53-1003717-03
14 September 2015

Brocade 5600 vRouter Multicast Routing

Reference Guide

Supporting Brocade 5600 vRouter 3.5R6

BROCADE

Contents

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

About This Guide **9**

Multicast Routing Overview **11**
IP multicast 11
Multicast channels 12
Multicast addresses 12
Multicast routing protocols 13
Types of multicast 13
Internet standard multicast 13
Source-specific multicast 13
Supported standards 14
RFCs 14
MIBs 14

Multicast Configuration **15**
Before you begin 15
Basic PIM-SM multicast configuration 15
Configure R1 16
Configure R2 17
Configure RP 18

Multicast Routing Commands **21**
clear ip mroute statistics 22
clear ipv6 mroute statistics 23
interfaces <interface> ip multicast ttl-threshold <ttl> 24
monitor command <mtrace-command> 25
monitor protocol multicast 26
mtrace <host> 28
protocols multicast ip log 29
protocols multicast ipv6 log 31
protocols multicast ip log-warning <warning-limit> 33
protocols multicast ip route-limit <route-limit> 34
protocols multicast ip routing 35
protocols multicast ipv6 log-warning <warning-limit> 36
protocols multicast ipv6 route-limit <route-limit> 37
protocols multicast ipv6 routing 38
reset ip mroute 39

reset ipv6 mroute..... 40
show ip mroute.....41
show ip multicast interface.....43
show ip multicast mrinfo <host>.....44
show ip rpf <source>.....45
show ipv6 mroute.....46
show ipv6 multicast interface.....47
show ipv6 rpf <source>.....48
show monitoring protocols multicast.....49

Supported Data Plane Interfaces.....51

List of Acronyms.....53

Preface

- Document conventions....5
- Brocade resources....7
- Contacting Brocade Technical Support....7
- Document feedback....8

Document conventions

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

Text formatting conventions

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

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at 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.

Convention	Description
[ ]	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.

Notes, cautions, and warnings

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

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

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

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

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

Brocade resources

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

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

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

Release notes are available on MyBrocade under Product Downloads.

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

Contacting Brocade Technical Support

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

Brocade customers

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

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

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: • My Cases through MyBrocade • Software downloads and licensing tools • Knowledge Base	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) • For areas unable to access toll free number: +1-408-333-6061 • Toll-free numbers are available in many countries.	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.

Document feedback

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

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

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

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

About This Guide

This guide describes how to enable and configure multicast routing on Brocade 5600 vRouter (referred to as virtual router, vRouter, or router in the guide).

Multicast Routing Overview

- IP multicast....11
- Multicast channels....12
- Multicast addresses....12
- Multicast routing protocols....13
- Types of multicast....13
- Supported standards....14

IP multicast

There are four types of transmission over a network:

- Unicast—In unicast transmission, a single sender transmits a message to a single receiver (one-to-one). Unicast transmission is signaled to the network by using an IP address in the unicast range. Unicast transmission is supported in both IPv4 and IPv6.
- Broadcast—In broadcast transmission, a sender transmits a message to all possible destinations (“all-hosts on this subnet”) and all receivers receive a copy of the message (one-to-many). In IPv4, broadcast transmission is signaled to the network by using the “broadcast address” 255.255.255.255 or a directed broadcast address formed from the network prefix but using all binary 1s for the host portion of the address. Broadcast transmission is not supported in IPv6; instead, IPv6 defines the “all-nodes” multicast address.
- Multicast—In multicast transmission, a group of receivers interested in a particular stream forms a group (one-to-many). The sender sends the message from its unicast address to the multicast group address. The network routers are responsible for propagating the message to all interested receivers. Multicast groups are identified using a special range of addresses. In IPv4, the former class D addresses compose the multicast range of addresses. In IPv6, multicast addresses are identified from the prefix FF00::/8.
- Anycast—In anycast transmission, a message from a single sender is sent to the topologically “closest” node in a group of potential receivers (one-to-one-of-many). Anycast is used in network load balancing and in certain network protocols, such as Domain Name System (DNS).

IP multicast uses multicast transmission over the IP infrastructure, transmitting to a multicast address at the IP routing level. Networks using IP multicast deliver content to multiple users in various groups—for example, IP multicast is often used for content delivery such as streaming media and IPTV. IP multicast is described in RFC 1112, *Host Extensions for IP Multicasting*.

NOTE

For specific information about the Internet Group Management Protocol (IGMP) and the Multicast Listener Discovery (MLD) protocol, see *Brocade 5600 vRouter IGMP and MLD Reference Guide*.

For specific information about Protocol Independent Multicast (PIM), see *Brocade 5600 vRouter PIM Reference Guide*.

For specific information about Multicast Source Discovery Protocol (MSDP), see *Brocade 5600 vRouter MSDP Reference Guide*.

Multicast channels

To receive a particular multicast data stream, hosts join a multicast group. The group is identified by its multicast address. The communication between the host and router for this purpose is managed by using the Internet Group Management Protocol (IGMP).

Hosts send an IGMP Join message to their local multicast router, signaling their intention to join the group (G), as represented by a multicast address. The source device (S) that delivers the content sends the message addressed to the multicast address of G. The multicast “channel” is the combination of the IP address of the content source and multicast address of the group—called an (S, G) pair. For messages for which the source can be any device, the S is replaced by the asterisk wildcard (“*”), which means “any source.”

Multicast addresses

For IPv4, addresses in the range 224.0.0.0 to 239.255.255.255 are reserved for multicasting. In the classful addressing system, this is registered as class D. In the Classless Inter-Domain Routing (CIDR) addressing model, the prefix of this group is 224.0.0.0/4.

Within the IPv4 multicast range, address assignments are specified in RFC 5771, *IANA Guidelines for IPv4 Multicast Address Assignments.* Table 1 lists a summary of these assignments. Note that, of these addresses, the network address 224.0.0.0 is guaranteed not to be assigned to any group.

