

AOS-CX 10.17 Multicast Guide

4100i, 6000, 6100 Switch Series



Hewlett Packard
Enterprise

Published: November 2025

Version: 1

Copyright Information

© Copyright 2025 Hewlett Packard Enterprise Development LP.

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at <https://myenterpriselicense.hpe.com/cwp-ui/software> but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd Spring, TX 77389
United States of America.



Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Contents

About this document	8
Applicable products	8
Latest version available online	8
Command syntax notation conventions	8
About the examples	9
Identifying switch ports and interfaces	9
Multicast overview	11
Multicast protocols	11
Multicast addresses	11
Important considerations	12
MLD snooping	14
MLD snooping global configuration commands	14
MLD snooping VLAN configuration commands	15
MLD snooping show commands	25
MLD configuration commands for interface VLAN	28
MLD show commands for interface VLAN	37
MLD configuration commands for interface	40
Internet Group Management Protocol (IGMP)	50
IGMP defaults, protocols, and supported configuration	50
How the IGMP protocol works	50
Considerations when configuring IGMP	51
IGMP configuration task list	52
Enabling or disabling IGMP	52
Specifying the IGMP version	53
Configuring IGMP static groups	53
Configuring IGMP query and response parameters	54
Disabling IGMP	54
Viewing IGMP information	55
IGMP configuration example	55
IGMP commands	56
ip igmp	56
ip igmp apply access-list	57
ip igmp last-member-query-interval	58
ip igmp querier	59
ip igmp querier interval	60
ip igmp querier query-max-response-time	61
ip igmp querier wait-time	62
ip igmp robustness	63
ip igmp router-alert-check	63
ip igmp static-group	64
ip igmp version	65
ip igmp version strict	66
no ip igmp	67
show ip igmp	68
show ip igmp counters	69
show ip igmp group	70
show ip igmp groups	72
show ip igmp interface	75
show ip igmp interface counters	76

show ip igmp interface group	77
show ip igmp interface groups	78
show ip igmp interface statistics	79
show ip igmp static-groups	80
show ip igmp statistics	81
IGMP snooping	83
IGMP snooping defaults, protocols, and supported configuration	83
How IGMP snooping works	84
IGMP snooping configuration task list	85
Enabling or disabling IGMP snooping	85
Specifying the IGMP snooping version	85
Configuring IGMP snooping static groups	86
Enabling drop-unknown filters	86
Configuring IGMP snooping fast learn ports globally	86
Configuring IGMP snooping per port filtering	87
Disabling IGMP snooping	87
Viewing IGMP snooping information	88
IGMP snooping commands	88
ip igmp snooping apply access list	88
ip igmp snooping (config mode)	89
ip igmp snooping (interface mode)	90
ip igmp snooping (vlan mode)	93
ip igmp snooping filter unknown mcast	94
ip igmp snooping preprogram-starg-flow	95
ip igmp snooping querier-address	97
ip igmp snooping static group	98
show ip igmp snooping	99
MLD snooping	102
MLD snooping global configuration commands	102
ipv6 mld snooping	102
MLD snooping VLAN configuration commands	103
ipv6 mld snooping (vlan)	103
ipv6 mld snooping apply access-list	104
ipv6 mld snooping auto vlan	105
ipv6 mld snooping blocked vlan	106
ipv6 mld snooping fastlearn	107
ipv6 mld snooping fastleave vlan	107
ipv6 mld snooping forced fastleave vlan	108
ipv6 mld snooping forward vlan	109
ipv6 mld snooping preprogram-starg-flow	110
ipv6 mld snooping querier-address	112
ipv6 mld snooping static-group	113
ipv6 mld snooping version	114
MLD snooping show commands	114
show ipv6 mld snooping	114
MLD configuration commands for interface VLAN	117
ipv6 mld (vlan)	117
ipv6 mld apply access-list (vlan)	118
no ipv6 mld	119
ipv6 mld querier (vlan)	120
ipv6 mld querier interval (vlan)	120
ipv6 mld last-member-query-interval (vlan)	121
ipv6 mld querier query-max-response-time (vlan)	122
ipv6 mld robustness (vlan)	122
ipv6 mld static-group (vlan)	123
ipv6 mld version (vlan)	124

ipv6 mld version strict (vlan)	124
MLD show commands for interface VLAN	125
show ipv6 mld	125
MLD configuration commands for interface	129
ipv6 mld (interface)	129
ipv6 mld apply access-list (interface)	129
no ipv6 mld	130
ipv6 mld querier (interface)	131
ipv6 mld querier interval (interface)	132
ipv6 mld last-member-query-interval (interface)	132
ipv6 mld querier query-max-response-time (interface)	133
ipv6 mld robustness (interface)	134
ipv6 mld static-group (interface)	134
ipv6 mld snooping filter-unknown-mcast	135
ipv6 mld version (interface)	136
ipv6 mld version strict (interface)	137
Support and Other Resources	138
Accessing HPE Aruba Networking Support	138
Accessing Updates	139
Warranty Information	139
Regulatory Information	139
Documentation Feedback	139

About this document

This document describes features of the AOS-CX network operating system. It is intended for administrators responsible for installing, configuring, and managing HPE Aruba Networking switches on a network.

Applicable products

This document applies to the following products:

- HPE Aruba Networking 4100i Switch Series (JL817A, JL818A)
- HPE Aruba Networking 6000 Switch Series (R8N85A, R8N86A, R8N87A, R8N88A, R8N89A, R9Y03A, S4R20A, S4R21A, S4R22A, S4R23A, S4R24A, S4R25A, S4R26A, S4R27A, S4R28, S4R29A)
- HPE Aruba Networking 6100 Switch Series (JL675A, JL676A, JL677A, JL678A, JL679A)

Latest version available online

Updates to this document can occur after initial publication. For the latest versions of product documentation, see the links provided in [Support and Other Resources](#).

Command syntax notation conventions

Convention	Usage
<code>example-text</code>	Identifies commands and their options and operands, code examples, filenames, pathnames, and output displayed in a command window. Items that appear like the example text in the previous column are to be entered exactly as shown and are required unless enclosed in brackets ([]).
example-text	In code and screen examples, indicates text entered by a user.
Any of the following: ■ <code><example-text></code> ■ <code><example-text></code> ■ <i>example-text</i> ■ <i>example-text</i>	Identifies a placeholder—such as a parameter or a variable—that you must substitute with an actual value in a command or in code: ■ For output formats where italic text cannot be displayed, variables are enclosed in angle brackets (<code>< ></code>). Substitute the text—including the enclosing angle brackets—with an actual value. ■ For output formats where italic text can be displayed, variables might or might not be enclosed in angle brackets. Substitute the text including the enclosing angle brackets, if any, with an actual value.
	Vertical bar. A logical OR that separates multiple items from which you can choose only one. Any spaces that are on either side of the vertical bar are included for readability and are not a required part of the command syntax.

Convention	Usage
{ }	Braces. Indicates that at least one of the enclosed items is required.
[]	Brackets. Indicates that the enclosed item or items are optional.
... or ...	Ellipsis: ■ In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information. ■ In syntax using brackets and braces, an ellipsis indicates items that can be repeated. When an item followed by ellipses is enclosed in brackets, zero or more items can be specified.

About the examples

Examples in this document are representative and might not match your particular switch or environment.

The slot and port numbers in this document are for illustration only and might be unavailable on your switch.

Understanding the CLI prompts

When illustrating the prompts in the command line interface (CLI), this document uses the generic term **switch**, instead of the host name of the switch. For example:

```
switch>
```

The CLI prompt indicates the current command context. For example:

```
switch>
```

Indicates the operator command context.

```
switch#
```

Indicates the manager command context.

```
switch(CONTEXT-NAME) #
```

Indicates the configuration context for a feature. For example:

```
switch(config-if) #
```

Identifies the **interface** context.

Variable information in CLI prompts

In certain configuration contexts, the prompt may include variable information. For example, when in the VLAN configuration context, a VLAN number appears in the prompt:

```
switch(config-vlan-100) #
```

When referring to this context, this document uses the syntax:

```
switch(config-vlan-<VLAN-ID>) #
```

Where **<VLAN-ID>** is a variable representing the VLAN number.

Identifying switch ports and interfaces

Physical ports on the switch and their corresponding logical software interfaces are identified using the format: **member/slot/port**.

On the HPE Aruba Networking 4100i Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface **1/1/4** in software is associated with physical port 4 on the switch.

On the HPE Aruba Networking 6000 and 6100 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface **1/1/4** in software is associated with physical port 4 on the switch.

Multicast overview

Multicast addressing allows one-to-many or many-to-many communication among hosts on a network. Typical applications of multicast communication include: audio and video streaming, desktop conferencing, collaborative computing, and similar applications.

IGMP snooping (Internet Group Management Protocol controls) can be configured per-VLAN basis to reduce unnecessary bandwidth usage. In the factory default state (IGMP and IGMP snooping disabled), the switch simply floods all IP multicast traffic it receives on a given VLAN through all ports on that VLAN (except the port on which it received the traffic). This can result in significant and unnecessary bandwidth usage in networks where IP multicast traffic is a factor. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP will be configured on the hosts, and multicast traffic will be generated by one or more servers (inside or outside of the local network). Switches in the network (that support IGMP snooping) can then be configured to direct the multicast traffic to only the ports where needed. If multiple VLANs are configured, you can configure IGMP snooping on a per-VLAN basis.

Multicast Listener Discovery (MLD) is an IPv6 protocol used on a local link for multicast group management. MLD snooping is a subset of the MLD protocol that operates at the port level and conserves network bandwidth by reducing the flooding of multicast IPv6 packets.



Static multicast routes can be configured in bridge mode to prevent traffic from being routed from one interface to another without impacting CPU usage by multicast daemons. If a multicast deployment is using ACLs or policies to block traffic for specific groups or sources, and a static multicast route is also configured to drop or allow traffic along with these policies, traffic will be forwarded/routed only if both the static multicast route and the policy are configured to allow traffic. If one or more of these are configured to drop the traffic, traffic will be dropped.

Multicast protocols

Layer 3 multicast protocols include:

- IGMP (Internet Group Management Protocol) for last-hop multicast group management. Current RFCs include:
 - IGMPv2 (RFC 2236)
 - IGMPv3 (RFC 3376)
- MLD (Multicast Listener Discovery) v1 and v2
 - MLD v1 - RFC 2710
 - MLD v2 - RFC 3810

Layer 2 multicast protocol:

- IGMP snooping for IPv4 multicast filtering.
- MLD snooping for IPv6 multicast filtering.

Multicast addresses

Each multicast host group is identified by a single IP address in the range of 224.0.0.0 through 239.255.255.255.

- **For the 6000/6100 switch:** AOS-CX supports 512 IPv4 multicast flows.

For a list of all reserved and well known multicast addresses, see the standards document at the following links:

- <https://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml>
- <https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml>

Important considerations

Note the following considerations for deployments using IPTV or SSDP advertisement packets.

IPTV considerations

To reduce join and leave latency, reduce the number of hops to the host- or client-connected access switch. An L3 access node will significantly reduce the join and leave latency, as compared to a purely L2 snooping switch. Limiting the number of users to 300 users or fewer at any point of time will also prevent join and leave failures in the event all logged in users are continuously using IPTV channels.

The default IGMP robustness value of 2 should not be modified. Configuring FFL will result in reduced leave latency but it will also result in join and leave failures.

In SSDP advertisement packets destined for the multicast address (Pv4) 239.255.255.250 and/Or ff0X::c , all scope ranges indicated by 'X' cause AOS-CX platforms to program a hardware bridged entry for the corresponding VLAN where such SSDP packets are received. However, these bridge entries are updated to a ROUTE entry whenever a Join is received causing the hash table to fill up.

If SSDP service is not enabled in the network, HPE Aruba Networking recommends disabling SSDP either through VLAN ACLs or through policy as shown in the following examples:

Example 1: Filter SSDP packets using ACL

```
access-list ip drop_ssdp
 10 deny udp any 239.255.255.250 eq 1900

vlan 10
 apply access-list ip drop_ssdp in

interface 1/1/1
 no shutdown
 no routing
 vlan access 10

interface vlan 10
 ip address 192.168.1.2/24
 ip igmp enable
 ip pim-sparse enable
router pim
 enable
```

Example 2: Filter SSDP packets using Policy

```
class ip drop_class
 10 match any any 239.255.255.250
```

```
policy drop_ssdp
  10 class ip drop_class action drop

vlan 10
  apply policy drop_ssdp in

interface 1/1/1
  no shutdown
  no routing
  vlan access 10

interface vlan 10
  ip address 192.168.1.2/24
  ip igmp enable
  ip pim-sparse enable

router pim
  enable
```

MLD snooping

Multicast Listener Discovery (MLD) snooping optimizes multicast traffic across the network to prevent traffic from flooding ports on a VLAN.

- For example, one of the features of MLD snooping lets you configure the network so that traffic is forwarded only to ports that initiate an MLD request for multicast.
- Another feature of MLD lets you enable a setting so that packets that do not match the configured version are dropped.
- You can also block ports from traffic.



MLD snooping is disabled by default and has to be enabled on all applicable VLANs.

Disabling and enabling IPv6 MLD snooping on a VLAN causes MLD querier reelection.



The 6000 and 6100 Switch series does not support router port detection via PIM control packets. As a result, IGMP reports are not forwarded to router ports learned through PIM. However, IGMP/MLD Querier port learning is fully supported on this platform and the device learns querier ports and forwards IGMP/MLD control packets to them as expected. This ensures proper multicast group management and protocol operation.

MLD snooping global configuration commands

ipv6 mld snooping

```
ipv6 mld snooping drop-unknown {vlan-shared | vlan-exclusive}
no ipv6 mld snooping drop-unknown {vlan-shared | vlan-exclusive}
```

Description

This command configures the drop unknown mode. While MLD snooping is enabled, the traffic will be forwarded only to ports that initiate an MLD request for multicast. Drop unknown mode can be a filter across all VLANs (vlan-shared) or per VLAN (exclusive-vlan). The default configuration is vlan-shared.

The **no** form of this command configures the drop unknown mode on the switch to the default **vlan-shared**.

Parameter	Description
vlan-shared	Required: Enable shared VLAN filter on the switch.
vlan-exclusive	Required: Enable exclusive drop unknown filter per VLAN.

Example

```
switch(config)# ipv6 mld snooping drop-unknown vlan-shared
switch(config)# ipv6 mld snooping drop-unknown vlan-exclusive
switch(config)# no ipv6 mld snooping drop-unknown
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config	Administrators or local user group members with execution rights for this command.

MLD snooping VLAN configuration commands

ipv6 mld snooping (vlan)

```
ipv6 mld snooping {enable | disable}
no ipv6 mld snooping [enable | disable]
```

Description

This command disables or reenables MLD snooping on the VLAN. Starting with AOS-CX 10.16, MLD snooping is enabled by default.

The **no** form of this command disables all MLD snooping configurations on the VLAN.

Parameter	Description
enable	Reenable MLD snooping on the VLAN.
disable	Disable MLD snooping on the VLAN.

Example

Disable and then reenables MLD snooping on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping disable
switch(config-vlan)# ipv6 mld snooping enable
```

Remove all MLD snooping configurations on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# no ipv6 mld snooping enable
```

Command History

Release	Modification
10.16	Starting with this release, MLD snooping is enabled on VLANs by default, including the Management VLAN (vlan 1) and VLANs with a associated VNI.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan-<VLAN-ID>	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping apply access-list

```
ipv6 mld snooping apply access-list <ACL-NAME>
no ipv6 mld snooping apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the MLD join or leave packets based on rules set in the particular ACL name.

The **no** form of this command disables the rules set for the ACL.



This configuration will override the ACL associated with IGMP snooping on the corresponding L2 VLAN.

Parameter	Description
access-list	Associates an ACL with the IGMP.
<ACL-NAME>	Specifies the name of the ACL.
	NOTE: If the access list is configured for both L2 VLAN and L3 VLAN, the L3 VLAN configuration will be applied.

Usage

- Existing classifier commands are used to configure the ACL.
- In case an IGMPv3 packet with multiple group addresses is received, the switch only processes the permitted group addresses based on the ACL rule set. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by ACL. This avoids the delay in learning of the permitted groups. Since the access switch configured with ACL blocks the traffic for the groups which are denied, forwarding of joins has no impact. If all the groups in the packet are denied by the ACL rule, the packet is not forwarded to the querier and PIM router. Existing joins will timeout.
- In case of IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.

Examples

Configuring the ACL to filter MLD packets based on permit/deny rules set in access list **mygroup**:

```
switch(config)# access-list ipv6 mygroup
switch(config-acl-ip)# 10 deny icmpv6 any ff55::2
switch(config-acl-ip)# 20 deny icmpv6 any ff55::3
switch(config-acl-ip)# 30 permit icmpv6 any ff55::1
switch(config-acl-ip)# exit
switch(config)# interface vlan 2
switch(config-vlan)# ipv6 mld snooping apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list **mygroup**:

```
switch(config-vlan)# no ipv6 mld snooping apply access-list mygroup
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping auto vlan

```
ipv6 mld snooping [auto vlan <VLAN-LIST>]
no ipv6 mld snooping [auto vlan <VLAN-LIST>]
```

Description

This command configures the given ports in auto mode, which is the default port mode.

The **no** form of this command disables auto ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as an auto port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Example

Configuring auto ports for VLANs on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
```

```
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping auto vlan 10
switch(config-vlan)# ipv6 mld snooping auto vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping blocked vlan

```
ipv6 mld snooping [blocked vlan <VLAN-LIST>]
no ipv6 mld snooping [blocked vlan <VLAN-LIST>]
```

Description

By default ports are configured in auto mode. This command configures the given ports in blocked mode.

The **no** form of this command removes blocked ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as a blocked port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Example

Configuring blocked ports for the VLANs on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping blocked vlan 10
switch(config-vlan)# ipv6 mld snooping blocked vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping fastlearn

ipv6 mld snooping fastlearn <port-list>

Description

This command enables the port to learn group information on receiving topology change notification. The **no** form of this command disables fastlearn on the ports.

Parameter	Description
port-list	Required: 1/1/1-1/1/2, ports to be configured as fastlearn ports.

