JUNIPER NETWORKS

JunosE™ Software for E Series™ Broadband Services Routers

IPv6 Multicast Routing

Release
14.3.x

Published: 2013-07-15

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

JunosE™ Software for E Series™ Broadband Services Routers IPv6 Multicast Routing
Release 14.3.x

Revision History
July 2013—FRS JunosE 14.3.x

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

E Series and JunosE Documentation and Release Notes

For a list of related JunosE documentation, see http://www.juniper.net/techpubs/software/index.html.

If the information in the latest release notes differs from the information in the documentation, follow the *JunosE Release Notes.*

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Audience

This guide is intended for experienced system and network specialists working with Juniper Networks E Series Broadband Services Routers in an Internet access environment.

E Series and JunosE Text and Syntax Conventions

Table 1 on page xii defines notice icons used in this documentation.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xii defines text and syntax conventions that we use throughout the E Series and JunosE documentation.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents commands and keywords in text.	• Issue the **clock source** command. • Specify the keyword **exp-msg**.
Bold text like this	Represents text that the user must type.	**host1(config)#traffic class low-loss1**

`Fixed-width text like this`	Represents information as displayed on your terminal's screen.	**host1#show ip ospf 2**
		`Routing Process OSPF 2 with Router ID 5.5.0.250`
		`Router is an Area Border Router (ABR)`

Italic text like this	• Emphasizes words. • Identifies variables. • Identifies chapter, appendix, and book names.	• There are two levels of access: *user* and *privileged*. • *clusterId, ipAddress.* • *Appendix A, System Specifications*
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Syntax Conventions in the Command Reference Guide		
Plain text like this	Represents keywords.	terminal length
Italic text like this	Represents variables.	*mask*, *accessListName*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
| (pipe symbol)	Represents a choice to select one keyword or variable to the left or to the right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic | line
[ ] (brackets)	Represent optional keywords or variables.	[internal | external]
[ ]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 | level2 | l1]*
{ } (braces)	Represent required keywords or variables.	{ permit | deny } { in | out } { *clusterId* | *ipAddress* }

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the Technical Documentation page on the Juniper Networks Web site at http://www.juniper.net/.

To download complete sets of technical documentation to create your own documentation CD-ROMs or DVD-ROMs, see the Portable Libraries page at

http://www.juniper.net/techpubs/resources/index.html

Copies of the Management Information Bases (MIBs) for a particular software release are available for download in the software image bundle from the Juniper Networks Web site athttp://www.juniper.net/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

Understanding IPv6 Multicast Features

IPv6 Multicast Overview

IPv6 defines three types of addresses: *unicast*, *anycast*, and *multicast*. Each type of address enables a device to send datagrams to selected recipients:

- A unicast address enables a device to send a datagram to a single recipient.
- An anycast address enables a device to send a datagram to one recipient out of a set of recipients.
- A multicast address enables a device to send a datagram to a specified set of hosts, known as a multicast group, in different subnetworks.

IPv6 multicast improves network efficiency by allowing a host to transmit a datagram to a targeted group of receivers. For example, a host may want to send a large video clip to a group of selected recipients. It would be time-consuming for the host to unicast the datagram to each recipient individually. If the host broadcasts the video clip throughout the network, network resources are not available for other tasks. The host uses only the resources it needs when multicasting the datagram.

Routers use multicast routing algorithms to determine the best route and transmit multicast datagrams throughout the network. E Series routers support a number of IPv6 multicast protocols on virtual routers. Each virtual router handles the interoperability of IPv6 multicast protocols automatically. To start IPv6 multicast operation on a virtual router, you access the context for that virtual router and configure the desired protocols on the selected interfaces. Table 3 on page 3 describes the function of each the protocol that the router supports.

Table 3: Function of Multicast Protocols on a Router

Protocol	Function
Multicast Listener Discovery (MLD)	Discovers hosts that belong to multicast group.

Table 3: Function of Multicast Protocols on a Router *(continued)*

Protocol	Function
Protocol Independent Multicast Protocol (PIM)	Discovers other multicast routers that should receive multicast packets.
BGP Multicast Protocol	Routes multicast datagrams between autonomous systems.

The router supports up to 16,384 multicast forwarding entries (multicast routes) at any time.

Reverse-Path Forwarding

IP multicasting uses reverse path forwarding (RPF) to verify that a router receives a multicast packet on the correct incoming interface. The RPF algorithm enables a router to accept a multicast datagram only on the interface from which the router sends a unicast datagram to the source of the multicast datagram.

When the router receives a multicast datagram from a source for a group, the router verifies that the packet was received on the correct RPF interface. If the packet was not received on the correct interface, the router discards the packet. Only packets received on the correct RPF interface are considered for forwarding to downstream receivers.

When operating in sparse-mode, the routers perform an RPF lookup to identify the upstream router from which to request the data and then send join messages for the multicast stream only to that router.

When operating in dense-mode, routers that have multiple paths to the source of the multicast stream initially receive the same stream on more than one interface. In this case, the routers perform an RPF lookup to identify multicast data streams that are not arriving on the best path and send prune messages to terminate these flows.

The RPF lookup need not always be towards the source of the multicast stream. The lookup is done towards the source only when the router is using a source-rooted tree to receive the multicast stream. If the router uses a shared tree instead, the RPF lookup is toward a rendezvous point and not toward the source of the multicast stream.

Multicast Packet Forwarding

Multicast packet forwarding is based on the source (S) of the multicast packet and the destination multicast group address (G). For each (S,G) pair, the router accepts multicast packets on an incoming interface (IIF), which satisfies the RPF check (RPF-IIF). The router drops packets received on IIFs other than the RPF-IIF and notifies the routing protocols that a packet was received on the wrong interface.

The router forwards packets received on the RPF-IIF to a list of outgoing interfaces (OIFs). The list of OIFs is determined by the exchange of routing information and local group membership information. The router maintains mappings of (S,G, IIF) to {OIF1, OIF2...} in the multicast routing table.

You can enable two or more multicast protocols on an IIF. However, only one protocol can forward packets on that IIF. The protocol that forwards packets on an IIF *owns* that IIF. A multicast protocol that owns an IIF also owns the (S,G) entry in the multicast routing table.

Related Documentation

- IPv6 Multicast Platform Considerations on page 5
- IPv6 Multicast References on page 5
- Switch Fabric Bandwidth Configuration on page 7

IPv6 Multicast Platform Considerations

For information about modules that support IPv6 multicasting on the ERX7xx models, ERX14xx models, and the ERX310 Broadband Services Router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support IPv6 multicasting.

For information about modules that support IPv6 multicasting on the E120 and E320 Broadband Services Routers:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support IPv6 multicasting.

Related Documentation

- IPv6 Multicast Overview on page 3
- IPv6 Multicast References on page 5

IPv6 Multicast References

For more information about IPv6 multicast, see the following resource:

- A " traceroute" Facility for IP Multicast—draft-ietf-idmr-traceroute-ipm-07.txt (January 2001 expiration)

Related Documentation

- IPv6 Multicast Overview on page 3
- IPv6 Multicast Platform Considerations on page 5

CHAPTER 2

How Switch Fabric Bandwidth Weighting Ratio Works

Switch Fabric Bandwidth Configuration

By default, the switch fabric for the ERX1440, ERX310, E120, and E320 Broadband Services Routers uses a bandwidth weighting ratio of 15:2 for multicast-to-unicast weighted round robin (WRR). In the absence of strict-priority traffic, and when both unicast and multicast traffic compete for switch fabric bandwidth, the switch fabric allocates 15/17ths of the available bandwidth to multicast traffic and 2/17ths of the available bandwidth to unicast traffic.

You can use the **fabric weights** command to change the ratio for multicast to unicast traffic on the router switch fabric. For more information about the **fabric weights** command, see *Configuring the Switch Fabric Bandwidth* in the *JunosE System Basics Configuration Guide*.

Related Documentation

- *IPv4 Multicast Overview*
- IPv6 Multicast Overview on page 3
- **fabric weights on page 57**

CHAPTER 3

Understanding the IPv6 Multicast Bandwidth Map

IPv6 Multicast Bandwidth Map Overview

Multicast interface-level admission control, port-level admission control, and QoS adjustment all use a single multicast bandwidth map. The multicast bandwidth map is a route map that uses the **set admission-bandwidth**, **set qos-bandwidth**, **set admission-bandwidth adaptive**, or **set qos-bandwidth adaptive** commands. The **adaptive** commands configure an auto-sense mechanism for measuring the multicast bandwidth.

NOTE: Even though you can include any of the above commands several times in a route map entry, only the last admission-bandwidth command or qos-bandwidth command in the bandwidth map is used. In other words, if you included the **set qos-bandwidth** command first and then the **set qos-bandwidth adaptive** command, the bandwidth map would use the **set qos-bandwidth adaptive** command.

Interface- and port-level admission control is performed when an outgoing interface (OIF) on the interface or port is added to the mroute for a given (S,G) multicast data stream and the multicast bandwidth map contains a **set admission-bandwidth** or **set admission-bandwidth adaptive** action for that (S,G).

QoS adjustment is performed on the joining interface when an OIF is added to the mroute for a given (S,G) data stream and the multicast bandwidth map contains a **set qos-bandwidth** or **set qos-bandwidth adaptive** action for that (S,G).

NOTE: You can create a single route map with the **set admission-bandwidth** command, the **set qos-bandwidth** command, or both. However, creating an entry with only one of these **set** commands enables only that specific function for the matched address (that is, only multicast traffic admission control or only QoS adjustment). The same is true for the **adaptive** commands.

Related Documentation

- IPv6 Multicast Overview on page 3
- Autosense Mechanism Overview on page 11
- Adaptive Mode Mechanism Overview for IPv6 on page 11
- Example: Configuring an IPv6 Multicast Bandwidth Map on page 49
- **set admission-bandwidth on page 77**
- **set qos-bandwidth on page 78**

CHAPTER 4

Understanding the Autosense Mechanism

Autosense Mechanism Overview

Video bandwidth is typically considered to be a constant rate—2 Mbps for standard definition television (SDTV) and 10 Mbps for high definition television (HDTV). However, in reality, and depending on achievable video compression, the bit rate can vary. For example, HDTV streams (using MPEG4 or WM9 encoding) can vary between 6 Mbps (for low-action programs) to 10 Mbps (for a fast-paced, high-action programs). The autosense mechanism causes the bandwidth value, used for admission control and QoS adjustment, to be the actual measured rate of the stream. Using this feature to measure the actual bandwidth avoids the need to configure arbitrary bandwidth limits and enables a channel to be reassigned to a different (S, G) without requiring a bandwidth map to be changed.

Related Documentation

- *Adaptive Mode Mechanism Overview for IPv4*
- Adaptive Mode Mechanism Overview for IPv6 on page 11
- *Defining a Multicast Bandwidth Map*

Adaptive Mode Mechanism Overview for IPv6

You can configure the auto-sense mechanism in the multicast bandwidth using the **set admission-bandwidth adaptive** command, **set qos-bandwidth adaptive** command, or both. For example:

```
host1(config)#route-map mcast-bandwidths permit 10
host1(config-route-map)#match ipv6 address sdtv
host1(config-route-map)#set admission-bandwidth adaptive
host1(config-route-map)#set qos-bandwidth adaptive
host1(config-route-map)#end
```

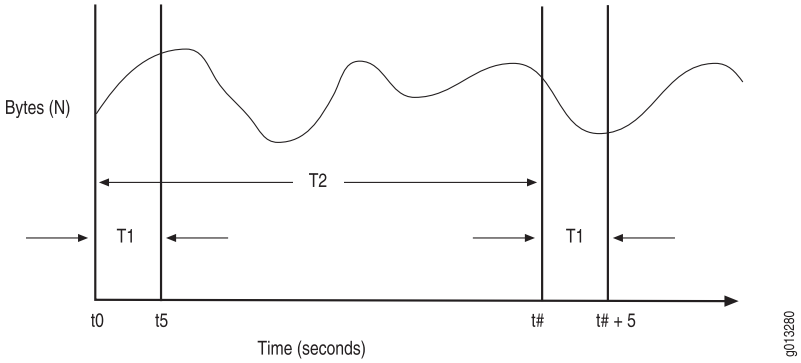
In this example, any stream with an (S,G) that matches the sdtv access list performs adaptive bandwidth detection for admission control and QoS adjustment.

A rate measurement mechanism runs on the ingress line card that polls the forwarding controller (FC) to obtain statistics for each mroute. This mechanism then reports the

rate measurement to the switch route processor (SRP) to update the bandwidth map. By computing the average bandwidth over a relatively short sampling period (T1; 5 seconds), the measurement approximates the peak bandwidth of the multicast stream.

As an example, assume that a new mroute (S1, G1) is added to the interface controller (IC) at time t0.

Figure 1: Example of Adaptive IPv6 Multicast Bandwidth Detection



To calculate the measured bandwidth of a stream, the router uses the following equation:

$R = (N_{t+5} - N_t) / 5$

Where

R = Calculated bandwidth of the stream during each sampling interval

N_t = Bytes measured at the start of each sampling period (t seconds)

N_{t+5} = Bytes measured at the end of each sampling period (t+5 seconds)

NOTE: When the mroute is first installed in the FC (at t = 0), R_0 is undetermined. For multicast admission control no joins are admitted until the first bandwidth measurement is computed (that is, for admission control, R_0 is considered to be infinite). Similarly, no QoS adjustment occurs until the first bandwidth measurement is computed (that is, for QoS adjustment, R_0 is considered to be zero [0]).

Using the earlier graph as a reference, the first bandwidth rate ($R1_0$) and at time t_5 (N_5) and the bytes received values are subtracted and divided by the time period T_1 to yield the average rate. This process is repeated every sampling interval, T_2, to yield rates R1, R2, R3, and so on.

The first two sampling interval calculations would look like the following:

$R_1 = (N_5 - N_0)/5$

$R_2 = (N_{\#+5} - N_\#)/5$

The router maintains a history of bandwidth measurements (H) for each mroute, up to a maximum of M measurements. The actual rate, R, reported to the SRP is the maximum rate measured in those H samples.

In order to minimize the IC to SRP traffic generated by the rate measurements, the IC reports a bandwidth change only when a newly computed rate (R#) differs from the current rate by a specified threshold. When R_s is computed at time t = 5 seconds, R is set to R_1. A rate update occurs whenever a newly calculated rate (R) differs from R_1 by at least a threshold value (specified as a percentage, P) of the measured peak bandwidth. This calculation would look like the following:

R = Rt, if and only if the absolute value of (R - Rt) > P * R.

The values assigned to variables associated with this algorithm are as shown in Table 4 on page 13.