TABLE 1 Multicast address assignments

Addresses	Usage
Link Local Scope	
224.0.0.1	All systems on this subnet
224.0.0.2	All routers on this subnet
224.0.0.13	All PIM routers address group
Global Scope	
224.0.1.0 to 238.255.255.255	Allocated for multicast traffic across the Internet. SSM reserves the range 232.0.0.0/8. The addresses 224.0.1.39 and 224.0.1.40 are used for Auto-RP negotiation. You can assign the remaining IP addresses to your ISM applications.
Administrative Scope (AS)	
239.0.0.0/8	Allocated for organizations that own an AS number to multicast across the Internet. The AS number of the organization is embedded in the second and third octets of the multicast IP address. For example, AS64501 is 0xFBF5, with FB and F5 (or 251 and 245 in decimal) representing the second and third octets of the IP address, respectively. The resulting subnet 233.251.24.0 is globally reserved for AS64201 to use. These addresses are called GLOP addresses.

For IPv6, multicast addressing is specified in RFC 3513, *IP Version 6 Addressing Architecture*. In essence, IPv6 multicast addresses are derived from the FF00::/8 prefix.

Multicast routing protocols

The multicast routing protocols supported by the Brocade vRouter are IGMP, Multicast Listener Discovery (MLD), and Protocol Independent Multicast (PIM).

- IGMP controls multicast communication between hosts and multicast routers on IPv4 networks, allowing hosts to manage membership of multicast groups. MLD performs this function on IPv6 networks.
- PIM controls multicast communication between multicast routers, so that they can track packet distribution.

Types of multicast

In IP networks, multicast information is propagated through the use of distribution trees created by the multicast routers. Routers create source trees that provide the shortest path to each destination; these trees are called shortest path trees (SPTs). The source of the multicast message is always the root of an SPT.

Multicast depends on which of two models of multicast is in effect:

- Internet standard multicast on page 13
- Source-specific multicast on page 13

Internet standard multicast

In Internet Standard Multicast (ISM), a receiver can receive messages from any source and from multiple sources. In ISM, receivers are not aware of sources; they express interest in receiving a traffic stream by subscribing to the group of interest (G).

In the ISM model, the multicast router discovers and tracks all multicast sources that are sending messages to an address, maintaining information about all sources, and routing data from all sources to all interested receivers. The router does this by maintaining a state table of (S, G) entries. When the number of sources is large, the burden on the multicast router can become heavy.

Source-specific multicast

In Source-Specific Multicast (SSM), receivers are aware of sources. A receiver explicitly requests a stream from a sender in a group the receiver has joined, using a Join message that specifies the source (an (S, G) Join), and explicitly excludes the use of the wildcard for source—that is, it disallows the (*, G) Join.

Because SSM-enabled hosts track sources of the multicast transmission themselves, multicast routers do not need to discover the multicast sources themselves, and they need to store and maintain only the (*, G) state in the multicast routing table. This greatly reduces the burden on the multicast router.

For IPv4, the destination addresses must be in the range 232.0.0.0/8. For IPv6, the addresses must be in the range FF3x::/96.

SSM is specified in RFC 3569, *An Overview of Source-Specific Multicast (SSM)*.

Supported standards

This section presents the following topics:

- RFCs on page 14
- MIBs on page 14

RFCs

The Brocade Communications Systems, Inc. implementation of multicast routing 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*

MIBs

The Vyatta implementation of multicast routing 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 on the Brocade vRouter, see *Brocade 5600 vRouter Remote Management Reference Guide*.

Multicast Configuration

- Before you begin.....15
- Basic PIM-SM multicast configuration.....15

Before you begin

It is assumed that routers depicted in the examples that follow are configured to provide basic connectivity. This configuration includes the host-name, Ethernet, or data plane interfaces, and gateway-address. See *Brocade 5600 vRouter Quick Start Guide* for information on basic system configuration.

NOTE
In the Brocade vRouter, a data plane interface is an abstraction that represents the underlying physical or virtual Ethernet interface of the system. The terms Ethernet interface and data plane interface are synonymous in this guide.

Basic PIM-SM multicast configuration

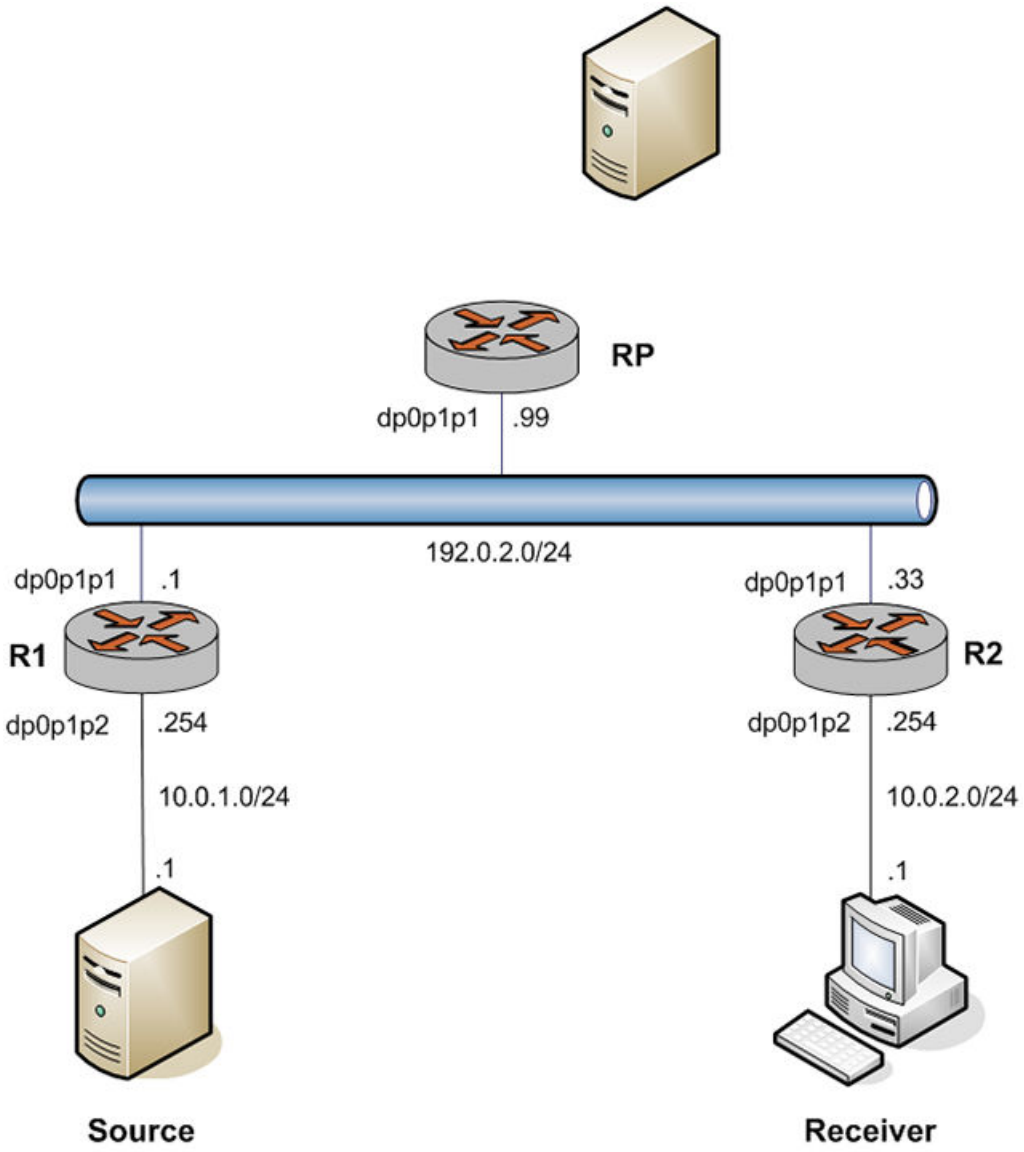
This section presents a configuration example that provides PIM sparse mode multicast capability between the sender of multicast traffic (Source) and a receiver of multicast traffic (Receiver). Three routers are configured for this example: R1, R2 and RP.

