BROCADE

CONFIGURATION GUIDE

Brocade SLX-OS IP Multicast Configuration Guide, 17s.1.01

Supporting the Brocade SLX 9140 and SLX 9240 Switches

53-1005176-01
29 June 2017

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.
`Courier font`	Identifies CLI output.

Format	Description
	Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. In Fibre Channel products, square brackets may be used instead for this purpose.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

White papers, data sheets, and the most recent versions of Brocade software and hardware manuals are available at www.brocade.com. Product documentation for all supported releases is available to registered users at MyBrocade.

Click the **Support** tab and select **Document Library** to access product documentation on MyBrocade or www.brocade.com. You can locate documentation by product or by operating system.

Release notes are bundled with software downloads on MyBrocade. Links to software downloads are available on the MyBrocade landing page and in the Document Library.

Document feedback

Quality is our first concern at Brocade, and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com
- By sending your feedback to documentation@brocade.com

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online or by telephone. Brocade OEM customers should contact their OEM/solution provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to www.brocade.com and select **Support**.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone
Preferred method of contact for non-urgent issues: • Case management through the MyBrocade portal. • Quick Access links to Knowledge Base, Community, Document Library, Software Downloads and Licensing tools	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • Toll-free numbers are available in many countries. • For areas unable to access a toll-free number: +1-408-333-6061

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/solution provider, contact your OEM/solution provider for all of your product support needs.

- OEM/solution providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/solution provider.

About This Document

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some devices but not to others, this guide identifies exactly which devices are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for SLX-OS Release 17s.1.00, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release:

- Brocade SLX 9140 switch
- Brocade SLX 9240 switch

NOTE
Some of the commands in this document use a slot/port designation. Because the Brocade SLX 9140 switch and the Brocade SLX 9240 switch do not contain line cards, the slot designation must always be "0" (for example, 0/1 for port 1).

To obtain information about other Brocade OS versions, refer to the documentation specific to that version.

What's new in this document

There has been no enhancement to this guide for the SLX OS 17s.1.01 software release.

IP Multicast

IP multicast overview

Multicast protocols allow a group or channel to be accessed over different networks by multiple stations (clients) for the receipt and transmission of multicast data. Distribution of stock quotes, video transmissions such as news services and remote classrooms, and video conferencing are all examples of applications that use multicast routing.

Brocade devices support the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD).

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to any immediately-neighboring multicast routers.

Multicast control packet and data forwarding through a Layer 2 switch is achieved by Layer 2 forwarding of the received multicast packets on all the member ports of the VLAN interfaces. This approach though simple is not bandwidth efficient, because only a subset of member ports may be connected to devices interested in receiving these multicast packets. In a worst-case scenario, the data gets forwarded to all port members of a VLAN with a large number of member ports even if only a single VLAN member is interested in receiving the data. Such scenarios can lead to loss of throughput for a switch upon receiving a high rate of multicast data traffic.

IGMP and MLD provide the functionality to save bandwidth and throughput by forwarding traffic to only interested receivers instead of all the member ports of the VLAN. IGMP snooping provides the specification for IPv4 and MLD snooping provides the specification for IPv6 data traffic forwarding.

MLD snooping is a multicast constraining mechanism that runs on Layer 2 or Layer 3 devices to manage and control IPv6 multicast groups. MLD snooping provides similar functionality for IPv6 as IGMP snooping for IPv4 by sending IPv6 multicast traffic only to the interested listeners. By listening to and analyzing MLD messages, a Layer 2 device running MLD snooping establishes mappings between ports and multicast MAC addresses or multicast IP addresses and forwards multicast data.

IP multicast message types

Multicast routers use IGMP or MLD to learn which groups have interested listeners on each of their attached physical networks. In any given subnet, one multicast router is elected to act as an IGMP or MLD querier.

The IGMP or MLD querier sends out the following types of queries to hosts:

- General query: Asks whether any host is listening to any group.
- Group-specific query: Asks whether any host is listening to a specific multicast group. This query is sent in response to a host leaving the multicast group and allows the router to quickly determine if any remaining hosts are interested in the group.

Hosts that are multicast listeners send the following kinds of messages:

- Membership report: Indicates that the host wants to join a particular multicast group.
- Leave report: Indicates that the host wants to leave a particular multicast group.

