## Contents

**Preface** ..................................................................................................................................... 5  
- Document conventions ........................................................................................................... 5  
- Text formatting conventions ................................................................................................. 5  
- Command syntax conventions ............................................................................................... 5  
- Notes, cautions, and warnings ............................................................................................... 6  
- Brocade resources .................................................................................................................. 7  
- Contacting Brocade Technical Support ................................................................................ 7  
- Document feedback ................................................................................................................ 8  

**About This Guide** .................................................................................................................... 9  

**IGMP and MLD overview** ......................................................................................................... 11  
- Comparing IGMP and MLD ..................................................................................................... 11  
- IGMP ........................................................................................................................................ 11  
  - Joining and leaving a multicast group by using IGMP .......................................................... 11  
  - IGMP messages ...................................................................................................................... 12  
  - IGMP versions ....................................................................................................................... 12  
- MLD ......................................................................................................................................... 12  
  - Joining and leaving a multicast group using MLD .............................................................. 12  
  - MLD messages ...................................................................................................................... 13  
  - MLD versions ....................................................................................................................... 14  
- Supported standards .................................................................................................................. 14  
- Supported MIBs ....................................................................................................................... 14  
- IGMP and MLD configuration ................................................................................................... 14  

**IGMP Commands** .................................................................................................................... 15  
- `interfaces <interface> ip igmp` .......................................................................................... 16  
- `interfaces <interface> ip igmp access-group <acl>` .......................................................... 19  
- `interfaces <interface> ip igmp enforce-router-alert` ....................................................... 20  
- `interfaces <interface> ip igmp immediate-leave group-list <acl>` ................................... 21  
- `interfaces <interface> ip igmp join-group <group>` ......................................................... 22  
- `interfaces <interface> ip igmp last-member-query-count <count>` .................................... 23  
- `interfaces <interface> ip igmp last-member-query-interval <interval>` ............................ 24  
- `interfaces <interface> ip igmp limit <limit>` ...................................................................... 25  
- `interfaces <interface> ip igmp limit-exception <acl>` ....................................................... 26  
- `interfaces <interface> ip igmp offlink` .............................................................................. 27  
- `interfaces <interface> ip igmp querier-timeout <interval>` .............................................. 28  
- `interfaces <interface> ip igmp query-interval <interval>` ............................................... 29  
- `interfaces <interface> ip igmp query-max-response-time <interval>` ............................... 30  
- `interfaces <interface> ip igmp robustness-variable <variable>` ....................................... 31  
- `interfaces <interface> ip igmp startup-query-count <count>` ......................................... 32  
- `interfaces <interface> ip igmp startup-query-interval <interval>` ...................................... 33  
- `interfaces <interface> ip igmp version <version>` ............................................................. 34  
- `interfaces <interface> ip igmp static-group <group> source <source>` ............................ 35  
- `monitor protocol multicast` .................................................................................................. 36  
- `protocols igmp limit <limit>` ............................................................................................. 37  
- `protocols igmp log` ............................................................................................................ 38
protocols igmp ssm-map
protocols igmp ssm-map static access-list <acl> source <source>
reset ip igmp
show ip igmp
show ip igmp interface
show ip igmp ssm-map
show monitoring protocols multicast igmp

MLD Commands
interfaces <interface> ipv6 mld
interfaces <interface> ipv6 mld access-group <acl6-name>
interfaces <interface> ipv6 mld immediate-leave group-list <acl6-name>
interfaces <interface> ipv6 mld last-member-query-count <count>
interfaces <interface> ipv6 mld last-member-query-interval <interval>
interfaces <interface> ipv6 mld limit <limit>
interfaces <interface> ipv6 mld limit-except <acl6-name>
interfaces <interface> ipv6 mld querier-timeout <interval>
interfaces <interface> ipv6 mld query-interval <interval>
interfaces <interface> ipv6 mld query-max-response-time <interval>
interfaces <interface> ipv6 mld robustness-variable <variable>
interfaces <interface> ipv6 mld static-group <group> source <source>
interfaces <interface> ipv6 mld version <version>
monitor protocol multicast
protocols mld limit <limit>
protocols mld log
protocols mld ssm-map
protocols mld ssm-map static <acl6-name> source <source>
reset ipv6 mld
show ipv6 mld groups
show ipv6 mld interface
show ipv6 mld ssm-map
show monitoring protocols multicast mld

List of Acronyms
Document conventions

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

Text formatting conventions

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

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>Identifies command names</td>
</tr>
<tr>
<td></td>
<td>Identifies keywords and operands</td>
</tr>
<tr>
<td></td>
<td>Identifies the names of user-manipulated GUI elements</td>
</tr>
<tr>
<td></td>
<td>Identifies text to enter at the GUI</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Identifies emphasis</td>
</tr>
<tr>
<td></td>
<td>Identifies variables</td>
</tr>
<tr>
<td></td>
<td>Identifies document titles</td>
</tr>
<tr>
<td><strong>Courier font</strong></td>
<td>Identifies CLI output</td>
</tr>
<tr>
<td></td>
<td>Identifies command syntax examples</td>
</tr>
</tbody>
</table>

Command syntax conventions

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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>Identifies command names, keywords, and command options.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Identifies a variable.</td>
</tr>
<tr>
<td>value</td>
<td>In Fibre Channel products, a fixed value provided as input to a command</td>
</tr>
<tr>
<td></td>
<td>option is printed in plain text, for example, <code>show WWN</code></td>
</tr>
</tbody>
</table>
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.
Brocade resources

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

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.

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

<table>
<thead>
<tr>
<th>Online</th>
<th>Telephone</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred method of contact for non-urgent issues:</td>
<td>Required for Sev 1-Critical and Sev 2-High issues:</td>
<td><a href="mailto:support@brocade.com">support@brocade.com</a></td>
</tr>
<tr>
<td>• My Cases through MyBrocade</td>
<td>• Continental US: 1-800-752-8061</td>
<td>Please include:</td>
</tr>
<tr>
<td>• Software downloads and licensing tools</td>
<td>• Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33)</td>
<td>• Problem summary</td>
</tr>
<tr>
<td>• Knowledge Base</td>
<td>• For areas unable to access toll free number: +1-408-333-6061</td>
<td>• Serial number</td>
</tr>
<tr>
<td></td>
<td>• Toll-free numbers are available in many countries.</td>
<td>• Installation details</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Environment description</td>
</tr>
</tbody>
</table>

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.

Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

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.
About This Guide

This guide describes how to configure IGMP and MLD on the Brocade vRouter (referred to as a virtual router, vRouter, or router in the guide).
Comparing IGMP and MLD

One of the main aspects of multicast routing is managing the network devices that receive the multicast. The key abstraction in multicasting is the multicast group: a given multicast stream is associated with a group, which is identified by a specific multicast IP address. Group members receive the multicast stream; nonmembers do not.

In IPv4 networks, multicast group membership is managed by using IGMP. In IPv6, the corresponding protocol for managing group membership is MLD. For more information on multicast routing fundamentals and Protocol Independent Multicast (PIM), refer to Brocade 5600 vRouter Multicast Routing Reference Guide and Brocade 5600 vRouter PIM Reference Guide.

IGMP

This section presents the following topics:

- Joining and leaving a multicast group by using IGMP on page 11
- IGMP messages on page 12
- IGMP versions on page 12

Joining and leaving a multicast group by using IGMP

This section describes the behavior of IGMP version 2.

IGMP allows a network host to inform a router that it is interested in receiving a particular multicast stream.

To begin, the multicast group is assigned a multicast address (that is, an IP address in the 224.0.0.0/4 address space). Hosts register to receive the stream join the group by sending an IGMP Report to the upstream multicast router. The router then adds that group to the list of multicast groups that should be forwarded onto the local subnet.

The router does not maintain state about which hosts on the subnet are to receive traffic for the group. Instead, the router continues to send traffic to the subnet until either a timeout value expires or there are no more hosts in that group on the subnet.

When a host no longer wants to receive multicast traffic, it sends the router an IGMP Leave message. After receiving this message, the router sends a query to the local subnet to determine whether any
group members remain, sending the message to all hosts on the subnet, at the multicast All-Hosts address (224.0.0.1). If any host responds, the router continues to send to the group; if not, the router removes the multicast group from its forwarding list and stops sending to the group.

NOTE
The behavior of IGMP version 1 and version 3 varies from version 2.

IGMP messages

IGMP communicates in three types of messages:

• Report (Join): A host sends an unsolicited message to the upstream multicast router signaling that it wants to become a member of a specific multicast group.
• Leave Group (Leave): A host in a multicast group sends a message to the upstream multicast router signaling that it is leaving a multicast group.
• Query: The multicast router sends a message to the local router to determine which groups have members on the attached network, or to determine if a specific group has members on the attached network.

IGMP versions

Three versions of IGMP are specified:

• IGMPv1, defined by RFC 1112, *Host Extensions for IP Multicasting*
• IGMPv2, defined by RFC 2236, *Internet Group Management Protocol, Version 2*

Relative to IGMPv1, IGMPv2 adds the ability for a host to leave a multicast group. Relative to IGMPv2, IGMPv3 adds support for source-specific multicast. For more information on IGMPv3 support for source-specific multicast, refer to *Brocade 5600 vRouter Multicast Routing Reference Guide*.

MLD

This section presents the following topics:

• Joining and leaving a multicast group using MLD on page 12
• MLD messages on page 13
• MLD versions on page 14

Joining and leaving a multicast group using MLD

MLD exchanges group information between hosts and multicast routers on IPv6 networks. MLD is based on IGMP; however, while IGMP is a distinct transport-layer protocol, MLD is an extension of Internet Control Message Protocol for Internet Protocol version 6 (ICMPv6).

An IPv6 host that wants to receive a multicast stream joins the multicast group by sending a Multicast Listener Report message with the multicast group of interest as the destination address. The router registers the host for that multicast group and forwards multicast traffic to the local network.
An IPv6 host in a multicast group also receives Report messages sent to the multicast address from other hosts joining the group. Having hosts track these Reports allows the network to manage the MLD leave process.

When a host leaves a multicast group, it checks to see whether it ever received a Report for another host in the group. If not, the host knows it was the last host to join the group. In this case, the host sends a Multicast Listener Done message to signal the router that it is leaving the group. The message is sent to the IPv6 All-Routers multicast group address (FF02::2).

