



## IGMP Commands

---

- [access-group \(IGMP\)](#), on page 2
- [clear igmp counters](#), on page 3
- [clear igmp group](#), on page 5
- [clear igmp reset](#), on page 7
- [explicit-tracking](#), on page 8
- [join-group](#), on page 10
- [maximum groups](#), on page 12
- [maximum groups-per-interface](#), on page 15
- [nsf lifetime \(IGMP\)](#) , on page 19
- [query-interval](#), on page 21
- [query-max-response-time](#), on page 23
- [query-timeout](#), on page 25
- [robustness-count](#), on page 27
- [router](#), on page 28
- [router igmp](#), on page 30
- [show igmp groups](#), on page 31
- [show igmp nsf](#), on page 33
- [show igmp nsr](#), on page 35
- [show igmp ssm map](#), on page 37
- [show igmp summary](#), on page 38
- [show igmp traffic](#), on page 41
- [show igmp vrf vrf\\_name groups](#), on page 44
- [ssm map](#), on page 45
- [static-group](#), on page 46
- [version](#), on page 48
- [vrf \(igmp\)](#), on page 50

# access-group (IGMP)

To set limits on an interface for multicast-group join requests by hosts, use the **access-group** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

```
access-group access-list
no access-group access-list
```

<b>Syntax Description</b>	<i>access-list</i> Number or name of a standard IP access list. Range is 1 to 99.
---------------------------	---

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	IGMP interface configuration
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 7.0.12	This command was introduced.

<b>Usage Guidelines</b>	If this command is not specified in router Internet Group Management Protocol (IGMP) configuration mode, the interface accepts all multicast join requests by hosts.
-------------------------	--

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	multicast	read, write

<b>Examples</b>	In the following example, hosts serviced by HundredGigE 0/0/0/24 can join only group 225.2.2.2:
-----------------	---

```
Router# configure
Router(config)# ipv4 access-list mygroup permit 225.2.2.2 0.0.0.0
Router(config)# router igmp
Router(config-igmp)# interface HundredGigE 0/0/0/24
Router(config-igmp-default-if)# access-group mygroup
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ipv4 access-list</b>	Defines a standard IP access list. For information, see <i>IP Addresses and Services Command Reference for Cisco 8000 Series Routers</i>

# clear igmp counters

To clear IGMP traffic statistics, use the **clear igmp counters** command in EXEC mode.

```
clear igmp [{ipv4 vrf vrf-name | vrf vrf-name}] counters
```

<b>Syntax Description</b>	<b>ipv4</b> (Optional) Specifies IPv4 addressing. IPv4 is the default for Internet Group Management Protocol (IGMP) groups.
---------------------------	---

<b>vrf</b> <i>vrf-name</i> (Optional) Specifies a VPN routing and forwarding (VRF) instance.
--

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 7.0.12	This command was introduced.

<b>Usage Guidelines</b>	After IGMP statistics are cleared, statistics begin incrementing again.
-------------------------	---

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	multicast	execute

## Examples

The following example shows sample output before and after clearing IGMP traffic statistics:

```
Router# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:00:19

Valid IGMP Packets          Received      Sent
Queries                     0             3
Reports                     0             9
Leaves                      0             0
Mtrace packets              0             0
DVMRP packets               0             0
PIM packets                  0             0

Errors:
Malformed Packets          0
Bad Checksums               0
Socket Errors               0
Bad Scope Errors           0
Auxiliary Data Len Errors  0
Subnet Errors               0
Packets dropped due to invalid socket 0
Packets which couldn't be accessed 0
Other packets drops        0
```

```
Router# clear igmp counters
```

```
Router# show igmp traffic
```

```
IGMP Traffic Counters
```

```
Elapsed time since counters cleared: 00:00:12
```

	Received	Sent
Valid IGMP Packets	0	1
Queries	0	1
Reports	0	0
Leaves	0	0
Mtrace packets	0	0
DVMRP packets	0	0
PIM packets	0	0
Errors:		
Malformed Packets		0
Bad Checksums		0
Socket Errors		0
Bad Scope Errors		0
Auxiliary Data Len Errors		0
Subnet Errors		0
Packets dropped due to invalid socket		0
Packets which couldn't be accessed		0
Other packets drops		0

---

**Related Commands**

Command	Description
<a href="#">show igmp traffic, on page 41</a>	Displays all the Internet Group Management Protocol (IGMP) traffic-related counters.

---

# clear igmp group

To clear Internet Group Management Protocol (IGMP) groups on one or all interfaces, use the **clear igmp group** command in EXEC mode.

```
clear igmp [{ipv4 vrf vrf-name | vrf vrf-name}] group [{ip-address | type interface-path-id}]
```

Syntax Description	
<b>ipv4</b>	(Optional) Specifies IPv4 addressing. IPv4 is the default for IGMP groups.
<b>vrf vrf-name</b>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<b>ip-address</b>	(Optional) IP hostname or group address.
<b>type</b>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<b>interface-path-id</b>	(Optional) Physical interface or virtual interface.
	<p><b>Note</b> Use the <b>show interfaces</b> command to see a list of all interfaces currently configured on the router.</p> <p>For more information about the syntax for the router, use the question mark (?) online help function.</p>

**Command Default** If no group address is specified, all IGMP groups are cleared.

**Command Modes** EXEC

Command History	Release	Modification
	Release 7.0.12	This command was introduced.

**Usage Guidelines** To clear all IGMP groups, use the **clear igmp group** command without using an argument. To clear a particular group, use the *ip-address* or *type interface-path-id* arguments.

The following groups cannot be cleared:

- 224.0.0.2
- 224.0.0.13
- 224.0.0.22
- 224.0.0.40

Task ID	Task ID	Operations
	multicast	execute

## Examples

The following example uses the **show igmp group** command to display the IGMP Connected Group Membership, the **clear igmp group** command to clear address 239.1.1.1, and the **show igmp groups** command again to display the updated list.

```
Router# show igmp groups HundredGigE 0/0/0/24
```

```
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires    Last Reporter
224.0.0.2       HundredGigE0/0/0/24     3w6d     never     10.114.8.44
224.0.0.5       HundredGigE0/0/0/24     3w6d     never     10.114.8.44
224.0.0.6       HundredGigE0/0/0/24     3w6d     never     10.114.8.44
224.0.0.13      HundredGigE0/0/0/24     3w6d     never     10.114.8.44
224.0.0.22      HundredGigE0/0/0/24     3w6d     never     10.114.8.44
```

```
Router# clear igmp groups HundredGigE0/0/0/24
```

```
Router# show igmp groups HundredGigE0/0/0/24
```

```
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires    Last Reporter
224.0.0.2       HundredGigE0/0/0/24     3w6d     never     10.114.8.44
224.0.0.5       HundredGigE0/0/0/24     3w6d     never     10.114.8.44
224.0.0.6       HundredGigE0/0/0/24     3w6d     never     10.114.8.44
224.0.0.13      HundredGigE0/0/0/24     3w6d     never     10.114.8.44
224.0.0.22      HundredGigE0/0/0/24     3w6d     never     10.114.8.44
```

## Related Commands

Command	Description
<a href="#">show igmp groups, on page 31</a>	Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).

# clear igmp reset

To clear all Internet Group Management Protocol (IGMP) membership entries and reset connection in the Multicast Routing Information Base (MRIB), use the **clear igmp reset** command in EXEC mode.

