IGMP Snooping Commands

access-group (snooping profile)

To instruct IGMP /MLD snooping to apply the specified access list filter to received membership reports, use the **access-group** command in the appropriate snooping profile configuration mode. To discontinue membership report filtering, use the **no** form of this command.

access-group *acl-name*
no **access-group**

Syntax Description

acl-name	Name of the ACL filter.

Command Default

Membership reports are not filtered by default.

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following examples shows how to configure an ACL to filter membership reports:

```
Router(config-igmp-snooping-profile)# access-group acl-name
```

```
Router(config-mld-snooping-profile)# access-group acl-name
```

Related Commands

Command	Description
group limit	Specifies the group limit of the port.
group policy	Instructs IGMP snooping to use the specified route policy to determine the weight contributed by a new <*,G> or <S,G> membership request.
show igmp snooping profile	Displays the contents of profiles and to see associations of profiles with bridge-domains and ports, including access group, group limit, and TCN flood parameters.

clear igmp snooping bridge-domain

To clear IGMP snooping information at the bridge domain level, use the **clear igmp snooping bridge-domain** command in EXEC mode.

clear igmp snooping bridge-domain [*bridge-domain-name*] **statistics** [**include-ports**]

Syntax Description

bridge-domain-name	(Optional) Clears information for the named bridge domain.
statistics	Clears counters and other statistics.

include-ports	(Optional) Clears port-level counters and statistics in addition to the bridge domain level.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You have the option to clear statistics for one or all bridge domains. You also have the option to clear only bridge domain statistics, or bridge domain statistics plus all statistics for all ports under the cleared bridge domains.

Task ID

Task ID	Operations
l2vpn	execute

Examples

The following example clears IGMP snooping statistics for all bridge domains on the router:

```
Router# clear igmp snooping bridge-domain statistics
```

The following example clears IGMP snooping statistics for one bridge domain and all ports under it:

```
Router# clear igmp snooping bridge-domain bd-1 statistics include-ports
```

Related Commands

Command	Description
show igmp snooping bridge-domain	Displays IGMP snooping configuration information and statistics for bridge domains.

clear igmp snooping group

To clear IGMP snooping group states, use the **clear igmp snooping group** command in EXEC mode.

clear igmp snooping group [*group-address*] [{**port** {**interface-name** | **neighbor** *ipaddr* **pw-id** *id*} | **bridge-domain** *bridge-domain*}]

Syntax Description

group-address	(Optional) Clears the specified group from the forwarding tables.

port *interface-name*	(Optional) Clears groups for the named interface from the forwarding tables.
port neighbor *ipaddr* **pw-id** *id*	(Optional) Clears groups for the named pseudowire (PW) from the forwarding tables.
bridge-domain *bridge-domain*	(Optional) Clears groups for the named bridge domain from the forwarding tables.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

IGMP snooping propagates the request to clear group information through the L2FIB to the forwarding plane. After this command is issued, IGMP snooping relearns group information by snooping packets as they are received from the network.

Use the **address** keyword to clear one group, identified by address. Otherwise, all groups are cleared. You can clear the named group from all ports or bridges, or from a specifically identified port or bridge.

Use the **bridge-domain** keyword to clear groups only for a named bridge domain. Use the **port** keyword to clear groups for a named port. A port can be an access interface or a pseudowire. The **bridge-domain** and **port** keywords are mutually exclusive.

Task ID

Task ID	Operations
l2vpn	execute

Examples

The following example clears all group membership information from the forwarding tables:

```
Router# clear igmp snooping group
```

The following example clears one group from the forwarding table for one identified access circuit:

```
Router# clear igmp snooping group port GigabitEthernet 0/0/0/1
```

The following example clears all group membership information from the forwarding table for one identified pseudowire:

```
Router# clear igmp snooping group port
neighbor
10.5.5.5 pw-id 5
```

The following example clears one group from the forwarding table for one identified pseudowire:

```
Router# clear igmp snooping group 10.10.10.1 port
neighbor
10.5.5.5 pw-id 5
```

Related Commands

Command	Description
show igmp snooping group	Displays IGMP snooping configuration information and statistics by group address.

clear igmp snooping port

To clear IGMP snooping port information, use the **clear igmp snooping port** command in EXEC mode.

clear igmp snooping port [{**interface-name** | **neighbor** *ipaddr* **pw-id** *id* | **bridge-domain** *bridge-domain-name*}] **statistics**

Syntax Description

interface-name	(Optional) Clears information for the named interface from the forwarding tables.
neighbor *ipaddr* **pw-id** *id*	(Optional) Clears information for the named PW from the forwarding tables.
bridge-domain *bridge-domain-name*	(Optional) Clears information for all ports under the named bridge domain.
statistics	Clears counters and other statistics.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can use this command to clear IGMP snooping information at the port level for:

- All ports on the router
- A specific port, using its interface name
- A specific PW, using the **neighbor** keyword

- All ports under a named bridge domain, using the **bridge-domain** keyword. In this case, only the port-level information is cleared under the bridge-domain. Use the **clear igmp snooping bridge-domain** command to clear statistics at the bridge-domain level.

Task ID

Task ID	Operations
l2vpn	execute

Examples

The following example clears IGMP snooping port-level counters for all ports on the router.

```
Router# clear igmp snooping port statistics
```

The following example clears IGMP snooping counters for one AC.

```
Router# clear igmp snooping port GigabitEthernet 0/0/0/1 statistics
```

The following example clears IGMP snooping counters for one PW.

```
Router# clear igmp snooping port neighbor 192.0.2.1 pw-id 5 statistics
```

Related Commands

Command	Description
clear igmp snooping bridge-domain	Clears IGMP snooping information at the bridge level.
show igmp snooping port	Displays IGMP snooping configuration information and statistics by port.

clear igmp snooping summary

To clear IGMP snooping summary counters, use the **clear igmp snooping summary** command in EXEC mode.

clear igmp snooping summary statistics

Syntax Description

statistics	Clears counters and other statistics.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command clears summary level statistics about IGMP snooping. This command does not affect statistics at the bridge domain level or the port level.

Task ID

Task ID	Operations
l2vpn	execute

Examples

The following example clears all IGMP snooping statistics.

```
Router# clear igmp snooping summary statistics
```

Related Commands

Command	Description
show igmp snooping summary	Displays IGMP snooping configuration and traffic statistics at a summary level for the router.

clear l2vpn forwarding bridge-domain mroute

To clear multicast routes from the Layer-2 forwarding tables, use the **clear l2vpn forwarding bridge-domain mroute** command in EXEC mode.

clear l2vpn forwarding bridge-domain [**bg** : **bd**] **mroute** [{**ipv4** | **ipv6**}] [**location** *node-id*]

Syntax Description

[*bg*:*bd*]	(Optional) Clears Layer-2 multicast routes only for the specified bridge group and bridge domain.
ipv4	(Optional) Specifies the IPv4 addressing scheme.
location *node-id*	(Optional) Clears Layer-2 multicast routes only for the specified node ID.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command removes multicast routes in the Layer-2 forwarding information base (l2fib) tables. If you issue the command without a specific bridge group and bridge domain, information for all bridge groups and domains is cleared.

Note This command does not remove the state from the control plane. So, multicast routes will not be recreated. You can use the **clear igmp snooping group** command which not only clears state from the control plane but also clears the state from the forwarding plane.

Task ID

Task ID	Operations
l2vpn	execute

Examples

The following example clears all multicast routes across all bridge domains on one module.

```
Router# clear l2vpn forwarding mroute location 0/5/CPU0
```

group limit

To specify the maximum number of groups or source-groups that may be joined on a port, use the **group limit** command in the appropriate snooping profile configuration mode. By default, each group or source-group contributes a weight of 1 towards this limit. To remove the group limit, use the **no** form of this command.

group limit *group-limit-value*
no group limit *group-limit-value*

Syntax Description

group-limit-value	Limit value for the port. Range is from 0-65535.

Command Default

No group limit

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

No new group or source group will be accepted if its contributed weight would cause this limit to be exceeded.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to set the group limit of a port for weighting:

```
Router# configure
Router(config)#igmp snooping profile
Router(config-igmp-snooping-profile)# group limit 699
```

```
Router# configure
Router(config)#mld snooping profile
Router(config-mld-snooping-profile)# group limit 699
```

Related Commands

Command	Description
access-group (snooping profile)	Instructs IGMP snooping to apply the specified access list filter to received membership reports
group policy	Instructs IGMP snooping to use the specified route policy to determine the weight contributed by a new <*,G> or <S,G> membership request.
show igmp snooping profile	Displays the contents of profiles and to see associations of profiles with bridge-domains and ports, including access group, group limit, and TCN flood parameters.
show igmp snooping group	Displays a summary of IGMP group information by group.
show igmp snooping group detail	Displays detailed IGMP group information in a multiline display per group.
show igmp snooping port	Displays IGMP snooping configuration information and traffic counters by router interface port.
show igmp snooping port detail	Displays IGMP snooping configuration information and traffic counters by router interface port. You can use this command to see groups admitted against the configured limit.
show igmp snooping port group detail	Displays detailed IGMP membership information by port. You can use this command to see how group limits are assigned to groups on a port.

group policy

To instruct IGMP / MLD snooping to use the specified route policy to determine the weight contributed by a new <*,G> or <S,G> membership request, use the **group policy** command in the appropriate snooping profile configuration mode. To remove the group weight route policy from the profile and use the default group weight of 1 for all groups, use the **no** form of this command.

group policy *policy-name*
no group policy

Syntax Description

policy-name	Name of the route policy that should determine the weight contributed by a new <*,G> or <S,G> membership request.

Command Default

Default weight for all groups is 1. By default, no route policy is configured to determine the weight of new <*,G> or <S,G> membership requests.

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

To limit the number of IGMP v2/v3 groups, in which the maximum number of concurrently allowed multicast channels must be configurable on a per EFP-basis and per PW-basis, configure group weighting.

IGMP snooping limits the membership on a bridge port to a configured maximum limit. This feature also supports IGMPv3 source groups and allows different weights to be assigned to individual groups or source groups. This enables the IPTV provider, for example, to associate standard and high- definition IPTV streams, as appropriate, to specific subscribers.

This feature does not limit the actual multicast bandwidth that may be transmitted on a port. Rather, it limits the number of IGMP groups and source-groups, of which a port can be a member. It is the responsibility of the IPTV operator to configure subscriber membership requests to the appropriate multicast flows.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure a group route policy for weighting new <*,G> or <S,G>membership requests:

```
Router# configure
Router(config)#igmp snooping profile
Router(config-igmp-snooping-profile)# group policy
policy name
```

```
Router# configure
Router(config)#mld snooping profile
Router(config-mld-snooping-profile)# group policy
policy name
```

Related Commands

Command	Description
access-group (snooping profile)	Instructs IGMP snooping to apply the specified access list filter to received membership reports
group limit	Specifies the group limit of a port for weighting purposes.
show run route-policy	Displays the route policy information.

igmp snooping profile

To create or change an IGMP snooping profile, or to attach an IGMP snooping profile to a bridge or a port, use the **igmp snooping profile** command in the appropriate configuration mode. To detach a profile from a bridge domain or port, use the **no** form of this command. To delete a profile from the database, use the **no** form of this command in global configuration mode.

igmp snooping profile *profile-name*
no igmp snooping

Syntax Description

profile-name	Name that uniquely identifies the IGMP snooping profile.

Command Default

IGMP snooping is inactive on a bridge domain until a profile is attached to the bridge domain.

Command Modes

Global configuration

L2 VPN bridge group bridge domain configuration

L2 VPN bridge group bridge domain interface configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command accomplishes different tasks depending on the configuration mode you are in when you issue it.

- In global configuration mode, this command creates and changes profiles.
- In L2 VPN bridge group bridge domain configuration mode, this command attaches profiles to bridge domains.

- In L2 VPN bridge group bridge domain interface configuration mode, this command attaches profiles to ports.

Use the **igmp snooping profile** command in global configuration mode to create a new IGMP snooping profile or to change an existing profile. The command enters you into IGMP snooping profile configuration mode, from which you can issue commands that configure IGMP snooping.

The minimum configuration is an empty profile. An empty profile enables IGMP snooping with a default configuration.

To enable IGMP snooping on a bridge domain, you must attach a profile to the bridge domain. To disable IGMP snooping on a bridge domain, detach the profile from the bridge domain.

To attach a profile to a bridge domain, use the **igmp snooping profile** command in Layer-2 VPN bridge group bridge domain configuration mode. At the bridge domain level, only one IGMP snooping profile can be attached to a bridge.

If a profile attached to a bridge domain contains port-specific configuration options, the values apply to all of the ports under the bridge, unless a port-specific profile is attached to one of the ports. In that case, the port with the attached profile is configured using only the commands in the port profile, and any port configurations in the bridge profile are ignored.

Optionally, profiles can be attached to specific ports under a bridge domain. To attach a profile to a port, use the **igmp snooping profile** command in Layer-2 VPN bridge group bridge domain interface configuration mode. Each port can have only one port-specific profile attached to it.

IGMP snooping must be enabled on the bridge domain for any port-specific configurations to take effect. When a profile is attached to a port, IGMP snooping reconfigures that port, disregarding any port configurations that may exist in the bridge-level profile.

To detach a profile from a bridge domain, use the **no** form of this command in Layer-2 VPN bridge group bridge domain configuration mode. To detach a profile from a port, use the **no** form of this command in the interface configuration mode under the bridge domain.

When you detach a profile from a bridge domain or a port, the profile still exists and is available for use at a later time.

Detaching a profile has the following results:

- If you detach a profile from a bridge domain, IGMP snooping is deactivated in the bridge domain.
- If you detach a profile from a port, IGMP snooping configuration values for the port are instantiated from the bridge domain profile.

An active profile is one that is currently attached.

If you need to change an active profile, you must detach it from all bridges or ports, change it, and reattach it. An alternate procedure is to create a new profile incorporating the desired changes, detach the existing one, and immediately attach the new one.

To access an existing profile, use the **igmp snooping profile** command with the existing *profile-name* in global configuration mode. The command enters you into IGMP snooping profile configuration mode, from which you can issue commands to add to the current configuration or enter the **no** form of existing commands to delete them from the configuration.

To delete a profile from the router database, use the **no** form of this command in global configuration mode.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to create a new IGMP snooping profile or edit an existing profile:

```
Router(config)# igmp snooping profile Profile-1
Router(config-igmp-snooping-profile)#
```

The following example attaches a profile to the bridge domain ISP1:

```
Router(config)# l2vpn
Router(config-l2vpn)# bridge group GRP1
Router(config-l2vpn-bg)# bridge-domain ISP1
Router(config-l2vpn-bg-bd)# igmp snooping profile profile-1
```

The following example attaches a profile to the GigabitEthernet 0/1/1/1 port:

```
Router(config)# l2vpn
Router(config-l2vpn)# bridge group GRP1
Router(config-l2vpn-bg)# bridge-domain ISP1
Router(config-l2vpn-bg-bd)# interface GigabitEthernet 0/1/1/1
Router(config-l2vpn-bg-bd-if)# igmp snooping profile mrouter-port-profile
Router(config-l2vpn-bg-bd-if)# commit
```

immediate-leave

To configure fast leave processing on a port for IGMPv2 / MLDv1 queriers, use the **immediate-leave** command in the appropriate snooping profile configuration mode. To remove the functionality, use the **no** form of this command.

immediate-leave
no immediate-leave

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Immediate leave is an optional port-level configuration parameter. Immediate leave processing causes IGMP snooping to remove a Layer-2 interface from the forwarding table entry immediately, without first sending IGMP group-specific queries to the interface. Upon receiving an IGMP leave message, IGMP snooping immediately removes the interface from the Layer-2 forwarding table entry for that multicast group, unless a multicast router was learned on the port.

Immediate leave processing improves leave latency but is appropriate only when one receiver is configured on a port. For example, immediate leave is appropriate in the following situations:

- Point-to-point configurations, such as an IPTV channel receiver.
- Downstream DSLAMs with proxy reporting.

⚠

Caution Do not use immediate leave on a port when the possibility exists for more than one receiver per port. Doing so could prevent an interested receiver from receiving traffic. For example, immediate leave is not appropriate in a LAN.

Immediate leave processing is a port-level option. You can configure this option explicitly per port in port profiles or in the bridge domain profile, in which case it applies to all ports under the bridge.

For MLD snooping - Immediate-leave should only be configured if there is a single MLD host on the port. Immediate-leave is implicitly enabled for MLDv2, if explicit-tracking is enabled.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to add immediate leave to a profile:

```
Router(config-igmp-snooping-profile)# immediate-leave

Router(config-mld-snooping-profile)# immediate-leave
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.

internal-querier

To configure an internal IGMP /MLD querier on a bridge domain, use the **internal-querier** command in the appropriate snooping profile configuration mode. To disable the internal querier, use the **no** form of this command.

internal-querier
no internal-querier

Syntax Description

This command has no arguments or keywords.

Command Default

The internal querier is disabled by default.

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to configure an IGMP querier in a bridge domain where no external querier exists. An internal querier injects query packets into the bridge domain.

In a network where IP multicast routing is configured, the IP multicast router acts as the IGMP querier. In situations when no mrouter port exists in the bridge domain (because the multicast traffic does not need to be routed), but local multicast sources exist, you must configure an internal querier to implement IGMP snooping. The internal querier solicits membership reports from hosts in the bridge domain so that IGMP snooping can build constrained multicast forwarding tables for the multicast traffic within the bridge domain.

An internal querier might also be useful when there are interoperability issues that prevent IGMP snooping from working correctly with an external querier. In this case, you can:

1. Prevent the uncooperative external querier from being discovered by placing the **router-guard** command on that port.
2. Configure an internal querier to learn group membership interests from the ports in the bridge domain.
3. Configure static mrouter ports to receive multicast traffic.

The minimum configuration for an internal querier is as follows. Both of the following commands are required.

- Add the **internal-querier** command to a profile attached to the bridge domain. This command configures the internal querier with the default configuration.
- Add the **system-ip-address** command to a profile attached to the bridge domain to configure an address other than the default 0.0.0.0.

You can disable the internal querier (using the **no** form of the **internal-querier** command) without removing any other internal querier commands. The additional internal querier commands are ignored in that case.

The scope for the **internal-querier** command is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

The local IGMP snooping process responds to the internal querier's general queries. In particular, the IGMPv3 proxy (if enabled) generates a current-state report and forwards it to all mrouters. For IGMPv2 or when the IGMPv3 proxy is disabled, IGMP snooping generates current-state reports for static group state only.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example activates an internal querier with default configuration values:

```
Router(config-igmp-snooping-profile)# system-ip-address 10.1.1.1
Router(config-igmp-snooping-profile)# internal-querier
```

```
Router(config-mld-snooping-profile)# internal-querier
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
internal-querier max-response-time	Configures the maximum response time advertised by the internal querier.
internal-querier query-interval	Configures the time between general queries issued by the internal querier.
internal-querier robustness-variable	Configures the robustness variable for the internal querier.
internal-querier tcn query count	Configures the number of queries the internal querier sends after receiving a group leave from IGMP snooping.
internal-querier tcn query interval	Configures the time between queries that the internal querier sends after receiving a group leave from IGMP snooping.
internal-querier timer expiry	Configure the time IGMP snooping waits to receive messages from an external querier before making the internal querier the active querier
internal-querier version	Configures the IGMP version that the internal querier runs,.
mrouter	Sets a port to receive query packets.
router-guard	Sets a port to block query packets.
system-ip-address	Configures an IP address for IGMP snooping use.

internal-querier (MLD)

To configure an internal MLD querier on a bridge domain, use the **internal querier** command in the MLD snooping profile configuration mode. To disable the internal querier, use the **no** form of the command.

internal-querier

nointernal-querier

Syntax Description

This command has no keywords or arguments.

Command Default

The internal querier is disabled by default.

Command Modes

MLD snooping profile configuration mode

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The internal-querier is disabled by default. However, if PIMv6 snooping is active in the domain, then the internal-querier is active. If queries are received from another querier in the domain, MLD querier election is performed (where the lowest ip-address wins). If the internal-querier is the election-loser, then a timer (the other-querier-present-timer) is run for the timer expiry interval. If this timer expires before another query is received from the election-winner, then the internal-querier becomes the querier.

Task ID

Task ID	Operation
l2vpn	read, write

Example

The following example shows how to use the internal-querier command:

```
Router(config-mld-snooping-profile) # internal-querier
```

internal-querier max-response-time

To configure the maximum response time advertised by the internal querier, use the **internal-querier max-response-time** command in the appropriate snooping profile configuration mode. To return to the default value, use the **no** form of this command.

internal-querier max-response-time *seconds*
no internal-querier max-response-time

Syntax Description

seconds	Configures the maximum response time included in queries from the internal querier. Valid values are from 1 to 25 (seconds).

Command Default

10 (seconds)

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

The maximum response time (MRT) is the amount of time during which receivers are required to report their membership state.

In addition, the maximum response time is used in the calculation of the Group Management Interval (GMI). GMI controls when IGMP snooping expires stale group membership states. See the "Implementing IGMP Snooping on Cisco XR 12000 Series RouterCisco CRS RouterCisco ASR 9000 Series RouterCisco NCS 6000 Series RouterCisco NCS 4000 Series Router Cisco NCS 5500 Series Router Cisco NCS 5000 Series RouterCisco NCS 540 Series Router" module in the *Cisco XR 12000 Series RoutersCisco CRS RoutersCisco ASR 9000 Series RoutersCisco NCS 6000 Series RoutersCisco NCS 4000 Series RouterCisco NCS 5500 Series Routers Cisco NCS 5000 Series Routers Cisco 8000 Series RoutersCisco NCS 540 Series Routers Multicast Configuration Guide* for more information about the GMI.

The maximum response time is advertised in general queries issued by the internal querier.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example configures a maximum response time for the internal querier, overriding the default value:

```
Router(config-igmp-snooping-profile)# internal-querier max-response-time 5
```

```
Router(config-mld-snooping-profile)# internal-querier max-response-time 5
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
internal-querier	Enables an internal querier in the bridge domain.

internal-querier query-interval

To configure the time between general queries issued by the internal querier, use the **internal-querier query-interval** command in the appropriate snooping profile configuration mode. To return to the default value, use the **no** form of this command.

internal-querier query-interval *seconds*
no internal-querier query-interval

Syntax Description

seconds	Configures the number of seconds between general queries for membership reports issued by the internal querier. Valid values are from 1 to 18000 (seconds).

Command Default

60 (seconds). This is a nonstandard default value.

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When the internal querier is the active querier in the domain, it solicits membership reports by sending IGMP general queries at the interval specified by this command on every active port in the bridge domain.

Note Cisco IOS and Cisco IOS XR software use the non-standard default value of 60 for query interval.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example sets a query interval for the internal querier, overriding the default value:

```
Router(config-igmp-snooping-profile)# internal-querier query-interval 125
```

```
Router(config-mld-snooping-profile)# internal-querier query-interval 125
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
internal-querier	Enables an internal querier in the bridge domain.

internal-querier robustness-variable

To configure the robustness variable for the internal querier, use the **internal-querier robustness-variable** command in the appropriate snooping profile configuration mode. To return to the default value, use the **no** form of this command.

internal-querier robustness-variable *number*
no internal-querier robustness-variable

Syntax Description

number	Valid values are from 1 to 7 (for IGMP snooping). For MLD snooping, range is from 1 to 3.

Command Default

2

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to set the internal querier's robustness variable to a value other than the default configuration value. If the internal querier is running IGMPv3, it advertises the robustness variable in its general queries.

In addition, the robustness variable is used in the calculation of the Group Management Interval (GMI). GMI controls when IGMP snooping expires stale group membership states. See the "Implementing IGMP Snooping on Cisco XR 12000 Series RoutersCisco CRS RoutersCisco ASR 9000 Series RoutersCisco NCS 6000 Series RoutersCisco NCS 4000 Series RouterCisco NCS 5500 Series Routers Cisco NCS 5000 Series Routers Cisco 8000 Series RoutersCisco NCS 540 Series Routers" module in the *Cisco XR 12000 Series RoutersCisco CRS RoutersCisco ASR 9000 Series RoutersCisco NCS 6000 Series RoutersCisco NCS 4000 Series RouterCisco NCS 5500 Series Routers Cisco NCS 5000 Series Routers Cisco 8000 Series RoutersCisco NCS 540 Series Routers Multicast Configuration Guide* for more information about GMI.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example configures the robustness variable for an internal querier, overriding the default value:

```
Router(config-igmp-snooping-profile)# internal-querier robustness-variable 3
```

```
Router(config-mld-snooping-profile)# internal-querier robustness-variable 3
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
internal-querier	Enables an internal querier in the bridge domain.

internal-querier tcn query count

To configure the number of queries the internal querier sends after receiving a group leave from the snooping process, use the **internal-querier tcn query count** command in the appropriate snooping profile configuration mode. To return to the default value, use the **no** form of this command.

internal-querier tcn query count *number*
no internal-querier tcn query count

Syntax Description

number	Configures the number of queries the internal querier sends after receiving a group leave from IGMP snooping. Valid values are from 0 to 3. The time between queries is controlled by the **internal-querier tcn query interval** command.

Command Default

2

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Snooping reacts to Spanning Tree Protocol (STP) topology change notifications (TCNs) by flooding all multicast traffic and sending group leaves to expedite relearning. When the internal querier receives a group leave, it sends queries to solicit membership reports. This command configures the number of queries to send. The time between queries is controlled by the **internal-querier tcn query interval** command.

If you set **internal-querier tcn query count** to 0, the internal querier does not respond to group leaves.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example configures the tcn query count for an internal querier, overriding the default value:

```
Router(config-igmp-snooping-profile)# internal-querier tcn query count 3
```

```
Router(config-mld-snooping-profile)# internal-querier tcn query count 3
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
internal-querier	Enables an internal querier in the bridge domain.
internal-querier tcn query interval	Configures the interval between queries the internal querier sends after receiving a group leave from IGMP snooping.

internal-querier tcn query interval

To configure the time between queries that the internal querier sends after receiving a group leave from IGMP / MLD snooping, use the **internal-querier tcn query interval** command in the appropriate snooping profile configuration mode. To return to the default value, use the **no** form of this command.

internal-querier tcn query interval *seconds*
no internal-querier tcn query interval

Syntax Description

seconds	Configures the time between queries. Valid values are from 1 to 18000.