IPv4 Multicast Traffic Reduction

IGMP snooping overview

The forwarding of multicast control packets and data through a Layer 2 device configured with VLANs is most easily achieved by the Layer 2 forwarding of received multicast packets on all the member ports of the VLAN interfaces. However, this simple approach is not bandwidth efficient, because only a subset of member ports may be connected to devices interested in receiving those multicast packets. In a worst-case scenario, the data would get forwarded to all port members of a VLAN with a large number of member ports, even if only a single VLAN member is interested in receiving the data. Such scenarios can lead to loss of throughput for a device that gets hit by a high rate of multicast data traffic.

Internet Group Management Protocol (IGMP) snooping is a mechanism by which a Layer 2 device can effectively address this issue of inefficient multicast forwarding to VLAN port members. Snooping involves "learning" forwarding states for multicast data traffic on VLAN port members from the IGMP control (join/leave) packets received on them. The Layer 2 device also provides for a way to configure forwarding states statically through the CLI.

Multicast routing and IGMP snooping

Multicast routers use IGMP snooping to learn which groups have members on each of their attached physical networks. A multicast router keeps a list of multicast group memberships for each attached network, and a timer for each membership.

> NOTE
> "Multicast group memberships" means that at least one member of a multicast group on a given attached network is available.

There are two ways that hosts join multicast routing groups:

- By sending an unsolicited IGMP join request.
- By sending an IGMP join request as a response to a general query from a multicast router.

In response to the request, the device creates an entry in its Layer 2 forwarding table for that VLAN. When other hosts send join requests for the same multicast, the device adds them to the existing table entry. Only one entry is created per VLAN in the Layer 2 forwarding table for each multicast group.

VLANs can be configured as snooping only or routing with snooping. When Layer 3 multicast routing is enabled on a particular VE, snooping for the underlying VLAN is enabled implicitly. Explicit snooping can be enabled on a VLAN in addition to implicit snooping. Implicit snooping is by default IGMP snooping. With routing enabled on a VE, when explicit snooping is disabled, snooping reverts back to implicit snooping. This does not change the functionality in any way, but only removes the configuration. When routing is disabled on a VE where explicit snooping is configured, the routing side of the programming stops and the snooping side programming takes over. When routing is enabled, the Layer 3 IGMP querier takes precedence on that VLAN. When routing is disabled, and if the snooping querier is configured, then the snooping querier takes effect.

Enabling IGMP snooping

1. Enter the **configure terminal** command to access global configuration mode.

```
device# configure terminal
```

2. Enter VLAN configuration mode.

```
device(config)# vlan 1
device(config-vlan-1)
```

3. Enable IGMP snooping.

```
device(config-vlan-1)# ip igmp snooping enable
```

Configuring the IGMP snooping querier

If your multicast traffic is not routed because Protocol-Independent Multicast (PIM) is not configured, use the IGMP snooping querier in a VLAN.

The IGMP snooping querier sends out IGMP queries to trigger IGMP responses from devices that are to receive IP multicast traffic. The IGMP snooping querier listens for these responses to map the appropriate forwarding addresses.

Use the following procedure to configure the IGMP snooping querier.

1. Enter the **configure terminal** command to access global configuration mode.

```
device# configure terminal
```

2. Enter the **vlan** command with the VLAN number.

```
device(config)# vlan 25
```

3. Set the IGMP query interval for the VLAN.

```
device(config-Vlan-25)# ip igmp snooping query-interval 125
```

   The valid range is from 1 through 18000 seconds. The default is 125 seconds.

4. Set the last member query interval.

```
device(config-Vlan-25)# ip igmp snooping last-member-query-interval 1000
```

   The valid range is from 1000 through 25500 milliseconds. The default is 1000 milliseconds.

5. Set the last member query count.

```
device(config-Vlan-25)# ip igmp snooping last-member-query-count 3
```

   The valid range is from 2 through 10. The default is 2.

6. Set the startup query count.

```
device(config-Vlan-25)# ip igmp snooping startup-query-count 3
```

   The valid range is from 1 through 10. The default is 1.

7. Set the startup query interval.

```
device(config-Vlan-25)# ip igmp snooping startup-query-interval 200
```

   The valid range is from 1 through 450 seconds. The default is 1 second.

8. Set the Maximum Response Time.

```
device(config-Vlan-25)# ip igmp snooping query-max-response-time 10
```

   The valid range is from 1 through 25 seconds. The default is 10 seconds.