R1 and R2 are configured for PIM sparse mode operation and point to RP as the rendezvous point router. RP is configured as the rendezvous point router.

NOTE
It is assumed that the Sender and Receiver contain software to send and receive multicast traffic.

When you have finished the example, these systems will be configured as shown in the following figure.

FIGURE 1 Basic PIM-SM multicast setup



Configure R1

The multicast network in the example extends from R1 through the 192.0.2.0/24 LAN segment to R2 and RP. In this example, you configure R1 for PIM sparse mode multicast operation.

Table 2 creates a PIM sparse mode multicast configuration on R1.

TABLE 2 Creating a PIM sparse mode configuration on R1

Step	Command
Configure PIM sparse mode on dp0p1p1.	`vyatta@R1# set interfaces dataplane dp0p1p1 ip pim mode sparse`

TABLE 2 Creating a PIM sparse mode configuration on R1 (Continued)

Step	Command
Commit the configuration.	`vyatta@R1# commit`

View the configuration.	`vyatta@R1# show interfaces dataplane dp0p1p1 ip`
	`  pim {`
	`  mode sparse`
	`  }`

Configure PIM sparse mode on dp0p1p2.	`vyatta@R1# set interfaces dataplane dp0p1p2 ip pim mode sparse`
Commit the configuration.	`vyatta@R1# commit`

View the configuration.	`vyatta@R1# show interfaces dataplane dp0p1p2 ip`
	`  pim {`
	`  mode sparse`
	`  }`

Configure multicast routing.	`vyatta@R1# set protocols multicast ip routing`
Specify the location of the rendezvous point router.	`vyatta@R1# set protocols pim rp-address 192.0.2.99`
Commit the configuration.	`vyatta@R1# commit`

View the configuration.	`vyatta@R1# show protocols`
	`  multicast {`
	`  ip {`
	`  routing {`
	`  }`
	`  }`
	`  }`
	`  pim {`
	`  rp-address 192.0.2.99 {`
	`  }`
	`  }`

Configure R2

The multicast network in the example extends from R1 through the 192.0.2.0/24 LAN segment to R2 and RP. In this example, you configure R2 for PIM sparse mode multicast operation.

Table 3 creates a PIM sparse mode multicast configuration on R2.

TABLE 3 Creating a PIM sparse mode configuration on R2

Step	Command
Configure PIM sparse mode on dp0p1p1.	`vyatta@R2# set interfaces dataplane dp0p1p1 ip pim mode sparse`
Commit the configuration.	`vyatta@R2# commit`

View the configuration.	`vyatta@R2# show interfaces dataplane dp0p1p1 ip`
	`  pim {`
	`  mode sparse`
	`  }`

Configure PIM sparse mode on dp0p1p2.	`vyatta@R2# set interfaces dataplane dp0p1p2 ip pim mode sparse`
Commit the configuration.	`vyatta@R2# commit`

TABLE 3 Creating a PIM sparse mode configuration on R2 (Continued)

Step	Command

View the configuration.	`vyatta@R2# show interfaces dataplane dp0p1p2 ip`
	`    pim {`
	`        mode sparse`
	`    }`

Configure multicast routing.	`vyatta@R2# set protocols multicast ip routing`
Specify the location of the rendezvous point router.	`vyatta@R2# set protocols pim rp-address 192.0.2.99`
Commit the configuration.	`vyatta@R2# commit`

View the configuration.	`vyatta@R2# show protocols`
	`    multicast {`
	`        ip {`
	`            routing {`
	`            }`
	`        }`
	`    }`
	`    pim {`
	`        rp-address 192.0.2.99 {`
	`        }`
	`    }`

Configure RP

The multicast network in the example extends from R1 through the 192.0.2.0/24 LAN segment to R2 and RP. In this example, you configure RP for PIM sparse mode multicast operation.

Table 4 creates a PIM sparse mode multicast configuration on RP.

