

AOS-CX 10.09 Multicast Guide

4100i, 6000, 6100 Switch Series



a Hewlett Packard
Enterprise company

Copyright Information

© Copyright 2023 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code 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, send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

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	3
About this document	7
Applicable products	7
Latest version available online	7
Command syntax notation conventions	7
About the examples	8
Identifying switch ports and interfaces	8
Multicast overview	10
Multicast protocols	10
Multicast addresses	10
Important considerations	11
Internet Group Management Protocol (IGMP)	13
IGMP defaults, protocols, and supported configuration	13
How the IGMP protocol works	13
Considerations when configuring IGMP	14
IGMP configuration task list	15
Enabling or disabling IGMP	15
Specifying the IGMP version	15
Configuring IGMP static groups	16
Configuring IGMP query and response parameters	16
Disabling IGMP	17
Viewing IGMP information	17
IGMP configuration example	18
IGMP commands	19
ip igmp	19
ip igmp apply access-list	20
ip igmp last-member-query-interval	21
ip igmp querier	22
ip igmp querier interval	23
ip igmp querier query-max-response-time	24
ip igmp robustness	25
ip igmp router-alert-check	25
ip igmp static-group	26
ip igmp version	27
ip igmp version strict	28
no ip igmp	29
show ip igmp	29
show ip igmp counters	30
show ip igmp group	32
show ip igmp groups	34
show ip igmp interface	36
show ip igmp interface counters	37
show ip igmp interface group	38
show ip igmp interface groups	39
show ip igmp interface statistics	40

show ip igmp static-groups	41
show ip igmp statistics	42
IGMP snooping	44
IGMP snooping defaults, protocols, and supported configuration	44
How IGMP snooping works	45
IGMP snooping configuration task list	46
Enabling or disabling IGMP snooping	46
Specifying the IGMP snooping version	46
Configuring IGMP snooping static groups	47
Enabling drop-unknown filters	47
Configuring IGMP snooping fast learn ports globally	47
Configuring IGMP snooping per port filtering	48
Disabling IGMP snooping	48
Viewing IGMP snooping information	49
IGMP snooping commands	49
ip igmp snooping	49
ip igmp snooping apply access-list	50
ip igmp snooping auto vlan	51
ip igmp snooping blocked	52
ip igmp snooping drop-unknown	53
ip igmp snooping fastlearn	54
ip igmp snooping fastleave vlan	55
ip igmp snooping forced fastleave vlan	56
ip igmp snooping forward vlan	57
ip igmp snooping static-group	58
ip igmp snooping version	58
no ip igmp snooping	59
show ip igmp snooping	60
show ip igmp snooping counters	60
show ip igmp snooping groups	61
show ip igmp snooping static-groups	62
show ip igmp snooping statistics	63
show ip igmp snooping vlan	63
show ip igmp snooping vlan counters	65
show ip igmp snooping vlan group port	66
show ip igmp snooping vlan statistics	68
MLD snooping	69
MLD snooping global configuration commands	69
ipv6 mld snooping	69
MLD snooping VLAN configuration commands	70
ipv6 mld snooping	70
ipv6 mld snooping apply access-list	71
ipv6 mld snooping auto vlan	72
ipv6 mld snooping blocked vlan	72
ipv6 mld snooping fastlearn	73
ipv6 mld snooping fastleave vlan	74
ipv6 mld snooping forced fastleave vlan	75
ipv6 mld snooping forward vlan	76
ipv6 mld snooping version	77
ipv6 mld snooping static-group	77
MLD snooping show commands	78
show ipv6 mld snooping	78
show ipv6 mld snooping counters	79
show ipv6 mld snooping groups	80

show ipv6 mld snooping statistics	81
show ipv6 mld snooping vlan counters	81
show ipv6 mld snooping vlan group port	83
show ipv6 mld snooping vlan group source	84
show ipv6 mld snooping static-groups	86
show ipv6 mld snooping vlan statistics	86
MLD configuration commands for interface VLAN	87
ipv6 mld	87
ipv6 mld apply access-list	88
no ipv6 mld	89
ipv6 mld querier	89
ipv6 mld querier interval	90
ipv6 mld last-member-query-interval	90
ipv6 mld querier query-max-response-time	91
ipv6 mld robustness	92
ipv6 mld static-group	92
ipv6 mld version	93
ipv6 mld version strict	94
MLD show commands for interface VLAN	94
show ipv6 mld	94
show ipv6 mld interface vlan	95
show ipv6 mld all-vrfs	96
show ipv6 mld interface vlan counters	97
show ipv6 mld interface vlan groups	98
show ipv6 mld interface vlan group source	99
show ipv6 mld groups	100
show ipv6 mld groups all-vrfs	101
show ipv6 mld interface counters	102
show ipv6 mld interface statistics	103
show ipv6 mld interface groups	104
show ipv6 mld interface vlan group source	105
show ipv6 mld group all-vrfs	106
show ipv6 mld group source all-vrfs	107
show ipv6 mld interface vlan statistics	108
show ipv6 mld static-groups all-vrfs	109
show ipv6 mld counters	110
MLD configuration commands for interface	111
ipv6 mld	111
ipv6 mld apply access-list	112
no ipv6 mld	113
ipv6 mld querier	114
ipv6 mld querier interval	114
ipv6 mld last-member-query-interval	115
ipv6 mld querier query-max-response-time	116
ipv6 mld robustness	116
ipv6 mld static-group	117
ipv6 mld version	118
ipv6 mld version strict	118

Support and Other Resources 120

Accessing Aruba Support	120
Accessing Updates	121
Aruba Support Portal	121
My Networking	121
Warranty Information	121
Regulatory Information	121

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

Applicable products

This document applies to the following products:

- Aruba 4100i Switch Series (JL817A, JL818A)
- Aruba 6000 Switch Series (R8N85A, R8N86A, R8N87A, R8N88A, R8N89A)
- Aruba 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: <ul style="list-style-type: none">▪ <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: <ul style="list-style-type: none">▪ For output formats where italic text cannot be displayed, variables are enclosed in angle brackets (< >). 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: <ul style="list-style-type: none"> ■ 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 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 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 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.