When the router receives a Done message, it responds with a multicast address-specific Multicast Listener Query. The Query requests any remaining group members to report their existence with a Report message. If any group member responds to the Query, the router continues multicast forwarding for this group. If no host responds, the router stops forwarding.

**MLD messages**

MLD messages usually use the IPv6 link-local as the source address. The hop limit is always set to 1, to prevent the router from forwarding the message. MLD messages are of three types:

- Multicast listener report
- Multicast listener done
- Multicast listener query

**Multicast listener report**

The Multicast Listener Report message is sent by a listening IPv6 host. The message either is unsolicited, sent to report its interest in receiving specific multicast traffic, or sent to respond to a Multicast Listener Query message from the multicast router.

The Multicast Listener Report message is equivalent to an IGMPv2 Host Membership Report message. It is ICMPv6 message type 131.

**Multicast listener done**

The Multicast Listener Done message is sent by a host in a specific multicast group to the multicast router, to signal the router that there may not be any further group members on the local subnet. When the router receives a Done message, it queries the subnet for further group members by sending a Multicast Listener Query message.

The Multicast Listener Report message is equivalent to an IGMPv2 Leave Group message. It is ICMPv6 message type 132.

**Multicast listener query**

The Multicast Listener Query message is sent by the multicast router to a local subnet, to determine whether any multicast group members still exist on the subnet. Multicast Listener Query messages are of two types:

- General: The router periodically sends a general Query to poll all hosts on the subnet for the presence of any multicast address. Link-local addresses, the All-Nodes multicast address (FF02::1), and reserved multicast addresses (addresses with a scope of 0) and interface-local addresses (addresses with a scope of 1) are excluded from the poll.
- Multicast-address-specific. The router sends a multicast-address-specific query only to members of a specific multicast group on the subnet.
The Multicast Listener Report message is equivalent to an IGMPv2 Host Membership Query message. It is ICMPv6 message type 130.

**MLD versions**

Two versions of MLD are specified:

- MLDv1, defined by RFC 2710, *Multicast Listener Discovery for IPv6*
- MLDv2, defined by RFC 3810, *Multicast Listener Discovery version 2 (MLDv2) for IPv6*

MLDv1 is based on IGMPv2. MLDv2 is based on IGMPv3.

In addition, RFC 4604: *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast* extends MLD to support source-specific multicast. For more information, refer to *Brocade 5600 vRouter Multicast Routing Reference Guide*.

**Supported standards**

The Brocade implementation of IGMP and MLD complies with the following standards:

- RFC 1112: *Host Extensions for IP Multicasting*
- RFC 2710: *Multicast Listener Discovery (MLD) for IPv6*
- RFC 3376: *Internet Group Management Protocol, Version 3*
- RFC 3810: *Multicast Listener Discovery version 2 (MLDv2) for IPv6*
- RFC 4604: *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*

**Supported MIBs**

The Brocade implementation of IGMP supports the following Simple Management Network Protocol (SNMP) management information bases (MIBs).

- IGMP-MIB, RFC2933: *Internet Group Management Protocol MIB*
- IPMROUTE, RFC 2932: *IPv4 Multicast Routing MIB*
- MLD-MIB, RFC 3019: *IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol*

For a list of all MIBs supported, refer to *Brocade 5600 vRouter Remote Management Reference Guide*.

**IGMP and MLD configuration**

IGMP and MLD configurations depend on other multicast-related commands. For this reason, the configuration examples are located elsewhere. For IGMP and MLD configuration examples, refer to *Brocade 5600 vRouter Multicast Routing Reference Guide*.
IGMP Commands

- `interfaces <interface> ip igmp` ........................................................................................................ 16
- `interfaces <interface> ip igmp access-group <acl>` ......................................................................... 19
- `interfaces <interface> ip igmp enforce-router-alert` ........................................................................ 20
- `interfaces <interface> ip igmp immediate-leave group-list <acl>` .................................................. 21
- `interfaces <interface> ip igmp join-group <group>` ........................................................................ 22
- `interfaces <interface> ip igmp last-member-query-count <count>` ................................................... 23
- `interfaces <interface> ip igmp last-member-query-interval <interval>` ........................................... 24
- `interfaces <interface> ip igmp limit <limit>` .................................................................................. 25
- `interfaces <interface> ip igmp limit-exception <acl>` ..................................................................... 26
- `interfaces <interface> ip igmp offlink` .......................................................................................... 27
- `interfaces <interface> ip igmp querier-timeout <interval>` ............................................................... 28
- `interfaces <interface> ip igmp query-interval <interval>` ............................................................... 29
- `interfaces <interface> ip igmp query-max-response-time <interval>` .............................................. 30
- `interfaces <interface> ip igmp robustness-variable <variable>` .................................................... 31
- `interfaces <interface> ip igmp startup-query-count <count>` .......................................................... 32
- `interfaces <interface> ip igmp startup-query-interval <interval>` ..................................................... 33
- `interfaces <interface> ip igmp version <version>` ........................................................................ 34
- `interfaces <interface> ip igmp static-group <group> source <source>` ........................................ 35
- `monitor protocol multicast` ........................................................................................................... 36
- `protocols igmp limit <limit>` ......................................................................................................... 37
- `protocols igmp log` ..................................................................................................................... 38
- `protocols igmp ssm-map` ............................................................................................................... 39
- `protocols igmp ssm-map static access-list <acl> source <source>` ............................................. 40
- `reset ip igmp` .............................................................................................................................. 41
- `show ip igmp groups` ................................................................................................................... 42
- `show ip igmp interface` ............................................................................................................... 43
- `show ip igmp ssm-map` ............................................................................................................... 44
- `show monitoring protocols multicast igmp` .................................................................................... 45
interfaces <interface> ip igmp

Enables IGMP on an interface.

Syntax

set interfaces interface ip igmp

delete interfaces interface ip igmp

show interfaces interface ip igmp

Parameters

interface

The type of interface. For detailed keywords and arguments for interfaces that support multicast routing, see the table in the Usage Guidelines below.

Modes

Configuration mode

Configuration Statement

interfaces interface {
  ip {
    igmp {
    }
  }
}

Usage Guidelines

Use this command to enable the Internet Group Management Protocol (IGMP) on an interface.

NOTE

Enabling IP on an interface enables the host side functionality of IGMP by default. The set interfaces interface ip igmp command enables the router side functionality of the IGMP on the given interface.

NOTE

To use IGMP for multicast routing, multicast routing must be enabled on the router. For information about multicast routing in general, see the Brocade 5600 vRouter Multicast Routing Reference Guide.

The following table shows the syntax and parameters for interface types. Some of these types may not apply to this command.

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Syntax</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bonding</td>
<td>bonding bondx</td>
<td>bondx: The identifier of a bonding interface. The identifier ranges from bond0 through bond99.</td>
</tr>
<tr>
<td>Bonding vif</td>
<td>bonding bondx vif vlan-id</td>
<td>bondx: The identifier of a bonding interface. The identifier ranges from bond0 through bond99. vlan-id: The VLAN ID of a vif. The ID ranges from 1 through 4094.</td>
</tr>
<tr>
<td>Bridge</td>
<td>bridge brx</td>
<td>brx: The name of a bridge group. The name ranges from br0 through br999.</td>
</tr>
<tr>
<td>Ethernet PPoE</td>
<td>ethernet ethx pppoe num</td>
<td>ethx: The name of an Ethernet interface. The name ranges from eth0 through eth23, depending on the physical interfaces available on your system. num: The name of a defined PPPoE unit. The name ranges from 0 through 15.</td>
</tr>
<tr>
<td>Interface Type</td>
<td>Syntax</td>
<td>Parameters</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Ethernet vif  | ethernet ethx vif vlan-id pppoe num | *ethx: The name of an Ethernet interface. The name ranges from eth0 through eth23, depending on the physical interfaces available on your system.  
  *vlan-id: The VLAN ID of a vif. The ID ranges from 1 through 4094.  
  *num: The name of a defined PPPoE unit. The name ranges from 0 through 15. |
| Data plane    | dataplane dp{x}y{z}v             | *dp{x}y{z}v: The name of a data plane interface to which the following applies:  
  - *dp identifies a data plane ID  
  - *x identifies a data plane ID  
  - *y specifies a physical or virtual PCI slot index  
  - *z specifies a port index  

**NOTE**  
Currently, only dp0 is supported.

- *py specifies a physical or virtual PCI slot index  
- *pz specifies a port index

Other supported name formats are the following:  
- *dp{x}emy—used for LAN-on-motherboard (LOM) devices that do not have a PCI slot. *emy specifies an embedded network interface number.  
- *dp{x}porty—used for devices in which the PCI slot cannot be identified. *porty specifies a port index. |

| Data plane vif | dataplane dp{x}y{z}v vif [vlan vlan-id ] | dp{x}y{z}v: The name of a data plane interface to which the following applies:  
  - *dp identifies a data plane ID  
  - *x identifies a data plane ID  
  - *y specifies a physical or virtual PCI slot index  
  - *z specifies a port index  

**NOTE**  
Currently, only dp0 is supported.

- *py specifies a physical or virtual PCI slot index  
- *pz specifies a port index

Other supported name formats are the following:  
- *dp{x}emy—used for LAN-on-motherboard (LOM) devices that do not have a PCI slot. *emy specifies an embedded network interface number.  
- *dp{x}porty—used for devices in which the PCI slot cannot be identified. *porty specifies a port index.  

