IGMP Snooping

Last Updated: November 19, 2012

This module describes how to enable and configure the Ethernet Virtual Connection (EVC)-based IGMP Snooping feature globally and on bridge domains.

Finding Feature Information

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

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

Information About IGMP Snooping

IGMP Snooping

Multicast traffic becomes flooded because a device usually learns MAC addresses by looking into the source address field of all the frames that it receives. A multicast MAC address is never used as the source address for a packet. Such addresses do not appear in the MAC address table, and the device has no method for learning them.

IP Multicast Internet Group Management Protocol (IGMP), which runs at Layer 3 on a multicast device, generates Layer 3 IGMP queries in subnets where the multicast traffic must be routed. IGMP (on a device) sends out periodic general IGMP queries.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

IGMP Snooping is an Ethernet Virtual Circuit (EVC)-based feature set. EVC decouples the concept of VLAN and broadcast domain. An EVC is an end-to-end representation of a single instance of a Layer 2 service being offered by a provider. In the Cisco EVC framework, bridge domains are made up of one or more Layer 2 interfaces known as service instances. A service instance is the instantiation of an EVC on a given port on a given device. A service instance is associated with a bridge domain based on the configuration.

Traditionally, a VLAN is a broadcast domain, and physical ports are assigned to VLANs as access ports; the VLAN tag in a packet received by a trunk port is the same number as the internal VLAN broadcast domain. With EVC, an Ethernet Flow Point (EFP) is configured and associated with a broadcast domain. The VLAN tag is used to identify the EFP only and is no longer used to identify the broadcast domain.

When you enable EVC-based IGMP snooping on a bridge domain, the bridge domain interface responds at Layer 2 to the IGMP queries with only one IGMP join request per Layer 2 multicast group. Each bridge domain represents a Layer 2 broadcast domain. The bridge domain interface creates one entry per subnet in the Layer 2 forwarding table for each Layer 2 multicast group from which it receives an IGMP join request. All hosts interested in this multicast traffic send IGMP join requests and are added to the forwarding table entry. During a Layer 2 lookup on a bridge domain to which the bridge domain interface belongs, the bridge domain forwards the packets to the correct EFP. When the bridge domain interface hears the IGMP Leave group message from a host, it removes the table entry of the host.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure Layer 2 multicast groups. If you specify group membership for a multicast group address statically, your static setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned-settings.

How to Configure IGMP Snooping

Enabling IGMP Snooping

Perform the following task to enable IGMP snooping only after IGMP snooping is explicitly disabled. By default, IGMP snooping is enabled on all existing VLAN interfaces and bridge domain interfaces.

Interfaces to be enabled for IGMP snooping must be configured for IP Multicast.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip igmp snooping**
4. **bridge-domain** *bridge-id*
5. **ip igmp snooping**
6. **end**

DETAILED STEPS

	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.

Configuring IGMP Snooping Globally

Perform this task to modify the global configuration for IGMP snooping.

IGMP snooping must be enabled. IGMP snooping is enabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip igmp snooping robustness-variable** *variable*
4. **ip igmp snooping tcn query solicit**
5. **ip igmp snooping tcn flood query count** *count*
6. **ip igmp snooping report-suppression**
7. **ip igmp snooping explicit-tracking-limit** *limit*
8. **ip igmp snooping last-member-query-count** *count*
9. **ip igmp snooping last-member-query-interval** *interval*
10. **ip igmp snooping check** { **ttl** | **rtr-alert-option** }
11. **exit**

DETAILED STEPS

	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 robustness-variable** *variable* **Example:** `Device(config)# ip igmp snooping robustness-variable 3`	(Optional) Configures IGMP snooping robustness variable.
Step 4	**ip igmp snooping tcn query solicit** **Example:** `Device(config)# ip igmp snooping tcn query solicit`	(Optional) Enables device to send TCN query solicitation even if it is not the spanning-tree root.

	Command or Action	Purpose
Step 5	**ip igmp snooping tcn flood query count** *count* **Example:** `Device(config)# ip igmp snooping tcn flood query count 4`	(Optional) Configures the TCN flood query count for IGMP snooping.
Step 6	**ip igmp snooping report-suppression** **Example:** `Device(config)# ip igmp snooping report-suppression`	(Optional) Enables report suppression for IGMP snooping.
Step 7	**ip igmp snooping explicit-tracking-limit** *limit* **Example:** `Device(config)# ip igmp snooping explicit-tracking-limit 200`	(Optional) Limits the number of reports in the IGMP snooping explicit-tracking database.
Step 8	**ip igmp snooping last-member-query-count** *count* **Example:** `Device (config)# ip igmp snooping last-member-query-count 5`	(Optional) Configures how often Internet Group Management Protocol (IGMP) snooping will send query messages in response to receiving an IGMP leave message. The default is 2 milliseconds.
Step 9	**ip igmp snooping last-member-query-interval** *interval* **Example:** `Device (config)# ip igmp snooping last-member-query-interval 200`	(Optional) Configures the length of time after which the group record is deleted if no reports are received. The default is 1000 milliseconds.
Step 10	**ip igmp snooping check** { **ttl** | **rtr-alert-option** } **Example:** `Device (config)# ip igmp snooping check ttl`	(Optional) Enforces IGMP snooping check.
Step 11	**exit** **Example:** `Device (config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring IGMP Snooping on a Bridge Domain Interface

Perform this task to modify the IGMP snooping configuration on a bridge domain interface.