9. Configure the static Mrouter port.

```
device(config-Vlan-25)# ip igmp snooping mrouter interface ethernet 3/2
```

10. Configure a static IGMP group.

```
device(config-vlan-25)# ip igmp snooping static-group 225.0.0.1 interface ethernet 6/15
```

11. Set the snooping robustness variable.

```
device(config-Vlan-25)# ip igmp snooping robustness-variable 5
```

    The valid range is from 2 through 10. The default is 2.

12. You can stop the flooding of the unknown multicast traffic using the **ip igmp snooping restrict-unknown-multicast** command.

```
device(config-vlan-25)# ip igmp snooping restrict-unknown-multicast
```

13. Use the **ip igmp snooping fast-leave** command to enable fast leave processing.

```
device(config-vlan-25)# ip igmp snooping fast-leave
```

14. Activate the IGMP snooping querier functionality for the VLAN.

```
device(config-Vlan-25)# ip igmp snooping querier enable
```

    NOTE
    The IGMP snooping querier and the static mrouter can be configured together on a VLAN interface.

Monitoring IGMP snooping

Monitoring the performance of your IGMP traffic allows you to diagnose any potential issues on your device. This helps you utilize bandwidth more efficiently by setting the device to forward IP multicast traffic only to connected hosts that request multicast traffic.

Use the following commands to monitor IGMP snooping on the device; the commands do not need to be entered in any specific order.

1. Enter the **show ip igmp groups** command to display all information on IGMP multicast groups for the device. Use this command to display the IGMP database, including configured entries for all groups on all interfaces, all groups on specific interfaces, or specific groups on specific interfaces.

```
device# show ip igmp groups
Total Number of Groups: 2
IGMP Connected Group Membership
Group Address  Interface Uptime      Expires      Last Reporter   Version
225.1.1.1      vlan25    00:05:27     00:02:32     25.1.1.1202
Member Ports: eth 2/24
```

2. Enter the **show ip igmp snooping** command specifying the VLAN ID to view snooping configuration information such as snooping querier enable, snooping query interval, IGMP operation mode, PIM snooping configuration, and IGMP snooping configuration.

```
device# show ip igmp snooping

 Vlan ID: 10
 Multicast Router ports:  eth1/1
 Querier - Disabled
 IGMP Operation mode: IGMPv3
 Is Fast-Leave Enabled : Enabled
 Max Response time = 10
 Last Member Query Interval = 1
 Query interval = 125
 Number of Multicast Groups: 0
```

3. Enter the **show ip igmp statistics interface** command to display the IGMP statistics for a VLAN or interface.

```
device# show ip igmp statistics interface vlan 1

IGMP packet statistics for all interfaces in vlan 1:
IGMP Message type     Edge-Received   Edge-Sent   Edge-Rx-Errors   ISL Received
Membership Query                  0           0                0              0
V1 Membership Report              0           0                0              0
V2 Membership Report              0           0                0              0
Group Leave                       0           0                0              0
V3 Membership Report              0           0                0              0
PIM hello                         0           0                0              0

IGMP Error Statistics:
Unknown types            0
Bad Length               0
Bad Checksum             0
```

4. Enter the **show ip igmp interface** command to display the Layer 3 IGMP interface configuration information.

```
device# show ip igmp interface
Interface Ve100
IGMP enabled
IGMP query interval 30 seconds
IGMP other-querierinterval 65 seconds
IGMP query response time 10 seconds
IGMP last-member query interval 1 seconds
IGMP immediate-leave disabled
IGMP querier100.0.0.1(this system)
IGMP version 2
```

5. Enter the **show ip igmp snooping mrouter vlan** command to display mrouter port-related information.

```
device# show ip igmp snooping mrouter vlan 10
Vlan     Interface    Expires (Sec)
10       eth1/4       250
10       eth1/1       238
```

When you have reviewed the IGMP statistics for the device, refer to Enabling IGMP snooping on page 14 or Configuring the IGMP snooping querier on page 14 to make any needed corrections.

IPv4 Multicast Snooping

IGMP

The Internet Group Management Protocol (IGMP) allows an IPv4 system to communicate IP multicast group membership information to its neighboring routers. The routers, in turn, limit the multicast of IP packets with multicast destination addresses to only those interfaces on the router that are identified as IP multicast group members.

In IGMPv2, when a router sends a query to the interfaces, the clients on the interfaces respond with a membership report of multicast groups to the router. The router can then send traffic to these groups, regardless of the traffic source. When an interface no longer needs to receive traffic from a group, it sends a leave message to the router, which in turn sends a group-specific query to that interface to see if any other clients on the same interface are still active.