Table 4: Adaptive Mode Algorithm Values

Variable	Value	Units	Description
T1	5	Seconds	Sampling period; the time in which a sample is taken
T2	0	Seconds	Sampling interval; zero (0) seconds indicates continuous sampling
H	12	Samples	Number of history samples over which to compute measurement
M	12	Samples	Maximum number of samples maintained in history
P	1	Percent	Threshold value; percent difference by which a newly calculated rate must differ from the measured peak bandwidth before a rate update occurs

Related Documentation

- IPv6 Multicast Bandwidth Map Overview on page 9
- Autosense Mechanism Overview on page 11
- Example: Configuring an IPv6 Multicast Bandwidth Map on page 49
- match ipv6 address on page 71
- route-map on page 75
- set admission-bandwidth on page 77
- set qos-bandwidth on page 78

CHAPTER 5

Understanding the IPv6 Multicast QoS Adjustment

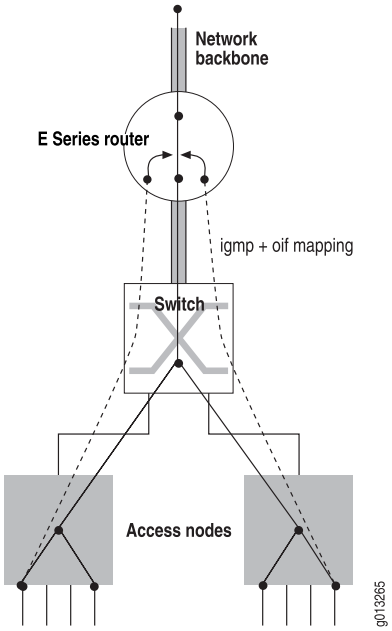
Multicast OIF Mapping Case for IPv6

Multicast outgoing interface (OIF) mapping enables the router to decrease the inefficiencies associated with replicating streams of multicast traffic. Using OIF maps, Multicast Listener Discovery (MLD) joins that the router receives on a subscriber interface can be mapped to a special interface for forwarding. This special interface can be on a different physical port or line module from that of the join interface.

NOTE: For additional information about how to configure OIF mapping, see *Configuring Group Outgoing Interface Mapping*.

Using this mapping function, the router can send a single copy of each multicast stream over the special interface and the access nodes are configured to perform any final replication to the subscribers and merge unicast and multicast data flows onto the subscriber interfaces as necessary. See Figure 2 on page 16.

Figure 2: Multicast OIF Mapping



One disadvantage to using multicast OIF mapping is that the multicast traffic bypasses any QoS treatment that is applied to subscriber interfaces. Configuring QoS adjustment resolves this problem. (See *Parameter Definition Attributes for QoS Administrators Overview* for additional information about configuring QoS adjustment.) With QoS adjustment configured, when a subscriber requests to receive a multicast stream (or, more appropriately, when an OIF is added to the mroute), the router reduces the unicast QoS bandwidth applied to the subscriber interface (that is, the join interface) by the amount of bandwidth for that multicast stream.

Related Documentation

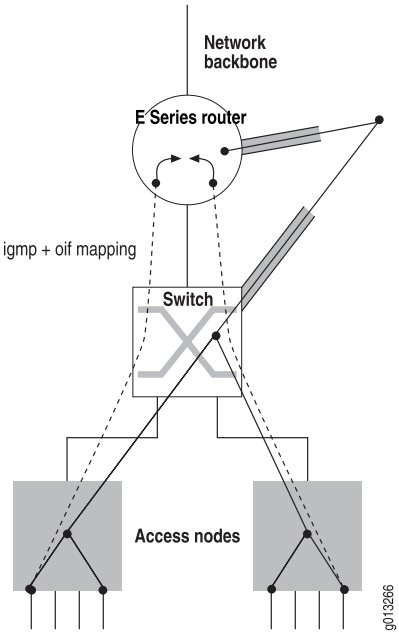
- Multicast Traffic Receipt Without Forwarding for IPv6 on page 16
- Activating IPv6 Multicast QoS Adjustment Functions on page 41

Multicast Traffic Receipt Without Forwarding for IPv6

In this case, the router is not given the responsibility of forwarding multicast streams. Instead, the service provider arranges for the router to receive the multicast streams so the router can detect the flow and perform QoS adjustment. An outgoing interface (OIF) map is installed that maps the traffic streams to a loopback interface configured for Multicast Listener Discovery (MLD) version passive. This means that when the traffic is received, a null mroute is installed (that is, an mroute with an empty OIF list) and the router applies the QoS adjustment to the join interface. See Figure 3 on page 17.

NOTE: Ensure that Protocol Independent Multicast-single mode (PIM-SM) (or any other upstream multicast protocol) is informed of the group (or source-group) interest.

Figure 3: Multicast Traffic Receipt Without Forwarding



Related Documentation

- Multicast OIF Mapping Case for IPv6 on page 15
- Activating IPv6 Multicast QoS Adjustment Functions on page 41

CHAPTER 6

How IPv6 Hardware Multicast Packet Replication Works

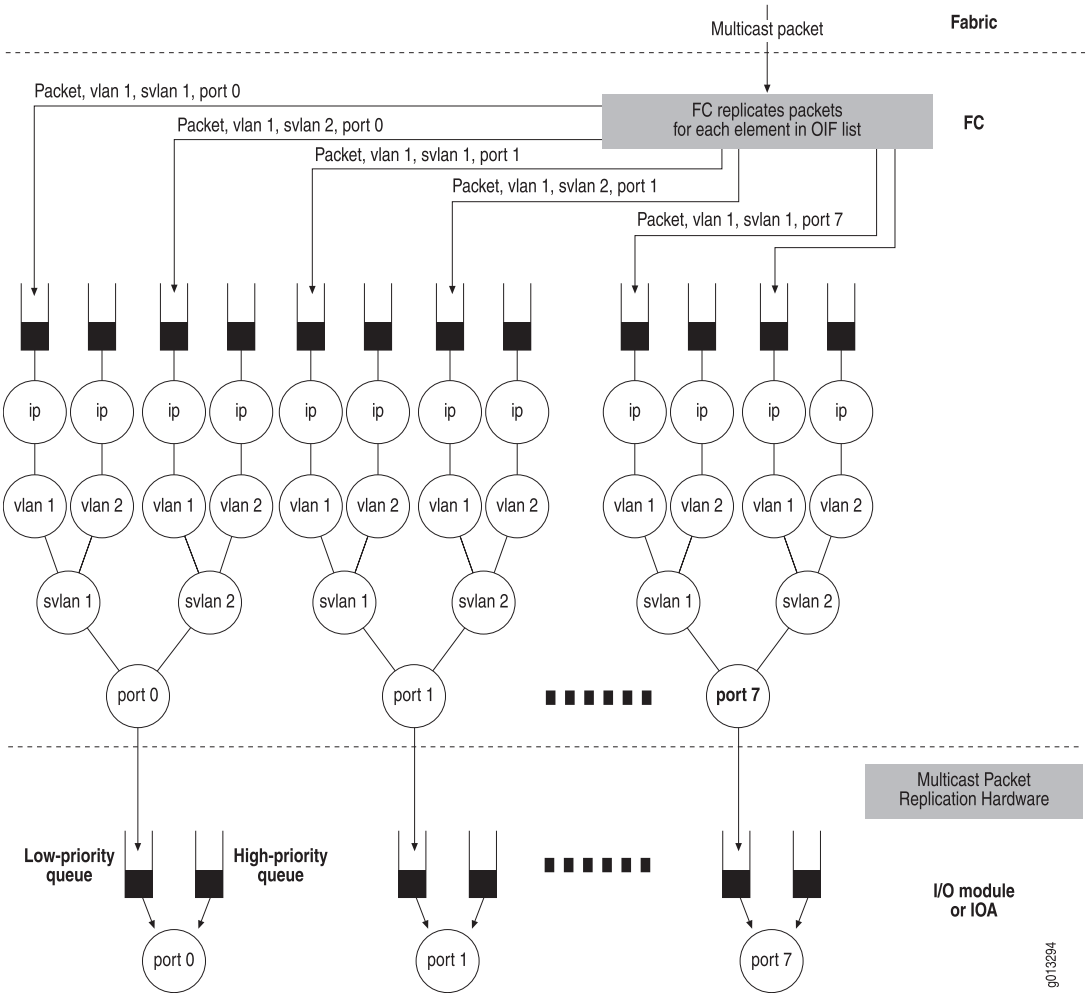
IPv6 Hardware Multicast Packet Replication Overview

You can configure IPv6 multicast to replicate packets to optimized hardware on a logical port instead of using the forwarding controller (FC) on the router.

The bandwidth between the line module and the I/O module or input/output adapter (IOA) on the E Series router is limited. A high-density Ethernet module provides eight physical ports that can consume the bandwidth between the line module and the I/O module or IOA before providing enough traffic to support egress line rate for all of these ports.

Figure 4 on page 20 displays how multicast traffic is typically replicated on the line module. Each of these replicated packets is transmitted from the line module to the I/O module or IOA.

Figure 4: Packet Flow Without Hardware Multicast Packet Replication



The hardware multicast packet replication feature enables you to configure multicast traffic for a virtual LAN (VLAN) or service VLAN (S-VLAN) to be replicated on the I/O module or IOA so that only one copy of the packet is transmitted from the line module to the I/O module or IOA. Replication for each of the ports is performed on the I/O module or IOA.

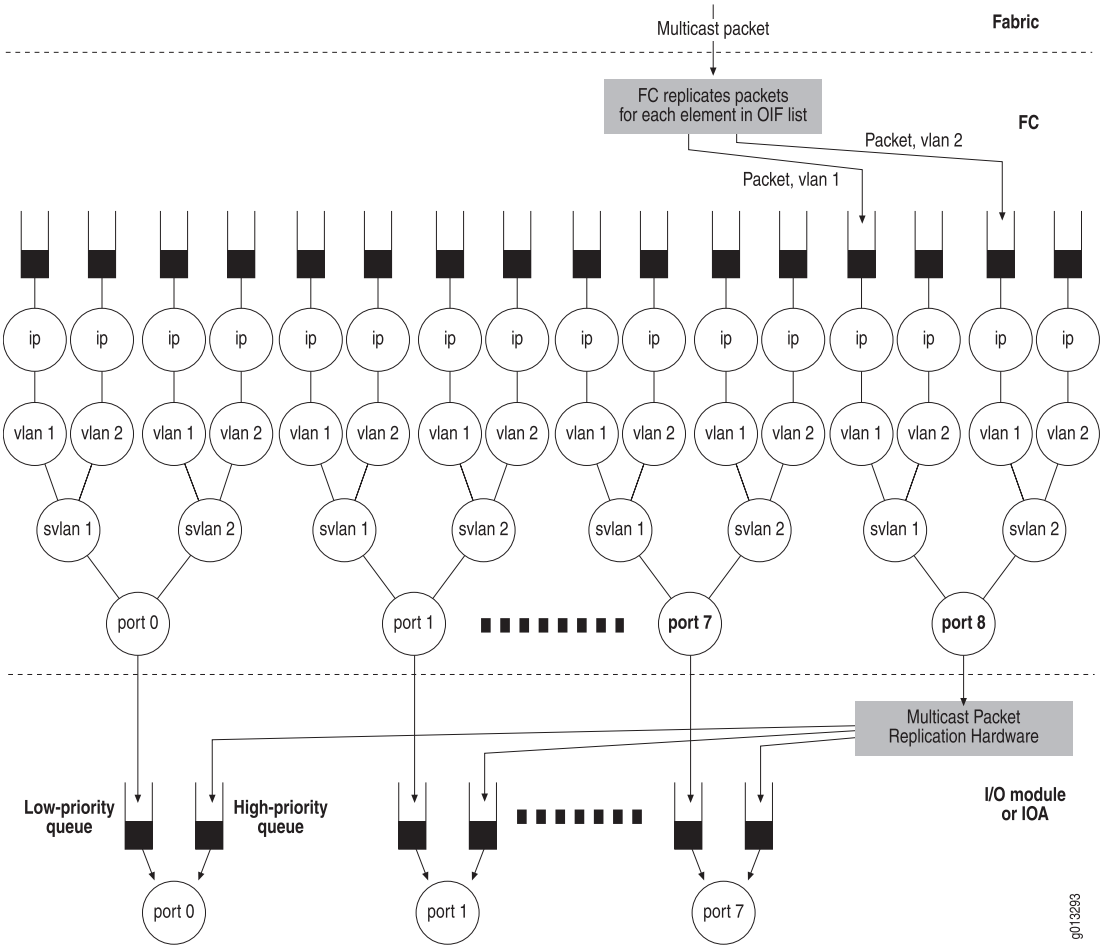
Configuring hardware multicast packet replication for high-density Ethernet is useful when you want to provide the same multicast stream out of some or all of the ports, such as for IP television (IPTV). Configuring hardware multicast packet replication enables you to:

- Reduce the number of packets sent from the FC to the module.
- Reduce the CPU consumed by the FC processing each elaboration of the packet.

You can use the feature to increase the bandwidth of multicast traffic out of each of the Gigabit Ethernet ports.

Figure 5 on page 21 displays the flow of a multicast packet using the hardware multicast packet feature.

Figure 5: Packet Flow with Optimized Multicast Packet Replication



Each high-density Ethernet module has eight physical ports, numbered 0–7. A logical port is available for the hardware multicast packet replication feature, numbered port 8.

JunosE tracks the outgoing interfaces (OIFs) in an mroute that have been redirected to use the hardware multicast packet replication hardware. The system accepts only egress multicast traffic to traverse the interface stack on the enabled port. The system drops unicast traffic that is routed to this port.

Each port on the I/O module or IOA displayed in Figure 5 on page 21 has two queues. These queues are further down the egress path than the queues found on the line module and populated by the FC.

The low-priority queue is dedicated to packets that are received from the line module queues that are dedicated to the physical ports. This queue blocks when full and provides backpressure to the line module. This queue services unicast and multicast traffic that is not using the hardware multicast packet replication feature.

The high-priority queue is dedicated to packets that are received from the line module queue for port 8. This queue is serviced at a higher priority than the first queue, and drops packets when full.

For more information about high-density Ethernet, see *Configuring Ethernet Interfaces* in *JunosE Physical Layer Configuration Guide*.

Supported Modules and Encapsulations

You can enable optimized multicast packet replication on port 8 of the following high-density Ethernet modules:

- GE-8 I/O module (pairs with the GE-HDE line module)
- ES2-S1 GE-8 IOA (pairs with the ES2 4G LM and the ES2 10G LM)

When enabled, the optimized multicast packet replication feature defines the encapsulation of the egress multicast packet. The following encapsulations are supported:

- IPv6 over Gigabit Ethernet
- IPv6 over VLAN
- IPv6 over S-VLAN

NOTE: **802.3ad link aggregation group (LAG) bundles do not support optimized multicast packet replication.**

The optimized multicast packet replication feature also provides an interface over which you can configure the following:

- IP maximum transmission unit (MTU)
- Ethernet MTU
- Egress IP policy
- Egress VLAN policy
- QoS

Relationship with OIF Mapping

Multicast OIF mapping enables the router to decrease the inefficiencies associated with replicating streams of multicast traffic. Using OIF maps, Multicast Listener Discovery (MLD) joins that the router receives on a subscriber interface can be mapped to a special interface for forwarding.