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 and 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.

SSDP considerations

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, Aruba 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
```

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 Aruba 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 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	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	<code>config-if-vlan</code>	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	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 platforms	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	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	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	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	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
<MULTICAST-GROUP-IP>	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
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if-vlan	

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
<VERSION>	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	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	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	config-if-vlan	Administrators or local user group members with execution rights for this command.

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 <code>all-vrfs</code> .

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	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 <code>all-vrfs</code> 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	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 <code>all-vrfs</code> 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         V2         Sources   Sources
-----  ---  -----  -----  Timer      Timer      Forwarded 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          V2          Sources    Sources
-----  ---  -----  -
3     EXC   17m 5s    4m 2s     Timer       Timer       Forwarded  Blocked

```

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          V2          Sources    Sources
-----  ---  -----  -
3     EXC   17m 35s   3m 32s     Timer       Timer       Forwarded  Blocked

```

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	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 <code>all-vrfs</code> 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 V2 Sources Sources
-----|-----|-----|-----|-----|-----|-----|-----
3   EXC  0m 36s   3m 44s  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  0m 36s   3m 44s  Timer  Timer  Forwarded Blocked
```

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          V2          Sources     Sources
-----  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
3      EXC  0m 13s    4m 7s      Timer       Timer       Forwarded   Blocked

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          V2          Sources     Sources
-----  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
3      EXC  0m 13s    4m 7s      Timer       Timer       Forwarded   Blocked

```

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

```

Command History

Release	Modification
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.

show ip igmp interface

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

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	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	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	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
-----
3     INC   4m 40s   3m 51s   Timer   Timer   Forwarded Blocked
-----
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

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	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	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 <code>all-vrfs</code> 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	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 <code>all-vrfs</code> 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

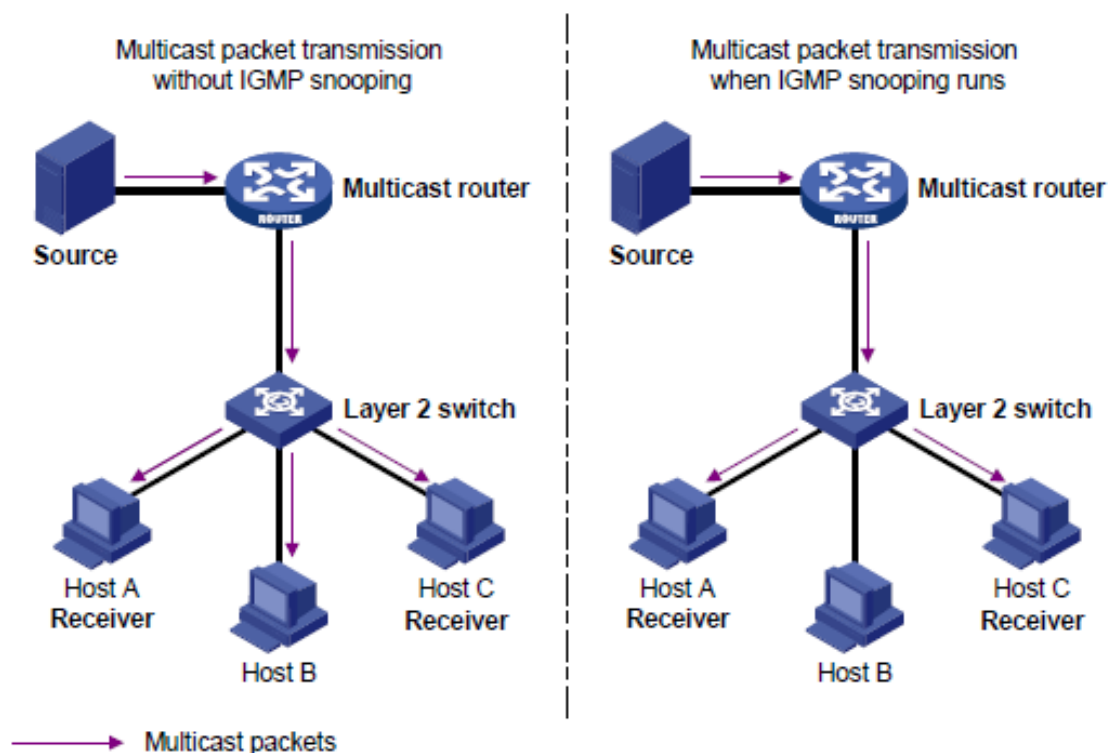
Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 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)# ip igmp snooping enable
```

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
```



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

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

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

Description

Enables or disables IGMP snooping on the VLAN. By default, IGMP snooping is disabled.

The `no` form of this command disables IGMP snooping on the VLAN.



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

Parameter	Description
{enable disable}	Specifies enabling or disabling IGMP snooping on the VLAN. Default: disable.