There are different types of query messages:

- A "General Query" is sent by a multicast router to learn the complete multicast reception state of the neighboring interfaces. In a General Query, both the Group Address field and the Number of Sources (N) field are zero.
- A "Group-Specific Query" is sent by a multicast router to learn the reception state, with respect to a *single* multicast address, of the neighboring interfaces. In a Group-Specific Query, the Group Address field contains the multicast address of interest, and the Number of Sources (N) field contains zero.

Default IGMP version

IGMPv2 is enabled by default only when snooping or multicast routing are enabled on the system.

Also, you can specify what version of IGMP you want to run on a device on a per-VLAN basis. If you do not specify an IGMP version, IGMPv2 is used.

Compatibility with IGMPv1 and IGMPv2

Different multicast groups, interfaces, and routers can run their own versions of IGMP. The version of IGMP is reflected in the membership reports that the hosts send to the router. Routers and interfaces must be configured to recognize the version of IGMP you want them to process.

An interface or router sends the queries and reports that include its IGMP version specified on it. The interface may recognize a query or report that has a different version. For example, an interface running IGMPv2 can recognize IGMPv3 packets, but cannot process them. When the router sends out IGMP queries over an IGMPv2 interface, the equal or lower version of reports is supported, but a higher version of reports is not supported.

The version of IGMP can be specified per interface (physical port or virtual routing interface), and per physical port within a virtual routing interface.

IPv6 Multicast VLAN Traffic Reduction

MLD snooping overview

Multicast Listener Discovery (MLD) snooping is a multicast-constraining mechanism that runs on Layer 2 or Layer 3 devices to manage and control IPv6 multicast groups.

A Layer 2 switch forwards all multicast control packets and data received on all the member ports of a VLAN interface. This approach, though simple, is not bandwidth efficient, because only a subset of member ports may be connected to devices interested in receiving those multicast packets. In the worst-case scenario the data are forwarded to all port members of a VLAN with a large number of member ports, even if only a single VLAN member is interested in receiving the data. Such scenarios can lead to loss of throughput for a switch when it receives high-rate multicast data traffic.

MLD snooping provides functionality for IPv6 that is similar to IGMP snooping for IPv4, by sending IPv6 multicast traffic only to interested listeners. By listening to and analyzing MLD messages, a Layer 2 device running MLD snooping establishes mappings between ports and multicast MAC addresses or multicast IP addresses, and forwards multicast data accordingly. Multicast routers in a network are found by means of either static configuration, dynamic learning, or PIM hello-based mrouter detection.

> NOTE
> This release supports the IPv6 version of MLDv1 snooping.

In any given subnet, one multicast router is elected to act as an MLD querier. The MLD querier sends out the following types of queries to hosts:

- General query: Querier asks whether any host is listening to any group.
- Group-specific query: Querier asks whether any host is listening to a specific multicast group. This query is sent in response to a host leaving the multicast group and allows the router to determine quickly whether any remaining hosts are interested in the group.

Hosts that are multicast listeners send the following kinds of messages:

- Report message: Indicates that the host wants to join a particular multicast group.
- Done message: Indicates that the host wants to leave a particular multicast group.

MLD traffic is forwarded as follows:

- MLD general queries received on a multicast-router interface are forwarded to all other interfaces in the VLAN.

- MLD group-specific queries received on a multicast-router interface are forwarded to only those interfaces in the VLAN that are members of the group.
- MLD report or done messages received on a host interface are forwarded to multicast-router interfaces in the same VLAN, but not to other host interfaces in the VLAN.
- Proxy MLD membership reports received with a null source IP address are accepted, to support report suppression.
- All unrecognized MLD packets are flooded to all (STP) unblocked member ports of the VLAN, to ensure that no data traffic is black-holed.

Data forwarding rules ensure that the multicast traffic received at the switch is forwarded to all interested downstream port members. Forwarding rules can be based on either the Layer 3 multicast destination IP group address or the Layer 2 destination MAC address.

- If a switch is already in a learned multicast group, multicast packets are forwarded only to those host interfaces in the VLAN that are members of the multicast group and to all multicast-router interfaces in the VLAN.
- If a switch is not in a learned multicast group, multicast packets for a group that has no current members are flooded to all member ports of the VLAN, as well as to all multicast-router interfaces in the VLAN.

The remainder of this section presents the tasks related to MLD configuration that are supported in this release.

Enabling and disabling MLD snooping at the VLAN level

You can enable or disable MLD snooping at the VLAN level.

