: Native]).
- In an EVPN dual-home AA scenario:
 - If the multicast source and receiver are in the same BD, the receiver might receive permanent traffic duplication.
 - Transient traffic duplication might occur when the DH node role changes between DF and nDF.
 - In a BD, the following EVPN configuration is not supported:
 - Multicast source—ESI1=BE-X.A
 - Multicast receiver—ESI1=BE-X.B



Note

ESI is the Ethernet Segment identifier, whereas X.A and X.B represents two AC ports for the bundle interface BE.

- In a BD, the following EVPN configuration is not supported:
 - Multicast source—ESI1=BE-X.A (NCS 5700 line cards)
 - Multicast receiver—ESI1=BE-Y.A (NCS 5500 line cards)



Note

ESI is the Ethernet Segment identifier, whereas X.A and Y.A represents two AC ports for the bundle interface BE.

Configure EVPN All-Active Multi-homed Multicast Source with a BVI Interface

To configure an EVPN All-Active Multi-homed multicast source with a BVI interface, use the following example configuration:

```
Router#configure
Router(config)#l2vpn
```

```

Router(config-l2vpn)#bridge group BG1
Router(config-l2vpn-bg)#bridge-domain BD1
Router(config-bg-bd)#multicast-source ipv4-ipv6
Router(config-bg-bd)#mld snooping profile mldsn
Router(config-bg-bd)#igmp snooping profile igmpsn
Router(config-bg-bd)#interface Bundle-Ether1
Router(config-bg-bd-ac)#exit
Router(config-bg-bd)#interface TenGigE0/0/0/23.1
Router(config-bg-bd-ac)#exit
Router(config-bg-bd)#routed interface BV11
Router(config-bg-bd)#evi 3000
Router(config-bg-bd-bvi)#commit

```

Running Configuration

This section shows the EVPN All-Active Multi-homed multicast source with BVI as accept interface running configuration.

```

l2vpn
bridge group bg1
bridge-domain bd1
multicast-source ipv4-ipv6
mld snooping profile mldsn
igmp snooping profile igmpsn
interface Bundle-Ether1
!
interface TenGigE0/0/0/23.1
!
routed interface BV11
!
evi 3000
!
!
!
!

```

Disable EVPN Core Replications

Default behavior in EVPN involves collapsing core replications into L2 multicast routes (BD, S, G). To modify this behaviour and collapse EVPN Core to Bridge ingress multicast ID (MCID) and Snooping default routes instead of L2 multicast routes, use the following command:

```
Router(config)# hw-module multicast evpn ole-collapse-disable
```

Sample Configuration

```

Router(config)# hw-module multicast evpn ole-collapse-disable
Mon Apr 3 20:37:39.218 UTC

```

```

/*To apply the disable or re-enable EVPN OLE collapse settings, you must reload the chassis
and all the installed line cards*/

```

```

Router# commit
Mon Apr 3 20:37:46.886 UTC
Router# end

```

```

Router# admin
Mon Apr 3 20:37:52.234 UTC
lab connected from 1.1.1.1 using ssh on sysadmin-vm:0_RP0
Reloading the RP in Order to apply the HW-cli Evpn ole collapse disable command to set

```

```
sysadmin-vm:0_RP0# hw-module location 0/RP0 reload
```

```

Mon Apr 3 20:38:15.290 UTC+00:00
Reload hardware module ? [no,yes]

/*Verification After Reload*/
Router# sh dpa objects global location 0/0/cPU0 | i evpn
Mon Apr 3 20:48:38.939 UTC
ofa_bool_t mcast_evpn_ole_collapse_disable => TRUE.

Router# sh running-config | i hw-
Mon Apr 3 20:48:43.575 UTC
hw-module multicast evpn ole-collapse-disable