Examples

Enable IGMP snooping on a VLAN:

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

Disable IGMP snooping on a VLAN:

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

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

Command History

Release	Modification
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 apply access-list

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

Examples

Configuring the ACL 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 snooping apply access-list mygroup
```

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

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

Command History

Release	Modification
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 auto vlan

```
ip igmp snooping [auto vlan <VLAN-LIST>]
no ip igmp snooping [auto vlan <VLAN-LIST>]
```

Description

Configures the specified ports in auto mode. In auto mode traffic flow is controlled by the IGMP joins/leaves. Auto mode is the default.

The `no` form of this command removes auto mode ports for the VLAN.

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

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
```

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.

ip igmp snooping blocked

```
ip igmp snooping [blocked vlan <VLAN-LIST>]
no ip igmp snooping [blocked vlan <VLAN-LIST>]
```

Description

Configures the specified ports in blocked mode for the specified VLAN list. In blocked mode, joins and traffic are always blocked on this port.

The `no` form of this command disables 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).

Examples

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
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ip igmp snooping drop-unknown

```
ip igmp snooping drop-unknown {vlan-shared | vlan-exclusive}
no ip igmp snooping drop-unknown {vlan-shared | vlan-exclusive}
```

Description

Configures drop-unknown mode. 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`.

The `no` form of this command disables drop unknown on the switch.

Parameter	Description
<code>vlan-shared</code>	Enables shared VLAN filter on the switch. Default: <code>vlan-shared</code> .
<code>vlan-exclusive</code>	Enables exclusive drop unknown filter per VLAN.

Examples

Configuring shared VLAN filter on the switch:

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

Configuring 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 fastlearn

```
ip igmp snooping fastlearn <PORT-LIST>  
no ip igmp snooping fastlearn <PORT-LIST>
```

Description

Enables the port to learn group information when receiving a topology change notification. By default, fast learn is not enabled on ports.

The `no` form of this command disables fast learn on the specified ports.

Parameter	Description
fastlearn <PORT-LIST>	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).

Examples

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
```

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 fastleave vlan

```
ip igmp snooping [fastleave vlan <VLAN-LIST>]
no ip igmp snooping [fastleave vlan <VLAN-LIST>]
```

Description

Enables the switch to immediately remove the IGMP client from its IGMP table and cease transmitting multicast traffic to the client.

The `no` form of this command disables fastleave on the specified ports.

Parameter	Description
<VLAN-LIST>	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

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.

Examples

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
```

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.

ip igmp snooping forced fastleave vlan

```
ip igmp snooping [forced-fastleave vlan <VLAN-LIST>]
no ip igmp snooping [forced-fastleave vlan <VLAN-LIST>]
```

Description

Configures the specified ports in forced fastleave mode.

The `no` form of this command disables forced fastleave on the specified 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, 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.

Examples

Configuring forced-fastleave ports for VLANs 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 forced-fastleave vlan 10
switch(config-if)# ip igmp snooping forced-fastleave vlan 10-20
```

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.

ip igmp snooping forward vlan

```
ip igmp snooping forward [vlan <VLAN-LIST>]
no ip igmp snooping forward [vlan <VLAN-LIST>]
```

Description

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.

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).

Examples

Configuring forward 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 forward vlan 10
switch(config-if)# ip igmp snooping forward vlan 10-20
```

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.

ip igmp snooping static-group

```
ip igmp snooping static-group <MULTICAST-IP-ADDRESS>  
no ip igmp snooping static-group <MULTICAST-IP-ADDRESS>
```

Description

Configures an IGMP snooping static multicast group. You can configure a maximum of 32 IGMP snooping static groups.

The `no` form of this command disables static multicast group.

Parameter	Description
<MULTICAST-IP-ADDRESS>	Specifies the IGMP static multicast group IP address. Format: A.B.C.D

Examples

Configuring 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
```

Command History

Release	Modification
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 version

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

Description

Configures the IGMP snooping version on the VLAN.

The `no` form of this command removes the IGMP snooping version on the VLAN.

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

Examples

Configuring IGMP snooping version on the VLAN:

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

Removing IGMP snooping version on the VLAN:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

no ip igmp snooping

no ip igmp snooping

Description

Disables all IGMP snooping configurations on the VLAN.



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

Examples

Disabling all IGMP snooping configurations on the VLAN:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ip igmp snooping

```
show ip igmp snooping
```

Description

Shows IGMP snooping configuration information and status for all VLANs.

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

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
Querier Address [this switch] : 20.1.1.1
Querier Port :
Querier UpTime :0m 21s
Querier Expiration Time :0m 2s
```

Command History

Release	Modification
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.

show ip igmp snooping counters

```
show ip igmp snooping counters
```

Description

Shows IGMP snooping query packet Tx, Rx, and Error packet counter details.

Examples

Showing IGMP snooping packet counters:

```

switch# show ip igmp snooping counters
IGMP Snooping VLAN Counters

Rx Counters :

V1 All Hosts Queries           0
V2 All Hosts Queries           0
V3 All Hosts Queries           3
V2 Group Specific Queries      0
V3 Group Specific Queries      0
Group And Source Specific Queries 0
V1 Member Reports              0
V2 Member Reports              0
V3 Member Reports              2
V2 Member Leaves               0

Tx Counters :

Flood on vlan                   44
V2 Group Specific Queries       0
V3 Group Specific Queries       0

Errors:

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

Port Counters:

Membership Timeout              0

```

Command History

Release	Modification
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.

show ip igmp snooping groups

```
show ip igmp snooping groups
```

Description

Shows IGMP snooping group information.

Examples

Showing IGMP snooping groups:

```
switch# show ip igmp snooping groups
IGMP Group Address Information

VLAN ID Group Address    Expires    UpTime    Last Reporter    Type
-----
2       239.1.1.3             0m 4s     0m 10s     10.1.1.1         Filter
```

Command History

Release	Modification
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.

show ip igmp snooping static-groups

```
show ip igmp snooping static-groups
```

Description

Shows IGMP snooping static group details.