The hardware multicast packet replication feature enables you to redirect each of the IPv6 interfaces on a line module over a dedicated multicast VLAN to a single IPv6 interface over port 8. The FC is only required to send a single packet per dedicated multicast VLAN to the I/O module or IOA. The module then replicates this packet to the appropriate ports.

For more information about configuring OIF mapping, see *Configuring MLD Group Outgoing Interface Mapping*.

Related Documentation

- IPv6 Hardware Multicast Packet Replication Considerations on page 23
- Configuring IPv6 Hardware Multicast Packet Replication on page 43

IPv6 Hardware Multicast Packet Replication Considerations

When configuring hardware multicast packet replication, the following considerations apply.

- Do not configure or transmit routing protocols over port 8. The FC drops traffic routed to an IPv6 interface stacked over port 8.
- We recommend that you configure the IP address of the IPv6 interface over port 8 to be unnumbered.
- We recommend that you configure an IPv6 interface over a VLAN over one of the physical ports to reference the IPv6 interface over the same VLAN over port 8.

  You cannot create the following configurations:

  - When two IPv6 interfaces configured over a port reference the same IPv6 interface over port 8. The system does not accept this configuration attempt because you typically configure the hardware multicast packet replication feature to redirect multicast traffic over one VLAN, then redirect it to the same VLAN on port 8.
  - When the IPv6 interface configured with the hardware multicast packet replication attribute is not installed on a line module that supports hardware multicast packet replication.
  - When the IPv6 interface designated by the hardware multicast packet replication attribute is not installed on a line module that supports hardware multicast packet replication.
  - When the IPv6 interface designated by the hardware multicast packet replication attribute is not on the same line module as the IPv6 interface configured with this attribute.

- When you configure a unique source MAC address for VLANs on port 8, the hardware multicast packet replication hardware stamps the source MAC address on the VLAN, overwriting any MAC address that you configured. For more information, see *Configuring Ethernet Interfaces* in *JunosE Physical Layer Configuration Guide*.
- The regular multicast implementation utilizes interface stacking that provides a unique IPv6 attachment point for each elaboration of the egress multicast packet.

  For the hardware multicast packet replication feature, you must attach policies to an interface stack over port 8 that defines the encapsulation of the egress multicast traffic. The system supports policies over port 8 just as it is above any of the other ports on this line module.

  Policies applied to the interface stack over port 8 affect the packets traversing this stack whether or not the packet is destined for one port or all of the physical ports.

Therefore, you cannot apply different egress policies to multicast traffic for the interfaces stacked above different ports, or rate limit on an individual interface over a port. You also cannot monitor policy statistics on individual interfaces over a port.

Instead, you can apply egress policy to an interface stacked over port 8. The system applies the policy before the packet has been elaborated for each of the ports.

- The JunosE QoS component provides hierarchical egress scheduling and shaping on Gigabit Ethernet ports 0–7. The regular multicast implementation replicates packets on the FC, with each replicated packet placed on a line module queue destined for a single physical port. The line module queue can also receive QoS behavior specific to that queue.

  For the hardware multicast packet replication feature, the FC does not replicate the packet for each of the individual ports. Instead, it places the packet on a special queue destined for port 8.

  You can configure QoS on the packets flowing through port 8, but this has limited value because each packet passed through this port can be transmitted through one of more of the physical ports. Therefore, the packets placed on this special queue might not receive the same QoS behavior as ports 0–7.

  We recommend that you configure the network so the I/O or IOA queues are not oversubscribed. The traffic transmitted by the physical port is a combination of packets from the two I/O or IOA queues. When the sum of the packets in these queues is greater than line rate, the system can drop traffic that is not using hardware multicast packet replication.

  When you configure a traffic shaper on a physical port and configure hardware multicast packet replication, the packets created using the feature avoid the traffic shaper for that port. To control this, you can use traffic shaper on the physical port and port 8. The sum of the traffic shapers must be less than or equal to the line rate of the port.

  A traffic shaper on port 8 can result in the overall utilization of egress bandwidth for any one port being less the line rate because the packets being replicated might not be transmitted to every port. Packets destined to some of the ports contribute to the traffic shaping for all of the ports on the I/O module or IOA.

Related Documentation

- IPv6 Hardware Multicast Packet Replication Overview on page 19
- Configuring IPv6 Hardware Multicast Packet Replication on page 43

CHAPTER 7

Understanding Interface-Level and Port-Level Multicast Admission Control for IPv6

Interface-Level Admission Bandwidth Limits for IPv6 Overview

Interface-level multicast admission control is performed when an outgoing interface (OIF) on the interface is added to the mroute for a given (S,G) multicast data stream and the multicast bandwidth map contains a **set admission-bandwidth** action for that (S,G). When enabled, the admission-bandwidth for a particular (S,G) is read from the multicast bandwidth map and recorded in the mroute when the (S,G) mroute is created.

CAUTION: **Before you can limit interface-level admission bandwidth, you must first create a bandwidth map. See** "Example: Configuring an IPv6 Multicast Bandwidth Map" on page 49 **for details.**

When an OIF is subsequently added to the mroute, the OIF is blocked from forwarding data if the additional bandwidth contributed by the (S,G) exceeds the admission-bandwidth limit for the interface. In JunosE releases earlier than Release 12.0.x, in an OIF mapping scenario where the digital subscriber line access multiplexer (DSLAM) does not perform per-subscriber multicast admission control, the router disregards the multicast admission bandwidth limit configured on the join interface. If the limit configured on the mapped interface exceeds the admission-bandwidth limit for the interface, the router blocks the mapped interface from forwarding data.

Now, in an OIF mapping scenario where the DSLAM performs per-subscriber multicast admission control, the router checks the bandwidth limit configured on the join interface. If the multicast stream is forwarded over the mapped interface, the router admits the multicast stream and forwards the stream to the join interfaces whose bandwidth does not exceed the configured bandwidth limit. The router also performs QoS Adjust for the

multicast stream on the unblocked (forwarding) subscriber interfaces. The router does not replicate the stream to the subscriber interfaces whose bandwidth exceeds the configured bandwidth limit and it does not perform QoS Adjust for the multicast stream on the blocked subscriber interfaces.

If the multicast stream is not forwarded over the mapped interface, the router blocks the multicast stream and does not forward the stream. The router also does not perform QoS Adjust for the multicast stream on the blocked subscriber interface.

Related Documentation

- Blocking IPv6 Mroutes on page 45
- Enabling Interface-Level Admission Bandwidth Limitation for IPv6 on page 45
- OIF Interface Reevaluation for IPv6 on page 26

OIF Interface Reevaluation for IPv6

If you change the admission bandwidth for an interface, all mroutes with that interface as an outgoing interface (OIF) are reevaluated as follows:

- If the bandwidth limit is increased, blocked OIFs may become unblocked. If the interface is a blocked OIF on multiple mroutes, the order in which the mroutes are visited, and which (S,G) streams become unblocked, is not specified.
- If the bandwidth limit is decreased, no currently admitted OIFs are blocked. However, no new OIFs are admitted until the total admitted bandwidth for the interface drops below the new limit.
- If the bandwidth is increased to the point that the bandwidth limit for an interface is now exceeded, no currently admitted OIFs for the affected mroutes are blocked. However, no new OIFs are admitted until the total admitted bandwidth drops below the configured limit.

NOTE: If the multicast bandwidth map that includes the **set admission-bandwidth** command is changed, all affected mroutes are reevaluated in the same manner described previously.

As an example of this function, if the interface has accepted a total bandwidth of 2000000 bits per second (bps), and you set a limit of 1000000 bps on the interface, the router does not disconnect any already connected OIFs but prevents the interfaces from accepting any more groups. Over time, some groups leave the interfaces and, eventually, the interface limit of 1000000 bps is reached and maintained by the router.

If you set limits for both a port and interfaces on that port, the router uses the lower of the two limits when determining whether or not an interface can accept any new Multicast Listener Discovery (MLD) groups. For example, if you specify an admission bandwidth limit of 2000000 bps for the port and 3000000 bps groups for each interface, additional groups can only be accepted until the port limit of 2000000 bps is reached.

Related Documentation

- Blocking IPv6 Mroutes on page 45
- Interface-Level Admission Bandwidth Limits for IPv6 Overview on page 25
- Enabling Interface-Level Admission Bandwidth Limitation for IPv6 on page 45

Port-Level Admission Bandwidth Limits for IPv6 Overview

Port-level multicast admission control is performed when an outgoing (OIF) on that port is added to the mroute for a given (S,G) multicast data stream and the multicast bandwidth map contains a **set admission-bandwidth** action for that (S,G).

When enabled, the admission-bandwidth for a particular (S,G) is read from the multicast bandwidth map and recorded in the mroute when the (S,G) mroute is created. When an IOF is subsequently added to the mroute, the OIF is blocked from forwarding data if the additional bandwidth contributed by the (S,G) would exceed the admission-bandwidth limit for the port on which the interface resides.

CAUTION: **Before you can limit port-level admission bandwidth, you must first create a bandwidth map. See** "Example: Configuring an IPv6 Multicast Bandwidth Map" on page 49 **for details.**

Related Documentation

- Creating IPv6 Mroute Port Limits on page 47
- Enabling Port-Level Admission Bandwidth Limitation for IPv6 on page 47
- OIF Port Reevaluation for IPv6 on page 27

OIF Port Reevaluation for IPv6

If you change the admission bandwidth for a port, all mroutes with an outgoing interface (OIF) on that port are reevaluated as follows:

- If the bandwidth limit is increased, blocked OIFs can become unblocked. However, the order in which the mroutes are visited, and which (S,G) streams become unblocked, is not specified.
- If the bandwidth limit of a port is decreased, no currently admitted OIFs are blocked. However, no new OIFs are admitted until the total admitted bandwidth for the port drops below the new limit.
- If the bandwidth is increased to the point that the bandwidth limit for an interface is now exceeded, no currently admitted OIFs for the affected mroutes are blocked. However, no new OIFs are admitted until the total admitted bandwidth drops below the configured limit.

NOTE: If the multicast bandwidth map that includes the **set admission-bandwidth** command is changed, all affected mroutes are reevaluated in the same manner described previously.

As an example of this function, if the port has accepted a total bandwidth of 3000000 bits per second (bps), and you set a limit of 2000000 bps on the port, the router does not disconnect any already connected OIFs but prevents the interfaces from accepting any more groups. Over time, some groups leave the interfaces and, eventually, the port limit of 2000000 bps is reached and maintained by the router.

If you set limits for both a port and interfaces on that port, the router uses the lower of the two limits when determining whether or not an interface can accept any new Multicast Listener Discovery (MLD) groups. For example, if you specify an admission bandwidth limit of 2000000 bps for the port and 3000000 bps groups for each interface, additional groups can only be accepted until the port limit of 2000000 bps is reached.

Related Documentation

- Creating IPv6 Mroute Port Limits on page 47
- Port-Level Admission Bandwidth Limits for IPv6 Overview on page 27
- Enabling Port-Level Admission Bandwidth Limitation for IPv6 on page 47

CHAPTER 8

Understanding BGP Multicasting

BGP Multicasting

BGP multicasting (MBGP) is an extension of the BGP unicast routing protocol. Many of the functions available for BGP unicasting are also available for MBGP.

The MBGP extensions specify that BGP can exchange information within different types of *address families*. The address families available are unicast IPv4, multicast IPv4, and VPN-IPv4. When you enable BGP, the router employs unicast IPv4 addresses by default.

We recommend you be thoroughly familiar with BGP before configuring MBGP. See *Configuring BGP Routing* in the *JunosE BGP and MPLS Configuration Guide* for detailed information about BGP and MBGP.

This topic discusses the following:

Investigating Multicast Routes

You can use the **mtrace** command to trace the path that multicast packets take from a source to a destination through a multicast group address. This command is similar to the **traceroute** command for investigating unicast routes.

```
host1#mtrace 100.4.4.4 40.1.1.1 232.1.1.1
Tracing multicast route from 100.4.4.4 to 40.1.1.1 for group 232.1.1.1 using response address
   10.6.129.56
(Press ^c to stop.)
Received mtrace response packet of length 88
1. 40.1.1.1 Protocol: PIM(3) FwdingCode: RPF iif(9)
2. 21.2.2.2 Protocol: PIM(3) FwdingCode: Reached RP(8)
```

Related Documentation

- mtrace on page 74

PART 2

Configuration

CHAPTER 9

Prerequisite for Configuring IPv6 Multicast

Before You Begin

Before you begin configuring multicast on IPv4 and IPv6 interfaces, you must:

- Configure IP interfaces. For more information about configuring IP interfaces, see *Configuring IP* in the *JunosE IP, IPv6, and IGP Configuration Guide*.
- Configure IPv6 interfaces. For more information about configuring IPv6 interfaces, see *Configuring IPv6* in *JunosE IP, IPv6, and IGP Configuration Guide*.

Related Documentation

- *Configuring IPv6 Multicast Attributes*
- Example: Configuring an IPv6 Multicast Bandwidth Map on page 49
- Activating IPv6 Multicast QoS Adjustment Functions on page 41
- Configuring IPv6 Hardware Multicast Packet Replication on page 43
- Blocking IPv6 Mroutes on page 45
- Enabling Interface-Level Admission Bandwidth Limitation for IPv6 on page 45
- Creating IPv6 Mroute Port Limits on page 47
- Enabling Port-Level Admission Bandwidth Limitation for IPv6 on page 47
- Deleting IPv6 Multicast Forwarding Entries on page 40

CHAPTER 10

Enabling the IPv6 Multicasting Support

Enabling IPv6 Multicast

IPv6 multicast works on virtual routers. By default, IPv6 multicast is disabled on a virtual router. To enable IPv6 multicast on a virtual router, access the context for a virtual router, and then issue the **ipv6 multicast-routing** command.

To enable IPv6 multicast routing on the default virtual router:

- Issue the **ipv6 multicast-routing** command in Global Configuration mode.

  ```
  host1(config)#ipv6 multicast-routing
  ```

Use the **no** version to disable IPv6 multicast routing on the virtual router (the default). In the disabled state, all multicast protocols are disabled, and the virtual router forwards no multicast packets.

Related Documentation

- Before You Begin on page 33
- Monitoring IPv6 Multicast Status on a Virtual Router on page 129
- **ipv6 multicast-routing on page 64**

CHAPTER 11

Configuration Tasks for RPF in IPv6

Defining IPv6 Static Routes for Reverse-Path Forwarding

You can use the **ipv6 rpf-route** command to define RPF to verify that a router receives a multicast packet on the correct incoming interface.

To customize the static IPv6 routes that the router may use for RPF:

- Issue the **ipv6 rpf-route** command in Global Configuration mode.

  host1(config)#ipv6 rpf-route 1000::/64 ATM2/1.200

Use the **no** version to remove the static route.