- The bridge domain interface must be created. See the "Configuring Bridge Domain Interfaces" section of the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*.
- IGMP snooping must be enabled on the interface to be configured. IGMP snooping is enabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge-domain** *bridge-id*
4. **ip igmp snooping immediate-leave**
5. **ip igmp snooping robustness-variable** *variable*
6. **ip igmp snooping report-suppression**
7. **ip igmp snooping explicit-tracking**
8. **ip igmp snooping explicit-tracking-limit** *limit*
9. **ip igmp snooping last-member-query-count** *count*
10. **ip igmp snooping last-member-query-interval** *interval*
11. **ip igmp snooping access-group** {*acl-number* | *acl-name*}
12. **ip igmp snooping limit** *num* [**except** {*acl-number* | *acl-name*}]
13. **ip igmp snooping minimum-version** {**2** | **3**}
14. **ip igmp snooping check** { **ttl** | **rtr-alert-option** }
15. **ip igmp snooping static source** *source-address* **interface** *port-type port-number*
16. **end**

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 3	**bridge-domain** *bridge-id* **Example:** `Device(config)# bridge-domain 100`	Enters bridge domain configuration mode.
Step 4	**ip igmp snooping immediate-leave** **Example:** `Device(config-bdomain)# ip igmp snooping immediate-leave`	(Optional) Enables IGMPv2 immediate-leave processing. **Note** When both immediate-leave processing and the query count are configured, fast-leave processing takes precedence.
Step 5	**ip igmp snooping robustness-variable** *variable* **Example:** `Device(config-bdomain)# ip igmp snooping robustness-variable 3`	(Optional) Configures the IGMP snooping robustness variable. The default is 2.
Step 6	**ip igmp snooping report-suppression** **Example:** `Device(config-bdomain)# ip igmp snooping report-suppression`	(Optional) Enables report suppression for all hosts on the bridge domain interface.
Step 7	**ip igmp snooping explicit-tracking** **Example:** `Device(config-bdomain)#  ip igmp snooping explicit-tracking`	(Optional) Enables IGMP snooping explicit tracking. Explicit tracking is enabled by default.
Step 8	**ip igmp snooping explicit-tracking-limit** *limit* **Example:** `Device(config-bdomain)# ip igmp snooping explicit-tracking-limit 200`	(Optional) Limits the number of reports in the IGMP snooping explicit-tracking database.
Step 9	**ip igmp snooping last-member-query-count** *count* **Example:** `Device(config-bdomain)# ip igmp snooping last-member-query-count 5`	(Optional) Configures the interval for snooping query messages sent in response to receiving an IGMP leave message. The default is 2 milliseconds. **Note** When both immediate-leave processing and the query count are configured, fast-leave processing takes precedence.

Command or Action	Purpose
Step 10 **ip igmp snooping last-member-query-interval** *interval* **Example:** `Device(config-bdomain)#  ip igmp snooping last-member-query-interval 2000`	(Optional) Configures the length of time after which the group record is deleted if no reports are received. The default is 1000 milliseconds.
Step 11 **ip igmp snooping access-group** {*acl-number* | *acl-name*} **Example:** `Device(config-bdomain)# ip igmp snooping access-group 1300`	Configures ACL-based filtering on a bridge domain.
Step 12 **ip igmp snooping limit** *num* [**except** {*acl-number* | *acl-name*}] **Example:** `Device(config-bdomain)# ip igmp snooping 4400 except test1`	(Optional) Limits the number of groups or channels allowed on a bridge domain.
Step 13 **ip igmp snooping minimum-version** {**2** | **3**} **Example:** `Device(config-bdomain)# ip igmp snooping minimum-version 2`	(Optional) Configures IGMP protocol filtering.
Step 14 **ip igmp snooping check** { **ttl** | **rtr-alert-option** } **Example:** `Device(config-bdomain)# ip igmp snooping check ttl`	(Optional) Enforces IGMP snooping check.
Step 15 **ip igmp snooping static source** *source-address* **interface** *port-type port-number* **Example:** `Device(config-bdomain)# ip igmp snooping static source 192.0.2.1 interface gigbitethernet 1/1/1`	(Optional) Configures a host statically for a Layer 2 LAN port.
Step 16 **end** **Example:** `Device(config-bdomain)# end`	Returns to privileged EXEC mode.