Examples

Showing IGMP snooping static group details:

```
switch# show ip igmp snooping static-groups
IGMP Static Group Address Information

VLAN ID Group Address
-----
10       239.1.1.10
10       239.1.1.11
```

Command History

Release	Modification
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.

show ip igmp snooping statistics

```
show ip igmp snooping statistics
```

Description

Shows IGMP snooping protocol information and the joined group statistics.

Examples

Showing IGMP snooping statistics:

```
switch# show ip igmp snooping statistics
IGMP Snooping Protocol Info

Total VLANs with IGMP enabled           : 1
IGMP Drop Unknown Multicast            : Global

IGMP Snooping Joined Groups Statistics

VLAN ID  VLAN Name          Total  Static  INCLUDE  EXCLUDE
-----  -
1        DEFAULT_VLAN_1         0      0       0        0
2        VLAN10                  2      2       0        0
```

Command History

Release	Modification
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.

show ip igmp snooping vlan

```
show ip igmp snooping vlan <VLAN-ID> [group [<group-ip>]
[source <source-ip>]]
```

Description

Shows IGMP snooping protocol information for the specified VLAN. You can also specify a group and source to show group and source information.

Parameter	Description
<VLAN-ID>	Specifies a VLAN. Range: 1-4094.
group <group-ip>	Specifies a group to display port and group information. Format: A.B.C.D
source <source-ip>	Specifies a source to display source information for the group. Format: A.B.C.D

Examples

Showing IGMP snooping protocol information for VLAN 2:

```
switch# show ip igmp snooping vlan 2

IGMP Snooping Protocol Info

Total VLANs with IGMP enabled           : 1
IGMP Drop Unknown Multicast            : Global

VLAN ID : 2
VLAN Name : VLAN2
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 20.1.1.1
Querier Port : 1/1/1
Querier UpTime :
Querier Expiration Time :

Active Group Address   Tracking   Vers   Mode   Uptime   Expires
-----
239.1.1.2             Filter     3     INC   0m 27s   0m 13s
```

Showing IGMP snooping group information for group 239.1.1.2 on VLAN 2:

```
switch# show ip igmp snooping vlan 2 group 239.1.1.2

IGMP ports and group information for group 239.1.1.2

VLAN ID   : 2
VLAN Name : VLAN2

Group Address : 239.1.1.2
Last Reporter : 10.1.1.1
Group Type    : Filter

Port      Vers   Mode   Uptime   Expires   V1      V2      Sources   Sources
-----  -
1/1/6    3     INC   0m 41s   3m 39s   Timer   Timer   Forwarded Blocked
                                         -----
                                         3       0

Group Address : 239.1.1.2
Source Address : 30.1.1.1
Source Type    : Filter

Port      Mode   Uptime   Expires   Configured Mode
-----  -
1/1/6    INC   0m 41s   3m 39s   Auto
```



```

Group Address : 239.1.1.2
Source Address : 30.1.1.2
Source Type : Filter

```

Port	Mode	Uptime	Expires	Configured Mode
1/1/6	INC	0m 41s	3m 39s	Auto

```

Group Address : 239.1.1.2
Source Address : 30.1.1.3
Source Type : Filter

```

Port	Mode	Uptime	Expires	Configured Mode
1/1/6	INC	0m 41s	3m 39s	Auto

Showing IGMP snooping group information for group 239.1.1.2 on VLAN 2 and source 30.1.1.1:

```

switch# show ip igmp snooping vlan 2 group 239.1.1.2 source 30.1.1.1

VLAN ID : 2
VLAN Name : VLAN2
Group Address : 239.1.1.2
Source Address : 30.1.1.1
Source Type : Filter

```

Port	Mode	Uptime	Expires	Configured Mode
1/1/6	INC	0m 41s	3m 39s	Auto

Command History

Release	Modification
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.

show ip igmp snooping vlan counters

```
show ip igmp snooping vlan <VLAN-ID> counters
```

Description

Shows IGMP snooping query packet Tx, Rx, Error packet counters for the specified VLAN.

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

Examples

Showing IGMP snooping counters for VLAN 2:

```
Switch# show ip igmp snooping vlan 2 counters
IGMP Snooping VLAN Counters

VLAN ID   :   2
VLAN Name : VLAN2

Rx Counters :

V1 All Hosts Queries           0
V2 All Hosts Queries           0
V3 All Hosts Queries           3
V2 Group Specific Queries      0
V3 Group Specific Queries      0
Group And Source Specific Queries 0
V1 Member Reports              0
V2 Member Reports              0
V3 Member Reports              2
V2 Member Leaves               0

Tx Counters :

Flood on vlan                   71
V2 Group Specific Queries      0
V3 Group Specific Queries      0

Errors:

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

Port Counters:

Membership Timeout              0
Switch#
```

Command History

Release	Modification
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.

show ip igmp snooping vlan group port

```
show ip igmp snooping vlan <VLAN-ID> group port <PORT-ID>
```

Description

Shows IGMP snooping group details for the specified VLAN. It shows information about all IGMP snooping groups or sources learned on a particular port.

Parameter	Description
<VLAN-ID>	Specifies a VLAN. Range: 1-4094.
<PORT-ID>	Specifies a port of a VLAN to display information about all IGMPv3 snooping groups/sources learned on a particular port.