Example

```
switch(config)# ipv6 mld snooping fastlearn 1/1/3
switch(config)# ipv6 mld snooping fastlearn 1/1/1-1/1/2
switch(config)# ipv6 mld snooping fastlearn 1/1/5,1/1/6
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping fastleave vlan

ipv6 mld snooping [fastleave vlan <VLAN-LIST>]
no ipv6 mld snooping [fastleave vlan <VLAN-LIST>]

Description

Configures the specified ports as fastleave ports. Enables the switch to immediately remove an interface from the bridge table upon receiving the leave group message.

The **no** form of this command disables fastleave configuration on the ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as a fastleave port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Usage

MLD fastleave is configured for ports on a per-VLAN basis. By default, the querier sends a MLD Group-Specific Query message out of the interface, upon which the leave group message is received to ensure that no other receivers are connected to the interface. If receivers are directly attached to the switch, it is inefficient to send the membership query as the receiver wanting to leave is the only connected host. Fastleave processing eliminates the MLD Group-Specific Query message. Thus, it allows the switch to immediately remove an interface from the bridge table upon receiving the leave Group message. This processing speeds up the overall leave process and also eliminates the CPU overhead of having to generate an MLD Group-Specific Query message.

Example

Configuring fastleave ports for the VLAN:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping fastleave vlan 10
switch(config-vlan)# ipv6 mld snooping fastleave vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping forced fastleave vlan

```
ipv6 mld snooping [forced-fastleave <VLAN-LIST>]
no ipv6 mld snooping [forced-fastleave <VLAN-LIST>]
```

Description

Configures the given ports in forced fastleave mode.

The **no** form of this command disables forced fastleave configuration on the ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as a forced fastleave port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Usage

With forced fastleave enabled, MLD speeds up the process of blocking unnecessary multicast traffic to a switch port that is connected to multiple end nodes. When a port having multiple end nodes receives a leave group request from one end node for a given multicast group, forced fastleave activates and waits a small amount of time to receive a join request from any other member of the same group on that port. If the port does not receive a join request for that group within the forced fastleave interval, the switch then blocks any further traffic to that group on that port.

Example

Configuring forced-fastleave ports for the VLAN:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping forced-fastleave vlan 10
switch(config-vlan)# ipv6 mld snooping forced-fastleave vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping forward vlan

```
ipv6 mld snooping [forward vlan <VLAN-LIST>]
no ipv6 mld snooping [forward vlan <VLAN-LIST>]
```

Description

By default ports are configured in auto mode. This command configures the given ports in forward mode.

The **no** form of this command disables forward ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as a forward port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Example

Configuring forward ports for VLANs on the interface:

```
switch# configureterminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping forward vlan 10
switch(config-vlan)# ipv6 mld snooping forward vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping preprogram-starg-flow

```
ipv6 mld snooping preprogram-starg-flow {enable | disable}
```

Description

This command configures the preprogramming of the starg flow feature on MLD snooping enabled VLANs.

Parameter	Description
enable	Enable preprogramming starg flows on the VLAN.
disable	Disable prprogramming starg flows on the VLAN.

Usage

When this feature is enabled, a summarized multicast bridge entry is programmed into the hardware table when a starg or sg MLD join is received on the MLD snooping enabled VLAN. This enables multicast flow to be programmed in the hardware even before the data packet arrives for multicast

flow. MLDv2 joins that are sent for a specific source are treated similar to starg joins and a summarized entry is programmed in the corresponding hardware.

Preprogramming of Starg Flows is supported only on the MLD snooping enabled VLANs. If MLD snooping is disabled on a VLAN, this feature is auto-disabled.

This feature is currently supported for MLDv1 and MLDv2 joins, which means a summarized multicast flow is programmed in advance when a MLDv1 or MLDv2 join for a specific group is received. For MLDv2 deployments, traffic from all of the sources for a specific multicast group are sent to all of the clients, regardless of whether they are sending MLDv1 or MLDv2 joins for this group. Keeping this feature disabled is recommended on VLANs where traffic from the specific source is only expected for the MLDv2 clients.

When an unknown multicast packet is received on a VLAN where the feature is enabled, it triggers programming of a starg entry in the hardware instead of SG.

On the HPE Aruba Networking 4100i, 6000, and 6100 Switch series, a single starg entry is programmed in advance for each join received and data driven programming of SG entries occurs when the traffic is received from a specific source for this group. As a result, the starg entry is used to forward the initial traffic and the SG entries programmed in the multicast forwarding table are used to forward subsequent traffic to all of the clients (that have sent either MLDv2 joins or MLDv3 joins) for all of the active joins in the feature enabled VLANs.

It is highly recommended to not enable this feature on devices where PIM or L3 multicast routing is enabled as it can lead to issues like permanent traffic loss.

Configuring this feature on devices where there are multiple sources sending traffic for the same group address is recommended.

This feature is mutually exclusive with the MLD snooping static group feature.



Optimization may vary environment to environment, based on scale.

Example

Enable preprogramming of starg flow on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping preprogramming-starg-flow enable
```

Remove all preprogramming of starg flow on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping preprogramming-starg-flow disable
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	config-vlan-<VLAN-ID>	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping version

```
ipv6 mld snooping [version <ver>]
no ipv6 mld snooping [version <ver>]
```

Description

This command configures the MLD snooping version on the VLAN. MLD version 2 is the default. The **no** form of the command configures the default MLD snooping version on the VLAN, **2**.

Parameter	Description
ver	Required: 1-2, MLD snooping version.

Example

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping version 2
```

```
switch(config-vlan)# no ipv6 mld snooping version 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan-<VLAN-ID>	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping static-group

```
ipv6 mld snooping [static-group <X:X::X:X>]
no ipv6 mld snooping [static-group <X:X::X:X>]
```

Description

This command configures static multicast group. The **no** form of this command disables static multicast group.

Parameter	Description
static-group	Required: <X:X::X:X>, MLD static multicast group.

Example

Configuring static multicast group:

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping static-group ff12::c
```

Removing the configuration of static multicast group:

```
switch(config)# vlan 2
switch(config-vlan)# no ipv6 mld snooping static-group ff12::c
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan-<VLAN-ID>	Administrators or local user group members with execution rights for this command.

MLD snooping show commands

show ipv6 mld snooping

```
show ipv6 mld snooping [vlan <vlan-id> [group <ip-addr>|{port <IF-NAME>}]
counters
detail
groups vlan <vlan-id>
no ...
packet-exceptions
static-groups
statistics
```

Description

This command shows MLD snooping details for all VLANs. Specify a VLAN ID or a VLAN and a group to display details for only that VLAN or VLAN group.

Parameter	Description
vlan <vlan-id>	Shows MLD snooping protocol information and number of

Parameter	Description
	different groups joined for the VLAN.
group	Shows MLD snooping details for the specified VLAN, including the number of different groups joined for the VLAN. Identify the group by IP address or interface name.
<ip-addr>	Display MLD snooping information for the selected group IP address.
port <IF-NAME>	Display information for a VLAN port. Specify the port name in member/slot/port format.
counters	Shows MLD query packets transmitted (Tx), received (Rx), and error packet counters.
detail	Shows the total VLANs with MLD enabled. When issued with the vlan <vlan-id> parameter, this command displays details for the selected VLAN.
groups	Show MLD snooping groups information.
vlan <vlan-id>	Display IGMP snooping operational information for specified VLAN
no ...	Negates any configured parameter.
packet-exceptions	Troubleshoot issues in an L2 multicast bridge entries for data packets forwarded to the CPU.
statistics	Show MLD snooping statistics.

Examples

```
switch# show ipv mld snooping vlan 2 group port 1/1/1

VLAN ID    : 2
VLAN Name  : VLAN2

Group Address : ff05::2:1
Last Reporter : fe80::1
Group Type   : Filter

Port      Vers Mode Uptime   Expires   V1      Sources  Sources
-----  -
1/1/1    2    INC  1m 46s  2m 34s   Timer   Forwarded Blocked
-----  -
Group Address : ff05::2:1
Source Address : 3000::1
Source Type   : Filter

Port      Mode Uptime   Expires   Configured Mode
-----  -
1/1/1    INC  1m 46s  2m 34s   Auto

Group Address : ff05::2:1
Source Address : 3000::2
Source Type   : Filter
```

Port	Mode	Uptime	Expires	Configured Mode
1/1/1	INC	1m 46s	2m 34s	Auto

Group Address : ff05::2:1
 Source Address : 3000::3
 Source Type : Filter

Port	Mode	Uptime	Expires	Configured Mode
1/1/1	INC	1m 46s	2m 34s	Auto

switch# **show ipv6 mld snooping counters**

MLD Snooping VLAN Counters

Rx Counters :

V1 All Hosts Queries	0
V2 All Hosts Queries	0
V2 Group Specific Queries	0
Group And Source Specific Queries	0
V1 Member Reports	0
V2 Member Reports	0
V1 Member Leaves	0

Tx Counters :

Flood on vlan	44
V1 Group Specific Queries	0
V2 Group Specific Queries	0

Errors:

Unknown Message Type	0
Malformed Packets	0
Bad Checksum	0
Packet received on MLD-disabled Interface	0
Interface Wrong Version Queries	0
Packets dropped by ACL	0

Port Counters:

Membership Timeout	0
--------------------	---

switch# **show ipv6 mld snooping groups**

MLD Group Address Information

VLAN ID	Group Address	Expires	UpTime	Last Reporter	Type
10	ff12::c	3m 54s	0m 26s	2001::1	Filter
10	ff12::d	4m 17s	0m 3s	2001::1	

switch# **show ipv6 mld snooping vlan 2 statistics**

MLD Snooping statistics

```
VLAN ID      :    2
VLAN Name    :  VLAN2
```

```
Number of Include Groups      :    1
Number of Exclude Groups     :    0
Number of Static Groups      :    1
Total Multicast Groups Joined :    2
```

switch# show ipv6 mld snooping packet-exceptions

List of L2 Multicast Bridge entries for which data packets are hitting CPU

Vlan	Group Address	Source-Address	Packet Count	Last Seen Time
10	ff03::10/128	1010::10/128	19	01h:02m:05s
10	ff03::12/128	1010::11/128	30	00d:02h:01m
10	ff04::10/12	1010::10/128	40	01m:02w:03d
20	ff03::11/128	5000::10/128	20	02m:02w:00d
20	ff03::12/128	5000::10/128	41	0001y:01m:02w:05d
20	ff04::10/128	5000::10/128	30	00d:02h:02m

Command History

Release	Modification
10.10	The packet-exceptions parameter is introduced.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

MLD configuration commands for interface VLAN

ipv6 mld (vlan)

```
ipv6 mld {enable | disable}
no ipv6 mld [enable | disable]
```

Description

This command enables or disables MLD on the interface VLAN.

The **no** form of this command disables MLD on the interface VLAN.

Parameter	Description
enable	Required: Enable MLD on the interface VLAN.
disable	Required: Disable MLD on the interface VLAN.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld enable
switch(config-if-vlan)# ipv6 mld disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld apply access-list (vlan)

```
ipv6 mld apply access-list <ACL-NAME>
no ipv6 mld apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the MLD join or leave packets based on rules set in the particular ACL name.

The **no** form of this command disables the rules set for the ACL.

Parameter	Description
access-list	Associates an ACL with the IGMP.
<ACL-NAME>	Specifies the name of the ACL.

Usage

- Existing classifier commands are used to configure the ACL.
- In case an IGMPv3 packet with multiple group addresses is received, the switch only processes the permitted group addresses based on the ACL rule set. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by ACL. This avoids the delay in learning of the permitted groups. Since the access switch configured with ACL blocks the traffic for the groups which are denied, forwarding of joins has no impact. If all the groups in the packet are

denied by the ACL rule, the packet is not forwarded to the querier and PIM router. Existing joins will timeout.

- In case of IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.

Examples

Configuring the ACL to filter MLD packets based on permit/deny rules set in access list **mygroup**:

```
switch(config)# access-list ipv6 mygroup
switch(config-acl-ip)# 10 deny icmpv6 any ff55::2
switch(config-acl-ip)# 20 deny icmpv6 any ff55::3
switch(config-acl-ip)# 30 permit icmpv6 any ff55::1
switch(config-acl-ip)# exit
switch(config)# interface vlan 2
switch(config-vlan)# ipv6 mld apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list **mygroup**:

```
switch(config-vlan)# no ipv6 mld apply access-list mygroup
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

no ipv6 mld

no ipv6 mld

Description

This command removes all MLD configurations on the interface.

Example

```
switch(config)# interface vlan 1
switch(config-if)# no ipv6 mld
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld querier (vlan)

ipv6 mld querier

Description

This command configures MLD querier.

The **no** form of this command disables MLD querier.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld querier
switch(config-if-vlan)# no ipv6 mld querier
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld querier interval (vlan)

ipv6 mld querier [interval <interval-value>]

Description

This command configures MLD querier interval. The default interval-value is 125.

Parameter	Description
interval-value	Required: 5-300, configures MLD querier interval. NOTE: Default interval-value is 125. Use the no ipv6 mld querier interval command to set interval-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld querier interval 100
switch(config-if-vlan)# no ipv6 mld querier interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld last-member-query-interval (vlan)

ipv6 mld last-member-query-interval <interval-value>

Description

This command configures MLD last member query interval value in seconds. The default interval-value is 1 second.

Parameter	Description
interval-value	Required: 1-2, configures MLD last-member-query-interval.



Default interval-value is 1 second. Use the `no ipv6 mld last-member-query-interval` command to set interval-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld last-member-query-interval 2
switch(config-if-vlan)# no ipv6 mld last-member-query-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld querier query-max-response-time (vlan)

```
ipv6 mld querier query-max-response-time <response-time>
```

Description

This command configures MLD max response time value in seconds. The default max-response-time-value is 10 seconds.

Parameter	Description
max-response-time-value	Required: 10-128, configures MLD querier max-response-time. NOTE: Default max-response-time-value is 10 seconds. Use the no ipv6 mld querier query-max-response-time command to set max-response-time-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld querier query-max-response-time 50
switch(config-if-vlan)# no ipv6 mld querier query-max-response-time
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld querier-wait-time(vlan)

```
ipv6 mld querier-wait-time <QUERIER-WAIT-TIME>
[no] ipv6 mld querier-wait-time <QUERIER-WAIT-TIME>
```

Description

Configures initial MLD querier-wait-time value in seconds.

The **no** form of this command sets the MLD querier-wait-time to the default value of 260 seconds. Note that the wait timer can be configured to any numbers within the 1-300 second range.

Parameter	Description
<QUERIER-WAIT-TIME-VALUE>	Configures MLD querier-wait-time to desired value.

Example

```
switch (config-if-vlan) # ipv6 mld querier-wait-time
<1-300> Querier Wait value (Default: 260)
switch (config-if-vlan) #
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld robustness (vlan)

ipv6 mld robustness <VALUE>

Description

This command configures MLD robustness. The robustness value represents the number of times the querier retries queries on the connected subnets. The default robustness-value is 2 seconds.

Parameter	Description
<VALUE>	Required: 1-7, configures MLD robustness.
	NOTE: Default robustness-value is 2 seconds. Use the no ipv6 mld robustness command to set robustness-value to the default.

Example

```
switch(config) # interface vlan 2
switch(config-if-vlan) # ipv6 mld robustness 5
switch(config-if-vlan) # no ipv6 mld robustness
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld static-group (vlan)

ipv6 mld static-group <MULTICAST-GROUP-IP>

Description

This command configures MLD static group.

Parameter	Description
<MULTICAST-GROUP-IP>	Required: X:X::X:X, configures MLD static group.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld static-group ff12::c
switch(config-if-vlan)# no ipv6 mld static-group ff12::c
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld version (vlan)

ipv6 mld version <VERSION>
no ipv6 mld version <VERSION>

Description

This command configures MLD version.

The **no** form of the command configures the default MLD version of **2**.

Parameter	Description
<code><VERSION></code>	Required: 1-2, configures MLD version.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld version 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld version strict (vlan)

```
ipv6 mld version <VERSION> [strict]
```

Description

This command configures MLD strict version. Packets that do not match the configured version will be dropped. By default, strict option is not enabled.

Parameter	Description
<code><VERSION></code>	Required: 1-2, configures MLD version.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld version 2 strict
switch(config-if-vlan)# no ipv6 mld version 2 strict
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

MLD show commands for interface VLAN



Only the default VRF is supported on the HPE Aruba Networking 4100i Switch Series.



Only the default VRF is supported on the HPE Aruba Networking 6000 and 6100 Switch Series.

show ipv6 mld

```
show ipv6 mld
  all-vrfs
  counters
  group <x:x::x:x> [source x:x::x:x]
  groups
  interface {<INTF-ID>} {vlan <vlan-id>}
  static-groups
  statistics [all-vrfs|{vrf <vrf-name>}]
```

Description

This command shows MLD groups joined details.

Parameter	Description
all-vrfs	Show MLD snooping info for all VRFs in all interfaces or groups, or for all VRFs in a specified group, interface or VLAN
counters	Show all MLD counters, or display counters for the specified interface or VLAN
group <x:x::x:x> [source <x:x::x:x>]	Show MLD group information for the specified group, group and interface, or group and vlan. Include the optional source <x:x::x:x> parameter to display source information for the group.
groups	Show MLD group information for all VRFs, or for groups in the specified interface or VLAN.
interface	Shows MLD configuration information for a specified interface or VLAN.
<INTF-ID>	Specify an Interface ID
vlan <vlan-id>	Specify a VLAN ID
static-groups	Display all static groups information, or include one of the

Parameter	Description
	additional parameters apply additional filters: ▪ all-vrfs: Display MLD static-group information for all VRFs ▪ vrf <vrf-name>: Display MLD static-group information for the selected VRF
statistics	Display all MLD statistics, or include one of the additional parameters apply additional filters: ▪ all-vrfs: Display MLD statistics information for all VRFs ▪ vrf <vrf-name>: Display MLD statistics information for the selected VRF

Examples

Showing the current MLD configuration and status

```
switch# show ipv6 mld

VRF Name           : default
Interface          : vlan10
MLD Configured Version : 2
MLD Operating Version  : 2
Querier State      : Querier
Querier IP [this switch] : fe80::7272:cfff:fe96:d3ec
Querier Uptime      : 39m 44s
Querier Expiration Time : 0m 31s
MLD Snoop Enabled on VLAN : True
```

Showing the MLD configuration on a specified VLAN or interface:

```
switch# show ipv6 mld interface vlan 10

MLD Configured Version : 2
MLD Operating Version  : 2
Querier State          : Querier
Querier IP [this switch] : fe80::7272:cfff:fe96:d3ec
Querier Uptime          : 40m 42s
Querier Expiration Time : 1m 39s
MLD Snoop Enabled on VLAN : True

switch# show ipv6 mld interface 1/1/2

MLD Configured Version : 2
MLD Operating Version  : 2
Querier State          : Querier
Querier IP [this switch] : fe80::7272:cfff:fe96:d3ec
Querier Uptime          : 40m 42s
Querier Expiration Time : 1m 39s
MLD Snoop Enabled on VLAN : True
```

Showing MLD groups information for a specified interface:

```
switch# show ipv6 mld interface 1/1/1 groups
```

MLD group information for group ff55::1

Interface Name : 1/1/1
VRF Name : default

Group Address : ff55::1
Last Reporter : fe80::a00:9ff:fe77:1062

Vers	Mode	Uptime	Expires	V1 Timer	Sources Forwarded	Sources Blocked
2	EXC	0m 14s	4m 6s			

Showing MLD static groups

```
switch# show ipv6 mld static-groups all-vrfs
```

MLD Static Group Address Information

VRF Name :default

Interface Name	Group Address
vlan2	ff12::c
vlan2	ff12::d

Showing MLD counters

```
switch# show ipv6 mld counters
```

MLD Counters

Interface Name : vlan2
VRF Name : default
Membership Timeout : 0

	Rx	Tx
V1 All Hosts Queries	0	0
V2 All Hosts Queries	0	12
V1 Group Specific Queries	0	0
V2 Group Specific Queries	0	0
Group And Source Specific Queries	0	0
V2 Member Reports	0	N/A
V1 Member Reports	0	N/A
V1 Member Leaves	0	N/A
Packets dropped by ACL	0	N/A

```
switch# show ipv6 mld counters vrf default
```

MLD Counters

Interface Name : vlan2
VRF Name : default
Membership Timeout : 0

	Rx	Tx
V1 All Hosts Queries	0	0
V2 All Hosts Queries	0	12

V1 Group Specific Queries	0	0
V2 Group Specific Queries	0	0
Group And Source Specific Queries	0	0
V2 Member Reports	0	N/A
V1 Member Reports	0	N/A
V1 Member Leaves	0	N/A
Packets dropped by ACL		

Showing MLD statistics on a specified interface:

```
switch# show ipv6 mld interface 1/1/1 statistics

MLD statistics

Interface Name : 1/1/1
VRF Name       : default

Number of Include Groups      : 2
Number of Exclude Groups     : 0
Number of Static Groups      : 0
Total Multicast Groups Joined : 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

MLD configuration commands for interface

ipv6 mld (interface)

```
ipv6 mld {enable | disable}
no ipv6 mld {enable | disable}
```

Description

This command enables or disables MLD on the interface.