TABLE 4 Creating a PIM sparse mode configuration on RP

Step	Command
Configure PIM sparse mode on dp0p1p1.	`vyatta@RP# set interfaces dataplane dp0p1p1 ip pim mode sparse`
Commit the configuration.	`vyatta@RP# commit`

View the configuration.	`vyatta@RP# show interfaces dataplane dp0p1p1 ip`
	`    pim {`
	`        mode sparse`
	`    }`

Configure multicast routing.	`vyatta@RP# set protocols multicast ip routing`
Specify the location of the rendezvous point router.	`vyatta@RP# set protocols pim rp-address 192.0.2.99`
Commit the configuration.	`vyatta@RP# commit`

TABLE 4 Creating a PIM sparse mode configuration on RP (Continued)

Step	Command

View the configuration.	`vyatta@RP# show protocols`
	`  multicast {`
	`  ip {`
	`  routing {`
	`  }`
	`  }`
	`  }`
	`  pim {`
	`  rp-address 192.0.2.99 {`
	`  }`
	`  }`

Multicast Routing Commands

- clear ip mroute statistics....22
- clear ipv6 mroute statistics....23
- interfaces <interface> ip multicast ttl-threshold <ttl>....24
- monitor command <mtrace-command>....25
- monitor protocol multicast....26
- mtrace <host>....28
- protocols multicast ip log....29
- protocols multicast ipv6 log....31
- protocols multicast ip log-warning <warning-limit>....33
- protocols multicast ip route-limit <route-limit>....34
- protocols multicast ip routing....35
- protocols multicast ipv6 log-warning <warning-limit>....36
- protocols multicast ipv6 route-limit <route-limit>....37
- protocols multicast ipv6 routing....38
- reset ip mroute....39
- reset ipv6 mroute....40
- show ip mroute....41
- show ip multicast interface....43
- show ip multicast mrinfo <host>....44
- show ip rpf <source>....45
- show ipv6 mroute....46
- show ipv6 multicast interface....47
- show ipv6 rpf <source>....48
- show monitoring protocols multicast....49

clear ip mroute statistics

Clears IPv4 statistics for multicast routing.

Syntax **clear ip mroute statistics** [**group** *group* [**source** *source*]]

Command Default When used with no option, this command clears all IPv4 statistics for multicast routing.

Parameters *group*

Clears statistics for the specified IPv4 multicast group in IPv4 multicast address format.

source

Used in source-specific multicast. Clears statistics for the specified IPv4 multicast source. The format is an IPv4 multicast address.

Modes Operational mode

Usage Guidelines Use this command to clear statistics for multicast routing.

clear ipv6 mroute statistics

Clears IPv6 statistics for multicast routing.

Syntax **clear ipv6 mroute statistics** [**group** *group* [**source** *source*]]

Command Default When used with no option, this command clears all IPv6 statistics for multicast routing.

Parameters

group *group*

Clears statistics for the specified IPv6 multicast group. The format is an IPv6 multicast address.

source *source*

Used in source-specific multicast. Clears statistics for the specified IPv6 multicast source. The format is an IPv6 multicast address.

Modes Operational mode

Usage Guidelines Use this command to clear IPv6 statistics for multicast routing.

interfaces <interface> ip multicast ttl-threshold <ttl>

Sets the time-to-live (TTL) threshold for multicast packets.

Syntax

set interfaces *interface* **ip multicast ttl-threshold** *ttl*

delete interfaces *interface* **ip multicast ttl-threshold**

show interfaces *interface* **ip multicast ttl-threshold**

Command Default

The TTL for multicast packets is 0. The default value 0 means that all multicast packets are forwarded out to the interface.

Parameters

interface

The type keyword and identifier of an interface. For detailed keywords and arguments that can be specified as interfaces, refer to Supported Data Plane Interfaces on page 51.

ttl

The TTL value is the hop count. The range is 0 through 255. The default is 0.

Modes

Configuration mode

Configuration Statement

```
interfaces interface {
    ip {
        multicast {
            ttl-threshold ttl
        }
    }
}
```

Usage Guidelines

Use this command to configure the TTL threshold for multicast packets being forwarded from the specified interface. Only multicast packets with a TTL value greater than the threshold are forwarded.

Use the **set** form of this command to configure the multicast TTL value.

Use the **delete** form of this command to restore the default TTL value for multicast.

Use the **show** form of this command to show multicast TTL configuration.

monitor command <mtrace-command>

Monitors an **mtrace** command.

Syntax **monitor command** *mtrace-command*

run monitor command *mtrace-command*

Parameters *mtrace-command*

The **mtrace** command to be monitored. The **mtrace** command must be enclosed in quotation marks.

Modes Operational mode.

Configuration mode

Usage Guidelines Use this command to display the output of an **mtrace** command. The session stays open and display information is refreshed every two seconds.

Use the **run** form of this command in configuration mode.

monitor protocol multicast

Sets debugging options for multicast routing.

Syntax **monitor protocol multicast** [[**background** { **start** | **stop** }] | { **enable** | **disable** } { **ip** | **ipv6** } [**event** | **fib-msg** | **mrib-msg** | **mrt** | **mtrace** | **mtrace-detail** | **nsm-msg** | **register-msg** | **stats** | **vif**]]

Command Default Multicast debugging is disabled.

Parameters

background
Performs debugging operations in the background.

start
Starts debugging in the background.

stop
Stops debugging in the background.

enable
Enables the specified debugging option.

disable
Disables the specified debugging option.

ip
Specifies IPv4 multicast debugging.

ipv6
Specifies IPv6 multicast debugging.

event
Displays debugging messages for multicast events.

fib-msg
Reports all forwarding information base messages.

mrib-msg
Reports all multicast routing information base messages.

mrt
Displays debugging messages for multicast routes.

mtrace
Displays multicast traceroute debugging.

mtrace-detail
Displays detailed multicast traceroute debugging.

nsm-msg
Reports all Network Services Module messages.

register-msg
Reports all Protocol Independent Multicast (PIM) register messages.

stats
Displays debugging messages for multicast statistics.

vif
Displays debugging messages for multicast-enabled vif interfaces.

Modes Operational mode

Usage Guidelines Use this command to enable or disable debugging for multicast and to configure multicast debugging options.

Examples The following example starts debugging in the background for IPv4 multicast events.

```
vyatta@vyatta:~$monitor protocol multicast enable ip event
```

The following example disables all IPv6 multicast debugging.

```
vyatta@vyatta:~$monitor protocol multicast disable ipv6
```

mtrace <host>

Displays the route that packets take from a multicast source.

Syntax **set mtrace** *host* [**destination** *addr* [**group** *group* [**detail**] | **detail**] | **group** *group* [**destination** *addr* [**detail**] | **detail**] | **detail**]

Command Default Output shows routes from the source host to the host on which the command is entered.

Parameters *host*

The host that is the source for the trace. The host is either a name (if DNS is being used on the network) or an IPv4 or IPv6 unicast address.

addr

The host that is the destination for the trace. The host is either an IPv4 or IPv6 unicast address.

group

The multicast group to trace. The format is an IPv4 or IPv6 multicast address.

detail

Displays detailed output. This output includes IP multicast packet-rate and packet-loss information.