*vlan-id: A virtual interface ID. The ID ranges from 1 through 4094.  
*vlan-id: The VLAN ID of a virtual interface. The ID ranges from 1 through 4094. |
<p>| Loopback      | loopback lo                      | *lo: The name of a loopback interface.                                       |
| OpenVPN       | openvpn vtunx                     | *vtunx: The identifier of an OpenVPN interface. The identifier ranges from vtun0 through vtunx, where *x is a nonnegative integer. |
| Pseudo-Ethernet| pseudo-ethernet pethx            | *pethx: The name of a pseudo-Ethernet interface. The name ranges from peth0 through peth999. |</p>
<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Syntax</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel</td>
<td>tunnel tunx</td>
<td>tunx: The identifier of a tunnel interface you are defining. The identifier ranges from tun0 through tunx, where x is a nonnegative integer.</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tunnel tunx</td>
<td></td>
</tr>
<tr>
<td></td>
<td>parameters</td>
<td></td>
</tr>
<tr>
<td>Virtual tunnel</td>
<td>vti vtix</td>
<td>vtix: The identifier of a virtual tunnel interface you are defining. The identifier ranges from vti0 through vtix, where x is a nonnegative integer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This interface does not support IPv6.</td>
</tr>
<tr>
<td>VRRP</td>
<td>interface parent-if</td>
<td>parent-if: The type and identifier of a parent interface; for example, dataplane dp0p1p2 or bridge br999.</td>
</tr>
<tr>
<td></td>
<td>vrrp vrrp-group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>group interface</td>
<td>group: A VRRP group identifier.</td>
</tr>
</tbody>
</table>

The name of a VRRP interface is not specified. The system internally constructs the interface name from the parent interface identifier plus the VRRP group number; for example, dp0p1p2v99. Note that VRRP interfaces support the same feature set as the parent interface does.

Use the **set** form of this command to enable IGMP on an interface.

Use the **delete** form of this command to remove all IGMP configuration and disable IGMP on an interface.

Use the **show** form of this command to display IGMP configuration.
interfaces <interface> ip igmp access-group <acl>

Controls the multicast local membership groups learned on an interface.

Syntax

set interfaces interface ip igmp access-group acl

delete interfaces interface ip igmp access-group

show interfaces interface ip igmp access-group

Parameters

- **interface**
  - The type of interface. For a list of supported interfaces and detailed syntax, see interfaces <interface> ip igmp on page 16.

- **acl**
  - A standard IP access list number to be used for filtering membership groups. The range is 1 to 99. Access control lists are a type of routing policy; see the Brocade 5600 vRouter Routing Policies Reference Guide for information on creating them.

Modes

Configuration mode

Configuration Statement

```
interfaces interface {
    ip {
        igmp {
            access-group acl
        }
    }
}
```

Usage Guidelines

Use this command to use an access control list to control multicast local membership groups learned on an interface.

Use the **set** form of this command to apply the access control list.

Use the **delete** form of this command to stop access-list filtering for IGMP.

Use the **show** form of this command to show access-list configuration for IGMP.
interfaces <interface> ip igmp enforce-router-alert

Enables strict Router Advertisement validation for IGMP.

Syntax

set interfaces interface ip igmp enforce-router-alert
delete interfaces interface ip igmp enforce-router-alert
show interfaces interface ip igmp enforce-router-alert

Command Default
A strict Router Advertisement validation is disabled.

Parameters

interface

The type of interface. For a list of supported interfaces and detailed syntax, see interfaces <interface> ip igmp on page 16.

Modes
Configuration mode

Configuration Statement

interfaces interface {
  ip {
    igmp {
      enforce-router-alert
    }
  }
}

Usage Guidelines
Use this command to put strict Router Advertisement (RA) validation into effect for IGMP.

RA validation helps prevent against spoofing attacks. When strict RA validation is in effect, the router silently discards any received RA messages that do not satisfy the validity checks specified in RFC 2461.

Use the set form of this command to enable strict RA validation.

Use the delete form of this command to restore the default behavior.

Use the show form of this command to show RA validation configuration.
interfaces <interface> ip igmp immediate-leave group-list <acl>

Minimizes latency for hosts leaving multicast groups.

**Syntax**

- set interfaces interface immediate-leave group-list acl
- delete interfaces interface immediate-leave group-list
- show interfaces interface immediate-leave group-list

**Command Default**
Immediate leave is disabled.

**Parameters**

- **interface**
  The type of interface. For a list of supported interfaces and detailed syntax, see interfaces <interface> ip igmp on page 16.

- **acl**
  An access list number used to define the membership group. Supported ranges of values are:
  - 1 to 99: IP access list number.
  - 1300 to 1999: IP access list number in the expanded range.
  
  Access control lists are a type of routing policy; see the Brocade 5600 vRouter Routing Policies Reference Guide for information on creating them.

**Modes**

Configuration mode

**Configuration Statement**

```
interfaces interface {
  ip {
    igmp {
      immediate-leave group-list acl
    }
  }
}
```

**Usage Guidelines**

Use this command to minimize the leave latency in IGMPv2 for IGMP memberships.

When this option is not set, the router sends an IGMP Query message when a receiver host has sent a Leave message. At this point, a timeout interval goes into effect. When this option is set, the Leave message is acted on immediately, without sending the Query or waiting for the timeout period to expire.

This command applies to IGMPv2, and it applies in situations where only one receiver is connected to each interface.

Use the **set** form of this command to enable IGMPv2 immediate leave.

Use the **delete** form of this command to restore the IGMPv2 immediate leave default behavior.

Use the **show** form of this command to view IGMPv2 immediate leave configuration.
interfaces <interface> ip igmp join-group <group>

Allows the router to join a multicast group.

Syntax

set interfaces interface ip igmp join-group group [source source]
delete interfaces interface ip igmp join-group group
show interfaces interface ip igmp join-group group

Parameters

interface
The type of interface. For a list of supported interfaces and detailed syntax, see interfaces <interface> ip igmp on page 16.
group
The multicast group being joined. The format is an IPv4 multicast address.
source
In source-specific multicast, the multicast source. The format is an IPv4 host address.

Modes
Configuration mode

Configuration Statement

interfaces interface {
  ip {
    igmp {
      join-group group
        source source
    }
  }
}

Usage Guidelines
Use this command to add the router to a multicast group.
Use the set form of this command to add the router to a multicast group.
Use the delete form of this command to have the router leave a multicast group.
Use the show form of this command to show multicast group membership configuration.
Manually sets the last member query count value.

**Syntax**

```
set interfaces interface ip igmp last-member-query-count count
```

```
delete interfaces interface ip igmp last-member-query-count
```

```
show interfaces interface ip igmp last-member-query-count
```

**Command Default**
The router sends two IGMP Query messages, after which it considers the host to have left the group.

**Parameters**

```
interface
```

The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ip igmp` on page 16.

```
count
```

The number of times the router sends a Query message after receiving a Leave message. The range is 2 to 7. The default is 2.

**Modes**

Configuration mode

**Configuration Statement**

```
interfaces interface {
  ip {
    igmp {
      last-member-query-count count
    }
  }
}
```

**Usage Guidelines**

Use this command to set the number of times that the router sends a group-specific or source-group specific Query message when it receives a Leave message from a receiver host.

The router uses this Query to determine whether any members of the multicast group remain on the network. The command is sent at the interval set in `interfaces <interface> ip igmp last-member-query-interval <interval>` on page 24. If the router receives no response to the configured number of queries, the router stops forwarding to that network.

Use the `set` form of this command to set the number of last-member queries sent.

Use the `delete` form of this command to restore the default value for last-member queries.

Use the `show` form of this command to show last-member query configuration.
**interfaces <interface> ip igmp last-member-query-interval <interval>**

Specifies the frequency at which IGMP group-specific host queries are sent.

**Syntax**

```
set interfaces interface ip igmp last-member-query-interval interval
```

```
delete interfaces interface ip igmp last-member-query-interval
```

```
show interfaces interface ip igmp last-member-query-interval
```

**Command Default**
The router waits 1000 milliseconds between last-member queries.

**Parameters**

- `interface`
  
The type of interface. For a list of supported interfaces and detailed syntax, see interfaces <interface> ip igmp on page 16.

- `interval`
  
The interval between last-member queries, in milliseconds. The range is 1000 to 25500. The default is 1000.

**Modes**

Configuration mode

**Configuration Statement**

```
interfaces interface {
  ip {
    igmp {
      last-member-query-interval interval
    }
  }
}
```

**Usage Guidelines**

Use this command to set the interval between IGMP group-specific or source specific Query messages sent by the router to determine whether any receivers remain in a multicast group.

The router uses this Query to determine whether any members of the multicast group remain on the network. If it receives no response to the configured number of queries (as set in interfaces <interface> ip igmp last-member-query-count <count> on page 23), the router stops forwarding to that network.

Use the `set` form of this command to set the interval for last-member queries.

Use the `delete` form of this command to restore the default interval for last-member queries.

Use the `show` form of this command to show last-member query interval configuration.
interfaces <interface> ip igmp limit <limit>

Sets the limit for IGMP group memberships on an interface.

**Syntax**

- `set interfaces <interface> ip igmp limit <limit>`
- `delete interfaces <interface> ip igmp limit <limit>`
- `show interfaces <interface> ip igmp limit`

**Parameters**

- **interface**
  
  The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ip igmp` on page 16.

- **limit**
  
  The maximum number of multicast group memberships that can be defined for the network served by the interface. The range is 1 to 2097152. By default, no limit is applied.

**Modes**

Configuration mode

**Configuration Statement**

```
interfaces interface {
    ip {
        igmp {
            limit limit
        }
    }
}
```

**Usage Guidelines**

Use this command to set an interface-specific limit on the number of multicast group memberships to be served by an interface. You can use this option to override the global limit set using `protocols igmp limit <limit>` on page 37.

When this option is in effect and the maximum is reached, the router ignores all further local requests for membership.

Use the `set` form of this command to set the limit on multicast group memberships on an interface.

Use the `delete` form of this command to restore the default behavior for multicast group membership limits.

Use the `show` form of this command to show group membership limit configuration.
interfaces <interface> ip igmp limit-exception <acl>

Specifies multicast groups unaffected by the IGMP group membership limits on an interface.

Syntax

```
set interfaces interface ip igmp limit-exception acl
delete interfaces interface ip igmp limit-exception acl
show interfaces interface ip igmp limit-exception
```

Parameters

- **interface**
  The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ip igmp` on page 16.

- **acl**
  An access list number used to define the membership group. Supported ranges of values are:
  - 1 to 99: IP access list number.
  - 1300 to 1999: IP access list number in the expanded range.

  Access control lists are a type of routing policy; see the `Brocade 5600 vRouter Routing Policies Reference Guide` for information on creating them.

Modes

- **Configuration mode**

  Configuration Statement

  ```
  interfaces interface {
    ip {
      igmp {
        limit-exception acl
      }
    }
  }
  ```

Usage Guidelines

Use this command to specify the multicast groups that are an exception to the membership limits imposed by `interfaces <interface> ip igmp limit <limit>` on page 25. As such, this command is dependent on `interfaces <interface> ip igmp limit <limit>` on page 25 being set.