The **no** form of this command disables MLD on the interface.

Parameter	Description
enable	Required: Enable MLD on the interface.
disable	Required: Disable MLD on the interface.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld enable
switch(config-if)# ipv6 mld disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld apply access-list (interface)

```
ipv6 mld apply access-list <ACL-NAME>
no ipv6 mld apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the MLD join or leave packets based on rules set in the particular ACL name.

The **no** form of this command removes the rules set for the ACL.

Parameter	Description
access-list	Associates an ACL with the IGMP.
<ACL-NAME>	Specifies the name of the ACL.

Usage

- Existing classifier commands are used to configure the ACL.
- In case an IGMPv3 packet with multiple group addresses is received, the switch only processes the permitted group addresses based on the ACL rule set. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by ACL. This avoids the delay in learning of the permitted groups. Since the access switch configured with ACL blocks the traffic for the groups which are denied, forwarding of joins has no impact. If all the groups in the packet are denied by the ACL rule, the packet is not forwarded to the querier and PIM router. Existing joins will timeout.
- In case of IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.

Examples

Configuring the ACL to filter MLD packets based on permit/deny rules set in access list **mygroup**:

```
switch(config)# access-list ipv6 mygroup
switch(config-acl-ip)# 10 deny icmpv6 any ff55::2
switch(config-acl-ip)# 20 deny icmpv6 any ff55::3
switch(config-acl-ip)# 30 permit icmpv6 any ff55::1
switch(config-acl-ip)# exit
switch(config)# interface vlan 1
switch(config-vlan)# ipv6 mld apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list **mygroup**:

```
switch(config-vlan)# no ipv6 mld apply access-list mygroup
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

no ipv6 mld

no ipv6 mld

Description

This command removes all MLD configurations on the interface.

Example

```
switch(config)# interface vlan 1
switch(config-if)# no ipv6 mld
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms,	config-if	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
except for S3L75A, S3L76A, S3L77A		

ipv6 mld querier (interface)

ipv6 mld querier

Description

This command configures MLD querier. This functionality will allow the interface to join in the querier-election process.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld querier
switch(config-if)# no ipv6 mld querier
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld querier interval (interface)

ipv6 mld querier [interval <interval-value>]

Description

This command configures MLD querier interval. The default interval-value is 125.

Parameter	Description
interval-value	Required: 5-300, configures MLD querier interval. NOTE: Default interval-value is 125. Use the <code>no ipv6 mld querier interval</code> command to set interval-value to the default.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld querier interval 100
switch(config-if)# no ipv6 mld querier interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld last-member-query-interval (interface)

ipv6 mld last-member-query-interval <interval-value>

Description

This command configures MLD last member query interval value in seconds. The default interval-value is 1 second.

Parameter	Description
interval-value	Required: 1-2, configures MLD last-member-query-interval.



Default interval-value is 1 second. Use the `no ipv6 mld last-member-query-interval` command to set interval-value to the default.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld last-member-query-interval 2
switch(config-if)# no ipv6 mld last-member-query-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld querier query-max-response-time (interface)

```
ipv6 mld querier query-max-response-time <response-time>
```

Description

This command configures MLD max response time value in seconds. The default max-response-time-value is 10 seconds.

Parameter	Description
max-response-time-value	Required: 10-128, configures MLD querier max-response-time. NOTE: Default max-response-time-value is 10 seconds. Use the no ipv6 mld querier query-max-response-time command to set max-response-time-value to the default.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld query-max-response-time 50
switch(config-if)# no ipv6 mld query-max-response-time
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld robustness (interface)

```
ipv6 mld robustness <value>
```

Description

This command configures MLD robustness. The robustness value represents the number of times the querier retries queries on the connected subnets. The default robustness-value is 2 seconds.

Parameter	Description
robustness-value	Required: 1-7, configures MLD robustness.



Default robustness-value is 2 seconds. Use the `no ipv6 mld robustness` command to set robustness-value to the default.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld robustness 5
switch(config-if)# no ipv6 mld robustness
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld static-group (interface)

`ipv6 mld static-group <multicast-group-ip>`

Description

This command configures MLD static group.

Parameter	Description
multicast-group-ip	Required: X:X::X:X, configures MLD static group.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld static-group ff12::c
switch(config-if)# no ipv6 mld static-group ff12::c
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping filter-unknown-mcast

```
ipv6 mld snooping filter-unknown-mcast
no ipv6 mld snooping filter-unknown-mcast
```

Description

Configures the unknown multicast to steal when the MLD snooping is enabled.

The **no** form of this command returns to the default behavior of initial flooding of unknown multicast traffic.

Usage

In the default behavior, the unknown multicast traffic is flooded until the IP Multicast Flow programming is done on the hardware. This is known as initial flooding of unknown multicast. Use this command to filter unknown multicast instead of flooding.



Initial flooding of multicast traffic is observed for a few seconds after the device comes up from a reboot. This issue is only seen when the multicast source connected device is rebooted. Once the device is up after a reboot, it takes a few seconds for the CPU Rx rule to be programmed during the timeframe that the initial flooding is observed. This is an expected behavior.

Example

Configure the unknown multicast to steal globally on IGMP snooping enabled VLANs.

```
switch# configure terminal
switch(config)# ipv6 mld snooping filter-unknown-multicast
```

Removing the configuration of the unknown multicast to steal globally on IGMP snooping enabled VLANs.

```
switch# configure terminal
switch(config)# no ipv6 mld snooping filter-unknown-multicast
```

Command History

Release	Modification
10.14	Command introduced on the 4100i, 6000, and 6100 Switch series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	config	Administrators or local user group members with execution rights for this command.

ipv6 mld version (interface)

```
ipv6 mld version <version>
no ipv6 mld version <version>
```

Description

This command configures MLD version.

The **no** form of this command removes MLD version from the interface.

Parameter	Description
version	Required: 1-2, configures MLD version.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld version 2
```

```
switch(config)# interface vlan 1
switch(config-if)# no ipv6 mld version 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld version strict (interface)

```
ipv6 mld version <version> [strict]
```

Description

This command configures MLD strict version. Packets that do not match the configured version will be dropped. By default, strict option is not enabled.

Parameter	Description
version	Required: 1-2, configures MLD version.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld version 2 strict
switch(config-if)# no ipv6 mld version 2 strict
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

Internet Group Management Protocol (IGMP)

In a network where IP multicast traffic is transmitted for various multimedia applications, you can use the switch to reduce unnecessary bandwidth usage on a per-port basis by configuring IGMP (Internet Group Management Protocol). IGMPv3 (RFC 3376) and IGMPv2 (RFC 2236) are the current RFCs for IGMP.

In the factory default state (IGMP disabled), the switch simply floods all IP multicast traffic it receives on a given VLAN through all ports on that VLAN (except the port on which it received the traffic). This can result in significant and unnecessary bandwidth usage in networks where IP multicast traffic is a factor. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch.

IGMP is useful in multimedia applications such as LAN TV, desktop conferencing, and collaborative computing, where there is MultiPoint communication; that is, communication from one to many hosts, or communication originating from many hosts and destined for many other hosts.

In such MultiPoint applications, IGMP will be configured on the hosts, and multicast traffic will be generated by one or more servers (inside or outside of the local network). Switches in the network (that support IGMP) can then be configured to direct the multicast traffic to only the ports where needed. If multiple VLANs are configured, you can configure IGMP on a per-VLAN basis.

Enabling IGMP allows the router to become querier. If there is another querier in the LAN, the router will resume non querier functionality and will respond to query/report packets.

IGMP defaults, protocols, and supported configuration

IGMP default configuration:

- IGMP is disabled by default.
- The default IGMP version is IGMPv3.

IGMP supported protocols include:

- IGMPv2 (RFC 2236)
- IGMPv3 (RFC 3376)

Static groups:

You can configure a maximum of 32 IGMP static groups on the HPE Aruba Networking 6000 and 6100 Switch Series.

How the IGMP protocol works

IGMP manages multicast group memberships based on the query and response mechanism.

IGMP is an internal protocol of the IP suite. IP manages multicast traffic by using switches, multicast routers, and hosts that support IGMP. A multicast router is not necessary as long as a switch is configured to support IGMP with the querier feature enabled. A set of hosts, routers, and/or switches that send or receive multicast data streams to or from the same sources, is called a multicast group. All devices in the group use the same multicast group address.

The multicast group uses three fundamental types of messages to communicate:

- **Query:** A message sent from the querier (multicast router or switch) asking for a response from each host belonging to the multicast group. If a multicast router supporting IGMP is not present, the switch must assume this function to elicit group membership information from the hosts on the network.
- **Join:** A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the join message.
- **Leave group:** A message sent by a host to the querier to indicate that the host has ceased to be a member of a specific multicast group.

An IP multicast packet includes the multicast group (address) to which the packet belongs. When an IGMP client connected to a switch port needs to receive multicast traffic from a specific group, it joins the group by sending an IGMP join request to the network. (The multicast group specified in the join request is determined by the requesting application running on the IGMP client.)

When the client is ready to leave the multicast group, it sends a Leave Group message to the network and ceases to be a group member. When the leave request is detected, the appropriate IGMP device ceases transmitting traffic for the designated multicast group through the port on which the leave request was received (as long as there are no other current members of that group on the affected port.)

Thus, IGMP identifies members of a multicast group (within a subnet) and allows IGMP-configured hosts (and routers) to join or leave multicast groups.

Considerations when configuring IGMP

With the factory default setting, multicast data transmitted from the sources will be flooded on all ports in the VLAN. Configuring IGMP snooping avoids flooding and causes the switch to forward data only to the receivers.

The function of the IGMP querier is to poll other IGMP-enabled devices in an IGMP-enabled interface to elicit group membership information. On enabling IGMP, the router performs this function if there is no other device in the interface to act as querier.

Basic steps to configure IGMP:

1. Configure VLANs.
2. Configure ports and assign them to the VLANs.
3. Configure the L3 interface (an interface VLAN) and assign an IP address to the interface.
4. Enable IGMP.
5. Choose the desired IGMP version. The default is version 3.

IGMP configuration considerations:

- For IGMP to be operational, the interface has to be administratively up. For interface VLANs, the L2 VLAN has to be up and one of the ports in the VLAN has to be up.
- The IP address must be assigned for the interface to become querier. Without an IP address, the device will remain in a non querier state.
- A querier is required for proper IGMP operation. For this reason, you must enable IGMP on the L3 Interface. If the querier functionality is not configured or disabled, you must ensure that there is an IGMP querier in the same VLAN.
- For IGMP snooping to be operational on a VLAN, the VLAN has to be administratively up and at least one port in the VLAN has to be up.

- If IGMP snooping is enabled on the VLAN, and IGMP is enabled on the interface VLAN, and the configured version does not match, the lowest version is chosen as the operating version.
- If the switch becomes the querier for a particular interface, then subsequently detects queries transmitted from another device on the same VLAN, the switch ceases to operate as the querier for that interface.
- The switch automatically ceases querier operation in an IGMP-enabled interface if it detects another querier on the interface. You can also use the switch CLI to disable the querier capability.
- Multicast traffic will be flooded on the VLAN, if TTL=1 or TTL>255 regardless of IGMP joins and group membership within the VLAN.
- The switch automatically ceases to be a querier if it receives a query message from another switch/router in its network with a lower IP address.

IGMP Troubleshooting

If the switch displays the error message **IGMP/MLD internal queue limit exceeded. Needs admin intervention** with event log ID 2628, take the following actions:

1. Check to see if a misbehaving client is sending too many reports or joins and leave messages. If so, fix the issue at the client side or apply appropriate ACLs.
2. Identify if there is a loop in the network causing too many IGMP/MLD control packets and address the loop issue.
3. If IGMP/MLD configuration processing is stuck, restart the MGMD daemon.
4. Reduce the CoPP limits for IGMP/MLD class based on the amount of control packets expected for the switch deployment.



The 6000 Switch series does not support router port detection via PIM control packets. As a result, IGMP reports are not forwarded to router ports learned through PIM. However, IGMP/MLD Querier port learning is fully supported on this platform and the device learns querier ports and forwards IGMP/MLD control packets to them as expected. This ensures proper multicast group management and protocol operation.

IGMP configuration task list

Tasks at a glance.

- [Enabling or disabling IGMP](#)
- [Specifying the IGMP version](#)
- [Configuring IGMP static groups](#)
- [Configuring IGMP query and response parameters](#)
- [Disabling IGMP](#)
- [Viewing IGMP information](#)

Enabling or disabling IGMP

Prerequisites

You must be in an interface configuration context, as indicated by the **switch(config-if-vlan)#** prompt. For IGMP to be operational, the interface has to be up. To become querier, the interface must have an IP address associated with it.

Procedure

IGMP is disabled by default. Enable IGMP on an interface using the following command.

```
ip igmp {enable | disable}
```

For example, the following command enables IGMP on interface VLAN 2:

```
switch(config)# interface vlan 2  
switch(config-if-vlan)# ip igmp enable
```

Use the **disable** parameter to disable IGMP on an interface.

Specifying the IGMP version

The version can be either 2 (IGMPv2) or 3 (IGMPv3). The default is 3. IGMPv2 supports filtering based on groups. IGMPv3 is more advanced and includes filtering based on source and groups.

If using the `strict` option, packets that do not match the configured version will be dropped.

Prerequisites

You must be in an interface configuration context, as indicated by the **switch(config-if-vlan)#** prompt.

Procedure

Specify the IGMP version for an interface using one of the following commands.

```
ip igmp version <VERSION>
```

```
ip igmp version <VERSION> strict
```

For example, the following command sets the IGMP version to 2 on interface VLAN 2:

```
switch(config)# interface vlan 2  
switch(config-if-vlan)# ip igmp version 2
```

And the following command sets IGMP strict version to 2 on interface VLAN 5:

```
switch(config)# interface vlan 5  
switch(config-if-vlan)# ip igmp version 2 strict  
switch(config-if-vlan)# no ip igmp version 2 strict
```

Configuring IGMP static groups

The switch will always flood the traffic destined for a group configured as static group. So the hosts will receive the traffic for static groups even if they have not subscribed for that group. You can configure a maximum of 32 IGMP static groups.

Prerequisites

You must be in an interface configuration context, as indicated by the **switch(config-if-vlan)#** prompt.

Procedure

Configure an IGMP static group on an interface using the following command.

```
ip igmp static-group <MULTICAST-GROUP-IP>
```

For example, the following command configures an IGMP static multicast group as 239.1.1.1 on interface VLAN 2:

```
switch(config)# interface vlan 2  
switch(config-if-vlan)# ip igmp static-group 239.1.1.1
```

The **no** form of the command removes an IGMP static group.

Configuring IGMP query and response parameters

Configure query and response parameters such as querier interval, last member query interval, max response time, and robustness.

Prerequisites

You must be in an interface configuration context, as indicated by the `switch(config-if-vlan)#` prompt.

Procedure

Configure IGMP query and response parameters on an interface using the following commands.

- Make sure that the IGMP querier is enabled. (In IGMPv3 the IGMP querier is enabled by default.) Configure the IGMP querier on an interface using the following command: `ip igmp querier`.
- Configure the IGMP querier interval on an interface using the following command: `ip igmp querier interval`
`<INTERVAL-VALUE>`. The interval is from 5-300 seconds, with a default of 125.
- Configure the IGMP last member query interval value in seconds on an interface using the following command: `ip igmp last-member-query-interval`
`<INTERVAL-VALUE>`. The interval is from 1-2 seconds, with a default of 1.
- Configure the IGMP max response time value in seconds on an interface using the following command: `ip igmp querier query-max-response-time <RESPONSE-TIME>`. The response time is from 10-128 seconds, with a default of 10.
- Configure the IGMP robustness (the number of times to retry a query) on an interface using the following command: `ip igmp robustness <VALUE>`. The robustness value is from 1-7 with default of 2.

For example, the following command configures the IGMP querier interface interval as 100 on interface VLAN 2. The **no** form of the command sets the interval to the default.

```
switch(config)# interface vlan 2  
switch(config-if-vlan)# ip igmp querier interval 100  
switch(config-if-vlan)# no ip igmp querier interval
```

Disabling IGMP

Prerequisites

You must be in an interface configuration context, as indicated by the **switch(config-if-vlan)#** prompt.

Procedure

Remove IGMP from an interface using the following command.

```
no ip igmp
```

For example, the following command removes IGMP on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip igmp
```

Viewing IGMP information

For some commands, you can specify viewing information by interface or by VRF.

Prerequisites

Use these show commands from the Operator (>) or Manager (#) context.

Procedure

To view IGMP information, use the following commands.

- To view IGMP configuration details and status, use: **show ip igmp** or use **show ip igmp interface**.
- To view IGMP statistics and groups joined, use: **show ip igmp statistics** or use **show ip igmp interface statistics**.
- To view IGMP counters, use: **show ip igmp counters** or use **show ip igmp interface counters**.
- To view IGMP static groups, use: **show ip igmp static-groups**.
- To view IGMP group information, use: **show ip igmp groups** or use **show ip igmp interface groups**.
- To view IGMP group details for a specific group and source, use: **show ip igmp group** or use **show ip igmp interface group**. Optionally you can also display joined group details by VRF.

IGMP configuration example

The output of the following `show running-config` command shows an example of an IGMP configuration with IGMP snooping.