Configuring an EFP

Perform this task to configure IGMP snooping features on an EFP.

The EFP and bridge domain must be previously configured. Configuring a service instance on a Layer 2 port creates a pseudoport or Ethernet Flow Point (EFP) on which you configure Ethernet Virtual Connection (EVC) features. See the "Configuring Ethernet Virtual Connections on the Cisco ASR 1000 Router" section of the *Carrier Ethernet Configuration Guide* for configuration information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router-guard ip multicast efps**
4. **interface** *type number*
5. **service instance** *id* **ethernet**
6. **router-guard multicast**
7. **ip igmp snooping tcn flood**
8. **ip igmp snooping access-group** {*acl-number* | *acl-name*}
9. **ip igmp snooping limit** *num* [**except** {*acl-number* | *acl-name*}]
10. **end**

DETAILED STEPS

	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	**router-guard ip multicast efps** **Example:** `Device(config)# router-guard ip multicast efps`	(Optional) Enables the router guard for all EFPs.

	Command or Action	Purpose
Step 4	**interface** *type number* **Example:** `Device(config)# interface BDI100`	(Optional) Specifies the bridge domain interface to be configured.
Step 5	**service instance** *id* **ethernet** **Example:** `Device(config-if)# service instance 333 ethernet`	(Optional) Enters Ethernet service configuration mode for configuring the EFP.
Step 6	**router-guard multicast** **Example:** `Device(config-if-srv)# router-guard multicast`	(Optional) Configures a router guard on an EFP.
Step 7	**ip igmp snooping tcn flood** **Example:** `Device(config-if-srv)# no ip igmp snooping tcn flood`	(Optional) Disables TCN flooding on an EFP. TCN flooding is enabled by default.
Step 8	**ip igmp snooping access-group** {*acl-number* | *acl-name*} **Example:** `Device(config-if-srv)# ip igmp snooping access-group 44`	(Optional) Configures ACL-based filtering on an EFP.
Step 9	**ip igmp snooping limit** *num* [**except** {*acl-number* | *acl-name*}] **Example:** `Device(config-if-srv)# ip igmp snooping limit 1300 except test1`	(Optional) Limits the number of IGMP groups or channels allowed on an EFP.
Step 10	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.

Verifying IGMP Snooping

SUMMARY STEPS

1. **enable**
2. **show igmp snooping** [**count** [**bd** *bd-id*]]
3. **show igmp snooping groups bd** *bd-id* [**count** | *ip-address* [**verbose**] [**hosts** | **sources** | **summary**]]
4. **show igmp snooping membership bd** *bd-id*
5. **show igmp snooping mrouter** [**bd** *bd-id*]
6. **show igmp snooping counters** [**bd** *bd-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show igmp snooping** [**count** [**bd** *bd-id*]] **Example:** `Device(config)# show igmp snooping`	Displays configuration for IGMP snooping, globally or by bridge domain.
Step 3	**show igmp snooping groups bd** *bd-id* [**count** | *ip-address* [**verbose**] [**hosts** | **sources** | **summary**]] **Example:** `Device(config)# show igmp snooping groups bd 100`	Displays snooping information for groups by bridge domain.
Step 4	**show igmp snooping membership bd** *bd-id* **Example:** `Device(config)# show igmp snooping membership bd 100`	Displays IGMPv3 host membership information.
Step 5	**show igmp snooping mrouter** [**bd** *bd-id*] **Example:** `Device(config)# show igmp snooping mrouter`	Displays multicast ports, globally or by bridge domain.

	Command or Action	Purpose
Step 6	**show igmp snooping counters** [**bd** *bd-id*] **Example:** `Device(config)# show snooping counters`	Displays IGMP snooping counters, globally or by bridge domain.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP Multicast commands	Cisco IOS IP Multicast Command Reference
Configuring the ASR 1000 series router	Cisco ASR 1000 Series Aggregation Services Routers Configuration Guides

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation 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 Configuring IGMP Snooping

Feature Name	Releases	Feature Information
IGMP Snooping	Cisco IOS XE Release 3.5S 15.2(4)S	IGMP snooping is an IP multicast constraining mechanism based on the Ethernet Virtual Connection (EVC) infrastructure. IGMP snooping examines Layer 3 information (IGMP Join/Leave messages) in the IGMP packets sent between hosts and routers. The following commands were introduced or modified: **ip igmp snooping**, **ip igmp snooping check**, **ip igmp snooping explicit-track ing limit**, **ip igmp snooping immediate leave**, **ip igmp snooping last-member-query count**, **ip igmp snooping last-member-query interval**, **ip igmp snooping report-suppression**, **ip igmp snooping robustness-variable**, **ip igmp snooping static**, **ip igmp snooping tcn flood** (if-srv), **ip igmp snooping tcn flood query**, **ip igmp snooping tcn flood query solicit**, **router guard ip multicast efps**