BROCADE

CONFIGURATION GUIDE

Brocade Vyatta Network OS IGMP and MLD Configuration Guide, 5.2R1

Supporting Brocade 5600 vRouter, VNF Platform, and Distributed Services Platform

53-1004721-01
24 October 2016

Contents

Preface

Document conventions

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

Notes, cautions, and warnings

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

NOTE

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

ATTENTION

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

CAUTION

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

DANGER

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

Text formatting conventions

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

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

Command syntax conventions

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

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

Brocade resources

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

White papers, data sheets, and the most recent versions of Brocade software and hardware manuals are available at www.brocade.com. Product documentation for all supported releases is available to registered users at MyBrocade.
Click the **Support** tab and select **Document Library** to access documentation on MyBrocade or www.brocade.com You can locate documentation by product or by operating system.

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

Document feedback

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

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

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

Contacting Brocade Technical Support

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

Brocade customers

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

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

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

Brocade OEM customers

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

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

About This Guide

This guide describes how to configure IGMP and MLD on Brocade products that run on the Brocade Vyatta Network OS (referred to as a virtual router, vRouter, or router in the guide).

IGMP and MLD overview

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 Vyatta Network OS Multicast Routing Configuration Guide* and *Brocade Vyatta Network OS PIM Configuration 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 class D 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*
- IGMPv3, defined by RFC 3376, *Internet Group Management Protocol, Version 3* and updated by RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*

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 Vyatta Network OS Multicast Routing Configuration Guide*.

MLD

This section presents the following topics:

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 of address range FF00::/8, 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 on page 13
- Multicast listener done on page 13
- Multicast listener query on page 13

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 Vyatta Network OS Multicast Routing Configuration Guide*).

Supported standards

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

- RFC 1112: *Host Extensions for IP Multicasting*
- RFC 2236: *Internet Group Management Protocol, Version 2*
- 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 Vyatta Network OS Remote Management Configuration 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 Vyatta Network OS Multicast Routing Configuration Guide*.

IGMP Commands

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 Vyatta Network OS Multicast Routing Configuration Guide*.

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

Interface Type	Syntax	Parameters
Bridge	bridge *brx*	*brx*: The name of a bridge group. The name ranges from br0 through br999.
Data plane	dataplane dp*xy*>pz*v*	dp*x*p*y*p*z*: The name of a data plane interface to which the following applies: • dp*x* identifies a data plane ID

Interface Type	Syntax	Parameters
		NOTE Currently, only dp0 is supported. • p*y* specifies a physical or virtual PCI slot index • p*z* specifies a port index Other supported name formats are the following: • dp*x*em*y*—used for LAN-on-motherboard (LOM) devices that do not have a PCI slot. em*y* specifies an embedded network interface number. • dp*x*port*y*—used for devices in which the PCI slot cannot be identified. port*y* specifies a port index.
Data plane vif	dataplane dp*x*p*y*p*z* vif *vif-id* [vlan *vlan-id*]	dp*x*p*y*p*z*: The name of a data plane interface to which the following applies: • dp*x* specifies a data plane ID NOTE Currently, only dp0 is supported. • p*y* specifies a physical or virtual PCI slot index • p*z* specifies a port index Other supported name formats are the following: • dp*x*em*y*—used for LAN-on-motherboard (LOM) devices that do not have a PCI slot. em*y* specifies an embedded network interface number. • dp*x*port*y*—used for devices in which the PCI slot cannot be identified. port*y* specifies a port index. *vif-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.
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 vtun*x*, where *x* is a nonnegative integer.
Tunnel	tunnel *tunx* or tunnel *tunx* parameters	*tunx*: The identifier of a tunnel interface you are defining. The identifier ranges from tun0 through tun*x*, where *x* is a nonnegative integer.
Virtual tunnel	vti *vtix*	*vtix*: The identifier of a virtual tunnel interface you are defining. The identifier ranges from

Interface Type	Syntax	Parameters
		vti0 through vti*x*, where *x* is a nonnegative integer. **Note:** This interface does not support IPv6.
VRRP	interface *parent-if* vrrp vrrp-group *group* interface	*parent-if*: The type and identifier of a parent interface; for example, dataplane dp0p1p2 or bridge br999. *group*: A VRRP group identifier. 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>

Applies an access control list to the multicast local membership groups on an interface.