```
switch# show running-config
Current configuration:
!
!
!
!
!
access-list ip mygroup
  10 permit any any 239.1.1.1/24
access-list ip mygroup1
  10 permit any any any
vlan 1
  no shutdown
vlan 2
  ip igmp snooping enable
  ip igmp snooping static group 239.1.1.10
  ip igmp snooping static group 239.1.1.11
! 'mygroup' will be ignored in this configuration as 'mygroup1' is configured in
'vlan2'.
  ip igmp snooping apply access-list mygroup
interface 1/1/1
  no shutdown
  ip address 100.1.1.1/24
  ip igmp enable
interface 1/1/2
  no shutdown
```

```

ip address 200.1.1.1/24
ip igmp enable
ip igmp querier interval 5
ip igmp last-member-query-interval 2
ip igmp query-max-response-time 50
ip igmp static-group 239.1.1.1
ip igmp apply access-list mygroup1
interface 1/1/3
no shutdown
no routing
vlan access 2
ip igmp snooping blocked vlan 2
interface 1/1/3
no shutdown
no routing
vlan access 2
ip igmp snooping forward vlan 2
interface vlan2
no shutdown
ip address 20.1.1.1/24
ip igmp enable
ip igmp querier interval 5
ip igmp robustness 5
ip igmp last-member-query-interval 2
ip igmp query-max-response-time 50
ip igmp static-group 239.1.1.1
ip igmp apply access-list mygroup1

```

IGMP commands

For commands in the interface configuration context, the interface must be an L3 interface. The supported contexts include: `config-if-vlan`.

ip igmp

```

ip igmp {enable | disable}
no ip igmp [enable | disable]

```

Description

Enables or disables IGMP on the current interface. IGMP is disabled by default. The **no** form of this command disables IGMP on the current interface.

Parameter	Description
enable	Enable IGMP.
disable	Disable IGMP.

Examples

Enabling IGMP on interface VLAN 2:

```

switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp enable
Disabling IGMP on interface VLAN 2:

```

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp disable
```

Enabling IGMP on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# routing

switch(config-subif)# ip igmp enable
```

Disabling IGMP on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-subif)# ip igmp disable
```

```
switch(config)# interface 1/1/1
switch(config-subif)# no ip igmp enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ip igmp apply access-list

```
ip igmp apply access-list <ACL-NAME>
no ip igmp apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the IGMP join or leave packets based on rules set in the particular ACL name.

The **no** form of this command unconfigures the rules set for the ACL.



This configuration will override the ACL associated with IGMP snooping on the corresponding L2 VLAN.

Parameter	Description
access-list	Associates an ACL with the IGMP.
<ACL-NAME>	Specifies the name of the ACL.

Usage

- Existing classifier commands are used to configure the ACL.
- In case an IGMPv3 packet with multiple group addresses is received, the switch only processes the permitted group addresses based on the ACL rule set. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by ACL. This avoids the delay in learning of the permitted groups. Since the access switch configured with ACL blocks the traffic for the groups which are denied, forwarding of joins has no impact. If all the groups in the packet are denied by the ACL rule, the packet is not forwarded to the querier and PIM router. Existing joins will timeout.
- In case of IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.

Examples

Configuring the ACL on a VLAN to filter IGMP packets based on permit/deny rules set in access list **mygroup**:

```
switch(config)# access-list ip mygroup
switch(config-acl-ip)# 10 deny igmp any 239.255.255.250
switch(config-acl-ip)# 20 deny igmp any 239.255.255.253
switch(config-acl-ip)# 30 permit igmp any 239.1.1.1
switch(config-acl-ip)# exit
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list **mygroup**:

```
switch(config-if-vlan)# no ip igmp apply access-list mygroup
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ip igmp last-member-query-interval

ip igmp last-member-query-interval <INTERVAL-VALUE>

```
no ip igmp last-member-query-interval <INTERVAL-VALUE>
```

Description

Configures an IGMP last member query interval value in seconds on an interface, depending on the command context you are in.

The **no** form of this command sets the value to a default of 1 second on an interface.

Parameter	Description
<INTERVAL-VALUE>	Specifies an IGMP last-member-query-interval on the interface. Default: 1 second. Range: 1-2 seconds.

Examples

Configuring an IGMP last member query interval of 2 on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp last-member-query-interval 2
switch(config-if-vlan)# no ip igmp last-member-query-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ip igmp querier

```
ip igmp querier
no ip igmp querier
```

Description

Configures an IGMP querier on an interface, depending on the command context you are in. This functionality will allow an interface to join in the querier-election process.

The **no** form of this command disables IGMP querier on an interface.

Examples

Configuring an IGMP querier on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp querier
```

Disabling an IGMP querier on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip igmp querier
```

Configuring an IGMP querier on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# routing
switch(config-subif)# ip igmp querier
```

Disabling an IGMP querier on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-subif)# no ip igmp querier
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All , except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ip igmp querier interval

```
ip igmp querier interval <INTERVAL-VALUE>
no ip igmp querier interval
```

Description

Configures the interval between IGMP queries on an interface, depending on the command context you are in.

The **no** form of this command sets the IGMP querier interval to the default value of 125 seconds on an interface.

Parameter	Description
<INTERVAL-VALUE>	Specifies the IGMP querier interval in seconds on the interface. Default: 125 seconds. Range: 5-300.

Examples

Configuring an IGMP querier interface interval of 100 on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp querier interval 100
```

Resetting an IGMP querier interval to the default value:

```
switch(config-if-vlan)# no ip igmp querier interval
```

Configuring an IGMP querier interface interval of 100 on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# routing
switch(config-subif)# ip igmp querier interval 100
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ip igmp querier query-max-response-time

```
ip igmp querier query-max-response-time <RESPONSE-TIME>
no ip igmp querier query-max-response-time <RESPONSE-TIME>
```

Description

Configures the IGMP querier max response time value in seconds on an interface, depending on the command context you are in.

The **no** form of this command sets the querier max response time value to the default of 10 seconds on an interface.

Parameter	Description
<RESPONSE-TIME>	Specifies the IGMP querier max response time value on the interface. Default: 10 seconds. Range: 10-128 seconds.

Examples

Configuring the IGMP querier maximum response time of 50 for interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp query-max-response-time 50
```

Resetting an IGMP querier interval to the default value:

```
switch(config-if-vlan)# no ip igmp query-max-response-time
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ip igmp querier-wait-time

```
ip igmp querier-wait-time <QUERIER-WAIT-TIME>
no ip igmp querier-wait-time <QUERIER-WAIT-TIME>
```

Description

Configures initial IGMP querier-wait-time value in seconds.

The **no** form of this command sets the IGMP querier-wait-time to the default value of 260 seconds. Note that the wait timer can be configured to any numbers within the 1-300 second range.

Parameter	Description
<QUERIER-WAIT-TIME>	Configures IGMP querier-wait-time to desired value.

Examples

Configuring IGMP querier-wait-time:

```
switch(config-if-vlan)# ip igmp querier-wait-time
<1-300> Querier Wait value (Default: 260)
switch(config-if-vlan)#
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ip igmp robustness

```
ip igmp robustness <VALUE>
no ip igmp robustness <VALUE>
```

Description

Configures IGMP robustness on an interface, depending on the command context. The robustness parameter allows tuning for the expected packet loss on a subnet.

The **no** form of this command sets the robustness value to the default of 2 on an interface.

Parameter	Description
<VALUE>	Specifies an IGMP robustness value on the interface. Default: 2. Range: 1-7.

Examples

Configuring an IGMP robustness of 5 on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp robustness 5
```

Resetting the IGMP robustness to the default:

```
switch(config-if-vlan)# no ip igmp robustness
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ip igmp router-alert-check

```
ip igmp router-alert-check [enable | disable]
no ip igmp router-alert-check [enable | disable]
```

Description

Enables or disables IGMP router alert check for IGMP packets. IGMP packets without the router alert field set are dropped if router alert check is enabled. Router alert check is disabled by default.

The **no** form of this command disables router alert check for IGMP packets.

Parameter	Description
enable	Enable IGMP router alert check.
disable	Disable IGMP router alert check.

Examples

Enabling IGMP router alert check on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp router-alert-check enable
```

Disabling IGMP router alert check on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp router-alert-check disable
```

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip igmp router-alert-check enable
```

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ip igmp static-group

```
ip igmp static-group <MULTICAST-GROUP-IP>
no ip igmp static-group <MULTICAST-GROUP-IP>
```

Description

Configures an IGMP static multicast group on an interface, depending on the command context you are in. You can configure a maximum of 32 IGMP static groups.

The **no** form of the command unconfigures IGMP static multicast group on an interface.

Parameter	Description
<code><MULTICAST-GROUP-IP></code>	Specifies an IGMP static multicast group IP address on the interface. Format: A.B.C.D

Examples

Administrators or local user group members with execution rights for this command.

Configuring an IGMP static group on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp static-group 239.1.1.1
```

Resetting an IGMP static group on an interface to the default (none):

```
switch(config-if)# no ip igmp static-group 239.1.1.10
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ip igmp version

```
ip igmp version <VERSION>
no ip igmp version <VERSION>
```

Description

Configures the IGMP version on an interface, depending on the command context you are in.

The **no** form of the command configures the default IGMP version, 3, on the interface.

Parameter	Description
<code><VERSION></code>	Specifies the IGMP version on the interface. Select 2 for IGMPv2 (RFC2236). Select 3 for IGMPv3 (RFC3376). Values: 2 or 3.

Examples

Configuring an IGMP version on interface VLAN 2:

```
switch(config)# interface vlan 2  
switch(config-if-vlan)# ip igmp version 2
```

Removing an IGMP version on interface VLAN 2:

```
switch(config)# interface vlan 2  
switch(config-if-vlan)# no ip igmp version 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ip igmp version strict

```
ip igmp version <VERSION> strict  
no ip igmp version <VERSION> strict
```

Description

Configures an IGMP strict version on an interface, depending on the command context you are in. Drops packets that do not match the configured version.

The **no** form of the command removes the strict version configuration from the interface.

Parameter	Description
<VERSION>	Specifies the IGMP version on the interface. Select 2 for IGMPv2 (RFC2236). Select 3 for IGMPv3 (RFC3376). Values: 2 or 3.

Examples

Configuring the IGMP strict version to 2 on interface VLAN 2:

```
switch(config)# interface vlan 2  
switch(config-if-vlan)# ip igmp version 2 strict
```

Resetting the IGMP strict version to the default (none):

```
switch(config-if)# no ip igmp version 2 strict
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

no ip igmp

```
no ip igmp
```

Description

Disables all IGMP configurations on an interface or sub-interface, depending on the command context you are in.

Examples

Removing IGMP on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip igmp
```

Removing IGMP on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-subif)# no ip igmp
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for	config-if-vlan	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
S3L75A, S3L76A, S3L77A		

show ip igmp

show ip igmp [all-vrfs]

Description

Shows IGMP configuration information and status, or shows information by VRF.

Parameter	Description
all-vrfs	To show information for all VRFs, specify all-vrfs .

Examples

Showing IGMP configuration and status:

```
switch# show ip igmp

VRF Name   : default
Interface  : vlan2
IGMP Configured Version   : 3
IGMP Operating Version    : 3
Querier State              : Querier
Querier IP [this switch]  : 20.1.1.1
Querier Uptime             : 1m 4s
Querier Expiration Time   : 0m 1s
IGMP Snoop Enabled on VLAN : True
```

Showing IGMP information for all VRFs:

```
switch# show ip igmp all-vrfs

VRF Name   : default
Interface  : vlan5
IGMP Configured Version   : 3
IGMP Operating Version    : 2
Querier State              : Querier
Querier IP [this switch]  : 50.1.1.1
Querier Uptime             : 1m 1s
Querier Expiration Time   : 0m 4s
IGMP Snoop Enabled on VLAN : False
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp counters

show ip igmp counters [all-vrfs]

Description

Shows IGMP counter details, or shows counters by VRF.

Parameter	Description
all-vrfs	Specify all-vrfs to show information for all VRFs.

Examples

Showing IGMP counters:

```
switch# show ip igmp counters

IGMP Counters

Interface Name      : vlan2
VRF Name            : default
Membership Timeout  : 0

Rx                  Tx
-----
V1 All Hosts Queries      0      0
V2 All Hosts Queries      0     12
V3 All Hosts Queries      0      0
V2 Group Specific Queries  0      0
V3 Group Specific Queries  0      0
Group And Source Specific Queries  0      0
V3 Member Reports         0     N/A
V2 Member Reports         0     N/A
V1 Member Reports         0     N/A
V2 Member Leaves          0     N/A
Packets dropped by ACL     0     N/A
```

Showing IGMP counters for the default VRF:

```
switch# show ip igmp counters vrf default

IGMP Counters

Interface Name      : vlan2
VRF Name            : default
Membership Timeout  : 0

Rx                  Tx
-----
V1 All Hosts Queries      0      0
V2 All Hosts Queries      0     12
```

V3 All Hosts Queries	0	0
V2 Group Specific Queries	0	0
V3 Group Specific Queries	0	0
Group And Source Specific Queries	0	0
V3 Member Reports	0	N/A
V2 Member Reports	0	N/A
V1 Member Reports	0	N/A
V2 Member Leaves	0	N/A
Packets dropped by ACL	0	N/A

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp group

show ip igmp group <GROUP-IP> [source <SOURCE-IP>] [all-vrfs]

Description

Shows IGMP joined group information for the specified group, or shows joined group source and display information by VRF.

Parameter	Description
<GROUP-IP>	Specifies the IP address of the group. Format: A.B.C.D
source <SOURCE-IP>	Specifies the IP address of the source. Format: A.B.C.D
all-vrfs	Specify all-vrfs to show information for all VRFs.

Examples

Showing IGMP joined group details for group 239.1.1.10:

```
switch# show ip igmp group 239.1.1.10

IGMP group information for group 239.1.1.10

Interface Name      : vlan2
VRF Name            : default

Group Address       : 239.1.1.10
Last Reporter       : 100.1.1.10
```

Vers	Mode	Uptime	Expires	V1 Timer	V2 Timer	Sources Forwarded	Sources Blocked
----	----	-----	-----	-----	-----	-----	-----
3	EXC	16m 34s	2m 27s				

Showing IGMP joined group details for group 239.1.1.10 and source 10.1.1.10:

```
switch# show ip igmp group 239.1.1.10 source 10.1.1.10
```

```
Interface Name : vlan2
VRF Name      : default
Group Address  : 239.1.1.10
Source Address : 10.1.1.10
```

Mode	Uptime	Expire
----	-----	-----
	0m 13s	4m 7s

Showing IGMP joined group details for group 239.1.1.10 for all VRFs:

```
switch# show ip igmp group 239.1.1.10 all-vrfs
```

```
IGMP group information for group 239.1.1.10
```

```
Interface Name : vlan10
VRF Name       : default
Group Address   : 239.1.1.10
Last Reporter   : 100.1.1.10
```

Vers	Mode	Uptime	Expires	V1 Timer	V2 Timer	Sources Forwarded	Sources Blocked
----	----	-----	-----	-----	-----	-----	-----
3	EXC	17m 5s	4m 2s				

Showing IGMP joined group details for group 239.1.1.10 source 10.1.1.10 for all VRFs:

```
switch# show ip igmp group 239.1.1.10 source 10.1.1.10 all-vrfs
```

```
Interface Name : vlan10
VRF Name       : default
Group Address   : 239.1.1.10
Source Address  : 10.1.1.10
```

Mode	Uptime	Expire
----	-----	-----
	0m 39s	3m 41s

Showing IGMP joined group details group 239.1.1.10 for the default VRF:

```
switch# show ip igmp group 239.1.1.10 vrf default
```

```
IGMP group information for group 239.1.1.10
```

```
Interface Name    : vlan2
VRF Name          : default

Group Address     : 239.1.1.10
Last Reporter     : 100.1.1.10
```

Vers	Mode	Uptime	Expires	V1 Timer	V2 Timer	Sources Forwarded	Sources Blocked
3	EXC	17m 35s	3m 32s				

Showing IGMP joined group details group 239.1.1.10 source 10.1.1.10 for the default VRF:

```
switch# show ip igmp group 239.1.1.10 source 10.1.1.10 vrf default
```

```
Interface Name    : vlan10
VRF Name          : default
Group Address     : 239.1.1.10
Source Address    : 10.1.1.10
```

Mode	Uptime	Expire
	0m 59s	3m 21s

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp groups

```
show ip igmp groups [all-vrfs]
```

Description

Shows IGMP group information, or you can display group information by VRF.

Parameter	Description
all-vrfs	Specify all-vrfs to show information for all VRFs.

Examples

Showing IGMP group information:

```
switch# show ip igmp groups
```

IGMP group information for group 239.1.1.10

Interface Name : vlan2
VRF Name : default

Group Address : 239.1.1.10
Last Reporter : 100.1.1.10

Vers	Mode	Uptime	Expires	V1 Timer	V2 Timer	Sources Forwarded	Sources Blocked
3	EXC	0m 36s	3m 44s				

IGMP group information for group 239.1.1.11

Interface Name : vlan2
VRF Name : default

Group Address : 239.1.1.11
Last Reporter : 100.1.1.10

Vers	Mode	Uptime	Expires	V1 Timer	V2 Timer	Sources Forwarded	Sources Blocked
3	EXC	0m 36s	3m 44s				

Showing IGMP groups for all VRFs:

```
switch# show ip igmp groups all-vrfs
```

IGMP group information for group 239.1.1.1

Interface Name : vlan20
VRF Name : default

Group Address : 239.1.1.1
Last Reporter : 200.1.1.10

Vers	Mode	Uptime	Expires	V1 Timer	V2 Timer	Sources Forwarded	Sources Blocked
3	EXC	0m 13s	4m 7s				

IGMP group information for group 239.1.1.2

Interface Name : vlan20
VRF Name : default

Group Address : 239.1.1.2
Last Reporter : 200.1.1.10

Vers	Mode	Uptime	Expires	V1 Timer	V2 Timer	Sources Forwarded	Sources Blocked
3	EXC	0m 13s	4m 7s				

Showing IGMP groups for the default VRF:

```

switch# show ip igmp groups vrf default

IGMP group information for group 239.1.1.10

Interface Name      : vlan2
VRF Name            : default

Group Address       : 239.1.1.10
Last Reporter       : 100.1.1.10

Vers  Mode  Uptime      Expires    V1         V2         Sources    Sources
-----  -
3      EXC   9m 23s      3m 20s    Timer      Timer      Forwarded  Blocked

IGMP group information for group 239.1.1.11

Interface Name      : vlan2
VRF Name            : default

Group Address       : 239.1.1.11
Last Reporter       : 100.1.1.10

Vers  Mode  Uptime      Expires    V1         V2         Sources    Sources
-----  -
3      EXC   9m 23s      3m 20s    Timer      Timer      Forwarded  Blocked

IGMP group information for group 239.1.1.10

Interface Name      : vlan2
VRF Name            : default

Group Address       : 239.1.1.10
Last Reporter       : 100.1.1.10

Vers  Mode  Uptime      Expires    V1         V2         Sources    Sources
-----  -
3      EXC   9m 23s      3m 20s    Timer      Timer      Forwarded  Blocked

IGMP group information for group 239.1.1.11

Interface Name      : vlan2
VRF Name            : default

Group Address       : 239.1.1.11
Last Reporter       : 100.1.1.10

Vers  Mode  Uptime      Expires    V1         V2         Sources    Sources
-----  -
3      EXC   9m 23s      3m 20s    Timer      Timer      Forwarded  Blocked

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp interface

```
show ip igmp interface [{vlan <VLAN-ID>}]
counters
group <A.B.C.D> [{source <A.B.C.D>}]
groups
statistics
```

Description

Shows IGMP configuration information for a specific interface (VLAN).

Parameter	Description
vlan <VLAN-ID>	Specifies a VLAN. Values: 1-4094.

Examples

Showing IGMP configuration information for interface VLAN 2:

```
switch# show ip igmp interface vlan 2

IGMP Configured Version   : 3
IGMP Operating Version    : 3
Querier State             : Querier
Querier IP [this switch]  : 20.1.1.1
Querier Uptime            : 1m 46s
Querier Expiration Time   : 0m 1s
Snoop Enabled on VLAN     : True

switch# show ip igmp interface vlan 10

IGMP is not enabled
```

Showing IGMP configuration information for the specified interface 1/1/2:

```
switch# show ip igmp interface 1/1/2

IGMP Configured Version   : 3
IGMP Operating Version    : 3
Querier State             : Querier
Querier IP [this switch]  : 100.1.1.1
Querier Uptime            : 51m 44s
Querier Expiration Time   : 1m 51s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp interface counters

```
show ip igmp interface { vlan <VLAN-ID>} counters
```

Description

Shows IGMP counter details for a specific interface or VLAN interface.