Command Default

10

Command Modes

IGMP snooping profile configuration

MLD snooping configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Snooping reacts to STP topology change notifications by flooding all multicast traffic and sending group leaves to expedite relearning. When the internal querier receives the group leave, it sends queries to solicit membership reports. This command configures the time between queries.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example configures the tcn query interval for an internal querier, overriding the default value:

```
Router(config-igmp-snooping-profile)# internal-querier tcn query interval 100

Router(config-mld-snooping-profile)# internal-querier tcn query interval 100
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
internal-querier	Enables an internal querier in the bridge domain.
internal-querier tcn query count	Configures the number of queries the internal querier sends after receiving a group leave from IGMP snooping.

internal-querier timer expiry

To configure the time IGMP /MLD snooping waits to receive messages from an external querier before making the internal querier the active querier, use the **internal-querier timer expiry** command in the appropriate snooping profile configuration mode. To return to the default value, use the **no** form of this command.

internal-querier timer expiry *seconds*
no internal-querier timer expiry

Syntax Description

seconds	The time IGMP snooping waits to receive messages from an external querier before making the internal querier the active querier. Valid values are from 60 to 300 (seconds).

Command Default

125 (seconds), as defined in RFC-3376, Section 8.5:

*(robustness-variable * query-interval)* + ½(*max-response-time*)

Using the default values for all components:

(2 * 60) + ½ (10) = 125

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

A bridge domain can have only one active querier at a time. If the internal querier receives queries from another querier in a bridge domain, it performs querier election. The lowest IP address wins. If the internal querier is the election loser, the snooping technique sets a timer to the **internal-querier timer expiry** value. If this timer expires before another query is received from the election winner, the internal querier becomes the active querier.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example configures the timer expiry value for an internal querier, overriding the default value:

```
Router(config-igmp-snooping-profile)# internal-querier timer expiry 100
```

```
Router(config-mld-snooping-profile)# internal-querier timer expiry 100
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
internal-querier	Enables an internal querier in the bridge domain.

internal-querier version

To configure the version for the internal querier, use the **internal-querier version** command in the appropriate snooping profile configuration mode. To return to the default value, use the **no** form of this command.

internal-querier version *version*
no internal-querier version

Syntax Description

version	Controls the version of the internal querier. Valid values are 2 or 3 (for IGMP) and 1 or 2 (for MLD).

Command Default

3

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The internal querier sends IGMP queries on the bridge domain. This command sets the internal querier to run as either an IGMPv2 or IGMPv3 querier.

This command sets the internal querier to run as either a MLDv1 or MLDv2 querier.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example configures the internal querier to send version2 queries, overriding the default value:

```
Router(config-igmp-snooping-profile)# internal-querier version 2
```

```
Router(config-mld-snooping-profile)# internal-querier version 2
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
internal-querier	Enables an internal querier in the bridge domain.

last-member-query count

To configure the number of group-specific queries IGMP snooping sends in response to a leave message, use the **last-member-query count** command in IGMP snooping profile configuration mode. To return to the default value, use the **no** form of this command.

last-member-query count *number*
no last-member-query count

Syntax Description

number	Specifies the number of queries IGMP snooping sends in response to a leave message. Valid values are from 1 to 7.

Command Default

2

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Last member query is the default group leave processing method used by IGMP snooping. With last member query processing, IGMP snooping processes leave messages as follows:

- IGMP snooping sends group-specific queries on the port that receives the leave message to determine if any other devices connected to that interface are interested in traffic for the specified multicast group. Using the following two configuration commands, you can control the latency between the request for a leave and the actual leave:
  - **last-member-query-count** command—Controls the number of group-specific queries IGMP snooping sends in response to a leave message.
  - **last-member-query-interval** command—Controls the amount of time between group-specific queries.
- If IGMP snooping does not receive an IGMP Join message in response to group-specific queries, it assumes that no other devices connected to the port are interested in receiving traffic for this multicast group, and it removes the port from its Layer-2 forwarding table entry for that multicast group.
- If the leave message was from the only remaining port, IGMP snooping removes the group entry and generates an IGMP leave to the multicast routers.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example configures the number of queries that IGMP snooping sends in response to a leave, overriding the default value:

```
Router(config-igmp-snooping-profile)# last-member-query count 1
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
last-member-query interval	Configures the time between queries sent in response to an IGMP leave.

last-member-query count (MLD)

To configure the number of group-specific queries MLD snooping sends in response to a leave message, use the **last-member-query count** command in MLD snooping profile configuration mode. To return to the default value, use the **no** form of this command.

last-member-query count *number*
no last-member-query count *number*

Syntax Description

number	Specifies the number of queries MLD snooping sends in response to a leave message. Range is from 1 to 7.

Command Default

The default count is 2.

Command Modes

MLD snooping profile configuration mode.

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Last member query is the default group leave processing method used by MLD snooping. MLD snooping sends group-specific queries on the port that receives the leave message to determine if any other devices connected to that interface are interested in traffic for the specified multicast group. Using the following two configuration commands, you can control the latency between the request for a leave and the actual leave:**last-member-query count** and **last-member-query interval**.

Task ID

Task ID	Operation
l2vpn	read, write

Example

The following example shows how to set the last member query count to 5:

```
Router(config-mld-snooping-profile) # last-member-query count 5
```

last-member-query interval

To configure the amount of time between group-specific queries, use the **last-member-query interval** command in IGMP snooping profile configuration mode. To return to the default value, use the **no** form of this command.

last-member-query interval *milliseconds*
no last-member-query interval

Syntax Description

milliseconds	Specifies the time between queries that IGMP snooping sends in response to a leave message. Valid values are from 100 to 5000 (milliseconds).

Command Default

1000 (milliseconds)

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Last member query is the default group leave processing method used by IGMP snooping. With last member query processing, IGMP snooping processes leave messages as follows:

- IGMP snooping sends group-specific queries on the port that receives the leave message to determine if any other devices connected to that interface are interested in traffic for the specified multicast group. Using the following two configuration commands, you can control the latency between the request for a leave and the actual leave:
  - **last-member-query-count** command—Controls the number of group-specific queries IGMP snooping sends in response to a leave message.
  - **last-member-query-interval** command—Controls the amount of time between group-specific queries.
- If IGMP snooping does not receive an IGMP Join message in response to group-specific queries, it assumes that no other devices connected to the port are interested in receiving traffic for this multicast group, and it removes the port from its Layer-2 forwarding table entry for that multicast group.
- If the leave message was from the only remaining port, IGMP snooping removes the group entry and generates an IGMP leave to the multicast routers.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example configures the interval between queries that IGMP snooping sends in response to a leave, overriding the default value:

```
Router(config-igmp-snooping-profile)# last-member-query interval 2000
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
last-member-query count	Configures the number of queries sent in response to an IGMP leave.

last-member-query interval (MLD)

To configure the amount of time between group-specific queries, use the **last-member-query interval** command in MLD snooping profile configuration mode. To return to the default value, use the **no** form of this command.

last-member-query interval *milliseconds*
no last-member-query interval *milliseconds*

Syntax Description

milliseconds	Specifies the time between queries that MLD snooping sends in response to a leave message. Valid values are from 100 to 5000 (milliseconds).

Command Default

1000 milliseconds

Command Modes

MLD snooping profile

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
l2vpn	read, write

Example

The following example shows how to set the last member query interval to 2000 ms:

```
Router(config-mld-snooping-profile) # last-member-query interval 2000
```

minimum-version

To change the IGMP versions supported by IGMP snooping, use the **minimum-version** command in IGMP snooping profile configuration mode. To return to the default value, use the **no** form of this command.

minimum-version *number*
no minimum-version

Syntax Description

number	Specifies the minimum IGMP version supported by IGMP snooping. Supported values are: • 2—Snoops messages from IGMPv2 and IGMPv3. • 3—Only IGMPv3 messages are snooped. All IGMPv2 messages are ignored by IGMP snooping.

Command Default

2 (supporting IGMPv2 and IGMPv3)

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **minimum-version** command controls which IGMP versions are supported by IGMP snooping in the bridge domain.

- When minimum-version is 2, IGMP snooping intercepts IGMPv2 and IGMPv3 messages. This is the default value.
- When minimum-version is 3, IGMP snooping intercepts only IGMPv3 messages and drops all IGMPv2 messages.

The scope for this configuration option is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example configures IGMP snooping to support only IGMPv3 and to ignore IGMPv2 reports and queries:

```
Router(config-igmp-snooping-profile)# minimum-version 3
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.

minimum version (MLD)

To enable MLD snooping to filter out all packets of MLD versions, less than the minimum-version, use the **minimum version** command in the MLD snooping profile configuration mode. To disable minimum version, use the **no** form of the command.

minimum-version *number*
nominimum-version *number*

Syntax Description

number	Specifies the MLD version supported by MLD snooping. The available values are - 1 and 2.

Command Default

By default, MLD snooping supports minimum-version 1.

Command Modes

MLD snooping profile configuration mode.

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If minimum version is set to 2, all MLD packets set to (minimum version) 1, are dropped.

Task ID

Task ID	Operation
multicast	read, write

Example

This example shows how to use the **minimum version** command:

```
Router#(config-mld-snooping-profile) # minimum-version 2
```

mld snooping profile

To enter Multicast Listener Discovery (MLD) snooping profile configuration mode, use the **mld snooping profile** command in configuration mode. To exit from the MLD snooping profile configuration mode, use the **no**form of the command.

mld snooping profile *profile-name*
nomld snooping profile *profile-name*

Syntax Description

profile-name	Name that uniquely identifies the MLD snooping profile.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
multicast	read, write

Example

This example shows how to use the **mld snooping profile** command:

```
Router(config) #mld snooping profile p1
```

mrouter

To statically configure a port to receive query packets, use the **mrouter** command in the appropriate snooping profile configuration mode. To remove the configuration, use the **no** form of this command.

mrouter
no mrouter

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can statically configure a port as an mrouter port with the **mrouter** command.

You can use the **router-guard** and the **mrouter** commands on the same port to configure a guarded port as a static mrouter. For example:

- In situations where there are a large number of downstream host ports, you may want to block dynamic mrouter discovery and configure static mrouters. In this case, configure the router guard feature at the domain level. By default, it will be applied to all ports, including the (typically) large number of downstream host ports. Then use another profile without router guard configured for the relatively few upstream ports on which you want to permit dynamic mrouter discovery or configure static mrouters.
- In situations when incompatibilities with non-Cisco equipment prevents correct dynamic discovery, you can disable all attempts for dynamic discovery using the router guard feature, and statically configure the mrouter.

  If you are using the router guard feature because there is an incompatible IGMP router on the port, you should also configure the **mrouter** command on the port to ensure that the router receives snooping reports and multicast flows.

The scope of this command is port level. If you use this command in a profile attached to a bridge domain, you are configuring all ports as mrouter ports.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to add static mrouter configuration to a profile:

```
Router(config-igmp-snooping-profile)# mrouter
Router(config-mld-snooping-profile)# mrouter
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
internal-querier	Sets a port to send query packets to bridge domain ports.
router-guard	Blocks query packets on the port.

nv satellite offload ipv4 multicast enable

To enable the IPv4 Multicast Satellite Offloading, use the nv satellite offload ipv4 multicast enable command in L2vpn bridge domain, nv satellite configuration sub mode.

nv satellite offload ipv4 multicast enable

Command Default

By default, the configuration command is disabled.

Command Modes

L2vpn bridge domain nv satellite configuration sub mode

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

Use this command only when you want to enable replication of IPv4 multicast on the satellite nodes. When set, the replication will be offloaded to the satellite devices that have offload eligible ports configured under this bridge-domain.

Task ID

Task ID	Operation
multicast	read, write

Example

This example shows how to enable the IPv4 Multicast Offload feature on the Satellite nV System:

```
RP/0/0/CPU0:ios(config)#l2vpn
RP/0/0/CPU0:ios(config-l2vpn)#bridge group <bg>
RP/0/0/CPU0:ios(config-l2vpn-bg)#bridge-domain <bd>
RP/0/0/CPU0:ios(config-l2vpn-bg-bd)#nv
RP/0/0/CPU0:ios(config-l2vpn-bg-bd-nv)#nv satellite offload ipv4 multicast enable
```

querier query-interval

To configure the query interval for processing IGMPv2 membership states, use the **querier query-interval** command in IGMP snooping profile configuration mode. To return to the default setting, use the **no** form of this command.

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

Syntax Description

seconds	Specifies the integer to use as the query interval in calculations performed by IGMP snooping when processing IGMPv2 messages. **Note** IGMPv3 messages convey the query interval from the querier. Valid values are integers from 1 to 18000 (seconds). The default is 60.

Command Default

60 (seconds). This is a nonstandard default value.

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Query interval is the interval between general queries and is used in the calculated group management interval (GMI). GMI controls when IGMP snooping expires stale group membership states. For more information about GMI, see the "Implementing IGMP Snooping on Cisco XR 12000 Series RoutersCisco CRS RoutersCisco ASR 9000 Series RoutersCisco NCS 6000 Series RoutersCisco NCS 4000 Series RouterCisco NCS 5500 Series Routers Cisco NCS 5000 Series Routers Cisco 8000 Series RoutersCisco NCS 540 Series Routers" module in the *Cisco XR 12000 Series RoutersCisco CRS RoutersCisco ASR 9000 Series RoutersCisco NCS 6000 Series RoutersCisco NCS 4000 Series RouterCisco NCS 5500 Series Routers Cisco NCS 5000 Series Routers Cisco 8000 Series RoutersCisco NCS 540 Series Routers Multicast Configuration Guide*.

If the querier is running IGMPv2, IGMP snooping uses the IGMP snooping configured values for robustness variable and query interval. These parameter values must match the configured values for the querier. In most cases, if you are interacting with other Cisco routers, you should not need to explicitly configure these values—the default values for IGMP snooping should match the default values of the querier. If they do not, use the **querier robustness-variable** and **querier query-interval** commands to configure matching values.

Note Cisco IOS and Cisco IOS XR software use the nonstandard default value of 60 for query interval.

Note IGMPv3 general queries convey values for robustness variable and query interval (QRV and QQI, respectively). IGMP snooping uses the values from the query, making the IGMP snooping GMI exactly match that of the querier.

The scope for this command is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to add the command to a profile that configures the query interval:

```
Router(config-igmp-snooping-profile)# querier query-interval 1500
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
internal-querier robustness-variable	Configures a robustness variable for an internal querier.
internal-querier query-interval	Configures the query interval for an internal querier.
querier robustness-variable	Configures the robustness variable required for processing IGMPv2 membership reports.

querier robustness-variable

To configure the robustness variable for processing IGMPv2 membership states, use the **querier robustness-variable** command in IGMP snooping profile configuration mode. To return to the default setting, use the **no** form of this command.

querier robustness-variable *robustness-number*
no querier robustness-variable

Syntax Description

robustness-number	Specifies the integer to use as the robustness variable in calculations performed by IGMP snooping when processing IGMPv2 messages. **Note** IGMPv3 messages convey the robustness variable from the querier. Valid values are integers from 1 to 7. The default is 2.

Command Default

2

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Robustness variable is an integer used to influence the calculated GMI. GMI controls when IGMP snooping expires stale group membership states. For more information about GMI, see the "Implementing IGMP Snooping on Cisco XR 12000 Series RoutersCisco CRS RoutersCisco ASR 9000 Series RoutersCisco NCS 6000 Series RoutersCisco NCS 4000 Series RouterCisco NCS 5500 Series Routers Cisco NCS 5000 Series Routers Cisco 8000 Series RoutersCisco NCS 540 Series Routers" module in the *Cisco XR 12000 Series RoutersCisco CRS RoutersCisco ASR 9000 Series RoutersCisco NCS 6000 Series RoutersCisco NCS 4000 Series RouterCisco NCS 5500 Series Routers Cisco NCS 5000 Series Routers Cisco 8000 Series RoutersCisco NCS 540 Series Routers Multicast Configuration Guide*.

If the querier is running IGMPv2, IGMP snooping uses the IGMP snooping configured values for robustness variable and query interval. These parameter values must match the configured values for the querier. In most cases, if you are interacting with other Cisco routers, you should not need to explicitly configure these values—the default values for IGMP snooping should match the default values of the querier. If they do not, use the **querier robustness-variable** and **querier query-interval** commands to configure matching values.

Note IGMPv3 general queries convey values for robustness variable and query interval (QRV and QQI, respectively). IGMP snooping uses the values from the query, making the IGMP snooping GMI exactly match that of the querier.

The scope for this command is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to add the command to a profile that configures the robustness variable:

```
Router(config-igmp-snooping-profile)# querier robustness-variable 1
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
internal-querier robustness-variable	Configures a robustness variable for an internal querier.
internal-querier query-interval	Configures the query interval for an internal querier.
querier query-interval	Configures the query interval required for processing IGMPv2 membership reports.

redundancy iccp-group report-standby-state disable

To enable IGMP Snooping for generating unsolicited state-change reports only when the port transitions from standby to active, use the **redundancy iccp-group report-standby-state disable** command in IGMP snooping profile configuration mode. To use the default behavior, use the **no** form of this command.

redundancy iccp-group report-standby-state disable
no redundancy iccp-group report-standby-state disable

Note By default, IGMP Snooping generates state-change and current-state reports to all mulicast routers to reflect state that exists on standby MC-LAG ports only. This causes the upstream sources to forward multicast streams to the router, where they will be dropped (on egress side).

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

IGMP snooping profile configuration (config-igmp-snooping-profile)

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note This command is applicable only when MC-LAG is configured.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example shows how to use the **redundancy iccp-group report-standby-state disable** command:

```
Router(config-igmp-snooping-profile)# redundancy iccp-group report-standby-state disable
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.

report-suppression disable

To disable IGMPv2 report suppression or IGMPv3 proxy reporting, use the **report-suppression disable** command in IGMP snooping profile configuration mode. To enable report suppression or proxy reporting functionality, use the **no** form of this command.

report-suppression disable
no report-suppression disable

Syntax Description

This command has no arguments or keywords.

Command Default

Report suppression and proxy reporting, whichever is appropriate, are enabled by default

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to disable report suppression for IGMPv2 queriers and proxy reporting for IGMPv3 queriers.

Both features are enabled by default, with the following results:

- IGMPv2 report suppression—For IGMPv2 bridge domain queriers, IGMP snooping suppresses reports from a host if the report was previously forwarded from another host. IGMP snooping sends only the first join and last leave to mrouter ports.

- IGMPv3 proxy reporting—For IGMPv3 bridge domain queriers, IGMP snooping acts as a proxy, generating state change reports from a proxy reporting IP address. You can configure that IP address using the **system-ip-address** command. The default is 0.0.0.0.

These features are enabled and disabled per bridge domain. This command is ignored if it appears in a profile attached to a port.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to add the command to a profile to turn off report suppression and proxy reporting:

```
Router(config-igmp-snooping-profile)# report-suppression disable
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
system-ip-address	Configures an IP address used by IGMP snooping.

report-suppression disable(MLD)

To minimize the number of MLD reports sent to the mrouters, use the **report-suppression disable** command in the MLD snooping profile configuration mode.

report-suppression disable
noreport-suppression disable

Syntax Description

This command has no keywords or arguments.

Command Default

By default, report suppression is enabled.

Command Modes

MLD snooping profile configuration mode.

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The report suppression command instructs MLD Snooping to suppress the forwarding of reports from individual hosts and instead to send the first-join and last-leave reports to the mrouters.

If the querier in the BD is running at MLD version 1, then report-suppression is performed and the snooper suppresses reports from a host if it has already forwarded the same report from another host. If the querier is on version 2, then proxy-reporting is performed. In this mode, the snooper acts as a proxy, generating reports from the proxy reporting IP address.

Task ID

Task ID	Operation
multicast	read, write

Example

This example shows how to use the report suppression disable command:

```
Router(config-mld-snooping-profile)# report suppression disable
```

router-alert-check disable

To disable the IGMP snooping check for the presence of the router alert option in the IP packet header, use the **router-alert-check disable** command in IGMP snooping profile configuration mode. To enable this functionality after a disable, use the **no** form of this command.

router-alert-check disable
no router-alert-check disable

Syntax Description

This command has no arguments or keywords.

Command Default

The router alert check feature is enabled by default.

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

By default, IGMP snooping checks for the presence of the router alert option in the IP packet header of the IGMP message and drops packets that do not include this option. If your network performs this validation elsewhere, you can disable this IGMP snooping validation.

You can disable this check using the **router-alert-check disable** command, in which case IGMP snooping does perform the validation before processing the message.

The scope for this configuration option is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to add the command to a profile that turns off the router alert check:

```
Router(config-igmp-snooping-profile)# router-alert-check disable
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.

router-guard

To block a port from receiving query packets, use the **router-guard** command in the appropriate snooping profile configuration mode. To remove the restriction, use the **no** form of this command.

router-guard
no router-guard

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Router guard is a security feature that prevents malicious users from making a host port into an mrouter port. (This undesirable behavior is known as spoofing.) When a port is protected with the **router-guard** command, it cannot be dynamically discovered as an mrouter. When router guard is on a port, IGMP snooping filters protocol packets sent to the port and discards any that are multicast router control packets.

Caution If you add the **router-guard** command in a bridge domain profile, you disable dynamic discovery of all mrouters in that bridge domain.

You can use the **router-guard** and the **mrouter** commands on the same port to configure a guarded port as a static mrouter. For example:

- In situations where there are a large number of downstream host ports, you may want to block dynamic mrouter discovery and configure static mrouters. In this case, configure the router guard feature at the domain level. By default, it will be applied to all ports, including the (typically) large number of downstream host ports. Then use another profile without router guard configured for the relatively few upstream ports on which you want to permit dynamic mrouter discovery or configure static mrouters.
- In situations when incompatibilities with non-Cisco equipment prevents correct dynamic discovery, you can disable all attempts for dynamic discovery using the router guard feature, and statically configure the mrouter.

  If you are using the router guard feature because there is an incompatible IGMP router on the port, you should also configure the **mrouter** command on the port to ensure that the router receives reports and multicast flows.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to add the command to a profile that prevents a port from being dynamically discovered as an mrouter:

```
Router(config-igmp-snooping-profile)# router-guard

Router(config-mld-snooping-profile)# router-guard
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
internal-querier	Sets a port to send query packets to bridge domain ports.
mrouter	Sets a port to receive query packets.

show igmp snooping bridge-domain

To display IGMP snooping configuration information and traffic statistics for bridge domains, use the **show igmp snooping bridge-domain** command in EXEC mode.

show igmp snooping bridge-domain [*bridge-domain-name*] [**detail** [**statistics** [**include-zeroes**]]]

Syntax Description

bridge-domain-name	(Optional) Displays information only for the specified bridge domain.
detail	(Optional) Includes more details, including configuration information about the bridge domain querier.
statistics	(Optional) Includes traffic counters and statistics.
include-zeroes	(Optional) Includes all statistics, even if they are zero. Without this keyword, many statistics are omitted from the display when their values are zero.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays IGMP snooping information by bridge domain. Use the command without any keywords to display summary information about all bridge domains, in a single line per bridge domain.

Use optional keywords to request additional details and traffic statistics per bridge domain. You can also limit the display to a single bridge domain.

The **statistics** keyword displays IGMP traffic information, including IGMP queries, reports, and leaves. The three columns in the statistics section of the display are:

- Received—Number of packets received.
- Reinjected—Number of packets received, processed, and reinjected back into the forwarding path.
- Generated—Number of packets generated by the IGMP snooping application and injected into the forwarding path.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example shows the basic command without any keywords.

```
Router# show igmp snooping bridge-domain

Bridge Domain        Profile              Act  Ver  #Ports  #Mrtrs  #Grps   #SGs
-------------        -------              ---  ---  ------  ------  -----   ----
Group1:BD-1          profile1               Y   v2       8       2      5      0
```

```
Group1:BD-2                                N   --       0       0      0      0
Group1:BD-3         profile1               Y   v3       6       3      2      2
Group1:BD-4                                N   --       0       0      0      0
Group1:BD-5         profile1               Y   v3       2       1      1      0
```

The following example shows the summary line for a named bridge domain.