Syntax

set interfaces *interface* **ip igmp access-group** *acl*

delete interfaces *interface* **ip igmp access-group** *acl*

show interfaces *interface* **ip igmp access-group** *acl*

Parameters

interface

A 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 control list number. The number ranges from 1 through 99. An access control list is a type of routing policy; see *Brocade Vyatta Network OS Routing Policies Configuration Guide* for information on creating one.

Modes

Configuration mode

Configuration Statement

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

Usage Guidelines

Use this command to apply an access control list to the multicast local membership groups on an interface.

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

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

Use the **show** form of this command to display the access control list configuration for IGMP.

interfaces <interface> ip igmp enforce-router-alert

Enables strict Router Alert 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 Alert 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 Vyatta Network OS Routing Policies Configuration 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.

interfaces <interface> ip igmp last-member-query-count <count>

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 25. 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 24), 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, a limit of 5000 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.

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 between to and static 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 Vyatta Network OS Routing Policies Configuration 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 26. As such, this command is dependent on interfaces <interface> ip igmp limit <limit> on page 26 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

Configuration Statement

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

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 31.

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

```
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

```
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

```
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 show static group membership configuration.

monitor protocol multicast

Enables IGMP debugging.

Syntax

monitor protocol multicast [**enable**|**disable**] **igmp**

Command Default

IGMP debugging is disabled.

Parameters

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.

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

Examples

The following example starts IGMP debugging.

```
vyatta@vyatta:~$monitor protocol multicast enable igmp
```

protocols igmp limit <limit>

Sets a global limit on the number of IGMP groups.

Syntax

set protocols igmp limit *limit*

delete protocols igmp limit *limit*

show protocols igmp limit

Parameters

limit

The maximum number of IGMP multicast groups. The number ranges from 1 through 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. When the limit is reached, the router ignores all further local requests for membership.

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

Use the **delete** form of this command to remove the limit applied on the number of multicast groups.

Use the **show** form of this command to display the limit on the number of multicast groups.

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 tree-information-base (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 disable IGMP logs.

Use the **show** form of this command to view IGMP logging configuration.

protocols igmp ssm-map

Enables source-specific multicast mapping globally.

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 43.

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 Vyatta Network OS Routing Policies Configuration 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 specified multicast group 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.

```
vyatta@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* [*group* [**detail**]] [**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.

```
vyatta@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 dp0p1s1 (Index 9)
     IGMP Enabled, Active, Forced Querier, Configured for version 3
     Internet address is 10.10.1.2
     IGMP interface limit is 5000
     IGMP interface has 0 group-record states
     IGMP activity: 0 joins, 0 leaves
     IGMP query interval is 126 seconds
     IGMP Startup query interval is 31 seconds
     IGMP Startup query count is 2
     IGMP querier timeout is 257 seconds
     IGMP max query response time is 10 seconds
     Group Membership interval is 262 seconds
     IGMP Last member query count is 2
     Last member query response interval is 1000 milliseconds
```

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 232.10.10.10.

```
vyatta@vyatta:~$show ip igmp ssm-map 232.10.10.10
Group address: 232.10.10.10
Database     : Static
Source list  : 10.10.10.10
```

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.

```
vyatta@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
```

MLD Commands

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.

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 Vyatta Network OS Multicast Routing Configuration Guide*.