Use the `set` form of this command to specify the multicast groups that are unaffected by the IGMP group membership limits on an interface.

Use the `delete` form of this command to remove the list of multicast groups that are unaffected by the IGMP group membership limits on an interface.

Use the `show` form of this command to show group membership limit exception configuration.
interfaces <interface> ip igmp offlink

Allows multicast transmissions to be forwarded off-link.

Syntax

set interfaces interface ip igmp offlink

delete interfaces interface ip igmp offlink

show interfaces interface ip igmp offlink

Parameters

interface

The type of interface. For a list of supported interfaces and detailed syntax, see interfaces <interface> ip igmp on page 16.

Modes

Configuration mode

Configuration Statement

interfaces interface {
    ip {
        igmp {
            offlink
        }
    }
}

Usage Guidelines

Use this command to enable IGMP off-link on the system.

Use the set form of this command to set IGMP off-link.

Use the delete form of this command to delete IGMP off-link.

Use the show form of this command to show IGMP interface configuration.
interfaces <interface> ip igmp querier-timeout <interval>

Sets the interval before the system takes over as querier on an interface.

Syntax

```
set interfaces interface ip igmp querier-timeout interval
```

```
delete interfaces interface ip igmp querier-timeout
```

```
show interfaces interface ip igmp querier-timeout
```

Command Default

The router waits to receive a query for 255 seconds before taking over as querier.

Parameters

```
interface
```

The type of interface. For a list of supported interfaces and detailed syntax, see interfaces <interface> ip igmp on page 16.

```
interval
```

The amount of time, in seconds, the router waits before taking over as querier when the previous querier fails to send an IGMP Query. The range is 60 to 300. The default is 255.

Modes

Configuration mode

Configuration Statement

```
interfaces interface {
  ip {
    igmp {
      querier-timeout interval
    }
  }
}
```

Usage Guidelines

Use this command to specify how long the router waits to receive an IGMP query from the previous querier. When this interval expires, the router takes over as querier.

Use the `set` form of this command to set the querier timeout interval.

Use the `delete` form of this command to restore the default querier timeout interval.

Use the `show` form of this command to show querier timeout interval configuration.
interfaces <interface> ip igmp query-interval <interval>

Specifies the frequency at which IGMP host queries are sent.

Syntax

set interfaces interface ip igmp query-interval interval
delete interfaces interface ip igmp query-interval
show interfaces interface ip igmp query-interval

Command Default

The router sends IGMP Query messages at intervals of 125 seconds.

Parameters

interface
The type of interface. For a list of supported interfaces and detailed syntax, see interfaces <interface> ip igmp on page 16.

interval
The interval, in seconds, at which the router sends IGMP Query messages. The range is 2 to 18000. The default is 125.

Modes

Configuration mode

Usage Guidelines

Use this command to set the frequency with which the router sends IGMP host Query messages.

NOTE

The interval for query-interval must be greater than the interval for query-max-response-time used in interfaces <interface> ip igmp query-max-response-time <interval> on page 30.

Use the set form of this command to set the query interval.
Use the delete form of this command to restore the default query interval.
Use the show form of this command to show query interval configuration.
interfaces <interface> ip igmp query-max-response-time <interval>

Specifies the maximum response time advertised in IGMP queries.

Syntax

set interfaces interface ipigmp query-max-response-time interval

delete interfaces interface ipigmp query-max-response-time

show interfaces interface ipigmp query-max-response-time

Command Default

The router waits 10 seconds for a response to an IGMP Query before deleting the multicast group.

Parameters

interface

The type of interface. For a list of supported interfaces and detailed syntax, see interfaces <interface> ip igmp on page 16.

interval

The amount of time, in seconds, that the router advertises as the maximum delay before a responder can respond to an IGMP Query. The range is 1 to 240. The default is 20.

Modes

Configuration mode

Configuration Statement

interfaces interface {
    ip {
        igmp {
            query-max-response-time interval
        }
    }
}

Usage Guidelines

Use this command to set the value to be advertised as the maximum time the router will wait to receive a response to IGMP Query messages. When this interval expires, the router deletes the multicast group.

Use the set form of this command to set the maximum query response time.

Use the delete form of this command to restore the default maximum query response time.

Use the show form of this command to show maximum query response time configuration.
interfaces <interface> ip igmp robustness-variable <variable>

Specifies the value of the robustness variable on an interface.

Syntax

set interfaces interface ip igmp robustness-variable variable
delete interfaces interface ip igmp robustness-variable
show interfaces interface ip igmp robustness-variable

Command Default
The robustness variable is set to 2.

Parameters

interface
The type of interface. For a list of supported interfaces and detailed syntax, see interfaces <interface> ip igmp on page 16.

variable
The value for the robustness variable. The range is 2 to 7. The default is 2.

Modes
Configuration mode

Configuration Statement

interfaces interface {
  ip {
    igmp {
      robustness-variable variable
    }
  }
}

Usage Guidelines
Use this command to set the robustness variable for an interface.

The robustness variable specifies how many IGMP refresh packets for a given state can be lost before the system times out and changes state. This helps tune the network for expected packet loss.

Use the set form of this command to set the robustness variable value.

Use the delete form of this command to restore the default robustness variable value.

Use the show form of this command to show robustness variable configuration.
interfaces <interface> ip igmp startup-query-count <count>

Specifies the number of IGMP Query messages to be sent on startup for an interface.

**Syntax**

- **set interfaces interface ip igmp startup-query-count count**
- **delete interfaces interface ip igmp startup-query-count**
- **show interfaces interface ip igmp startup-query-count**

**Command Default**

Two IGMP Query messages are sent when the router starts up.

**Parameters**

- **interface**
  
  The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ip igmp` on page 16.

- **count**
  
  The number of IGMP Query messages to be sent when the router starts up.
  
  The range is 2 to 10. The default is 2.

**Modes**

Configuration mode

**Configuration Statement**

```plaintext
interfaces interface {
  ip {
    igmp {
      startup-query-count count
    }
  }
}
```

**Usage Guidelines**

Use this command to specify the number of IGMP Query messages to be sent when the router starts up.

Use the **set** form of this command to set the query startup count.

Use the **delete** form of this command to restore the default value for query startup count.

Use the **show** form of this command to show query startup count configuration.
interfaces <interface> ip igmp startup-query-interval <interval>

Sets the interval at which IGMP Query messages will be sent on startup for an interface.

**Syntax**

- set interfaces interface ip igmp startup-query-interval interval
- delete interfaces interface ip igmp startup-query-interval
- show interfaces interface ip igmp startup-query-interval

**Command Default**

At startup, Query messages are sent at 31-second intervals.

**Parameters**

- **interface**
  - The type of interface. For a list of supported interfaces and detailed syntax, see interfaces <interface> ip igmp on page 16.

- **interval**
  - The interval, in seconds, between IGMP Query messages sent when the router starts up. The range is 1 to 18000. The default is 31.

**Modes**

Configuration mode

**Configuration Statement**

```
interfaces interface {
  ip {
    igmp {
      startup-query-interval interval
    }
  }
}
```

**Usage Guidelines**

Use this command to specify the interval at which IGMP query messages are sent when the router starts.

Use the set form of this command to set the query startup interval.

Use the delete form of this command to restore the default query startup interval.

Use the show form of this command to show query startup interval configuration.
interfaces <interface> ip igmp version <version>

Sets the IGMP version in use on an interface.

Syntax

- `set interfaces interface ip igmp version version`
- `delete interfaces interface ip igmp version`
- `show interfaces interface ip igmp version`

Command Default

- IGMPv3 is used on the router.

Parameters

- `interface`
  - The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ip igmp` on page 16.

- `version`
  - The IGMP version number. Supported values are 1, 2, and 3. The default is 3.

Modes

- Configuration mode

Configuration Statement

```plaintext
interfaces interface {
    ip {
        igmp {
            version version
        }
    }
}
```

Usage Guidelines

- Use this command to specify which IGMP version the router should use for multicast routing.
- Use the `set` form of this command to set the IGMP version number.
- Use the `delete` form of this command to restore the default IGMP version number.
- Use the `show` form of this command to show IGMP version number configuration.
interfaces <interface> ip igmp static-group <group> source <source>

Specifies static multicast group membership on an interface.

Syntax

**set interfaces** interface ip igmp static-group group source source

**delete interfaces** interface ip igmp static-group group source source

**show interfaces** interface ip igmp static-group group source source

Parameters

- **interface**: The type of interface. For a list of supported interfaces and detailed syntax, see *interfaces <interface> ip igmp* on page 16.
- **group**: The IP multicast address of the group the router is being made a member of.
- **source**: The static source of multicast packets. Supported values are:
  - *x.x.x.x*: The IP address of a multicast source.
  - **ssm-map**: Use Source Specific Multicast (SSM) mapping to determine the multicast source associated with this group.

Modes

- **Configuration mode**

Configuration Statement

```plaintext
interfaces interface {
  ip {
    igmp {
      static-group group {
        source source
      }
    }
  }
}
```

Usage Guidelines

Use this command to specify static multicast group membership on an interface.

When the multicast group is statically configured on an interface, packets to the group are fast-switched out the interface ensuring all upstream routers maintain routing information for the group.

When the **ssm-map** keyword is used, the router uses Source Specific Multicast (SSM) mapping to determine the multicast source associated with this group. The resulting (S, G) channels are statically forwarded.

Use the **set** form of this command to specify static multicast group membership on an interface.

Use the **delete** form of this command to remove multicast group membership on the interface.

Use the **show** form of this command to static group membership configuration.
**monitor protocol multicast**

Enables IGMP debugging.