```
Router# show igmp snooping bridge-domain Group1:BD-1


Bridge Domain       Profile               Act  Ver  #Ports  #Mrtrs  #Grps   #SGs
-------------       -------               ---  ---  ------  ------  -----   ----
Group1:BD-1         profile1                Y   v2       8       2      5      0
```

The following example shows detailed information about all bridge domains:

```
Router# show igmp snooping bridge-domain detail

Bridge Domain       Profile               Act  Ver  #Ports  #Mrtrs  #Grps   #SGs
-------------       -------               ---  ---  ------  ------  -----   ----
1:1                 1                       Y   v3       3       0      1      0

  Profile Configured Attributes:
    System IP Address:                    10.1.1.1
    Minimum Version:                      2
    Report Suppression:                   Enabled
    Unsolicited Report Interval:          1000 (milliseconds)
    TCN Query Solicit:                    Disabled
    TCN Membership Sync:                  Disabled
    TCN Flood:                            Enabled
    TCN Flood Query Count:                2
    Router Alert Check:                   Enabled
    TTL Check:                            Enabled
    nV Mcast Offload:                     Enabled
    Internal Querier Support:             Enabled
    Internal Querier Version:             3
    Internal Querier Timeout:             0 (seconds)
    Internal Querier Interval:            60 (seconds)
    Internal Querier Max Response Time:   10.0 (seconds)
    Internal Querier Robustness:          2
    Internal Querier TCN Query Interval:  10 (seconds)
    Internal Querier TCN Query Count:     2
    Internal Querier TCN Query MRT:       0 (seconds)
    Querier Query Interval:               60 (seconds)
    Querier LMQ Interval:                 1000 (milliseconds)
    Querier LMQ Count:                    2
    Querier Robustness:                   2
    Startup Query Interval:               15 seconds
    Startup Query Count:                  2
    Startup Query Max Response Time:      10.0 seconds
    Mrouter Forwarding:                   Enabled
    P2MP Capability:                      Disabled
    Default IGMP Snooping profile:        Disabled
    IP Address:                           10.1.1.1
    Port:                                 Internal
    Version:                              v3
    Query Interval:                       60 seconds
    Robustness:                           2
    Max Resp Time:                        10.0 seconds
    Time since last G-Query:              12 seconds
  Mrouter Ports:                          0
  STP Forwarding Ports:                   0
  ICCP Group Ports:                       0
  Groups:                                 1
```

```
    Member Ports:                        2
  V3 Source Groups:                      0
    Static/Include/Exclude:              0/0/0
    Member Ports (Include/Exclude):      0/0
```

The following example displays traffic statistics with detailed information. The display omits many statistics whose values are zero.

```
Router# show igmp snooping bridge-domain Group1:BD-1 detail statistics
```

```
Bridge Domain        Profile              Act  Ver  #Ports  #Mrtrs  #Grps   #SGs
-------------        -------              ---  ---  ------  ------  -----   ----
Group1:BD-1          profile1               Y   v2       8       2      5      0

  Profile Configured Attributes:
    System IP Address:                   0.0.0.0
    Minimum Version:                     2
    Report Suppression:                  Enabled
    TCN Query Solicit:                   Disabled
   TCN Flood:                           Enabled
    TCN Flood Query Count:               2
   TCN Membership Sync:                 Disabled
  ICCP Group Report Standby State:     Disabled
    Router Alert Check:                  Enabled
    TTL Check:                           Enabled
   Unsolicited Report Interval:         1000 (milliseconds)
   Internal Querier Support:            Disabled
    Querier Query Interval:              60 (seconds)
    Querier LMQ Interval:                1000 (milliseconds)
    Querier LMQ Count:                   2
    Querier Robustness:                  2
   Startup Query Interval:              15 seconds
    Startup Query Count:                 2
    Startup Query Max Response Time:     10.0 seconds

  Querier:
    IP Address:                          192.1.1.10
    Port:                                GigabitEthernet0/2/0/10.1
    Version:                             v2
    Query Interval:                      60 seconds
    Robustness:                          2
    Max Resp Time:                       1.0 seconds
    Time since last G-Query:             3 seconds
  Mrouter Ports:                         2
    Dynamic:                             GigabitEthernet0/2/0/10.1
    Static:                              GigabitEthernet0/2/0/10.2
  STP Forwarding Ports:                  0
  Groups:                                5
    Member Ports:                        9
  V3 Source Groups:                      0
    Static/Include/Exclude:              0/0/0
    Member Ports (Include/Exclude):      0/0
  Traffic Statistics (elapsed time since last cleared 00:32:04):
                                     Received  Reinjected   Generated
    Messages:                             473         236         236
      IGMP General Queries:               237           0           0
      IGMP Group Specific Queries:          0           0           0
      IGMP G&S Specific Queries:            0           0           0
      IGMP V2 Reports:                    236         236         236
      IGMP V3 Reports:                      0           0           0
      IGMP V2 Leaves:                       0           0           0
      IGMP Global Leaves:                   0           -           0
      PIM Hellos:                          0           0           -
    Rx Packet Treatment:
      Packets Flooded:                                 0
      Packets Forwarded To Members:                    0
      Packets Forwarded To Mrouters:                 236
      Packets Consumed:                              237
    Rx Errors:
      None
    Tx Errors:
      None
  Startup Query Sync Statistics:
    None
  ICCP Group Port Statistics (elapsed time since last cleared 01:21:27):
    Port Created Standby:                              6
    Port Created Active:                               1
    Port Goes Standby:                                 6
    Port Goes Active:                                  7
  ICCP Traffic Statistics (elapsed time since last cleared 01:21:27):
    Rx Messages:
      App State TLVs:                              24006
      App State start of sync:                         6
      App State end of sync:                           6
      Request Sync TLVs:                               2
      Port Membership TLVs:                        24002
      Port Membership adds:                        23966
      Port Membership removes:                      8000
      Querier Info TLVs:                               2
    Rx Errors:
      App State sync TLVs ignored:                     2
    Tx Messages:
      App State replay attempts:                       2
      Request Sync TLVs:                               6
      Port Membership TLVs:                        16651
      Port Membership adds:                        16123
      Port Membership removes:                      5543
    Tx Errors:
      None
```

The following example shows details for all statistics regardless of whether their values are zero.

```
Router# show igmp snooping bridge-domain Group1:BD-1 detail statistics include-zeroes


Bridge Domain        Profile              Act  Ver  #Ports  #Mrtrs  #Grps   #SGs
-------------        -------              ---  ---  ------  ------  -----   ----
Group1:BD-1          profile1               Y   v2       8       2      5      0

  Profile Configured Attributes:
    System IP Address:                  0.0.0.0
    Minimum Version:                    2
    Report Suppression:                 Enabled
  TCN Query Solicit:                  Disabled
  TCN Flood:                          Enabled
    TCN Flood Query Count:              2
   TCN Membership Sync:                Disabled
  ICCP Group Report Standby State:    Disabled
  Router Alert Check:                 Enabled
    TTL Check:                          Enabled
    Internal Querier Support:           Disabled
    Querier Query Interval:             60 (seconds)
    Querier LMQ Interval:               1000 (milliseconds)
    Querier LMQ Count:                  2
    Querier Robustness:                 2
  Querier:
```

```
  IP Address:                          192.1.1.10
  Port:                                GigabitEthernet0/2/0/10.1
  Version:                             v2
  Query Interval:                      60 seconds
  Robustness:                          2
  Max Resp Time:                       1.0 seconds
  Time since last G-Query:             3 seconds
Mrouter Ports:                         2
  Dynamic:                             GigabitEthernet0/2/0/10.1
  Static:                              GigabitEthernet0/2/0/10.2
STP Forwarding Ports:                  0
Groups:                                5
  Member Ports:                        9
V3 Source Groups:                      0
  Static/Include/Exclude:              0/0/0
  Member Ports (Include/Exclude):      0/0
Traffic Statistics (elapsed time since last cleared 00:32:52):
                                   Received  Reinjected   Generated
  Messages:                             486         243         242
    IGMP General Queries:               243           0           0
    IGMP Group Specific Queries:          0           0           0
    IGMP G&S Specific Queries:            0           0           0
    IGMP V2 Reports:                    243         243         242
    IGMP V3 Reports:                      0           0           0
    IGMP V2 Leaves:                       0           0           0
    IGMP Global Leaves:                   0           -           0
    PIM Hellos:                           0           0           -
  Rx Packet Treatment:
    Packets Flooded:                                  0
    Packets Forwarded To Members:                     0
    Packets Forwarded To Mrouters:                  243
    Packets Consumed:                               243
  Reports Suppressed:                                 0
  IGMP Blocks Ignored in V2 Compat Mode:              0
  IGMP EX S-lists Ignored in V2 Compat Mode:          0
  Rx Errors:
    Packets On Inactive Bridge Domain:                0
    Packets On Inactive Port:                         0
    Packets Martian:                                  0
    Packets Bad Protocol:                             0
    Packets DA Not Multicast:                         0
    Packets Missing Router Alert:                     0
    Packets Missing Router Alert Drop:                0
    Packets Bad IGMP Checksum:                        0
    Packets TTL Not One:                              0
    Packets TTL Not One Drop:                         0
    Queries Too Short:                                0
    V1 Reports Too Short:                             0
    V2 Reports Too Short:                             0
    V3 Reports Too Short:                             0
    V2 Leaves Too Short:                              0
    IGMP Messages Unknown:                            0
    IGMP Messages GT Max Ver:                         0
    IGMP Messages LT Min Ver:                         0
    Queries Bad Source:                               0
    Queries Dropped by S/W Router Guard:              0
    General Queries DA Not All Nodes:                 0
    GS-Queries Invalid Group:                         0
    GS-Queries DA Not Group:                          0
    GS-Queries Not From Querier:                      0
    GS-Queries Unknown Group:                         0
    Reports Invalid Group:                            0
    Reports Link-Local Group:                         0
    Reports DA Not Group:                             0
```

```
      Reports No Querier:                             0
      Leaves Invalid Group:                           0
      Leaves DA Not All Routers:                      0
      Leaves No Querier:                              0
      Leaves Non-Member:                              0
      Leaves Non-Dynamic Member:                      0
      Leaves Non-V2 Member:                           0
      V3 Reports Invalid Group:                       0
      V3 Reports Link-Local Group:                    0
      V3 Reports DA Not All V3 Routers:               0
      V3 Reports No Querier:                          0
      V3 Reports Older Version Querier:               0
      V3 Reports Invalid Group Record Type:           0
      V3 Reports No Sources:                          0
      V3 Leaves Non-Member:                           0
      PIM Msgs Dropped by S/W Router Guard:           0
    Tx Errors:
      V3 Sources Not Reported:                        0
  Startup Query Sync Statistics:
    None
  ICCP Group Port Statistics (elapsed time since last cleared 01:21:27):
    Port Created Standby:                             6
    Port Created Active:                              1
    Port Goes Standby:                                6
    Port Goes Active:                                 7
  ICCP Traffic Statistics (elapsed time since last cleared 01:21:27):
    Rx Messages:
      App State TLVs:                             24006
      App State start of sync:                        6
      App State end of sync:                          6
      Request Sync TLVs:                              2
      Port Membership TLVs:                       24002
      Port Membership adds:                       23966
      Port Membership removes:                     8000
      Querier Info TLVs:                              2
    Rx Errors:
      App State sync TLVs ignored:                    2
    Tx Messages:
      App State replay attempts:                      2
      Request Sync TLVs:                              6
      Port Membership TLVs:                       16651
      Port Membership adds:                       16123
      Port Membership removes:                     5543
    Tx Errors:
      None
```

The detail statistics display shows the following new bridge-domain counters:

```
Router# show igmp snooping bridge-domain Group1:BD-1 detail statistics
#Access Group Permits
#Access Group Denials
#Group Limits Exceeded
```

Related Commands

Command	Description
clear igmp snooping bridge-domain	Clears traffic counters at the bridge domain level.

show igmp snooping group

To display IGMP group membership information, use the **show igmp snooping group** command in EXEC mode.

{**show igmp snooping group** [**summary** [*group-address*] [{**bridge-domain** *bridge-domain-name* | **port** {**interface-name** | **neighbor** *ipaddr* **pw-id** *id*}}]] | [[*group-address*] [{**bridge-domain** *bridge-domain-name* | **port** {*interface-name* | **neighbor** *ipaddr* **pw-id** *id*}}] [**source** *source-address*] [**detail**]]}

Syntax Description

summary	(Optional) Provides per group summary information.
group-address	(Optional) Provides IP group address information for the specified group in *A.B.C.D* format.
bridge-domain *bridge-domain-name*	(Optional) Provides group membership information for the specified bridge domain.
port *interface-name*	(Optional) Provides group membership information for the specified AC port.
port neighbor *ipaddr* **pw-id** *id*	(Optional) Provides group membership information for the specified PW port.
source *source-address*	(Optional) Provides group membership information for groups indicating interest in a specified source address.
detail	(Optional) Provides detailed information in a multiline display per group.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to display information about group membership in the Layer -2 forwarding tables. The display includes indicators identifying whether the group information was obtained dynamically (for example, snooped) or statically configured.

The command offers the following levels of detail:

- The basic command with no keywords displays group membership information as one line per port within group.

- The **summary** keyword summarizes the port statistics into one line per group. The **summary** keyword is mutually exclusive with the **port-view**, **source**, and **detail** keywords.
- The **detail** keyword includes traffic statistics and counters.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example shows group membership information by groups within bridge domains.

```
Router# show igmp snooping group

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

                            Bridge Domain Group1:BD-1

Group           Ver GM Source          PM Port                         Exp   Flg
-----           --- -- ------          -- ----                         ---   ---
225.1.1.1       V2  -  -               -  GigabitEthernet0/2/0/10.1    never S
238.1.1.1       V2  -  -               -  GigabitEthernet0/2/0/10.1    71    D
238.1.1.1       V2  -  -               -  GigabitEthernet0/2/0/10.5    103   D
238.1.1.2       V2  -  -               -  GigabitEthernet0/2/0/10.2    79    D
238.1.1.2       V2  -  -               -  GigabitEthernet0/2/0/10.6    111   D
238.1.1.3       V2  -  -               -  GigabitEthernet0/2/0/10.3    87    D
238.1.1.3       V2  -  -               -  GigabitEthernet0/2/0/10.7    119   D
238.1.1.4       V2  -  -               -  GigabitEthernet0/2/0/10.4    95    D
238.1.1.4       V2  -  -               -  GigabitEthernet0/2/0/10.8    63    D

                            Bridge Domain Group1:BD-3

Group           Ver GM Source          PM Port                         Exp   Flg
-----           --- -- ------          -- ----                         ---   ---
227.1.1.1       V3  EX 10.1.1.1        EX GigabitEthernet0/2/0/10.10   -     D
227.1.1.1       V3  EX 10.1.1.1        EX GigabitEthernet0/2/0/10.11   -     D
227.1.1.1       V3  EX 10.1.1.1        EX GigabitEthernet0/2/0/10.12   -     D
227.1.1.1       V3  EX 10.1.1.1        EX GigabitEthernet0/2/0/10.13   -     D
227.1.1.1       V3  EX 10.1.1.1        EX GigabitEthernet0/2/0/10.14   -     D
227.1.1.1       V3  EX 10.1.1.1        EX GigabitEthernet0/2/0/10.9    -     D
227.1.1.1       V3  EX *               EX GigabitEthernet0/2/0/10.10   123   D
227.1.1.1       V3  EX *               EX GigabitEthernet0/2/0/10.11   83    D
227.1.1.1       V3  EX *               EX GigabitEthernet0/2/0/10.12   91    D
227.1.1.1       V3  EX *               EX GigabitEthernet0/2/0/10.13   99    D
227.1.1.1       V3  EX *               EX GigabitEthernet0/2/0/10.14   107   D
227.1.1.1       V3  EX *               EX GigabitEthernet0/2/0/10.9    115   D
227.1.1.2       V3  EX 10.2.3.4        IN GigabitEthernet0/2/0/10.10   121   D
227.1.1.2       V3  EX 10.2.3.4        IN GigabitEthernet0/2/0/10.11   129   D
227.1.1.2       V3  EX 10.2.3.4        IN GigabitEthernet0/2/0/10.12   89    D
227.1.1.2       V3  EX 10.2.3.4        IN GigabitEthernet0/2/0/10.13   97    D
227.1.1.2       V3  EX 10.2.3.4        IN GigabitEthernet0/2/0/10.14   105   D
227.1.1.2       V3  EX *               EX GigabitEthernet0/2/0/10.9    124   D

                            Bridge Domain Group1:BD-5
Group           Ver GM Source          PM Port                         Exp   Flg
-----           --- -- ------          -- ----                         ---   ---
227.1.1.1       V3  EX *               EX GigabitEthernet0/2/0/10.15   114   D
227.1.1.1       V3  EX *               EX GigabitEthernet0/2/0/10.16   122   D
```

```
Router# show igmp snooping group

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

                            Bridge Domain satellite:10

Group           Ver GM Source          PM Port                          Exp   Flgs
-----           --- -- ------          -- ----                          ---   ----
232.0.0.1       V3  IN 192.10.1.2      IN Gi100/0/0/22                  129   D
232.0.0.1       V3  IN 192.10.1.2      IN Gi100/0/0/32                  129   D
232.0.0.1       V3  IN 192.10.1.2      IN Gi200/0/0/34                  129   D

                            Bridge Domain satellite:20

Group           Ver GM Source          PM Port                          Exp   Flgs
-----           --- -- ------          -- ----                          ---   ----
232.0.0.1       V3  IN 192.10.1.2      IN Gi200/0/0/23                  129   D
232.0.0.1       V3  IN 192.10.1.2      IN Gi300/0/0/25                  129   D
232.0.0.1       V3  IN 192.10.1.2      IN Gi300/0/0/34                  129   D
```

For an active node:

```
Router# show igmp snooping group debug
Fri Oct 10 08:41:45.968 UTC

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

                            Bridge Domain native:native

Group           Ver GM Source          PM Port                          Exp   Flgs
-----           --- -- ------          -- ----                          ---   ----
229.107.0.1     V3  IN 5.1.25.2        IN Gi100/0/0/10.7                79    D
229.107.0.1     V3  IN 5.1.25.2        IN Gi200/0/0/6.7                 79    D
232.107.0.1     V3  IN 5.1.25.2        IN Gi100/0/0/10.7                79    D
232.107.0.1     V3  IN 5.1.25.2        IN Gi200/0/0/6.7                 79    D
```

For a standby node:

```
Router# show igmp snooping group debug
Fri Oct 10 09:36:55.146 UTC

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

                            Bridge Domain native:native

Group           Ver GM Source          PM Port                          Exp   Flgs
-----           --- -- ------          -- ----                          ---   ----
229.107.0.1     V3  IN 5.1.25.2        IN Gi100/0/0/10.7                11    DR
229.107.0.1     V3  IN 5.1.25.2        IN Gi200/0/0/6.7                 11    DR
232.107.0.1     V3  IN 5.1.25.2        IN Gi100/0/0/10.7                11    DR
232.107.0.1     V3  IN 5.1.25.2        IN Gi200/0/0/6.7                 11    DR
```

The following example shows group membership information by group within a specific bridge domain.

```
Router# show igmp snooping group bridge-domain Group1:BD-1

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

```
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

                            Bridge Domain Group1:BD-1

Group           Ver GM Source          PM Port                         Exp   Flg
-----           --- -- ------          -- ----                         ---   ---
225.1.1.1       V2  -  -               -  GigabitEthernet0/2/0/10.1    never S
238.1.1.1       V2  -  -               -  GigabitEthernet0/2/0/10.1    84    D
238.1.1.1       V2  -  -               -  GigabitEthernet0/2/0/10.5    116   D
238.1.1.2       V2  -  -               -  GigabitEthernet0/2/0/10.2    92    D
238.1.1.2       V2  -  -               -  GigabitEthernet0/2/0/10.6    60    D
238.1.1.3       V2  -  -               -  GigabitEthernet0/2/0/10.3    100   D
238.1.1.3       V2  -  -               -  GigabitEthernet0/2/0/10.7    68    D
238.1.1.4       V2  -  -               -  GigabitEthernet0/2/0/10.4    108   D
238.1.1.4       V2  -  -               -  GigabitEthernet0/2/0/10.8    76    D
```

The following example shows group membership information by groups within a specific port.

```
Router# show igmp snooping group port GigabitEthernet 0/2/0/10.10

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

                            Bridge Domain Group1:BD-3

Group           Ver GM Source          PM Port                         Exp   Flg
-----           --- -- ------          -- ----                         ---   ---
227.1.1.1       V3  EX 10.1.1.1        EX GigabitEthernet0/2/0/10.10   -     D
227.1.1.1       V3  EX *               EX GigabitEthernet0/2/0/10.10   111   D
227.1.1.2       V3  EX 10.2.3.4        IN GigabitEthernet0/2/0/10.10   109   D
```

The following example summarizes each group's membership information into a single line.

```
Router# show igmp snooping group summary

                            Bridge Domain Group1:BD-1

                                        #Mem  #Inc  #Exc
Group           Source          Ver GM  Ports Ports Ports
-----           ------          --- --  ----- ----- -----
225.1.1.1       -               V2  -   1     -     -
238.1.1.1       -               V2  -   2     -     -
238.1.1.2       -               V2  -   2     -     -
238.1.1.3       -               V2  -   2     -     -
238.1.1.4       -               V2  -   2     -     -

                            Bridge Domain Group1:BD-3

                                        #Mem  #Inc  #Exc
Group           Source          Ver GM  Ports Ports Ports
-----           ------          --- --  ----- ----- -----
227.1.1.1       10.1.1.1        V3  EX  -     0     6
227.1.1.1       *               V3  EX  6     -     -
227.1.1.1       *               V3  EX  6     -     -
227.1.1.2       10.2.3.4        V3  EX  -     5     0
227.1.1.2       *               V3  EX  1     -     -
227.1.1.2       *               V3  EX  1     -     -

                            Bridge Domain Group1:BD-5

                                        #Mem  #Inc  #Exc
Group           Source          Ver GM  Ports Ports Ports
```

```
-----           ------          --- --  ----- ----- -----
227.1.1.1       *               V3  EX  2     -     -
```