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

Interface Type	Syntax	Parameters
Bridge	bridge *brx*	*brx*: The name of a bridge group. The name ranges from br0 through br999.
Data plane	dataplane dp*xy*>pz*v*	dp*x*p*y*p*z*: The name of a data plane interface to which the following applies: • dp*x* identifies a data plane ID

Interface Type	Syntax	Parameters
		NOTE Currently, only dp0 is supported. • p*y* specifies a physical or virtual PCI slot index • p*z* specifies a port index Other supported name formats are the following: • dp*x*em*y*—used for LAN-on-motherboard (LOM) devices that do not have a PCI slot. em*y* specifies an embedded network interface number. • dp*x*port*y*—used for devices in which the PCI slot cannot be identified. port*y* specifies a port index.
Data plane vif	dataplane dp*x*p*y*p*z* vif *vif-id* [vlan *vlan-id*]	dp*x*p*y*p*z*: The name of a data plane interface to which the following applies: • dp*x* specifies a data plane ID NOTE Currently, only dp0 is supported. • p*y* specifies a physical or virtual PCI slot index • p*z* specifies a port index Other supported name formats are the following: • dp*x*em*y*—used for LAN-on-motherboard (LOM) devices that do not have a PCI slot. em*y* specifies an embedded network interface number. • dp*x*port*y*—used for devices in which the PCI slot cannot be identified. port*y* specifies a port index. *vif-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.
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 vtun*x*, where *x* is a nonnegative integer.
Tunnel	tunnel *tunx* or tunnel *tunx* parameters	*tunx*: The identifier of a tunnel interface you are defining. The identifier ranges from tun0 through tun*x*, where *x* is a nonnegative integer.
Virtual tunnel	vti *vtix*	*vtix*: The identifier of a virtual tunnel interface you are defining. The identifier ranges from

Interface Type	Syntax	Parameters
		vti0 through vti*x*, where *x* is a nonnegative integer. **Note:** This interface does not support IPv6.
VRRP	interface *parent-if* vrrp vrrp-group *group* interface	*parent-if*: The type and identifier of a parent interface; for example, dataplane dp0p1p2 or bridge br999. *group*: A VRRP group identifier. 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 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

set interfaces *interface* **ipv6 mld access-group** *acl6-name*

delete interfaces *interface* **ipv6 mld access-group**

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 50.

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 Vyatta Network OS Routing Policies Configuration Guide* for information on creating them.

Modes

Configuration mode

Configuration Statement

```
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 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

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

delete interfaces *interface* **ipv6 mld immediate-leave group-list**

show interfaces *interface* **ipv6 mld 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> ipv6 mld on page 50.

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 Vyatta Network OS Routing Policies Configuration Guide* for information on creating them.

Modes

Configuration mode

Configuration Statement

```
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 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.

interfaces <interface> ipv6 mld last-member-query-count <count>

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 50.

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 {
    ipv6 {
        mld {
            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.

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 57. 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 50.

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 56), 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 50.

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, a limit of 5000 is applied.

Modes

Configuration mode

Configuration Statement

```
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.

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 50.

acl6-name

The name of an IPv6 access control list to be used to define the membership groups. Access control lists are a type of routing policy; see the *Brocade Vyatta Network OS Routing Policies Configuration 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 58. As such, this command is dependent on interfaces <interface> ipv6 mld limit <limit> on page 58 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 50.

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 50.

interval

The interval, in seconds, at which the router sends MLD Query messages. The range is 1 to 18000. 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 50.

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.

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 50.

variable

The robustness variable. The range is 2 to 7.

Modes

Configuration mode

Configuration Statement

```
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 MLD 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> 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 50.

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 50.

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 { **enable** | **disable** } **mld**

Command Default

MLD debugging is disabled.

Parameters

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.

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

Examples

The following example starts MLD debugging.

```
vyatta@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 learned. 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 that is learned.

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 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

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

```
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 globally.

Syntax

set protocols mld ssm-map

delete protocols mld ssm-map

show protocols mld ssm-map

Command Default

SSM mapping is disabled.

Modes

Configuration mode

Configuration Statement

```
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 72.

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 Vyatta Network OS Routing Policies Configuration Guide* for information on creating them.

source

The IPv6 source address to associate with SSM mapping.

Modes

Configuration mode

Configuration Statement

```
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

Clears the specified multicast group and deletes MLD group cache entries. The format is an IPv6 multicast address.

interface

Clears the specified multicast group learned from the specified interface. The format is an interface type, as described in interfaces <interface> ipv6 mld on page 50.

interface *interface*

Clears all multicast groups learned from the specified interface. The format is an interface type, as described in interfaces <interface> ipv6 mld on page 50.