Parameter	Description
vlan <VLAN-ID>	Specifies a VLAN. Values: 1-4094.

Examples

Showing IGMP counters for interface VLAN 2:

```
switch# show ip igmp interface vlan 2 counters

IGMP Counters

Interface Name      : vlan2
VRF Name            : default
Membership Timeout  : 0

                                Rx          Tx
                                -----
V1 All Hosts Queries      0          0
V2 All Hosts Queries      0          0
V3 All Hosts Queries      0         29
V2 Group Specific Queries  0          0
V3 Group Specific Queries  0          2
Group And Source Specific Queries  0          2
V3 Member Reports         0         N/A
V2 Member Reports         0         N/A
V1 Member Reports         0         N/A
V2 Member Leaves          0         N/A
Packets dropped by ACL    0         N/A
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp interface group

```
show ip igmp [interface { vlan <VLAN-ID>} [group <GROUP-IP> [source <SOURCE-IP>]]]
```

Description

Shows IGMP joined group information for a specific interface or VLAN interface, or specify a source IP.

Parameter	Description
vlan <VLAN-ID>	Specifies a VLAN. Values: 1-4094.
<GROUP-IP>	Specifies the IP address of the group. Format: A.B.C.D
source <SOURCE-IP>	Specifies the IP address of the source. Format: A.B.C.D

Examples

Showing IGMP joined group details for group 239.1.1.1 for interface VLAN 10:

```
switch# show ip igmp interface vlan 10 group 239.1.1.1

IGMP group information for group 239.1.1.1

Interface Name      : vlan10
VRF Name            : default

Group Address       : 239.1.1.1
Last Reporter       : 100.1.1.10

Vers  Mode  Uptime    Expires    V1          V2          Sources    Sources
-----  -
3      INC    8m 10s      2m 21s      Timer       Timer       Forwarded  Blocked

Group Address       : 239.1.1.1
Source Address      : 10.1.1.1

Mode  Uptime    Expire
----  -
INC   8m 10s      2m 21s
```

Showing IGMP joined group details for group 239.1.1.1 for interface VLAN 10 with source details for 10.1.1.1:

```
switch# show ip igmp interface vlan 10 group 239.1.1.1 source 10.1.1.1
```

```
Interface Name : vlan10
VRF Name      : default
Group Address  : 239.1.1.1
Source Address : 10.1.1.1
```

```
Mode Uptime      Expire
----
INC  8m 52s      3m 51s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp interface groups

```
show ip igmp [interface {vlan <VLAN-ID>} [groups]]
```

Description

Shows IGMP group information for a specific interface or VLAN interface.

Parameter	Description
vlan <VLAN-ID>	Specifies a VLAN. Values: 1-4094.
<GROUP-IP>	Specifies the IP address of the group. Format: A.B.C.D

Examples

Showing IGMP groups for interface VLAN 2:

```
switch# show ip igmp interface vlan 2 groups

IGMP group information for group 239.1.1.1

Interface Name      : vlan2
VRF Name            : default

Group Address       : 239.1.1.1
Last Reporter       : 100.1.1.10

Vers Mode Uptime      Expires      V1          V2          Sources    Sources
----  ---  -
Timer Timer          Forwarded Blocked
```

```

3      INC  4m 40s      3m 51s      1

Group Address   : 239.1.1.1
Source Address  : 10.1.1.1

Mode Uptime      Expire
-----
INC  4m 40s      3m 51s

IGMP group information for group 239.1.1.2

Interface Name   : vlan2
VRF Name         : default

Group Address    : 239.1.1.2
Last Reporter    : 100.1.1.10

Vers Mode Uptime      Expires      V1      V2      Sources      Sources
-----
3      INC  4m 40s      3m 51s      Timer      Timer      Forwarded      Blocked
-----
3      INC  4m 40s      3m 51s      1

Group Address   : 239.1.1.2
Source Address  : 10.1.1.1

Mode Uptime      Expire
-----
INC  4m 40s      3m 51s

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp interface statistics

show ip igmp interface { vlan <VLAN-ID>} statistics

Description

Shows IGMP statistics for a specific interface or VLAN interface, including groups joined.

Parameter	Description
vlan <VLAN-ID>	Specifies a VLAN. Values: 1-4094.

Examples

Showing IGMP statistics for interface VLAN 2:

```
switch# show ip igmp interface vlan 2 statistics

IGMP statistics

Interface Name : vlan2
VRF Name       : default

Number of Include Groups      : 2
Number of Exclude Groups     : 0
Number of Static Groups      : 0
Total Multicast Groups Joined : 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp static-groups

```
show ip igmp static-groups [all-vrfs]
```

Description

Shows IGMP static groups, or shows information by VRF.

Parameter	Description
all-vrfs	Specify all-vrfs to show information for all VRFs.

Examples

Showing IGMP static-group information:

```
switch# show ip igmp static-groups

IGMP Static Group Address Information

VRF Name      default
Interface Name Group Address
-----
vlan10        238.1.1.1
```

Showing IGMP statics-group information for all VRFs:

```
switch# show ip igmp static-groups all-vrfs
```

IGMP Static Group Address Information

```
VRF Name      :default
Interface Name  Group Address
-----
vlan10         238.1.1.1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp statistics

```
show ip igmp statistics [all-vrfs]
```

Description

Shows IGMP statistics, including groups joined, or shows statistics by VRF.

Parameter	Description
all-vrfs	Specify all-vrfs to show information for all VRFs.

Examples

Showing IGMP statistics:

```
switch# show ip igmp statistics
IGMP statistics

VRF Name      : default

Number of Include Groups      : 1
Number of Exclude Groups     : 0
Number of Static Groups      : 0
Total Multicast Groups Joined : 1
```

Showing IGMP statistics for all VRFs:

```
switch# show ip igmp statistics all-vrfs
IGMP statistics

VRF Name          : default

Number of Include Groups      : 1
Number of Exclude Groups     : 0
Number of Static Groups      : 0
Total Multicast Groups Joined : 1
```

Command History

Release	Modification
10.07 or earlier	--

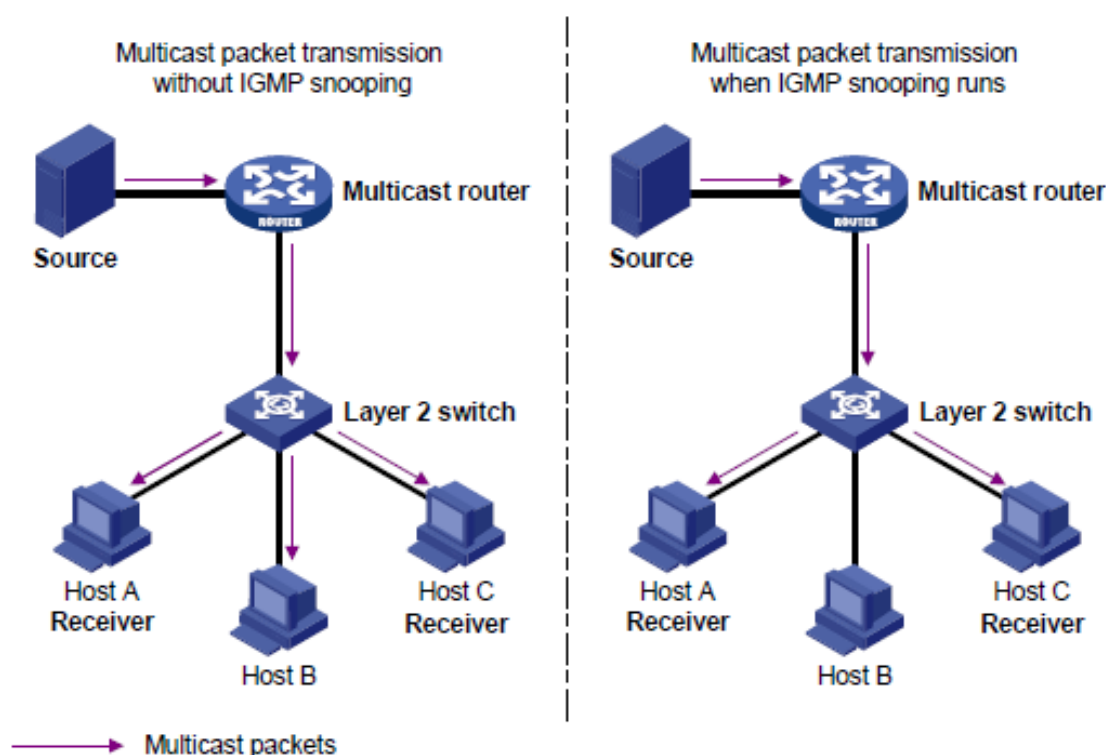
Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

IGMP snooping

IGMP snooping runs on a Layer 2 device as a multicast constraining mechanism to improve multicast forwarding efficiency. It creates Layer 2 multicast forwarding entries from IGMP packets that are exchanged between the hosts and the router.

When IGMP snooping is not enabled, the snooping switch floods multicast packets to all hosts in a VLAN. IGMP L2 snooping switch provides the benefit of conserving bandwidth on those segments of the network where no node has expressed interest in receiving packets addressed to the group address. When IGMP snooping is enabled, the L2 snooping switch forwards multicast packets of known multicast groups to only the receivers.



IGMP snooping defaults, protocols, and supported configuration

IGMP snooping default configuration

- IGMP snooping is disabled by default and has to be enabled on all applicable VLANs.
- Version 3 is used by default.

IGMP snooping related protocols

- IGMPv2 (RFC 2236)
- IGMPv3 (RFC 3376)

- Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches (RFC 4541)

Static groups

You can configure a maximum of 32 IGMP snooping static groups.

How IGMP snooping works

IGMP message types include: Query, Report (Join), and Leave Group. An IGMP snooping enabled Layer 2 device performs differently depending on the message type.

Query

A message sent from the querier (multicast router or switch) asking for a response from each host belonging to the multicast group. If a multicast router supporting IGMP is not present, then the switch must assume this function in order to elicit group membership information from the hosts on the network.

The IGMP querier periodically sends IGMP general queries to all hosts and routers on the local subnet to check for the existence of multicast group members. After receiving an IGMP general query, the snooping switch forwards the query to all ports in the VLAN except the receiving port.

Report (Join)

A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.

A host sends an IGMP report to the IGMP querier for the following purposes:

- Responds to queries if the host is a multicast group member.
- Applies for a multicast group membership.

After receiving an IGMP report from a host, the snooping switch forwards the report through all the router ports in the VLAN. It also looks up the forwarding table for a matching entry as follows:

- If no match is found, the snooping switch creates a forwarding entry with the receiving port as an outgoing interface. It also starts group membership expiry timer for the port to track the amount of time that must pass before a multicast router decides there are no more members of a group on a network.
- If a match is found but the matching forwarding entry does not contain the receiving port, the snooping switch adds the receiving port to the outgoing interface list. It also starts group membership expiry timer for the port.
- If a match is found and the matching forwarding entry contains the receiving port, the snooping switch restarts the group membership expiry timer for the port.

Leave Group

A message sent by a host to the querier to indicate that the host has ceased to be a member of a specific multicast group.

An IGMPv1 receiver host does not send any leave messages when it leaves a multicast group. The snooping switch cannot immediately update the status of the port that connects to the receiver host. The snooping switch does not remove the port from the outgoing interface list in the associated forwarding entry until the group membership timer expires.

An IGMPv2 or IGMPv3 host sends an IGMP leave message when it leaves a multicast group. Upon receiving leave message, the switch forwards the IGMP leave message to all router ports in the VLAN .

IGMP querier then sends an IGMP group-specific query to the multicast group to identify whether the group has active receivers attached to the receiving port.

After receiving the IGMP group-specific query, the switch forwards the query through all router ports and member ports of the group in the VLAN. Then, it waits for the responding IGMP report message from the directly connected hosts. If the port does not receive an IGMP report message when the group membership timer expires, the snooping switch removes the port from the forwarding entry for the multicast group.

IGMP snooping configuration task list

- [Enabling or Disabling IGMP Snooping](#)
- [Specifying the IGMP snooping version](#)
- [Configuring IGMP snooping static groups](#)
- [Enabling Drop-Unknown Filters](#)
- [Configuring IGMP snooping fast learn ports globally](#)
- [Configuring IGMP snooping per port filtering](#)
- [Disabling IGMP Snooping](#)
- [Viewing IGMP snooping information](#)

Enabling or disabling IGMP snooping

IGMP snooping is disabled by default. The default behavior is to flood multicast traffic in the VLAN. Use the following to enable IGMP snooping.

Prerequisites

You must be in the VLAN configuration context, as indicated by the **switch(config-vlan)#** prompt. The VLAN has to be configured and up.

Procedure

Enable IGMP snooping on a VLAN using the following command.

```
ip igmp snooping {enable | disable}
```

For example, the following command enables IGMP snooping on VLAN 2:

```
switch(config)# vlan 2  
switch(config-vlan)#
```

Use the **no** command to disable IGMP snooping on a VLAN.

Specifying the IGMP snooping version

The IGMP snooping version can be either 2 (IGMPv2) or 3 (IGMPv3). The default is 3. IGMPv2 supports filtering based on groups. IGMPv3 is more advanced and includes filtering based on source and groups.

Prerequisites

You must be in the VLAN configuration context, as indicated by the **switch(config-vlan)#** prompt.

Procedure

Specify the IGMP snooping version for a VLAN using the following command.

```
ip igmp snooping version <VERSION>
```

For example, the following command sets the IGMP snooping version to 2 on VLAN 2:

```
switch(config)# vlan 2  
switch(config-vlan)# ip igmp snooping version 2
```

Configuring IGMP snooping static groups

Configure IGMP snooping static groups.

Prerequisites

You must be in the VLAN configuration context, as indicated by the **switch(config-vlan)#** prompt.

Procedure

Configure an IGMP snooping static group on a VLAN using the following command.

```
ip igmp snooping static-group <MULTICAST-IP-ADDRESS>
```

For example, the following command configures the IGMP snooping static multicast group as 239.1.1.1 on VLAN 2:

```
switch(config)# vlan 2  
switch(config-vlan)# ip igmp snooping static-group 239.1.1.1
```

The **no** form of the command removes the IGMP snooping static group.

Enabling drop-unknown filters

While IGMP snooping is enabled, the traffic will be forwarded only to joined ports. Configuring drop unknown filters, ensures that packets are not forwarded to ports where a request for the traffic stream has not been received.

This could either be a filter across all VLANs (**vlan-shared**) or per VLAN (**vlan-exclusive**). The default is **vlan-shared**.

Prerequisites

You must be in the configuration context, as indicated by the **switch(config)#** prompt.

Procedure

Globally enable dropping multicast data using the following command.

```
ip igmp snooping drop-unknown {vlan-shared | vlan-exclusive}
```

For example, the following command configures a shared VLAN filter on the switch:

```
switch(config)# ip igmp snooping drop-unknown vlan-shared
```

Configuring IGMP snooping fast learn ports globally

Configuring fast learn on a port enables faster response to topology change notifications. When spanning tree changes the port state from blocked to forwarding, the device acting as querier will immediately send a general query on the fast learn enabled port. Then the device acting as a non-querier will replay the joins. This will help in faster convergence of multicast flows.

Prerequisites

You must be in the configuration context, as indicated by the **switch(config)#** prompt.

Procedure

Configure one or more ports as IGMP snooping fast learn ports using the following command.

```
ip igmp snooping fastlearn <PORT-LIST>
```

For example, the following command configures ports 1/1/1-1/1/3 as fast learn ports:

```
switch(config)# ip igmp snooping fastlearn 1/1/1-1/1/3
```

Configuring IGMP snooping per port filtering

Configure IGMP snooping traffic handling by specifying auto, blocked, or forward for a port, list of ports or range of ports. In auto mode traffic flow is controlled by the IGMP joins/leaves. Auto mode is the default. In blocked mode, joins and traffic are always blocked on this port. In forward mode traffic is always forwarded on this port, irrespective of joins.

Prerequisites

You must be in the VLAN configuration context, as indicated by the **switch(config-vlan)#** prompt.

Procedure

Configure IGMP snooping traffic handling for ports on a VLAN using the following commands.

- Configure the specified ports in auto mode using the following command: **ip igmp snooping auto <PORT-LIST>**.
- Configure the specified ports in blocked mode using the following command: **ip igmp snooping blocked <PORT-LIST>**.
- Configure the specified ports in forward mode using the following command: **ip igmp snooping forward <PORT-LIST>**.

For example, the following command configures ports 1/1/1, 1/1/2, and 1/1/3 in auto mode for VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping auto 1/1/1,1/1/2-1/1/3
```

Disabling IGMP snooping

Prerequisites

You must be in the VLAN configuration context, as indicated by the **switch(config-vlan)#** prompt.