```
clear igmp [{ipv4 vrf vrf-name | vrf vrf-name}] reset
```

<b>Syntax Description</b>	<b>ipv4</b> (Optional) Specifies IPv4 addressing. IPv4 is the default for IGMP groups.
	<b>vrf vrf-name</b> (Optional) Specifies a VPN routing and forwarding (VRF) instance.

**Command Default** No default behavior or values

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 7.0.12	This command was introduced.

**Usage Guidelines** Every IGMP group membership that IGMP learns is downloaded to the MRIB database. The **clear igmp reset** command is used to clear all information from the IGMP topology table and reset the MRIB connection.



**Note** This command is reserved to force synchronization of IGMP and MRIB entries when communication between the two components is malfunctioning.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	multicast	execute

**Examples** The following example shows how to clear the group memberships in MRIB:

```
Router# clear igmp reset
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show igmp groups, on page 31</a>	Displays the multicast groups that are directly connected to the router and that were learned through IGMP
	<b>show mrrib route</b>	Displays all route entries in the MRIB table.

# explicit-tracking

To configure explicit host tracking under Internet Group Management Protocol (IGMP) Version 3, use the **explicit-tracking** command in the appropriate configuration mode. To disable explicit host tracking, use the **no** form of this command.

**explicit-tracking** [{*access-list* | **disable**}]  
**no explicit-tracking**

Syntax Description	
	<i>access-list</i> (Optional) Access list that specifies the group range for host tracking.
	<b>disable</b> (Optional) Disables explicit host tracking on a specific interface. This option is available only in interface configuration mode.

**Command Default** If this command is not specified in IGMP configuration mode, then explicit host tracking is disabled.

**Command Modes** IGMP VRF configuration  
 IGMP interface configuration

Command History	Release	Modification
	Release 7.0.12	This command was introduced.

**Usage Guidelines** By default, IGMP supports Version 3, unless a Version 2 or Version 1 IGMP host message is detected in the network. For backward compatibility, IGMP downgrades to run at the IGMP version level that is installed.

This feature allows the router to achieve minimal leave latencies when hosts leave a multicast group or channel. To monitor IGMP membership of hosts, use the **show igmp groups** command in EXEC mode.

In router configuration mode, the **explicit-tracking** command enables explicit host tracking for all interfaces. To disable explicit tracking for all interfaces, use the **no** form of the command from IGMP configuration mode. To disable the feature on specific interfaces, use the **explicit-tracking** command in interface configuration mode with the **disable** keyword, as shown in the following example.



**Note** If you configure this command in IGMP VRF configuration mode, parameters are inherited by all new and existing interfaces. However, you can override these parameters on individual interfaces from IGMP interface configuration mode.

Task ID	Task ID	Operations
	multicast	read, write

**Examples** The following example shows how to enable explicit host tracking for the access list named router1 on all interfaces and how to disable explicit host tracking for a specific GigabitEthernet interface:

```
Router# configure
Router(config)# router igmp
Router(config-igmp)# explicit-tracking router1
Router(config-igmp)# interface hundredGigE 0/0/0/24
Router(config-igmp-default-if)# explicit-tracking disable
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show igmp groups, on page 31</a>	Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).

---

# join-group

To have the router join a multicast group, use the **join-group** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

```
join-group group-address [source-address]
no join-group group-address [source-address]
```

## Syntax Description

*group-address* Address of the multicast group. This is a multicast IP address group in IPv4 format

- IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format *A.B.C.D* .

*source-address* (Optional) Source address of the multicast group to include in IPv4 prefixing format

- IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format *A.B.C.D* .

## Command Default

No multicast group memberships are predefined. If not specified, include is the default.

## Command Modes

IGMP interface configuration

## Command History

Release	Modification
Release 7.0.12	This command was introduced.

## Usage Guidelines

The **join-group** command permits the IP packets that are addressed to the group address to pass to the IP client process in the Cisco IOS XR software.

If all the multicast-capable routers that you administer are members of a multicast group, pinging that group causes all routers to respond. This command can be a useful administrative and debugging tool.

Another reason to have a router join a multicast group is when other hosts on the network are prevented from correctly answering IGMP queries. When the router joins the multicast group, upstream devices learn multicast routing table information for that group and keep the paths for that group active.



**Caution** Joining a multicast group can result in a significant performance impact, because all subscribed multicast packets are punted to the route processor.

## Task ID

### Task ID Operations

multicast read,  
write

## Examples

In the following example, the router joins multicast group 225.2.2.2:

```
Router(config)# router igmp
Router(config-igmp)# interface GigabitEthernet 0/1/0/0
Router(config-igmp-default-if)# join-group 225.2.2.2
```

The **join-group** command can have an include/exclude mode for IGMPv3 interfaces as shown in the following example:

```
Router(config)#router igmp
Router(config-igmp)#int gigabitEthernet 0/5/0/1
RP/0/RSP0/CPU0:router(config-igmp-default-if)#join-group ?
A.B.C.D IP group address
Router(config-igmp-default-if)#join-group 225.0.0.0 ?
A.B.C.D Source address to include
exclude Exclude the only following source address include Include only the following
source address <cr>
Router(config-igmp-default-if)#join-group 225.0.0.0 10.10.10.10 ?
<cr>
Router(config-igmp-default-if)#join-group 225.0.0.0 ?
A.B.C.D Source address to include
exclude Exclude the only following source address
include Include only the following source address <cr>
Router(config-igmp-default-if)#join-group 225.0.0.0
```

#### Related Commands

Command	Description
<b>ping</b>	Checks host reachability and network connectivity on IP networks. For information, see <i>IP Addresses and Services Command Reference for Cisco 8000 Series Routers</i> .

## maximum groups

To configure the maximum number of groups used by Internet Group Management Protocol (IGMP) and accepted by a router, use the **maximum groups** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

**maximum groups** *number*  
**no maximum groups**

<b>Syntax Description</b>	<i>number</i> Maximum number of groups accepted by a router. Range is 1 to 75000.
---------------------------	---

<b>Command Default</b>	<i>number</i> : 50000
------------------------	-----------------------

<b>Command Modes</b>	IGMP configuration IGMP VRF configuration
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 7.0.12	This command was introduced.

<b>Usage Guidelines</b>	<p>When configuring this command within IGMP VRF configuration mode, you may either use the default (unspecified) VRF or a specific VRF by specifying its name.</p> <p>The maximum combined number of groups on all interfaces can be 75000. After the maximum groups value is met, all additional memberships learned are ignored. The maximum number includes external and local membership.</p> <p>The following groups obtain local membership on each interface when multicast is enabled and are added into the group totals for each interface: 224.0.0.13 (for PIM), 224.0.0.22 and 224.0.0.2 (for IGMP).</p> <p>You cannot use the <b>maximum groups</b> command to configure the maximum number of groups below the number of existing groups. For instance, if the number of groups is 39, and you set the maximum number of groups to 10, the configuration is rejected.</p> <p>The router supports a maximum of 16,000 multicast routes per system.</p> <p>Furthermore, you can use the <b>maximum groups per-interface</b> command to configure the maximum number of groups for each interface accepted by a router.</p>
-------------------------	---

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	multicast	read, write

<b>Examples</b>	<p>The following example shows how to display the number of groups (39) and the maximum number of groups configured (50000) . Through use of the <b>maximum groups</b> command, a configuration is committed to change the maximum number of groups to 40. Before and after configuration, the <b>show igmp summary</b> command is used to confirm the configuration change:</p>
-----------------	--