1. Enter the configure terminal command to access global configuration mode.

```
device# configure terminal
```

2. Enter the VLAN configuration mode.

```
device(config)# vlan 1
device(config-vlan-1)
```

3. Enter the **ipv6 mld snooping enable** command.

```
device(config-vlan-1# ipv6 mld snooping enable
```

4. Enter the **no** form of the command to disable MLD snooping.

```
device(config-vlan-1# no ipv6 mld snooping enable
```

Enabling and disabling MLD querier functionality on a VLAN

You can use the MLD querier functionality to support MLD snooping on a VLAN where PIM and MLD are not enabled (for example, because multicast traffic does not need to be routed). MLD querier functionality is disabled by default.

To enable this functionality, use the **ipv6 mld snooping querier enable** command on a VLAN interface:

```
device(config-Vlan-2000)# ipv6 mld snooping querier enable
```

To disable this functionality, use the **no ipv6 mld snooping querier enable** command on a VLAN interface:

```
device(config-Vlan-2000)# no ipv6 mld snooping querier enable
```

Configuring and unconfiguring an MLD static group on a VLAN

You can forward traffic statically for a multicast group onto a specified interface, so that the interface behaves as if MLD were enabled.

1. To enable this functionality, use the **ipv6 mld snooping static-group** command on a VLAN interface, then select a multicast address to be joined, as well as a physical interface, as in the following example:

   ```
   device(config-Vlan-2000)# ipv6 mld snooping static-group ff1e::1 interface ethernet 0/1
   ```

2. To disable this functionality, use the **no ipv6 mld snooping static-group** command on a VLAN interface, as in the following example:

   ```
   device(config-Vlan-2000)# no ipv6 mld snooping static-group ff1e::1 interface ethernet 0/1
   ```

Enabling and disabling MLD fast-leave on a VLAN

MLD fast-leave allows a group entry to be removed immediately from the receiver as soon as a done message is received, as long as the receiver is the only one on the segment that is subscribed to a group. This minimizes the leave latency of group memberships on an interface, because the device does not send group-specific queries. As a result, the group entry is removed from the multicast forwarding table as soon as a group done (leave) message is received.

> NOTE
> Use the **ipv6 mld snooping fast-leave** command only if there is one receiver behind the interface for a given group.

Use the **ipv6 mld snooping fast-leave** command on a VLAN interface to enable MLD fast-leave.

```
device(config-Vlan-2000)# ipv6 mld snooping fast-leave
```

Use the **no ipv6 mld snooping fast-leave** command on a VLAN interface to disable MLD fast-leave.

```
device(config-Vlan-2000)# no ipv6 mld snooping fast-leave
```

Configuring the MLD query interval

You can configure the frequency at which MLD host query messages are sent. Larger values cause queries to be sent less often.

To set the MLD query interval, use the **ipv6 mld snooping query-interval** command on a VLAN interface, as in the following example:

```
device(config-Vlan-2000)# ipv6 mld snooping query-interval 1200
```

> NOTE
> The value set by the **ipv6 mld snooping query-interval** command must be greater than the query maximum response time, set by the **ipv6 mld query-max-response-time** command. Refer to the *Brocade SLX-OS Command Reference* for Brocade SLX 9140 and 9240 switches for all ranges and defaults for the commands in this section.

To restore the MLD query interval default value, use the **no ipv6 mld snooping query-interval** command on a VLAN interface:

```
device(config-Vlan-2000)# no ipv6 mld snooping query-interval
```

Configuring the MLD last-member query interval

You can set the frequency at which MLD last-member query messages are sent. This is the interval for the response to a query sent after a host leave message is received from the last known active host on the subnet. The group is deleted if no reports are received in this interval. This interval adjusts the speed at which messages are transmited on the subnet. Smaller values detect the loss of a group member faster.

> NOTE
> If the last-member query interval is not configured explicitly, the value is taken from the robustness variable.

To set the MLD last-member query interval, use the **ipv6 mld snooping last-member-query-interval** command on a VLAN interface:

```
switch(config-Vlan-2000)# ipv6 mld snooping last-member-query-interval 1500
```

To restore the default value, use the **no ipv6 mld snooping last-member-query-interval** command on a VLAN interface:

```
switch(config-Vlan-2000)# no ipv6 mld snooping last-member-query-interval
```

Configuring the MLD last-member query count

You can set the number of times that an MLD query is sent in response to a host leave message. This is the number of times, separated by the last-member query-response interval (configured by the **ipv6 mld last-member-query-interval** command), that an MLD query is sent in response to a host leave message from the last known active host on the subnet.