Procedure

Disable IGMP snooping on a VLAN using the following command.

```
no ip igmp snooping
```

For example, the following command removes IGMP snooping on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# no ip igmp snooping
```



Viewing IGMP snooping information

Prerequisites

Use these show commands from the Operator (>) or Manager (#) context.

Procedure

To view IGMP snooping information, use the following commands.

- To view IGMP snooping configuration details and status, use: **show ip igmp snooping**.
- To view IGMP snooping query packet Tx, Rx, and Error packet counter details, use: **show ip igmp snooping counters**.
- To view IGMP snooping group information, use: **show ip igmp snooping groups**.
- To view IGMP snooping protocol information and the number of groups joined, use: **show ip igmp snooping statistics**.
- To view IGMP snooping query packet Tx, Rx, and Error packet counters for the specified VLAN, use: **show ip igmp snooping vlan counters**.
- To view IGMP snooping statistics details for the specified VLAN including the number of different groups joined for the VLAN, use: **show ip igmp snooping vlan statistics**.
- To view IGMP snooping group information for the specified VLAN, use: **show ip igmp snooping vlan**.
- To view IGMP snooping group details for the specified VLAN including information about all IGMP snooping groups or sources learned on a particular port, use: **show ip igmp snooping vlan group port**.
- To view IGMP snooping static groups details for the specified VLAN, use: **show ip igmp snooping static-groups**.

IGMP snooping commands

ip igmp snooping apply access list

```
ip igmp snooping apply access list <ACL-NAME>
no ip igmp snooping apply access list <ACL-NAME>
```

Description

Configures the access list (ACL) in a particular interface to filter IGMP join or leave packets based on rules set in a particular access list name. The **no** form of this command removes the configuration.

Parameter	Description
<ACL-NAME>	Specifies the access list name.

Usage

Existing classifier commands are used to configure ACL. In case of IGMPv3 packets with multiple group addresses received, only permitted group addresses based on the ACL rule set are processed. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by ACL to avoid the delay in learning of the permitted groups because the access switch

configured with the ACL blocks the traffic for the groups which are denied forwarding of joins have no impact. If all of the groups in a packet are denied by the ACL rule packet, it is not forwarded to the querier and PIM router. If the ACE has the source address configured, the source address in the IGMPv3 report is matched against the ACL and corresponding action is taken. Existing joins timeout. With IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.



If the access list is configured for both L2 VLAN and L3 VLAN, then the L3 VLAN configuration is applied.

Example

Configure the access list:

```
switch(config)# vlan 2
switch(config-vlan-2)# ip igmp snooping apply access-list mygroup
```

Remove the access list:

```
switch(config)# vlan 2
switch(config-vlan-2)# no ip igmp snooping apply access-list mygroup
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
All platform	config-vlan	Administrators or local user group members with execution rights for this command.

ip igmp snooping (config mode)

```
ip igmp snooping
drop-unknown vlan-shared|vlan-exclusive
fastlearn <PORT-LIST>
```

Description

Configures drop-unknown and fastlearn modes on the ports. While IGMP snooping is enabled, the traffic will be forwarded only to ports that made an IGMP request for the multicast. Drop unknown filters ensure that packets are not forwarded to ports that did not make a request for the traffic stream. This could either be a filter across all VLANs (**vlan-shared**) or per VLAN (**vlan-exclusive**). The default is **vlan-shared**. Fast learn enables the port to learn group information when receiving a topology change notification. By default, fast learn is not enabled on ports.

Parameter	Description
drop-unknown	Drop unknown filters ensure that packets are not forwarded to

Parameter	Description
	ports that did not make a request for the traffic stream.
vlan-shared	Enables a shared VLAN filter on the switch. Default is vlan-shared .
vlan-exclusive	Enables an exclusive drop unknown filter per VLAN.
fastlearn <PORT-LIST>	Enable fast learn on ports. This parameter specifies a list of one or more ports to be configured as fast learn ports. You can specify a single port, a comma-separated list of ports or a range of ports such as 1/1/1-1/1/3. You may also enter an L2 LAG (1-128)
no ...	Negates any configured parameter.

Example

Configuring fast learn ports:

```
switch(config)# ip igmp snooping fastlearn 1/1/3
switch(config)# ip igmp snooping fastlearn 1/1/1-1/1/2
switch(config)# ip igmp snooping fastlearn 1/1/5,1/1/6
```

Configuring a shared VLAN filter on the switch:

```
switch(config)# ip igmp snooping drop-unknown vlan-shared
```

Configuring a exclusive drop unknown filter per VLAN:

```
switch(config)# ip igmp snooping drop-unknown vlan-exclusive
```

Disabling drop unknown on the switch:

```
switch(config)# no ip igmp snooping drop-unknown
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ip igmp snooping (interface mode)

```
ip igmp snooping
auto vlan <VLAN-LIST>
```

```

blocked vlan <VLAN-LIST>
fastleave vlan <VLAN-LIST>
forced-fastleave vlan <VLAN-LIST>
forward vlan <VLAN-LIST>
no ...

```

Description

Configure IP IGMP snooping for the VLAN on the interface. When IGMP snooping is enabled, the L2 snooping switch forwards multicast packets of known multicast groups to only the receivers. When IGMP snooping is not enabled, the snooping switch floods multicast packets to all hosts on the VLAN.

Parameter	Description
<code>auto vlan <VLAN-LIST></code>	Instruct the device to monitor incoming multicast traffic on the specified ports on a VLAN or VLAN range. This is the default behavior. Enter the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).
<code>blocked vlan <VLAN-LIST></code>	Configures the specified ports in blocked mode for the specified VLAN list. In blocked mode, joins and traffic are always blocked on this port. Enter the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).
<code>fastleave vlan <VLAN-LIST></code>	IGMP fastleave is configured for ports on a per-VLAN basis. Upon receiving a Leave Group message, the querier sends an IGMP Group-Specific Query message out of the interface to ensure that no other receivers are connected to the interface. If receivers are directly attached to the switch, it is inefficient to send the membership query as the receiver wanting to leave is the only connected host. When a fastleave-enabled switch port is connected to a single host and receives a leave, the switch does not wait for the querier status update interval, but instead immediately removes the IGMP client from its IGMP table and ceases transmitting multicast traffic to the client. (If the switch detects multiple end nodes on the port, Fastleave does not activate regardless of whether one or more of these end nodes are IGMP clients.) This processing speeds up the overall leave process and also eliminates the CPU overhead of having to generate an IGMP Group-Specific Query message. This parameter specifies a list of VLANs on which the port should be configured as a fastleave port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).
<code>forced-fastleave vlan <VLAN-LIST></code>	With forced fastleave enabled, IGMP speeds up the process of blocking unnecessary multicast traffic to a switch port that is connected to multiple end nodes. When a port having multiple end nodes receives a leave group request from one end node for a given multicast group, forced fastleave activates and waits for a second to receive a join request from any other member of the same group on that port. If the port does not receive a join request for that group within the forced fastleave interval, the switch then blocks any further traffic to that group on that port. This parameter specifies a list of VLANs on which the port should be configured as a forced fastleave port. Specifies the

Parameter	Description
	number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60). This command is available in config-if mode.
<code>forward vlan <VLAN-LIST></code>	Configures the specified ports in forward mode in the given VLAN list. In forward mode, traffic is always forwarded on this port, irrespective of joins. Specify a list of VLANs on which the port should be configured as a forward port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60). This command is available in config-if mode.
<code>no ...</code>	Negates any configured parameter.

Example

Configure auto ports for VLAN on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-if)# no shut
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 10-20
switch(config-if)# ip igmp snooping auto vlan 10
switch(config-if)# ip igmp snooping auto vlan 10-20
```

Configuring fastleave ports for the VLAN on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-if)# no shut
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 10-20
switch(config-if)# ip igmp snooping fastleave vlan 10
switch(config-if)# ip igmp snooping fastleave vlan 10-20
```

Configuring blocked ports for the VLAN on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-if)# no shut
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 10-20
switch(config-if)# ip igmp snooping blocked vlan 10
switch(config-if)# ip igmp snooping blocked vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	config-if	Administrators or local user group members with execution rights for this command.

ip igmp snooping (vlan mode)

```
ip igmp snooping
  apply access-list <ACL-NAME>
  enable|disable
  no ...
  static-group <MULTICAST-IP-ADDRESS>
  version <2-3> (vlan interface mode)
```

Description

These commands enable or disable IP IGMP snooping on the VLAN, create IGMP snooping static multicast groups, set the IGMP snooping version and configure the ACL on a particular interface.



Disabling and enabling IGMP snooping on a VLAN causes IGMP querier re-election.

Parameter	Description
access-list	Associates an ACL with the IGMP.
enable disable	Enables or disables IGMP snooping on the VLAN. Starting with AOS-CX 10.16, IGMP snooping is enabled by default.
no ...	Negates any configured parameter.
static-group <MULTICAST-IP-ADDRESS>	This parameter configures an IGMP snooping static multicast group. Specify the IGMP static multicast group IP address in A.B.C.D format. You can configure a maximum of 32 IGMP snooping static
version <2-3>	Configures the IGMP snooping version on the VLAN. Select 2 for IGMPv2 (RFC2236). Select 3 for IGMPv3 (RFC3376).

Usage

- Existing classifier commands are used to configure the ACL.
- In case an IGMPv3 packet with multiple group addresses is received, the switch only processes the permitted group addresses based on the ACL rule set. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by the ACL. This avoids the delay in learning of the permitted groups. Since the access switch configured with ACL blocks the traffic for the groups which are denied, forwarding of joins has no impact. If all the groups in the packet are denied by the ACL rule, the packet is not forwarded to the querier and PIM router. Existing joins will timeout.
- In case of IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.



If the access list is configured for both L2 VLAN and L3 VLAN, the L3 VLAN configuration will be applied.

Example

Disable IGMP snooping on a VLAN:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping disable
```

Reenable IGMP snooping on a VLAN:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping enable
```

Configuring an IGMP snooping static group:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping static-group 239.1.1.1
switch(config-vlan)# no ip igmp snooping static-group 239.1.1.1
```

Configuring IGMP snooping version on the VLAN:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping version 2
```

Command History

Release	Modification
10.16	Starting with this release, IGMP snooping is enabled on VLANs by default, including the Management VLAN (vlan 1) and VLANs with a associated VNI.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-vlan-<VLAN-ID>	Administrators or local user group members with execution rights for this command.

ip igmp snooping filter unknown mcast

```
ip igmp snooping filter-unknown-mcast
no ip igmp snooping filter-unknown-mcast
```

Description

Enables the avoidance of initial flooding of unknown multicast traffic on IGMP-snooping-enabled VLANs. The no form of this command returns to the default behavior of initial flooding of unknown multicast traffic.

Usage

In the default behavior, the unknown multicast traffic is flooded until the IP Multicast Flow programming is done on the hardware. This is known as initial flooding of unknown multicast. Use this command to filter unknown multicast instead of flooding.



Initial flooding of multicast traffic is observed for a few seconds after the device comes up from a reboot. This issue is only seen when the multicast source connected device is rebooted. Once the device is up after a reboot, it takes a few seconds for the CPU Rx rule to be programmed during the timeframe that the initial flooding is observed. This is an expected behavior.

Example

Configure the unknown multicast to steal globally on IGMP snooping enabled VLANs.

```
switch# configure terminal
switch(config)# ip igmp snooping filter-unknown-mcast
```

Removing the configuration of the unknown multicast to steal globally on IGMP snooping enabled VLANs.

```
switch# configure terminal
switch(config)# no ip igmp snooping filter-unknown-mcast
```

Command History

Release	Modification
10.14	Command introduced on the 4100i, 6000, and 6100 Switch series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	config	Administrators or local user group members with execution rights for this command.

ip igmp snooping preprogram-starg-flow

```
ip igmp snooping preprogram-starg-flow {enable | disable}
```

Description

Configures preprogramming of the starg flow feature on the IGMP snooping enabled VLAN.

Parameter	Description
enable	Enables preprogramming starg flows on the VLAN.
disable	Disables preprogramming starg flows on the VLAN.

Usage

When this feature is enabled, a summarized multicast bridge entry is programmed into the hardware table when an IGMPv2 or IGMPv3 join is received on the IGMP snooping enabled VLAN. This enables multicast flow to be programmed in the hardware before the data packet arrives for a multicast flow. If an unknown packet is received for a multicast flow, having this feature enabled triggers programming of starg entry in the hardware on selected platforms, which is helpful in optimizing hardware resource utilization and PIM registration in deployments where a L2 device is connected along the PIM registration path.

This feature is currently supported for IGMPv2 and IGMPv3 joins, so IGMPv3 joins that are sent for a specific source are treated as IGMPv2 joins and summarized entry is programmed in the corresponding hardware.

Preprogramming of starg flows is supported only on the IGMP snooping enabled VLANs. If IGMP snooping is disabled on a VLAN, this feature is auto-disabled.

This feature is currently supported for IGMPv2 and IGMPv3 joins, as a result, summarized multicast flow is programmed in advance when an IGMPv2 join or IGMPv3 join for a specific group is received. For IGMPv3 deployments, traffic from all sources for a specific multicast group is sent to all clients, regardless of whether they send IGMPv2 or IGMPv3 joins for this group. Keeping this feature disabled is recommended on VLANs where traffic from the specific source is only expected for the IGMPv3 clients.

On the HPE Aruba Networking 4100i, 6000, and 6100 Switch series, a single starg entry is programmed in advance for each join received and data driven programming of SG entries occurs when the traffic is received from a specific source for this group. As a result, the starg entry is used to forward the initial traffic and the SG entries programmed in the multicast forwarding table are used to forward subsequent traffic to all of the clients (that have sent either IGMPv2 joins or IGMPv3 joins) for all of the active joins in the feature enabled VLANs.

When an unknown multicast packet is received on a VLAN where this feature is enabled, it triggers programming of a starg entry in the hardware instead of the SG.

It is highly recommended to not enable this feature on devices where PIM or L3 multicast routing is enabled as it can lead to issues like permanent traffic loss.

Configuring this feature on devices where there are multiple sources sending traffic for the same group address is recommended.

This feature is mutually exclusive with the IGMP snooping static group feature.

Example

Enable preprogramming multicast starg flows:

```
switch(config)# vlan 2
switch(config-vlan-2)# ip igmp snooping preprogram-starg-flow enable
```

Disable preprogramming multicast starg flows:

```
switch(config)# vlan 2
switch(config-vlan-2)# ip igmp snooping preprogram-starg-flow disable
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	config-vlan	Administrators or local user group members with execution rights for this command.

ip igmp snooping querier-address

```
ip igmp snooping querier-address <QUERIER-IP-ADDRESS>  
no ip igmp snooping querier-address <QUERIER-IP-ADDRESS>
```

Description

Configures the querier IP address for the IGMP-MLD proxy feature in EVPN.

The **no** form of this command removes the configuration.

Parameter	Description
<QUERIER-IP-ADDRESS>	Specifies the proxy querier IP address.

Usage

Fabrics running the IGMP-MLD Proxy feature must perform distributed querier functionality on every VTEP where the VLAN is extended. Typically, a valid IP address must be configured on the SVI for IGMP querier functionality. However, in centralized routing scenarios within the fabric, most VTEPs only have Layer 2 VLANs. In such cases, IGMP querier functionality needs to be enabled on those VTEPs. This configuration provides a valid querier IP address for those Layer 2 VLANs.

This command is used in conjunction with the IGMP-MLD proxy feature of EVPN.



This is an optional command applicable to VTEPs that have Layer 2 VLANs (without an IP address) and requires IGMP-MLD proxy querier functionality.

If a Layer 3 SVI with an IP address is configured for the VLAN, it takes precedence. In the absence of a valid IP address or SVI, the given IP address is used for querier operations. This configuration is global and applies to all tenants' Layer 2 VLANs where the IGMP-MLD proxy feature is enabled. Fabrics running the **igmp-mlt proxy** feature must perform distributed querier functionality on every VTEP where the VLAN is extended. Typically, a valid IP address must be configured on the SVI for IGMP querier functionality needs to be enabled on those VTEPs. This configuration provides a valid querier IP address for those Layer 2 VLANs. This configuration is applicable only when **igmp-mlt-proxy** configuration is configured under EVPN.

In the event of underlay tunnel fluctuations, the querier state reinitializes and transitions back to the querier state only after the default querier wait of 260 seconds.

This configuration is not applicable to VLANs that are not mapped to a VNI.



The specified IP address does not need to be assigned to any interface.

Example

Configure the querier IP address for the IGMP-MLD proxy feature in EVPN.

```
switch(config)# ip igmp snooping querier-address 10.10.10.1
```

Remove the configuration of the querier IP address for the IGMP-MLD proxy feature in EVPN:

```
switch(config)# no ip igmp snooping querier-address 10.10.10.1
```

Command History

Release	Modification
10.16	Command introduced.

Command Information

Platforms	Command context	Authority
All platform	config	Administrators or local user group members with execution rights for this command.

ip igmp snooping static group

```
ip igmp snooping static group <GROUP-NAME>  
no ip igmp snooping static group <GROUP-NAME>
```

Description

Configures static multicast group. The **no** form of this command removes the configuration.

Parameter	Description
<GROUP-NAME>	Specifies the group name.

Example

Configure static multicast group on group 239.1.1.1:

```
switch(config)# vlan 2  
switch(config-vlan-2)# ip igmp snooping static-group 239.1.1.1
```

Remove static multicast group on group 239.1.1.1:

```
switch(config)# vlan 2  
switch(config-vlan-2)# no ip igmp snooping static-group 239.1.1.1
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config-vlan	Administrators or local user group members with execution rights for this command.

show ip igmp snooping

```
show ip igmp snooping
  counters
  detail
  groups [vlan <vlan-id>]
  no ...
  packet-exceptions
  static-groups
  statistics
  vlan <vlan-id> [group {<ip-addr> [client_details]}|{port <IF-NAME>}|{vtep-peer
<A.B.C.D>}]
  vsx-peer
```

Description

Shows IGMP snooping configuration information and status for all VLANs. Specify a VLAN ID or a VLAN and a group to display details for only that VLAN or VLAN group.

Parameter	Description
counters	Shows IGMP query packets transmitted (Tx), received (Rx), and error packet counters.
detail	Shows IGMP Snooping details for all VLANs, including joined ports or VXLAN tunnel endpoints (VTEPs) for each group in the VLAN.
groups	Shows IGMP snooping groups information. Include the optional vlan <vlan-id> parameter to display information for groups on a specific VLAN.
no ...	Negates any configured parameter.
packet-exceptions	Troubleshoot issues in L2 multicast bridge entries for data packets forwarded to the CPU.
static-groups	Shows MLD snooping static group details, including the number of static groups joined.
statistics	Shows MLD snooping statistics.
vlan <vlan-id>	Shows IGMP snooping protocol information and number of different groups joined for the VLAN.
group	Shows IGMP snooping group information for the specified VLAN, including the number of different groups joined for the VLAN. Identify the group by IP address or interface name.
<ip-addr> [client-details]	Shows IGMP snooping group address information. Include the optional client details parameter to display IGMP snooping client details.
port <IF-NAME>	Shows IGMP snooping group information for the interface name in member/slot/port format.

Parameter	Description
vtep-peer <A.B.C.D>	Shows IGMP snooping info for the specified VTEP.

Examples

Showing IGMP snooping configuration and status:

```
switch# show ip igmp snooping

IGMP Snooping Protocol Info

Total VLANs with IGMP enabled           : 1
IGMP Drop Unknown Multicast             : Global
Configured IGMP Proxy Querier address   :10.10.10.1

VLAN ID : 1
VLAN Name : DEFAULT_VLAN_1
IGMP Snooping is not enabled

VLAN ID : 2
VLAN Name : VLAN2
IGMP Configured Version : 3
IGMP Operating Version : 3
IGMP preprogram-starg-flow is operational
Querier Address [this switch] : 20.1.1.1
Querier Port :
Querier UpTime :0m 21s
Querier Expiration Time :0m 2s
```

Include the **detail** parameter for additional information on joined ports or VTEPs, as shown in the example below:

```
switch# show ip igmp snooping detail

IGMP Snooping Protocol Info

Total VLANs with IGMP enabled           : 1
Current count of multicast groups joined : 4

IGMP Drop Unknown Multicast             : Global
VLAN ID : 100
VLAN Name : VLAN100
IGMP Configured Version : 3
IGMP Operating Version : 3
IGMP preprogram-starg-flow is not operational
Querier Address [this switch] : 15.1.1.1
Querier Port :
Querier UpTime :9m 32s
Querier Expiration Time :0m 10s
Router Detected Port(s) :

Active Group Address   Tracking   Vers  Mode  Uptime   Expires   Ports/Vteps
-----
225.1.1.1              Filter    3     EXC   1m 2s    0s
200.1.1.1,200.1.1.2

1/6/22
```

225.1.1.2	Filter	3	EXC	1m 2s	0s	
200.1.1.1, 200.1.1.2						1/6/22
226.1.1.1	Filter	3	EXC	1m 4s	0s	200.1.1.3
226.1.1.2	Filter	3	EXC	1m 4s	0s	200.1.1.3



With standard based IGMP-MLD Proxy mode, the membership reports from remote VTEPs does not have an expiry timer associated and shall be shown as 0 seconds.

Command History

Release	Modification
10.16	Updated example to include new IGMP proxy querier address.
10.13	Programming starg flow is now supported.
10.10	The packet-exceptions parameter is introduced.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

MLD snooping

Multicast Listener Discovery (MLD) snooping optimizes multicast traffic across the network to prevent traffic from flooding ports on a VLAN.

- For example, one of the features of MLD snooping lets you configure the network so that traffic is forwarded only to ports that initiate an MLD request for multicast.
- Another feature of MLD lets you enable a setting so that packets that do not match the configured version are dropped.
- You can also block ports from traffic.



MLD snooping is disabled by default and has to be enabled on all applicable VLANs.

Disabling and enabling IPv6 MLD snooping on a VLAN causes MLD querier reelection.



The 6000 and 6100 Switch series does not support router port detection via PIM control packets. As a result, IGMP reports are not forwarded to router ports learned through PIM. However, IGMP/MLD Querier port learning is fully supported on this platform and the device learns querier ports and forwards IGMP/MLD control packets to them as expected. This ensures proper multicast group management and protocol operation.

MLD snooping global configuration commands

ipv6 mld snooping

```
ipv6 mld snooping drop-unknown {vlan-shared | vlan-exclusive}
no ipv6 mld snooping drop-unknown {vlan-shared | vlan-exclusive}
```

Description

This command configures the drop unknown mode. While MLD snooping is enabled, the traffic will be forwarded only to ports that initiate an MLD request for multicast. Drop unknown mode can be a filter across all VLANs (vlan-shared) or per VLAN (exclusive-vlan). The default configuration is vlan-shared.

The **no** form of this command configures the drop unknown mode on the switch to the default **vlan-shared**.

Parameter	Description
vlan-shared	Required: Enable shared VLAN filter on the switch.
vlan-exclusive	Required: Enable exclusive drop unknown filter per VLAN.

Example

```
switch(config)# ipv6 mld snooping drop-unknown vlan-shared
switch(config)# ipv6 mld snooping drop-unknown vlan-exclusive
switch(config)# no ipv6 mld snooping drop-unknown
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config	Administrators or local user group members with execution rights for this command.

MLD snooping VLAN configuration commands

ipv6 mld snooping (vlan)

```
ipv6 mld snooping {enable | disable}
no ipv6 mld snooping [enable | disable]
```

Description

This command disables or reenables MLD snooping on the VLAN. Starting with AOS-CX 10.16, MLD snooping is enabled by default.

The **no** form of this command disables all MLD snooping configurations on the VLAN.

Parameter	Description
enable	Reenable MLD snooping on the VLAN.
disable	Disable MLD snooping on the VLAN.

Example

Disable and then reenables MLD snooping on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping disable
switch(config-vlan)# ipv6 mld snooping enable
```

Remove all MLD snooping configurations on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# no ipv6 mld snooping enable
```

Command History

Release	Modification
10.16	Starting with this release, MLD snooping is enabled on VLANs by default, including the Management VLAN (vlan 1) and VLANs with a associated VNI.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan-<VLAN-ID>	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping apply access-list

```
ipv6 mld snooping apply access-list <ACL-NAME>
no ipv6 mld snooping apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the MLD join or leave packets based on rules set in the particular ACL name.

The **no** form of this command disables the rules set for the ACL.



This configuration will override the ACL associated with IGMP snooping on the corresponding L2 VLAN.

Parameter	Description
access-list	Associates an ACL with the IGMP.
<ACL-NAME>	Specifies the name of the ACL. NOTE: If the access list is configured for both L2 VLAN and L3 VLAN, the L3 VLAN configuration will be applied.

Usage

- Existing classifier commands are used to configure the ACL.
- In case an IGMPv3 packet with multiple group addresses is received, the switch only processes the permitted group addresses based on the ACL rule set. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by ACL. This avoids the delay in learning of the permitted groups. Since the access switch configured with ACL blocks the traffic for the groups which are denied, forwarding of joins has no impact. If all the groups in the packet are denied by the ACL rule, the packet is not forwarded to the querier and PIM router. Existing joins will timeout.
- In case of IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.

Examples

Configuring the ACL to filter MLD packets based on permit/deny rules set in access list **mygroup**:

```
switch(config)# access-list ipv6 mygroup
switch(config-acl-ip)# 10 deny icmpv6 any ff55::2
switch(config-acl-ip)# 20 deny icmpv6 any ff55::3
switch(config-acl-ip)# 30 permit icmpv6 any ff55::1
switch(config-acl-ip)# exit
switch(config)# interface vlan 2
switch(config-vlan)# ipv6 mld snooping apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list **mygroup**:

```
switch(config-vlan)# no ipv6 mld snooping apply access-list mygroup
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping auto vlan

```
ipv6 mld snooping [auto vlan <VLAN-LIST>]
no ipv6 mld snooping [auto vlan <VLAN-LIST>]
```

Description

This command configures the given ports in auto mode, which is the default port mode. The **no** form of this command disables auto ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as an auto port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Example

Configuring auto ports for VLANs on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
```

```
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping auto vlan 10
switch(config-vlan)# ipv6 mld snooping auto vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping blocked vlan

```
ipv6 mld snooping [blocked vlan <VLAN-LIST>]
no ipv6 mld snooping [blocked vlan <VLAN-LIST>]
```

Description

By default ports are configured in auto mode. This command configures the given ports in blocked mode.

The **no** form of this command removes blocked ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as a blocked port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Example

Configuring blocked ports for the VLANs on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping blocked vlan 10
switch(config-vlan)# ipv6 mld snooping blocked vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping fastlearn

```
ipv6 mld snooping fastlearn <port-list>
```

Description

This command enables the port to learn group information on receiving topology change notification. The **no** form of this command disables fastlearn on the ports.

Parameter	Description
port-list	Required: 1/1/1-1/1/2, ports to be configured as fastlearn ports.

Example

```
switch(config)# ipv6 mld snooping fastlearn 1/1/3
switch(config)# ipv6 mld snooping fastlearn 1/1/1-1/1/2
switch(config)# ipv6 mld snooping fastlearn 1/1/5,1/1/6
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping fastleave vlan

```
ipv6 mld snooping [fastleave vlan <VLAN-LIST>]
no ipv6 mld snooping [fastleave vlan <VLAN-LIST>]
```

Description

Configures the specified ports as fastleave ports. Enables the switch to immediately remove an interface from the bridge table upon receiving the leave group message.

The **no** form of this command disables fastleave configuration on the ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as a fastleave port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Usage

MLD fastleave is configured for ports on a per-VLAN basis. By default, the querier sends a MLD Group-Specific Query message out of the interface, upon which the leave group message is received to ensure that no other receivers are connected to the interface. If receivers are directly attached to the switch, it is inefficient to send the membership query as the receiver wanting to leave is the only connected host. Fastleave processing eliminates the MLD Group-Specific Query message. Thus, it allows the switch to immediately remove an interface from the bridge table upon receiving the leave Group message. This processing speeds up the overall leave process and also eliminates the CPU overhead of having to generate an MLD Group-Specific Query message.

Example

Configuring fastleave ports for the VLAN:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping fastleave vlan 10
switch(config-vlan)# ipv6 mld snooping fastleave vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping forced fastleave vlan

```
ipv6 mld snooping [forced-fastleave <VLAN-LIST>]
no ipv6 mld snooping [forced-fastleave <VLAN-LIST>]
```

Description

Configures the given ports in forced fastleave mode.

The **no** form of this command disables forced fastleave configuration on the ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as a forced fastleave port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Usage

With forced fastleave enabled, MLD speeds up the process of blocking unnecessary multicast traffic to a switch port that is connected to multiple end nodes. When a port having multiple end nodes receives a leave group request from one end node for a given multicast group, forced fastleave activates and waits a small amount of time to receive a join request from any other member of the same group on that port. If the port does not receive a join request for that group within the forced fastleave interval, the switch then blocks any further traffic to that group on that port.

Example

Configuring forced-fastleave ports for the VLAN:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping forced-fastleave vlan 10
switch(config-vlan)# ipv6 mld snooping forced-fastleave vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping forward vlan

```
ipv6 mld snooping [forward vlan <VLAN-LIST>]
no ipv6 mld snooping [forward vlan <VLAN-LIST>]
```

Description

By default ports are configured in auto mode. This command configures the given ports in forward mode.

The **no** form of this command disables forward ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as a forward port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Example

Configuring forward ports for VLANs on the interface:

```
switch# configureterminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping forward vlan 10
switch(config-vlan)# ipv6 mld snooping forward vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping preprogram-starg-flow

```
ipv6 mld snooping preprogram-starg-flow {enable | disable}
```

Description

This command configures the preprogramming of the starg flow feature on MLD snooping enabled VLANs.

Parameter	Description
enable	Enable preprogramming starg flows on the VLAN.
disable	Disable prprogramming starg flows on the VLAN.

Usage

When this feature is enabled, a summarized multicast bridge entry is programmed into the hardware table when a starg or sg MLD join is received on the MLD snooping enabled VLAN. This enables multicast flow to be programmed in the hardware even before the data packet arrives for multicast

flow. MLDv2 joins that are sent for a specific source are treated similar to starg joins and a summarized entry is programmed in the corresponding hardware.

Preprogramming of Starg Flows is supported only on the MLD snooping enabled VLANs. If MLD snooping is disabled on a VLAN, this feature is auto-disabled.

This feature is currently supported for MLDv1 and MLDv2 joins, which means a summarized multicast flow is programmed in advance when a MLDv1 or MLDv2 join for a specific group is received. For MLDv2 deployments, traffic from all of the sources for a specific multicast group are sent to all of the clients, regardless of whether they are sending MLDv1 or MLDv2 joins for this group. Keeping this feature disabled is recommended on VLANs where traffic from the specific source is only expected for the MLDv2 clients.

When an unknown multicast packet is received on a VLAN where the feature is enabled, it triggers programming of a starg entry in the hardware instead of SG.

On the HPE Aruba Networking 4100i, 6000, and 6100 Switch series, a single starg entry is programmed in advance for each join received and data driven programming of SG entries occurs when the traffic is received from a specific source for this group. As a result, the starg entry is used to forward the initial traffic and the SG entries programmed in the multicast forwarding table are used to forward subsequent traffic to all of the clients (that have sent either MLDv2 joins or MLDv3 joins) for all of the active joins in the feature enabled VLANs.

It is highly recommended to not enable this feature on devices where PIM or L3 multicast routing is enabled as it can lead to issues like permanent traffic loss.

Configuring this feature on devices where there are multiple sources sending traffic for the same group address is recommended.

This feature is mutually exclusive with the MLD snooping static group feature.



Optimization may vary environment to environment, based on scale.

Example

Enable preprogramming of starg flow on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping preprogramming-starg-flow enable
```

Remove all preprogramming of starg flow on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping preprogramming-starg-flow disable
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	config-vlan-<VLAN-ID>	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping querier-address

```
ipv6 mld snooping querier-address <QUERIER-IP-ADDRESS>
no ipv6 mld snooping querier-address <QUERIER-IP-ADDRESS>
```

Description

Configures the MLD querier IPv6 address for the IGMP-MLD proxy feature in EVPN. The **no** form of this command removes the configuration.

Parameter	Description
<QUERIER-IP-ADDRESS>	Specifies the proxy querier IPv6 address.

Usage

This command is used in conjunction with the IGMP-MLD proxy feature of EVPN.



This is an optional command applicable to VTEPs that have Layer 2 VLANs (without an IPv6 address) and require IGMP-MLD proxy querier functionality.

If a Layer 3 SVI with an IPv6 address is configured for the VLAN, it takes precedence. In the absence of a valid IPv6 address or SVI, the given IP address is used for querier operations.

This configuration is global and applies to all tenants' Layer 2 VLANs where the IGMP-MLD proxy feature is enabled.

Fabrics running the **igmp-mld proxy** feature must perform distributed querier functionality on every VTEP where the VLAN is extended. This configuration is applicable only when **igmp-mld-proxy** configuration is configured under EVPN.

In the event of underlay tunnel fluctuations, the querier state reinitializes and transitions back to the querier state only after the default querier wait of 260 seconds.

This configuration is not applicable to VLANs that are not mapped to a VNI.



The specified IP address does not need to be assigned to any interface.

Example

Configures the MLD querier IPv6 address for the IGMP-MLD proxy feature in EVPN.

```
switch(config)# ipv6 mld snooping querier-address fe80::2002
```

Remove the configuration of the MLD querier IPv6 address for the IGMP-MLD proxy feature in EVPN.

```
switch(config)# no ipv6 mld snooping querier-address fe80::2002
```

Command History

Release	Modification
10.16	Command introduced

Command Information

Platforms	Command context	Authority
All platforms,	config	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping static-group

```
ipv6 mld snooping [static-group <X:X::X:X>]
no ipv6 mld snooping [static-group <X:X::X:X>]
```

Description

This command configures static multicast group.

The **no** form of this command disables static multicast group.

Parameter	Description
static-group	Required: <X:X::X:X>, MLD static multicast group.

Example

Configuring static multicast group:

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping static-group ff12::c
```

Removing the configuration of static multicast group:

```
switch(config)# vlan 2
switch(config-vlan)# no ipv6 mld snooping static-group ff12::c
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan-<VLAN-ID>	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping version

```
ipv6 mld snooping [version <ver>]  
no ipv6 mld snooping [version <ver>]
```

Description

This command configures the MLD snooping version on the VLAN. MLD version 2 is the default. The **no** form of the command configures the default MLD snooping version on the VLAN, **2**.

Parameter	Description
ver	Required: 1-2, MLD snooping version.

Example

```
switch(config)# vlan 2  
switch(config-vlan)# ipv6 mld snooping version 2
```

```
switch(config-vlan)# no ipv6 mld snooping version 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan-<VLAN-ID>	Administrators or local user group members with execution rights for this command.

MLD snooping show commands

show ipv6 mld snooping

```
show ipv6 mld snooping [vlan <vlan-id> [group <ip-addr>|{port <IF-NAME>}]  
  counters  
  detail  
  groups vlan <vlan-id>  
  no ...  
  packet-exceptions  
  static-groups  
  statistics
```

Description

This command shows MLD snooping details for all VLANs. Specify a VLAN ID or a VLAN and a group to display details for only that VLAN or VLAN group.

Parameter	Description
vlan <vlan-id>	Shows MLD snooping protocol information and number of different groups joined for the VLAN.
group	Shows MLD snooping details for the specified VLAN, including the number of different groups joined for the VLAN. Identify the group by IP address or interface name.
<ip-addr>	Display MLD snooping information for the selected group IP address.
port <IF-NAME>	Display information for a VLAN port. Specify the port name in member/slot/port format.
counters	Shows MLD query packets transmitted (Tx), received (Rx), and error packet counters.
detail	Shows the total VLANs with MLD enabled. When issued with the vlan <vlan-id> parameter, this command displays details for the selected VLAN.
groups	Show MLD snooping groups information.
vlan <vlan-id>	Display IGMP snooping operational information for specified VLAN
no ...	Negates any configured parameter.
packet-exceptions	Troubleshoot issues in an L2 multicast bridge entries for data packets forwarded to the CPU.
statistics	Show MLD snooping statistics.

Examples

```
switch# show ipv mld snooping vlan 2 group port 1/1/1

VLAN ID    : 2
VLAN Name  : VLAN2

Group Address : ff05::2:1
Last Reporter : fe80::1
Group Type    : Filter

Port      Vers Mode Uptime    Expires    V1      Sources    Sources
-----  ---  ---  -----  -
1/1/1     2    INC  1m 46s   2m 34s     Timer    Forwarded  Blocked

Group Address : ff05::2:1
Source Address : 3000::1
Source Type    : Filter

Port      Mode Uptime    Expires    Configured Mode
-----  ---  -----  -
1/1/1     INC  1m 46s   2m 34s     Auto

Group Address : ff05::2:1
Source Address : 3000::2
```

Source Type : Filter

Port	Mode	Uptime	Expires	Configured Mode
1/1/1	INC	1m 46s	2m 34s	Auto

Group Address : ff05::2:1

Source Address : 3000::3

Source Type : Filter

Port	Mode	Uptime	Expires	Configured Mode
1/1/1	INC	1m 46s	2m 34s	Auto

switch# **show ipv6 mld snooping counters**

MLD Snooping VLAN Counters

Rx Counters :

V1 All Hosts Queries	0
V2 All Hosts Queries	0
V2 Group Specific Queries	0
Group And Source Specific Queries	0
V1 Member Reports	0
V2 Member Reports	0
V1 Member Leaves	0

Tx Counters :

Flood on vlan	44
V1 Group Specific Queries	0
V2 Group Specific Queries	0

Errors:

Unknown Message Type	0
Malformed Packets	0
Bad Checksum	0
Packet received on MLD-disabled Interface	0
Interface Wrong Version Queries	0
Packets dropped by ACL	0

Port Counters:

Membership Timeout	0
--------------------	---

switch# **show ipv6 mld snooping groups**

MLD Group Address Information

VLAN ID	Group Address	Expires	UpTime	Last Reporter	Type
10	ff12::c	3m 54s	0m 26s	2001::1	
Filter					
10	ff12::d	4m 17s	0m 3s	2001::1	

```
switch# show ipv6 mld snooping vlan 2 statistics
MLD Snooping statistics
```

```
VLAN ID      :    2
VLAN Name    :   VLAN2
```

```
Number of Include Groups      :    1
Number of Exclude Groups      :    0
Number of Static Groups       :    1
Total Multicast Groups Joined :    2
```

```
switch# show ipv6 mld snooping packet-exceptions
```

List of L2 Multicast Bridge entries for which data packets are hitting CPU

Vlan	Group Address	Source-Address	Packet Count	Last Seen Time
10	ff03::10/128	1010::10/128	19	01h:02m:05s
10	ff03::12/128	1010::11/128	30	00d:02h:01m
10	ff04::10/12	1010::10/128	40	01m:02w:03d
20	ff03::11/128	5000::10/128	20	02m:02w:00d
20	ff03::12/128	5000::10/128	41	0001y:01m:02w:05d
20	ff04::10/128	5000::10/128	30	00d:02h:02m

Command History

Release	Modification
10.10	The packet-exceptions parameter is introduced.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

MLD configuration commands for interface VLAN

ipv6 mld (vlan)

```
ipv6 mld {enable | disable}
no ipv6 mld [enable | disable]
```

Description

This command enables or disables MLD on the interface VLAN.

The **no** form of this command disables MLD on the interface VLAN.

Parameter	Description
enable	Required: Enable MLD on the interface VLAN.
disable	Required: Disable MLD on the interface VLAN.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld enable
switch(config-if-vlan)# ipv6 mld disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld apply access-list (vlan)

```
ipv6 mld apply access-list <ACL-NAME>
no ipv6 mld apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the MLD join or leave packets based on rules set in the particular ACL name.