**Syntax**

```monitor protocol multicast { background { start | stop } } { enable|disable } igmp```

**Command Default**

IGMP debugging is disabled.

**Parameters**

- `background`
  - Performs debugging operations in the background.
  - `start`
    - Starts debugging in the background.
  - `stop`
    - Stops debugging in the background.
  - `enable`
    - Enables the specified debugging option.
  - `disable`
    - Disables the specified debugging option.
  - `igmp`
    - Specifies debugging of IGMP.

**Modes**

Operational mode

**Usage Guidelines**

Use this command to enable debugging for IGMP, or a specific component of IGMP.

When enabled, debugging messages are generated for all interfaces running the IGMP protocol.

**Examples**

The following example starts IGMP event debugging:

```
vyatta@vyatta:~$monitor protocol multicast enable igmp
```
protocols igmp limit <limit>

Sets the global limit for IGMP group memberships.

**Syntax**

```
set protocols igmp limit limit
delete protocols igmp limit limit
show protocols igmp limit
```

**Parameters**

`limit`

The maximum number of multicast groups that can be defined for the network served by the interface. The range is 1 to 2097152. By default, no limit is applied.

**Modes**

Configuration mode

**Configuration Statement**

```
protocols {
    igmp {
        limit limit
    }
}
```

**Usage Guidelines**

Use this command to set a global limit on the number of multicast groups to be served by an interface.

When this option is in effect and the maximum is reached, the router ignores all further local requests for membership.

The global limit set using this command can be overridden per-interface using `interfaces <interface> ip igmp limit <limit>` on page 25.

Use the **set** form of this command to set the limit on multicast groups.

Use the **delete** form of this command to restore the default behavior for multicast group limits.

Use the **show** form of this command to show group membership limit configuration.
protocols igmp log

Enables IGMP logs.

Syntax

set protocols igmp log { all | decode | encode | events | fsm | tib }
delete protocols igmp log { all | decode | encode | events | fsm | tib }
show protocols igmp log { all | decode | encode | events | fsm | tib }

Command Default

None

Parameters

all

Enables all IGMP logs.

decode

Enables only IGMP decode logs.

encode

Enables only IGMP encode logs.

events

Enables only IGMP event logs.

fsm

Enables only IGMP finite-state machine (FSM) logs.

tib

Enables only IGMP thread-information-block (TIB) logs.

Modes

Configuration mode

Configuration Statement

protocols {
  igmp {
    log {
      all
      decode
      encode
      fsm
      tib
    }
  }
}

Usage Guidelines

Use the set form of this command to enable Internet Group Management Protocol (IGMP) logs.
Use the delete form of this command to remove IGMP logs.
Use the show form of this command to view IGMP logs.
protocols igmp ssm-map

Enables source-specific multicast mapping on an interface.

Syntax

- set protocols igmp ssm-map
- delete protocols igmp ssm-map
- show protocols ip igmp

Command Default

SSM mapping is disabled.

Modes

Configuration mode

Configuration Statement

```
protocols {
  igmp {
    ssm-map
  }
}
```

Usage Guidelines

Use this command to globally enable source-specific multicast (SSM) mapping for groups in a configured SSM range. The range is configured globally using `protocols igmp ssm-map static access-list <acl> source <source>` on page 40.

A value set at the interface level overrides the global value.

Use the **set** form of this command to enable SSM mapping.

Use the **delete** form of this command to restore the default behavior for SSM mapping.

Use the **show** form of this command to show SSM mapping configuration.
protocols igmp ssm-map static access-list <acl> source <source>

Globally associates a multicast source for static SSM map group.

**Syntax**

```
set protocols igmp ssm-map static access-list acl source source
```

```
delete protocols igmp ssm-map static access-list acl source source
```

```
show protocols igmp ssm-map static access-list acl
```

**Parameters**

`acl`

The name of an IPv4 access control list to be used for filtering membership groups. Supported ranges of values are:

- 1 to 99: IP access list number.
- 1300 to 1999: IP access list number in the expanded range.

Access control lists are a type of routing policy; see the Brocade 5600 vRouter Routing Policies Reference Guide for information on creating them.

`source`

The source address to associate with SSM mapping. The format is an IPv4 address in dotted quad format.

**Modes**

Configuration mode

**Configuration Statement**

```
protocols {
  igmp {
    ssm-map {
      static {
        access-list acl{
          source source
        }
      }
    }
  }
}
```

**Usage Guidelines**

Use this command to globally define a group for static SSM mapping.

A value set at the interface level overrides the global value.

This command statically assigns source values to IGMPv1 and IGMPv2 groups to translate the sources represented with the wildcard in (*,G) entries to (S, G) entries.

Use the **set** form of this command to associate the specified group with SSM mapping.

Use the **delete** form of this command to delete the SSM mapping association.

Use the **show** form of this command to show SSM group association configuration.
reset ip igmp

Clears the specified IGMP local memberships.

Syntax

reset ip igmp [ group group [ interface ] | interface interface ]

Parameters

- **group**
  - Clears the specified multicast group and deletes IGMP group cache entries. The format is an IPv4 multicast address.

- **interface**
  - Clears the multicast groups learned from the specified interface. The format is an interface type, as described in interfaces <interface> ip igmp on page 16.

- **interface interface**
  - Clears all multicast groups learned from the specified interface. The format is an interface type, as described in interfaces <interface> ip igmp on page 16.

Modes

- Operational mode

Usage Guidelines

Use this command to clear IGMP group membership information.

Examples

The following example clears group membership information for the multicast group 224.1.1.1.

```
vyatta@vyatta:#reset ip igmp group 224.1.1.1
```

The following example clears group membership information for interface dp0p1p2.

```
vyyatta@vyatta:#reset ip igmp interface dp0p1p2
```
**show ip igmp groups**

Displays the multicast groups with receivers connected to the system and learned through IGMP.

Syntax

```
show ip igmp groups [[ group-address group [ detail ] ] | interface interface [ detail ] | detail ]
```

Command Default

When used with no option, displays all available group information in summary format.

Parameters

- **group**
  
  Shows multicast group information for the specified IPv4 multicast group.

- **interface**
  
  Shows multicast group information for the specified interface. For a list of supported interfaces, see interfaces <interface> ip igmp on page 16.

- **detail**
  
  Provides detailed group information.

Modes

- Operational mode

Usage Guidelines

Use this command to display the multicast groups with receivers connected to the system and learned through IGMP.

Examples

The following example shows group membership information.

```
vty@vyatta:~$show ip igmp groups
IGMP Connected Group Membership
Group Address  Interface  Uptime   Expires  Last Reporter
225.0.0.2      dp0s4    00:00:06 00:04:16 10.0.3.6
225.0.0.3      dp0s4    00:00:06 00:04:16 10.0.3.6
225.0.0.4      dp0s4    00:00:06 00:04:16 10.0.3.6
```
show ip igmp interface

Displays the operational state of IGMP on an interface.

Syntax  show ip igmp interface [ interface ]

Command Default  When used with no option, this command displays the operational state of all IGMP-enabled interfaces.

Parameters  interface

Displays the operational state of the specified interface.

Modes  Operational mode

Usage Guidelines  Use this command to display the state of IGMP on interfaces.

Examples  The following example shows IGMP interface information for interface dp0p1p2.

vyatta@vyatta:~$show ip igmp interface dp0p1p2
Interface dp0p1p2 (Index 4294967295)
IGMP Active, Non-Querier, Version 3 (default)
IGMP querying router is 0.0.0.0
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds
IGMP Snooping is globally enabled
IGMP Snooping is enabled on this interface
IGMP Snooping fast-leave is not enabled
IGMP Snooping querier is not enabled
IGMP Snooping report suppression is enabled
**show ip igmp ssm-map**

Displays information about IGMP SSM-mapping.

**Syntax**  
`show ip igmp ssm-map [group]`

**Command Default**  
When used with no option, this command displays all SSM-mapping information.

**Parameters**  
`group`  
Displays SSM mapping information for the specified group. The format is an IP address of an IPv4 multicast group.

**Modes**  
Operational mode

**Usage Guidelines**  
Use this command to display information about SSM mapping.

**Examples**  
The following example shows IGMP SSM mapping information for multicast group 123.12.3.123.

```
vtyatta@vtyatta:$show ip igmp ssm-map 123.12.3.123
```
**show monitoring protocols multicast igmp**

Displays IGMP debugging status.

**Syntax**

```
show monitoring protocols multicast igmp
```

**Modes**

Operational mode

**Usage Guidelines**

Use this command to show the status of IGMP debugging.

**Examples**

The following example shows the status of IGMP debugging.

```
vytta@vyatta:~$ show monitoring protocols multicast igmp
IGMP Debugging status:
IGMP Decoder debugging is on
IGMP Encoder debugging is on
IGMP Events debugging is on
IGMP FSM debugging is on
IGMP Tree-Info-Base (TIB) debugging is on
```
show monitoring protocols multicast igmp
MLD Commands

- interfaces <interface> ipv6 mld ................................................................. 48
- interfaces <interface> ipv6 mld access-group <acl6-name> .................. 49
- interfaces <interface> ipv6 mld immediate-leave group-list <acl6-name> 50
- interfaces <interface> ipv6 mld last-member-query-count <count> ........... 51
- interfaces <interface> ipv6 mld last-member-query-interval <interval> .... 52
- interfaces <interface> ipv6 mld limit <limit> ........................................... 53
- interfaces <interface> ipv6 mld limit-exception <acl6-name> .................. 54
- interfaces <interface> ipv6 mld querier-timeout <interval> ..................... 55
- interfaces <interface> ipv6 mld query-interval <interval> ....................... 56
- interfaces <interface> ipv6 mld query-max-response-time <interval> ...... 57
- interfaces <interface> ipv6 mld robustness-variable <variable> ............... 58
- interfaces <interface> ipv6 mld static-group <group> source <source> ....... 59
- interfaces <interface> ipv6 mld version <version> ................................. 60
- monitor protocol multicast ...................................................................... 61
- protocols mld limit <limit> ...................................................................... 62
- protocols mld log ..................................................................................... 63
- protocols mld ssm-map ............................................................................. 64
- protocols mld ssm-map static <acl6-name> source <source> ...................... 65
- reset ipv6 mld ......................................................................................... 66
- show ipv6 mld groups .............................................................................. 67
- show ipv6 mld interface .......................................................................... 68
- show ipv6 mld ssm-map ........................................................................... 69
- show monitoring protocols multicast mld ............................................... 70
interfaces <interface> ipv6 mld

Enables MLD on an interface.

Syntax

set interfaces interface ipv6 mld
delete interfaces interface ipv6 mld
show interfaces interface ipv6 mld

Parameters

interface

The type of interface. For detailed keywords and arguments for interfaces that support multicast routing, see the table in the Usage Guidelines below.

Modes

Configuration mode

Configuration Statement

interfaces interface {
    ipv6 {
        mld {
        }
    }
}

Usage Guidelines

Use this command to enable Multicast Listener Discovery (MLD) on an interface.

This command enables MLD operation in stand-alone mode, and can be used to learn local membership information prior to enabling a multicast routing protocol on the interface.

This command can only be issued on VLAN interfaces.

NOTE

Enabling IP on an interface enables the host-side functionality of MLD by default. The set interfaces interface ipv6 mld command enables the router-side functionality of the MLD on the given interface.

NOTE

To use MLD for multicast routing, multicast routing must be enabled on the router. For information about multicast routing in general, see the Brocade 5600 vRouter Multicast Routing Reference Guide.

Use the set form of this command to enable MLD on an interface.

Use the delete form of this command to remove all MLD configuration and disable MLD on an interface.

Use the show form of this command to display MLD configuration.
interfaces <interface> ipv6 mld access-group <acl6-name>

Controls the multicast local membership groups learned on an interface.

**Syntax**