> NOTE
> If this interval is not configured explicitly, the value is taken from the robustness variable.

To change the MLD last-member query count from the default, use the **ipv6 mld last-member query count** command on a VLAN:

```
device(config-Vlan-2000)# ipv6 mld snooping last-member-query-count 3
```

To restore the default value, use the **no ipv6 mld last-member-query-count** command on a VLAN:

```
device(config-Vlan-2000)# no ipv6 mld snooping last-member-query-count
```

Configuring the MLD query maximum response time

You can configure the maximum response time for IPv6 MLDv1 snooping MLD queries for a specific VLAN interface:

```
device(config)# vlan 2
device(config Vlan-2)# ipv6 mld snooping query-max-response-time 15
```

> NOTE
> Larger values spread out host responses over a longer time. The value set by this command must be less than the general query interval, set by the **ipv6 mld query-interval** command.

To restore the default value, use the **no ipv6 mld query-max-response-time** command on a VLAN interface:

```
device(config-Vlan-2)# no ipv6 mld query-max-response-time
```

Configuring the MLD snooping robustness variable

A robustness value can be configured to compensate for packet loss in congested networks. This value determines the number of general MLD snooping queries that are sent before a multicast address is aged out for lack of a response. The default is 2.

To change the default robustness variable on a VLAN, use the **ipv6 mld snooping robustness-variable** command, as in the following example:

```
switch(config-Vlan-2000)# ipv6 mld snooping robustness-variable 7
```

To restore the default value, use the **no ipv6 snooping mld robustness-variable** command on a VLAN interface, as in the following example:

```
switch(config-Vlan-2000)# no ipv6 snooping mld robustness-variable
```

Configuring the MLD startup query count

The IPv6 MLDv1 startup query count is the number of queries that are separated by the startup interval. The default is 1.

Do the following to change the startup-query interval on a VLAN, as in the following example.

```
device(config-Vlan-2000)# ipv6 mld snooping startup-query-count 2
```

To restore the default value, use the **no ipv6 mld snooping startup-query-count** command on a VLAN interface, as in the following example:

```
device(config-Vlan-2000)# no ipv6 mld snooping startup-query-count
```

Configuring the MLD startup query interval

You can change the query interval between the general queries that are sent by the querier on startup. The default interval is 1. The querier may be the MLD snooping querier or an external querier.

To change the startup-query interval on a VLAN use **ipv6 mld startup-query-interval** command.

```
device(config-Vlan-2000)# ipv6 mld snooping startup-query-interval 2
```

To restore the default value, use the **no ipv6 mld snooping startup-query-interval** command on a VLAN interface:

```
device(config-Vlan-2000)# no ipv6 mld snooping startup-query-interval
```

Configuring a VLAN port member to be a multicast router port

You can configure a VLAN port member to be a multicast router (mrouter) port.

To configure a VLAN port member to be a multicast router (mrouter) port., use the **ipv6 mld snooping mrouter interface** command on a VLAN interface:

```
device(config-Vlan-2000)# ipv6 mld snooping mrouter interface ethernet 0/1
```

To disable the VLAN port member from being an mrouter port., use the **no ipv6 mld snooping mrouter interface** command on a VLAN interface:

```
device(config-Vlan-2000)# no ipv6 mld snooping mrouter interface ethernet 0/1
```

Monitoring and managing MLD snooping

You can monitor MLD snooping by using a variety of **show** commands.

In addition, you can clear the data for MLD groups and statistics by using **clear** commands. A **debug** command is also available. For command details, refer to the *Brocade SLX-OS Command Reference* for Brocade SLX 9140 and 9240 switches.

The following table lists the available **show** commands for MLD snooping.

TABLE 1 MLD snooping show commands

Command	Description
show ipv6 mld groups	Displays information about IPv6 MLDv1 groups.
show ipv6 mld snooping	Displays IPv6 MLD snooping details.
show ipv6 mld statistics	Displays IPv6 MLDv1 statistics.

The following table lists the available **clear** and **debug** commands.

TABLE 2 MLD snooping clear and debug commands

Command	Description
clear ipv6 mld groups	Clears IPv6 MLDv1 group cache entries.
clear ipv6 mld statistics	Clears IPv6 MLDv1 snooping statistics.
debug ipv6 mld	Displays information related to IPv6 MLD, with a variety of options.