```
Router# show igmp summary
```

```
IGMP summary
```

```
Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 50000
```

```
Supported Interfaces : 18
Unsupported Interfaces : 2
Enabled Interfaces : 18
Disabled Interfaces : 2
```

Interface	Grp No	Max Grp No
MgmtEth0/RSP0/CPU0/0	0	25000
Loopback0	4	25000
Bundle-Ether24	3	25000
Bundle-Ether28	3	25000
Bundle-Ether28.1	3	25000
Bundle-Ether28.2	3	25000
Bundle-Ether28.3	3	25000
MgmtEth0/RP1/CPU0/0	0	25000
HundredGigE0/0/0/24	3	25000
HundredGigE0/0/0/25	5	25000
HundredGigE0/0/0/26	5	25000

```
Router# configure
```

```
Router(config)# router igmp
```

```
Router(config-igmp)# maximum groups 65
```

```
Router(config-igmp)# commit
```

```
Router:May 13 12:26:59.108 : config[65704]: %LIBTARCFG-6-COMMIT : Configuration committed
by user 'cisco'. Use 'show commit changes 1000000025' to view the changes.
```

```
Router# show igmp summary
```

```
Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 65
```

```
Supported Interfaces : 18
Unsupported Interfaces : 2
Enabled Interfaces : 18
Disabled Interfaces : 2
```

Interface	Grp No	Max Grp No
MgmtEth0/RSP0/CPU0/0	0	25000
Loopback0	4	25000
Bundle-Ether28	3	25000
Bundle-Ether28.1	3	25000
Bundle-Ether28.2	3	25000
Bundle-Ether28.3	3	25000
MgmtEth0/RP1/CPU0/0	0	25000
HundredGigE0/0/0/25	5	25000
HundredGigE0/0/0/26	5	25000

## Related Commands

Command	Description
<a href="#">maximum groups-per-interface, on page 15</a>	Configures the maximum number of groups for each interface accepted by a router.

Command	Description
<a href="#">show igmp summary, on page 38</a>	Displays group membership information for Internet Group Management Protocol (IGMP).

## maximum groups-per-interface

To configure the maximum number of groups for each interface accepted by a router, use the **maximum groups-per-interface** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

```
maximum groups-per-interface number
no maximum groups-per-interface
```

<b>Syntax Description</b>	<i>number</i> Maximum number of groups accepted by a router for each interface. Range is 1 to 40000.
---------------------------	--

<b>Command Default</b>	<i>number</i> : 20000
------------------------	-----------------------

<b>Command Modes</b>	IGMP configuration IGMP VRF configuration IGMP interface configuration
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 7.0.12	This command was introduced.

<b>Usage Guidelines</b>	The following groups obtain local membership on each interface when multicast is enabled and are added into the group totals for each interface: 224.0.0.13 (for Protocol Independent Multicast [PIM]), 224.0.0.22 and 224.0.0.2 (for Internet Group Management Protocol [IGMP]). The number of groups for each interface reflects both external and local group membership.
-------------------------	--



<b>Note</b>	You cannot use the <b>maximum groups-per-interface</b> command to configure the maximum number of groups for each interface below the number of existing groups on an interface. For example, if the number of groups is 39, and you set the maximum number of groups to 10, the configuration is rejected.
-------------	---

When you use the **maximum groups-per-interface** command for a specific interface, it overrides the inheritance property of this command specified under IGMP configuration mode.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	multicast	read, write

### Examples

The following example shows how to display the maximum number of groups for each interface. A configuration is committed to change the maximum number of groups for each interface to 12. Before and after configuration, use the **show igmp summary** command to confirm the configuration change:

```
Router# show igmp summary
```

IGMP summary

Robustness Value 2  
 No. of Group x Interfaces 61  
 Maximum number of Group x Interfaces 50000

Supported Interfaces : 18  
 Unsupported Interfaces : 2  
 Enabled Interfaces : 18  
 Disabled Interfaces : 2

Interface	Grp No	Max Grp No
MgmtEth0/RSP0/CPU0/0	0	25000
Loopback0	4	25000
Bundle-Ether28	3	25000
Bundle-Ether28.1	3	25000
Bundle-Ether28.2	3	25000
Bundle-Ether28.3	3	25000
MgmtEth0/RP1/CPU0/0	0	25000
HundredGigE 0/0/0/24	3	25000
HundredGigE 0/0/0/25	5	25000
HundredGigE 0/0/0/26	5	25000
HundredGigE 0/0/0/27	3	25000

```
Router# configure
Router(config)# router igmp
Router(config-igmp)# maximum groups-per-interface 5
Router(config-igmp)# commit
```

Router# show igmp summary

Robustness Value 2  
 No. of Group x Interfaces 61  
 Maximum number of Group x Interfaces 65

Supported Interfaces : 18  
 Unsupported Interfaces : 2  
 Enabled Interfaces : 18  
 Disabled Interfaces : 2

Interface	Grp No	Max Grp No
MgmtEth0/RSP0/CPU0/0	0	5
Loopback0	4	5
Bundle-Ether28	3	5
Bundle-Ether28.1	3	5
Bundle-Ether28.2	3	5
Bundle-Ether28.3	3	5
MgmtEth0/RP1/CPU0/0	0	5
HundredGigE 0/0/0/24	3	5
HundredGigE 0/0/0/25	5	5
HundredGigE 0/0/0/26	5	5

The following example shows how to configure all interfaces with 3000 maximum groups per interface except HundredGigE 0/0/0/24, which is set to 4000:

```
Router# configure
Router(config)# router igmp
Router(config-igmp)# maximum groups-per-interface 3000
Router(config-igmp)# interface HundredGigE 0/0/0/24
Router(config-igmp-default-if)# maximum groups-per-interface 4000
```

IGMP summary

Robustness Value 2  
 No. of Group x Interfaces 61  
 Maximum number of Group x Interfaces 50000

Supported Interfaces : 18  
 Unsupported Interfaces : 2  
 Enabled Interfaces : 18  
 Disabled Interfaces : 2

Interface	Grp No	Max Grp No
MgmtEth0/RP0/CPU0/0	0	25000
Loopback0	4	25000
Bundle-POS24	3	25000
Bundle-Ether28	3	25000
Bundle-Ether28.1	3	25000
Bundle-Ether28.2	3	25000
Bundle-Ether28.3	3	25000
MgmtEth0/RP1/CPU0/0	0	25000
HundredGigE 0/0/0/25	3	25000
HundredGigE 0/0/0/26	5	25000
HundredGigE 0/0/0/27	5	25000

```
Router# configure
Router(config)# router igmp
Router(config-igmp)# maximum groups-per-interface 5
Router(config-igmp)# commit
Router# show igmp summary
```

Robustness Value 2  
 No. of Group x Interfaces 61  
 Maximum number of Group x Interfaces 65

Supported Interfaces : 18  
 Unsupported Interfaces : 2  
 Enabled Interfaces : 18  
 Disabled Interfaces : 2

Interface	Grp No	Max Grp No
MgmtEth0/RP0/CPU0/0	0	5
Loopback0	4	5
Bundle-POS24	3	5
Bundle-Ether28	3	5
Bundle-Ether28.1	3	5
Bundle-Ether28.2	3	5
Bundle-Ether28.3	3	5
MgmtEth0/RP1/CPU0/0	0	5
HundredGigE 0/0/0/24	3	5
HundredGigE 0/0/0/25	5	5
HundredGigE 0/0/0/26	5	5
POS0/1/0/1	5	5
POS0/1/4/2	3	5

```
Router# configure
Router(config)# router igmp
Router(config-igmp)# maximum groups-per-interface 3000
```

```
Router(config-igmp)# interface POS 0/4/0/0  
Router(config-igmp-default-if)# maximum groups-per-interface 4000
```

Related Commands	Command	Description
	<a href="#">maximum groups, on page 12</a>	Configures the maximum number of groups used by Internet Group Management Protocol (IGMP).
	<a href="#">show igmp summary, on page 38</a>	Displays group membership information for Internet Group Management Protocol (IGMP).

## nsf lifetime (IGMP)

To configure the maximum time for the nonstop forwarding (NSF) timeout on the Internet Group Management Protocol (IGMP) process, use the **nsf lifetime** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

**nsf lifetime** *seconds*  
**no nsf lifetime**

<b>Syntax Description</b>	<i>seconds</i> Maximum time for NSF mode. Range is 10 to 3600 seconds.
---------------------------	--

<b>Command Default</b>	<i>seconds</i> : 60
------------------------	---------------------

<b>Command Modes</b>	IGMP configuration IGMP VRF configuration
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 7.0.12	This command was introduced.

<b>Usage Guidelines</b>	The IGMP NSF process is triggered by the restart of the IGMP process. While in IGMP NSF mode, the Multicast Routing Information Base (MRIB) purges the routes installed by the previous IGMP process when the IGMP NSF process times out.
-------------------------	---

The IGMP NSF lifetime is the period for IGMP to relearn all the host membership of the attached network through membership queries and reports. During this NSF period, PIM continues to maintain forwarding state for the local members while IGMP recovers their membership reports.

Additionally, IGMP recovers the internal receiver state from Local Packet Transport Services (LPTS) for IP group member applications (including the Session Announcement Protocol (SAP) Listener) and updates the MRIB.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	multicast	read, write

<b>Examples</b>	The following example shows how to set the IGMP NSF timeout value to 120 seconds:
-----------------	---

```
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# nsf lifetime 120
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>nsf (multicast)</b>	Enables NSF capability for the multicast routing system.
	<b>nsf lifetime (PIM)</b>	Configures the NSF timeout value for the PIM process.

Command	Description
<a href="#">show igmp nsf, on page 33</a>	Displays the state of NSF operation in IGMP.
<b>show mfib nsf</b>	Displays the state of NSF operation for the MFIB line cards.

# query-interval

To configure the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages, use the **queryinterval** command in the appropriate configuration mode. To return to the default frequency, use the **no** form of this command.

**query-interval** *seconds*  
**no query-interval**

## Syntax Description

*seconds* Frequency used to send IGMP host-query messages. Range is 1 to 3600.

## Command Default

If this command is not specified in interface configuration mode, the interface adopts the query interval parameter specified in IGMP configuration mode.

If this command is not specified in IGMP configuration mode, the query interval time is 60 seconds.

## Command Modes

IGMP VRF configuration

IGMP interface configuration

## Command History

Release	Modification
Release 7.0.12	This command was introduced.

## Usage Guidelines

Multicast routers send host membership query messages (host-query messages) to discover which multicast groups have members on the attached networks of the router. Hosts respond with IGMP report messages indicating that they want to receive multicast packets for specific groups (that is, that the host wants to become a member of the group). Host-query messages are addressed to the all-hosts multicast group, which has the address 224.0.0.1, and has an IP time-to-live (TTL) value of 1.

The designated router for a LAN is the only router that sends IGMP host-query messages:

- For IGMP Version 1 (only), the designated router is elected according to the multicast routing protocol that runs on the LAN.
- For IGMP Versions 2 and 3, the designated querier is the lowest IP-addressed multicast router on the subnet.

If the router hears no queries for the timeout period (controlled by the query-timeout command), it becomes the querier.



**Note** Changing the value of the *seconds* argument may severely impact network performance. A short query interval may increase the amount of traffic on the attached network, and a long query interval may reduce the querier convergence time.



**Note** If you configure the **query-interval** command in IGMP configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from interface configuration mode.

**Task ID****Task ID Operations**

multicast read,  
write

**Examples**

This example shows how to change the frequency at which the designated router sends IGMP host-query messages to 2 minutes:

```
Router(config)# router igmp
Router(config-igmp)# interface HundredGigE 0/0/0/24
Router(config-igmp-default-if)# query-interval 120
```

**Related Commands**

Command	Description
<b>hello-interval (PIM)</b>	Configures the frequency of PIM hello messages.
query-timeout	Configures the timeout value before the router takes over as the querier for the interface.
<a href="#">show igmp groups, on page 31</a>	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.