Examples

Showing IGMP snooping group details for VLAN 2 port 1/1/6:

```
switch# show ip igmp snooping vlan 2 group port 1/1/6

VLAN ID    : 2
VLAN Name  : VLAN2

Group Address : 239.1.1.1
Last Reporter : 10.1.1.1
Group Type   : Filter

Port      Vers Mode Uptime   Expires   V1      V2      Sources  Sources
-----  - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1/1/6    2   EXC  0m 21s  1m 12s          Timer    Timer    Forwarded Blocked

VLAN ID    : 2
VLAN Name  : VLAN2

Group Address : 239.1.1.2
Last Reporter : 10.1.1.1
Group Type   : Filter

Port      Vers Mode Uptime   Expires   V1      V2      Sources  Sources
-----  - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1/1/6    2   EXC  0m 21s  1m 32s          Timer    Timer    Forwarded Blocked
```

Command History

Release	Modification
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.

show ip igmp snooping vlan statistics

show ip igmp snooping vlan <VLAN-ID> statistics

Description

Shows IGMP snooping statistics details for the specified VLAN. It also shows information on the different groups joined in the VLAN.

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

Examples

Showing IGMP snooping statistics for VLAN 2:

```
switch# show ip igmp snooping vlan 2 statistics
IGMP 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
```

Command History

Release	Modification
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.

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.

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
<code>vlan-shared</code>	Required: Enable shared VLAN filter on the switch.
<code>vlan-exclusive</code>	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	config	Administrators or local user group members with execution rights for this command.

MLD snooping VLAN configuration commands

ipv6 mld snooping

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

Description

This command enables or disables MLD snooping on the VLAN.

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

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

Example

Enable MLD snooping on VLAN 2:

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

Remove all MLD snooping configurations on VLAN 2:

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

Command History

Release	Modification
10.07 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.

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
<code>access-list</code>	Associates an ACL with the IGMP.
<code><ACL-NAME></code>	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	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	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	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	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
All platforms	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	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	config-vlan	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	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>]
```

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

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

Description

This command shows MLD snooping configuration details for all VLANs.

Example

```
switch# show ipv6 mld snooping

MLD Snooping Protocol Info

Total VLANs with MLD enabled           : 1
Current count of multicast groups joined : 0

MLD Drop Unknown Multicast             : Global

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

VLAN ID                                  : 2
VLAN Name                                : VLAN2
MLD Configured Version                   : 2
MLD Operating Version                    : 2
Querier Address [this switch]            : fe80::218:71ff:fec4:2f00
Querier Port                              :
Querier UpTime                            : 0m 21s
Querier Expiration Time                   : 0m 2s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld snooping counters

```
show ipv6 mld snooping [counters]
```

Description

This command shows MLD snooping query packet Tx, Rx, and Error packet counter details.

Parameter	Description
counters	Optional, show MLD snooping counters.

Example

```
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:
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld snooping groups

```
show ipv6 mld snooping [groups]
```

Description

This command shows MLD snooping group details for the specified VLAN.

Parameter	Description
groups	Optional, show MLD snooping groups information.

Example

```
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	

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with

Platforms	Command context	Authority
		execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld snooping statistics

show ipv6 mld snooping [statistics]

Description

This command shows MLD snooping statistics information.

Parameter	Description
statistics	Optional, show MLD snooping statistics.

Example

```
switch# show ipv6 mld snooping statistics
MLD Snooping Protocol Info

Total VLANs with MLD enabled           : 1
Current count of multicast groups joined : 2

MLD Drop Unknown Multicast             : Global

MLD Snooping Joined Groups Statistics

VLAN ID  VLAN Name           Total  Static  INCLUDE  EXCLUDE
-----  -
1         DEFAULT_VLAN_1           0      0       0        0
2         VLAN2                    2      2       0        0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld snooping vlan counters

show ipv6 mld snooping [vlan <vlan-id> [counters]]

Description

This command shows MLD snooping protocol information and number of different groups joined for the VLAN.

Parameter	Description
vlan-id	Required, 1-4094, shows MLD snooping information.
counters	Optional, shows MLD query packet Tx, Rx, Error packet counters on a specified VLAN.

Example

```

switch# show ipv6 mld snooping vlan 2 counters
MLD Snooping VLAN Counters

VLAN ID      :    2
VLAN Name    :   VLAN2

Rx Counters :

V1 All Hosts Queries           0
V2 All Hosts Queries           0
V1 Group Specific 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                   71
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#

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with

Platforms	Command context	Authority
		execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld snooping vlan group port

```
show ipv6 mld snooping [vlan <vlan-id> [group [port <port_id>]]]
```

Description

This command shows MLD snooping details for the specified VLAN, including the number of different groups joined for the VLAN.

Parameter	Description
port-id	Required: <PORT>, shows MLD protocol information for the specified port of a VLAN.

Example

```
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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld snooping vlan group source

```
show ipv6 mld snooping [vlan <vlan-id> [group [<group-ip>] [source <source-ip>]]]
```

Description

This command shows MLD snooping details for the specified VLAN, including the number of different groups joined for the VLAN.

Parameter	Description
vlan-id	Required: 1-4094, shows MLD protocol information for the specified VLAN.
group-ip	Optional: X:X::X:X, MLD source information for the specified group.
source-ip	Optional: X:X::X:X, MLD source information for the specified group.

Example

```
switch# show ipv6 mld snooping vlan 2

MLD Snooping Protocol Info

Total VLANs with MLD enabled           : 2
Current count of multicast groups joined : 0

MLD Drop Unknown Multicast             : Global

VLAN ID                                : 2
VLAN Name                               : VLAN2
MLD Configured Version                  : 2
MLD Operating Version                    : 2
Querier Address [this switch]           : fe80::218:71ff:fec4:2f00
Querier Port                             :
Querier UpTime                           : 0m 21s
Querier Expiration Time                  : 0m 2s

Active Group Address                    Tracking Vers Mode  Uptime    Expires
-----
--
ff05::2:1                               Filter      2    EXC    0m 17s    4m 3s
```