```plaintext
set interfaces interface ipv6 mld access-group acl6-name
```

```plaintext
delete interfaces interface ipv6 mld access-group
```

```plaintext
show interfaces interface ipv6 mld access-group
```

**Parameters**

- `interface`
  
  The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ipv6 mld` on page 48.

- `acl6-name`
  
  The name of an IPv6 access control list to be used for filtering membership groups. Access control lists are a type of routing policy; see the *Brocade 5600 vRouter Routing Policies Reference Guide* for information on creating them.

**Modes**

Configuration mode

**Configuration Statement**

```plaintext
interfaces interface {
  ipv6 {
    mld {
      access-group acl6-name
    }
  }
}
```

**Usage Guidelines**

Use this command to use an access control list to control multicast local membership groups learned on an interface.

This command can only be issued on VLAN interfaces.

This command applies to interfaces configured for MLD Layer 3 multicast protocols.

Use the `set` form of this command to apply the access control list.

Use the `delete` form of this command to stop access-list filtering for MLD.

Use the `show` form of this command to show access-list configuration for MLD.
interfaces <interface> ipv6 mld immediate-leave group-list <acl6-name>

Minimizes latency for hosts leaving multicast groups.

**Syntax**

```plaintext
set interfaces interface ipv6 mld immediate-leave group-list acl6-name
```

```plaintext
delete interfaces interface ipv6 mld immediate-leave group-list
```

```plaintext
show interfaces interface ipv6 mld immediate-leave group-list
```

**Command Default**
Immediate leave is enabled.

**Parameters**

- **interface**
  The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ipv6 mld` on page 48.

- **acl6-name**
  The name of an IPv6 access control list to be used to define the membership group. Access control lists are a type of routing policy; see the Brocade 5600 vRouter Routing Policies Reference Guide for information on creating them.

**Modes**

Configuration mode

**Configuration Statement**

```plaintext
interfaces interface {
    ipv6 {
        mld {
            immediate-leave {
                group-list acl6-name
            }
        }
    }
}
```

**Usage Guidelines**

Use this command to minimize the leave latency for MLD memberships.

When this option is not set, the router sends a Query message when a receiver host has sent a Leave message. At this point, a timeout interval goes into effect. When this option is set, the Leave message is acted on immediately, without sending the Query or waiting for the timeout period to expire.

This command can only be issued on VLAN interfaces.

This command applies to interfaces configured for MLD Layer 3 multicast protocols. It applies when only one receiver host is connected to each interface.

Use the **set** form of this command to enable MLD immediate leave.

Use the **delete** form of this command to restore the MLD immediate leave default behavior.

Use the **show** form of this command to view MLD immediate leave configuration.
Manually sets the last member query count value.

**Syntax**

```
set interfaces interface ipv6 mld last-member-query-count count
```

```
delete interfaces interface ipv6 mld last-member-query-count
```

```
show interfaces interface ipv6 mld last-member-query-count
```

**Command Default**
The router sends two Query messages, after which it considers the host to have left the group.

**Parameters**

- **interface**
  - The type of interface. For a list of supported interfaces and detailed syntax, see **interfaces <interface> ipv6 mld** on page 48.

- **count**
  - The number of times the router sends a Query message after receiving a Leave message. The range is 2 to 7. The default is 2.

**Modes**

Configuration mode

**Usage Guidelines**

Use this command to set the number of times that the router sends a group-specific or source-group specific Query message when it receives a Leave message from a receiver host.

This command applies to interfaces configured for MLD Layer 3 multicast protocols.

The router uses this Query to determine whether any members of the multicast group remain on the network. The command is sent at the interval set in **interfaces <interface> ipv6 mld last-member-query-interval <interval>** on page 52. If the router receives no response to the configured number of queries, the router stops forwarding to that network.

Use the **set** form of this command to set the number of last-member queries sent.

Use the **delete** form of this command to restore the default value for last-member queries.

Use the **show** form of this command to show last-member query configuration.
interfaces <interface> ipv6 mld last-member-query-interval <interval>

Specifies the frequency at which MLD group-specific host queries are sent.

Syntax

set interfaces interface ipv6 mld last-member-query-interval interval
delete interfaces interface ipv6 mld last-member-query-interval
show interfaces interface ipv6 mld last-member-query-interval

Command Default
The router waits 1000 milliseconds between last-member queries.

Parameters

interface
The type of interface. For a list of supported interfaces and detailed syntax, see interfaces <interface> ipv6 mld on page 48.
interval
The interval between last-member queries, in milliseconds. The range is 1000 to 25500. The default is 1000.

Modes
Configuration mode

Configuration Statement

interfaces interface {
  ipv6 {
    mld {
      last-member-query-interval interval
    }
  }
}

Usage Guidelines
Use this command to set the interval between MLD group-specific or source-specific Query messages sent by the router to determine whether any receivers remain in a multicast group.

The router uses this Query to determine whether any members of the multicast group remain on the network. If it receives no response to the configured number of queries (as set in interfaces <interface> ipv6 mld last-member-query-count <count> on page 51), the router stops forwarding to that network.

This command applies to interfaces configured for MLD Layer 3 multicast protocols.

Use the set form of this command to set the interval for last-member queries.
Use the delete form of this command to restore the default interval for last-member queries.
Use the show form of this command to show last-member query interval configuration.
interfaces <interface> ipv6 mld limit <limit>

Sets the limit for MLD group memberships on an interface.

**Syntax**

```
set interfaces interface ipv6 mld limit limit
delete interfaces interface ipv6 mld limit
show interfaces interface ipv6 mld limit
```

**Parameters**

- **interface**
  
  The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ipv6 mld` on page 48.

- **limit**
  
  The maximum number of multicast group memberships that can be defined for the network served by the interface. The range is 1 to 2097152. By default, no limit is applied.

**Modes**

Configuration mode

**Configuration Statement**

```bash
interfaces interface {
    ipv6 {
        mld {
            limit limit
        }
    }
}
```

**Usage Guidelines**

Use this command to set an interface-specific limit on the number of multicast group memberships to be served by an interface. You can use this option to override the global limit set using `protocols mld limit <limit>` on page 62.

This command applies to interfaces configured for MLD Layer 3 multicast protocols.

When this option is in effect and the maximum is reached, the router ignores all further local requests for membership.

Use the `set` form of this command to set the limit on multicast group memberships on an interface.

Use the `delete` form of this command to restore the default behavior for multicast group membership limits.

Use the `show` form of this command to show group membership limit configuration.
interfaces <interface> ipv6 mld limit-exception <acl6-name>

Specifies multicast groups unaffected by the MLD group membership limits on an interface.

**Syntax**

```
set interfaces interface ipv6 mld limit-exception acl6-name
```

```
delete interfaces interface ipv6 mld limit-exception acl6-name
```

```
show interfaces interface ipv6 mld limit-exception
```

**Parameters**

- **interface**
  - The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ipv6 mld` on page 48.

- **acl6-name**
  - The name of an IPv6 access control list to be used to define the membership group. Access control lists are a type of routing policy; see the *Brocade 5600 vRouter Routing Policies Reference Guide* for information on creating them.

**Modes**

Configuration mode

**Configuration Statement**

```
interfaces interface {
    ipv6 {
        mld {
            limit-exception acl6-name
        }
    }
}
```

**Usage Guidelines**

Use this command to specify the multicast groups that are an exception to the membership limits imposed by `interfaces <interface> ipv6 mld limit <limit>` on page 53. As such, this command is dependent on `interfaces <interface> ipv6 mld limit <limit>` on page 53 being set.

Use the **set** form of this command to specify the multicast groups that are unaffected by the MLD group membership limits on an interface.

Use the **delete** form of this command to remove the list of multicast groups that are unaffected by the MLD group membership limits on an interface.

Use the **show** form of this command to show group membership limit exception configuration.
interfaces <interface> ipv6 mld querier-timeout <interval>

Sets the interval before the system takes over as querier on an interface.

**Syntax**

```
set interfaces interface ipv6 mld querier-timeout interval
```

```
delete interfaces interface ipv6 mld querier-timeout
```

```
show interfaces interface ipv6 mld querier-timeout
```

**Command Default**
The router waits to receive a query for 255 seconds before taking over as querier.

**Parameters**

- `interface`
  The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ipv6 mld` on page 48.

- `interval`
  The amount of time, in seconds, the router waits before taking over as querier when the previous querier fails to send an MLD Query. The range is 60 to 300. The default is 255.

**Modes**

Configuration mode

**Configuration Statement**

```
interfaces interface {
  ipv6 {
    mld {
      querier-timeout interval
    }
  }
}
```

**Usage Guidelines**

Use this command to specify how long the router waits to receive an MLD query from the previous querier. When this interval expires, the router takes over as querier.

This command applies to interfaces configured for MLD Layer 3 multicast protocols.

Use the `set` form of this command to set the querier timeout interval.

Use the `delete` form of this command to restore the default querier timeout interval.

Use the `show` form of this command to show querier timeout interval configuration.
interfaces <interface> ipv6 mld query-interval <interval>

Specifies the frequency at which MLD host queries are sent.

**Syntax**

- `set interfaces interface ipv6 mld query-interval interval`
- `delete interfaces interface ipv6 mld query-interval`
- `show interfaces interface ipv6 mld query-interval`

**Command Default**
The router sends MLD Query messages at intervals of 125 seconds.

**Parameters**

- `interface`
  - The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ipv6 mld` on page 48.
- `interval`
  - The interval, in seconds, at which the router sends MLD Query messages. The range is 1 to 180. The default is 125.

**Modes**
Configuration mode

**Configuration Statement**