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.

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

The following example clears group membership information for interface dp0p1p2.

```
vyatta@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] | 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 50.

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.

```
vyatta@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
```

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 activity: 0 joins, 0 leaves
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
```

VRF support

Command support for VRF routing instances

VRF allows a Brocade 5600 vRouter to support multiple routing tables, one for each VRF routing instance. Some commands in this guide support VRF and can be applied to particular routing instances.

Use the guidelines in this section to determine correct syntax when adding VRF routing instances to commands. For more information about VRF, refer to *Brocade Vyatta Network OS Basic Routing Configuration Guide*. This guide includes an overview of VRF, VRF configuration examples, information about VRF-specific features, and a list of commands that support VRF routing instances.

Adding a VRF routing instance to a Configuration mode command

For most Configuration mode commands, specify the VRF routing instance at the beginning of a command. Add the appropriate VRF keywords and variable to follow the initial action (**set**, **show**, or **delete**) and before the other keywords and variables in the command.

Configuration mode example: syslog

The following command configures the syslog logging level for the specified syslog host. The command does not include a VRF routing instance, so the command applies to the default routing instance.

```
vyatta@R1# set system syslog host 10.10.10.1 facility all level debug
vyatta@R1# show system syslog
syslog {
    host 10.10.10.1 {
            facility all {
                    level debug
            }
    }
}
```

The following example shows the same command with the VRF routing instance (GREEN) added. Notice that **routing routing-instance GREEN** has been inserted between the basic action (**set** in the example) and the rest of the command. Most Configuration mode commands follow this convention.

```
vyatta@R1# set routing routing-instance GREEN system syslog host 10.10.10.1 facility all level debug
vyatta@R1# show routing
routing {
     routing-instance GREEN {
             system {
                     syslog {
                            host 11.12.13.2:514 {
                                     facility all {
                                             level debug
                                     }
                             }
                     }
             }
     }
}
```

Configuration mode example: SNMP

Some features, such as SNMP, are not available on a per-routing instance basis but can be bound to a specific routing instance. For these features, the command syntax is an exception to the convention of specifying the routing instance at the beginning of Configuration mode commands.

The following example shows how to configure the SNMPv1 or SNMPv2c community and context for the RED and BLUE routing instances. The first two commands specify the RED routing instance as the context for community A and BLUE routing instance as the context for community B. The subsequent commands complete the configuration.

For more information about configuring SNMP, refer to *Brocade Vyatta Network OS Remote Management Configuration Guide*.

```
vyatta@R1# set service snmp community commA context RED
vyatta@R1# set service snmp community commB context BLUE
vyatta@R1# set service snmp view all oid 1
vyatta@R1# set service snmp community commA view all
vyatta@R1# set service snmp community commB view all
vyatta@R1# show service snmp community
 community commA {
        context RED
        view all
 }
 community commB {
        context BLUE
        view all
 }
[edit]
vyatta@vyatta#
```

Adding a VRF routing instance to an Operational mode command

The syntax for adding a VRF routing instance to an Operational mode command varies according to the type of command parameters:

- If the command does not have optional parameters, specify the routing instance at the end of the command.
- If the command has optional parameters, specify the routing instance after the required parameters and before the optional parameters.

Operational mode examples without optional parameters

The following command displays dynamic DNS information for the default routing instance.

```
vyatta@vyatta:~$ show dns dynamic status
```

The following command displays the same information for the specified routing instance (GREEN). The command does not have any optional parameters, so the routing instance is specified at the end of the command.

```
vyatta@vyatta:~$ show dns dynamic status routing-instance GREEN
```

Operational mode example with optional parameters

The following command obtains multicast path information for the specified host (10.33.2.5). A routing instance is not specified, so the command applies to the default routing instance.

```
vyatta@vyatta:~$ mtrace 10.33.2.5 detail
```

The following command obtains multicast path information for the specified host (10.33.2.5) and routing instance (GREEN). Notice that the routing instance is specified before the optional **detail** keyword.

```
vyatta@vyatta:~$ mtrace 10.33.2.5 routing-instance GREEN detail
```