Modes Operational mode

Usage Guidelines Use this command to show the path from a source to a receiver in a multicast network.

Examples The following example displays a trace from 10.14.0.1 through 10.12.0.2 using group 226.0.0.1.

```
vyatta@vyatta:~$mtrace 10.14.0.1 destination 10.12.0.2 group 226.0.0.1
Mtrace from 10.14.0.1 to 10.12.0.2 via group 226.0.0.1
Querying full reverse path...
  0  ? (10.12.0.2)
 -1  ? (10.12.0.2)  PIM  thresh^ 1  RPF interface
 -2  ? (10.12.0.1)  PIM  thresh^ 1
 -3  ? (10.14.0.1)
Round trip time 1 ms
```

The following example displays a detailed trace from 10.14.0.1 through 10.12.0.2 using group 226.0.0.1.

```
vyatta@vyatta:~$mtrace 10.14.0.1 destination 10.12.0.2 group 226.0.0.1 detail
Mtrace from 10.14.0.1 to 10.12.0.2 via group 226.0.0.1
Round trip time 0 ms

Waiting to accumulate statistics... Results after 10 seconds:

  Source        Response Dest    Packet Statistics For     Only For Traffic
10.14.0.1       10.12.0.2        All Multicast Traffic     From 10.14.0.1
     v        __/  rtt    0 ms    Lost/Sent = Pct  Rate       To 226.0.0.1
10.14.0.1
10.12.0.1
     v     ^      ttl    1          0            0 pps       0            0 pps
10.12.0.2                    RPF interface
     v      \__    ttl    2
10.12.0.2       10.12.0.2
  Receiver      Query Source
```

protocols multicast ip log

Enables IPv4 MRIB logs.

Syntax **set protocols multicast ip log** { **all**|**event**|**fib-msg**|**mrib-msg**|**mrt**|**mtrace**|**mtrace-detail**|**nsm-msg**|**register-msg**|**stats**|**vif**}

delete protocols multicast ip log { **all**|**event**|**fib-msg**|**mrib-msg**|**mrt**|**mtrace**|**mtrace-detail**|**nsm-msg**|**register-msg**|**stats**|**vif**}

show protocols multicast ip log { **all**|**event**|**fib-msg**|**mrib-msg**|**mrt**|**mtrace**|**mtrace-detail**|**nsm-msg**|**register-msg**|**stats**|**vif**}

Command Default None

Parameters

all
Enables MRIB debugging for all multicast protocol parameters.

event
Enables MRIB debugging for all multicast events.

fib-msg
Enables MRIB debugging for only multicast FIB events.

mrib-msg
Enables MRIB debugging for only multicast RIB events.

mrt
Enables MRIB debugging for multicast routes.

mtrace
Enables MRIB debugging for multicast trace routes.

mtrace-detail
Enables MRIB debugging for multicast traceroute messages.

nsm-msg
Enables MRIB debugging for multicast NSM messages.

register-msg
Enables MRIB debugging for multicast PIM register messages.

stats
Enables MRIB debugging for multicast statistics.

vif
Enables MRIB debugging for multicast virtual interfaces.

Modes Configuration mode

Configuration Statement

```
protocols {
multicast ip {
          log {
            all
          event
        fib-msg
       mrib-msg
            mrt
         mtrace
   mtrace-detail
        nsm-msg
    register-msg
          stats
            vif
            }
          }
        }
```

Usage Guidelines Use the **set** form of this command to enable IPv4 multicast routing information base (MRIB) logs.

Use the **delete** form of this command to remove IPv4 MRIB logs.

Use the **show** form of this command to view IPv4 MRIB logs.

protocols multicast ipv6 log

Enables IPv6 MRIB logs.

Syntax **set protocols multicast ipv6 log** { **all**|**event**|**fib-msg**|**mrib-msg**|**mrt**|**mtrace**|**mtrace-detail**|**nsm-msg**|**register-msg**|**stats**|**vif**}

delete protocols multicast ipv6 log { **all**|**event**|**fib-msg**|**mrib-msg**|**mrt**|**mtrace**|**mtrace-detail**|**nsm-msg**|**register-msg**|**stats**|**vif**}

show protocols multicast ipv6 log { **all**|**event**|**fib-msg**|**mrib-msg**|**mrt**|**mtrace**|**mtrace-detail**|**nsm-msg**|**register-msg**|**stats**|**vif**}

Command Default None

Parameters

all
Enables MRIB debugging for all multicast protocol parameters.

event
Enables MRIB debugging for all multicast events.

fib-msg
Enables MRIB debugging for only multicast FIB events.

mrib-msg
Enables MRIB debugging for only multicast RIB events.

mrt
Enables MRIB debugging for multicast routes.

mtrace
Enables MRIB debugging for multicast trace routes.

mtrace-detail
Enables MRIB debugging for multicast traceroute messages.

nsm-msg
Enables MRIB debugging for multicast NSM messages.

register-msg
Enables MRIB debugging for multicast PIM register messages.

stats
Enables MRIB debugging for multicast statistics.

vif
Enables MRIB debugging for multicast virtual interfaces.

Modes Configuration mode

Configuration Statement

```
protocols {
multicast ipv6 {
          log {
            all
          event
        fib-msg
       mrib-msg
            mrt
         mtrace
   mtrace-detail
        nsm-msg
    register-msg
          stats
            vif
              }
           }
         }
```

Usage Guidelines Use the **set** form of this command to enable IPv6 multicast routing information base (MRIB) logs.

Use the **delete** form of this command to remove IPv6 MRIB logs.

Use the **show** form of this command to view IPv6 MRIB logs.

protocols multicast ip log-warning <warning-limit>

Sets a warning threshold for IPv4 multicast routes.

Syntax **set protocols multicast ip log-warning** *warning-limit*

delete protocols multicast ip log-warning

show protocols multicast ip log-warning

Command Default If this value is not configured, the system issues a warning only when the maximum number of routes has been reached.

Parameters *warning-limit*

The number of IPv4 multicast routes that causes the system to generate a warning. The value configured for this argument must not exceed the value set for the maxmimum route limit that is configured by using the **protocols multicast ip route-limit** *route-limit* command. The range is 1 through 2147483647.

