



## **IP Multicast: Multicast Configuration Guide, Cisco IOS XE 17 (Cisco NCS 520 Series)**

**First Published:** 2019-11-26

**Last Modified:** 2020-01-12

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### **IGMP Snooping 1**

Information About IGMP Snooping 1

IGMP Snooping 1

Prerequisites for IGMP Snooping 2

Restrictions for IGMP Snooping 2

How to Configure IGMP Snooping 3

Enabling IGMP Snooping 3

Disabling IGMP Snooping Globally 3

Disabling IGMP Snooping on a Bridge Domain 4

Verifying IGMP Snooping 5

Additional References 7

Feature Information for IGMP Snooping 7





# CHAPTER 1

## 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, on page 1](#)
- [Prerequisites for IGMP Snooping, on page 2](#)
- [Restrictions for IGMP Snooping, on page 2](#)
- [How to Configure IGMP Snooping, on page 3](#)
- [Verifying IGMP Snooping, on page 5](#)
- [Additional References, on page 7](#)
- [Feature Information for IGMP Snooping, on page 7](#)

## 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-learned 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 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
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ip igmp snooping</b> <b>Example:</b> Device(config)# ip igmp snooping	Globally enables IGMP snooping after it has been disabled.
<b>Step 4</b>	<b>bridge-domain <i>bridge-id</i></b> <b>Example:</b> Device(config)# bridge-domain 100	(Optional) Enters bridge domain configuration mode.
<b>Step 5</b>	<b>ip igmp snooping</b> <b>Example:</b> Device(config-bdomain)# ip igmp snooping	(Optional) Enables IGMP snooping on the bridge domain interface being configured. <ul style="list-style-type: none"><li>• Required only if IGMP snooping was previously explicitly disabled on the specified bridge domain.</li></ul>
<b>Step 6</b>	<b>end</b> <b>Example:</b> Device(config-bdomain)# end	Returns to privileged EXEC mode.

## Disabling IGMP Snooping Globally

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>	Enables privileged EXEC mode.

	Command or Action	Purpose
	<b>Example:</b> Device> <b>enable</b>	<ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>no ip igmp snooping</b> <b>Example:</b> Device(config)# <b>no ip igmp snooping</b>	Disables IGMP snooping on the router.
<b>Step 4</b>	<b>exit</b> <b>Example:</b> Device(config)# <b>exit</b>	Exits global configuration mode and returns to privileged EXEC mode.

## Disabling IGMP Snooping on a Bridge Domain

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>bridge-domain <i>bridge-id</i></b> <b>Example:</b> Device(config)# <b>bridge-domain 4000</b>	Enters bridge domain configuration mode.
<b>Step 4</b>	<b>no ip igmp snooping</b> <b>Example:</b> Device(config-bdomain)# <b>no ip igmp snooping</b>	Disables IGMP snooping on the bridge domain.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-bdomain)# <b>end</b>	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	<a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html</a>

### Standards and RFCs

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

### MIBs

MB	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:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

*Table 1: Feature Information for IGMP Snooping*

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