## query-max-response-time

To configure the maximum response time advertised in Internet Group Management Protocol (IGMP) queries, use the **query-max-response-time** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

**query-max-response-time** *seconds*  
**no query-max-response-time**

<b>Syntax Description</b>	<i>seconds</i> Maximum response time, in seconds, advertised in IGMP queries. Range is 1 to 12.				
<b>Command Default</b>	If this command is not specified in interface configuration mode, the interface adopts the maximum response time parameter specified in IGMP configuration mode.  If this command is not specified in IGMP configuration mode, the maximum response time is 10 seconds.				
<b>Command Modes</b>	IGMP VRF configuration  IGMP interface configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Release 7.0.12</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Release 7.0.12	This command was introduced.
Release	Modification				
Release 7.0.12	This command was introduced.				
<b>Usage Guidelines</b>	<p>The <b>query-max-response-time</b> command is not supported on IGMP Version 1.</p> <p>This command is used to control the maximum response time for hosts to answer an IGMP query message. Configuring a value less than 10 seconds enables the router to prune groups much faster, but this action results in network burstiness because hosts are restricted to a shorter response time period.</p> <p>If you configure this command in IGMP configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces in interface configuration mode.</p>				



**Note** If the hosts do not read the maximum response time in the query message correctly, group membership might be pruned inadvertently. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

Task ID	Task ID	Operations
	multicast	read, write

### Examples

The following example shows how to configure a maximum response time of 8 seconds:

```
Router(config)# router igmp
Router(config-igmp)# interface HundredGigE 0/0/0/24
Router(config-igmp-default-if)# query-max-response-time 8
```

**Related Commands**

Command	Description
<b>hello-interval (PIM)</b>	Configures the frequency of PIM hello messages.
<a href="#">show igmp groups, on page 31</a>	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.

## query-timeout

To configure the timeout value before the router takes over as the querier for the interface, use the **query-timeout** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

**query-timeout** *seconds*  
**no query-timeout**

<b>Syntax Description</b>	<i>seconds</i> Number of seconds that the router waits after the previous querier has stopped querying before it takes over as the querier. Range is 60 to 300.
---------------------------	---

<b>Command Default</b>	If this command is not specified in interface configuration mode, the interface adopts the timeout value parameter specified in IGMP VRF configuration mode. If this command is not specified in IGMP VRF configuration mode, the maximum response time is equal to twice the query interval set by the <b>query-interval</b> command.
------------------------	--

<b>Command Modes</b>	IGMP VRF configuration IGMP interface configuration
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 7.0.12	This command was introduced.

<b>Usage Guidelines</b>	<p>The <b>query timeout</b> command is not supported on Internet Group Management Protocol (IGMP) Version 1. By default, the router waits twice the query interval specified by the <b>query-interval</b> command, after which, if the router has heard no queries, it becomes the querier. By default, the query interval is 60 seconds, which means that the <b>query timeout</b> value defaults to 120 seconds.</p> <p>If you configure a query timeout value less than twice the query interval, routers in the network may determine a query timeout and take over the querier without good reason.</p>
-------------------------	--



<b>Note</b>	If you configure this command in IGMP configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces in interface configuration mode.
-------------	--

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	multicast	read, write

<b>Examples</b>	The following example shows how to configure the router to wait 30 seconds from the time it received the last query before it takes over as the querier for the interface:
-----------------	--

```
Router(config)# router igmp
```

```
Router(config-igmp)# interface HundredGigE 0/0/0/24
Router(config-igmp-default-if)# query-timeout 30
```

---

**Related Commands**

Command	Description
<a href="#">query-interval, on page 21</a>	Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.

---

# robustness-count

To set the robustness variable to tune for expected packet loss on a network, use the **robustness-count** command in the appropriate configuration mode. To return to the default setting, use the **no** form of this command.

```
robustness-count count
no robustness-count
```

<b>Syntax Description</b>	<i>count</i> Value of the robustness count variable. Range is 2 to 10 packets.
---------------------------	--

<b>Command Default</b>	Default is 2 packets.
------------------------	-----------------------

<b>Command Modes</b>	IGMP VRF configuration IGMP interface configuration
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 7.0.12	This command was introduced.

<b>Usage Guidelines</b>	IGMP is a soft-state protocol. State must be periodically refreshed or it times out. At a <b>robustness-count</b> command setting, for example, of 4, a network might lose three IGMP packets related to some specific state yet still maintain the state. If, however, a network lost more than three IGMP packets in the sequence, the state would time out. You might then consider changing the <b>robustness-count</b> setting to maintain state.
-------------------------	--

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	multicast	read, write

<b>Examples</b>	The following example illustrates the use of the <b>robustness-count</b> command:
-----------------	---

```
RP/0/RP0/CPU0:router(config)# configure
RP/0/RP0/CPU0:router(config)# router igmp
RP/0/RP0/CPU0:router(config-igmp)# robustness-count 2
```

# router

To disable or enable Internet Group Management Protocol (IGMP) membership tracking, use the **router** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

```
router {disable | enable}
no router {disable | enable}
```

Syntax Description	
<b>disable</b>	Turns off IGMP membership tracking.
<b>enable</b>	Turns on IGMP membership tracking.

Command Default	
	If this command is not specified in IGMP VRF configuration mode, router functionality is enabled on all interfaces.

Command Modes	
	IGMP interface configuration

Command History	Release	Modification
	Release 7.0.12	This command was introduced.

Usage Guidelines	
	The <b>router</b> command is used to enable and disable the IGMP router functionality on a specific interface. For instance, IGMP stops queries from an interface when the router functionality is disabled on that interface. Disabling IGMP router functionality does not prevent local group membership from being announced through the group membership report.



Note	
	This command is useful if you want to disable or enable IGMP interfaces that have been previously enabled through the <b>multicast-routing</b> command.

Task ID	Task ID	Operations
	multicast	read, write

Examples	
	The following example shows how to enable IGMP membership tracking functionality on all multicast enabled interfaces, except Packet-over-SONET/SDH (POS) interface HundredGigE 0/0/0/24:

```
Router(config)# router igmp
Router(config-igmp)# interface HundredGigE 0/0/0/24
Router(config-igmp-default-if)# router enable
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>multicast routing</b>	Enables multicast routing and forwarding on all enabled interfaces of the router and enters multicast routing configuration mode.

# router igmp

To enter Internet Group Management Protocol (IGMP) configuration mode, use the **router igmp** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

**router igmp**  
**no router igmp**

**Syntax Description** This command has no keywords or arguments.

**Command Default** No default behavior or values

**Command Default** Global configuration

Command History	Release	Modification
	Release 7.0.12	This command was introduced.

**Usage Guidelines** From IGMP VRF configuration mode, you can configure the maximum response time advertised in IGMP queries and modify the host query interval.



**Note** The IGMP process is turned on when the **router igmp** command or the **multicast-routing** command is initiated.

Task ID	Task ID	Operations
	multicast	read, write

## Examples

The following example shows how to enter IGMP configuration mode:

```
Router(config)# router igmp
Router(config-igmp)#
```

## Related Commands

Command	Description
<b>interface all disable</b>	Disables IGMP membership tracking on all interfaces.
<b>multicast routing</b>	Enables multicast routing and forwarding on all enabled interfaces of the router and enters multicast routing configuration mode.

# show igmp groups

To display the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the **show igmp groups** command in EXEC mode.