```
interfaces interface {
  ipv6 {
    mld {
      query-interval interval
    }
  }
}
```

**Usage Guidelines**
Use this command to set the frequency with which the router sends MLD host Query messages.

This command applies to interfaces configured for MLD Layer 3 multicast protocols.

Use the `set` form of this command to set the query interval.

Use the `delete` form of this command to restore the default query interval.

Use the `show` form of this command to show query interval configuration.
interfaces <interface> ipv6 mld query-max-response-time <interval>

Specifies the maximum response time advertised in MLD queries.

**Syntax**

```
set interfaces interface ipv6 mld query-max-response-time interval
```

```
delete interfaces interface ipv6 mld query-max-response-time
```

```
show interfaces interface ipv6 mld query-max-response-time
```

**Command Default**
The router waits 10 seconds for a response to an MLD Query before deleting the multicast group.

**Parameters**

- **interface**
  
  The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ipv6 mld` on page 48.

- **interval**
  
  The amount of time, in seconds, that the router advertises as the maximum delay before a responder can respond to an MLD Query. The range is 1 to 240. The default is 20.

**Modes**

Configuration mode

**Configuration Statement**

```
interfaces interface {
  ipv6 {
    mld {
      query-max-response-time interval
    }
  }
}
```

**Usage Guidelines**

Use this command to set the value to be advertised as the maximum time the router will wait to receive a response to MLD Query messages. When this interval expires, the router deletes the multicast group. This command applies to interfaces configured for MLD Layer 3 multicast protocols.

Use the `set` form of this command to set the maximum query response time. Use the `delete` form of this command to restore the default maximum query response time. Use the `show` form of this command to show maximum query response time configuration.
**interfaces <interface> ipv6 mld robustness-variable <variable>**

Specifies the value of the robustness variable on an interface.

**Syntax**

- `set interfaces interface ipv6 mld robustness-variable variable`
- `delete interfaces interface ipv6 mld robustness-variable`
- `show interfaces interface ipv6 mld robustness-variable`

**Command Default**
The robustness variable is set to 2.

**Parameters**

- `interface`
  - The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ipv6 mld` on page 48.
- `variable`
  - The robustness variable. The range is 2 to 7. The default is 2.

**Modes**

- Configuration mode

**Configuration Statement**

```plaintext
interfaces interface {
  ipv6 {
    mld {
      robustness-variable variable
    }
  }
}
```

**Usage Guidelines**

Use this command to set the robustness variable for an interface.

This command applies to interfaces configured for MLD Layer 3 multicast protocols.

The robustness variable specifies how many refresh packets for a given state can be lost before the system without timing out and changing state. This helps tune the network for expected packet loss.

Use the `set` form of this command to set the robustness variable value.

Use the `delete` form of this command to restore the default robustness variable value.

Use the `show` form of this command to show robustness variable configuration.
interfaces <interface> ipv6 mld static-group <group> source <source>

Specifies static multicast group membership on an interface.

**Syntax**

```
set interfaces interface ipv6 mld static-group group source source
delete interfaces interface ipv6 mld static-group group source source
show interfaces interface ipv6 mld static-group group source
```

**Parameters**

- **interface**
  - The type of interface. For a list of supported interfaces and detailed syntax, see interfaces <interface> ipv6 mld on page 48.
- **group**
  - The IPv6 multicast address of the group the router is being made a member of.
- **source**
  - The static source of multicast packets. Supported values are:
    - `x:x:x:x:x:x:x:x:`: The IPv6 address of a multicast source.
    - `ssm-map`: Use Source Specific Multicast (SSM) mapping to determine the multicast source associated with this group.

**Modes**

Configuration mode

**Configuration Statement**

```
interfaces interface {
  ipv6 {
    mld {
      static-group group
      {
        source source
      }
    }
  }
}
```

**Usage Guidelines**

Use this command to add MLD group or source records to a specific interface.

When the router is statically configured to be a member of a group, packets to the group are fast-switched out the interface ensuring all upstream routers maintain routing information for the group.

When the `ssm-map` keyword is used, the router uses Source Specific Multicast (SSM) mapping to determine the multicast source associated with this group. The resulting (S, G) channels are statically forwarded.

Use the `set` form of this command to specify static multicast group membership on an interface.

Use the `delete` form of this command to remove multicast group membership on the interface.

Use the `show` form of this command to static group membership configuration.
interfaces <interface> ipv6 mld version <version>

Sets the MLD version in use on an interface.

Syntax

```
set interfaces interface ipv6 mld version version
delete interfaces interface ipv6 mld version
show interfaces interface ipv6 mld version
```

Command Default

MLDv2 is used.

Parameters

- **interface**
  - The type of interface. For a list of supported interfaces and detailed syntax, see `interfaces <interface> ipv6 mld` on page 48.
- **version**
  - The MLD version number. Supported values are 1 and 2. The default is 2.

Modes

- **Configuration mode**

Configuration Statement

```
interfaces interface {
    ipv6 {
        mld {
            version version
        }
    }
}
```

Usage Guidelines

Use this command to specify which MLD version the router should use for multicast routing.

This command applies to interfaces configured for MLD Layer 3 multicast protocols.

Use the `set` form of this command to set the MLD version number.

Use the `delete` form of this command to restore the default MLD version number.

Use the `show` form of this command to show MLD version number configuration.
monitor protocol multicast

Enables MLD debugging.

Syntax

```
monitor protocol multicast [ background { start | stop } ] { enable | disable } mld
```

Command Default

MLD debugging is disabled.

Parameters

- **background**
  - Performs debugging operations in the background.
  - `start`
    - Starts debugging in the background.
  - `stop`
    - Stops debugging in the background.
  - `enable`
    - Enables the specified debugging option.
  - `disable`
    - Disables the specified debugging option.
  - `mld`
    - Specifies debugging of MLD.

Modes

Operational mode

Usage Guidelines

Use this command to enable debugging for MLD, or a specific component of MLD.

When enabled, debugging messages are generated for all interfaces running the MLD protocol.

Examples

The following example starts MLD event debugging.

```
vyyatta@vyatta:~$ monitor protocol multicast enable mld
```
protocols mld limit <limit>

Sets the global limit for MLD group memberships.

Syntax

set protocols mld limit limit
delete protocols mld limit
show protocols mld limit

Command Default
No limit is applied.

Parameters

limit

The maximum number of multicast groups that can be defined for the network served by the interface. The range is 1 to 2097152. By default, no limit is applied.

Modes

Configuration mode

Configuration Statement

protocols {
    mld {
        limit limit
    }
}

Usage Guidelines

Use this command to set a global limit on the number of multicast groups to be served by an interface.

When this option is in effect and the maximum is reached, the router ignores all further local requests for membership.

The global limit set using this command can be overridden per-interface using interfaces <interface> ipv6 mld limit <limit> on page 53.

Use the set form of this command to set the limit on multicast groups.

Use the delete form of this command to restore the default behavior for multicast group limits.

Use the show form of this command to show group membership limit configuration.
**protocols mld log**

Enables MLD logs.

**Syntax**

```plaintext
set protocols mld log { all | decode| encode | events| fsm| tib}

delete protocols mld log { all | decode| encode | events| fsm| tib}

show protocols mld log { all | decode| encode | events| fsm| tib}
```

**Command Default** None

**Parameters**

- **all**
  
  Enables all MLD logs.

- **decode**
  
  Enables only MLD decode logs.

- **encode**
  
  Enables only MLD encode logs.

- **events**
  
  Enables only MLD event logs.

- **fsm**
  
  Enables only MLD finite-state machine (FSM) logs.

- **tib**
  
  Enables only MLD thread-information-block (TIB) logs.

**Modes**

Configuration mode

**Configuration Statement**

```plaintext
protocols {
    mld {
        log {
            all
            decode
            encode
            fsm
            tib
        }
    }
}
```

**Usage Guidelines**

Use the `set` form of this command to enable Multicast Listener Discovery (MLD) logs.

Use the `delete` form of this command to remove MLD logs.

Use the `show` form of this command to view MLD logs.
**protocols mld ssm-map**

Enables source-specific multicast mapping on an interface.

**Syntax**

```bash
set protocols mld ssm-map
```

```bash
delete protocols mld ssm-map
```

```bash
show protocols mld
```

**Command Default**

SSM mapping is disabled.

**Modes**

Configuration mode

**Configuration Statement**

```bash
protocols {
    mld {
        ssm-map
    }
}
```

**Usage Guidelines**

Use this command to globally enable source-specific multicast (SSM) mapping for groups in a configured SSM range. The range is configured globally using `protocols mld ssm-map static <acl6-name> source <source>` on page 65.

A value set at the interface level overrides the global value.

Use the **set** form of this command to enable SSM mapping.

Use the **delete** form of this command to restore the default behavior for SSM mapping.

Use the **show** form of this command to show SSM mapping configuration.
protocols mld ssm-map static <acl6-name> source <source>

Globally associates a multicast source for static SSM map group.

**Syntax**

- `set protocols mld ssm-map static acl6-name source source`
- `delete protocols mld ssm-map static acl6-name source source`
- `show protocols gmp ssm-map static acl6-name source`

**Parameters**

- `acl6-name` The name of an IPv6 access control list to be used for filtering membership groups. Access control lists are a type of routing policy; see the Brocade 5600 vRouter Routing Policies Reference Guide for information on creating them.
- `source` The IPv6 source address to associate with SSM mapping.

**Modes**

Configuration mode

**Configuration Statement**

```plaintext
protocols {
  mld {
    ssm-map {
      static acl6-name {
        source-address source
      }
    }
  }
}
```

**Usage Guidelines**

Use this command to globally define a group for static SSM mapping.

A value set at the interface level overrides the global value.

This command statically assigns source values to multicast group entries to translate the sources represented with the wildcard in (*,G) entries to (S, G) entries.

Use the **set** form of this command to associate the specified group with SSM mapping.

Use the **delete** form of this command to delete the SSM mapping association.

Use the **show** form of this command to show SSM group association configuration.
**reset ipv6 mld**

Clears the specified MLD local memberships.

**Syntax**

```
reset ipv6 mld { group group [ interface ] | interface interface }
```

**Parameters**

- `group` Clear the specified multicast group and deletes MLD group cache entries. The format is an IPv6 multicast address.
- `interface` Clear the multicast groups learned from the specified interface. The format is an interface type, as described in `interfaces <interface> ipv6 mld` on page 48.
- `interfaceinterface` Clear all multicast groups learned from the specified interface. The format is an interface type, as described in `interfaces <interface> ipv6 mld` on page 48.

**Modes**

Operational mode

**Usage Guidelines**

Use this command to clear MLD group membership information.

**Examples**

The following example clears group membership information for the multicast group FF1E::10.