Operational mode example output: SNMP

The following SNMP **show** commands display output for routing instances.

```
vyatta@vyatta:~$ show snmp routing-instance
Routing Instance SNMP Agent is Listening on for Incoming Requests:
Routing-Instance            RDID
-----------------           ----
RED                         5

vyatta@vyatta:~$ show snmp community-mapping
SNMPv1/v2c Community/Context Mapping:
Community                   Context
---------                   -------
commA                       'RED'
commB                       'BLUE'
deva                        'default'


vyatta@vyatta:~$ show snmp trap-target
SNMPv1/v2c Trap-targets:
Trap-target                   Port   Routing-Instance Community
-----------                   ----   ---------------- ---------
1.1.1.1                              'RED'           'test'


vyatta@vyatta:~$ show snmp v3 trap-target
SNMPv3 Trap-targets:
Trap-target                   Port   Protocol Auth Priv Type   EngineID              Routing-Instance User
-----------                   ----   -------- ---- ---- ----   --------              ---------------- ----
2.2.2.2                       '162'  'udp'    'md5'      'infor                      'BLUE'           'test'
```

List of Acronyms

Acronym	Description
ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
AMI	Amazon Machine Image
API	Application Programming Interface
AS	autonomous system
ARP	Address Resolution Protocol
AWS	Amazon Web Services
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CA	certificate authority
CCMP	AES in counter mode with CBC-MAC
CHAP	Challenge Handshake Authentication Protocol
CLI	command-line interface
DDNS	dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DLCI	data-link connection identifier
DMI	desktop management interface
DMVPN	dynamic multipoint VPN
DMZ	demilitarized zone
DN	distinguished name
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	external BGP
EBS	Amazon Elastic Block Storage
EC2	Amazon Elastic Compute Cloud
EGP	Exterior Gateway Protocol
ECMP	equal-cost multipath
ESP	Encapsulating Security Payload
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HDLC	High-Level Data Link Control
I/O	Input/Output
ICMP	Internet Control Message Protocol

Acronym	Description
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IPS	Intrusion Protection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPOA	IP over ATM
IPsec	IP Security
IPv4	IP Version 4
IPv6	IP Version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISM	Internet Standard Multicast
ISP	Internet Service Provider
KVM	Kernel-Based Virtual Machine
L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
MAC	medium access control
mGRE	multipoint GRE
MIB	Management Information Base
MLD	Multicast Listener Discovery
MLPPP	multilink PPP
MRRU	maximum received reconstructed unit
MTU	maximum transmission unit
NAT	Network Address Translation
NBMA	Non-Broadcast Multi-Access
ND	Neighbor Discovery
NHRP	Next Hop Resolution Protocol
NIC	network interface card
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OSPFv2	OSPF Version 2
OSPFv3	OSPF Version 3
PAM	Pluggable Authentication Module
PAP	Password Authentication Protocol
PAT	Port Address Translation
PCI	peripheral component interconnect
PIM	Protocol Independent Multicast
PIM-DM	PIM Dense Mode

Acronym	Description
PIM-SM	PIM Sparse Mode
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PTMU	Path Maximum Transfer Unit
PVC	permanent virtual circuit
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RHEL	Red Hat Enterprise Linux
RIB	Routing Information Base
RIP	Routing Information Protocol
RIPng	RIP next generation
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RSA	Rivest, Shamir, and Adleman
Rx	receive
S3	Amazon Simple Storage Service
SLAAC	Stateless Address Auto-Configuration
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SPT	Shortest Path Tree
SSH	Secure Shell
SSID	Service Set Identifier
SSM	Source-Specific Multicast
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TBF	Token Bucket Filter
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
ToS	Type of Service
TSS	TCP Maximum Segment Size
Tx	transmit
UDP	User Datagram Protocol
VHD	virtual hard disk
vif	virtual interface
VLAN	virtual LAN
VPC	Amazon virtual private cloud
VPN	virtual private network
VRRP	Virtual Router Redundancy Protocol

Acronym	Description
WAN	wide area network
WAP	wireless access point
WPA	Wired Protected Access