The following example shows detail information about each group.

```
Router# show igmp snooping group detail

                            Bridge Domain Group1:BD-1

Group Address:                          225.1.1.1
  Version:                              V2
  Uptime:                               00:42:13
  Port Count:                           1
    GigabitEthernet0/2/0/10.1:
      Uptime:                           00:42:13
      Persistence:                      static
      Expires:                          never
Group Address:                          238.1.1.1
  Version:                              V2
  Uptime:                               00:41:38
  Port Count:                           2
    GigabitEthernet0/2/0/10.1:
      Uptime:                           00:41:38
      Persistence:                      dynamic
      Expires:                          119
    GigabitEthernet0/2/0/10.5:
      Uptime:                           00:41:06
      Persistence:                      dynamic
      Expires:                          87
Group Address:                          238.1.1.2
  Version:                              V2
  Uptime:                               00:41:30
  Port Count:                           2
    GigabitEthernet0/2/0/10.2:
      Uptime:                           00:41:30
      Persistence:                      dynamic
      Expires:                          63
    GigabitEthernet0/2/0/10.6:
      Uptime:                           00:40:58
      Persistence:                      dynamic
      Expires:                          95
Group Address:                          238.1.1.3
  Version:                              V2
  Uptime:                               00:41:22
  Port Count:                           2
    GigabitEthernet0/2/0/10.3:
      Uptime:                           00:41:22
      Persistence:                      dynamic
      Expires:                          71
    GigabitEthernet0/2/0/10.7:
      Uptime:                           00:40:50
      Persistence:                      dynamic
      Expires:                          103
Group Address:                          238.1.1.4
  Version:                              V2
  Uptime:                               00:41:14
  Port Count:                           2
    GigabitEthernet0/2/0/10.4:
      Uptime:                           00:41:14
      Persistence:                      dynamic
      Expires:                          79
    GigabitEthernet0/2/0/10.8:
      Uptime:                           00:40:42
      Persistence:                      dynamic
      Expires:                           111
                Bridge Domain bg1:bg1_bd1

Group Address:                           225.0.0.1
 Version:                               V3
 Uptime:                                01:47:00
 Group Filter Mode:                     Exclude
 Source:                                {}
 Exclude Port Count:                  1
  Bundle-Ether10
   ICCP Group:                      1
   Redundancy State:                Active
   Uptime:                          01:47:00
   Persistence:                     dynamic
   Expires:                         197

                            Bridge Domain Group1:BD-3

Group Address:                           227.1.1.1
  Version:                               V3
  Uptime:                                00:41:35
  Group Filter Mode:                     Exclude
  Source Count:                          1
  Static/Include/Exclude Source Count:   0/0/1
  Source:                                10.1.1.1
    Static/Include/Exclude Port Count:   0/0/6
    Exclude Port Count:                  6
      GigabitEthernet0/2/0/10.10:
        Uptime:                          00:41:27
        Persistence:                     dynamic
        Expires:                         -
      GigabitEthernet0/2/0/10.11:
        Uptime:                          00:41:19
        Persistence:                     dynamic
        Expires:                         -
      GigabitEthernet0/2/0/10.12:
        Uptime:                          00:41:11
        Persistence:                     dynamic
        Expires:                         -
      GigabitEthernet0/2/0/10.13:
        Uptime:                          00:41:03
        Persistence:                     dynamic
        Expires:                         -
      GigabitEthernet0/2/0/10.14:
        Uptime:                          00:40:55
        Persistence:                     dynamic
        Expires:                         -
      GigabitEthernet0/2/0/10.9:
        Uptime:                          00:41:35
        Persistence:                     dynamic
        Expires:                         -
  Source:                                *
    Exclude Port Count:                  6
      GigabitEthernet0/2/0/10.10
        Uptime:                          00:41:27
        Persistence:                     dynamic
        Expires:                         91
      GigabitEthernet0/2/0/10.11
        Uptime:                          00:41:19
        Persistence:                     dynamic
        Expires:                         99
      GigabitEthernet0/2/0/10.12
        Uptime:                          00:41:11
        Persistence:                     dynamic
        Expires:                         107
      GigabitEthernet0/2/0/10.13
        Uptime:                          00:41:03
        Persistence:                     dynamic
        Expires:                         115
      GigabitEthernet0/2/0/10.14
        Uptime:                          00:40:55
        Persistence:                     dynamic
        Expires:                         123
      GigabitEthernet0/2/0/10.9
        Uptime:                          00:41:35
        Persistence:                     dynamic
        Expires:                         83
Group Address:                           227.1.1.2
  Version:                               V3
  Uptime:                                00:41:37
  Group Filter Mode:                     Exclude
  Source Count:                          1
  Static/Include/Exclude Source Count:   0/1/0
  Source:                                10.2.3.4
    Static/Include/Exclude Port Count:   0/5/0
    Include Port Count:                  5
      GigabitEthernet0/2/0/10.10:
        Uptime:                          00:41:29
        Persistence:                     dynamic
        Expires:                         89
      GigabitEthernet0/2/0/10.11:
        Uptime:                          00:41:21
        Persistence:                     dynamic
        Expires:                         97
      GigabitEthernet0/2/0/10.12:
        Uptime:                          00:41:13
        Persistence:                     dynamic
        Expires:                         105
      GigabitEthernet0/2/0/10.13:
        Uptime:                          00:41:05
        Persistence:                     dynamic
        Expires:                         113
      GigabitEthernet0/2/0/10.14:
        Uptime:                          00:40:57
        Persistence:                     dynamic
        Expires:                         121
  Source:                                *
    Exclude Port Count:                  1
      GigabitEthernet0/2/0/10.9
        Uptime:                          00:41:34
        Persistence:                     dynamic
        Expires:                         124

                            Bridge Domain Group1:BD-5

Group Address:                           227.1.1.1
  Version:                               V3
  Uptime:                                00:41:36
  Group Filter Mode:                     Exclude
  Source:                                *
    Exclude Port Count:                  2
      GigabitEthernet0/2/0/10.15
        Uptime:                          00:41:36
        Persistence:                     dynamic
        Expires:                         114
      GigabitEthernet0/2/0/10.16
        Uptime:                          00:41:28
        Persistence:                     dynamic
        Expires:                         122
```

If a group limit is configured on an output port, the detail display shows the group weight value associated with each group or source group on that port:

```
Router1# show igmp snooping port group detail

                            Bridge Domain bg1:bg1_bd1

Group Address:                            225.0.0.1
 Version:                                V3
 Uptime:                                 01:43:25
 Group Filter Mode:                      Exclude
 Source:                                 {}
   Exclude Port Count:                   1
    Bundle-Ether10
     ICCP Group:                       1
     Redundancy State:                 Active
     Uptime:                           01:43:25
     Persistence:                      dynamic
     Expires:                          249

Router2# show igmp snooping group detail

                 Bridge Domain bg1:bg1_bd1

Group Address:                            225.0.0.1
 Version:                                V3
 Uptime:                                 01:43:25
 Group Filter Mode:                      Exclude
 Source:                                 {}
  Exclude Port Count:                   1
   Bundle-Ether10
     ICCP Group:                       1
     Redundancy State:                 Standby
     Uptime:                           01:43:25
     Persistence:                      dynamic
     Expires:                          249
```

Related Commands

Command	Description
clear igmp snooping group	Clears group states.

show igmp snooping port

To display IGMP snooping configuration information and traffic counters by router interface port, use the **show igmp snooping port** command in EXEC mode.

show igmp snooping port
interface-name | **neighbor** *ipaddr* **pw-id** *id* | **bridge-domain bridge-domain-name**
detail [**statistics** [**include-zeroes**]]
group [*group-address*] [**source** *source-address*] [**detail**]

Syntax Description

interface-name	(Optional) Displays information only for the specified AC port.

neighbor *ipaddr* **pw-id** *id*	(Optional) Displays information only for the specified PW port.
bridge-domain *bridge-domain-name*	(Optional) Displays information for ports in the specified bridge domain.
detail	(Optional) Includes port details, rather than a single line summary.
statistics	(Optional) Includes IGMP traffic counters and statistics in the detail display.
include-zeroes	(Optional) Includes all statistics, even if they are zero. Without this keyword, many statistics are omitted from the display when their values are zero.
group	(Optional) Provides group membership information in its entirety as received at each port. The display is organized by port, showing groups within ports.
group-address	(Optional) Displays information only for the specified group address, organized by port.
source *source-address*	(Optional) Displays information only for the specified source address, organized by port.
detail	(Optional) Includes group details.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays IGMP snooping information organized by IGMP snooping port. Use the command without any keywords to display summary information about all ports, in a single line per port.

Use optional arguments and keywords to request the following:

- Limit the display to a specified port.
- Limit the display to ports under a specified bridge.
- Request details and traffic statistics per port.

Note The **statistics** keyword cannot be used in the same command with the **group** keyword.

- Organize the display by group within ports. Use the **group** keyword with or without a specified interface or bridge domain.
- Limit the group information to specific groups or source addresses.

The **statistics** keyword displays IGMP traffic information, including IGMP queries, reports, and leaves. The three columns in the statistics section of the display are:

- Received—Number of packets received.
- Reinjected—Number of packets received, processed, and reinjected back into the forwarding path.
- Generated—Number of packets generated by the IGMP snooping application and injected into the forwarding path.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example shows summary information per port:

```
Router# show igmp snooping port

                        Bridge Domain bg1:bg1_bd1

                                                         State
Port                                                Oper  STP  Red   #Grps   #SGs
----                                                ----  ---  ---   -----   ----
Bundle-Ether10                       Up    -    S    1      0
Neighbor 40.40.40.40 pw-id 1               Up    -    -       4      0
```

The following example shows summary information for a specific port.

```
Router# show igmp snooping port GigabitEthernet 0/1/0/3.215

                        Bridge Domain 215:215
                                  State
Port                                                Oper  STP  Red   #Grps   #SGs
----                                                ----  ---  ---   -----   ----
GigabitEthernet0/1/0/3.215                            Up    -    -       1      0
```

The following example shows detail information about a specified port.

```
Router# show igmp snooping port Bundle-Ether10 detail

Bundle-Ether10 is Up
  Bridge Domain:        bg1:bg1_bd1
  ICCP Group:                1
    Redundancy State:        Active since Thu Aug 26 12:52:37 2010
 IGMP Snoop Profile:        profile2
   Dynamic Mrouter Port:      Querier(192.1.1.10)
    Expires:                 116 seconds
  IGMP Groups:              2
    Static/Dynamic:          1/1
  IGMP Source Groups:        0
```

```
    Static/Include/Exclude:  0/0/0
  Admitted Weight       1/(no limit)
```

The following example shows detail information that includes the total group weight accumulated by all groups and source groups on the port and the configured limit—Admitted Weight: 12/16:

```
Router# show igmp snooping port gigabitEthernet 0/0/0/10.2 detail
```

GigabitEthernet0/0/0/10.2 is Up

Bridge Domain: bg1:bd1

IGMP Groups: 4

Static/Dynamic: 0/4

IGMP Source Groups: 0

Static/Include/Exclude: 0/0/0

Admitted Weight: 33/36

The following example shows detail, including statistics, for a specified port.

```
Router# show igmp snooping port GigabitEthernet 0/0/0/10.1 detail statistics

GigabitEthernet0/0/0/10.1 is Up
  Bridge Domain:             Group1:BD-1
  IGMP Snoop Profile:        profile2
  Dynamic Mrouter Port:      Querier(192.1.1.10)
    Expires:                 117 seconds
  IGMP Groups:               2
    Static/Dynamic:          1/1
  IGMP Source Groups:        0
    Static/Include/Exclude:  0/0/0


Access Group Permits
Access Group Denials
Group Limits Exceeded



  Traffic Statistics (elapsed time since last cleared 01:19:32):
                                     Received  Reinjected   Generated
    Messages:                             668          75           0
      IGMP General Queries:               593           0           0
      IGMP Group Specific Queries:          0           0           0
      IGMP G&S Specific Queries:            0           0           0
      IGMP V2 Reports:                     75          75           0
      IGMP V3 Reports:                      0           0           0
      IGMP V2 Leaves:                       0           0           0
      IGMP Global Leaves:                   0           -           0
      PIM Hellos:                           0           0           -
    Rx Packet Treatment:
      Packets Flooded:                                  0
      Packets Forwarded To Members:                     0
      Packets Forwarded To Mrouters:                   75
      Packets Consumed:                               593
    Rx Errors:
      None
    Tx Errors:
      None
```

The following example shows all statistics, even those with zero values, for a specified port.

```
Router# show igmp snooping port GigabitEthernet 0/0/0/10.1 detail statistics include-zeroes

GigabitEthernet0/0/0/10.1 is Up
  Bridge Domain:             Group1:BD-1
  IGMP Snoop Profile:        profile2
  Dynamic Mrouter Port:      Querier(192.1.1.10)
    Expires:                 120 seconds
  IGMP Groups:               2
    Static/Dynamic:          1/1
  IGMP Source Groups:        0
    Static/Include/Exclude:  0/0/0
  Traffic Statistics (elapsed time since last cleared 01:20:42):
                                     Received  Reinjected   Generated
    Messages:                             678          76           0
      IGMP General Queries:               602           0           0
      IGMP Group Specific Queries:          0           0           0
      IGMP G&S Specific Queries:            0           0           0
      IGMP V2 Reports:                     76          76           0
      IGMP V3 Reports:                      0           0           0
      IGMP V2 Leaves:                       0           0           0
      IGMP Global Leaves:                   0           -           0
      PIM Hellos:                           0           0           -
    Rx Packet Treatment:
      Packets Flooded:                                  0
      Packets Forwarded To Members:                     0
      Packets Forwarded To Mrouters:                   76
      Packets Consumed:                               602
    Reports Suppressed:                                 0
    IGMP Blocks Ignored in V2 Compat Mode:              0
    IGMP EX S-lists Ignored in V2 Compat Mode:          0
    Rx Errors:
      Packets On Inactive Bridge Domain:                0
      Packets On Inactive Port:                         0
      Packets Martian:                                  0
      Packets Bad Protocol:                             0
      Packets DA Not Multicast:                         0
      Packets Missing Router Alert:                     0
      Packets Missing Router Alert Drop:                0
      Packets Bad IGMP Checksum:                        0
      Packets TTL Not One:                              0
      Packets TTL Not One Drop:                         0
      Queries Too Short:                                0
      V1 Reports Too Short:                             0
      V2 Reports Too Short:                             0
      V3 Reports Too Short:                             0
      V2 Leaves Too Short:                              0
      IGMP Messages Unknown:                            0
      IGMP Messages GT Max Ver:                         0
      IGMP Messages LT Min Ver:                         0
      Queries Bad Source:                               0
      Queries Dropped by S/W Router Guard:              0
      General Queries DA Not All Nodes:                 0
      GS-Queries Invalid Group:                         0
      GS-Queries DA Not Group:                          0
      GS-Queries Not From Querier:                      0
      GS-Queries Unknown Group:                         0
      Reports Invalid Group:                            0
      Reports Link-Local Group:                         0
      Reports DA Not Group:                             0
      Reports No Querier:                               0
      Leaves Invalid Group:                             0
      Leaves DA Not All Routers:                        0
      Leaves No Querier:                                0
      Leaves Non-Member:                                0
      Leaves Non-Dynamic Member:                        0
      Leaves Non-V2 Member:                             0
      V3 Reports Invalid Group:                         0
      V3 Reports Link-Local Group:                      0
      V3 Reports DA Not All V3 Routers:                 0
      V3 Reports No Querier:                            0
      V3 Reports Older Version Querier:                 0
      V3 Reports Invalid Group Record Type:             0
      V3 Reports No Sources:                            0
      V3 Leaves Non-Member:                             0
      PIM Msgs Dropped by S/W Router Guard:             0
    Tx Errors:
      V3 Sources Not Reported:                          0
```

The following information shows summary information for all port groups under a specific bridge domain.

```
Router# show igmp snooping port bridge-domain Group1:BD-1 group

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

                            Bridge Domain Group1:BD-1

Port                         PM Group           Ver GM Source           Exp   Flg
----                         -- -----           --- -- ------           ---   ---
GigabitEthernet0/2/0/10.1    -  225.1.1.1       V2  -  -                never S
GigabitEthernet0/2/0/10.1    -  238.1.1.1       V2  -  -                77    D
GigabitEthernet0/2/0/10.2    -  238.1.1.2       V2  -  -                85    D
GigabitEthernet0/2/0/10.3    -  238.1.1.3       V2  -  -                93    D
GigabitEthernet0/2/0/10.4    -  238.1.1.4       V2  -  -                101   D
GigabitEthernet0/2/0/10.5    -  238.1.1.1       V2  -  -                109   D
GigabitEthernet0/2/0/10.6    -  238.1.1.2       V2  -  -                117   D
GigabitEthernet0/2/0/10.7    -  238.1.1.3       V2  -  -                61    D
GigabitEthernet0/2/0/10.8    -  238.1.1.4       V2  -  -                69    D
```

The following information shows detail information for all port groups under a specific bridge domain.

```
Router# show igmp snooping port bridge-domain Group1:BD-1 group detail

                            Bridge Domain Group1:BD-1

Port:                                     GigabitEthernet0/2/0/10.1
  Group Address:                          225.1.1.1
    Version:                              V2
    Uptime:                               01:27:20
    Persistence:                          static
    Expires:                              never
  Group Address:                          238.1.1.1
    Version:                              V2
    Uptime:                               01:26:45
    Persistence:                          dynamic
    Expires:                              100
Port:                                     GigabitEthernet0/2/0/10.2
  Group Address:                          238.1.1.2
    Version:                              V2
    Uptime:                               01:26:37
    Persistence:                          dynamic
    Expires:                              108
Port:                                     GigabitEthernet0/2/0/10.3
```

```
  Group Address:                     238.1.1.3
    Version:                         V2
    Uptime:                          01:26:29
    Persistence:                     dynamic
    Expires:                         116
Port:                                GigabitEthernet0/2/0/10.4
  Group Address:                     238.1.1.4
    Version:                         V2
    Uptime:                          01:26:21
    Persistence:                     dynamic
    Expires:                         60
Port:                                GigabitEthernet0/2/0/10.5
  Group Address:                     238.1.1.1
    Version:                         V2
    Uptime:                          01:26:13
    Persistence:                     dynamic
    Expires:                         68
Port:                                GigabitEthernet0/2/0/10.6
  Group Address:                     238.1.1.2
    Version:                         V2
    Uptime:                          01:26:05
    Persistence:                     dynamic
    Expires:                         76
Port:                                GigabitEthernet0/2/0/10.7
  Group Address:                     238.1.1.3
    Version:                         V2
    Uptime:                          01:25:57
    Persistence:                     dynamic
    Expires:                         84
Port:                                GigabitEthernet0/2/0/10.8
  Group Address:                     238.1.1.4
    Version:                         V2
    Uptime:                          01:25:49
    Persistence:                     dynamic
    Expires:                         92
```

Related Commands

Command	Description
clear igmp snooping port	Clears traffic counters at the port level.

show igmp snooping profile

To display IGMP snooping profile information, use the **show igmp snooping profile** command in EXEC mode.

{**show igmp snooping profile** [**summary**] | [*profile-name*] [**detail** [**include-defaults**]] [{**references** [**bridge-domain** [*bridge-domain-name*]] | **port** [{**interface-name** | **neighbor** *ipaddr* **pw-id** *id*}]}]}

Syntax Description

summary	(Optional) Displays a summary of profile instances, bridge domain references, and port references.
profile-name	(Optional) Displays information only for the named profile.
detail	(Optional) Displays the contents of profiles.

include-defaults	(Optional) Displays all default configurations with the profile contents. Without this keyword, only configured profile information is displayed.
references	(Optional) Shows which bridge domains and bridge ports reference each profile.
bridge-domain [*bridge-domain-name*]	(Optional) Provides a bridge domain filter for the **references** keyword. Without *bridge-domain-name* , the display shows profiles attached to all bridge domains. With *bridge-domain-name* , the display shows only the profile attached to the specified bridge domain.
port [*interface-name*] or **port** [**neighbor** *ipaddr* **pw-id** *id*]	(Optional) Provides a port filter for the **references** keyword. • With *interface-name* or **neighbor** specified, the display shows the profile attached to the named AC or PW. • Using the **port** keyword alone shows profiles attached to all ports.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

Use this command to display the contents of profiles and to see associations of profiles with bridge-domains and ports.

The **summary** keyword lists profile names and summarizes their usage on bridge domains and ports. No other keywords can be used with **summary** .

Use the **details** keyword with a profile name to show the contents of a specific profile. Without a profile name, the **detail** keyword shows the contents of all profiles.

Use the **references** keyword to list the relationships between profiles and bridge domains or profiles and ports. You have the following options:

- Use the **references** keyword without any other keywords to show all profiles and the ports and bridge domains they are attached to.
- Use the **references** keyword with the **name** keyword to show a specific profile and where it is attached.
- Use the **port** keyword to list all ports and the profiles attached to them.
- Use the **port** keyword with a specific AC interface or PW to see the profile attached to the named port.
- Use the **bridge-domain** keyword to list all bridge domains and the profiles attached to them.
- Use the **bridge-domain** keyword with a specific bridge domain name to see the profile attached to a specific bridge domain.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example lists profile names and shows summary level profile usage.

```
Router# show igmp snooping profile

Profile                                    Bridge Domain       Port
-------                                    -------------       ----
profile1                                               3          0
profile2                                               0          1
profile3                                               0          1
```

The following example shows summary level profile usage for a named profile.

```
Router# show igmp snooping profile profile1

Profile                                    Bridge Domain       Port
-------                                    -------------       ----
profile1                                               3          0
```

The following example shows the contents of each profile.

```
Router# show igmp snooping profile detail

IGMP Snoop Profile profile1:

  Bridge Domain References:            3
  Port References:                     0

IGMP Snoop Profile profile2:

  Static Groups:                       225.1.1.1

  Bridge Domain References:            0
  Port References:                     1

IGMP Snoop Profile profile3:

  Static Mrouter:                      Enabled

  Bridge Domain References:            0
  Port References:                     1
```

The following example shows output reflecting the **access-group** , **group limit** , and **tcn flood disable** parameters:

```
Router# show igmp snooping profile detail


IGMP Snoop Profile profile:

  Querier LMQ Count:                   2

  Access Group ACL:                    iptv-white-list
  Group Policy:                        iptv-group-weights
  Group Limit:                         16
  Immediate Leave:                      Enabled
  TCN Flood:                            Disabled


  Bridge Domain References:             1
  Port References:                      0
```

The following example shows the contents of a named profile. In this example, the profile is empty.

```
Router# show igmp snooping profile profile1 detail

IGMP Snoop Profile profile1:

  Bridge Domain References:             3
  Port References:                      0
```

The following example shows the contents of a named profile and the implied default configurations:

```
Router# show igmp snooping profile profile1 detail include-defaults

IGMP Snoop Profile profile p1:

  System IP Address:                    10.144.144.144
  Minimum Version:                      2
  Report Suppression:                   Enabled
  Unsolicited Report Interval:          1000 (milliseconds)
  TCN Query Solicit:                    Enabled
  TCN Membership Sync:                  Disabled
  TCN Flood:                            Enabled
  TCN Flood Query Count:                2
  Router Alert Check:                   Disabled
  TTL Check:                            Disabled

  Internal Querier Support:             Enabled
  Internal Querier Version:             3
  Internal Querier Timeout:             0 (seconds)
  Internal Querier Interval:            60 (seconds)
  Internal Querier Max Response Time:   10 (seconds)
  Internal Querier TCN Query Interval:  10 (seconds)
  Internal Querier TCN Query Count:     2
  Internal Querier TCN Query MRT:       0
  Internal Querier Robustness:          2

  Querier Query Interval:               60 (seconds)
  Querier LMQ Interval:                 1000 (milliseconds)
  Querier LMQ Count:                    2
  Querier Robustness:                   2

  Immediate Leave:                      Disabled
  Explicit Tracking:                    Disabled
  Static Mrouter:                       Disabled
  Router Guard:                         Disabled

Access Group ACL:                      (empty)

  Group Policy:
  Group Limit:                          -1

  ICCP Group Report Standby State:      Enabled

  Startup Query Interval:               15 (seconds)
  Startup Query Count:                  2
  Startup Query Max Response Time:      10 (seconds)
  Startup Query on Port Up:             Enabled
  Startup Query on IG Port Active:      Disabled
  Startup Query on Topology Change:     Disabled
  Startup Query on Process Start:       Disabled

  Bridge Domain References:             1
  Port References:                      0
```

The following command shows a summary of profile usage, by profile name.

```
Router# show igmp snooping profile summary

  Number of profiles:                 3
  Number of bridge domain references: 3
  Number of port references:          2
```

The following command lists all IGMP snooping profiles and shows which bridge domains and ports are configured to use each profile.

```
Router# show igmp snooping profile references

Profile:            profile1
  Bridge Domains:   Group1:BD-5
                    Group1:BD-3
                    Group1:BD-1
  No Port References

Profile:            profile2
  No Bridge Domain References
  Ports:            GigabitEthernet0/2/0/10.1

Profile:            profile3
  No Bridge Domain References
  Ports:            GigabitEthernet0/2/0/10.2
```

The following command lists all bridges or ports that are configured to use the profile named profile1.

```
Router# show igmp snooping profile profile1 references

Profile:            profile1
  Bridge Domains:   None
  Ports:            GigabitEthernet 0/1/0/0
                    GigabitEthernet 0/1/0/1
                    GigabitEthernet 0/1/0/2
                    GigabitEthernet 0/1/0/3
                    GigabitEthernet 0/1/0/4
                    GigabitEthernet 0/1/0/5
                    (… missing lines)
                    GigabitEthernet 0/3/3/1109
                    GigabitEthernet 0/3/3/1110
                    GigabitEthernet 0/3/3/1111
```

The following example shows the profile attached to a specific bridge domain.

```
Router# show igmp snooping profile references bridge-domain Group1:BD-1

Profile:            profile1
  Bridge Domains:   Group1:BD-1
```

The following example shows the profile attached to a specific port.

```
Router# show igmp snooping profile references port GigabitEthernet 0/2/0/10.1

Profile:            profile2
  Ports:            GigabitEthernet0/2/0/10.1
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile.
show l2vpn forwarding bridge-domain mroute	Shows profile names associated with the bridge domain and its ports.

show igmp snooping redundancy

To display IGMP snooping redundancy information, use the **show igmp snooping redundancy** command in EXEC mode.

{**show igmp snooping redundancy iccp** | [*profile-name*] [**detail** [**include-defaults**]] [{**references** [**bridge-domain** [*bridge-domain-name*]] | **port** [{**interface-name** | **neighbor** *ipaddr* **pw-id** *id*}]}]}

Syntax Description

iccp	Displays ICCP redundancy information.
profile-name	(Optional) Displays information only for the named profile.
detail	(Optional) Displays the contents of profiles.
include-defaults	(Optional) Displays all default configurations with the profile contents. Without this keyword, only configured profile information is displayed.
references	(Optional) Shows which bridge domains and bridge ports reference each profile.
bridge-domain [*bridge-domain-name*]	(Optional) Provides a bridge domain filter for the **references** keyword. Without *bridge-domain-name* , the display shows profiles attached to all bridge domains. With *bridge-domain-name* , the display shows only the profile attached to the specified bridge domain.
port [*interface-name*] or **port** [**neighbor** *ipaddr* **pw-id** *id*]	(Optional) Provides a port filter for the **references** keyword. • With *interface-name* or **neighbor** specified, the display shows the profile attached to the named AC or PW. • Using the **port** keyword alone shows profiles attached to all ports.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to display the contents of profiles and to see associations of profiles with bridge-domains and ports.

The **summary** keyword lists profile names and summarizes their usage on bridge domains and ports. No other keywords can be used with **summary** .

Use the **details** keyword with a profile name to show the contents of a specific profile. Without a profile name, the **detail** keyword shows the contents of all profiles.

Use the **references** keyword to list the relationships between profiles and bridge domains or profiles and ports. You have the following options:

- Use the **references** keyword without any other keywords to show all profiles and the ports and bridge domains they are attached to.
- Use the **references** keyword with the **name** keyword to show a specific profile and where it is attached.
- Use the **port** keyword to list all ports and the profiles attached to them.
- Use the **port** keyword with a specific AC interface or PW to see the profile attached to the named port.
- Use the **bridge-domain** keyword to list all bridge domains and the profiles attached to them.
- Use the **bridge-domain** keyword with a specific bridge domain name to see the profile attached to a specific bridge domain.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example lists profile names and shows summary level profile usage.