```
vytta@vyatta:~$reset ipv6 mld group FF1E::10
```

The following example clears group membership information for interface dp0p1p2.

```
vytta@vyatta:~$reset ipv6 mld group dp0p1p2
```
**show ipv6 mld groups**

Displays the multicast groups with receivers connected to the system and learned through MLD.

**Syntax**

```
show ipv6 mld groups [ [ group-address group [ detail ] | interface interface [ detail ] ] ]
```

- **Command Default**
  - When used with no option, displays all available group information in summary format.

- **Parameters**
  - **group**
    - Shows multicast group information for the specified IPv6 multicast group.
  - **interface**
    - Shows multicast group information for the specified interface. For a list of supported interfaces, see `interfaces <interface> ipv6 mld` on page 48.
  - **detail**
    - Provides detailed group information for the specified interface.

- **Modes**
  - Operational mode

- **Usage Guidelines**
  - Use this command to display the multicast groups with receivers connected to the system and learned through MLD.

- **Examples**
  - The following example shows MLD group membership information.

```
vty@vyatta:~$ show ipv6 mld groups
MLD Connected Group Membership
  Group Address    Interface   Uptime       Expires   Last Reporter
ff1e::10          ge10       00:03:16 00:01:09
fe80::202:b3ff:fef0:79d8
```

*Brocade 5600 vRouter IGMP and MLD Reference Guide*
show ipv6 mld interface

Displays the operational state of MLD on an interface.

Syntax  
show ipv6 mld interface [ interface ]

Command Default  
When used with no option, this command displays the operational state of all MLD-enabled interfaces.

Parameters  
interface  
Displays the operational state of the specified interface.

Modes  
Operational mode

Usage Guidelines  
Use this command to display the state of MLD on interfaces.

Examples  
The following example shows MLD interface information for interface dp0p1p2.

vyatta@vyatta:~$show ipv6 mld interface dp0p1p2
Interface dp0p1p2 (Index 2)
MLD Enabled, Active, Querier, Version 2 (default)
Internet address is fe80::2fd:6cff:fe1c:b
MLD interface has 0 group-record states
MLD query interval is 125 seconds
MLD querier timeout is 255 seconds
MLD max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds
show ipv6 mld ssm-map

Displays information about MLD SSM-mapping.

Syntax

show ipv6 mld ssm-map [group ]

Command Default

When used with no option, this command displays all SSM-mapping information.

Parameters

group

Displays SSM mapping information for the specified group. The format is an IPv6 multicast address.

Modes

Operational mode

Usage Guidelines

Use this command to display information about SSM mapping.
show monitoring protocols multicast mld

Displays MLD debugging status.

**Syntax**
show monitoring protocols multicast mld

**Modes**
Operational mode

**Usage Guidelines**
Use this command to show the status of MLD debugging.

**Examples**
The following example shows the status of MLD debugging.

vyatta@vyatta:~$ show monitoring protocols multicast mld
MLD Debugging status:
MLD Decoder debugging is on
MLD Encoder debugging is on
MLD Events debugging is on
MLD FSM debugging is on
MLD Tree-Info-Base (TIB) debugging is on
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>access control list</td>
</tr>
<tr>
<td>ADSL</td>
<td>Asymmetric Digital Subscriber Line</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header</td>
</tr>
<tr>
<td>AMI</td>
<td>Amazon Machine Image</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>AS</td>
<td>autonomous system</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>AWS</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input Output System</td>
</tr>
<tr>
<td>BPDU</td>
<td>Bridge Protocol Data Unit</td>
</tr>
<tr>
<td>CA</td>
<td>certificate authority</td>
</tr>
<tr>
<td>CCMP</td>
<td>AES in counter mode with CBC-MAC</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CLI</td>
<td>command-line interface</td>
</tr>
<tr>
<td>DDNS</td>
<td>dynamic DNS</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DHCPv6</td>
<td>Dynamic Host Configuration Protocol version 6</td>
</tr>
<tr>
<td>DLCI</td>
<td>data-link connection identifier</td>
</tr>
<tr>
<td>DMI</td>
<td>desktop management interface</td>
</tr>
<tr>
<td>DMVPN</td>
<td>dynamic multipoint VPN</td>
</tr>
<tr>
<td>DMZ</td>
<td>demilitarized zone</td>
</tr>
<tr>
<td>DN</td>
<td>distinguished name</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DSCP</td>
<td>Differentiated Services Code Point</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>eBGP</td>
<td>external BGP</td>
</tr>
<tr>
<td>EBS</td>
<td>Amazon Elastic Block Storage</td>
</tr>
<tr>
<td>EC2</td>
<td>Amazon Elastic Compute Cloud</td>
</tr>
<tr>
<td>EGP</td>
<td>Exterior Gateway Protocol</td>
</tr>
<tr>
<td>ECMP</td>
<td>equal-cost multipath</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>FIB</td>
<td>Forwarding Information Base</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation</td>
</tr>
<tr>
<td>HDLC</td>
<td>High-Level Data Link Control</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>IGP</td>
<td>Interior Gateway Protocol</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Protection System</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPOA</td>
<td>IP over ATM</td>
</tr>
<tr>
<td>IPsec</td>
<td>IP Security</td>
</tr>
<tr>
<td>IPv4</td>
<td>IP Version 4</td>
</tr>
<tr>
<td>IPv6</td>
<td>IP Version 6</td>
</tr>
<tr>
<td>ISAKMP</td>
<td>Internet Security Association and Key Management Protocol</td>
</tr>
<tr>
<td>ISM</td>
<td>Internet Standard Multicast</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>KVM</td>
<td>Kernel-Based Virtual Machine</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
</tr>
<tr>
<td>LACP</td>
<td>Link Aggregation Control Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>local area network</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LLDP</td>
<td>Link Layer Discovery Protocol</td>
</tr>
<tr>
<td>MAC</td>
<td>medium access control</td>
</tr>
<tr>
<td>mGRE</td>
<td>multipoint GRE</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>MLD</td>
<td>Multicast Listener Discovery</td>
</tr>
<tr>
<td>MLP PPP</td>
<td>multilink PPP</td>
</tr>
<tr>
<td>MRRU</td>
<td>maximum received reconstructed unit</td>
</tr>
<tr>
<td>MTU</td>
<td>maximum transmission unit</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NBMA</td>
<td>Non-Broadcast Multi-Access</td>
</tr>
<tr>
<td>ND</td>
<td>Neighbor Discovery</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>NHRP</td>
<td>Next Hop Resolution Protocol</td>
</tr>
<tr>
<td>NIC</td>
<td>network interface card</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>OSPFv2</td>
<td>OSPF Version 2</td>
</tr>
<tr>
<td>OSPFv3</td>
<td>OSPF Version 3</td>
</tr>
<tr>
<td>PAM</td>
<td>Pluggable Authentication Module</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol</td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
</tr>
<tr>
<td>PCI</td>
<td>peripheral component interconnect</td>
</tr>
<tr>
<td>PIM</td>
<td>Protocol Independent Multicast</td>
</tr>
<tr>
<td>PIM-DM</td>
<td>PIM Dense Mode</td>
</tr>
<tr>
<td>PIM-SM</td>
<td>PIM Sparse Mode</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>PPPoA</td>
<td>PPP over ATM</td>
</tr>
<tr>
<td>PPPoE</td>
<td>PPP over Ethernet</td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol</td>
</tr>
<tr>
<td>PTMU</td>
<td>Path Maximum Transfer Unit</td>
</tr>
<tr>
<td>PVC</td>
<td>permanent virtual circuit</td>
</tr>
<tr>
<td>QoS</td>
<td>quality of service</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>RHEL</td>
<td>Red Hat Enterprise Linux</td>
</tr>
<tr>
<td>RIB</td>
<td>Routing Information Base</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Information Protocol</td>
</tr>
<tr>
<td>RIPng</td>
<td>RIP next generation</td>
</tr>
<tr>
<td>RP</td>
<td>Rendezvous Point</td>
</tr>
<tr>
<td>RPF</td>
<td>Reverse Path Forwarding</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, and Adleman</td>
</tr>
<tr>
<td>Rx</td>
<td>receive</td>
</tr>
<tr>
<td>S3</td>
<td>Amazon Simple Storage Service</td>
</tr>
<tr>
<td>SLAAC</td>
<td>Stateless Address Auto-Configuration</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SONET</td>
<td>Synchronous Optical Network</td>
</tr>
<tr>
<td>SPT</td>
<td>Shortest Path Tree</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SSM</td>
<td>Source-Specific Multicast</td>
</tr>
<tr>
<td>STP</td>
<td>Spanning Tree Protocol</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access Control System Plus</td>
</tr>
<tr>
<td>TBF</td>
<td>Token Bucket Filter</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>ToS</td>
<td>Type of Service</td>
</tr>
<tr>
<td>TSS</td>
<td>TCP Maximum Segment Size</td>
</tr>
<tr>
<td>Tx</td>
<td>transmit</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VHD</td>
<td>virtual hard disk</td>
</tr>
<tr>
<td>vif</td>
<td>virtual interface</td>
</tr>
<tr>
<td>VLAN</td>
<td>virtual LAN</td>
</tr>
<tr>
<td>VPC</td>
<td>Amazon virtual private cloud</td>
</tr>
<tr>
<td>VPN</td>
<td>virtual private network</td>
</tr>
<tr>
<td>VRRP</td>
<td>Virtual Router Redundancy Protocol</td>
</tr>
<tr>
<td>WAN</td>
<td>wide area network</td>
</tr>
<tr>
<td>WAP</td>
<td>wireless access point</td>
</tr>
<tr>
<td>WPA</td>
<td>Wired Protected Access</td>
</tr>
</tbody>
</table>