```

switch# show ipv6 mld snooping vlan 2 group

MLD ports and group information for group ff05::2:1

VLAN ID                : 2
VLAN Name               : VLAN2

Group Address           : ff05::2:1
Last Reporter          : 2001::1
Group Type              : Filter

Port      Vers Mode Uptime    Expires    V1      Sources  Sources
-----  -  ---  -  -  -  -  -  -  -  -  -
1/1/1    2   EXC  0m 5s    4m 15s    4m 15s   0        0

switch# show ipv6 mld snooping vlan 2 group ff05::2:1

MLD ports and group information for group ff05::2:1

VLAN ID                : 2
VLAN Name               : VLAN2

Group Address           : ff05::2:1
Last Reporter          : 2001::1
Group Type              : Filter

Port      Vers Mode Uptime    Expires    V1      Sources  Sources
-----  -  ---  -  -  -  -  -  -  -  -
1/1/1    2   EXC  0m 5s    4m 15s    4m 15s   0        0

switch# show ipv mld snooping vlan 2 group ff05::2:1 source 3000::3

VLAN ID                : 2
VLAN Name               : VLAN2
Group Address           : ff05::2:1
Source Address          : 3000::3
Source Type             : Filter

Port      Mode Uptime    Expires    Configured Mode
-----  -  ---  -  -  -  -  -  -  -  -
1/1/1    INC  0m 27s    3m 53s    Auto

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld snooping static-groups

```
show ipv6 mld snooping [static-groups]
```

Description

This command shows MLD snooping static group details, including the number of static groups joined.

Example

```
switch# show ipv6 mld snooping static-groups

MLD Static Group Address Information

VLAN ID Group Address
-----
10      ff12::1
10      ff12::2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld snooping vlan statistics

```
show ipv6 mld snooping [vlan <vlan-id> [statistics]]
```

Description

This command shows MLD snooping statistics details for the specified VLAN, including the number of different groups joined for the VLAN.

Parameter	Description
vlan-id	Required, 1-4094, shows MLD query packet Tx, Rx, error packet counters on VLAN.

Example

```
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

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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

```

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	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld apply access-list

```
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
<code>access-list</code>	Associates an ACL with the IGMP.
<code><ACL-NAME></code>	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	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.

ipv6 mld querier

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	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld querier interval

```
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 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	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld last-member-query-interval

```
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	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld querier query-max-response-time

`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 <code>no ipv6 mld querier query-max-response-time</code> 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	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld robustness

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 <code>no ipv6 mld robustness</code> 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	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld static-group

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	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld version

```
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	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld version strict

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	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 Aruba 4100i Switch Series.



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

show ipv6 mld

show ipv6 mld

Description

This command shows MLD configuration on VLAN.

Example

```
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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld interface vlan

```
show ipv6 mld [interface <IFNAME> | vlan <VLAN-ID>]
```

Description

This command shows MLD configuration on a specific VLAN.

Parameter	Description
<VLAN-ID>	Required: 1-4094, shows MLD configuration on a specified VLAN.
<IFNAME>	Required: Shows MLD configuration on a specified interface.

Examples

Showing MLD configuration on a specified 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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld all-vrfs

```
show ipv6 mld [all-vrfs ]
```

Description

This command shows MLD information for the specified VRF.

Parameter	Description
all-vrfs	Optional: shows MLD information status for all VRFs.

Example

```
switch(config)# show ipv6 mld all-vrfs
VRF Name      : default
Interface     : vlan2
MLD Configured Version   : 2
MLD Operating Version    : 2
Querier State            : Querier
Querier IP [this switch] : fe80::a00:9ff:fe06:67cd
Querier Uptime           : 23m 53s
Querier Expiration Time  : 0m 17s
MLD Snoop Enabled on VLAN : True

Active Group Address      Vers Mode Uptime    Expires
-----
ff05::2:1                2    INC  3m 56s    1m 47s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld interface vlan counters

```
show ipv6 mld [interface <INTF-ID> | vlan <VLAN-ID>] [counters]
```

Description

This command shows MLD query packet Tx and Rx on a specific VLAN.

Parameter	Description
<VLAN-ID>	Required: 1-4094, shows MLD configuration on a specified VLAN.
<INTF-ID>	Required: IFNAME, shows MLD configuration on a specified interface.
counters	Optional: Shows MLD query packet counter Tx-Rx on a specified VLAN.

Example

Showing MLD query packet Tx and Rx on a specified interface:

```
switch# show ipv6 mld interface vlan 2 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	0
V1 Group Specific Queries	0	0
V2 Group Specific Queries	0	2
Group And Source Specific Queries	0	2
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 interface 1/1/1 counters
```

```
MLD Counters
```

```

Interface Name      : 1/1/1
VRF Name           : default
Membership Timeout  : 0

```

	Rx	Tx

V1 All Hosts Queries	0	0
V2 All Hosts Queries	0	0
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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld interface vlan groups

```
show ipv6 mld [interface <INTF-ID> | vlan <VLAN-ID>] [groups]
```

Description

This command shows MLD groups joined details.

Parameter	Description
<INTF-ID>	Required: 1-4094, shows MLD information on a specified VLAN.
	Required: IFNAME, shows MLD information on a specified interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)
<VLAN-ID>	Required: 1-4094, shows MLD configuration on a specified VLAN.
groups	Optional: Shows MLD groups information on a specified interface.

Example

Showing MLD groups information on the specified VLAN:

```

switch# show ipv6 mld interface vlan 2 groups

MLD group information for group ff05::2:1

Interface Name      : vlan2
VRF Name           : default

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

Vers  Mode  Uptime    Expires    V1      Sources   Sources
-----  ---  -----  -----  ---  -----  -----
2      INC   6m 2s     0m 4s     1      Forwarded Blocked

Group Address      : ff05::2:1
Source Address     : 3000::1

Mode  Uptime    Expire
-----  -----  -----
INC   6m 2s     0m 4s

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld interface vlan group source

```
show ipv6 mld [interface (<intf-id> | vlan <vlan-id>) [group <group_ip>] [source <source_ip>]]
```

Description

This command shows MLD joined group details on a specified interface.