Modes Configuration mode

Configuration Statement

```
protocols {
    multicast {
        ip {
            log-warning warning-limit
        }
    }
}
```

Usage Guidelines Use this command to configure the warning threshold for IPv4 routes in the multicast routing table. When this limit is exceeded, the system continues to generate a message until the maximum number of multicast routes is reached that is configured by using the **protocols multicast ip route-limit** *route-limit* command.

Use the **set** form of this command to configure the warning threshold for IPv4 multicast routes.

Use the **delete** form of this command to restore the default IPv4 warning threshold.

Use the **show** form of this command to show the IPv4 warning threshold configuration.

protocols multicast ip route-limit <route-limit>

Sets the maximum number of IPv4 routes that can be added to the multicast routing table.

Syntax **set protocols multicast ip route-limit** *route-limit*

delete protocols multicast ip route-limit

show protocols multicast ip route-limit

Command Default The maximum number of IPv4 multicast routes is 2,147,483,647.

Parameters *route-limit*

The maximum number of IPv4 routes that can be added to the multicast routing table. The value configured for this argument must be greater than or equal to the log warning limit that is configured by using the **protocols multicast ip log-warning** *warning-limit* command. The range is 1 through 2147483647.

Modes Configuration mode

Configuration Statement

```
protocols {
    multicast {
        ip {
            route-limit route-limit
        }
    }
}
```

Usage Guidelines Use this command to limit the number of IPv4 routes that can be added to the multicast routing table.

Use the **set** form of this command to specify the IPv4 multicast route limit.

Use the **delete** form of this command to restore the default IPv4 multicast route limit.

Use the **show** form of this command to show the IPv4 multicast route limit configuration.

protocols multicast ip routing

Enables IPv4 multicast routing.

Syntax **set protocols multicast ip routing**

delete protocols multicast ip routing

show protocols multicast ip routing

Command Default IPv4 multicast routing is disabled.

Modes Configuration mode

Configuration Statement

```
protocols {
    multicast {
        ip {
            routing {
            }
        }
    }
}
```

Usage Guidelines Use this command to enable the system to use multicast routing protocols for IPv4 traffic.

When this configuration node is deleted, multicast routing protocols such as the Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM) do not work for IPv4 traffic, even if configured.

Use the **set** form of this command to enable multicast routing.

Use the **delete** form of this command to remove the multicast routing configuration.

Use the **show** form of this command to display the multicast routing configuration.

protocols multicast ipv6 log-warning <warning-limit>

Sets the warning threshold for IPv6 multicast routes.

Syntax **set protocols multicast ipv6 log-warning** *warning-limit*

delete protocols multicast ipv6 log-warning

show protocols multicast ipv6 log-warning

Command Default If this value is not configured, the system issues a warning only when the maximum number of routes has been reached.

Parameters *warning-limit*

The number of IPv6 multicast routes that causes the system to generate a warning. The value configured for this argument must not exceed the value set for the maximum route limit that is configured by using the **protocols multicast ipv6 route-limit** *route-limit* command. The range is 1 through 2147483647.

Modes Configuration mode

Configuration Statement

```
protocols {
    multicast {
        ipv6 {
            log-warning warning-limit
        }
    }
}
```

Usage Guidelines Use this command to configure the warning threshold for IPv6 routes in the multicast routing table. When this limit is exceeded, the system continues to generate a message until the maximum number of multicast routes is reached that is configured by using the **protocols multicast ipv6 route-limit** *route-limit* command.

Use the **set** form of this command to configure the IPv6 warning threshold.

Use the **delete** form of this command to restore the default IPv6 warning threshold.

Use the **show** form of this command to show the IPv6 warning threshold configuration.

protocols multicast ipv6 route-limit <route-limit>

Sets the maximum number of IPv6 routes that can be added to the multicast routing table.

Syntax **set protocols multicast ipv6 route-limit** *route-limit*

delete protocols multicast ipv6 route-limit

show protocols multicast ipv6 route-limit

Command Default The maximum number of IPv6 multicast routes is 2,147,483,647.

Parameters *route-limit*

The maximum number of IPv6 routes that can be added to the multicast routing table. The value configured for this argument must be greater than or equal to the log warning limit that is configured by using the **protocols multicast ip log-warning** *warning-limit* command. The range is 1 through 2147483647.

Modes Configuration mode

Configuration Statement

```
protocols {
    multicast {
        ip {
            route-limit route-limit
        }
    }
}
```

Usage Guidelines Use this command to limit the number of IPv6 routes that can be added to the multicast routing table.

Use the **set** form of this command to specify the IPv6 multicast route limit.

Use the **delete** form of this command to restore the default IPv6 multicast route limit.

Use the **show** form of this command to show the IPv6 multicast route limit configuration.

protocols multicast ipv6 routing

Enables IPv6 multicast routing.

Syntax **set protocols multicast ipv6 routing**

delete protocols multicast ipv6 routing

show protocols multicast ipv6 routing

Command Default IPv6 multicast routing is disabled.

Modes Configuration mode

Configuration Statement

```
protocols {
    multicast {
        ipv6 {
            routing {
            }
        }
    }
}
```

Usage Guidelines Use this command to enable the system to use multicast routing protocols for IPv6 traffic.

When this configuration is deleted, multicast routing protocols such as the Multicast Listener Discovery (MLD) and PIM do not work for IPv6 traffic, even if configured.

Use the **set** form of this command to enable IPv6 multicast routing.

Use the **delete** form of this command to remove IPv6 multicast routing configuration.

Use the **show** form of this command to display the IPv6 multicast routing configuration.

reset ip mroute

Removes IPv4 entries from the multicast routing information base of the specified group.

Syntax **reset ip mroute** [**group** *group* [**source** *source*]]

Command Default When used with no option, this command deletes all routes from the multicast routing information base.

Parameters *group*

The IPv4 multicast group in IPv4 multicast address format. Routes are removed for the specified group.

source

Used in source-specific multicast. Removes routes for the specified IPv4 multicast source. The format is an IPv4 multicast address.

Modes Operational mode

Usage Guidelines Use this command to remove IPv4 routes from the multicast routing and forwarding information bases.