Related Documentation

- IPv6 Multicast Overview on page 3
- Before You Begin on page 33
- Monitoring Available IPv6 Routes for Reverse-Path Forwarding on page 83
- Monitoring IPv6 Multicast Forwarding Entries on page 111
- Monitoring Active IPv6 Multicast Routes on page 114
- Monitoring Join Interface Details When IPv6 OIF Mapping Is Configured on page 117
- Monitoring IPv6 Multicast Statistics on page 120
- Monitoring Summary Information of IPv6 Multicast Routes on page 123
- **ipv6 rpf-route on page 69**

Enabling and Disabling RPF Checks for IPv6

By default, the router accepts multicast packets for each (S,G) pair on an IIF, which satisfies the RPF check (RPF-IIF). When the router performs RPF checks, only the interface that first accepts traffic for an (S,G) pair accepts subsequent traffic for that pair. If traffic

stops coming on that interface and starts arriving on another interface, the router does not accept or forward the traffic.

Some network configurations require the router to accept traffic on any interface. To do so, you can disable the RPF check on a specified set of (S,G) pairs by issuing the **ipv6 multicast-routing disable-rpf-check** command.

When you disable RPF checks, the router accepts multicast packets for (S,G) pairs on any incoming interface. When the router has added the new route to its multicast routing table, it accepts multicast packets for these pairs on any interface in the virtual router and forwards them accordingly. Multicast routes established before you issue this command are not affected.

To enable and disable RPF checks:

- Enable RPF checks for all (S,G) pairs (the default situation).

  host1(config)#no ipv6 multicast-routing disable-rpf-check

- Disable RPF checks for the (S,G) pair specified using a standard IPv6 access list.

  host1(config)#ipv6 multicast-routing disable-rpf-check denver-list

Related Documentation

- IPv6 Multicast Overview on page 3
- Before You Begin on page 33
- **ipv6 multicast-routing disable-rpf-check on page 66**

Specifying Unicast Routes for RPF in IPv6

You can use the **ipv6 route-type** command to specify that BGP or OSPF IPv6 routes should be available for RPF. Routes available for RPF appear in the multicast view of the routing table.

To specify that BGP IPv6 routes are available for both unicast protocols and multicast protocols to perform RPF checks:

```
host1(config)#router bgp
host1(config-router)#ipv6 route-type both
```

Related Documentation

- IPv6 Multicast Overview on page 3
- Before You Begin on page 33
- **ipv6 route-type on page 68**

CHAPTER 12

Configuration Tasks for IPv6 Multicast Forwarding Entries

Defining Permanent IPv6 Multicast Forwarding Entries

An mroute is a multicast traffic flow, a (S,G) entry used for forwarding multicast traffic. By default, forwarding mroutes (with a valid RPF incoming interface) are timed out if data for them is not received for 210 seconds. However, you can specify an mroute as permanent by using the **ipv6 multicast-routing permanent-mroute** command.

To specify that any newly created mroutes that match the specified access-list do not time out:

- Issue the **ipv6 multicast-routing permanent-mroute** command in Global Configuration mode.

  host1(config)#ipv6 multicast-routing permanent-mroute routesv61

Use the **no** version to prevent any new mroutes from becoming permanent. To remove existing permanent mroutes, use the **clear ipv6 mroute** command.

NOTE:

- The **ipv6 multicast-routing permanent-mroute** command does not change existing mroutes.
- Permanent mroutes are removed if a topology change occurs that affects the mroute.
- Permanent mroutes may be removed due to certain protocol actions (for example, PIM sparse mode switching from shared to shortest path tree).
- Outgoing interface lists of permanent mroutes may change due to protocol actions.

Deleting IPv6 Multicast Forwarding Entries

You can clear one or more forwarding entries from the multicast routing table. However, if you do so, the entries may reappear in the routing table if they are rediscovered. If you specify an *, the router clears all IP multicast forwarding entries. If you specify the IPv6 address of a multicast group, the router clears all multicast forward entries for that group. If you specify the IPv6 address of a multicast group and the IPv6 address of a multicast source, the router clears the multicast entry that matches that group and source.

To delete IPv6 multicast forwarding entries:

- Issue the **clear ipv6 mroute** command in Privileged Exec mode.

  ```
  host1:boston#clear ipv6 mroute *
  ```

Related Documentation

- Before You Begin on page 33
- Defining Permanent IPv6 Multicast Forwarding Entries on page 39
- **clear ipv6 mroute on page 55**

CHAPTER 13

Configuration Task for IPv6 Multicast QoS Adjustment

Activating IPv6 Multicast QoS Adjustment Functions

The **ipv6 multicast-routing bandwidth-map** command activates the specified bandwidth map. By activating the bandwidth map, this command also activates the multicast QoS adjustment function contained in the bandwidth map.

CAUTION: To activate multicast QoS adjustment, you must first create a bandwidth map. See "Example: Configuring an IPv6 Multicast Bandwidth Map" on page 49 for details.

To enable the QoS adjust function on the router with the configured route map:

- Issue the **ipv6 multicast-routing bandwidth-map** command in Global Configuration mode.

  host1(config)#ipv6 multicast-routing bandwidth-map mcast-bandwidths

Use the **no** version to disable the multicast QoS adjustment function on the router.

Related Documentation

- Multicast OIF Mapping Case for IPv6 on page 15
- Multicast Traffic Receipt Without Forwarding for IPv6 on page 16
- **ipv6 multicast-routing bandwidth-map on page 65**

CHAPTER 14

Configuration Tasks for IPv6 Hardware Multicast Packet Replication

Configuring IPv6 Hardware Multicast Packet Replication

To configure hardware multicast packet replication:

1. Configure port 8 on a high-density Ethernet module to accept redirected egress multicast traffic.
   a. Specify the Gigabit Ethernet interface on port 8.
   b. Create a VLAN major interface.
   c. Create a VLAN subinterface.
   d. Assign a VLAN ID.
   e. Configure an unnumbered IPv6 interface.
   f. Enable MLD on the interface with only multicast-data-forwarding capability.

```
host1(config)#interface gigabitEthernet 2/8
host1(config-if)#encapsulation vlan
host1(config-if)#interface gigabitEthernet 2/8.1
host1(config-if)#vlan id 1
host1(config-if)#ipv6 unnumbered loopback 0
host1(config-if)#ipv6 mld version passive
```

2. Configure an IPv6 interface to redirect egress multicast traffic to port 8.
   a. Create a VLAN subinterface.
   b. Assign a VLAN ID.
   c. Assign an IPv6 address.
   d. Configure the interface to redirect egress multicast traffic to port 8.

```
host1(config)#interface gigabitEthernet 2/0.101
host1(config-if)#vlan id 1
host1(config-if)#ipv6 address 1::1/64
host1(config-if)#ipv6 multicast ioa-packet-replication gigabitEthernet 2/8.1
```

Related Documentation

- Before You Begin on page 33
- IPv6 Hardware Multicast Packet Replication Overview on page 19
- IPv6 Hardware Multicast Packet Replication Considerations on page 23
- *Monitoring IPv6 Hardware Multicast Packet Replication*
- encapsulation vlan on page 56
- interface gigabitEthernet on page 58
- ipv6 address on page 59
- ipv6 mld version on page 61
- ipv6 multicast ioa-packet-replication on page 63
- ipv6 unnumbered on page 70
- vlan id on page 79

CHAPTER 15

Configuration Tasks for Interface-Level Multicast Admission Control for IPv6

Blocking IPv6 Mroutes

By default, when an interface receives multicast traffic, even when the scope of that traffic exceeds link-local, the virtual router creates an mroute. You can use the **ipv6 block-multicast-sources** command to block all multicast traffic with a scope larger than link-local (for example, global) and prevent mroute creation under these conditions.

NOTE: **Issuing this command does not affect reception of link-local multicast packets.**

To block all multicast traffic with a scope larger than link-local:

- Issue the **ipv6 block-multicast-sources** command in Global Configuration mode.

  host1(config)#ipv6 block-multicast-sources

Use the **no** version to restore the default behavior of creating mroutes on receiving multicast packets.

Related Documentation

- Interface-Level Admission Bandwidth Limits for IPv6 Overview on page 25
- Enabling Interface-Level Admission Bandwidth Limitation for IPv6 on page 45
- OIF Interface Reevaluation for IPv6 on page 26
- **ipv6 block-multicast-sources on page 60**

Enabling Interface-Level Admission Bandwidth Limitation for IPv6

You can use the **ipv6 multicast admission-bandwidth-limit** command to enable multicast admission control on interfaces (including dynamic IP interfaces) that are configured to run MLD. You can also use this command on a PIM (sparse-mode,

dense-mode, or sparse-dense-mode) interface if MLD is configured on the interface (including the **ipv6 mld version passive** command).

To limit bandwidth for an interface that accepts MLD groups:

- Issue the **ipv6 multicast admission-bandwidth-limit** command in Interface Configuration mode.

```
host1:boston(config-if)#ipv6 multicast admission-bandwidth-limit 2000000
```

Use the **no** version to remove the bandwidth limitation for the interface.

Related Documentation

- Blocking IPv6 Mroutes on page 45
- Interface-Level Admission Bandwidth Limits for IPv6 Overview on page 25
- OIF Interface Reevaluation for IPv6 on page 26
- **ipv6 multicast admission-bandwidth-limit on page 62**

CHAPTER 16

Configuration Tasks for Port-Level Multicast Admission Control for IPv6

Creating IPv6 Mroute Port Limits

When a multicast forwarding entry (that is, an mroute) is added with an OIF on a port, the OIF count for that port is incremented. If you configure a port limit and the OIF count on the port count exceeds that limit, no OIFs on that port are added to mroutes (that is, new OIFs are blocked).

To configure a limit on the number of mroute OIFs that can be added across different virtual routers on a port:

- Issue the **mroute port limit** command in Global Configuration mode.

  ```
  host1(config)#mroute port 3/0 limit 10
  ```

Use the **no** version to remove any OIF port limits.

Related Documentation

- Port-Level Admission Bandwidth Limits for IPv6 Overview on page 27
- Enabling Port-Level Admission Bandwidth Limitation for IPv6 on page 47
- OIF Port Reevaluation for IPv6 on page 27
- **mroute port limit on page 73**

Enabling Port-Level Admission Bandwidth Limitation for IPv6

You can use the **mroute port admission-bandwidth-limit** command to limit the total multicast bandwidth that can be admitted on a port. The admitted bandwidth is summed across all virtual routers with IPv4 and IPv6 mroutes that have OIFs on the port.

NOTE: Admission bandwidth values for a given (S,G) mroute are determined from the bandwidth map. See "Example: Configuring an IPv6 Multicast Bandwidth Map" on page 49 for details.

To configure a limit on the admission bandwidth of OIFs containing IPv4 or IPv6 mroutes, across different virtual routers, on a port:

- Issue the **mroute port admission-bandwidth-limit** command in Global Configuration mode.

  ```
  host1(config)#mroute port admission-bandwidth-limit 3000000
  ```

Use the **no** version to remove any OIF admission bandwidth limits.

Related Documentation

- Creating IPv6 Mroute Port Limits on page 47
- Port-Level Admission Bandwidth Limits for IPv6 Overview on page 27
- OIF Port Reevaluation for IPv6 on page 27
- **mroute port admission-bandwidth-limit on page 72**

CHAPTER 17

Examples

Example: Configuring an IPv6 Multicast Bandwidth Map

This example shows how to create a multicast bandwidth map for both multicast traffic admission control and QoS adjustment.

Requirements

This example uses the following hardware and software components:

- JunosE Release 7.1.0 or higher-numbered releases
- E Series router (ERX7xx models, ERX14xx models, the ERX310 router, the E120 router, or the E320 router)
- ASIC-based line modules that support Fast Ethernet or Gigabit Ethernet

Before you begin configuring multicast on IPv6 interfaces, you must:

- Configure IPv6 interfaces. For more information about configuring IPv6 interfaces, see *Configuring IPv6* in *JunosE IP, IPv6, and IGP Configuration Guide*.

Overview

The multicast bandwidth map is a route map that uses the **set admission-bandwidth**, **set qos-bandwidth**, **set admission-bandwidth adaptive**, or **set qos-bandwidth adaptive** commands. Multicast interface-level admission control, port-level admission control, and QoS adjustment all use a single multicast bandwidth map.

The **adaptive** commands configure an auto-sense mechanism for measuring the multicast bandwidth.

Configuring an IPv6 Multicast Bandwidth Map

Configuring a Route Map

Step-by-Step Procedure

Define a route map using the **set admission-bandwidth** and **set qos-bandwidth** commands.

NOTE: In this example, you can replace the **set admission-bandwidth** command and **set qos-bandwidth** command with their **adaptive** command counterparts.

1. Define a route map.

   ```
   [edit]
   host1(config)#route-map mcast-bandwidths permit 10
   ```

2. Match the route map to an access list.

   ```
   [edit]
   host1(config-route-map)#match ipv6 address sdtv
   ```

3. Configure multicast bandwidths.

   ```
   [edit multicast bandwidths for admission control and QoS adjustment]
   host1(config-route-map)#set admission-bandwidth 2000000
   host1(config-route-map)#set qos-bandwidth 2000000
   ```

4. Configure the route map.

   ```
   [edit]
   host1(config-route-map)#route-map mcast-bandwidths permit 20
   ```

5. Match the route map to an access list.

   ```
   [edit]
   host1(config-route-map)#match ipv6 address hdtv
   ```

6. Configure multicast bandwidths.

   ```
   [edit multicast bandwidths for admission control and QoS adjustment]
   host1(config-route-map)#set admission-bandwidth 10000000
   host1(config-route-map)#set qos-bandwidth 10000000
   ```

Configuring an Access List

Step-by-Step Procedure

Define the access list for use by the **match ipv6 address** command to match (S,G) and (*,G) entries.

NOTE: You can also define a prefix-list or a prefix-tree for use by the **match ipv6 address** command to match (S,G) and (*,G) entries.

1. Configure access lists.

```
[edit access lists]
host1(config)#access-list sdtv permit ip host 31::1 ff3e::0/112
host1(config)#access-list hdtv permit ip host 32::1 ff3e::0/112
host1(config)#access-list hdtv permit ip host 32::2 ff3e::0/112
```

Related Documentation

- IPv6 Multicast Bandwidth Map Overview on page 9
- *Configuring Routing Policy* in *JunosE IP Services Configuration Guide*
- access-list on page 54
- match ipv6 address on page 71
- route-map on page 75
- set admission-bandwidth on page 77
- set qos-bandwidth on page 78

CHAPTER 18

Configuration Commands

access-list

Syntax Standard IP access list:

access-list *accessListName* { permit | deny }
{ *srcIP srcWildIp* | [host] *srcIPHost* | any } [log]

no access-list *accessListName* [{ permit | deny }
{ *srcIP srcWildIp* | [host] *srcIPHost* | any } [log]]

Extended IP access list:

access-list *accessListName* { permit | deny } ip { *srcIP srcWildIp* |
host *srcIPHost* | any } { *dstIP dstWildIp* | host *dstIPHost* | any } [log]

no access-list *accessListName* [{ permit | deny } ip { *srcIP srcWildIp* |
host *srcIPHost* | any } { *dstIP dstWildIp* | host *dstIPHost* | any } [log]]

Release Information Command introduced before JunosE Release 7.1.0.