Parameter	Description
<VLAN-ID>	Required: 1-4094, shows MLD joined group details on a specified VLAN.
<INTF-ID>	Required: IFNAME, shows MLD joined group details on a specified interface.
group_ip	Required: X:X::X:X, shows MLD joined group details.
source_ip	Required: X:X::X:X, shows MLD joined group details for a specified source.

Example

```
switch# show ipv6 mld interface vlan 2 group ff55::5

MLD group information for group ff55::5

Interface Name      : vlan2
VRF Name            : default

Group Address       : ff55::5
Last Reporter       : fe80::1

Vers Mode Uptime    Expires      V1          Sources    Sources
-----
2      INC  6m 2s      0m 4s      Timer       Forwarded  Blocked

Group Address       : ff55::5
Source Address      : 3000::1

Mode Uptime        Expire
-----
INC  6m 2s         0m 4s

switch# show ipv6 mld interface vlan 2 group ff55::5 source 3000::1

Interface Name      : vlan2
VRF Name            : default
Group Address       : ff55::5
Source Address      : 3000::1

Mode Uptime        Expire
-----
INC  9m 37s       2m 0s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld groups

```
show ipv6 mld [groups]
```

Description

This command shows MLD groups joined details.

Parameter	Description
groups	Options: shows MLD groups information.

Example

```
switch# show ipv6 mld groups

MLD group information for group ff05::2:11

Interface Name   : vlan2
VRF Name         : default

Group Address    : ff05::2:11
Last Reporter    : 2001::1

Vers  Mode  Uptime    Expires    V1         Sources    Sources
-----  -
1         2m 27s    1m 53s     1m 53s
-----  -

MLD group information for group ff05::2:12

Interface Name   : vlan2
VRF Name         : default

Group Address    : ff05::2:12
Last Reporter    : 2001::1

Vers  Mode  Uptime    Expires    V1         Sources    Sources
-----  -
1         0m 3s     4m 18s     4m 18s
-----  -
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld groups all-vrfs

```
show ipv6 mld groups [all-vrfs]
```

Description

This command shows MLD groups joined details on VRFs.

Parameter	Description
all-vrfs	Optional: shows MLD groups joined in all VRFs.

Example

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

MLD group information for group ff05::2:11

Interface Name   : vlan1
VRF Name         : default

Group Address    : ff05::2:11
Last Reporter    : 2001::1

Vers Mode Uptime   Expires   V1         Sources   Sources
-----
1           4m 4s     2m 38s    2m 38s    Forwarded Blocked

switch# show ipv6 mld groups vrf default

MLD group information for group ff05::2:11

Interface Name   : vlan2
VRF Name         : default

Group Address    : ff05::2:11
Last Reporter    : 2001::1

Vers Mode Uptime   Expires   V1         Sources   Sources
-----
1           5m 25s    1m 17s    1m 17s    Forwarded Blocked
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld interface counters

```
show ipv6 mld [interface {<INTF-ID> }[counters]]
```

Description

This command shows MLD query packet Tx and Rx on a specific interface.

Parameter	Description
<INTF-ID>	Required: shows MLD configuration on a specified interface
counters	Optional: shows MLD query packet counter Tx-Rx on a specified interface.

Examples

Showing MLD configuration on a specified interface:

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

```
MLD Counters
```

```
Interface Name      : 1/1/1
VRF Name            : default
Membership Timeout  : 0
```

	Rx	Tx
	-----	-----
V1 All Hosts Queries	0	0
V2 All Hosts Queries	0	9
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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld interface statistics

```
show ipv6 mld [interface {<INTF-ID>} [statistics]]
```

Description

This command shows MLD statistics on a specific interface.

Parameter	Description
<INTF-ID>	Required: shows MLD statistics on a specified interface.

Parameter	Description
statistics	Optional: shows MLD statistics on a specified interface.

Examples

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	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 ipv6 mld interface groups

```
show ipv6 mld [interface {<INTF-ID>}[groups]]
```

Description

This command shows MLD groups joined details.

Parameter	Description
<INTF-ID>	Required: shows MLD configuration on a specified interface.
groups	Optional: shows MLD groups information.

Example

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          Sources    Sources
-----  -
2      EXC    0m 14s    4m 6s      Timer       Forwarded  Blocked

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld interface vlan group source

```
show ipv6 mld [interface (<intf-id> | vlan <vlan-id>) [group <group_ip>] [source <source_ip>]]
```

Description

This command shows MLD joined group details on a specified interface.

Parameter	Description
<VLAN-ID>	Required: 1-4094, shows MLD joined group details on a specified VLAN.
<INTF-ID>	Required: IFNAME, shows MLD joined group details on a specified interface.
group_ip	Required: X:X::X:X, shows MLD joined group details.
source_ip	Required: X:X::X:X, shows MLD joined group details for a specified source.