```
show igmp [vrf vrf-name] groups [{group-address | type interface-path-id | not-active | summary}]
[detail] [explicit]
```

Syntax Description	
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
<i>group-address</i>	(Optional) Address or name of the multicast group. An address is a multicast IP address in four-part dotted-decimal notation. A name is as defined in the Domain Name System (DNS) hosts table.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-path-id</i>	(Optional) Either a physical interface or a virtual interface.  <b>Note</b> Use the <b>show interfaces</b> command in EXEC mode to see a list of all interfaces currently configured on the router.  For more information about the syntax for the router, use the question mark (?) online help function.
<b>not-active</b>	(Optional) Displays group joins that are not processed.
<b>summary</b>	(Optional) Displays the total number of (*, G) and (S, G) states in IGMP.
<b>detail</b>	(Optional) Displays detail information such as IGMP Version 3 source list, host, and router mode.
<b>explicit</b>	(Optional) Displays explicit tracking information.

**Command Default** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 7.0.12	This command was introduced.

**Usage Guidelines** If you omit all optional arguments, the **show igmp groups** command displays (by group address and interface name) all the multicast memberships that the directly connected networks have subscribed.

Task ID	Task ID	Operations
	multicast	read

## Examples

The following is sample output from the **show igmp groups** command on a specific (HundredGigE) interface:

```
Router# show igmp groups HundredGigE 0/0/0/24

IGMP Connected Group Membership
Group Address      Interface          Uptime    Expires    Last Reporter
224.0.0.2         HundredGigE 0/0/0/24 3w6d     never      10.114.8.44
224.0.0.5         HundredGigE 0/0/0/24 3w6d     never      10.114.8.44
224.0.0.6         HundredGigE 0/0/0/24 3w6d     never      10.114.8.44
224.0.0.13        HundredGigE 0/0/0/24 3w6d     never      10.114.8.44
224.0.0.22        HundredGigE 0/0/0/24 3w6d     never      10.114.8.44
```

This table describes the significant fields shown in the display.

**Table 1: show igmp groups Field Descriptions**

Field	Description
Group Address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	How long (in hours, minutes, and seconds) this multicast group has been known.
Expires	How long (in hours, minutes, and seconds) until the entry is removed from the IGMP groups table.
Last Reporter	Last host to report being a member of the multicast group.

# show igmp nsf

To display the state of the nonstop forwarding (NSF) operation in Internet Group Management Protocol (IGMP), use the **show igmp nsf** command in EXEC mode

```
show igmp [vrf vrf-name] nsf
```

## Syntax Description

**old-output** (Optional) Displays the old show output—available for backward compatibility.

**vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.

## Command Default

No default behavior or values

## Command Modes

EXEC

## Command History

Release	Modification
Release 7.0.12	This command was introduced.

## Usage Guidelines

The **show igmp nsf** command displays the current multicast NSF state for IGMP. The NSF state that is displayed may be either normal or activated for NSF. The activated state indicates that recovery is in progress due to an IGMP failure. The total NSF timeout and time remaining are displayed until NSF expiration.

## Task ID

Task ID	Operations
multicast	read

## Examples

The following is sample output from the **show igmp nsf** command:

```
RP/0/RP0/CPU0:router# show igmp nsf

IGMP_AFD
Non-Stop Forwarding Status: Multicast routing state: Normal

NSF Lifetime
:          00:01
:00
```

This table describes the significant fields shown in the display.

**Table 2: show igmp nsf Field Descriptions**

Field	Description
Multicast routing state	Multicast NSF status of IGMP (Normal or Non-Stop Forwarding Activated).

Field	Description
NSF Lifetime	Timeout for IGMP NSF. IGMP remains in the NSF state, recovering the IGMP route state through IGMP reports for this period of time, before making the transition back to the normal state and signaling the Multicast Routing Information Base (MRIB).
NSF Time Remaining	If IGMP NSF state is activated, the time remaining until IGMP reverts to Normal mode displays.

---

**Related Commands**

Command	Description
<b>nsf (multicast)</b>	Enables NSF capability for the multicast routing system.
<b>nsf lifetime (IGMP)</b>	Configures the NSF timeout value for the IGMP or MLD process. Configures the NSF timeout value for the IGMP process.
<b>nsf lifetime (PIM)</b>	Configures the NSF timeout value for the PIM process.
<b>show mfib nsf</b>	Displays the state of NSF operation for the MFIB line cards.
<b>show mrrib nsf</b>	Displays the state of NSF operation in the MRIB.
<b>show pim nsf</b>	Displays the state of NSF operation for PIM.

## show igmp nsr

To display the nonstop routing (NSR) information in Internet Group Management Protocol (IGMP), use the **show igmp nsr** command in EXEC mode.

```
show igmp ipv4|ipv6 nsr
```

<b>Syntax Description</b>	ipv4 (Optional) Specifies IPv4 address prefixes.
	ipv6 (Optional) Specifies IPv6 address prefixes

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 7.0.12	This command was introduced.

<b>Usage Guidelines</b>	The <b>show igmp nsr</b> command displays the current multicast NSR information for IGMP. The NSR state that is displayed may be either normal or activated for NSR. The activated state indicates that recovery is in progress due to an IGMP failure. The total NSR timeout and time remaining are displayed until NSR expiration.
-------------------------	--

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	multicast	read

### Examples

The following is sample output from the **show igmp nsr** command:

```
Router# show igmp nsr

IGMP NSR Data :-
NSR State                : Not Ready (uptime 4w0d)
Converged with collaborators : Y
Partner connection state  : Not-covered/Down
RMF Notif done           : Y
Last RMF ready notified   : Never [0]
Last RMF not ready notified : 4w0d [1]
Last partner process conn up   : Never [0]
Last partner process conn down : Never [0]
```

This table describes the significant fields shown in the display.

**Table 3: show igmp nsr Field Descriptions**

Field	Description
NSR State	Multicast Non-Stop Routing State: Ready or Not Ready

Field	Description
Converged with collaborators	Yes or No
Partner connection state	Converged/Yes or Non-converged/No
RMF Notif done	RMF notification whether activated: Yes or No
Last RMF ready notified	The Time when the last RMF ready notification was received: Yes, No, or Never.  The number in the brackets indicate the number of times the RMF ready notification was received.
Last RMF not ready notified	The Time when the last RMF not ready notification was received: Yes, No, or Never.  The number in the brackets indicate the number of times the RMF ready notification was received.

#### Related Commands

Command	Description
<b>show msdp nsr</b>	Displays the state of NSR operation for MSDP.
<b>show mrrib nsr</b>	Displays the state of NSR operation in MRIB.
<b>show pim nsr</b>	Displays the state of NSR operation for PIM.

## show igmp ssm map

To query the source-specific mapping (SSM) state, use the **show igmp ssm map** command in EXEC mode.