Description Defines a standard or extended IP access list. The extended access list enables you to specify a destination address or host, precedence, and type of service. This command imposes an implicit last rule of " deny ip any any" to deny all routes that do not match previous rules in the access list. The **no** version removes the IP access list, the specified entry in an access list, or the log for a specified entry.

Options

- *accessListName*—String of up to 32 alphanumeric characters
- permit—Permits access if the conditions are matched
- deny—Denies access if the conditions are matched
- *srcIP*—Source IP address from which the packet is being sent
- *srcWildIp*—Wildcard mask IP address
- host—Identifies the address as a host
- *srcIPHost*—Source host IP address; assumes a wildcard mask of 0
- any—Creates an address of 0.0.0.0 with a wildcard mask of 255.255.255.255
- *dstIP*—Destination IP address
- *dstWildIp*—Wildcard mask IP address for destination
- *dstIPHost*—Destination host IP address to which the packet is being sent
- log—Logs an Info event into the ipAccessList log whenever the access-list rule is matched

Mode Global Configuration

clear ipv6 mroute

Syntax clear ipv6 mroute { * | *grpAddress* [*sourceAddress*] }

Release Information Command introduced before JunosE Release 7.1.0.

Description Clears all or the specified IPv6 multicast forwarding entries. There is no **no** version.

Options
- *—Clears all IPv6 multicast forwarding entries
- *grpAddress*—Address of the multicast group for which forwarding entries should be cleared
- *sourceAddress*—Address of the multicast source for which forwarding entries should be cleared

Mode Privileged Exec, User Exec

Related Documentation
- Deleting IPv6 Multicast Forwarding Entries on page 40

encapsulation vlan

Syntax [no] encapsulation vlan

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures VLAN as the encapsulation method for the interface. The **no** version removes VLAN encapsulation from the interface.

Mode Interface Configuration, Subinterface Configuration

Related Documentation

- *Configuring Ethernet/VLAN Layer 2 Services*
- *Configuring S-VLAN Tunnels for Layer 2 Services*
- *Configuring Local Cross-Connects Between Ethernet/VLAN Interfaces*

fabric weights

Syntax fabric weights multicast *multicastValue* unicast *unicastValue*

no fabric weights

Release Information Command introduced in JunosE Release 7.2.0.

Description Defines the multicast-to-unicast traffic ratio for the ERX1440, ERX310, E120, or E320 router switch fabric. The **no** version returns the switch fabric to its default multicast:unicast ratio (15:2).

Options

- *multicastValue*—Ratio value of multicast bandwidth in the range 1–15
- *unicastValue*—Ratio value of unicast bandwidth in the range 1–15

Mode Global Configuration

Related Documentation

- *Configuring the Switch Fabric Bandwidth*
- *Monitoring the Multicast-to-Unicast Ratio for the Router Switch Fabric*
- *show fabric weights*

interface gigabitEthernet

Syntax [no] interface gigabitEthernet *interfaceSpecifier*

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies or creates a Gigabit Ethernet interface or a subinterface over a Gigabit Ethernet interface. The **no** version removes the interface or subinterface. You must issue the **no** version from the highest level down; you cannot remove an interface or subinterface if the one above it still exists.

NOTE: On the GE I/O module, you can configure only the primary port, 0. The router automatically uses the redundant port, 0R, if the primary port fails.

On the GE-2 APS I/O module, you can configure only the primary ports, 0 and 1. The router automatically uses the corresponding redundant port, 0R or 1R, if the primary port fails.

On the OC3-2 GE APS I/O module, you can configure only a Gigabit Ethernet interface in port 2. Ports 0 and 1 are reserved for OC3/STM1 ATM interfaces.

On the ES-2 GE-4 IOA, you can configure all four ports.

Options

- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*

Mode Global Configuration

Related Documentation

- *Configuring the QoS Shaping Mode for Ethernet Interfaces*
- *Creating a QoS Interface Hierarchy for Bulk-Configured VLAN Subinterfaces with RADIUS*
- *Configuring a Parameter Definition to Shape Ethernet Traffic Using Cell Mode*

ipv6 address

Syntax [no] ipv6 address *ipv6Prefix* [eui-64]

[no] ipv6 address [*ipv6Address maskLength* [eui-64]]

Release Information Command introduced before JunosE Release 7.1.0.

Description Assigns an IPv6 address (or network) to an interface and enables IPv6 processing on that interface. The **no** version deletes the association from the interface.

NOTE: The link-local address for an interface is automatically configured when IPv6 is enabled on the interface.

Options

- *ipv6Prefix*—Prefix that defines the IPv6 interface or network in the format *ipv6Address* **/** *length*, where
  - *ipv6Address*—Base IPv6 address of the network route that you want to filter (for example, ::ffff:a:b:c:d)
  - *length*—Length of the network prefix; number of bits masking base address to produce address to be matched
- *ipv6Address*—Base IPv6 address of the network route that you want to filter (for example, ::ffff:a:b:c:d); the *ipv6Address* must appear in hexadecimal format using 16-bit values between colons. Refer to RFC 2373—IP Version 6 Addressing Architecture (July 1998) for details.
- *maskLength*—Length of the IPv6 mask. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
- eui-64—Specifies the use of the eui-64 interface identifier

Mode Interface Configuration, Profile Configuration

ipv6 block-multicast-sources

Syntax [no] ipv6 block-multicast-sources

Release Information Command introduced before JunosE Release 7.1.0.

Description Prevents mroute creation by blocking multicast traffic that has a scope larger than link-local (for example, global). The **no** version restores the default behavior of creating mroutes upon receiving multicast packets.

Mode Global Configuration

Related Documentation

- Blocking IPv6 Mroutes on page 45

ipv6 mld version

Syntax ipv6 mld version { 1 | 2 | passive }

no ipv6 mld version

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets the MLD version for the interface. The **no** version restores the default value, MLDv1.

Options
- 1—Sets MLD version 1
- 2—Sets MLD version 2
- passive—Configures a mapped OIF as a passive interface with only multicast-data-forwarding capability

Mode Interface Configuration, Profile Configuration

ipv6 multicast admission-bandwidth-limit

Syntax [no] ipv6 multicast admission-bandwidth-limit *limitValue*

Release Information Command introduced in JunosE Release 7.1.0.

Description Specifies multicast admission bandwidth (in kilobits per second) for a given interface. The **no** version removes the admission bandwidth limit.

Options
- *limitValue*—Maximum admission bandwidth (in kilobits per second) permitted on an interface; default value is 0, which disables the limit

Mode Interface Configuration, Profile Configuration

Related Documentation
- Enabling Interface-Level Admission Bandwidth Limitation for IPv6 on page 45

ipv6 multicast ioa-packet-replication

Syntax ipv6 multicast ioa-packet-replication *interfaceType interfaceSpecifier*

no ipv6 multicast ioa-packet-replication

Release Information Command introduced in JunosE Release 7.3.0.

Description Enables IPv6 hardware multicast packet replication on port 8 of a high-density Ethernet I/O module or IOA. The **no** version disables hardware multicast packet replication.

Options

- *interfaceType*—Interface type; see *Interface Types and Specifiers*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*

Mode Interface Configuration

Related Documentation

- Configuring IPv6 Hardware Multicast Packet Replication on page 43

ipv6 multicast-routing

Syntax [no] ipv6 multicast-routing

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables IPv6 multicast routing on the router. The **no** version disables IPv6 multicast routing on the router.

Mode Global Configuration

Related Documentation
- Enabling IPv6 Multicast on page 35

ipv6 multicast-routing bandwidth-map

Syntax ipv6 multicast-routing bandwidth-map *routeMapName*

no ipv6 multicast-routing bandwidth-map

Release Information Command introduced in JunosE Release 7.1.0.

Description Enables the QoS adjust function on the router. The **no** version disables the QoS adjust function on the router.

Options
- *routeMapName*—Name of the route map you want to use for the bandwidth map

Mode Global Configuration

Related Documentation
- Activating IPv6 Multicast QoS Adjustment Functions on page 41

ipv6 multicast-routing disable-rpf-check

Syntax ipv6 multicast-routing disable-rpf-check *accessListName*

no ipv6 multicast-routing disable-rpf-check

Release Information Command introduced before JunosE Release 7.1.0.

Description Disables RPF checks for the (S,G) pairs in the specified access list. The **no** version restores the default situation, in which the router performs RPF checks for all (S,G) pairs.

Options
- *accessListName*—Name of the IPv6 access list that specifies the (S,G) pairs

Mode Global Configuration

Related Documentation
- Enabling and Disabling RPF Checks for IPv6 on page 37

ipv6 multicast-routing permanent-mroute

Syntax ipv6 multicast-routing permanent-mroute *accessListName*

no ipv6 multicast-routing permanent-mroute

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies that newly created mroutes that match the specified access-list do not get timed out. The **no** version of this command prevents any new mroutes from becoming permanent. However, it does not remove any existing permanent mroutes. To remove existing permanent mroutes, use the **clear ipv6 mroute** command.

Options
- *accessListName*—Name of the IPv6 access list that specifies the mroutes

Mode Global Configuration

Related Documentation
- Defining Permanent IPv6 Multicast Forwarding Entries on page 39

ipv6 route-type

Syntax

For BGP

ipv6 route-type [unicast | both]

no ipv6 route-type

For OSPF

ipv6 route-type [unicast | multicast | both]

no ipv6 route-type

Release Information

Command introduced before JunosE Release 7.1.0.

Description

For BGP, specifies whether BGP IPv6 routes are available only for other unicast protocols or for both unicast protocols and multicast protocols to perform RPF checks. The **no** version restores the default value, unicast.

For OSPF, specifies whether OSPF IPv6 routes are available only for unicast forwarding, only for multicast reverse path forwarding checks, or for both. The **no** version restores the default value, both.

Options

- unicast—Specifies that routes for the protocol are available only for unicast forwarding
- both—Specifies that routes for the protocol are available for both unicast forwarding and multicast route path forwarding checks
- multicast—Specifies that routes for the protocol are available only for multicast route path forwarding checks

Mode

Router Configuration

Related Documentation

- Specifying Unicast Routes for RPF in IPv6 on page 38

ipv6 rpf-route

Syntax

ipv6 rpf-route [vrf *vrfName*] *ipv6Address/addressMask*
{ *nextHopIpv6Address* | *interfaceType interfaceSpecifier* } [*distance*]

no ipv6 rpf-route [vrf *vrfName*] *ipv6Address/addressMask*
[*nextHopIpv6Address* | *interfaceType interfaceSpecifier*] [*distance*]

Release Information

Command introduced before JunosE Release 7.1.0.
vrf keyword and *vrfName* variable added in JunosE Release 7.2.0.

Description

Customizes static IPv6 routes that the router can use to verify source addresses in multicast packets. The **no** version removes the static route.

Options

- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
- *ipv6Address*—IPv6 address of the destination network
- *addressMask*—Subnet mask for the destination network
- *nextHopIpv6Address*—IPv6 address of the next hop
- *interfaceType*—Interface type; see *Interface Types and Specifiers*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*
- *distance*—Number in the range 0–255 that indicates the preference for this route

Mode

Global Configuration

Related Documentation

- Defining IPv6 Static Routes for Reverse-Path Forwarding on page 37

ipv6 unnumbered

Syntax ipv6 unnumbered *interfaceType interfaceSpecifier*

no ipv6 unnumbered

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables or disables IPv6 processing on an interface without assigning an explicit IPv6 address to that interface. The global IPv6 address of the interface, specified by the *interfaceType interfaceSpecifier* values, becomes the source address in packets that the unnumbered interface generates. Unnumbered interfaces are often used in point-to-point connections where an IPv6 address is not required. You must specify an interface location, which is the identifier of another interface on which the router has an assigned IPv6 address. This interface cannot be another unnumbered interface. The **no** version of the command removes the IPv6 address from the interface.

NOTE: Enabling IPv6 on an interface automatically configures the link-local address on an unnumbered interface.

Options

- *interfaceType*—Interface type; see *Interface Types and Specifiers*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*

Mode Interface Configuration, Profile Configuration

match ipv6 address

Syntax match ipv6 address
{ *accessListName* [*accessListName*]* | prefix-list *prefixListName*
[*prefixListName*]* }

no match ipv6 address [[*accessListName*]* | prefix-list [*prefixListName*]*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Matches any routes that have a destination network number address that is permitted by an access list or prefix list. The **no** version removes all address match clauses from a route map unless you specify either an access list or a prefix list, in which case only the list match is removed from the route map.

Options
- *accessListName*—String of up to 32 alphanumeric characters
- *prefixListName*—Name of a single prefix list; string of up to 32 characters
- *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Policy List Configuration, Route Map Configuration

mroute port admission-bandwidth-limit

Syntax

mroute port *portNumber* admission-bandwidth-limit *limitValue*
[priority-bandwidth-limit *priorityBandwidthValue*] [hysteresis *hysteresisValue*]

no mroute port *portNumber* admission-bandwidth-limit

Release Information

Command introduced in JunosE Release 7.1.0.
hysteresis and **priority-bandwidth limit** keywords and *hysteresisValue* and *priorityBandwidthValue* variables added in JunosE Release 8.2.0.

Description

Configures a limit on the admission bandwidth of outgoing interfaces (OIFs) containing IPv4 or IPv6 mroutes, across different virtual routers, on a port. The **no** version removes any OIF admission bandwidth limits.

Options

- *portNumber*—Port number in the form *slot/port*.
- *limitValue*—Limit on the admission bandwidth (in bits per second) of outgoing interfaces containing IPv4 or IPv6 mroutes, across different virtual routers, on a port. The default is no limit.
- *priorityBandwidthValue*— Minimum value of admitted priority bandwidth in bps. The default is no limit.
- *hysteresisValue*—Minimum priority bandwidth limit before the system evaluates mroutes and admits any blocked OIFs; in the range 0-100 percent.

Mode

Global Configuration

Related Documentation

- *Enabling Port-Level Admission Bandwidth Control*
- *Dynamic Port Admission Bandwidth Control*
- Enabling Port-Level Admission Bandwidth Limitation for IPv6 on page 47

mroute port limit

Syntax mroute port *portNumber* limit *limitValue*

no mroute port *portNumber* limit

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures a limit on the number of outgoing interfaces (OIFs) containing IPv4 or IPv6 mroutes, across different virtual routers, on a port. The **no** version removes any OIF port limits.

Options

- *portNumber*—Port number in the form *slot/port*.
- *limitValue*—Limit on the number of outgoing interfaces containing IPv4 or IPv6 mroutes, across different virtual routers, on a port. The default is no limit.

Mode Global Configuration

Related Documentation

- *Creating Mroute Port Limits*
- Creating IPv6 Mroute Port Limits on page 47

mtrace

Syntax mtrace *sourceAddress* [*destinationAddress* [*groupAddress* [*responseAddress*]]] [*maxHops*] [detailed]

Release Information Command introduced before JunosE Release 7.1.0.

Description Discovers the routes that multicast packets follow when travelling to their destinations. There is no **no** version.