```

Verification

Verify that you have configured multicast over BVI. The BVI acts as a forwarding interface for the L3 multicast packets.

```

/*PE-0*/
Router# show mrrib vrf green ipv4 route 40.0.0.5
Mon May 8 12:15:44.924 UTC
(40.0.0.5,232.0.0.1) RPF nbr: 40.0.0.5 Flags: RPF
Up: 00:04:03
Incoming Interface List
BVI1 Flags: F A LI, Up: 00:04:03
Outgoing Interface List
BVI1 Flags: F A LI, Up: 00:04:03

/*Local L3 multicast join*/
TenGigE0/0/0/0.2 Flags: F NS LI, Up: 00:04:03

/*PE-1*/
Router# show mrrib vrf green ipv4 route 40.0.0.5 detail
Thu May 11 09:19:07.958 UTC
(40.0.0.5,232.0.0.1) Ver: 0x1008 RPF nbr: 40.0.0.5 Flags: RPF EID, FGID: 15481, Statistics
enabled: 0x0, Tunnel RIF: 0xffffffff, Tunnel LIF: 0xffffffff
Up: 05:29:49
RPF-ID: 0, Encap-ID: 262146
Incoming Interface List
BVI1 Flags: F A LI, Up: 05:29:49
Outgoing Interface List
BVI1 Flags: F A LI, Up: 05:29:49
/*Remote L3 join from multicast receiver learnt on PE-1. Multicast traffic to remote L3
multicast receiver is forwarded from PE-1*/
Lmdtgreen Flags: F LMI TR, Up: 05:27:02, Head LSM-ID: 0x00001

/*Local L3 multicast join*/
TenGigE0/0/0/23.2 Flags: F NS LI, Up: 05:29:48

```

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 <i>profile-name</i> Example: RP/0/RP0/CPU0:router(config)# igmp snooping profile default-bd-profile	<p>Enters IGMP snooping profile configuration mode and creates a named profile.</p> <p>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.</p>
Step 3	Optionally, add commands to override default configuration values.	<p>If you are creating a bridge domain profile, consider the following:</p> <ul style="list-style-type: none"> • 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. <p>If you are creating a port-specific profile, consider the following:</p> <ul style="list-style-type: none"> • 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. <p>You can detach a profile, change it, and reattach it to add commands to a profile at a later time.</p>
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/RP0/CPU0:router(config)# l2vpn	Enters Layer 2 VPN configuration mode.
Step 3	bridge group <i>bridge-group-name</i> Example: RP/0/RP0/CPU0:router(config-l2vpn)# bridge group GRP1	Enters Layer 2 VPN bridge group configuration mode for the named bridge group.
Step 4	bridge-domain <i>bridge-domain-name</i> Example: RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1	Enters Layer 2 VPN bridge group bridge domain configuration mode for the named bridge domain.

	Command or Action	Purpose
Step 5	multicast-source ipv4 Example: <pre>RP/0/RP0/CPU0:router(config)# multicast-source ipv4</pre>	Configures Layer 2 multicast routes with IGMP snooping.
Step 6	igmp snooping profile <i>profile-name</i> Example: <pre>RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# igmp snooping profile default-bd-profile</pre>	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: <pre>RP/0/RP0/CPU0:router# show igmp snooping bridge-domain detail</pre>	(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 9	show l2vpn bridge-domain detail Example: <pre>RP/0/RP0/CPU0:router# show l2vpn bridge-domain</pre>	(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: <pre>RP/0/RP0/CPU0:router(config)# l2vpn</pre>	Enters Layer 2 VPN configuration mode.
Step 3	bridge group <i>bridge-group-name</i> Example: <pre>RP/0/RP0/CPU0:router(config-l2vpn)# bridge group GRP1</pre>	Enters Layer 2 VPN bridge group configuration mode for the named bridge group.
Step 4	bridge-domain <i>bridge-domain-name</i> Example: <pre>RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1</pre>	Enters Layer 2 VPN bridge group bridge domain configuration mode for the named bridge domain.
Step 5	no igmp snooping disable Example: <pre>RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# no igmp snooping disable</pre>	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: <pre>RP/0/RP0/CPU0:router# show igmp snooping bridge-domain detail</pre>	(Optional) Verifies that IGMP snooping is disabled on a bridge domain.
Step 8	show l2vpn bridge-domain detail Example: <pre>RP/0/RP0/CPU0:router# show l2vpn bridge-domain</pre>	(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. **mcast-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/RP0/CPU0:router(config)# l2vpn	Enters Layer 2 VPN configuration mode.
Step 3	bridge group <i>bridge-group-name</i> Example: RP/0/RP0/CPU0:router(config-l2vpn)# bridge group GRP1	Enters Layer 2 VPN bridge group configuration mode for the named bridge group.
Step 4	bridge-domain <i>bridge-domain-name</i> Example: RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1	Enters Layer 2 VPN bridge group bridge domain configuration mode for the named bridge domain.