```
show igmp [vrf vrf-name] ssm map [group-address] [detail]
```

Syntax Description	
<b>vrf</b>	(Optional) Specifies a VPN routing and forwarding (VRF) instance to be queried.
<i>vrf-name</i>	(Optional) Specifies the name of the specific VRF instance.
<i>group-address</i>	(Optional) Specifies the address of the SSM group for which to obtain the mapping state.
<b>detail</b>	(Optional) Displays detailed source information.

**Command Default** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 7.0.12	This command was introduced.

**Usage Guidelines** No specific guidelines impact the use of this command.

Task ID	Task ID	Operations
	multicast	read

**Examples** The following example illustrates the use of the **show igmp ssm map** command:

```
Router# show igmp ssm map 232.1.1.1
```

```
232.1.1.1 is static with 1 source
```

# show igmp summary

To display group membership information for Internet Group Management Protocol (IGMP), use the **show igmp summary** command in EXEC mode.

**show igmp** [**vrf vrf-name**] **summary**

<b>Syntax Description</b>	<b>old-output</b> (Optional) Displays the old show output—available for backward compatibility.
	<b>vrf vrf-name</b> (Optional) Specifies a VPN routing and forwarding (VRF) instance.

**Command Default** No default behavior or values

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 7.0.12	This command was introduced.

**Usage Guidelines** The **show igmp summary** command is used to display the total group membership. The value for number of groups is the total number of group members on all interfaces. The value for maximum number of groups is the total number of external and local members possible for all interfaces. The maximum number of groups and the default value for the maximum number of groups is 50000 members. The maximum number of groups for each interface, and the default value for the maximum number of groups for each interface, is 25000 members.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	multicast	read

**Examples** The following example shows the number of groups for each interface that are IGMP members and the maximum number of groups that can become members on each interface:

```
Router# show igmp summary

IGMP summary

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 65

Supported Interfaces   : 18
Unsupported Interfaces : 2
Enabled Interfaces    : 18
Disabled Interfaces   : 2

Interface

Grp No
```

```

Max Grp No
Bundle-Ether28.1      3      5
MgmtEth0/RSP0/CPU0/0
0
    5
Loopback0
    4
    5
MgmtEth0/RP1/CPU0/0  0      5
Bundle-Ether28
    3      5
Bundle-Ether28
3
    5
Bundle-Ether28.1
3
    5
Bundle-Ether28.2
3
    5
Bundle-Ether28.3
    3      5
MgmtEth0
/RP1
/CPU0
/0
    0
    5
GigabitEthernet0/1
/5/0
    3      5
GigabitEthernet0/1
/5/1
5
    5

```

This table describes the significant fields shown in the display.

**Table 4: show igmp summary Field Descriptions**

Field	Description
No. of Group x Interfaces	Number of multicast groups that are joined through the interface.
Maximum number of Group x Interfaces	Maximum number of multicast groups that can be joined through the interface.
Supported Interfaces	Interfaces through which the multicast groups are reachable.
Unsupported Interfaces	Number of unsupported interfaces.
Enabled Interfaces	Number of enabled interfaces.

Field	Description
Disabled Interfaces	Number of disabled interfaces.

**Related Commands**

Command	Description
<a href="#">show igmp groups, on page 31</a>	Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).

# show igmp traffic

To display all the Internet Group Management Protocol (IGMP) traffic-related counters, use the **show igmp traffic** command in EXEC mode.

```
show igmp [vrf vrf-name] traffic
```

<b>Syntax Description</b>	<b>vrf vrf-name</b> (Optional) Specifies a VPN routing and forwarding (VRF) instance.
---------------------------	---

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 7.0.12	This command was introduced.

**Usage Guidelines** The **show igmp traffic** command is used to display the state of all counters for IGMP traffic. It gives information about the length of time the counters have been active and the count of different types of IGMP packets received, such as queries, leaves, and reports. Also, this command keeps a count of all the erroneous IGMP packets received.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	multicast	read

## Examples

The following is sample output from the **show igmp traffic** command:

```
RP/0/RP0/CPU0:router# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 15:27:38

Valid IGMP Packet          Received      Sent
Queries                    0            2784
Reports                    2784         2792
Leaves                     0            0
Mtrace packets             0            0
DVMRP packets              0            0
PIM packets                0            0

Errors:
Malformed Packets          0
Bad Checksums              0
Socket Errors              0
Bad Scope Errors           0
Auxiliary Data Len Error   0
Subnet Errors              0
```

```
Packets dropped due to invalid socket          0
Packets which couldn't be accessed            0
```

This table describes the significant fields shown in the display for the **show igmp traffic** command.

**Table 5: show igmp traffic Field Descriptions**

Field	Description
Valid IGMP Packet	Total number of valid protocol packets sent and received. Valid packet types include: <ul style="list-style-type: none"> <li>• Queries</li> <li>• Membership reports</li> <li>• Leaves</li> </ul>
Queries	Total number of query packets sent and received. IP Multicast routers send queries to determine the multicast reception state of neighboring interfaces.
Reports	Total number of membership report packets received. Membership reports indicate either the current multicast reception state of a neighboring interface or a change to that state.
Leaves	Total number of leaves received. A leave group packet indicates a neighboring interface no longer has multicast reception state for a particular group.
Mtrace packets	Total number of Mtrace packets sent and received. Mtrace traces the route from a receiver to a source using a particular multicast address.
DVMRP packets	Total number of Distance Vector Multicast Routing Protocol (DVMRP) packets sent and received. DVMRP is an Internet routing protocol that provides a mechanism for connectionless datagram delivery to a group of hosts across an internetwork. This protocol dynamically generates IP multicast delivery trees using Reverse Path Multicasting. Packet type 0x13 indicates a DVMRP packet.
PIM packets	Total number of sent and received Protocol Independent Multicast (PIM) packets.
Malformed Packets	Total number of malformed packets received. A malformed packet is a packet smaller than the smallest valid protocol packet.
Bad Checksums	Total number of packets received with a bad protocol header checksum.
Socket Errors	Total number of read and write failures on the protocol socket.
Bad Scope Errors	Total number of packets received with an invalid multicast scope. <p><b>Note</b> IGMP has no invalid scopes; this counter, therefore, never increments in IGMP.</p>
Auxiliary Data Len Errors	Total number of packets received with a non-zero auxiliary data length.

Field	Description
Subnet Errors	Total number of packets received that were not sourced on the same subnet as the router.  DVMRP and MTRACE packets received are not checked for this error as they may be validly sourced from a different subnet.
Packets dropped due to invalid socket	Total number of packets dropped due to an invalid socket.
Packets which couldn't be accessed	Total number of packets that could not be sent or received.  This might occur if: <ul style="list-style-type: none"> <li>• Packet buffer does not form a valid protocol packet.</li> <li>• IP header is not written to the packet.</li> <li>• Outgoing packet interface handle was not set.</li> <li>• Errors occurred calculating the protocol checksum.</li> </ul>
Other Packet Drops	Packets dropped for any other reason.

**Related Commands**

Command	Description
<b>show pim traffic</b>	Displays PIM traffic counter information.

## show igmp vrf vrf\_name groups

To display the IGMP group membership information, use the **show igmp vrf vrf\_name groups** command in the EXEC mode.

**show igmp vrf vrf\_name groups ip\_address**

<b>Syntax Description</b>	<i>ip_address</i> Specifies the IP address or group address.
---------------------------	--

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 7.0.12	This command was introduced.

<b>Usage Guidelines</b>	No specific guidelines impact the use of this command.
-------------------------	--

<b>Task ID</b>	<b>Task ID</b>	<b>Operation</b>
	multicast	read

```
Router# show igmp vrf vrf1 groups 232.1.1.1
IGMP Connected Group Membership
Group Address    Interface          Uptime    Expires    Last Reporter
232.1.1.1       tunnel-mte1       12:39:31  never      110.110.110.110
```

## ssm map

To map group memberships from legacy hosts in Source-Specific Multicast (SSM) groups accepted by an access control list (ACL) to a Protocol Independent Multicast (PIM)-SSM source or to configure DNS mapping for PIM-SSM sources to a set of SSM groups, use the **ssm map** command in the appropriate configuration mode. To revert to default behavior, use the **no** form of this command.