Example

```
switch# show ipv6 mld interface vlan 2 group ff55::5

MLD group information for group ff55::5
```

```

Interface Name      : vlan2
VRF Name           : default

Group Address      : ff55::5
Last Reporter      : fe80::1

Vers  Mode  Uptime    Expires    V1         Sources    Sources
-----  ---  -----  -
2     INC   6m 2s     0m 4s     Timer      Forwarded  Blocked

Group Address      : ff55::5
Source Address     : 3000::1

Mode  Uptime    Expire
-----  -----
INC   6m 2s     0m 4s

switch# show ipv mld interface vlan 2 group ff55::5 source 3000::1

Interface Name      : vlan2
VRF Name           : default
Group Address      : ff55::5
Source Address     : 3000::1

Mode  Uptime    Expire
-----  -----
INC   9m 37s   2m 0s

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld group all-vrfs

```
show ipv6 mld [group <group_ip> [all-vrfs]]
```

Description

This command shows MLD joined group details on VRF.

Parameter	Description
group_ip	Required: X:X::X:X, shows MLD joined group details.
all-vrfs	Optional: shows MLD groups joined in all VRFs.

Example

```

switch# show ipv6 mld group ff55::1

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          Sources    Sources
-----  -----  -----  -----  -----  -----  -----
2      EXC   3m 12s   3m 46s   Timer     Forwarded  Blocked

switch# show ipv6 mld group ff05::2:11 all-vrfs

MLD group information for group ff05::2:11

Interface Name      : vlan2
VRF Name            : default

Group Address       : ff05::2:11
Last Reporter       : 2001::1

Vers Mode Uptime    Expires    V1          Sources    Sources
-----  -----  -----  -----  -----  -----  -----
1              1m 16s   3m 4s     3m 4s     Timer     Forwarded  Blocked

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld group source all-vrfs

```
show ipv6 mld [group <group_ip> [source <source_ip> [all-vrfs]]]
```

Description

This command shows MLD joined group details for a source on VRF.

Parameter	Description
group_ip	Required: X:X::X:X, shows MLD joined group details.

Parameter	Description
source_ip	Required: X:X::X:X, shows MLD joined group details for a source.
all-vrfs	Optional: shows MLD groups joined in all VRFs.

Example

```
switch# show ipv6 mld group ff05::2:1 source 3000::1

Interface Name   : vlan2
VRF Name        : default
Group Address    : ff05::2:1
Source Address   : 3000::1

Mode Uptime      Expire
----
INC  0m 53s     3m 27s

switch# show ipv6 mld group ff05::2:1 source 3000::1 all-vrfs

Interface Name   : vlan2
VRF Name        : default
Group Address    : ff05::2:1
Source Address   : 3000::1

Mode Uptime      Expire
----
INC  1m 38s     4m 5s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld interface vlan statistics

```
show ipv6 mld [interface vlan <vlan-id> [statistics]]
```

Description

This command shows MLD statistics on a specific interface VLAN.

Parameter	Description
vlan-id	Required: 1-4094, shows MLD information on a specified VLAN.
statistics	Optional: shows MLD query packet Tx, Rx, Error packet counters on a specified VLAN.

Example

```
switch# show ipv6 mld interface vlan 2 statistics

MLD 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	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 ipv6 mld static-groups all-vrfs

```
show ipv6 mld [static-groups [all-vrfs]]
```

Description

This command shows MLD static groups.

Parameter	Description
all-vrfs	Optional: shows MLD groups joined in all VRFs.

Example

```
switch# show ipv6 mld static-groups

MLD Static Group Address Information
```

```

VRF Name      :default
Interface Name  Group Address
-----
vlan2          ff12::c
vlan2          ff12::d

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

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ipv6 mld counters

show ipv6 mld [counters]

Description

This command shows MLD counters.

Parameter	Description
vrf	Optional: shows MLD counter status in a specific VRF.

Example

```

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	0	N/A

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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

```

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

ipv6 mld apply access-list

```
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	<code>config-vlan</code>	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.

ipv6 mld querier

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

ipv6 mld querier interval

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

ipv6 mld last-member-query-interval

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

ipv6 mld querier query-max-response-time

```
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 <code>no ipv6 mld querier query-max-response-time</code> command to set max-response-time-value to the default.

Example

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

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.

ipv6 mld robustness

```
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	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld static-group

`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	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld version

```
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	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld version strict

```
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	config-if	Administrators or local user group members with execution rights for this command.

Accessing Aruba Support

Aruba Support Services	https://www.arubanetworks.com/support-services/
Aruba Support Portal	https://asp.arubanetworks.com/
North America telephone	1-800-943-4526 (US & Canada Toll-Free Number) +1-408-754-1200 (Primary - Toll Number) +1-650-385-6582 (Backup - Toll Number - Use only when all other numbers are not working)
International telephone	https://www.arubanetworks.com/support-services/contact-support/

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:

Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
AOS-CX Switch Software Documentation Portal	https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
Aruba Hardware Documentation and Translations Portal	https://www.arubanetworks.com/techdocs/hardware/DocumentationPortal/Content/home.htm

Aruba software	https://asp.arubanetworks.com/downloads
Software licensing	https://lms.arubanetworks.com/
End-of-Life information	https://www.arubanetworks.com/support-services/end-of-life/
Aruba Developer Hub	https://developer.arubanetworks.com/

Accessing Updates

You can access updates from the Aruba Support Portal or the HPE My Networking Website.

Aruba Support Portal

<https://asp.arubanetworks.com/downloads>

If you are unable to find your product in the Aruba Support Portal, you may need to search My Networking, where older networking products can be found:

My Networking

<https://www.hpe.com/networking/support>

To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

<https://support.hpe.com/portal/site/hpsc/aae/home/>

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

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://asp.arubanetworks.com/notifications/subscriptions> (requires an active Aruba Support Portal (ASP) account to manage subscriptions). Security notices are viewable without an ASP 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

Aruba 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

Aruba 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.