	Command or Action	Purpose
Step 5	interface <i>interface-type interface-number</i> Example: <pre>RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# interface gig 1/1/1/1</pre>	Enters Layer 2 VPN bridge group bridge domain interface configuration mode for the named interface or PW.
Step 6	multicast-source ipv4 Example: <pre>RP/0/RP0/CPU0:router(config)# multicast-source ipv4</pre>	Configures L2 multicast routes in L2 multicast with IGMP Snooping.
Step 7	Do one of the following: <ul style="list-style-type: none"> • igmp snooping profile <i>profile-name</i> • no igmp snooping Example: <pre>RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-if)# igmp snooping profile mrouter-port-profile</pre>	Attaches the named IGMP snooping profile to the port. Note 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: <pre>RP/0/RP0/CPU0:router# show igmp snooping bridge-domain detail</pre>	(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: <pre>RP/0/RP0/CPU0:router# show l2vpn bridge-domain</pre>	(Optional) Verifies that IGMP snooping is implemented in the forwarding plane (Layer 2) on a bridge domain.

Verifying Multicast Forwarding

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure	
Step 2	show l2vpn forwarding bridge-domain <code>[bridge-group-name:bridge-domain-name] mroute ipv4</code> <code>[group group_IPaddress] [hardware {ingress egress}]</code> <code>[detail]location node-id</code> Example: <pre>RP/0/RP0/CPU0:router# show l2vpn forwarding bridge-domain bg1:bd1 mroute ipv4 group 234.192.4.1 hardware ingress detail location 0/1/cPU0</pre>	<p>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.</p> <p>If these routes are not as expected, check the control plane configuration and correct the corresponding IGMP snooping profiles.</p>
Step 3	show l2vpn forwarding bridge-domain <code>[bridge-group-name:bridge-domain-name] mroute ipv4</code> summary location node-id Example: <pre>RP/0/RP0/CPU0:router# show l2vpn forwarding bridge-domain bg1:bd1 mroute ipv4 summary location 0/3/CPU0</pre>	<p>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.</p>

Configuration Examples for IGMP Snooping

The following examples show how to enable IGMP snooping on Layer 2 bridge domains on Cisco NCS 5500 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
!
```

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
!

```

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. Configure two IGMP snooping profiles.

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

2. 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
!
```

3. Configure the bundle interfaces for L2 transport.

```

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

```

4. 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
    !
  !
!

```

5. Verify the configured bridge ports.

```
show igmp snooping port
```

Configuring Multicast over Integrated Routing Bridging Active/Active Multihome

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 shut
!

```

2. EVPN Configuration

```

hostname peer1
!
router bgp 100
  bgp router-id 1.1.1.1

```

```

    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
        bgp route-target 0002.0002.0002
    !
    !
    !

```

3. IGMPv2 Snoop Configurations

```

hostname peer1
!
router igmp

    version 2
    !
    !
    l2vpn
    bridge group VLAN2
    bridge-domain VLAN2
    multicast-source ipv4
    igmp snooping profile 1
    interface Bundle-Ether2.2
    !

    evi 2
    !
    !
    !
    multicast-source ipv4
    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
    bgp route-target 0002.0002.0002
  !
!
!

```

3. IGMPv2 Snoop Configurations

```

hostname peer2
!
router igmp

  version 2
  !
!
l2vpn
  bridge group VLAN2
    bridge-domain VLAN2
    multicast-source ipv4
    igmp snooping profile 1
    interface Bundle-Ether2.2
  !

  evi 2
  !
!
!
multicast-source ipv4
igmp snooping profile 1
!

```

Verifying IGMP Snooping and EVPN Sync

In this example, the receiver sends an IGMPv2 join for the group 239.0.0.2. On Peer2, this group has a D Flag, that means the actual IGMP joined peer2, but not peer1. On Peer1, this group has a B flag, that means this group is learnt from BGP with the EVPN sync feature.