Options

- *sourceAddress*—DNS name or unicast IP address of the multicast-capable device at the beginning of the path.
- *destinationAddress*—DNS name or unicast address of the device at the end of the path. The default destination is the router from which you type the command.
- *groupAddress*—DNS name or multicast address of the group for which you want to trace routes. The default address is 224.2.0.1 (the group used for MBONE Audio).
- *responseAddress*—IP address that receives the results of the trace. If you do not specify a response address, the router sends the trace to an IP address on the router.
- *maxHops*—Maximum number of hops allowed for the trace; default value is 64.
- detailed—Provides a detailed description of the trace, rather than a summary

Mode Privileged Exec, User Exec

Related Documentation

- BGP Multicasting on page 29

route-map

Syntax Specifying a route map for DVMRP or RIP:

[no] route-map *mapTag* [*interfaceType interfaceSpecifier*]

Defining a route map:

[no] route-map *mapTag* [permit | deny] [*sequence*]

Defining a route map for data MDTs:

route-map *routeMapName*

no route-map

Release Information Command introduced before JunosE Release 7.1.0.
IP PIM Data MDT Configuration mode added in JunosE Release 8.2.0.

Description Specifies a route map for DVMRP, RIP, or data MDTs, or defines the conditions for applying routing policies to filter or modify routes redistributed into or propagated by a routing protocol. The **no** version deletes the route map.

Options

- *mapTag*—String of up to 32 alphanumeric characters.
- *interfaceType*—Interface type; see *Interface Types and Specifiers*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*
- *mapTag*—String of up to 32 alphanumeric characters. The **redistribute** Router Configuration command uses this string to reference this route map. Multiple route maps may share the same map tag.
- permit—If the match criteria are met for this route map and **permit** is specified, the route is redistributed as controlled by the set actions.
- deny—If the match criteria are met for the route map and **deny** is specified, the route is not redistributed, and no further route maps sharing the same map tag are examined.
- *sequence*—Number, in the range 0–65535, that indicates the position a new route map is to have in the list of route maps already configured with the same map tag. If given with the **no** version of this command, it specifies the position of the route map that should be deleted.

Mode Address Family Configuration (RIP), Global Configuration, IP PIM Data MDT Configuration

Related Documentation

- *show route-map*

router bgp

Syntax [no] router bgp *autonomousSystem*

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures the BGP routing process. Allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between ASs. All subsequent BGP configuration commands are placed within the context of this router and AS; you can have only a single BGP instance per virtual router. The **no** version removes the BGP routing process.

Options
- *autonomousSystem*—Number, in the range 1–4294967295; the AS number that identifies the router to other BGP routers

Mode Global Configuration

Related Documentation
- *BGP Signaling for L2VPNs Overview*
- *Configuring BGP Signaling for VPLS*

set admission-bandwidth

Syntax

set admission-bandwidth { *bandwidthValue* | adaptive }

no set admission-bandwidth

Release Information

Command introduced in JunosE Release 7.1.0.
adaptive keyword added in JunosE Release 7.2.0.

Description

Sets a specific multicast bandwidth for admission control or defines the bandwidth as adaptive (automatically sensed). The **no** version removes the set clause from a route map.

Options

- *bandwidthValue*—Number in the range 0–4294967259 kilobits per second used for admission control
- adaptive—Defines the admission bandwidth as being automatically sensed

Mode

Route Map Configuration

Related Documentation

- *Defining a Multicast Bandwidth Map*
- *Example: Configuring a Multicast Bandwidth Map*
- Example: Configuring an IPv6 Multicast Bandwidth Map on page 49
- IPv6 Multicast Bandwidth Map Overview on page 9

set qos-bandwidth

Syntax set qos-bandwidth { *bandwidthValue* | adaptive }

no set qos-bandwidth

Release Information Command introduced in JunosE Release 7.1.0.
adaptive keyword added in JunosE Release 7.2.0.

Description Sets a multicast bandwidth for QoS adjustment or defines the bandwidth as adaptive (automatically sensed). The **no** version removes the set clause from a route map.

Options
- *bandwidthValue*—Number, in the range 0–4294967259 kilobits per second, used for QoS adjustment
- adaptive—Defines the QoS bandwidth as being automatically sensed

Mode Route Map Configuration

Related Documentation
- *Defining a Multicast Bandwidth Map*
- *Example: Configuring a Multicast Bandwidth Map*
- Example: Configuring an IPv6 Multicast Bandwidth Map on page 49
- IPv6 Multicast Bandwidth Map Overview on page 9

vlan id

Syntax vlan id *idValue* [icr-control-interface] [untagged] [mac-address *macAddress*]

Release Information Command introduced before JunosE Release 7.1.0.
icr-control-interface keyword added in JunosE Release 10.3.0.

Description Specifies a VLAN ID to a VLAN subinterface. Assigns a VLAN ID to a VLAN subinterface on which an ICR partition is to be configured. Issue the **vlan id** command before you configure any upper-layer interfaces, such as IP. There is no **no** version.

Options

- *idValue*—Number unique within the Ethernet interface, in the range 0–4095.
- icr-control-interface—Sets the VLAN subinterface as an ICR control interface on which you want to configure the ICR partition. We recommend that you use this option only if you want the VLAN subinterface to be used to create ICR partitions.
- untagged—Specifies that frames be sent untagged; valid only for VLAN ID 0. Tagged frames can be received, but untagged frames are sent.
- *macAddress*—MAC address of the interface; when you do not specify a unique MAC address, the VLAN uses the MAC address of the Ethernet interface.

Mode Interface Configuration

Related Documentation

- *Configuring Ethernet/VLAN Layer 2 Services*
- *Configuring Local ATM Cross-Connects with AAL5 Encapsulation*
- *Configuring Local Cross-Connects Between Ethernet/VLAN Interfaces*

PART 3

Administration

CHAPTER 19

Monitoring the IPv6 Routes Used for RPF

Monitoring Available IPv6 Routes for Reverse-Path Forwarding

Purpose Display the IPv6 routes that the router can use for RPF. You can specify the IPv6 address and the network mask to view routes to a particular destination. You can use the **detail** keyword to view more detailed information about routes to a particular destination. You can specify a unicast routing protocol to view routes associated with that protocol.

Action To display all IPv6 routes that the router can use for RPF:

```
host1#show ipv6 rpf-route
Protocol/Route type codes:
  O- OSPF, E1- external type 1, E2- external type2,
  N1- NSSA external type1, N2- NSSA external type2
  L- MPLS label, V- VR/VRF, *- indirect next-hop

        Prefix/Length              Type    Dst/Met         Intf
-------------------------------- --------- ------- --------------------
11:1:1:10::/60                   Static    1/0     ATM2/0.300
21:2:2:20::/60                   Static    1/0     ATM2/0.300
31:2:2:20::/60                   Connect   0/0     ATM2/0.300
131:1:1:10::/60                  Connect   0/0     ATM2/1.1300
1000::/64                        Static    1/0     ATM2/0.300
```

To display more detailed information about an IPv6 route to a particular destination:

```
host1#show ipv6 rpf-route 1000::/64 detail

1000::/64 Type:Static  Distance:1  Metric:0
        NextHop:31:2:2:23::2:3  IntfIndex 18  Intf ATM2/0.300
```

Meaning Table 5 on page 83 lists the **show ipv6 rpf-route** command output fields.

Table 5: show ipv6 rpf-route Output Fields

Field Name	Field Description
Protocol/Route type codes	Protocol and route type codes for the table that follows
Prefix	Value of the logical AND of the IPv6 address of the destination network and the subnet address

Table 5: show ipv6 rpf-route Output Fields *(continued)*

Field Name	Field Description
Length	Length of the subnet mask in bits
Type	• Connect—Subnet directly connected to the interface • Static—Static route
Dst	Distance configured for this route
Met	Learned or configured cost associated with this route
Intf	Type of interface and interface specifier for the next hop. For details about interface types and specifiers, see *Interface Types and Specifiers* in *JunosE Command Reference Guide*.

Related Documentation

- Defining IPv6 Static Routes for Reverse-Path Forwarding on page 37
- show ipv6 rpf-route on page 140

CHAPTER 20

Monitoring the IPv6 Hardware Multicast Packet Replication

Monitoring Port Statistics

Purpose Display the status of Gigabit Ethernet interfaces. You can use the **delta** keyword to view baselined statistics. You can use the **brief** keyword to view the operational status of all configured interfaces.

NOTE: The E120 and E320 routers output for **monitor** and **show** commands is identical to output from other E Series routers, except that the E120 and E320 router output also includes information about the adapter identifier in the interface specifier (*slot/adapter/port*).

Action To display the status of a Gigabit Ethernet interface:

```
host1#show interfaces gigabitEthernet 14/0/0
 GigabitEthernet14/0/0 is Up, Administrative status is Up
 Hardware is Intel IXF1104, address is 0090.1a42.0b87
 MAU is 1000BASE-SX
 TX Output Power: 469.6 uW RX Input Power: 0.5 uW
 MTU: Operational 1518, Administrative 1518
 Duplex Mode: Operational Full Duplex, Administrative Auto Negotiate
 Speed: Operational 1000 Mbps, Administrative Auto Negotiate
 Debounce: State is Disabled
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 In: Bytes 0, Unicast 0
 Multicast 0, Broadcast 0
 Errors 0, Discards 0, Mac Errors 0, Alignment 0
 CRC 0, Too Longs 0, Symbol Errors 0
 Out: Bytes 0, Unicast 0
 Multicast 0, Broadcast 0
 Errors 0, Discards 0, Mac Errors 0, Deferred 0, No Carrier 0
```

```
Collisions: Single 0, Multiple 0, Late 0, Excessive 0
Policed Statistics:
In: 0, Out: 0
ARP Statistics:
In: ARP requests 0, ARP responses 0
Errors 0, Discards 0
Out: ARP requests 0, ARP responses 0
```

Meaning Table 6 on page 86 lists the output fields of the **show interfaces gigabitEthernet** command.

Table 6: show interfaces gigabitEthernet Output Fields

Field Name	Field Description
GigabitEthernet or tenGigabitEthernet *interfaceSpecifier*	Status of the hardware on this interface: • up—Hardware is operational • down—Hardware is not operational
Administrative status	Operational state that you configured for this interface: • up—Interface is enabled • down—Interface is disabled
Hardware	Type of MAC device on this interface
Address	MAC address of the processor on this interface
MAU	Type of MAU on the primary and secondary physical ports: • SFP—1000BASE-LH, 1000BASE-SX, 1000BASE-ZX; for SFPs that are empty, SFP (Empty) appears in this field; for SFPs that are installed in the OC3-2 GE APS I/O module and do not have a Juniper Networks part number programmed, SFP (GE Compliant) appears in this field • XFP—10GBASE-SR (10 Gbps), 10GBASE-LR (10 Gbps), 10GBASE-ER (10 Gbps); for XFPs that are empty, XFP (Empty) appears in this field
TX Output Power	Transmitted output optical power
RX Input Power	Received input optical power
MTU	Size of the MTU for this interface: • Operational—Size of the largest packet processed • Administrative—Setting for MTU size that you specified

Table 6: show interfaces gigabitEthernet Output Fields *(continued)*

Field Name	Field Description
Duplex Mode	Duplex option for this interface: • Operational—Duplex option currently used • Administrative—Setting for duplex that you specified
Speed	Line speed for this interface: • Operational—Current rate at which packets are processed • Administrative—Setting for line speed that you specified
Debounce	Debounce configuration for this interface: • State is—Enabled, Disabled • Interval is—Number of seconds that this interface maintains a given state before the state change is reported to the upper-layer links
Clear arp	State of the removal of the ARP entries on an interface with redundant ports: • Enabled—Clears ARP entries on the interface when the primary link fails • Disabled—Maintains ARP entries on the interface until the specified timeout elapses

Link	Link information for this interface:
	• Operational Link Selected—Port that the I/O module is currently using: primary or secondary
	• Administrative link selected—Port that the I/O module is configured to use:
	  ◦ primary—Only primary port is configured to operate
	  ◦ secondary—Only redundant port is configured to operate
	  ◦ automatically—Software controls port redundancy automatically

Link Failover Timeout	Time to wait for a failed link to be active before the router uses a different active link
Primary link selected x times	Number of times that the I/O has used the primary port since the module was last rebooted
Secondary link selected x times	Number of times that the I/O has used the secondary port since the module was last rebooted`

Table 6: show interfaces gigabitEthernet Output Fields *(continued)*

Field Name	Field Description
Primary/Secondary link signal detected, Primary/Secondary link signal not detected	Specifies the port (primary or secondary) on which the router detects a signal (not displayed on GE I/O modules that do not support SFPs)
5 minute input rate	Data rates based on the traffic received in the last 5 minutes
5 minute output rate	Data rates based on the traffic sent in the last 5 minutes
In	Analysis of inbound traffic on this interface: • Bytes—Number of bytes received in error-free packets • Unicast—Number of unicast packets received • Multicast—Number of multicast packets received • Broadcast—Number of broadcast packets received • Errors—Total number of errors in all received packets; some packets might contain more than one error • Discards—Total number of discarded incoming packets • Mac Errors—Number of incoming packets discarded because of MAC sublayer failures • Alignment—Number of incomplete octets received • CRC—Number of packets discarded because the checksum that the router computed from the data does not match the checksum generated by the originating devices • Too Longs—Number of packets discarded because the size exceeded the MTU • Symbol Errors—Number of symbols received that the router did not correctly decode

Table 6: show interfaces gigabitEthernet Output Fields *(continued)*

Field Name	Field Description
Out	Analysis of outbound traffic on this interface: • Bytes—Number of bytes sent • Unicast—Number of unicast packets sent • Multicast—Number of multicast packets sent • Broadcast—Number of broadcast packets sent • Errors—Total number of errors in all transmitted packets; note that some packets might contain more than one error • Discards—Total number of discarded outgoing packets • Mac Errors—Number of outgoing packets discarded because of MAC sublayer failures • Deferred—Number of packets that the router delayed sending because the line was busy. In half duplex mode, a high number of deferrals means the link is very busy with traffic from other stations. In full duplex mode, when the link is always available for transmission, this number is zero. • No Carrier—Number of packets sent when carrier sense was unavailable
Collisions	Analysis of the collisions that occurred : • Single—Number of packets sent after one collision • Multiple—Number of packets sent after multiple collisions • Late—Number of packets aborted during sending because of collisions after 64 bytes • Excessive—Number of packets not sent because of too many collisions
Policed Statistics	Number of packets that exceeded the number allowed and were policed (or dropped)
ARP Statistics	Analysis of ARP traffic on this interface; In fields are for traffic received on the interface and Out fields are for traffic sent on the interface: • ARP requests—Number of ARP requests • ARP responses—Number of ARP responses • Errors—Total number of errors in all ARP packets • Discards—Total number of discarded ARP packets

Table 6: show interfaces gigabitEthernet Output Fields *(continued)*

Field Name	Field Description
Administrative qos-shaping-mode	QoS shaping mode: • disabled—Shaping mode is configured but not operational • frame—Statistics are reported about bytes in frames, such as transmitted bytes and dropped bytes. • cell—Shaping mode for shaping and policing rates is cell-based; resulting traffic stream conforms exactly to the policing rates configured in downstream devices. Reports statistics in bytes in cells and accounts for cell encapsulation and padding overhead. • none—Shaping mode is not configured
Operational qos-shaping-mode	Actual shaping mode for the interface: • disabled • frame • cell • none
queue	Hardware packet queue associated with the specified traffic class and interface : • traffic class—Name of traffic class • bound to—Interface to which queue is bound • Queue length—Length of the queue, in bytes • Forwarded packets, bytes—Number of packets and bytes that were forwarded on this queue • Dropped committed packets, bytes—Number of committed packets and bytes that were dropped • Dropped conformed packets, bytes—Number of conformed packets and bytes that were dropped • Dropped exceeded packets, bytes—Number of exceeded packets and bytes that were dropped

Related Documentation

- Configuring IPv6 Hardware Multicast Packet Replication on page 43
- show interfaces on page 134

Monitoring VLAN Statistics

Purpose Display configuration and status information for a specified VLAN subinterface or for all VLAN subinterfaces configured on the router. You can use the **mac-address** keyword to display information about the VLAN subinterfaces that were configured with unique MAC addresses.