```
Router# show igmp snooping redundancy

Profile                                    Bridge Domain       Port
-------                                    -------------       ----
profile1                                               3          0
profile2                                               0          1
profile3                                               0          1
```

From an active host:

```
Router# show igmp snooping redundancy  iccp group 1
Fri Oct 10 08:40:26.231 UTC


ICCP                          Ports
Group Id   #Peers    Active    Standby   Down     ICCP Group State
```

```
------------------------------------------------------------------
       1        1        15          0      0     Connected Peer Present

Router#
```

From a standby host:

```
Router# show igmp snooping redundancy  iccp group 1
Fri Oct 10 09:35:19.273 UTC


ICCP                           Ports
Group Id   #Peers    Active    Standby   Down     ICCP Group State
------------------------------------------------------------------
       1        1         0         15      0     Connected Peer Present


Router#
```

show igmp snooping summary

To display summary information about IGMP snooping configuration and traffic statistics for the router, use the **show igmp snooping summary** command in EXEC mode.

show igmp snooping summary [**statistics** [**include-zeroes**]]

Syntax Description

statistics	(Optional) Displays IGMP traffic counters and statistics.
include-zeroes	(Optional) Displays all statistics, even if they are zero. Without this keyword, many statistics are omitted from the display when their values are zero.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command summarizes the number of bridge domains, mrouter ports, host ports, groups, and sources configured on the router.

The **statistics** keyword displays IGMP traffic information, including IGMP queries, reports, and leaves. The three columns in the statistics section of the display are:

- Received—Number of packets received.

- Reinjected—Number of packets received, processed, and reinjected back into the forwarding path.
- Generated—Number of packets generated by the IGMP snooping application and injected into the forwarding path.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example summarizes IGMP snooping configuration on the router:

```
Router# show igmp snooping summary
Bridge Domains:                                      5
  IGMP Snooping Bridge Domains:                        3
  Ports:                                              16
  IGMP Snooping Ports:                                16
  Mrouters:                                            6
  STP Forwarding Ports:                                0
  IGMP Groups:                                         8
    Member Ports:                                     18
  IGMP Source Groups:                                  2
    Static/Include/Exclude:                        0/1/1
    Member Ports (Include/Exclude):                  5/6
```

The following example summarizes IGMP snooping configuration on the router and includes non-zero traffic statistics:

```
Router# show igmp snooping summary statistics
Bridge Domains:                                      5
IGMP Snooping Bridge Domains:                        3
Ports:                                              16
IGMP Snooping Ports:                                16
Mrouters:                                            6
STP Forwarding Ports:                                0
ICCP Group Ports:                                    2
IGMP Groups:                                         8
    Member Ports:                                     18
  IGMP Source Groups:                                  2
    Static/Include/Exclude:                        0/1/1
    Member Ports (Include/Exclude):                  5/6


Access Group Permits
Access Group Denials
Group Limits Exceeded



  Traffic Statistics (elapsed time since last cleared 02:08:21):
                                     Received  Reinjected   Generated
    Messages:                            7150         894        2381
      IGMP General Queries:              2682           0           0
      IGMP Group Specific Queries:          0           0           0
      IGMP G&S Specific Queries:            0           0           0
      IGMP V2 Reports:                   1787         894         893
      IGMP V3 Reports:                   2681           0        1488
      IGMP V2 Leaves:                       0           0           0
      IGMP Global Leaves:                   0           -           0
      PIM Hellos:                           0           0           -
    Rx Packet Treatment:
      Packets Flooded:                                  0
      Packets Forwarded To Members:                     0
      Packets Forwarded To Mrouters:                  894
      Packets Consumed:                              6256
    Rx Errors:
      None
    Tx Errors:
      None
Startup Query Sync Statistics:
  Stale Port Groups deleted:                    1
  Stale Port SGs deleted:                       1

ICCP Statistics:
  ICCP Up                                       1
  ICCP Down                                     1
  Congestion Detected                           1
Congestion Cleared                            1
  Peer Up                                       1
  Peer Down                                     1

ICCP Group Port Statistics:
  Port Goes Active:                             1
  Port Goes Standby:                            1

ICCP Traffic Statistics (elapsed time since last cleared 01:01:01):
  RX Messages:
    App Data messages:                          1
    App Data NAKs:                              1
    App Data TLVs:                              1
    App State TLVs:                             1
    Request Sync TLVs:                          1
    Port Membership TLVs:                       1
    Querier Info TLVs:                          1
    Dynamic Mrouter TLVs:                       1
  RX Errors:
    None

  TX Messages:
    Request Sync TLVs:                          1
    Port Membership TLVs:                       1
    Querier Info TLVs:                          1
    Dynamic Mrouter TLVs:                       1
  TX Errors:
    None
```

The following example shows all summary statistics, including those whose value is zero.

```
Router# show igmp snooping summary statistics include-zeroes

  Bridge Domains:                                      5
  IGMP Snooping Bridge Domains:                        3
  Ports:                                             16
  IGMP Snooping Ports:                               16
  Mrouters:                                            6
  STP Forwarding Ports:                                0
  IGMP Groups:                                         8
    Member Ports:                                    18
  IGMP Source Groups:                                  2
    Static/Include/Exclude:                        0/1/1
    Member Ports (Include/Exclude):                  5/6
  Traffic Statistics (elapsed time since last cleared 02:08:56):
```

```
                                 Received  Reinjected   Generated
Messages:                            7185         898        2395
  IGMP General Queries:              2695           0           0
  IGMP Group Specific Queries:          0           0           0
  IGMP G&S Specific Queries:            0           0           0
  IGMP V2 Reports:                   1796         898         898
  IGMP V3 Reports:                   2694           0        1497
  IGMP V2 Leaves:                       0           0           0
  IGMP Global Leaves:                   0           -           0
  PIM Hellos:                           0           0           -
Rx Packet Treatment:
  Packets Flooded:                                  0
  Packets Forwarded To Members:                     0
  Packets Forwarded To Mrouters:                  898
  Packets Consumed:                              6287
Reports Suppressed:                                 0
IGMP Blocks Ignored in V2 Compat Mode:              0
IGMP EX S-lists Ignored in V2 Compat Mode:          0
Rx Errors:
  Packets On Inactive Bridge Domain:                0
  Packets On Inactive Port:                         0
  Packets Martian:                                  0
  Packets Bad Protocol:                             0
  Packets DA Not Multicast:                         0
  Packets Missing Router Alert:                     0
  Packets Missing Router Alert Drop:                0
  Packets Bad IGMP Checksum:                        0
  Packets TTL Not One:                              0
  Packets TTL Not One Drop:                         0
  Queries Too Short:                                0
  V1 Reports Too Short:                             0
  V2 Reports Too Short:                             0
  V3 Reports Too Short:                             0
  V2 Leaves Too Short:                              0
  IGMP Messages Unknown:                            0
  IGMP Messages GT Max Ver:                         0
  IGMP Messages LT Min Ver:                         0
  Queries Bad Source:                               0
  Queries Dropped by S/W Router Guard:              0
  General Queries DA Not All Nodes:                 0
  GS-Queries Invalid Group:                         0
  GS-Queries DA Not Group:                          0
  GS-Queries Not From Querier:                      0
  GS-Queries Unknown Group:                         0
  Reports Invalid Group:                            0
  Reports Link-Local Group:                         0
  Reports DA Not Group:                             0
  Reports No Querier:                               0
  Leaves Invalid Group:                             0
  Leaves DA Not All Routers:                        0
  Leaves No Querier:                                0
  Leaves Non-Member:                                0
  Leaves Non-Dynamic Member:                        0
  Leaves Non-V2 Member:                             0
  V3 Reports Invalid Group:                         0
  V3 Reports Link-Local Group:                      0
  V3 Reports DA Not All V3 Routers:                 0
  V3 Reports No Querier:                            0
  V3 Reports Older Version Querier:                 0
  V3 Reports Invalid Group Record Type:             0
  V3 Reports No Sources:                            0
  V3 Leaves Non-Member:                             0
  PIM Msgs Dropped by S/W Router Guard:             0
Tx Errors:
    V3 Sources Not Reported:                          0
ICCP Statistics (elapsed time since last cleared 10:56:58):
ICCP Up:                                              3
ICCP Down:                                            3
Congestion Detected:                                  0
Congestion Cleared:                                   0
Peer Up:                                              5
Peer Down:                                            1
ICCP Group Connect attempts:                          4
ICCP Group Connect failures:                          0
ICCP Group Disconnect attempts:                       3
ICCP Group Disconnect failures:                       0
ICCP Group Port Statistics (elapsed time since last cleared 10:56:58):
 Port Created Down:                                  0
 Port Created Standby:                               4
 Port Created Active:                                0
 Port Goes Down:                                     0
 Port Goes Standby:                                  1
 Port Goes Active:                                   2
ICCP Traffic Statistics (elapsed time since last cleared 10:56:58):
 Rx Messages:
  App Data messages:                               21
  App Data NAKs:                                    3
  App Data TLVs:                                   21
  App State TLVs:                                  20
  App State start of sync:                          6
  App State end of sync:                            6
  Global Request Sync TLVs:                         0
  Request Sync TLVs:                                1
  Port Membership TLVs:                            16
  Port Membership adds:                            10
  Port Membership removes:                          2
  Querier Info TLVs:                                0
  Querier Info delete TLVs:                         0
  Dynamic Mrouter TLVs:                             0
  Dynamic Mrouter delete TLVs:                      0
 Rx Errors:
  App State sync TLVs ignored:                      4
  App State TLVs ignored:                           0
  App Data unknown ICCP Group:                      0
  App Data unknown ICCP Group Port:                 0
  App Data wrong ICCP Group:                        0
  App Data BD inactive:                             0
  App Data BD port inactive:                        0
  App Data ICCP Group port not standby:             0
  App Data ICCP Group port not active:              0
  App Data unsupported global TLV type:             0
  App Data truncated:                               0
  App Data length error:                            0
  App Data unsupported TLV type:                    0
  Port Membership TLV ignored, No Querier:          0
  Port Membership TLV error:                        0
  Port Membership TLV too long:                     0
  Querier Info TLV error:                           0
  Dynamic Mrouter TLV error:                        0
  ICCP Rx buffer parse failures:                    0
 Tx Messages:
  ICCP Tx buffer send count:                       11
  App State replay attempts:                        2
  Request Sync TLVs:                                7
  Port Membership TLVs:                             4
  Port Membership adds:                             4
  Port Membership removes:                          2
  Querier Info TLVs:                                0
  Querier Info delete TLVs:                          0
  Dynamic Mrouter TLVs:                              0
  Dynamic Mrouter delete TLVs:                       0
 Tx Errors:
  Request to send App State refused:                 0
  App State replay failures:                         0
  Request Sync TLV Tx failures:                      0
  Port Membership TLV Tx failures:                   0
  Querier Info TLV Tx failures:                      0
  Querier Info delete TLV Tx failures:               0
  Dynamic Mrouter TLV Tx failures:                   0
  Dynamic Mrouter delete TLV Tx failures:            0
  ICCP Get Tx buffer parse failures:                 0
  ICCP Get Tx buffer send failures:                  0
```

show igmp snooping trace

To display IGMP snooping process activity, use the **show igmp snooping trace** command in EXEC mode.

show igmp snooping trace [{**all** | **error** | **packet-error**}]

Syntax Description

all	(Optional) Displays all IGMP snooping process activity.
error	(Optional) Displays only error tracepoints.
packet-error	(Optional) Displays packet error tracepoints.

Command Default

The **all** keyword is the default when no keywords are used.

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to research IGMP snooping process activity.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example shows IGMP snooping process status during a restart and a new profile configuration.

```
Router# show igmp snooping summary trace all
51 wrapping entries (1024 possible, 0 filtered, 51 total)
Feb  2 14:30:24.902 igmpsn/all 0/5/CPU0 t1  TP001:
Feb  2 14:30:24.902 igmpsn/all 0/5/CPU0 t1  TP002: ******** IGMP SNOOP PROCESS RESTART
********
Feb  2 14:30:24.902 igmpsn/all 0/5/CPU0 t1  TP001:
Feb  2 14:30:24.902 igmpsn/all 0/5/CPU0 t1  TP286: initialize profile wavl tree
Feb  2 14:30:24.902 igmpsn/all 0/5/CPU0 t1  TP185: initialize bd wavl tree
Feb  2 14:30:24.902 igmpsn/all 0/5/CPU0 t1  TP230: initialize port wavl tree
Feb  2 14:30:24.902 igmpsn/all 0/5/CPU0 t1  TP019: entered init_chkpt
Feb  2 14:30:24.934 igmpsn/all 0/5/CPU0 t1  TP165: igmpsn_init_l2fib entered
Feb  2 14:30:24.934 igmpsn/all 0/5/CPU0 t1  TP611: l2fib_restart_timer_init
Feb  2 14:30:24.935 igmpsn/all 0/5/CPU0 t1  TP680: igmpsn_pd_mgid_api_init entered
Feb  2 14:30:24.937 igmpsn/all 0/5/CPU0 t1  TP681: failed to open
libl2mc_snoop_mgid_client_pd.dll
Feb  2 14:30:24.937 igmpsn/all 0/5/CPU0 t1  TP683: l2mc_snoop_pd_mgid funcs are stubbed
Feb  2 14:30:25.037 igmpsn/all 0/5/CPU0 t1  TP080: socket open succeeded
Feb  2 14:30:25.037 igmpsn/all 0/5/CPU0 t1  TP031: connection open for socket
Feb  2 14:30:25.037 igmpsn/all 0/5/CPU0 t1  TP614: igmpsn_l2fib_restart_timer_start, 300
secs
Feb  2 14:30:25.038 igmpsn/all 0/5/CPU0 t1  TP555: IGMP SNOOP PROCESS READY
Feb  2 14:30:25.038 igmpsn/all 0/5/CPU0 t1  TP017: entered event loop
Feb  2 14:30:25.038 igmpsn/all 0/5/CPU0 t1  TP112: sysdb register verification
Feb  2 14:30:25.038 igmpsn/all 0/5/CPU0 t1  TP286: initialize profile wavl tree
Feb  2 14:30:25.040 igmpsn/all 0/5/CPU0 t1  TP110: sysdb event verify func (CREATE & SET,
profile/profile1/enter)
Feb  2 14:30:25.040 igmpsn/all 0/5/CPU0 t1  TP287: create profile profile1
Feb  2 14:30:25.040 igmpsn/all 0/5/CPU0 t1  TP534: profile profile1 (0x4826b838): initialized
 static_group tree
(… missing lines)
```

show l2vpn forwarding bridge-domain mroute

To display multicast routes in the forwarding tables, use the **show l2vpn forwarding bridge-domain mroute** command in EXEC mode.

show l2vpn forwarding bridge-domain [*bridge-group-name* **:** *bridge-domain-name*] **mroute** [**ipv4**] **location** *rack*/*slot*/*module*

Syntax Description

bridge-group-name bridge-domain-name	(Optional) Displays information for a specific bridge domain. The colon that separates the two arguments is required.
ipv4	This keyword is required.
location *rack*/*slot*/*module*	Displays route information for a specific rack/slot/module.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays multicast routes as they are converted into the forwarding plane forwarding tables. The source for the conversion is the multicast routes configured in the control plane with IGMP snooping configuration commands. If the routes displayed by this command are not as expected, check the control plane configuration and correct the corresponding IGMP snooping profiles.

Use optional arguments to limit the display to a specific bridge domain.

Task ID

Task ID	Operations
l2vpn	read

Examples

This example displays high-level statistics about routes for one bridge domain:

```
Router# show l2vpn forwarding bridge-domain mroute ipv4 location 0/5/cPU0

mroute ipv4 location 0/5/cPU0
Bridge-Domain Name: nv-mcast:nv-mcast-1
Prefix: (0.0.0.0,224.0.0.0/4) P2MP enabled: N
IRB platform data: {0x84a0000, 0x0, 0x4a00008d, 0x123bb4e0}, len: 16
Ingress
Forwarded (Packets/Bytes): 0/0
Received (Packets/Bytes): 0/0
Punted (Packets/Bytes): 0/0
Dropped (Packets/Bytes): 0/0
```

show l2vpn forwarding bridge-domain mroute detail

To display multicast routes in the forwarding tables, use the **show l2vpn forwarding bridge-domain mroute detail** command in EXEC mode.

show l2vpn forwarding bridge-domain [*bridge-group-name* **:** *bridge-domain-name*] **mroute** [**ipv4**] **detaillocation** *rack*/*slot*/*module*

Syntax Description

bridge-group-name bridge-domain-name	(Optional) Displays information for a specific bridge domain. The colon that separates the two arguments is required.
ipv4	This keyword is required.
location *rack*/*slot*/*module*	Displays route information for a specific rack/slot/module.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 5.2.2	The show output command was enhanced to include the satellite multicast offload information.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays multicast routes as they are converted into the forwarding plane forwarding tables. The source for the conversion is the multicast routes configured in the control plane with IGMP snooping configuration commands. If the routes displayed by this command are not as expected, check the control plane configuration and correct the corresponding IGMP snooping profiles.

Use optional arguments to limit the display to a specific bridge domain.

Task ID

Task ID	Operations
l2vpn	read

Examples

This example displays satellite multicast offload information for one bridge domain.

```
RP/0/0RP0RSP0/CPU0:router:hostname# show l2vpn forwarding bridge-domain mroute ipv4 detail
 location 0/1/cPU0

Bridge-Domain: nv-mcast:nv-mcast-1, ID: 2122
Prefix: (0.0.0.0,224.31.0.1/32) P2MP enabled: N
IRB platform data: {0x84a0001, 0x0, 0x4a000093, 0x115444e0}, len: 16
Ingress
Forwarded (Packets/Bytes): 9278034/7220724021
Received (Packets/Bytes): 0/0
Core Received (Packets/Bytes): 0/0
Core Forwarded (Packets/Bytes): 0/0
Punted (Packets/Bytes): 0/0
Dropped (Packets/Bytes): 0/0
Bridge Port:
GigabitEthernet301/0/0/4, Xconnect id: 0x3880015 SatId: 301, Isid: 0x3fd, Ver: 0x1 , Ring
Id: 0xe000600, oleIsOffLoaded
Forwarded (Packets/Bytes): 9278034/7220724021
Punted (Packets/Bytes): 0/0
Dropped (Packets/Bytes): 0/0
```

show l2vpn forwarding bridge-domain mroute hardware ingress detail

To display multicast routes in the forwarding tables, use the **show l2vpn forwarding bridge-domain mroute hardware ingress detail** command in EXEC mode.

show l2vpn forwarding bridge-domain [*bridge-group-name* **:** *bridge-domain-name*] **mroute** [**ipv4**] **hardware ingressdetaillocation** *rack/slot/module*

Syntax Description

bridge-group-name bridge-domain-name	(Optional) Displays information for a specific bridge domain. The colon that separates the two arguments is required.
ipv4	This keyword is required.
location *rack/slot/module*	Displays route information for a specific rack/slot/module.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 5.2.2	The show output command was enhanced to include the satellite multicast offload information.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays multicast routes as they are converted into the forwarding plane forwarding tables. The source for the conversion is the multicast routes configured in the control plane with IGMP snooping configuration commands. If the routes displayed by this command are not as expected, check the control plane configuration and correct the corresponding IGMP snooping profiles.

Use optional arguments to limit the display to a specific bridge domain.

Task ID

Task ID	Operations
l2vpn	read

Examples

This example displays satellite multicast offload information for one bridge domain. The text in bold indicates the hardware ingress detail information.

```
RP/0/0RP0RSP0/CPU0:router:hostname# show l2vpn forwarding bridge-domain mroute ipv4 hardware
 ingress detail location 0/1/cPU0

Bridge-Domain: satellite:10, ID: 0
  Prefix: (0.0.0.0,224.0.0.0/4)              P2MP enabled: N
  IRB platform data: {0x0, 0x0, 0x8a, 0x939070e0}, len: 16
    Ingress
      Forwarded (Packets/Bytes): 0/0
      Received (Packets/Bytes): 0/0
      Core Received (Packets/Bytes): 0/0
      Core Forwarded (Packets/Bytes): 0/0
      Punted (Packets/Bytes): 0/0
      Dropped (Packets/Bytes): 0/0
  Platform multicast leaf context:
--------------------------------------------------------------------------
Legend:
Route information - (Ingress)
C: NP ID, IR: MGID Mask
IS: Single SHG0 on LC, IX: Single SHG0 XID
IA0: FGID_SHG0, IA1: FGID_SHG1, IA2: FGID_SHG2
IG: Multicast group ID, IB: Base statistics pointer
Route information - (Egress)
ET: Table ID for OLIST lookup, EO: OLIST count bit, ER: MLI
EC1: SHG1 OLIST members count on this chip,
EC2: SHG2 OLIST members count on this chip,
EC: Total count of OLIST members on this chip,
SD: Single OLIST member Optimization,
Hardware Information
C: NP ID; T: Table ID; M: Member ID;  I: IRB OLE; U: XID-ID,
RF0: R_FGID_SHG0, RF1: R_FGID_SHG1, RF2: R_FGID_SHG2, O: Offloaded
Statistics Information
S: Source, G: Group, Pr: Prefix Length, C: NP ID, R: Received,
FF: Forwarded to fabric, P: Punted to CPU, D: Dropped,
F: Forwarded, CR: Core Received, CF: Core Forwarded
--------------------------------------------------------------------------

Source: *               Group: 224.0.0.0       Mask length: 4

  IRB Route Notification Information

------------------------------------------------------------------------------------------

  Bridge_ID:0x0       NP_Mask:0x0    Rack0 Slot_Mask:0x0   Rack1 Slot_Mask:0x0
Master_Slot:0x0

------------------------------------------------------------------------------------------


   VPLS LSM Inclusive Tree Local Rack Information

------------------------------------------------------------------------------------------

  Route_LSM_Flag: F                                 Head Label NP Mask:[old:0x0, new:0x0]
  Latest Update from Bud Label MGID:     0           All Route OLE NP Mask: 0x1

------------------------------------------------------------------------------------------


   VPLS LSM Inclusive Tree Remote Rack Information

------------------------------------------------------------------------------------------

  Head Label Slot Mask:[old:0x0, new:0x0]       Aggregated Bud Label Slot Mask:[old:0x0,
new:0x0]

------------------------------------------------------------------------------------------


  Route Information

------------------------------------------------------------------------------------------

  C  IR    IS IX       IA0     IA1     IA2     IG      IB         ET EO ER      EC1   EC2
 EC    SD

------------------------------------------------------------------------------------------
```

```
  0  0x0   F  0x0      0x0     0x0     0x0     0x4233  0x53017c   0  F  2      0     0
 0     0
  1  0x0   F  0x0      0x0     0x0     0x0     0x4233  0x53031c   0  F  2      0     0
 0     0

-----------------------------------------------------------------------------------------



  Statistics Information:  S: *  G: 224.0.0.0  Pr: 4
  -----------------------------------------------------------------------
  C     R(packets:bytes)/FF(packets:bytes)/P(packets)/D(packets)
  -----------------------------------------------------------------------
  0     0:0 / 0:0 / 0 / 0
  1     0:0 / 0:0 / 0 / 0
  -----------------------------------------------------------------------


Bridge-Domain: satellite:10, ID: 0
  Prefix: (192.10.1.2,232.0.0.1/64)          P2MP enabled: N
  IRB platform data: {0x1, 0x0, 0x8b, 0x92203ce8}, len: 16
    Ingress
      Forwarded (Packets/Bytes): 886211028/239276977560
      Received (Packets/Bytes): 0/0
      Core Received (Packets/Bytes): 0/0
      Core Forwarded (Packets/Bytes): 0/0
      Punted (Packets/Bytes): 0/0
      Dropped (Packets/Bytes): 0/0
  Bridge Port:
  GigabitEthernet100/0/0/22, Xconnect id: 0x1880010  SatId: 100, Isid: 0x3f2, Ver: 0x1 ,
Ring Id: 0x60000c0, oleIsOffLoaded
      Forwarded (Packets/Bytes): 0/0
      Punted (Packets/Bytes): 0/0
      Dropped (Packets/Bytes): 0/0
  GigabitEthernet100/0/0/32, Xconnect id: 0x1880011  SatId: 100, Isid: 0x3f2, Ver: 0x1 ,
Ring Id: 0x60000c0, oleIsOffLoaded
      Forwarded (Packets/Bytes): 0/0
      Punted (Packets/Bytes): 0/0
      Dropped (Packets/Bytes): 0/0
  GigabitEthernet200/0/0/34, Xconnect id: 0x1880013  SatId: 200, Isid: 0x3f2, Ver: 0x1 ,
Ring Id: 0x60000c0, oleIsOffLoaded
      Forwarded (Packets/Bytes): 886236660/239283898200
      Punted (Packets/Bytes): 0/0
      Dropped (Packets/Bytes): 0/0