Each multicast routing protocol has a distinct command for clearing multicast routes from the routing table for the protocol.

reset ipv6 mroute

Removes IPv6 entries from the multicast routing information base.

Syntax **reset ipv6 mroute** [**group** *group* [**source** *source*]]

Command Default When used with no option, this command deletes all routes from the multicast routing information base.

Parameters

group *group*

Removes IPv6 routes for the specified multicast group. The format is an IPv6 multicast address.

source *source*

Used in source-specific multicast. Shows multicast routes for the specified IPv6 multicast source. The format is an IPv6 address.

Modes Operational mode

Usage Guidelines Use this command to remove IPv6 routes from the multicast routing and forwarding information bases. Each multicast routing protocol has a distinct command for clearing multicast routes from the routing table for the protocol.

show ip mroute

Displays the IPv4 multicast routing table.

Syntax **show ip mroute** [**group** *group* [**source** *source*]] [**dense** | **sparse** | **count** | **summary**]

Command Default When used with no option, this command displays information for the complete IPv4 multicast routing table.

Parameters

group *group*

Shows IPv4 multicast routes for the specified multicast group. The format is an IPv4 multicast address.

source *source*

Used in source-specific multicast. Shows multicast routes for the specified IPv4 multicast source. The format is an IPv4 multicast address.

dense

Shows dense-mode IPv4 multicast routes.

sparse

Shows sparse-mode IPv4 multicast routes.

count

Shows IPv4 multicast-route and packet-count information.

summary

Shows abbreviated IPv4 multicast route information.

Modes Operational mode

Usage Guidelines Use this command to display the IPv4 multicast routing table.

Examples The following example shows how to display an IPv4 multicast routing table.

```
vyatta@vyatta:~$show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:00:31, stat expires 00:02:59
Owner PIM-SM, Flags: TF
Incoming interface: wm0
Outgoing interface list:
wm1 (1)
vyatta@vyatta:~$
```

The following example shows how to display routes for multicast group 224.0.1.3 and source 10.10.1.52.

```
vyatta@vyatta:~$show ip mroute group 224.0.1.3 source 10.10.1.52
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:03:24, stat expires 00:01:28
Owner PIM-SM, Flags: TF
Incoming interface: wm0
Outgoing interface list:
wm1 (1)vyatta@vyatta:~$
```

The following example shows how to display packet counts for multicast routes.

```
vyatta@vyatta:~$show ip mroute count

IP Multicast Statistics
Total 1 routes using 132 bytes memory
Route limit/Route threshold: 2147483647/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 1/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 1/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:10
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent
(10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
vyatta@vyatta:~$
```

The following example shows how to display a summary of the multicast routing table.

```
vyatta@vyatta:~$show ip mroute summary

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), 00:01:32/00:03:20, PIM-SM, Flags: TF
vyatta@vyatta:~$
```

show ip multicast interface

Displays information about IPv4 multicast-enabled interfaces.

Syntax **show ip multicast interface** [*interface*]

Command Default When used with no option, this command shows information for all IPv4 multicast-enabled interfaces.

Parameters *interface*

Mandatory. The type keyword and identifier of an interface. For detailed keywords and arguments that can be specified as interfaces, refer to Supported Data Plane Interfaces on page 51.

Modes Operational mode

Usage Guidelines Use this command to show operational information for IPv4 multicast-enabled interfaces.

Examples The following example shows how to display all IPv4 multicast interface information.

```
vyatta@vyatta:~$ show ip multicast

Interface Vif Owner TTL Local Remote Uptime
Idx Module Address Address
wlm0 0 PIM-SM 1 192.168.1.53 0.0.0.0 00:04:26
Register 1 1 192.168.1.53 0.0.0.0 00:04:26
wlm1 2 PIM-SM 1 192.168.10.53 0.0.0.0 00:04:25
vyatta@vyatta:~$
```

The following example shows how to display IPv4 multicast interface information for the wlm0 interface.

```
vyatta@vyatta:~$ show ip multicast interface wlm0

Interface Vif Owner TTL Local Remote Uptime
Idx Module Address Address
wlm0 0 PIM-SM 1 192.168.1.53 0.0.0.0 00:05:17
vyatta@vyatta:~$
```

show ip multicast mrinfo <host>

Displays information about IPv4 multicast neighbors.

Syntax **show ip multicast mrinfo host** [**source-addr** | **interface**]

Parameters

host

The host that is being queried. The host is either a name (if DNS is being used on the network) or an IPv4 unicast address.

source-addr

Optional. The source address used in the mrinfo request. If omitted, the IPv4 address of the interface on which the request is sent is used.

interface

Optional. The source address used in the mrinfo request is the IPv4 address of the interface specified. If omitted, the IPv4 address of the interface on which the request is sent is used. For detailed keywords and arguments that can be specified as interfaces, refer to Supported Data Plane Interfaces on page 51.

Modes Operational mode

Usage Guidelines Use this command to show information about IPv4 multicast neighbors.

Examples The following example shows how to display information about the IPv4 multicast neighbor mbone.phony.dom.net.

```
vyatta@vyatta:~$ show ip multicast mrinfo mbone.phony.dom.net
127.148.176.10 (mbone.phony.dom.net) [version 3.3]:
127.148.176.10 -> 0.0.0.0 (?) [1/1/querier]
127.148.176.10 -> 127.0.8.4 (mbone2.phony.dom.net) [1/45/tunnel]
127.148.176.10 -> 105.1.41.9 (momoney.com) [1/32/tunnel/down]
127.148.176.10 -> 143.192.152.119 (mbone.dipu.edu) [1/32/tunnel]
vyatta@vyatta:~$
```

show ip rpf <source>

Displays Reverse Path Forwarding (RPF) information for a specific IPv4 multicast source address.

Syntax **show ip rpf** *source*

Parameters *source*

An IPv4 multicast source address.

Modes Operational mode

Usage Guidelines Use this command to display the RPF information for a specific IPv4 multicast source address.

Examples The following example shows how to display RPF information for the source address 172.18.92.1.

```
vyatta@vyatta:~$show ip rpf 172.18.92.1
RPF Information for 172.18.92.1
    RPF interface: dp0p1p1
    RPF neighbor: 172.18.93.100
    RPF prefix length: 24
    RPF distance: 1
    RPF mteric: 1
vyatta@vyatta:~$
```

show ipv6 mroute

Displays the IPv6 multicast routing table.