The **no** form of this command disables the rules set for the ACL.

Parameter	Description
access-list	Associates an ACL with the IGMP.
<ACL-NAME>	Specifies the name of the ACL.

Usage

- Existing classifier commands are used to configure the ACL.
- In case an IGMPv3 packet with multiple group addresses is received, the switch only processes the permitted group addresses based on the ACL rule set. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by ACL. This avoids the delay in learning of the permitted groups. Since the access switch configured with ACL blocks the traffic for the groups which are denied, forwarding of joins has no impact. If all the groups in the packet are

denied by the ACL rule, the packet is not forwarded to the querier and PIM router. Existing joins will timeout.

- In case of IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.

Examples

Configuring the ACL to filter MLD packets based on permit/deny rules set in access list **mygroup**:

```
switch(config)# access-list ipv6 mygroup
switch(config-acl-ip)# 10 deny icmpv6 any ff55::2
switch(config-acl-ip)# 20 deny icmpv6 any ff55::3
switch(config-acl-ip)# 30 permit icmpv6 any ff55::1
switch(config-acl-ip)# exit
switch(config)# interface vlan 2
switch(config-vlan)# ipv6 mld apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list **mygroup**:

```
switch(config-vlan)# no ipv6 mld apply access-list mygroup
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

no ipv6 mld

no ipv6 mld

Description

This command removes all MLD configurations on the interface.

Example

```
switch(config)# interface vlan 1
switch(config-if)# no ipv6 mld
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld querier (vlan)

ipv6 mld querier

Description

This command configures MLD querier.

The **no** form of this command disables MLD querier.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld querier
switch(config-if-vlan)# no ipv6 mld querier
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld querier interval (vlan)

ipv6 mld querier [interval <interval-value>]

Description

This command configures MLD querier interval. The default interval-value is 125.

Parameter	Description
interval-value	Required: 5-300, configures MLD querier interval.
	NOTE: Default interval-value is 125. Use the no ipv6 mld querier interval command to set interval-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld querier interval 100
switch(config-if-vlan)# no ipv6 mld querier interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld last-member-query-interval (vlan)

ipv6 mld last-member-query-interval <interval-value>

Description

This command configures MLD last member query interval value in seconds. The default interval-value is 1 second.

Parameter	Description
interval-value	Required: 1-2, configures MLD last-member-query-interval.



Default interval-value is 1 second. Use the `no ipv6 mld last-member-query-interval` command to set interval-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld last-member-query-interval 2
switch(config-if-vlan)# no ipv6 mld last-member-query-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld querier query-max-response-time (vlan)

ipv6 mld querier query-max-response-time <response-time>

Description

This command configures MLD max response time value in seconds. The default max-response-time-value is 10 seconds.

Parameter	Description
max-response-time-value	Required: 10-128, configures MLD querier max-response-time. NOTE: Default max-response-time-value is 10 seconds. Use the no ipv6 mld querier query-max-response-time command to set max-response-time-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld query-max-response-time 50
switch(config-if-vlan)# no ipv6 mld query-max-response-time
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld robustness (vlan)

ipv6 mld robustness <VALUE>

Description

This command configures MLD robustness. The robustness value represents the number of times the querier retries queries on the connected subnets. The default robustness-value is 2 seconds.

Parameter	Description
<VALUE>	Required: 1-7, configures MLD robustness.
	NOTE: Default robustness-value is 2 seconds. Use the no ipv6 mld robustness command to set robustness-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld robustness 5
switch(config-if-vlan)# no ipv6 mld robustness
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld static-group (vlan)

ipv6 mld static-group <MULTICAST-GROUP-IP>

Description

This command configures MLD static group.

Parameter	Description
<MULTICAST-GROUP-IP>	Required: X:X::X:X, configures MLD static group.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld static-group ff12::c
switch(config-if-vlan)# no ipv6 mld static-group ff12::c
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld version (vlan)

```
ipv6 mld version <VERSION>
no ipv6 mld version <VERSION>
```

Description

This command configures MLD version.

The **no** form of the command configures the default MLD version of **2**.

Parameter	Description
<VERSION>	Required: 1-2, configures MLD version.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld version 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld version strict (vlan)

```
ipv6 mld version <VERSION> [strict]
```

Description

This command configures MLD strict version. Packets that do not match the configured version will be dropped. By default, strict option is not enabled.

Parameter	Description
<VERSION>	Required: 1-2, configures MLD version.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld version 2 strict
switch(config-if-vlan)# no ipv6 mld version 2 strict
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

MLD show commands for interface VLAN



Only the default VRF is supported on the HPE Aruba Networking 4100i Switch Series.



Only the default VRF is supported on the HPE Aruba Networking 6000 and 6100 Switch Series.

show ipv6 mld

```
show ipv6 mld
  all-vrfs
  counters
  group <x:x::x:x> [source x:x::x:x]
  groups
  interface {<INTF-ID>}|{vlan <vlan-id>}
  static-groups
  statistics [all-vrfs|{vrf <vrf-name>}]
```

Description

This command shows MLD groups joined details.

Parameter	Description
all-vrfs	Show MLD snooping info for all VRFs in all interfaces or groups, or for all VRFs in a specified group, interface or

Parameter	Description
	VLAN
counters	Show all MLD counters, or display counters for the specified interface or VLAN
group <x:x::x:x> [source <x:x::x:x>]	Show MLD group information for the specified group, group and interface, or group and vlan. Include the optional source <x:x::x:x> parameter to display source information for the group.
groups	Show MLD group information for all VRFs, or for groups in the specified interface or VLAN.
interface	Shows MLD configuration information for a specified interface or VLAN.
<INTF-ID>	Specify an Interface ID
vlan <vlan-id>	Specify a VLAN ID
static-groups	Display all static groups information, or include one of the additional parameters apply additional filters: ▪ all-vrfs: Display MLD static-group information for all VRFs ▪ vrf <vrf-name>: Display MLD static-group information for the selected VRF
statistics	Display all MLD statistics, or include one of the additional parameters apply additional filters: ▪ all-vrfs: Display MLD statistics information for all VRFs ▪ vrf <vrf-name>: Display MLD statistics information for the selected VRF

Examples

Showing the current MLD configuration and status

```
switch# show ipv6 mld

VRF Name           : default
Interface          : vlan10
MLD Configured Version : 2
MLD Operating Version : 2
Querier State      : Querier
Querier IP [this switch] : fe80::7272:cfff:fe96:d3ec
Querier Uptime     : 39m 44s
Querier Expiration Time : 0m 31s
MLD Snoop Enabled on VLAN : True
```

Showing the MLD configuration on a specified VLAN or interface:

```
switch# show ipv6 mld interface vlan 10

MLD Configured Version : 2
```

```

MLD Operating Version      : 2
Querier State              : Querier
Querier IP [this switch]  : fe80::7272:cfff:fe96:d3ec
Querier Uptime             : 40m 42s
Querier Expiration Time   : 1m 39s
MLD Snoop Enabled on VLAN : True

```

```
switch# show ipv6 mld interface 1/1/2
```

```

MLD Configured Version    : 2
MLD Operating Version     : 2
Querier State              : Querier
Querier IP [this switch]  : fe80::7272:cfff:fe96:d3ec
Querier Uptime             : 40m 42s
Querier Expiration Time   : 1m 39s
MLD Snoop Enabled on VLAN : True

```

Showing MLD groups information for a specified interface:

```
switch# show ipv6 mld interface 1/1/1 groups
```

```
MLD group information for group ff55::1
```

```
Interface Name      : 1/1/1
VRF Name            : default
```

```
Group Address       : ff55::1
Last Reporter       : fe80::a00:9ff:fe77:1062
```

Vers	Mode	Uptime	Expires	V1 Timer	Sources Forwarded	Sources Blocked
2	EXC	0m 14s	4m 6s			

Showing MLD static groups

```
switch# show ipv6 mld static-groups all-vrfs
```

```
MLD Static Group Address Information
```

```
VRF Name      :default
```

```
Interface Name  Group Address
```

```

-----
vlan2           ff12::c
vlan2           ff12::d

```

Showing MLD counters

```
switch# show ipv6 mld counters
```

```
MLD Counters
```

```
Interface Name      : vlan2
VRF Name            : default
Membership Timeout   : 0
```

```

Rx      Tx
-----

```

```

V1 All Hosts Queries          0          0
V2 All Hosts Queries          0         12
V1 Group Specific Queries     0          0
V2 Group Specific Queries     0          0
Group And Source Specific Queries 0          0
V2 Member Reports             0         N/A
V1 Member Reports             0         N/A
V1 Member Leaves              0         N/A
Packets dropped by ACL         0         N/A

```

```
switch# show ipv6 mld counters vrf default
```

MLD Counters

```

Interface Name      : vlan2
VRF Name            : default
Membership Timeout   : 0

```

	Rx	Tx
	-----	-----
V1 All Hosts Queries	0	0
V2 All Hosts Queries	0	12
V1 Group Specific Queries	0	0
V2 Group Specific Queries	0	0
Group And Source Specific Queries	0	0
V2 Member Reports	0	N/A
V1 Member Reports	0	N/A
V1 Member Leaves	0	N/A
Packets dropped by ACL		

Showing MLD statistics on a specified interface:

```
switch# show ipv6 mld interface 1/1/1 statistics
```

MLD statistics

```

Interface Name : 1/1/1
VRF Name       : default

```

```

Number of Include Groups      : 2
Number of Exclude Groups     : 0
Number of Static Groups       : 0
Total Multicast Groups Joined : 2

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

MLD configuration commands for interface

ipv6 mld (interface)

```
ipv6 mld {enable | disable}
no ipv6 mld {enable | disable}
```

Description

This command enables or disables MLD on the interface.

The **no** form of this command disables MLD on the interface.

Parameter	Description
enable	Required: Enable MLD on the interface.
disable	Required: Disable MLD on the interface.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld enable
switch(config-if)# ipv6 mld disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld apply access-list (interface)

```
ipv6 mld apply access-list <ACL-NAME>
no ipv6 mld apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the MLD join or leave packets based on rules set in the particular ACL name.

The **no** form of this command removes the rules set for the ACL.

Parameter	Description
access-list	Associates an ACL with the IGMP.

Parameter	Description
<ACL-NAME>	Specifies the name of the ACL.

Usage

- Existing classifier commands are used to configure the ACL.
- In case an IGMPv3 packet with multiple group addresses is received, the switch only processes the permitted group addresses based on the ACL rule set. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by ACL. This avoids the delay in learning of the permitted groups. Since the access switch configured with ACL blocks the traffic for the groups which are denied, forwarding of joins has no impact. If all the groups in the packet are denied by the ACL rule, the packet is not forwarded to the querier and PIM router. Existing joins will timeout.
- In case of IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.

Examples

Configuring the ACL to filter MLD packets based on permit/deny rules set in access list **mygroup**:

```
switch(config)# access-list ipv6 mygroup
switch(config-acl-ip)# 10 deny icmpv6 any ff55::2
switch(config-acl-ip)# 20 deny icmpv6 any ff55::3
switch(config-acl-ip)# 30 permit icmpv6 any ff55::1
switch(config-acl-ip)# exit
switch(config)# interface vlan 1
switch(config-vlan)# ipv6 mld apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list **mygroup**:

```
switch(config-vlan)# no ipv6 mld apply access-list mygroup
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

no ipv6 mld

no ipv6 mld

Description

This command removes all MLD configurations on the interface.

Example

```
switch(config)# interface vlan 1
switch(config-if)# no ipv6 mld
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld querier (interface)

ipv6 mld querier

Description

This command configures MLD querier. This functionality will allow the interface to join in the querier-election process.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld querier
switch(config-if)# no ipv6 mld querier
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld querier interval (interface)

ipv6 mld querier [interval <interval-value>]

Description

This command configures MLD querier interval. The default interval-value is 125.

Parameter	Description
interval-value	Required: 5-300, configures MLD querier interval.
	NOTE: Default interval-value is 125. Use the <code>no ipv6 mld querier interval</code> command to set interval-value to the default.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld querier interval 100
switch(config-if)# no ipv6 mld querier interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld last-member-query-interval (interface)

ipv6 mld last-member-query-interval <interval-value>

Description

This command configures MLD last member query interval value in seconds. The default interval-value is 1 second.

Parameter	Description
interval-value	Required: 1-2, configures MLD last-member-query-interval.



Default interval-value is 1 second. Use the `no ipv6 mld last-member-query-interval` command to set interval-value to the default.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld last-member-query-interval 2
switch(config-if)# no ipv6 mld last-member-query-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld querier query-max-response-time (interface)

```
ipv6 mld querier query-max-response-time <response-time>
```

Description

This command configures MLD max response time value in seconds. The default max-response-time-value is 10 seconds.

Parameter	Description
max-response-time-value	Required: 10-128, configures MLD querier max-response-time. NOTE: Default max-response-time-value is 10 seconds. Use the no ipv6 mld querier query-max-response-time command to set max-response-time-value to the default.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld query-max-response-time 50
switch(config-if)# no ipv6 mld query-max-response-time
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld robustness (interface)

ipv6 mld robustness <value>

Description

This command configures MLD robustness. The robustness value represents the number of times the querier retries queries on the connected subnets. The default robustness-value is 2 seconds.

Parameter	Description
robustness-value	Required: 1-7, configures MLD robustness.



Default robustness-value is 2 seconds. Use the `no ipv6 mld robustness` command to set robustness-value to the default.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld robustness 5
switch(config-if)# no ipv6 mld robustness
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld static-group (interface)

ipv6 mld static-group <multicast-group-ip>

Description

This command configures MLD static group.

Parameter	Description
multicast-group-ip	Required: X:X::X:X, configures MLD static group.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld static-group ff12::c
switch(config-if)# no ipv6 mld static-group ff12::c
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping filter-unknown-mcast

```
ipv6 mld snooping filter-unknown-mcast
no ipv6 mld snooping filter-unknown-mcast
```

Description

Configures the unknown multicast to steal when the MLD snooping is enabled.

The **no** form of this command returns to the default behavior of initial flooding of unknown multicast traffic.

Usage

In the default behavior, the unknown multicast traffic is flooded until the IP Multicast Flow programming is done on the hardware. This is known as initial flooding of unknown multicast. Use this command to filter unknown multicast instead of flooding.



Initial flooding of multicast traffic is observed for a few seconds after the device comes up from a reboot. This issue is only seen when the multicast source connected device is rebooted. Once the device is up after a reboot, it takes a few seconds for the CPU Rx rule to be programmed during the timeframe that the initial flooding is observed. This is an expected behavior.

Example

Configure the unknown multicast to steal globally on IGMP snooping enabled VLANs.

```
switch# configure terminal
switch(config)# ipv6 mld snooping filter-unknown-multicast
```

Removing the configuration of the unknown multicast to steal globally on IGMP snooping enabled VLANs.

```
switch# configure terminal
switch(config)# no ipv6 mld snooping filter-unknown-multicast
```

Command History

Release	Modification
10.14	Command introduced on the 4100i, 6000, and 6100 Switch series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	config	Administrators or local user group members with execution rights for this command.

ipv6 mld version (interface)

```
ipv6 mld version <version>
no ipv6 mld version <version>
```

Description

This command configures MLD version.

The **no** form of this command removes MLD version from the interface.

Parameter	Description
version	Required: 1-2, configures MLD version.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld version 2
```

```
switch(config)# interface vlan 1
switch(config-if)# no ipv6 mld version 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld version strict (interface)

ipv6 mld version <version> [strict]

Description

This command configures MLD strict version. Packets that do not match the configured version will be dropped. By default, strict option is not enabled.

Parameter	Description
version	Required: 1-2, configures MLD version.

Example

```
switch(config)# interface vlan 1
switch(config-if)# ipv6 mld version 2 strict
switch(config-if)# no ipv6 mld version 2 strict
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

Support and Other Resources

Accessing HPE Aruba Networking Support

HPE Aruba Networking Support Services	https://www.hpe.com/us/en/networking/hpe-aruba-networking-support-services.html
AOS-CX Switch Software Documentation Portal	https://arubanetworking.hpe.com/techdocs/AOS-CX/help_portal/Content/home.htm
HPE Aruba Networking Support Portal	https://networkingsupport.hpe.com/home
North America telephone	1-800-943-4526 (US & Canada Toll-Free Number) +1-650-750-0350 (Backup—Toll Number)
International telephone	https://www.hpe.com/psnow/doc/a50011948enw

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Other useful sites

Other websites that can be used to find information:

HPE Aruba Networking Developer Hub	https://developer.arubanetworks.com/hpe-aruba-networking-aoscx/docs/about
Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
AOS-CX Software Technical Update channel on YouTube.	Videos on new features introduced in this release: https://www.youtube.com/playlist?list=PLsYGHuNuBZcbWPEjjHuVMqP-Q_UL3CskS

HPE Aruba Networking Hardware Documentation and Translations Portal	https://arubanetworking.hpe.com/techdocs/hardware/DocumentationPortal/Content/home.htm
HPE Aruba Networking software	https://networkingsupport.hpe.com/downloads
Software licensing and Feature Packs	https://licensemanagement.hpe.com/
End-of-Life information	https://networkingsupport.hpe.com/end-of-life

Accessing Updates

You can access updates from the HPE Aruba Networking Support Portal at <https://networkingsupport.hpe.com>.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To subscribe to eNewsletters and alerts:

<https://networkingsupport.hpe.com/notifications/subscriptions> (requires an active HPE Aruba Networking Support Portal account to manage subscriptions). Security notices are viewable without an HPE Aruba Networking Support Portal account.

Warranty Information

To view warranty information for your product, go to <https://www.arubanetworks.com/support-services/product-warranties/>.

Regulatory Information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at <https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts>

Additional regulatory information

HPE Aruba Networking is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements, environmental data (company programs, product recycling, energy efficiency), and safety information and compliance data, (RoHS and WEEE). For more information, see <https://www.arubanetworks.com/company/about-us/environmental-citizenship/>.

Documentation Feedback

HPE Aruba Networking is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback-switching@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help

content, include the product name, product version, help edition, and publication date located on the legal notices page.