IGMP Snooping

This module describes how to enable and configure the Ethernet Virtual Connection (EVC)-based IP Multicast Internet Group Management Protocol (IGMP) Snooping feature both globally and on bridge domains.

Information About IGMP Snooping

IGMP Snooping

IGMP snooping is the process of listening to IGMP network traffic between hosts and routers. It sends multicast traffic only to the interfaces that are subscribed to a particular multicast group and thus restricts flooding of multicast traffic. Switch maintains a map of the links and the associated IP multicast streams.

IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group that have not explicitly joined. IGMP snooping takes place internally on switches and is not a protocol feature. Hence, it is especially useful for bandwidth-intensive IP multicast applications such as IPTV.

Cisco NCS 520 Series Routers dynamically configure layer 2 interfaces so that multicast traffic is forwarded to those interfaces only that are associated with the multicast devices. Thus, these routers use IGMP snooping to constrain the flooding of multicast traffic.

IGMP snooping requires the router to snoop on the IGMP transmissions between the host and the router to keep a track of the multicast groups and member ports. The router receives an IGMP report from a host for a particular multicast group and then adds the host port number to the forwarding table entry. The router receives an IGMP Leave signal and removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

IGMP snooping is supported on Metro Access licenses.

Prerequisites for IGMP Snooping

- IGMP snooping is implemented based on layer 2 multicast frames.
- Basic IGMP v3 snooping support (BISS) is supported.
- POP operation for all vlan tags should be configured on EFP.
- Bridge domain (BD) interfaces from 1 to 4094 support IGMP snooping.
- IGMP static joins are *not* supported.

Restrictions for IGMP Snooping

- IGMP snooping is implemented based on layer 2 multicast frames. So, any unregistered multicast traffic is flooded to all ports in a bridge-domain (BD), even when IGMP snooping is enabled.
- Any multicast traffic that does not have IGMP group entry is flooded, irrespective of the presence of a mrouter.
- When multicast traffic is received for a group that has IGMP receivers, traffic is forwarded to that IGMP-learnt port only and not to other mrouter port on the same BD.
- Do not use overlapping addresses. Only the last 24 bits in the DMAC field can be used to create unique group entries.
- L2 Multicast reserved MAC addresses are punted to CPU.
- IGMP with ACL is *not* supported.
- When multicast traffic is sent over ring protocols like REP or G8032 or MST, packet drops for a maximum of 60 seconds is expected during various cut over scenarios.
- Static mrouter configuration is *not* supported.
- Multicast routing is *not* supported.
- Since IGMP snooping is based on L2 MAC, TTL validation check is disabled.
- Maximum number of of IGMP entries supported is 100.
- IGMP snooping querier functionality is *not* supported.

How to Configure IGMP Snooping

Enabling IGMP Snooping

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip igmp snooping** **Example:** `Device(config)# ip igmp snooping`	Globally enables IGMP snooping after it has been disabled.
Step 4	**bridge-domain** *bridge-id* **Example:** `Device(config)# bridge-domain 100`	(Optional) Enters bridge domain configuration mode.
Step 5	**ip igmp snooping** **Example:** `Device(config-bdomain)# ip igmp snooping`	(Optional) Enables IGMP snooping on the bridge domain interface being configured. • Required only if IGMP snooping was previously explicitly disabled on the specified bridge domain.

Step 6	**end**
	Example:
	`Device(config-bdomain)# end`
		Returns to privileged EXEC mode.

Disabling IGMP Snooping Globally

Procedure

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

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no ip igmp snooping** **Example:** `Device(config)# no ip igmp snooping`	Disables IGMP snooping on the router.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Disabling IGMP Snooping on a Bridge Domain

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**bridge-domain** *bridge-id* **Example:** `Device(config)# bridge-domain 4000`	Enters bridge domain configuration mode.
Step 4	**no ip igmp snooping** **Example:** `Device(config-bdomain)# no ip igmp snooping`	Disables IGMP snooping on the bridge domain.

Step 5	**end**
	Example:
	`Device(config-bdomain)# end`
		Returns to privileged EXEC mode.