  Platform multicast leaf context:Source: 192.10.1.2     Group: 232.0.0.1      Mask length:
 64

  IRB Route Notification Information

-----------------------------------------------------------------------------------------

  Bridge_ID:0x0       NP_Mask:0x1    Rack0 Slot_Mask:0x8   Rack1 Slot_Mask:0x0
Master_Slot:0x0

-----------------------------------------------------------------------------------------


   VPLS LSM Inclusive Tree Local Rack Information

-----------------------------------------------------------------------------------------

  Route_LSM_Flag: F                                 Head Label NP Mask:[old:0x0, new:0x0]
  Latest Update from Bud Label MGID:     0           All Route OLE NP Mask: 0x1
```

```
------------------------------------------------------------------------------------------


   VPLS LSM Inclusive Tree Remote Rack Information

------------------------------------------------------------------------------------------

  Head Label Slot Mask:[old:0x0, new:0x0]       Aggregated Bud Label Slot Mask:[old:0x0,
new:0x0]

------------------------------------------------------------------------------------------


  Route Information

------------------------------------------------------------------------------------------

  C  IR    IS IX       IA0     IA1     IA2     IG      IB         ET EO ER     EC1   EC2
 EC    SD

------------------------------------------------------------------------------------------

  0  0x1   T  0x6300013 0x0     0x8     0x8     0x4234  0x530f98   1  T  3      0     0
  1     1
  1  0x1   T  0x6300013 0x0     0x8     0x8     0x4234  0x530390   1  F  3      0     0
  0     0

------------------------------------------------------------------------------------------


  Hardware Information
  -----------------------------------------------------------------------
  C  T  M  I                U      RF0     RF1     RF2     O  ISID  VER
  -----------------------------------------------------------------------
  0  1  0  F                0x13   0x0     0x0     0x0     T  0x3f2 0x1
  -----------------------------------------------------------------------

  Statistics Information:  S: 192.10.1.2  G: 232.0.0.1  Pr: 64
  -----------------------------------------------------------------------
  C     R(packets:bytes)/FF(packets:bytes)/P(packets)/D(packets)
  -----------------------------------------------------------------------
  0     0:0 / 886721677:239414852790 / 0 / 0
  1     0:0 / 0:0 / 0 / 0
  -----------------------------------------------------------------------
  XID Statistics:
  -----------------------------------------------------------------------
  C     XID-ID          Stats Ptr  F/P/D (packets:bytes)
  -----------------------------------------------------------------------
  0     0x13            0x530fa4    886211028:239276977560 / 0:0 / 0:0

  Offloaded XID Information
  ----------------------------------------------------------------------------------------

  XID-ID     IFHandle Ring CSFL       ISID  VER  O:M SAT-ID   F/P/D (packets:bytes)
  ----------------------------------------------------------------------------------------

  0x10       0x6009600  0  0x60000c0  0x3f2 0x1  1:0 100        0:0   0:0   0:0
  0x11       0x6009880  0  0x60000c0  0x3f2 0x1  1:0 100        0:0   0:0   0:0
  0x13       0x600a400  0  0x60000c0  0x3f2 0x1  1:1 200        0:0   0:0   0:0
  ----------------------------------------------------------------------------------------


Bridge-Domain: satellite:20, ID: 1
```

```
  Prefix: (0.0.0.0,224.0.0.0/4)              P2MP enabled: N
  IRB platform data: {0x10000, 0x0, 0x100008a, 0x939ea8e0}, len: 16
    Ingress
      Forwarded (Packets/Bytes): 0/0
      Received (Packets/Bytes): 0/0
      Core Received (Packets/Bytes): 0/0
      Core Forwarded (Packets/Bytes): 0/0
      Punted (Packets/Bytes): 0/0
      Dropped (Packets/Bytes): 0/0

 Platform multicast leaf context:Source: *             Group: 224.0.0.0      Mask length:
 4

  IRB Route Notification Information

------------------------------------------------------------------------------------------

  Bridge_ID:0x1       NP_Mask:0x0    Rack0 Slot_Mask:0x0   Rack1 Slot_Mask:0x0
Master_Slot:0x0

------------------------------------------------------------------------------------------


   VPLS LSM Inclusive Tree Local Rack Information

------------------------------------------------------------------------------------------

  Route_LSM_Flag: F                                Head Label NP Mask:[old:0x0, new:0x0]
  Latest Update from Bud Label MGID:     0           All Route OLE NP Mask: 0x1

------------------------------------------------------------------------------------------


   VPLS LSM Inclusive Tree Remote Rack Information

------------------------------------------------------------------------------------------

  Head Label Slot Mask:[old:0x0, new:0x0]       Aggregated Bud Label Slot Mask:[old:0x0,
new:0x0]

------------------------------------------------------------------------------------------


  Route Information

------------------------------------------------------------------------------------------

  C  IR    IS IX       IA0     IA1     IA2     IG      IB         ET EO ER     EC1   EC2
 EC    SD

------------------------------------------------------------------------------------------

  0  0x0   F  0x0      0x0     0x0     0x0     0x4232  0x530178   0  F  1      0     0
 0     0
  1  0x0   F  0x0      0x0     0x0     0x0     0x4232  0x530318   0  F  1      0     0
 0     0

------------------------------------------------------------------------------------------



  Statistics Information:  S: *  G: 224.0.0.0  Pr: 4
  -----------------------------------------------------------------------
  C     R(packets:bytes)/FF(packets:bytes)/P(packets)/D(packets)
  -----------------------------------------------------------------------
  0     0:0 / 0:0 / 0 / 0
  1     0:0 / 0:0 / 0 / 0
  -----------------------------------------------------------------------


Bridge-Domain: satellite:20, ID: 1
  Prefix: (192.10.1.2,232.0.0.1/64)          P2MP enabled: N
  IRB platform data: {0x10001, 0x0, 0x100008b, 0x920484e8}, len: 16
    Ingress
      Forwarded (Packets/Bytes): 886199961/239273989470
      Received (Packets/Bytes): 0/0
      Core Received (Packets/Bytes): 0/0
      Core Forwarded (Packets/Bytes): 0/0
      Punted (Packets/Bytes): 0/0
      Dropped (Packets/Bytes): 0/0
  Bridge Port:
  GigabitEthernet200/0/0/23, Xconnect id: 0x1880012  SatId: 200, Isid: 0x3f3, Ver: 0x1 ,
Ring Id: 0x60000c0, oleIsOffLoaded
      Forwarded (Packets/Bytes): 0/0
      Punted (Packets/Bytes): 0/0
      Dropped (Packets/Bytes): 0/0
  GigabitEthernet300/0/0/25, Xconnect id: 0x1880014  SatId: 300, Isid: 0x3f3, Ver: 0x1 ,
Ring Id: 0x60000c0, oleIsOffLoaded
      Forwarded (Packets/Bytes): 0/0
      Punted (Packets/Bytes): 0/0
      Dropped (Packets/Bytes): 0/0
  GigabitEthernet300/0/0/34, Xconnect id: 0x1880015  SatId: 300, Isid: 0x3f3, Ver: 0x1 ,
Ring Id: 0x60000c0, oleIsOffLoaded
      Forwarded (Packets/Bytes): 886308945/239303415150
      Punted (Packets/Bytes): 0/0
      Dropped (Packets/Bytes): 0/0

  Platform multicast leaf context:Source: 192.10.1.2     Group: 232.0.0.1      Mask length:
 64

  IRB Route Notification Information

------------------------------------------------------------------------------------------

  Bridge_ID:0x1       NP_Mask:0x1    Rack0 Slot_Mask:0x8   Rack1 Slot_Mask:0x0
Master_Slot:0x0

------------------------------------------------------------------------------------------


   VPLS LSM Inclusive Tree Local Rack Information

------------------------------------------------------------------------------------------

  Route_LSM_Flag: F                                 Head Label NP Mask:[old:0x0, new:0x0]
  Latest Update from Bud Label MGID:     0           All Route OLE NP Mask: 0x1

------------------------------------------------------------------------------------------


   VPLS LSM Inclusive Tree Remote Rack Information

------------------------------------------------------------------------------------------

  Head Label Slot Mask:[old:0x0, new:0x0]       Aggregated Bud Label Slot Mask:[old:0x0,
new:0x0]

------------------------------------------------------------------------------------------
```

```
  Route Information

------------------------------------------------------------------------------------------

  C  IR    IS IX       IA0     IA1     IA2     IG      IB         ET EO ER     EC1   EC2
 EC    SD

------------------------------------------------------------------------------------------

  0  0x1   T  0x6300015 0x0     0x8     0x8     0x4236  0x530f9c   0  T  4      0     0
  1     1
  1  0x1   T  0x6300015 0x0     0x8     0x8     0x4236  0x530394   0  F  4      0     0
  0     0

------------------------------------------------------------------------------------------


  Hardware Information
  -----------------------------------------------------------------------
  C  T  M  I                U      RF0     RF1     RF2     O  ISID  VER
  -----------------------------------------------------------------------
  0  0  0  F                0x15   0x0     0x0     0x0     T  0x3f3 0x1
  -----------------------------------------------------------------------

  Statistics Information:  S: 192.10.1.2  G: 232.0.0.1  Pr: 64
  -----------------------------------------------------------------------
  C     R(packets:bytes)/FF(packets:bytes)/P(packets)/D(packets)
  -----------------------------------------------------------------------
  0     0:0 / 886721671:239414851170 / 0 / 0
  1     0:0 / 0:0 / 0 / 0
  -----------------------------------------------------------------------
  XID Statistics:
  -----------------------------------------------------------------------
  C     XID-ID          Stats Ptr  F/P/D (packets:bytes)
  -----------------------------------------------------------------------
  0     0x15            0x530fac    886199961:239273989470 / 0:0 / 0:0

  Offloaded XID Information
  ----------------------------------------------------------------------------------------

  XID-ID     IFHandle Ring CSFL       ISID  VER  O:M SAT-ID   F/P/D (packets:bytes)
  ----------------------------------------------------------------------------------------

  0x12       0x600a140  0  0x60000c0  0x3f3 0x1  1:0 200        0:0   0:0   0:0
  0x14       0x600acc0  0  0x60000c0  0x3f3 0x1  1:0 300        0:0   0:0   0:0
  0x15       0x600af00  0  0x60000c0  0x3f3 0x1  1:1 300        0:0   0:0   0:0
  ----------------------------------------------------------------------------------------
```

show mld snooping bridge-domain

To display MLD snooping configuration information and traffic statistics for bridge domains, use the **show mld snooping bridge-domain** command in EXEC mode.

show mld snooping bridge-domain [*bridge-domain-name*] [**detail** [**statistics** [**include-zeroes**]]]

Syntax Description

bridge-domain-name	(Optional) Displays information only for the specified bridge domain.
detail	(Optional) Includes more details, including configuration information about the bridge domain querier.
statistics	(Optional) Includes traffic counters and statistics.
include-zeroes	(Optional) Includes all statistics, even if they are zero. Without this keyword, many statistics are omitted from the display when their values are zero.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays mld snooping information by bridge domain. Use the command without any keywords to display summary information about all bridge domains, in a single line per bridge domain.

Use optional keywords to request additional details and traffic statistics per bridge domain. You can also limit the display to a single bridge domain.

The **statistics** keyword displays mld traffic information, including mld queries, reports, and leaves. The three columns in the statistics section of the display are:

- Received—Number of packets received.
- Reinjected—Number of packets received, processed, and reinjected back into the forwarding path.
- Generated—Number of packets generated by the mld snooping application and injected into the forwarding path.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example shows the basic command without any keywords.

```
Router# show mld snooping bridge-domain

Bridge Domain         Profile               Act Ver  #Ports #Mrtrs  #Grps  #Srcs
-------------         -------               --- ---  ------ ------  -----  -----
Domain1:BD-1          profile1                Y  V2    8195      0   4096      0
Domain1:BD-4          profile1                Y  V2     100      2    512      0
Domain1:BD-7          profile1                Y  V2      55      0     44      0
```

The following example shows the summary line for a named bridge domain.

```
Router# show mld snooping bridge-domain Group1:BD-1


Bridge Domain        Profile              Act Ver  #Ports #Mrtrs  #Grps  #Srcs
-------------        -------              --- ---  ------ ------  -----  -----
Domain1:BD-1         profile1               Y  V2    8195      0   4096      0
```

The following example shows detailed information about all bridge domains:

```
Router# show mld snooping bridge-domain detail


Bridge Domains:                  5
MLD Snooping Bridge Domains:     3

Bridge Domain        Profile              Act Ver  #Ports #Mrtrs  #Grps  #Srcs
-------------        -------              --- ---  ------ ------  -----  -----
Domain1:BD-1         profile1               Y  V2    8195      0   4096      0

  Profile Configured Attributes:
    System IP Address:                   fe80::1aef:63ff:fee2:5fc6
    Minimum Version:                     1
    Report Suppression:                  Enabled
    Unsolicited Report Interval:         1000 (milliseconds)
    TCN Query Solicit:                   Disabled
    TCN Membership Sync:                 Disabled
    TCN Flood:                           Enabled
    TCN Flood Query Count:               2
    Router Alert Check:                  Enabled
    TTL Check:                           Enabled
    Internal Querier Support:            Disabled
    Querier Query Interval:              125 (seconds)
    Querier LMQ Interval:                1000 (milliseconds)
    Querier LMQ Count:                   2
    Querier Robustness:                  2
    Startup Query Interval:              0 seconds
    Startup Query Count:                 0
    Startup Query Max Response Time:     0.0 seconds
    Mrouter Forwarding:                  Enabled
  Querier:                               Not Present
  Mrouter Ports:                         0
  STP Forwarding Ports:                  0
  ICCP Group Ports:                      0
  Groups:                                0
   Member Ports:                         0
  V2 Source Groups:                      0
   Static/Include/Exclude:               0/0/0
   Member Ports (Include/Exclude):       0/0
Bridge Domain        Profile              Act Ver  #Ports #Mrtrs  #Grps  #Srcs
-------------        -------              --- ---  ------ ------  -----  -----
Domain1:BD-4         profile1               Y  V2     100      3    512      0
  Profile Configured Attributes:
    System IP Address:                   fe80::1aef:63ff:fee2:5fc6
    Minimum Version:                     1
    Report Suppression:                  Enabled
    Unsolicited Report Interval:         1000 (milliseconds)
    TCN Query Solicit:                   Disabled
    TCN Membership Sync:                 Disabled
    TCN Flood:                           Enabled
    TCN Flood Query Count:               2
    Router Alert Check:                  Enabled
    TTL Check:                           Enabled
    Internal Querier Support:            Disabled
    Querier Query Interval:              125 (seconds)
    Querier LMQ Interval:                1000 (milliseconds)
    Querier LMQ Count:                   2
    Querier Robustness:                  2
    Startup Query Interval:              0 seconds
    Startup Query Count:                 0
    Startup Query Max Response Time:     0.0 seconds
    Mrouter Forwarding:                  Enabled
  Querier:                               Not Present
  Mrouter Ports:                         0
  STP Forwarding Ports:                  0
  ICCP Group Ports:                      0
  Groups:                                0
   Member Ports:                         0
  V2 Source Groups:                      0
   Static/Include/Exclude:               0/0/0
   Member Ports (Include/Exclude):       0/0
```

The following example displays traffic statistics with detailed information. The display omits many statistics whose values are zero.

```
Router# show mld snooping bridge-domain Group1:BD-1 detail statistics


Bridge Domain        Profile              Act Ver  #Ports #Mrtrs  #Grps  #Srcs
-------------        -------              --- ---  ------ ------  -----  -----
Domain1:BD-1         profile1               Y  V2    8195      0   4096      0

  Profile Configured Attributes:
    System IP Address:                   fe80::1aef:63ff:fee2:5fc6
    Minimum Version:                     1
    Report Suppression:                  Enabled
    Unsolicited Report Interval:         1000 (milliseconds)
    TCN Query Solicit:                   Disabled
    TCN Membership Sync:                 Disabled
    TCN Flood:                           Enabled
    TCN Flood Query Count:               2
    Router Alert Check:                  Enabled
    TTL Check:                           Enabled
    Internal Querier Support:            Disabled
    Querier Query Interval:              125 (seconds)
    Querier LMQ Interval:                1000 (milliseconds)
    Querier LMQ Count:                   2
    Querier Robustness:                  2
    Startup Query Interval:              0 seconds
    Startup Query Count:                 0
    Startup Query Max Response Time:     0.0 seconds
    Mrouter Forwarding:                  Enabled
  Querier:                               Not Present
  Mrouter Ports:                         0
  STP Forwarding Ports:                  0
  ICCP Group Ports:                      0
  Groups:                                0
    Member Ports:                        0
  V2 Source Groups:                      0
    Static/Include/Exclude:              0/0/0
    Member Ports (Include/Exclude):      0/0
  Traffic Statistics (elapsed time since last cleared 00:54:30):
```

```
                                    Received  Reinjected   Generated
   Messages:                               0           0           0
     MLD  General Queries:                 0           0           0
     MLD  Group Specific Queries:          0           0           0
     MLD  G&S Specific Queries:            0           0           0
     MLD  V1 Reports:                      0           0           0
     MLD  V2 Reports:                      0           0           0
     MLD  V1 Leaves:                       0           0           0
     MLD  Global Leaves:                   0           -           0
     PIM Hellos:                           0           0           -
   Rx Packet Treatment:
      Packets Flooded:                                  0
      Packets Forwarded To Members:                     0
      Packets Forwarded To Mrouters:                    0
      Packets Consumed:                                 0
   Rx Errors:
    Packets DA Not Multicast:                         4
   Rx Other:
    None
   Tx Errors:
      None
   Startup Query Sync Statistics:
     None
```

The following example shows details for all statistics regardless of whether their values are zero.

```
Router# show mld snooping bridge-domain Group1:BD-1 detail statistics include-zeroes

Bridge Domain        Profile             Act Ver  #Ports #Mrtrs  #Grps  #Srcs
-------------        -------             --- ---  ------ ------  -----  -----
BD-1                 profile1              Y  V2    8195      0   4096      0

  Profile Configured Attributes:
    System IP Address:                   fe80::1aef:63ff:fee2:5fc6
    Minimum Version:                     1
    Report Suppression:                  Enabled
    Unsolicited Report Interval:         1000 (milliseconds)
    TCN Query Solicit:                   Disabled
    TCN Membership Sync:                 Disabled
    TCN Flood:                           Enabled
    TCN Flood Query Count:               2
    Router Alert Check:                  Enabled
    TTL Check:                           Enabled
    Internal Querier Support:            Disabled
    Querier Query Interval:              125 (seconds)
    Querier LMQ Interval:                1000 (milliseconds)
    Querier LMQ Count:                   2
    Querier Robustness:                  2
    Startup Query Interval:              0 seconds
    Startup Query Count:                 0
    Startup Query Max Response Time:     0.0 seconds
    Mrouter Forwarding:                  Enabled
  Querier:                               Not Present
  Mrouter Ports:                         0
  STP Forwarding Ports:                  0
  ICCP Group Ports:                      0
  Groups:                                0
    Member Ports:                        0
  V2 Source Groups:                      0
    Static/Include/Exclude:              0/0/0
    Member Ports (Include/Exclude):      0/0
  Traffic Statistics (elapsed time since last cleared 00:55:19):
                                     Received  Reinjected   Generated
```

```
Messages:                               0           0           0
  MLD  General Queries:                 0           0           0
  MLD  Group Specific Queries:          0           0           0
  MLD  G&S Specific Queries:            0           0           0
  MLD  V1 Reports:                      0           0           0
  MLD  V2 Reports:                      0           0           0
  MLD  V1 Leaves:                       0           0           0
  MLD  Global Leaves:                   0           -           0
  PIM Hellos:                           0           0           -
Rx Packet Treatment:
  Packets Flooded:                                  0
  Packets Forwarded To Members:                     0
  Packets Forwarded To Mrouters:                    0
  Packets Consumed:                                 0
  Reports Suppressed:                               0
  Access Group Permits:                             0
  Access Group Denials:                             0
  Group Limits Exceeded:                            0
  MLD  Blocks Ignored in V1 Compat Mode:            0
  MLD  EX S-lists Ignored in V1 Compat Mode:        0
Rx MLD  V2 Report Group Record Types:
  Is Include:                                       0
  Change To Include:                                0
  Is Exclude:                                       0
  Change To Exclude:                                0
  Allow New Sources:                                0
  Block Old Sources:                                0
Rx Errors:
  Packets On Inactive Bridge Domain:                0
  Packets On Inactive Port:                         0
  Packets Martian:                                  0
  Packets Bad Protocol:                             0
  Packets DA Not Multicast:                         4
  Packets Missing Router Alert:                     0
  Packets Missing Router Alert Drop:                0
  Packets Bad mld  Checksum:                        0
  Packets TTL Not One:                              0
  Packets TTL Not One Drop:                         0
  Queries Too Short:                                0
  V1 Reports Too Short:                             0
  V2 Reports Too Short:                             0
  V1 Leaves Too Short:                              0
  MLD  Messages Unknown:                            0
  MLD  Messages GT Max Ver:                         0
  MLD  Messages LT Min Ver:                         0
  Queries Bad Source:                               0
  Queries Dropped by S/W Router Guard:              0
  General Queries DA Not All Nodes:                 0
  GS-Queries Invalid Group:                         0
  GS-Queries DA Not Group:                          0
  GS-Queries Not From Querier:                      0
  GS-Queries Unknown Group:                         0
  Reports Invalid Group:                            0
  Reports Link-Local Group:                         0
  Reports DA Not Group:                             0
  Reports No Querier:                               0
  Leaves Invalid Group:                             0
  Leaves Invalid DA:                                0
  Leaves No Querier:                                0
  Leaves Non-Member:                                0
  Leaves Non-Dynamic Member:                        0
  Leaves Non-V1 Member:                             0
  V2 Reports Invalid Group:                         0
  V2 Reports Link-Local Group:                      0
```

```
      V2 Reports DA Not All V2 Routers:                 0
      V2 Reports No Querier:                            0
      V2 Reports Older Version Querier:                 0
      V2 Reports Invalid Group Record Type:             0
      V2 Reports No Sources:                            0
      V2 Leaves Non-Member:                             0
      PIM Msgs Dropped by S/W Router Guard:             0
    Rx Other:
      Proxy General Queries:                            0
      Proxy GS-Queries:                                 0
      Proxy Reports:                                    0
    Tx Errors:
      V2 Sources Not Reported:                          0
      No Querier in BD:                                 0
      No L2 Info for BD:                                0
  Startup Query Sync Statistics:
    Stale Port Groups Deleted:                          0
    Stale Port Group Sources Deleted:                   00
```

show mld snooping group

To display MLD group membership information, use the **show mld snooping group** command in EXEC mode.

{**show mld snooping group** [**summary** [*group-address*] [{**bridge-domain** *bridge-domain-name* | **port** {**interface-name** | **neighbor** *ipaddr* **pw-id** *id*}}]] | [[*group-address*] [{**bridge-domain** *bridge-domain-name* | **port** {*interface-name* | **neighbor** *ipaddr* **pw-id** *id*}}] [**source** *source-address*] [**detail**]]}

Syntax Description

summary	(Optional) Provides per group summary information.
group-address	(Optional) Provides IP group address information for the specified group in *A.B.C.D* format.
bridge-domain *bridge-domain-name*	(Optional) Provides group membership information for the specified bridge domain.
port *interface-name*	(Optional) Provides group membership information for the specified AC port.
port neighbor *ipaddr* **pw-id** *id*	(Optional) Provides group membership information for the specified PW port.
source *source-address*	(Optional) Provides group membership information for groups indicating interest in a specified source address.
detail	(Optional) Provides detailed information in a multiline display per group.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to display information about group membership in the Layer -2 forwarding tables. The display includes indicators identifying whether the group information was obtained dynamically (for example, snooped) or statically configured.

The command offers the following levels of detail:

- The basic command with no keywords displays group membership information as one line per port within group.
- The **summary** keyword summarizes the port statistics into one line per group. The **summary** keyword is mutually exclusive with the **port-view**, **source**, and **detail** keywords.
- The **detail** keyword includes traffic statistics and counters.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example shows group membership information by groups within bridge domains.