Syntax **show ipv6 mroute** [**group** *group* [**source** *source*]] [**dense** | **sparse** | **count** | **summary**]

Command Default When used with no option, this command displays information for the complete IPv6 multicast routing table.

Parameters

group *group*

Shows IPv6 multicast routes for the specified multicast group. The format is an IPv6 multicast address.

source *source*

Used in source-specific multicast. Shows multicast routes for the specified IPv6 multicast source. The format is an IPv6 multicast address.

dense

Shows dense-mode IPv6 multicast routes.

sparse

Shows sparse-mode IPv6 multicast routes.

count

Shows IPv6 multicast-route and packet-count information.

summary

Shows abbreviated IPv6 multicast route information.

Modes Operational mode

Usage Guidelines Use this command to display the IPv6 multicast routing table.

Examples The following example shows how to display an IPv6 multicast routing table.

```
vyatta@vyatta:~$show ipv6 mroute

IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface
(3ffe:10:10:1::96, ff1e::10), uptime 00:00:09, stat expires 00:03:21
Owner PIM-SMv6, Flags: TF
Incoming interface: wm0
Outgoing interface list:
wm1
(3ffe:10:10:1::96, ff1e::12), uptime 00:00:02, stat expires 00:03:28
Owner PIM-SMv6, Flags: TF
Incoming interface: wm0
Outgoing interface list:
wm1
vyatta@vyatta:~$
```

show ipv6 multicast interface

Displays information about IPv6 multicast-enabled interfaces.

Syntax **show ipv6 multicast interface** [*interface*]

Command Default When used with no option, this command shows information for all IPv6 multicast-enabled interfaces.

Parameters *interface*

The type keyword and identifier of an interface. For detailed keywords and arguments that can be specified as interfaces, refer to Supported Data Plane Interfaces on page 51.

Modes Operational mode

Usage Guidelines Use this command to show operational information for IPv6 multicast-enabled interfaces.

Examples The following example shows how to display all IPv6 multicast interface information.

```
vyatta@vyatta:~$show ipv6 multicast

Interface Mif Owner Uptime
Idx Module
wlm0 0 PIM-SMv6 00:17:18
Register 1 00:17:18
wlm1 2 PIM-SMv6 00:17:18
vyatta@vyatta:~$
```

The following example shows how to display all IPv6 multicast interface information for the wlm0 interface.

```
vyatta@vyatta:~$show ipv6 multicast wlm0

Interface Mif Owner Uptime
Idx Module
wlm0 0 PIM-SMv6 00:19:06
vyatta@vyatta:~$
```

show ipv6 rpf <source>

Displays Reverse Path Forwarding (RPF) information for a specific IPv6 multicast source address.

Syntax **show ipv6 rpf** *source*

Parameters *source*

An IPv6 multicast source address.

Modes Operational mode

Usage Guidelines Use this command to display RPF information for a specific IPv6 multicast source address.

Examples The following example shows how to display RPF information for the IPv6 source address 2036::6.

```
vyatta@vyatta:~$show ipv6 rpf 2036::6
RPF Information for 2036::6
    RPF interface: dp0p1p3
    RPF neighbor: fe80::250:56ff:fe9b:5aaf
    RPF prefix length: 64
    RPF distance: 2
    RPF mteric: 110
vyatta@vyatta:~$
```

show monitoring protocols multicast

Shows information about multicast debugging configuration.

Syntax **show monitoring protocols multicast** { **ip** | **ipv6** }

Parameters **ip**

Shows what IPv4 multicast debugging options are enabled.

ipv6

Shows what IPv6 multicast debugging options are enabled.

Modes Operational mode

Usage Guidelines Use this command to see what debugging options are currently enabled for IPv4 or IPv6 multicast routing.

Examples The following example shows how to display the current configuration for IPv4 multicast debugging.

```
vyatta@vyatta:~$show monitoring protocols multicast ip

Debugging status:
MRIBv4 event debugging is on
MRIBv4 VIF debugging is on
MRIBv4 route debugging is on
MRIBv4 route statistics debugging is on
MRIBv4 FIB message debugging is on
MRIBv4 PIM Register message debugging is on
MRIBv4 NSM IPC message debugging is on
MRIBv4 MRIB IPC message debugging is on
MRIBv4 traceroute debugging is on
MRIBv4 traceroute detailed debugging is on
vyatta@vyatta:~$
```

Supported Data Plane Interfaces

The following table shows the syntax and parameters of the supported types of data plane interfaces.

Interface Type	Syntax	Parameters
Data plane	**dataplane** *interface-name*	*interface-name*: The name of a data plane interface. Following are the supported formats of the interface name: • **dp***x***p***y***p***z*—The name of a data plane interface, where — **dp***x* specifies the data plane identifier (ID). Currently, only dp0 is supported. — p*y* specifies a physical or virtual PCI slot index (for example, p129). — **p***z* specifies a port index (for example, p1). For example, dp0p1p2, dp0p160p1, and dp0p192p1. • **dp***x***em***y* —The name of a data plane interface on a LAN-on-motherboard (LOM) device that does not have a PCI slot, where **em***y* specifies an embedded network interface number (typically, a small number). For example, dp0em3. • **dp***x***s***y* —The name of a data plane interface on a device that is installed on a virtual PCI slot, where *x***s***y* specifies an embedded network interface number (typically, a small number). For example, dp0s2. Currently, this format applies only when using the KVM or Hyper-V platforms. • **dp***x***P***n***p***y***p***z* —The name of a data plane interface on a device that is installed on a secondary PCI bus, where **P***n* specifies the bus number. You can use this format to name data plane interfaces on large physical devices with multiple PCI buses. For these devices, it is possible to have network interface cards installed on different buses with these cards having the same slot ID. The value of *n* must be an integer greater than 0. For example, dp0P1p162p1 and dp0P2p162p1.
Data plane vif	**dataplane** *interface-name* **vif** *vif-id* [**vlan** *vlan-id*]	*interface-name*: Refer to the preceding description. *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.

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

Acronym	Description
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
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

Acronym	Description
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
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

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