Verifying IGMP Snooping

Use these commands to verify IGMP Snooping on the router.

- **show ip igmp snooping**

  This command displays the IGMP snooping configuration globally on the router. The following is a sample output from the command:

  ```
  Router# show ip igmp snooping

  Global IGMP Snooping configuration:
  -------------------------------------------
  IGMP snooping Oper State     : Enabled
  IGMPv3 snooping (minimal)    : Enabled
  Report suppression           : Enabled
  TCN solicit query            : Enabled
  Robustness variable          : 3
  Last member query count      : 2
  Last member query interval   : 200
  Check TTL=1                  : Yes
  Check Router-Alert-Option    : No

  Vlan 1:
  --------
  IGMP snooping Admin State           : Enabled
  IGMP snooping Oper State            : Enabled
  IGMPv2 immediate leave              : Disabled
  Report suppression                  : Enabled
  Robustness variable                 : 3
  Last member query count             : 2
  Last member query interval          : 200
  Check TTL=1                         : Yes
  Check Router-Alert-Option           : Yes
  .
  .
  .
  ```

- **show ip igmp snooping** [**bd** *bd-id*]

  This command displays configuration for IGMP snooping by bridge domain. The following is a sample output from the command:

  ```
  Router# show ip igmp snooping bd 100

  Global IGMP Snooping configuration:
  -------------------------------------------
  IGMP snooping Oper State     : Enabled
  IGMPv3 snooping (minimal)    : Enabled
  Report suppression           : Enabled
  TCN solicit query            : Enabled
  Robustness variable          : 3
  Last member query count      : 2
  Last member query interval   : 200
  Check TTL=1                  : Yes
  Check Router-Alert-Option    : No

  Vlan 100:
  --------
  IGMP snooping Admin State           : Enabled
  IGMP snooping Oper State            : Enabled
  IGMPv2 immediate leave              : Disabled
  ```

```
Report suppression                  : Enabled
Robustness variable                 : 3
Last member query count             : 2
Last member query interval          : 200
Check TTL=1                         : Yes
Check Router-Alert-Option           : Yes
Query Interval                      : 0
Max Response Time                   : 10000
```

- **show ip igmp snooping groups count**

  This command displays snooping information for groups. This is a sample output from the command:

  ```
  Router# show ip igmp snooping groups count

  Total number of groups:   4
  Total number of  (S,G):   0
  ```

- **show ip igmp snooping mrouter**

  This command displays multicast ports, globally or by bridge domain.. This is a sample output from the command:

  ```
  Router# show ip igmp snooping mrouter

  Vlan    ports
  ----    -----
  100    Gi0/3/4-efp1(dynamic)
   10    Gi0/4/5-tefp1(dynamic)
  100    Po64-efp100(dynamic)
  ```

- **show ip igmp snooping querier**

  This command displays the IGMP querier information globally or by a bridge domain. This is a sample output from the command:

  ```
  Router# show ip igmp snooping querier

  Vlan      IP Address               IGMP Version   Port
  -------------------------------------------------------------
  100       10.0.0.2                 v2            Gi0/3/4-efp1
  10        10.0.0.2                 v2            Gi0/4/5-tefp1
  100       30.1.1.12                v2            Po64-efp100
  ```

- **show ip igmp snooping group**

  This command displays the IGMP snooping information about multicast groups by VLAN. This is a sample output from the command:

  ```
  Router# show ip igmp snooping  group

  Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode
  Vlan      Group/source             Type        Version     Port List
  -----------------------------------------------------------------------
  100       226.0.1.1                I           v2          Gi0/1/1-efp100
  10        225.1.1.1                I           v2          Gi0/4/2-tefp1
  100       235.1.1.3                I           v2          Po64-efp1
  ```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

Standards and RFCs

Standard/RFC	Title
No specific Standards and RFCs are supported by the features in this document.	—

MIBs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IGMP Snooping

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1: Feature Information for IGMP Snooping

Feature Name	Releases	Feature Information
IGMP Snooping	Cisco IOS XE Release 16.12.1	This feature was introduced on the NCS 520 Routers.