```
Router# show mld snooping group

Flags Key: S=Static, D=Dynamic, E=Explicit Tracking

                 Bridge Domain bg1:bd1

Group           Ver GM  Source           PM  Port                     Exp Flg

Ff12:1:1::1     V2  Exc  -               -   GigabitEthernet0/1/1/0   122  DE
Ff12:1:1::1     V2  Exc  2002:1::1       Inc GigabitEthernet0/1/1/1     5  DE
Ff12:1:1::1     V2  Exc  2002:1::1       Inc GigabitEthernet0/1/1/2 never   S
Ff12:1:1::1     V2  Exc  2002:1::1       Exc GigabitEthernet0/1/1/3     -  DE
Ff12:1:1::1     V2  Exc  2002:1::2       Inc GigabitEthernet0/1/1/0   202  DE
Ff12:1:1::1     V2  Exc  2002:1::2       Exc GigabitEthernet0/1/1/1     -  DE
Ff12:1:1::2     V2  Exc  2002:1::1       Inc GigabitEthernet0/1/1/0   145  DE
Ff12:1:1::2     V2  Exc  2002:1::1       Inc GigabitEthernet0/1/1/1     0  DE
Ff12:1:1::2     V2  Exc  2002:1::1       Exc GigabitEthernet0/1/1/2    11  DE


                 Bridge Domain bg1:bd4

Group           Ver GM  Source           PM  Port                     Exp Flg

Ff24:1:1::2     V1  Exc  -               -   GigabitEthernet0/1/1/0   122  DE
Ff28:1:1::1     V1  -    -               -   GigabitEthernet0/1/1/1    33  DE
Ff29:1:2::3     V1  Exc  -               -   GigabitEthernet0/1/2/0   122  DE
```

```
Ff22:1:2::3     V2  Exc  2000:1:1::2     Exc GigabitEthernet0/1/2/1     5  DE
```

The following example shows group membership information by group within a specific bridge domain.

```
Router# show mld snooping group bridge-domain Group1:BD-1

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking

                 Bridge Domain bg1:bd1

Group           Ver GM  Source           PM  Port                     Exp Flg

Ff12:1:1::1     V2  Exc  -               -   GigabitEthernet0/1/1/0   122  DE
Ff12:1:1::1     V2  Exc  2002:1::1       Inc GigabitEthernet0/1/1/1     5  DE
Ff12:1:1::1     V2  Exc  2002:1::1       Inc GigabitEthernet0/1/1/2 never   S
Ff12:1:1::1     V2  Exc  2002:1::1       Exc GigabitEthernet0/1/1/3     -  DE
Ff12:1:1::1     V2  Exc  2002:1::2       Inc GigabitEthernet0/1/1/0   202  DE
Ff12:1:1::1     V2  Exc  2002:1::2       Exc GigabitEthernet0/1/1/1     -  DE
Ff12:1:1::2     V2  Exc  2002:1::1       Inc GigabitEthernet0/1/1/0   145  DE
Ff12:1:1::2     V2  Exc  2002:1::1       Inc GigabitEthernet0/1/1/1     0  DE
Ff12:1:1::2     V2  Exc  2002:1::1       Exc GigabitEthernet0/1/1/2    11  DE
```

The following example shows group membership information by groups within a specific port.

```
Router# show mld snooping group port GigabitEthernet 0/1/1/1

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking

                 Bridge Domain bg1:bd1

Group           Ver GM  Source           PM  Port                     Exp Flg

Ff12:1:1::1     V2  Exc  2002:1::1       Inc GigabitEthernet0/1/1/1     5  DE
Ff12:1:1::2     V2  Exc  2002:1::2       Exc GigabitEthernet0/1/1/1     -  DE
Ff12:1:1::3     V2  Exc  2002:1::3       Inc GigabitEthernet0/1/1/1     0  DE
```

The following example summarizes each group's membership information into a single line.

```
Router# show mld snooping group summary

                            Bridge Domain bg1:bd1

Group           Ver GM #Ports   #Srcs  #Hosts
Ff12:1:1::1     V1  -       5       -       -
Ff12:1:1::2     V2  Exc    22      55      78
Ff12:1:1::3     V2  Exc     2       2       2
Ff12:1:1::4     V2  Inc    12      12      12
Ff12:1:1::5     V2  Exc    22      22      22

                 Bridge Domain bg1:bd4

Group           Ver  GM #Ports   #Srcs  #Hosts
Ff22:1:1::1     V2  Inc     9      21      28
```

```
Ff22:1:1::2     V2  Exc    23      23      25
```

The following example shows detail information about each group.

```
Router# show mld snooping group detail

                Flags Key: S=Static, D=Dynamic, E=Explicit Tracking

                 Bridge Domain bg1:bd1

Group Address:                             ff28:1:2::3
  Version:                                        V2
  Uptime:                                   02:22:22
  Group Filter Mode:                         Exclude
  Expires:                                       158
  Static Port Group Count:                         2
  Source Count:                                   10
  Include Source Count:                            6
  Exclude Source Count:                            6
  Static Include Source Count:                     2
  Source:                                       star
    Include Port Count:                            1
    Exclude Port Count:                            1
    Static Include Port Count:                     0
    Include Ports:
      GigabitEthernet0/1/1/0           02:02:22   145 D
    Exclude Ports:
      GigabitEthernet0/1/1/1           02:02:22   222 DE
Source:                                     2000:1:2::3
    Include Port Count:                            4
    Exclude Port Count:                            3
        Static Include Port Count:                     3
    Include Ports:
      GigabitEthernet0/1/1/0           02:02:22 never S
      GigabitEthernet0/1/1/1           02:02:22    15 DE
      GigabitEthernet0/1/1/2           02:02:22    98 SE
      GigabitEthernet0/1/1/3           02:02:22 never S
    Exclude Ports:
      GigabitEthernet0/1/1/4           02:02:22    22 D
      GigabitEthernet0/1/1/5           02:02:22     2 DE
      GigabitEthernet0/1/1/6           02:02:22     0 D
  Source:                                   2000:1:2::4
    Include Port Count:                            1
    Exclude Port Count:                            1
    Static Include Port Count:                     0
    Include Ports:
      GigabitEthernet0/1/1/0           02:02:22    34 D
    Exclude Ports:
      GigabitEthernet0/1/1/1           02:02:22    34 E
Group Address:                             ff28:2:2::4
  Version:                                        V1
  Uptime:                                   02:22:22
  Expires:                                       115
      Port Count:                                      3
  Ports:
   GigabitEthernet0/1/1/0              02:02:22    29 D
   GigabitEthernet0/1/1/1              02:02:22   310 D
   GigabitEthernet0/1/1/2              02:02:22    12 D
```

show mld snooping port

To display MLD snooping configuration information and traffic counters by router interface port, use the **show mld snooping port** command in EXEC mode.

show mld snooping port
interface-name | **neighbor** *ipaddr* **pw-id** *id* | **bridge-domain** **bridge-domain-name**
detail [**statistics** [**include-zeroes**]]
group [*group-address*] [**source** *source-address*] [**detail**]

Syntax Description

interface-name	(Optional) Displays information only for the specified AC port.
neighbor *ipaddr* **pw-id** *id*	(Optional) Displays information only for the specified PW port.
bridge-domain *bridge-domain-name*	(Optional) Displays information for ports in the specified bridge domain.
detail	(Optional) Includes port details, rather than a single line summary.
statistics	(Optional) Includes mld traffic counters and statistics in the detail display.
include-zeroes	(Optional) Includes all statistics, even if they are zero. Without this keyword, many statistics are omitted from the display when their values are zero.
group	(Optional) Provides group membership information in its entirety as received at each port. The display is organized by port, showing groups within ports.
group-address	(Optional) Displays information only for the specified group address, organized by port.
source *source-address*	(Optional) Displays information only for the specified source address, organized by port.
detail	(Optional) Includes group details.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays mld snooping information organized by mld snooping port. Use the command without any keywords to display summary information about all ports, in a single line per port.

Use optional arguments and keywords to request the following:

- Limit the display to a specified port.
- Limit the display to ports under a specified bridge.
- Request details and traffic statistics per port.

Note The **statistics** keyword cannot be used in the same command with the **group** keyword.

- Organize the display by group within ports. Use the **group** keyword with or without a specified interface or bridge domain.
- Limit the group information to specific groups or source addresses.

The **statistics** keyword displays mld traffic information, including mld queries, reports, and leaves. The three columns in the statistics section of the display are:

- Received—Number of packets received.
- Reinjected—Number of packets received, processed, and reinjected back into the forwarding path.
- Generated—Number of packets generated by the mld snooping application and injected into the forwarding path.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example shows summary information per port:

```
Router# show mld snooping port

                        Bridge Domain Domain1:BD-1

Port                          State  #Grps  #Srcs #Hosts
----                          -----  -----  ----- ------
GigabitEthernet0/1/0/1           Up      4      5      6
GigabitEthernet0/1/0/2           Up      4     22      2
GigabitEthernet0/1/0/3           Up      4      5      6
GigabitEthernet0/1/0/4           Up      4     23      2
GigabitEthernet0/1/0/5           Up      4      4      4
GigabitEthernet0/1/0/6           Up      4      4      4
GigabitEthernet0/1/0/7           Up      4      4      4
GigabitEthernet0/1/0/8           Up      4      4      4
GigabitEthernet0/1/0/9           Up      4      4      4
GigabitEthernet0/1/0/10          Up      4      4      4
GigabitEthernet0/1/0/11          Up      4      4      4
GigabitEthernet0/1/0/12          Up      4      4      4
```

```
 (… missing lines)

                        Bridge Domain Domain1:BD-4

Port                          State  #Grps  #Srcs #Hosts
----                          -----  -----  ----- ------
GigabitEthernet0/1/0/1           Up      4      4      4
GigabitEthernet0/2/0/2           Up      4      4      4
GigabitEthernet0/2/0/3           Up      4      4      4
GigabitEthernet0/2/0/4           Up      4      4      4
GigabitEthernet0/2/0/5           Up      4      4      4
GigabitEthernet0/2/0/6           Up      4      4      4
GigabitEthernet0/2/0/7           Up      4      4      4
GigabitEthernet0/2/0/8           Up      4      4      4
GigabitEthernet0/2/0/9           Up      4      4      4
GigabitEthernet0/2/0/10          Up      4      4      4
GigabitEthernet0/2/0/11          Up      4      4      4
GigabitEthernet0/2/0/12          Up       4      4      4
 (… missing lines)

                        Bridge Domain BD-1

Port                          State  #Grps  #Srcs #Hosts
----                          -----  -----  ----- ------
GigabitEthernet0/3/0/1           Up      4      4      4
GigabitEthernet0/3/0/2           Up      4      4      4
GigabitEthernet0/3/0/3           Up      4      4      4
GigabitEthernet0/3/0/4           Up      4      4      4
GigabitEthernet0/3/0/5           Up      4      4      4
GigabitEthernet0/3/0/6           Up      4      4      4
GigabitEthernet0/3/0/7           Up      4      4      4
GigabitEthernet0/3/0/8           Up      4      4      4
GigabitEthernet0/3/0/9           Up      4      4      4
GigabitEthernet0/3/0/10          Up      4      4      4
GigabitEthernet0/3/0/11          Up      4      4      4
GigabitEthernet0/3/0/12          Up      4      4      4
 (… missing lines
```

The following example shows summary information for a specific port.

```
Router# show mld snooping port GigabitEthernet 0/1/0/2

                        Bridge Domain Domain1:BD-1

Port                          State  #Grps   #Srcs #Hosts
----                          -----  ------  ----- ------
GigabitEthernet0/1/0/2           Up       4      4      4
```

The following example shows detail information about a specified port.

```
Router# show mld snooping port gigabitEthernet0/1/0/2 detail statistics
GigabitEthernet0/1/0/2 is up
  Bridge Domain: Domain1:BD-1
  MLD Snoop Profile: profile1
  Explicit Tracking Enabled
  MLD Group Count: 4
  Traffic Statistics (elapsed time since last cleared 00:58:04):
                                   Received  Reinjected   Generated
    Valid Packets:                 110869512      120327          28
      MLD  General Queries:             4950           0          28
      MLD  Group Specific Queries:         0           0           0
      MLD  V1 Reports:                      0           -           -
      MLD  V2 Reports:              110864562      120327           0
      MLD  V3 Reports:                      0           0           -
      MLD  V2 Leaves:                       0           0           0
      MLD  Global Leaves:                   0           -           0
      PIM Hellos:                           0           0           -
    Rx Packets Flooded:                                 0
    Rx Packets Forwarded To Members:                    0
    Rx Packets Forwarded To Mrouters:              120327
    Rx Packets Consumed:                        110749185
    Reports Suppressed:                         110749185
    Errors:
      None
```

The following example shows detail, including statistics, for a specified port (with the include zeroes option).

```
Router# show mld snooping port GigabitEthernet 0/1/0/2 detail statistics include-zeroes

GigabitEthernet0/1/0/2 is up
  Bridge Domain: Domain1:BD-1
  MLD Snoop Profile: profile1
  Explicit Tracking Enabled
  MLD  Group Count: 4
  Traffic Statistics (elapsed time since last cleared 00:58:04):
                                    Received  Reinjected   Generated
    Valid Packets:                  110869512      120327          28
      MLD  General Queries:              4950           0          28
      MLD  Group Specific Queries:          0           0           0
      MLD  V1 Reports:                      0           -           -
      MLD  V2 Reports:              110864562      120327           0
      MLD  V1 Leaves:                       0           0           0
      MLD  Global Leaves:                   0           -           0
      PIM Hellos:                           0           0           -
    Rx Packets Flooded:                                 0
    Rx Packets Forwarded To Members:                    0
    Rx Packets Forwarded To Mrouters:              120327
    Rx Packets Consumed:                        110749185
    Reports Suppressed:                         110749185
    Errors:
      Rx Packets On Inactive Port:                      0
      Rx Packet Martian:                                0
      Rx Packet Bad Protocol:                           0
      Rx Packet DA Not Multicast:                       0
      Rx Packet Missing Router Alert:                   0
      Rx Packet Missing Router Alert Drop:              0
      Rx Packet Bad MLD  Checksum:                      0
      Rx Packets TTL Not One:                           0
      Rx Packets TTL Not One  Drop:                     0
      Rx Queries Too Short:                             0
      Rx V1 Reports Too Short:                          0
      Rx V2 Reports Too Short:                          0
      Rx MLD  Messages Unknown:                         0
      Rx MLD  Messages GT Max Ver:                      0
      Rx MLD  Messages LT Min Ver:                      0
      Rx Queries Bad Source:                            0
      Rx General Queries DA Not All Nodes:              0
      Rx Reports DA Not Group:                          0
      Rx Reports No Querier:                            0
      Rx Leaves Invalid Group:                          0
      Rx Leaves DA Not All Routers:                     0
      Rx Leaves No Querier:                    0
      Rx Leaves Unknown Group:                 0
      Rx Leaves Non Member:                    0
```

show mld snooping profile

To display MLD snooping profile information, use the **show mld snooping profile** command in EXEC mode.

{**show mld snooping profile** [**summary**] | [*profile-name*] [**detail** [**include-defaults**]] [{**references** [**bridge-domain** [*bridge-domain-name*]] | **port** [{**interface-name** | **neighbor** *ipaddr* **pw-id** *id*}]}]}

Syntax Description

summary	(Optional) Displays a summary of profile instances, bridge domain references, and port references.
profile-name	(Optional) Displays information only for the named profile.
detail	(Optional) Displays the contents of profiles.
include-defaults	(Optional) Displays all default configurations with the profile contents. Without this keyword, only configured profile information is displayed.
references	(Optional) Shows which bridge domains and bridge ports reference each profile.
bridge-domain [*bridge-domain-name*]	(Optional) Provides a bridge domain filter for the **references** keyword. Without *bridge-domain-name* , the display shows profiles attached to all bridge domains. With *bridge-domain-name* , the display shows only the profile attached to the specified bridge domain.
port [*interface-name*] or **port** [**neighbor** *ipaddr* **pw-id** *id*]	(Optional) Provides a port filter for the **references** keyword. • With *interface-name* or **neighbor** specified, the display shows the profile attached to the named AC or PW. • Using the **port** keyword alone shows profiles attached to all ports.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

Use this command to display the contents of profiles and to see associations of profiles with bridge-domains and ports.

The **summary** keyword lists profile names and summarizes their usage on bridge domains and ports. No other keywords can be used with **summary** .

Use the **details** keyword with a profile name to show the contents of a specific profile. Without a profile name, the **detail** keyword shows the contents of all profiles.

Use the **references** keyword to list the relationships between profiles and bridge domains or profiles and ports. You have the following options:

- Use the **references** keyword without any other keywords to show all profiles and the ports and bridge domains they are attached to.
- Use the **references** keyword with the **name** keyword to show a specific profile and where it is attached.
- Use the **port** keyword to list all ports and the profiles attached to them.
- Use the **port** keyword with a specific AC interface or PW to see the profile attached to the named port.
- Use the **bridge-domain** keyword to list all bridge domains and the profiles attached to them.
- Use the **bridge-domain** keyword with a specific bridge domain name to see the profile attached to a specific bridge domain.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example lists profile names and shows summary level profile usage.

```
Router# show mld snooping profile

Profile                      Bridge Domain       Port
-------                      -------------       ----
profile1                                 0       8193
profile2                                 1          0
profile3                                 1          0
profile4                                 0          0
profile5                                 1          0
profile6                                 0          0
profile7                                 1          2
```

The following example shows summary level profile usage for a named profile.

```
Router# show mld snooping profile profile1

Profile                                  Bridge Domain       Port
-------                                  -------------       ----
profile1                                             0          8193
```

The following example shows the contents of each profile.

```
Router# show mld snooping profile detail

mld Snoop Profile profile1:
  Bridge Domain References:             3
  Port References:                      0

MLD Snoop Profile profile2:

  Static Groups:                        ff28:1:1::2
                                        ff29:1:1::4     2000:1::2

  Bridge Domain References:             0
  Port References:                      1

MLD Snoop Profile profile3:

  Static Mrouter:                       Enabled

  Bridge Domain References:             0
  Port References:                      1
```

The following example shows output reflecting the **access-group** , **group limit** , and **tcn flood disable** parameters:

```
Router# show mld snooping profile detail
MLD Snoop Profile profile:

  Querier LMQ Count:                    2

  Access Group ACL:                     iptv-white-list
  Group Policy:                         iptv-group-weights
  Group Limit:                          16
  Immediate Leave:                      Enabled
  TCN Flood:                            Disabled


  Bridge Domain References:             1
  Port References:                      0
```

The following example shows the contents of a named profile and the implied default configurations:

```
Router# show mld snooping profile profile1 detail include-defaults

mld Snoop Profile profile p1:

  System IP Address:                    fe80::1aef:63ff:fee2:5fc6
  Minimum Version:                      2
  Report Suppression:                   Enabled
  Unsolicited Report Interval:          1000 (milliseconds)
  TCN Query Solicit:                    Enabled
  TCN Membership Sync:                  Disabled
  TCN Flood:                            Enabled
  TCN Flood Query Count:                2
  Router Alert Check:                   Disabled
  TTL Check:                            Disabled

  Internal Querier Support:             Enabled
  Internal Querier Version:             3
  Internal Querier Timeout:             0 (seconds)
  Internal Querier Interval:            60 (seconds)
  Internal Querier Max Response Time:   10 (seconds)
  Internal Querier TCN Query Interval:  10 (seconds)
  Internal Querier TCN Query Count:     2
  Internal Querier TCN Query MRT:       0
  Internal Querier Robustness:          2
  Querier Query Interval:              60 (seconds)
  Querier LMQ Interval:                1000 (milliseconds)
  Querier LMQ Count:                   2
  Querier Robustness:                  2

  Immediate Leave:                     Disabled
  Explicit Tracking:                   Disabled
  Static Mrouter:                      Disabled
  Router Guard:                        Disabled

Access Group ACL:                     (empty)

  Group Policy:
  Group Limit:                         -1

  ICCP Group Report Standby State:     Enabled

  Startup Query Interval:              15 (seconds)
  Startup Query Count:                 2
  Startup Query Max Response Time:     10 (seconds)
  Startup Query on Port Up:            Enabled
  Startup Query on IG Port Active:     Disabled
  Startup Query on Topology Change:    Disabled
  Startup Query on Process Start:      Disabled

  Static Groups:                       ff28:1:1::2
                                       ff29:1:1::4     2000:1::2

  Bridge Domain References:            1
  Port References:                     0
```

The following command shows a summary of profile usage, by profile name.

```
Router# show mld snooping profile summary

  Number of profiles:                3
  Number of bridge domain references: 3
  Number of port references:         8195
```

The following command lists all MLD snooping profiles and shows which bridge domains and ports are configured to use each profile.

```
Router# show mld snooping profile references

Profile:            profile1
  Bridge Domains:   None
  Ports:            GigabitEthernet0/1/0/0
                    GigabitEthernet0/1/0/1
                    GigabitEthernet0/1/0/2
                    GigabitEthernet0/1/0/3
                    GigabitEthernet0/1/0/4
                    GigabitEthernet0/1/0/5
                      (… missing lines)
                    GigabitEthernet0/3/3/1109
                    GigabitEthernet0/3/3/1110
                    GigabitEthernet0/3/3/1111

Profile:            profile2
  Bridge Domains:   Domain1:BD-1
  Ports:            None

Profile:            profile3
```

```
  Bridge Domains:   Domain1:BD103
  Ports:            None

Profile:            profile4
  Bridge Domains:   None
  Ports:            None

Profile:            profile5
  Bridge Domains:   Domain1:BD105
  Ports:            None

Profile:            profile6
  Bridge Domains:   None
  Ports:            None

Profile:            profile7
  Bridge Domains:   Domain1:BD107
  Ports:            None
```

The following command lists all bridges or ports that are configured to use the profile named profile1.

```
Router# show mld snooping profile profile1 references

Profile:            profile1
  Bridge Domains:   None
  Ports:            GigabitEthernet 0/1/0/0
                    GigabitEthernet 0/1/0/1
                    GigabitEthernet 0/1/0/2
                    GigabitEthernet 0/1/0/3
                    GigabitEthernet 0/1/0/4
                    GigabitEthernet 0/1/0/5
                     (… missing lines)
                    GigabitEthernet 0/3/3/1109
                    GigabitEthernet 0/3/3/1110
                    GigabitEthernet 0/3/3/1111
```

The following example shows the profile attached to a specific bridge domain.

```
Router# show mld snooping profile references bridge-domain Group1:BD-1

Profile:            profile1
  Bridge Domains:   Group1:BD-1
```

The following example shows the profile attached to a specific port.