```

RP/0/RP0/CPU0:peer1#show igmp snooping group
Fri Aug 31 22:27:46.363 UTC

```

Key: GM=Group Filter Mode, PM=Port Filter Mode

Flags Key: S=Static, D=Dynamic, B=BGP Learnt, E=Explicit Tracking, R=Replicated

Bridge Domain VLAN10:VLAN10

Group	Ver	GM	Source	PM	Port	Exp	Flgs
239.0.0.2	V2	-	*	-	BE2.2	never	B

RP/0/RP0/CPU0:peer2#show igmp snooping group
Fri Aug 31 22:27:49.686 UTC

Key: GM=Group Filter Mode, PM=Port Filter Mode

Flags Key: S=Static, D=Dynamic, B=BGP Learnt, E=Explicit Tracking, R=Replicated

Bridge Domain VLAN10:VLAN10

Group	Ver	GM	Source	PM	Port	Exp	Flgs
239.0.0.2	V2	-	*	-	BE2.2	74	D

Verifying Dual DR PIM Uplink

In this example, when the source 126.0.0.100 sends traffic to group 239.0.0.2, you see both Peer1 and Peer2 are sending PIM join upstream. The incoming interface for (*,G) and (S,G) should be the interface toward the RP and source respectively. For both Peer1 and Peer2, the outgoing interface should be the BVI interface facing the receiver.

RP/0/RP0/CPU0:peer1#show mrib route
:
:

```
(* ,239.0.0.2) RPF nbr: 30.0.0.4 Flags: C RPF
Up: 00:13:41
Incoming Interface List
  HundredGigE0/0/0/1 Flags: A NS, Up: 00:13:41
Outgoing Interface List
  BVI2 Flags: F NS LI, Up: 00:13:41
```

```
(126.0.0.100,239.0.0.2) RPF nbr: 30.0.0.4 Flags: RPF
Up: 00:03:34
Incoming Interface List
  HundredGigE0/0/0/1 Flags: A, Up: 00:03:34
Outgoing Interface List
  BVI2 Flags: F NS, Up: 00:03:34
```

:
:

RP/0/RP0/CPU0:peer2#show mrib route
:
:

```
(* ,239.0.0.2) RPF nbr: 50.0.0.4 Flags: C RPF
Up: 00:13:33
Incoming Interface List
  HundredGigE0/0/0/2 Flags: A NS, Up: 00:13:33
Outgoing Interface List
  BVI2 Flags: F NS LI, Up: 00:13:33
```

```
(126.0.0.100,239.0.0.2) RPF nbr: 50.0.0.4 Flags: RPF
Up: 00:03:24
```

```

Incoming Interface List
  HundredGigE0/0/0/2 Flags: A, Up: 00:03:24
Outgoing Interface List
  BVI2 Flags: F NS, Up: 00:03:24
:
:

```

Verifying Designated Forwarder Election

As described in the previous example, both peer1 and peer2 have BVI2 as outgoing interface. However, only one of the peer should forward the traffic. Designated forwarder election elects one of them to do the forwarding. In this example, peer2 is selected as the forwarder. Peer1 has Bundle-Ether2.2 marked as NDF.

```

RP/0/RP0/CPU0:peer1#show l2vpn forwarding bridge-domain VLAN2:VLAN2 mroute ipv4 hardware
ingress detail location 0/0/cPU0
Bridge-Domain: VLAN2:VLAN2, ID: 0
:
:

```

```

Bridge-Domain: VLAN2:VLAN2, ID: 0
  Prefix: (0.0.0.0,239.0.0.2/32)
  P2MP enabled: N
  IRB platform data: {0x0, 0x2d, 0x0, 0x0}, len: 32
  Bridge Port:
  EVPN, Xconnect id: 0x80000001 NH:2.2.2.2
  Bundle-Ether2.2, Xconnect id: 0xa0000015 (NDF)

```

```

RP/0/RP0/CPU0:peer2#show l2vpn forwarding bridge-domain VLAN2:VLAN2 mroute ipv4 hardware
ingress detail location 0/0/cPU0
:
:

```

```

Bridge-Domain: VLAN2:VLAN2, ID: 0
  Prefix: (0.0.0.0,239.0.0.2/32)
  P2MP enabled: N
  IRB platform data: {0x0, 0x30, 0x0, 0x0}, len: 32
  Bridge Port:
  EVPN, Xconnect id: 0x80000001 NH:1.1.1.1
  Bundle-Ether2.2, Xconnect id: 0xa0000029

```

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 <i>MPLS Configuration Guide for Cisco NCS 5500 Series Routers</i>
Getting started information	
Configuring EFPs and EFP bundles	<i>Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers</i>

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