Action To display full status and configuration information for the specified VLAN subinterface:

```
host1#show vlan subinterface fastEthernet 0/0.1
    Interface       Status  MTU  Svlan Id Vlan Id Ethertype Type
------------------- ------ ---- -------- ------ --------- -------
FastEthernet 0/0.1    Up    1526    1      0    0x9100    Static

In: Bytes 39256, Packets 612
   Multicast 0, Broadcast 0
   Errors 0, Discards 0
  Out: Bytes 4538652, Packets 70911
   Multicast 0, Broadcast 70296
   Errors 0, Discards 0
ARP Statistics:
  In: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
  Out: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
```

Meaning Table 7 on page 91 lists the **show vlan subinterface** command output fields.

Table 7: show vlan subinterface Output Fields

Field Name	Field Description
Interface	Type and specifier of the VLAN subinterface
Status	Status of the VLAN subinterface: up, down, dormant, lowerLayerDown, absent
MTU	Maximum allowable size (in bytes) of the MTU for the VLAN subinterface
Svlan Id	S-VLAN ID value, if configured
Vlan Id	VLAN ID value for the VLAN subinterface
Ethertype	S-VLAN Ethertype value, if configured
Type	Type of VLAN subinterface: • Static—VLAN or S-VLAN subinterface was configured statically • Dynamic—VLAN or S-VLAN subinterface was configured dynamically

Table 7: show vlan subinterface Output Fields *(continued)*

Field Name	Field Description
In	Analysis of inbound traffic on this interface: • Bytes—Number of bytes received on the VLAN or S-VLAN subinterface • Packets—Sum of all unicast, broadcast, and multicast packets received on the VLAN or S-VLAN subinterface • Multicast—Number of multicast packets received on the VLAN or S-VLAN subinterface • Broadcast—Number of broadcast packets received on the VLAN or S-VLAN subinterface • Errors—Total number of errors in all received packets; some packets might contain more than one error • Discards—Total number of discarded incoming packets
Out	Analysis of outbound traffic on this interface: • Bytes—Number of bytes sent on the VLAN or S-VLAN subinterface • Packets—Number of packets sent on the VLAN or S-VLAN subinterface • Multicast—Number of multicast packets received on the VLAN or S-VLAN subinterface • Broadcast—Number of broadcast packets received on the VLAN or S-VLAN subinterface • Errors—Total number of errors in all transmitted packets; some packets might contain more than one error • Discards—Total number of discarded outgoing packets
ARP Statistics	Analysis of ARP traffic on this interface; In fields are for traffic received on the interface and Out fields are for traffic sent on the interface: • ARP requests—Number of ARP requests • ARP responses—Number of ARP responses • Errors—Total number of errors in all ARP packets • Discards—Total number of discarded ARP packets

Related Documentation

- Configuring IPv6 Hardware Multicast Packet Replication on page 43
- show vlan subinterface on page 143

Monitoring IPv6 Statistics

Purpose Display detailed or summary information for a particular IPv6 interface or for all IPv6 interfaces.

Action To display statistics for all IPv6 interfaces:

```
host1#show ipv6 interface
null0 line protocol IpLoopback is up, ipv6 is up
  Network Protocols: IPv6
  Link local address: fe80::90:1a00:740:1d44
  Unnumbered Interface: Corresponding Numbered Interface not specified or
removed
  Operational MTU 1500 Administrative MTU 0
  Operational speed 100000000 Administrative speed 0
  Creation type Static
  Neighbor Discovery is disabled

  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Packets 0, Bytes 0
  In Total Dropped Packets 0, Bytes 0
    In Policed Packets 0
    In Invalid Source Address Packets 0
    In Error Packets 0
    In Discarded Packets 0

  Out Forwarded Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Routed Packets 0, Bytes 0
  Out Total Dropped Packets 0, Bytes 0
    Out Scheduler Dropped Packets 0, Bytes 0
    Out Policed Packets 0
    Out Discarded Packets 0

FastEthernet9/1.5 line protocol VlanSub is up, ipv6 is up
  Description: IPv6 interface in Virtual Router Hop5
  Network Protocols: IPv6
  Link local address: fe80::90:1a00:740:31ce
  Internet address: 5:1:1::2/64
  Operational MTU 1500 Administrative MTU 0
  Operational speed 100000000 Administrative speed 0
  Creation type Static
  ND reachable time is 3600000 milliseconds
  ND duplicate address detection attempts is 100
  ND neighbor solicitation retransmission interval is 1000 milliseconds
  ND proxy is enabled

  In Received Packets 13, Bytes 1356
    Unicast Packets 5, Bytes 588
    Multicast Packets 8, Bytes 768
  In Total Dropped Packets 0, Bytes 0
    In Policed Packets 0
    In Invalid Source Address Packets 0
    In Error Packets 0
    In Discarded Packets 0

  Out Forwarded Packets 22, Bytes 2480
    Unicast Packets 22, Bytes 2480
    Multicast Routed Packets 0, Bytes 0
  Out Total Dropped Packets 8, Bytes 0
    Out Scheduler Dropped Packets 0, Bytes 0
    Out Policed Packets 0
    Out Discarded Packets 8

  queue 0: traffic class best-effort, bound to ipv6 FastEthernet9/1.5
    Queue length 0 bytes
    Forwarded packets 4, bytes 680
    Dropped committed packets 0, bytes 0
```

```
    Dropped conformed packets 0, bytes 0
    Dropped exceeded packets 0, bytes 0

FastEthernet9/0.6 line protocol VlanSub is up, ipv6 is up
  Description: IPv6 interface in Virtual Router Hop6
  Network Protocols: IPv6
  Link local address: fe80::90:1a00:740:31cd
  Internet address: 6:1:1::1/64
  Operational MTU 1500 Administrative MTU 0
  Operational speed 100000000 Administrative speed 0
  Creation type Static
  ND reachable time is 3600000 milliseconds
  ND duplicate address detection attempts is 100
  ND neighbor solicitation retransmission interval is 1000 milliseconds
  ND proxy is enabled
ND RA source link layer is advertised
  ND RA interval is 200 seconds, lifetime is 1800 seconds
  ND RA managed flag is disabled, other config flag is disabled
  ND RA advertising prefixes configured on interface

  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Packets 0, Bytes 0
  In Total Dropped Packets 0, Bytes 0
    In Policed Packets 0
    In Invalid Source Address Packets 0
    In Error Packets 0
    In Discarded Packets 0

  Out Forwarded Packets 8, Bytes 768
    Unicast Packets 8, Bytes 768
    Multicast Routed Packets 0, Bytes 0
  Out Total Dropped Packets 5, Bytes 0
    Out Scheduler Dropped Packets 0, Bytes 0
    Out Policed Packets 0
    Out Discarded Packets 5

  queue 0: traffic class best-effort, bound to ipv6 FastEthernet9/0.6
    Queue length 0 bytes
    Forwarded packets 0, bytes 0
    Dropped committed packets 0, bytes 0
    Dropped conformed packets 0, bytes 0
    Dropped exceeded packets 0, bytes 0

loopback5 line protocol IpLoopback is up, ipv6 is up
  Network Protocols: IPv6
  Link local address: fe80::90:1a00:740:1d44
  Internet address: 10:1:1:0:290:1aff:fe40:1d44/64 (eui-64)
  Operational MTU 1500 Administrative MTU 0
  Operational speed 100000000 Administrative speed 0
  Creation type Static
  Neighbor Discovery is disabled

  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Packets 0, Bytes 0
  In Total Dropped Packets 0, Bytes 0
    In Policed Packets 0
    In Invalid Source Address Packets 0
    In Error Packets 0
    In Discarded Packets 0

  Out Forwarded Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
```

```
    Multicast Routed Packets 0, Bytes 0
  Out Total Dropped Packets 0, Bytes 0
    Out Scheduler Dropped Packets 0, Bytes 0
    Out Policed Packets 0
    Out Discarded Packets 0

IPv6 policy input ipv6InPol25
    rate-limit-profile Rlp2Mb classifier-group clgA entry 1
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
    rate-limit-profile Rlp8Mb
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
  IPv6 policy output ipv6PolOut2
    rate-limit-profile RlpOutA classifier-group clgB entry 1
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
    rate-limit-profile RlpOutB
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
  IPv6 policy local-input ipv6PolLocIn5
    rate-limit-profile Rlp1Mb classifier-group clgC entry 1
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
    rate-limit-profile Rlp5Mb
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
  queue 0: traffic class best-effort, bound to ipv6 FastEthernet9/0.6
    Queue length 0 bytes
    Forwarded packets 0, bytes 0
    Dropped committed packets 0, bytes 0
    Dropped conformed packets 0, bytes 0
    Dropped exceeded packets 0, bytes 0
```

To display statistics for a particular IPv6 interface:

```
host1#show ipv6 interface FastEthernet 9/0.6
FastEthernet9/0.6 line protocol VlanSub is up, ipv6 is up
  Description: IPv6 interface in Virtual Router Hop6
  Network Protocols: IPv6
  Link local address: fe80::90:1a00:740:31cd
  Internet address: 6:1:1::1/64
  Operational MTU 1500 Administrative MTU 0
  Operational speed 100000000 Administrative speed 0
  Creation type Static
  ND reachable time is 3600000 milliseconds
  ND duplicate address detection attempts is 100
  ND neighbor solicitation retransmission interval is 1000 milliseconds
  ND proxy is enabled
ND RA source link layer is advertised
  ND RA interval is 200 seconds, lifetime is 1800 seconds
  ND RA managed flag is disabled, other config flag is disabled
  ND RA advertising prefixes configured on interface

  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
```

```
    Multicast Packets 0, Bytes 0
  In Total Dropped Packets 0, Bytes 0
    In Policed Packets 0
    In Invalid Source Address Packets 0
    In Error Packets 0
    In Discarded Packets 0

  Out Forwarded Packets 8, Bytes 768
    Unicast Packets 8, Bytes 768
    Multicast Routed Packets 0, Bytes 0
  Out Total Dropped Packets 5, Bytes 0
    Out Scheduler Dropped Packets 0, Bytes 0
    Out Policed Packets 0
    Out Discarded Packets 5

  queue 0: traffic class best-effort, bound to ipv6 FastEthernet9/0.6
    Queue length 0 bytes
    Forwarded packets 0, bytes 0
    Dropped committed packets 0, bytes 0
    Dropped conformed packets 0, bytes 0
    Dropped exceeded packets 0, bytes 0

IPv6 policy input ipv6InPol25
    rate-limit-profile Rlp2Mb classifier-group clgA entry 1
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
    rate-limit-profile Rlp8Mb
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
  IPv6 policy output ipv6PolOut2
    rate-limit-profile RlpOutA classifier-group clgB entry 1
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
    rate-limit-profile RlpOutB
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
  IPv6 policy local-input ipv6PolLocIn5
    rate-limit-profile Rlp1Mb classifier-group clgC entry 1
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
    rate-limit-profile Rlp5Mb
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
  queue 0: traffic class best-effort, bound to ipv6 FastEthernet9/0.6
    Queue length 0 bytes
    Forwarded packets 0, bytes 0
    Dropped committed packets 0, bytes 0
    Dropped conformed packets 0, bytes 0
    Dropped exceeded packets 0, bytes 0
Http Redirect Url: http://www.juniper.net
```