```
Router# show mld snooping profile references port GigabitEthernet 0/1/0/2

Profile:            profile2
  Ports:            GigabitEthernet0/1/0/2
```

show mld snooping summary

To display summary information about MLD snooping configuration and traffic statistics for the router, use the **show mld snooping summary** command in EXEC mode.

show mld snooping summary [**statistics** [**include-zeroes**]]

Syntax Description

statistics	(Optional) Displays mld traffic counters and statistics.
include-zeroes	(Optional) Displays all statistics, even if they are zero. Without this keyword, many statistics are omitted from the display when their values are zero.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command summarizes the number of bridge domains, mrouter ports, host ports, groups, and sources configured on the router.

Task ID

Task ID	Operation
l2vpn	read

Example

The following example shows the output of the command:

```
Bridge Domains:                                         1
  MLD  Snooping Bridge Domains:                           1
  Ports:                                                  3
  MLD  Snooping Ports:                                    3
  Mrouters:                                               0
  STP Forwarding Ports:                                   0
  ICCP Group Ports:                                       0
  MLD  Groups:                                            0
    Member Ports:                                         0
  MLD  Source Groups:                                     0
    Static/Include/Exclude:                           0/0/0
    Member Ports (Include/Exclude):                     0/0
```

The following example shows the output of the command with the**statistics** keyword:

```
Bridge Domains:                                      1
  MLD  Snooping Bridge Domains:                        1
  Ports:                                               3
  MLD  Snooping Ports:                                 3
  Mrouters:                                            0
  STP Forwarding Ports:                                0
  ICCP Group Ports:                                    0
  MLD  Groups:                                         0
    Member Ports:                                      0
  MLD  Source Groups:                                  0
    Static/Include/Exclude:                        0/0/0
    Member Ports (Include/Exclude):                  0/0
  Traffic Statistics (elapsed time since last cleared 00:57:42):
                                     Received  Reinjected   Generated
    Messages:                               0           0           0
      MLD  General Queries:                 0           0           0
      MLD  Group Specific Queries:          0           0           0
      MLD  G&S Specific Queries:            0           0           0
      MLD  V1 Reports:                      0           0           0
      MLD  V2 Reports:                      0           0           0
      MLD  V1 Leaves:                       0           0           0
      MLD  Global Leaves:                   0           -           0
      PIM Hellos:                           0           0           -
    Rx Packet Treatment:
      Packets Flooded:                                  0
      Packets Forwarded To Members:                     0
      Packets Forwarded To Mrouters:                    0
      Packets Consumed:                                 0
    Rx Errors:
      Packets DA Not Multicast:                         4
    Rx Other:
      None
    Tx Errors:
      None
  Startup Query Sync Statistics:
    None
```

The following example shows the output of the command with the **include-zeroes**keyword:

```
Bridge Domains:                                      1
  MLD  Snooping Bridge Domains:                        1
  Ports:                                               3
  MLD  Snooping Ports:                                 3
  Mrouters:                                            0
  STP Forwarding Ports:                                0
  ICCP Group Ports:                                    0
  MLD  Groups:                                         0
    Member Ports:                                      0
  MLD  Source Groups:                                  0
    Static/Include/Exclude:                        0/0/0
    Member Ports (Include/Exclude):                  0/0
  Traffic Statistics (elapsed time since last cleared 00:57:52):
                                     Received  Reinjected   Generated
    Messages:                               0           0           0
      MLD  General Queries:                 0           0           0
      MLD  Group Specific Queries:          0           0           0
      MLD  G&S Specific Queries:            0           0           0
      MLD  V1 Reports:                      0           0           0
      MLD  V2 Reports:                      0           0           0
      MLD  V1 Leaves:                       0           0           0
      MLD  Global Leaves:                   0           -           0
      PIM Hellos:                           0           0           -
    Rx Packet Treatment:
      Packets Flooded:                                  0
      Packets Forwarded To Members:                     0
      Packets Forwarded To Mrouters:                    0
      Packets Consumed:                                 0
      Reports Suppressed:                               0
      Access Group Permits:                             0
      Access Group Denials:                             0
      Group Limits Exceeded:                            0
      MLD  Blocks Ignored in V1 Compat Mode:            0
      MLD  EX S-lists Ignored in V1 Compat Mode:        0
    Rx MLD  V2 Report Group Record Types:
      Is Include:                                       0
      Change To Include:                                0
      Is Exclude:                                       0
      Change To Exclude:                                0
      Allow New Sources:                                0
      Block Old Sources:                                0
    Rx Errors:
      Packets On Inactive Bridge Domain:                0
      Packets On Inactive Port:                         0
      Packets Martian:                                  0
      Packets Bad Protocol:                             0
      Packets DA Not Multicast:                         4
      Packets Missing Router Alert:                     0
      Packets Missing Router Alert Drop:                0
      Packets Bad mld Checksum:                        0
      Packets TTL Not One:                              0
      Packets TTL Not One Drop:                         0
      Queries Too Short:                                0
      V1 Reports Too Short:                             0
      V2 Reports Too Short:                             0
      V1 Leaves Too Short:                              0
      MLD  Messages Unknown:                            0
      MLD  Messages GT Max Ver:                         0
      MLD  Messages LT Min Ver:                         0
      Queries Bad Source:                               0
      Queries Dropped by S/W Router Guard:              0
      General Queries DA Not All Nodes:                 0
      GS-Queries Invalid Group:                         0
      GS-Queries DA Not Group:                          0
      GS-Queries Not From Querier:                      0
      GS-Queries Unknown Group:                         0
      Reports Invalid Group:                            0
      Reports Link-Local Group:                         0
      Reports DA Not Group:                             0
      Reports No Querier:                               0
      Leaves Invalid Group:                             0
      Leaves Invalid DA:                                0
      Leaves No Querier:                                0
      Leaves Non-Member:                                0
      Leaves Non-Dynamic Member:                        0
      Leaves Non-V1 Member:                             0
      V2 Reports Invalid Group:                         0
      V2 Reports Link-Local Group:                      0
      V2 Reports DA Not All V2 Routers:                 0
      V2 Reports No Querier:                            0
      V2 Reports Older Version Querier:                 0
      V2 Reports Invalid Group Record Type:             0
      V2 Reports No Sources:                            0
      V2 Leaves Non-Member:                             0
      PIM Msgs Dropped by S/W Router Guard:             0
    Rx Other:
      Proxy General Queries:                            0
      Proxy GS-Queries:                                 0
      Proxy Reports:                                    0
    Tx Errors:
      V2 Sources Not Reported:                          0
      No Querier in BD:                                 0
      No L2 Info for BD:                                0
  Startup Query Sync Statistics:
    Stale Port Groups Deleted:                          0
    Stale Port Group Sources Deleted:                   0
```

show mld snooping trace

To display MLD snooping process activity, use the **show mld snooping trace** command in EXEC mode.

show mld snooping trace [{**all** | **error** | **packet-error**}]

Syntax Description

all	(Optional) Displays all mld snooping process activity.
error	(Optional) Displays only error tracepoints.
packet-error	(Optional) Displays packet error tracepoints.

Command Default

The **all** keyword is the default when no keywords are used.

Command Modes

EXEC

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to research mld snooping process activity.

Task ID

Task ID	Operations
l2vpn	read

Examples

The following example shows MLD snooping process status during a restart and a new profile configuration.

```
Router# show mld snooping summary trace all
51 wrapping entries (1024 possible, 0 filtered, 51 total)
Feb  2 14:30:24.902 mldsn/all 0/5/CPU0 t1  TP001:
Feb  2 14:30:24.902 mldsn/all 0/5/CPU0 t1  TP002: ******** mld SNOOP PROCESS RESTART ********
Feb  2 14:30:24.902 mldsn/all 0/5/CPU0 t1  TP001:
Feb  2 14:30:24.902 mldsn/all 0/5/CPU0 t1  TP286: initialize profile wavl tree
Feb  2 14:30:24.902 mldsn/all 0/5/CPU0 t1  TP185: initialize bd wavl tree
Feb  2 14:30:24.902 mldsn/all 0/5/CPU0 t1  TP230: initialize port wavl tree
Feb  2 14:30:24.902 mldsn/all 0/5/CPU0 t1  TP019: entered init_chkpt
Feb  2 14:30:24.934 mldsn/all 0/5/CPU0 t1  TP165: mldsn_init_l2fib entered
Feb  2 14:30:24.934 mldsn/all 0/5/CPU0 t1  TP611: l2fib_restart_timer_init
Feb  2 14:30:24.935 mldsn/all 0/5/CPU0 t1  TP680: mldsn_pd_mgid_api_init entered
Feb  2 14:30:24.937 mldsn/all 0/5/CPU0 t1  TP681: failed to open
libl2mc_snoop_mgid_client_pd.dll
Feb  2 14:30:24.937 mldsn/all 0/5/CPU0 t1  TP683: l2mc_snoop_pd_mgid funcs are stubbed
Feb  2 14:30:25.037 mldsn/all 0/5/CPU0 t1  TP080: socket open succeeded
Feb  2 14:30:25.037 mldsn/all 0/5/CPU0 t1  TP031: connection open for socket
Feb  2 14:30:25.037 mldsn/all 0/5/CPU0 t1  TP614: mldsn_l2fib_restart_timer_start, 300 secs
Feb  2 14:30:25.038 mldsn/all 0/5/CPU0 t1  TP555: mld SNOOP PROCESS READY
Feb  2 14:30:25.038 mldsn/all 0/5/CPU0 t1  TP017: entered event loop
Feb  2 14:30:25.038 mldsn/all 0/5/CPU0 t1  TP112: sysdb register verification
Feb  2 14:30:25.038 mldsn/all 0/5/CPU0 t1  TP286: initialize profile wavl tree
Feb  2 14:30:25.040 mldsn/all 0/5/CPU0 t1  TP110: sysdb event verify func (CREATE & SET,
profile/profile1/enter)
Feb  2 14:30:25.040 mldsn/all 0/5/CPU0 t1  TP287: create profile profile1
Feb  2 14:30:25.040 mldsn/all 0/5/CPU0 t1  TP534: profile profile1 (0x4826b838): initialized
 static_group tree
(… missing lines)
```

startup query count

To configure the number of startup G-queries that are to be sent to the recipient routers, use the **startup query count** command in the appropriate snooping profile configuration mode. To restore the default startup query count to be the Querier's Robustness Value (QRV), use the **no** form of this command.

startup query count *number*
no startup query count

Syntax Description

number	Indicates the number of startup queries sent. The range is from 0-7.

Command Default

2

Command Modes

IGMP snooping profile configuration (config-igmp-snooping-profile)MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following examples show how to configure the startup query count:

```
Router(config-igmp-snooping-profile)# startup query count
```

```
Router(config-mld-snooping-profile)# startup query count
```

Related Commands

Command	Description
igmp snooping profile	
	Creates or edits a profile, and attaches a profile to a bridge domain or port.

startup query iccp-group

To enable the generation of startup G-query on a port, when an MC-LAG transitions from standby state to active state, use the **startup query iccp-group** command in the appropriate snooping profile configuration mode. The snooping technique performs a mark and sweep synchronization of the snooping state over the startup query period.

To disable the startup query generation on this event, use the **no** form of this command.

startup query iccp-group port-active
no startup query iccp-group

Syntax Description

port-active	(Optional) Issues startup queries when iccp-group goes active. This parameter is specific to IGMP Snooping over MC-LAG.

Command Default

None

Command Modes

IGMP snooping profile configurationMLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If configured in a bridge-domain profile, the **startup query iccp-group** command applies to all ports in that bridge-domain. If configured in a profile attached to a specific port, this command applies to that port only.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following examples show how to enable the startup G-query configuration:

```
Router(config-igmp-snooping-profile)# startup query iccp-group
```

```
Router(config-mld-snooping-profile)# startup query iccp-group
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.

startup query interval

To configure the time between successive startup G-queries, use the **startup query interval** command in the appropriate snooping profile configuration mode. To restore the default startup query interval of 1/4 querier's query-interval (up to a max of 32 secs), use the **no** form of this command.

startup query interval *number*
no startup query interval

Syntax Description

number	Interval, in seconds. The range is from 1 to 18000.

Command Default

15 seconds

Command Modes

IGMP snooping profile configurationMLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following examples show how to configure the startup query interval:

```
Router(config-igmp-snooping-profile)# startup query interval
```

```
Router(config-mld-snooping-profile)# startup query interval
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.

startup query max-response-time

To configure the maximum response time (MRT) transmitted in the startup G-queries in seconds, use the **startup query max-response-time** command in the appropriate snooping profile configuration mode. To restore the default startup query max-response-time to be the querier's max-response-time (MRT), use the **no** form of this command.

startup query max-response-time *number*
no startup query max-response-time

Syntax Description

number	Enter an interval between 1 to 25 seconds.

Command Default

10 seconds

Command Modes

IGMP snooping profile configurationMLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following examples show how to configure the MRT :

```
Router(config-igmp-snooping-profile)# startup query max-reponse-time
Router(config-mld-snooping-profile)# startup query max-reponse-time
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.

startup query port-up disable

To disable the sending of startup G-queries on port-up, use the **startup query port-up disable** command in IGMP snooping profile configuration mode. To restore the default behavior that sends G-queries on port-up, use the **no** form of this command.

startup query port-up disable
no startup query port-up disable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If configured in a bridge-domain profile, this command applies to all ports in the bridge-domain. If configured in a profile attached to a specific port, this command applies to only the specific port.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following examples show how to use the **startup query port-up disable** command:

```
Router(config-igmp-snooping-profile)# startup query port-up disable
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.

startup query process start

To enable the startup G-query generation on all ports in the bridge domain when the IGMP Snooping (IGMPSN) process restarts, use the **startup query process start** command in IGMP snooping profile configuration mode. To disable the startup query generation of this event, use the **no** form of this command. This command must be included in the bridge-domain profile.

startup query process start [**sync**]
no startup query process start

Syntax Description

sync	(Optional) Removes the unrefreshed membership state. This parameter instructs the IGMPSN to perform a mark and sweep synchronization of the IGMP snooping state over the startup query period.

Command Default

None

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following examples show how to use the **startup query process start** command into an IGMP snooping profile:

```
Router(config-igmp-snooping-profile)# startup query process start
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.

startup query topology-change

To enable startup G-query generation on all ports in the bridge domain when a topology change is indicated and the bridge is the root, use the **startup query topology-change** command in IGMP snooping profile configuration mode.

To disable the startup query generation on this event, use the **no** form of this command.

startup query topology-change [{**sync** | **always**}]
no startup query topology-change

Syntax Description

sync	(Optional) Removes the unrefreshed membership state. Instructs the IGMP Snooping profile to perform a mark and sweep synchronization of the IGMP snooping state over the startup query period.
always	(Optional) Instructs the IGMP Snooping profile to generate startup G-queries regardless of whether the bridge is the root.

Command Default

None

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to use the **startup query topology-change** command into an IGMP snooping profile in the Command Line Interface:

```
Router(config-igmp-snooping-profile)# startup query topology-change
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.

static group

To configure static group membership entries in the Layer-2 forwarding tables, use the **static group** command in IGMP snooping profile configuration mode. To remove a static group entry from the forwarding tables, use the **no** form of this command.

static group *group-addr* [**source** *source-addr*]
no static group *group-addr* [**source** *source-addr*]

Syntax Description

group-addr	IP multicast group address.
source	(Optional) Statically forwards an (S, G) channel out of the port.
source-addr	IP multicast source address.

Command Default

None

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

IGMP snooping learns Layer-2 multicast groups dynamically. You can also statically configure Layer-2 multicast groups.

You can use the **static group** command in profiles intended for bridge domains or ports. I f you configure this option in a profile attached to a bridge domain, it applies to all ports under the bridge.

A profile can contain multiple static groups. You can define different source addresses for the same group address. Using the **source** keyword, you can configure IGMPv3 source groups.

Static group membership supersedes any dynamic manipulation by IGMP snooping. Multicast group membership lists can contain both static and dynamic group definitions.

When you configure a static group or source group on a port, IGMP snooping adds the port as an outgoing port to the corresponding <S/*,G> forwarding entry and sends an IGMPv2 join or IGMPv3 report to all mrouter ports. IGMP snooping continues to send the membership report in response to general queries for as long as the static group remains configured on the port.

The scope of this command can be either bridge domain level or port level. If you use this command in a profile attached to a bridge domain, the static group membership applies to all ports under the bridge. If you use the command in a profile attached to a port, the static group membership applies only to that port.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following examples show how to add static group membership configuration into an IGMP snooping profile:

```
Router(config-igmp-snooping-profile)# static group 10.1.1.1
Router(config-igmp-snooping-profile)# static group 10.1.1.1 source 10.1.12.0
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.

system-ip-address

To configure an IP address for the internal querier, use the **system-ip-address** command in IGMP snooping profile configuration mode. To return to the default value, use the **no** form of this command.

system-ip-address *ip-address*
no system-ip-address

Syntax Description

ip-address	Assigns an IP address for IGMP use.

Command Default

0.0.0.0

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **system-ip-address** command configures an IP address for IGMP snooping use. If not explicitly configured, the default address is 0.0.0.0. The default is adequate except in the following circumstances:

- If you are configuring an internal querier. The internal querier cannot use 0.0.0.0.
- If the bridge needs to communicate with a non-Cisco IGMP router that does not accept the 0.0.0.0 address.

IGMP snooping uses the value set by the **system-ip-address** command in the following ways:

- The internal-querier sends queries from the system IP address. An address other than the default 0.0.0.0 must be configured.
- IGMPv3 sends proxy reports from the system IP address. The default address 0.0.0.0 is preferred but may not be acceptable to some IGMP routers.
- In response to topology change notifications (TCNs) in the bridge domain, IGMP snooping sends global-leaves from the system IP address. The default address 0.0.0.0 is preferred but may not be acceptable to some IGMP routers.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example assigns a system IP address, overriding the default value:

```
Router(config-igmp-snooping-profile)# system-ip-address 10.1.1.1
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.

tcn flood disable

To disable Spanning Tree Protocol (STP) port flooding during a topology change, use the **tcn flood disable** command in the appropriate snooping profile configuration mode. To reenable STP port flooding, use the **no** form of this command.

tcn flood disable
no tcn flood disable

Syntax Description

This command has no arguments or keywords.

Command Default

TCN flooding is enabled by default.

Command Modes

IGMP snooping profile configuration

MLD snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

This example illustrates how to disable TCN flooding:

```
Router(config-igmp-snooping-profile)# tcn flood disable
```

```
Router(config-mld-snooping-profile)# tcn flood disable
```

Related Commands

Command	Description
show igmp snooping profile	Displays the contents of profiles and to see associations of profiles with bridge-domains and ports, including access group, group limit, and TCN flood parameters.
tcn flood query count	Configures the number of general queries that must be sent before IGMP snooping stops flooding all routes in response to STP topology changes
tcn query solicit	Enables global leave messaging on non-root bridges in response to STP topology changes.

tcn flood query count

To configure how long IGMP snooping floods all routes in response to topology changes, use the **tcn flood query count** command in IGMP snooping profile configuration mode. To return to the default value, use the **no** form of this command.

tcn flood query count *number*
no tcn flood query count

Syntax Description

number	Specifies the number of general queries that must occur after a TCN before IGMP snooping stops multicast flooding to all ports and resumes restricted forwarding. Valid values are integers from 1 to 10.

Command Default

2

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

In a Spanning Tree Protocol (STP) topology, a topology change notification (TCN) indicates that an STP topology change has occurred. As a result of a topology change, mrouters and hosts reporting group membership may migrate to other STP ports under the bridge domain. Mrouter and membership states must be relearned after a TCN.

IGMP snooping reacts to TCNs in the following way:

1. IGMP snooping temporarily extends the flood set for all known multicast routes to include all ports participating in STP that are in forwarding state. The short term flooding ensures that multicast delivery continues to all mrouters and all member hosts in the bridge domain while mrouter and membership states are relearned.
2. The STP root bridge issues a global leave (leave for group 0.0.0.0) on all ports. This action triggers mrouters to send general queries, expediting the relearning process.

Note Sending global leaves for query solicitation is a Cisco-specific implementation.

1. When the TCN refresh period ends, IGMP snooping withdraws the non-mrouter and non-member STP ports from the multicast route flood sets. You can control the amount of time that flooding occurs with the **tcn flood query count** command. This command sets the number of IGMP general queries for which the multicast traffic is flooded following a TCN, thus influencing the refresh period.

IGMP snooping default behavior is that the STP root bridge always issues a global leave in response to a TCN, and the non-root bridges do not issue global leaves.

With the **tcn query solicit** command, you can enable a bridge to always issue a global leave in response to TCNs, even when it is not the root bridge. In that case, the root bridge and the non-root bridge would issue the global leave and both would solicit general queries in response to a TCN. Use the **no** form of the command to turn off soliciting when the bridge is not the root.

The root bridge always issues a global leave in response to a TCN. This behavior can not be disabled.

The internal querier has its own set of configuration options that control its reactions to TCNs.

The scope for this configuration option is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure the tcn flood query count in an IGMP snooping profile, overriding the default:

```
Router(config-igmp-snooping-profile)# tcn flood query count 5
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
tcn query solicit	Enables global leave messaging on non-root bridges in response to STP topology changes.

tcn flood query count (MLD)

To configure how long MLD snooping floods all routes in response to topology changes, use the **tcn flood query count** command in the MLD snooping profile configuration mode. To retun to the default value, use the **no** form of the command.

tcn flood query count *number*

notcn flood query count *number*

Syntax Description

number	Specifies the number of queries. range is from 1 to 10.

Command Default

2

Command Modes

MLD snooping profile

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

In a Spanning Tree Protocol (STP) topology, a topology change notification (TCN) indicates that an STP topology change has occurred. As a result of a topology change, mrouters and hosts reporting group membership may migrate to other STP ports under the bridge domain. Mrouter and membership states must be relearned after a TCN.

IGMP snooping reacts to TCNs in the following way:

- MLD snooping temporarily extends the flood set for all known multicast routes to include all ports participating in STP that are in forwarding state. The short term flooding ensures that multicast delivery continues to all mrouters and all member hosts in the bridge domain while mrouter and membership states are relearned.

- The STP root bridge issues a global leave (leave for group 0.0.0.0) on all ports. This action triggers mrouters to send general queries, expediting the relearning process.

Task ID

Task ID	Operation
l2vpn	read, write

Example

The following example shows how to set the query count to 5:

```
Router(config-mld-snooping-profile) # tcn flood query count 5
```

tcn query solicit

To enable global leave messaging on non-root bridges in response to STP topology changes, use the **tcn query solicit** command in IGMP snooping profile configuration mode. To disable this functionality (on non-root bridges), use the **no** form of this command.

tcn query solicit
no tcn query solicit

Syntax Description

This command has no arguments or keywords.

Command Default

It is disabled by default.

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

In a Spanning Tree Protocol (STP) topology, a topology change notification (TCN) indicates that an STP topology change has occurred. As a result of a topology change, mrouters and hosts reporting group membership may migrate to other STP ports under the bridge domain. Mrouter and membership states must be relearned after a TCN.

IGMP snooping reacts to TCNs in the following way:

1. IGMP snooping temporarily extends the flood set for all known multicast routes to include all ports participating in STP that are in forwarding state. The short term flooding ensures that multicast delivery

continues to all mrouters and all member hosts in the bridge domain while mrouter and membership states are relearned.

2. The STP root bridge issues a global leave (leave for group 0.0.0.0) on all ports. This action triggers mrouters to send general queries, expediting the relearning process.

Note Sending global leaves for query solicitation is a Cisco-specific implementation.

1. When the TCN refresh period ends, IGMP snooping withdraws the non-mrouter and non-member STP ports from the multicast route flood sets. You can control the amount of time that flooding occurs with the **tcn flood query count** command. This command sets the number of IGMP general queries for which the multicast traffic is flooded following a TCN, thus influencing the refresh period.

IGMP snooping default behavior is that the STP root bridge always issues a global leave in response to a TCN, and the non-root bridges do not issue global leaves.

With the **tcn query solicit** command, you can enable a bridge to always issue a global leave in response to TCNs, even when it is not the root bridge. In that case, the root bridge and the non-root bridge would issue the global leave and both would solicit general queries in response to a TCN. Use the **no** form of the command to turn off soliciting when the bridge is not the root.

The root bridge always issues a global leave in response to a TCN. This behavior can not be disabled.

The internal querier has its own set of configuration options that control its reactions to TCNs.

The scope for this configuration option is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to ensure that a bridge will always issue a global leave in response to a TCN, even when it is not the STP root bridge:

```
Router(config-igmp-snooping-profile)# tcn query solicit
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.
tcn flood query count	Configures how many general queries must be sent before IGMP snooping stops flooding all routes in response to STP topology changes

tcn query solicit (MLD)

To enable global leave messaging on non-root bridges in response to STP topology changes, use the **tcn query solicit** command in MLD snooping profile configuration mode. To disable this functionality, in non-root bridges, use the **no** form of the command.

tcn query solicit

no tcn query solicit

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

MLD snooping profile

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

With the tcn query solicit command, you can enable a bridge to always issue a global leave in response to TCNs, even when it is not the root bridge. In that case, the root bridge and the non-root bridge would issue the global leave and both would solicit general queries in response to a TCN. Use the no form of the command to turn off soliciting when the bridge is not the root. The root bridge always issues a global leave in response to a TCN. This behavior can not be disabled. The internal querier has its own set of configuration options that control its reactions to TCNs. The scope for this configuration option is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

Task ID

Task ID	Operation
l2vpn	read, write

Example

The following example shows how to ensure that a bridge will always issue a global leave in response to a TCN, even when it is not the STP root-bridge:

```
Routeer(config-mld-snooping-profile) # tcn query solicit
```

ttl-check disable

To disable the IGMP snooping check on the time-to-live (TTL) field in the IGMP header, use the **ttl-check disable** command in IGMP snooping profile configuration mode. To enable this functionality after a disable, use the **no** form of this command.

ttl-check disable
no ttl-check disable

Syntax Description

This command has no arguments or keywords.

Command Default

It is enabled by default.

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

By default, IGMP snooping examines the time-to-live (TTL) field in the IGMP header and processes packets as follows:

- If the TTL field is 1, IGMP snooping processes the packet. The TTL field is always set to 1 in the headers of IGMP reports and queries.
- If the TTL field is not 1, IGMP snooping drops the packet

When the IGMP snooping TTL check feature is disabled, IGMP snooping processes all packets without examining the TTL field in the IGMP header.

The scope for this configuration option is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to turn off the check on the ttl field:

```
Router(config-igmp-snooping-profile)# ttl-check disable5
```

Related Commands

Command	Description
igmp snooping profile	Creates or edits a profile, and attaches a profile to a bridge domain or port.

unsolicited-report-interval

To set the length of time that IGMP snooping has to send state change reports for IGMPv3 queriers when proxy reporting is enabled, use the **unsolicited-report-interval** command in IGMP snooping profile configuration mode. To return to the default value, use the **no** form of this command.

unsolicited-report-interval *timer-value*
no unsolicited-report-interval

Syntax Description

timer-value	Specifies the length of time that IGMP snooping can take to send state change reports for IGMPv3 queriers. Valid values are integers from 100 to 5000 (milliseconds).

Command Default

1000 (milliseconds)

Command Modes

IGMP snooping profile configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If a bridge domain querier is running IGMPv3 and proxy reporting is enabled, IGMP snooping acts as a proxy, generating reports from the proxy reporting address. As insurance against lost reports, IGMP snooping generates and forwards state change reports *robustness-variable* times, where the *robustness-variable* is the QRV value in the querier's general query. IGMP snooping forwards the reports at random intervals within the timeframe configured with the **unsolicited-report-timer** command.

Proxy reporting is enabled by default. To disable proxy reporting, use the **report-suppression disable** command.

Task ID

Task ID	Operations
l2vpn	read, write

Examples

The following example shows how to configure the unsolicited report interval:

```
Router(config-igmp-snooping-profile)# unsolicited-report-interval 2000
```

Related Commands

Command	Description
report-suppression disable	Disables IGMPv2 report suppression and IGMPv3 proxy reporting.
system-ip-address	Configures the proxy reporting address.