```
ssm map { static source-address access-list }
no ssm map { static source-address access-list }
```

### Syntax Description

<i>source-address</i>	PIM-SSM source address to be used to create a static mapping.
<i>access-list</i>	ACL specifying the groups to be used to create a static mapping.

### Command Default

Legacy host membership reports in the SSM group range are discarded.

### Command Modes

IGMP VRF configuration

### Command History

Release	Modification
Release 7.0.12	This command was introduced.

### Usage Guidelines

PIM-SSM requires the use of IGMPv3 (IPv4) to determine local memberships. Under normal operating conditions, IGMP discards older version group membership reports for groups in the SSM group range. This means that a host with a legacy group membership protocol is unable to receive data from a PIM-SSM source.

The **ssm map static** command maps an older group membership report to a set of PIM-SSM sources. If the ACL associated with a configured source accepts the SSM group, then that source is included in its set of sources for the SSM group.

### Task ID

Task ID	Operations
	multicast read, write

### Examples

The following example shows PIM-SSM mapping in IGMP routing configuration mode:

```
Router(config)# configuration
Router(config)# router igmp
Router(config-igmp)# ssm map static 10.0.0.1 mc2
Router(config-igmp)#
```

## static-group

To configure the router to be a statically configured member of the specified group on the interface, or to statically forward for a multicast group onto the interface, use the **static-group** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

```
static-group group-address [inc-mask mask count cnt] [source-address [inc-mask mask count cnt]]
no static-group group-address [inc-mask mask count cnt] [source-address [inc-mask mask count cnt]]
```

### Syntax Description

<i>group-address</i>	IP address of the multicast group in IPv4 prefixing format: <ul style="list-style-type: none"> <li>IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format <i>A.B.C.D</i>.</li> </ul>
<b>inc-mask</b> <i>mask</i>	(Optional) Specifies a mask for the increment range. This is an IP address expressed range in IPv4 format. This mask is used with the group address to generate subsequent group addresses: <ul style="list-style-type: none"> <li>IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format <i>A.B.C.D</i></li> </ul> <p><b>Note</b> This mask is used with the group address to generate subsequent group addresses.</p>
<b>count</b> <i>cnt</i>	(Optional) Specifies a number of group addresses to generate using the increment mask. Range is 1 to 512.
<i>source address</i>	(Optional) Source address of the multicast group to include in IPv4 prefixing format: <ul style="list-style-type: none"> <li>IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format <i>A.B.C.D</i>.</li> </ul>

### Command Default

A router is not a statically connected member of an IP multicast group.

### Command Modes

IGMP interface configuration

### Command History

Release	Modification
Release 7.0.12	This command was introduced.

### Usage Guidelines

When you configure the **static-group** command, packets to the group are switched out the interface, provided that packets were received on the correct Reverse Path Forwarding (RPF) interface.

The **static-group** command differs from the **join-group** command. The **join-group** command allows the router to join the multicast group and draw traffic to an IP client process (that is, the route processor). If you configure both the **join-group** and **static-group** command for the same group address, the **join-group** command takes precedence and the group behaves like a locally joined group.



---

**Note** The **static-group** command has no impact on system performance. Configuring a static-group on a loopback interface has no effect on the router.

---

Task ID	Task ID	Operations
	multicast	read, write

### Examples

In the following example, the router statically joins two multicast groups 225.2.2.2 and 225.2.2.4 for the specific source 1.1.1.1:

```
Router(config)# router igmp
Router(config-igmp)# interface HundredGigE 0/0/0/24
Router(config-igmp-default-if)# static-group 225.2.2.2 inc-mask 0.0.0.2 count 2 1.1.1.1
```

# version

To configure an Internet Group Management Protocol (IGMP) version for the router, use the **version** command in the appropriate configuration mode. To restore the default value, use the **no** form of this command.

**version** {1 | 2 | 3}  
**no version**

## Syntax Description

- 1 Specifies IGMP Version 1.
- 2 Specifies IGMP Version 2.
- 3 Specifies IGMP Version 3.

## Command Default

If this command is not specified in interface configuration mode, the interface adopts the IGMP version parameter specified in IGMP VRF configuration mode.

If this command is not specified in IGMP configuration mode, IGMP uses Version 3.

## Command Modes

IGMP configuration  
 IGMP VRF configuration  
 IGMP interface configuration

## Command History

Release	Modification
Release 7.0.12	This command was introduced.

## Usage Guidelines

All routers on the subnet must be configured with the same version of IGMP. For example, a router running Cisco IOS XR software does not automatically detect Version 1 systems and switch to Version 1. Hosts can have any IGMP version and the router will correctly detect their presence and query them appropriately.

The **query-max-response-time** and **query-timeout** commands require IGMP Version 2 or 3.



**Note** If you configure this command in IGMP configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from interface configuration mode.

## Task ID

Task ID	Operations
multicast	read, write

## Examples

The following example shows how to configure the router to use IGMP Version 3:

```
Router(config)# router igmp  
Router(config-igmp)# version 3
```

Related Commands	Command	Description
	<a href="#">query-max-response-time, on page 23</a>	Configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries.
	<a href="#">query-timeout, on page 25</a>	Configures the timeout value before the router takes over as the querier for the interface.

## vrf (igmp)

To configure a virtual private network (VRF) instance, use the **vrf** command in IGMP routing configuration mode. To remove the VRF instance from the configuration file and restore the system to its default condition, use the **no** form of this command.

```
vrf vrf-name
no vrf vrf-name
```

<b>Syntax Description</b>	<i>vrf-name</i> Name of the VRF instance.
---------------------------	---

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	IGMP configuration
----------------------	--------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 7.0.12	This command was introduced.

<b>Usage Guidelines</b>	When you use the <b>vrf</b> command from the IGMP routing configuration mode to configure a VRF instance, you enter the IGMP VRF configuration submode.
-------------------------	---

A VRF instance is a collection of VPN routing and forwarding tables maintained at the provider edge (PE) router.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	multicast	read, write

### Examples

The following example shows how to configure a VRF instance in IGMP configuration submode and to enter VRF configuration submode:

```
Router(config)# router igmp
Router(config-igmp)# vrf vrf_1
Router(config-igmp-vrf_1)#
```