To display detailed IPv6 status and configuration information for all IPv6 interfaces:

```
host1#show ipv6 interface detail
null0 line protocol IpLoopback is up, ipv6 is up
  Network Protocols: IPv6
  Link local address: fe80::90:1a00:740:1d44
```

```
  Unnumbered Interface: Corresponding Numbered Interface not specified or
removed
IPv6 statistics:
  Rcvd:  0 local destination
         0 hdr errors, 0 addr errors
         0 unkn proto, 0 discards
  Sent:  0 generated, 0 no routes, 0 discards

ICMPv6 statistics:
  Rcvd:  0 destination unreach, 0 admin unreach, 0 parameter problem
         0 time exceeded, 0 pkt too big, 0 echo requests
         0 echo replies
  Sent:  0 destination unreach, 0 admin unreach, 0 parameter problem
         0 time exceeded, 0 pkt too big, 0 echo requests
         0 echo replies

  Operational MTU 1500 Administrative MTU 0
  Operational speed 100000000 Administrative speed 0
  Creation type Static
  Neighbor Discovery is disabled

  ICMPv6 statistics:
    Rcvd:  0 total, 0 errors
           0 rtr solicits, 0 rtr advertisements
           0 neighbor solicits, 0 neighbor advertisements
           Group membership: 0 queries, 0 responses, 0 reductions
           0 redirects
    Sent:  0 total, 0 errors
           0 rtr solicits, 0 rtr advertisements
           0 neighbor solicits, 0 neighbor advertisements
           Group membership: 0 queries, 0 responses, 0 reductions
           0 redirects

  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Packets 0, Bytes 0
  In Total Dropped Packets 0, Bytes 0
    In Policed Packets 0
    In Invalid Source Address Packets 0
    In Error Packets 0
    In Discarded Packets 0

  Out Forwarded Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Routed Packets 0, Bytes 0
  Out Total Dropped Packets 0, Bytes 0
    Out Scheduler Dropped Packets 0, Bytes 0
    Out Policed Packets 0
    Out Discarded Packets 0

FastEthernet9/1.5 line protocol VlanSub is up, ipv6 is up
  Description: IPv6 interface in Virtual Router Hop5
  Network Protocols: IPv6
  Link local address: fe80::90:1a00:740:31ce

  Internet address: 5:1:1::2/64
IPv6 statistics:
  Rcvd:  0 local destination
         0 hdr errors, 0 addr errors
         0 unkn proto, 0 discards
  Sent:  0 generated, 0 no routes, 0 discards

ICMPv6 statistics:
  Rcvd:  0 destination unreach, 0 admin unreach, 0 parameter problem
```

```
        0 time exceeded, 0 pkt too big, 0 echo requests
        3 echo replies
  Sent:  0 destination unreach, 0 admin unreach, 0 parameter problem
        0 time exceeded, 0 pkt too big, 5 echo requests
        0 echo replies

  Operational MTU 1500 Administrative MTU 0
  Operational speed 100000000 Administrative speed 0
  Creation type Static
  ND reachable time is 3600000 milliseconds
  ND duplicate address detection attempts is 100
  ND neighbor solicitation retransmission interval is 1000 milliseconds
  ND proxy is enabled
ND RA source link layer is advertised
  ND RA interval is 200 seconds, lifetime is 1800 seconds
  ND RA managed flag is disabled, other config flag is disabled
  ND RA advertising prefixes configured on interface

  ICMPv6 statistics:
    Rcvd:  13 total, 0 errors
           0 rtr solicits, 8 rtr advertisements
           1 neighbor solicits, 1 neighbor advertisements
           Group membership: 0 queries, 0 responses, 0 reductions
           0 redirects
    Sent:  31 total, 0 errors
           0 rtr solicits, 16 rtr advertisements
           5 neighbor solicits, 5 neighbor advertisements
           Group membership: 0 queries, 0 responses, 0 reductions
           0 redirects

  In Received Packets 13, Bytes 1356
    Unicast Packets 5, Bytes 588
    Multicast Packets 8, Bytes 768
  In Total Dropped Packets 0, Bytes 0
    In Policed Packets 0
    In Invalid Source Address Packets 0
    In Error Packets 0
    In Discarded Packets 0

  Out Forwarded Packets 22, Bytes 2480
    Unicast Packets 22, Bytes 2480
    Multicast Routed Packets 0, Bytes 0
  Out Total Dropped Packets 8, Bytes 0
    Out Scheduler Dropped Packets 0, Bytes 0
    Out Policed Packets 0
    Out Discarded Packets 8

  queue 0: traffic class best-effort, bound to ipv6 FastEthernet9/1.5
    Queue length 0 bytes
    Forwarded packets 4, bytes 680
    Dropped committed packets 0, bytes 0
    Dropped conformed packets 0, bytes 0
    Dropped exceeded packets 0, bytes 0

FastEthernet9/0.6 line protocol VlanSub is up, ipv6 is up
  Description: IPv6 interface in Virtual Router Hop6
  Network Protocols: IPv6
  Link local address: fe80::90:1a00:740:31cd

  Internet address: 6:1:1::1/64
IPv6 statistics:
  Rcvd:  0 local destination
        0 hdr errors, 0 addr errors
```

```
        0 unkn proto, 0 discards
  Sent:  0 generated, 0 no routes, 0 discards

ICMPv6 statistics:
  Rcvd:  0 destination unreach, 0 admin unreach, 0 parameter problem
         0 time exceeded, 0 pkt too big, 0 echo requests
         0 echo replies
  Sent:  0 destination unreach, 0 admin unreach, 0 parameter problem
         0 time exceeded, 0 pkt too big, 0 echo requests
         0 echo replies

  Operational MTU 1500 Administrative MTU 0
  Operational speed 100000000 Administrative speed 0
  Creation type Static
  ND reachable time is 3600000 milliseconds
  ND duplicate address detection attempts is 100
  ND neighbor solicitation retransmission interval is 1000 milliseconds
  ND proxy is enabled
ND RA source link layer is advertised
  ND RA interval is 200 seconds, lifetime is 1800 seconds
  ND RA managed flag is disabled, other config flag is disabled
  ND RA advertising prefixes configured on interface

  ICMPv6 statistics:
    Rcvd:  0 total, 0 errors
           0 rtr solicits, 0 rtr advertisements
           0 neighbor solicits, 0 neighbor advertisements
           Group membership: 0 queries, 0 responses, 0 reductions
           0 redirects
    Sent:  13 total, 0 errors
           0 rtr solicits, 9 rtr advertisements
           2 neighbor solicits, 2 neighbor advertisements
           Group membership: 0 queries, 0 responses, 0 reductions
           0 redirects

  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Packets 0, Bytes 0
  In Total Dropped Packets 0, Bytes 0
    In Policed Packets 0
    In Invalid Source Address Packets 0
    In Error Packets 0
    In Discarded Packets 0

  Out Forwarded Packets 8, Bytes 768
    Unicast Packets 8, Bytes 768
    Multicast Routed Packets 0, Bytes 0
  Out Total Dropped Packets 5, Bytes 0
    Out Scheduler Dropped Packets 0, Bytes 0
    Out Policed Packets 0
    Out Discarded Packets 5

  queue 0: traffic class best-effort, bound to ipv6 FastEthernet9/0.6
    Queue length 0 bytes
    Forwarded packets 0, bytes 0
    Dropped committed packets 0, bytes 0
    Dropped conformed packets 0, bytes 0
    Dropped exceeded packets 0, bytes 0

loopback5 line protocol IpLoopback is up, ipv6 is up
  Network Protocols: IPv6
  Link local address: fe80::90:1a00:740:1d44
```

```
  Internet address: 10:1:1:0:290:1aff:fe40:1d44/64 (eui-64)
IPv6 statistics:
  Rcvd:  0 local destination
         0 hdr errors, 0 addr errors
         0 unkn proto, 0 discards
  Sent:  0 generated, 0 no routes, 0 discards

ICMPv6 statistics:
  Rcvd:  0 local destination
         0 hdr errors, 0 addr errors
         0 unkn proto, 0 discards
  Sent:  0 generated, 0 no routes, 0 discards

ICMPv6 statistics:
  Rcvd:  0 destination unreach, 0 admin unreach, 0 parameter problem
         0 time exceeded, 0 pkt too big, 0 echo requests
         0 echo replies
  Sent:  0 destination unreach, 0 admin unreach, 0 parameter problem
         0 time exceeded, 0 pkt too big, 0 echo requests
         0 echo replies

  Operational MTU 1500 Administrative MTU 0
  Operational speed 100000000 Administrative speed 0
  Creation type Static
  Neighbor Discovery is disabled

  ICMPv6 statistics:
    Rcvd:  0 total, 0 errors
           0 rtr solicits, 0 rtr advertisements
           0 neighbor solicits, 0 neighbor advertisements
           Group membership: 0 queries, 0 responses, 0 reductions
           0 redirects
    Sent:  0 total, 0 errors
           0 rtr solicits, 0 rtr advertisements
           0 neighbor solicits, 0 neighbor advertisements
           Group membership: 0 queries, 0 responses, 0 reductions
           0 redirects


  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Packets 0, Bytes 0
  In Total Dropped Packets 0, Bytes 0
    In Policed Packets 0
    In Invalid Source Address Packets 0
    In Error Packets 0
    In Discarded Packets 0

  Out Forwarded Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Routed Packets 0, Bytes 0
  Out Total Dropped Packets 0, Bytes 0
    Out Scheduler Dropped Packets 0, Bytes 0
    Out Policed Packets 0
    Out Discarded Packets 0
IPv6 policy input ipv6InPol25
    rate-limit-profile Rlp2Mb classifier-group clgA entry 1
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
    rate-limit-profile Rlp8Mb
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
```



```
  IPv6 policy output ipv6PolOut2
    rate-limit-profile RlpOutA classifier-group clgB entry 1
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
    rate-limit-profile RlpOutB
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
  IPv6 policy local-input ipv6PolLocIn5
    rate-limit-profile Rlp1Mb classifier-group clgC entry 1
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
    rate-limit-profile Rlp5Mb
      Committed: 0 packets, 0 bytes
      Conformed: 0 packets, 0 bytes
      Exceeded:  0 packets, 0 bytes
  queue 0: traffic class best-effort, bound to ipv6 FastEthernet9/0.6
    Queue length 0 bytes
    Forwarded packets 0, bytes 0
    Dropped committed packets 0, bytes 0
    Dropped conformed packets 0, bytes 0
    Dropped exceeded packets 0, bytes 0
```

To display brief summary of IPv6 status and configuration information for all IPv6 interfaces:

```
host1# show ipv6 interface brief
    Interface         IPv6-Address    Status  Protocol   Description
----------------- ------------------ ------- -------- ----------------
null0                 Unnumbered       up      up
FastEthernet9/1.5     5:1:1::2/64      up      up     IPv6 interface in
                                                      Virtual Router Hop
                                                            5
FastEthernet9/0.6     6:1:1::1/64      up      up     IPv6 interface in
                                                      Virtual Router Hop
                                                             6
loopback5          10:1:1:0:290:1aff:fe up      up
                   40:1d44/64
```

Meaning Table 8 on page 101 lists the **show ipv6 interface** command output fields.

Table 8: show ipv6 interface Output Fields

Field Name	Field Description
Description	Optional description for the interface or address specified
Network Protocols	Network protocols configured on this interface
Link local address	Local IPv6 address of this interface
Internet address	External address of this interface

Table 8: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
IPv6 statistics Rcvd	• local destination—Frames with this router as their destination • hdr errors—Number of packets containing header errors • addr errors—Number of packets containing addressing errors • unkn proto—Number of packets received containing unknown protocols • discards—Number of discarded packets
IPv6 statistics Sent	• generated—Number of packets generated • no routes—Number of packets that could not be routed • discards—Number of packets that could not be routed that were discarded NOTE: If you configure the router to discard packets for static routes with null 0 interfaces as the next-hop points using the **reject** keyword with the **ipv6 route** command, the value displayed in this field also includes the packets that reached the null 0 interface and were dropped.

Table 8: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
ICMPv6 statistics Rcvd	• total—Total number of received packets • errors—Error packets received • destination unreach—Packets received with destination unreachable • admin unreach—Packets received because the destination was administratively unreachable (for example, the packet encountered a firewall filter) • parameter problem—Packets received with parameter errors • time exceeded—Packets received with time-to-live exceeded • pkt too big—Number of packet-too-big messages received that indicate a packet was too large to forward because of the allowed MTU size • redirects—Received packet redirects • echo requests—Echo request (ping) packets • echo replies—Echo replies received • rtr solicits—Number of received router solicitations • rtr advertisements—Number of received router advertisements • neighbor solicits—Number of received neighbor solicitations • neighbor advertisements—Number or received neighbor advertisements • Group membership (queries, responses, reductions)—Number of queries, responses, and reduction requests received from within a group to which the interface is assigned

Table 8: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
ICMPv6 statistics Sent	• total—Total number of sent packets • errors—Error packets sent • destination unreach—Packets sent with destination unreachable NOTE: If you configure the router to discard packets for static routes with null 0 interfaces as the next-hop points using the **reject** keyword with the **ipv6 route** command, the value displayed in this field also includes the number of ICMPv6 unreachable messages sent out for packets that reached null 0 interfaces with static routes. • admin unreach—Packets sent because the destination was administratively unreachable (for example, due to a firewall filter) • parameter problem—Packets sent with parameter errors • time exceeded—Packets sent with time-to-live exceeded • pkt too big—Number of packet-too-big messages sent because a received packet was too large to forward because of the allowed MTU size • redirects—Sent packet redirects • echo requests—Echo request (ping) packets • echo replies—Echo replies sent • rtr solicits—Number of sent router solicitations • rtr advertisements—Number of sent router advertisements • neighbor solicits—Number of sent neighbor solicitations • neighbor advertisements—Number of sent neighbor advertisements • Group membership (queries, responses, reductions)—Number of queries, responses, and reduction requests sent to a group of which the interface is assigned
Operational MTU	Value of the MTU
Administrative MTU	Value of the MTU if it has been administratively overridden using the configuration
Operational speed	Speed of the interface
Administrative speed	Value of the speed if it has been administratively overridden using the configuration
Creation type	Method by which the interface was created (static or dynamic)

Table 8: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
HTTP Redirect Url	URL to which a subscriber's initial web browser session is redirected
ND reachable time	Amount of time (in milliseconds) that the neighbor is expected to remain reachable
ND duplicate address detection attempts	Number of times that the router attempts to determine a duplicate address
ND neighbor solicitation retransmission interval	Interval in which the router retransmits neighbor solicitations
ND proxy	Indicates whether the router will reply to solicitations on behalf of a known neighbor
ND RA source link layer	Indicates whether the RA includes the link layer
ND RA interval	Interval (in seconds) of the neighbor discovery router advertisement
ND RA lifetime	Lifetime (in seconds) of the neighbor discovery router advertisement
ND RA managed flag	State of the neighbor discovery router advertisement managed flag
ND RA other config flag	State of the neighbor discovery router advertisement other config flag
ND RA advertising prefixes	Configured advertisement prefixes for neighbor discovery router advertisement
In Received Packets, Bytes	Total number of packets and bytes received on this interface: • Unicast Packets, Bytes—Unicast packets and bytes received on the IPv6 interface; link-local received multicast packets (non-multicast-routed frames) are counted as unicast packets • Multicast Packets, Bytes—Multicast packets and bytes received on the IPv6 interface which are then multicast-routed are counted as multicast packets

Table 8: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
In Total Dropped Packets, Bytes	Total number of inbound packets and bytes dropped on this interface: • In Policed Packets—Packets that were received and dropped on the interface for any of the following reasons: exceeding the token bucket limit, exceeding the rate limit, a drop action in a policy, discarded MAC validation packets, a destination address lookup failure, or when the destination address is an IP interface that has a route configured to the null 0 interface. • In Invalid Source Address Packets—Packets received with invalid source address (for example, spoofed packets) • In Error Packets—Number of packets received with errors • In Discarded Packets—Packets received that were discarded for reasons other than rate limits, errors, and invalid source address
Out Forwarded Packets, Bytes	Total number of packets and bytes that were sent from this interface: • Unicast Packets, Bytes—Unicast packets and bytes that were sent from this interface • Multicast Routed Packets, Bytes—Multicast packets and bytes that were sent from this interface
Out Total Dropped Packets	Total number of outbound packets and bytes dropped by this interface: • Out Scheduler Dropped Packets, Bytes—Number of outbound packets and bytes dropped by the scheduler • Out Policed Packets, Bytes—Number of outbound packets and bytes dropped because of rate limits • Out Discarded Packets—Number of outbound packets that were discarded for reasons other than those dropped by the scheduler and those dropped because of rate limits
IPv6 policy	Type (input, output, local-input) and name of policy: • rate-limit-profile—Name of profile • classifier-group entry—Entry index • Committed—Number of packets and bytes conforming to the committed access rate • Conformed—Number of packets and bytes that exceed the committed access rate but conform to the peak access rate • Exceeded—Number of packets and bytes exceeding the peak access rate

Table 8: show ipv6 interface Output Fields *(continued)*

Field Name	Field Description
queue, traffic class, bound to ipv6	Queue and traffic class bound to the specified IPv6 interface: • Queue length—Number of bytes in queue • Dropped committed packets, bytes—Total number of committed packets and bytes dropped by this interface • Dropped conformed packets, bytes—Total number of conformed packets and bytes dropped by this interface • Dropped exceeded packets, bytes—Total number of exceeded packets and bytes dropped by this interface

Related Documentation

- Configuring IPv6 Hardware Multicast Packet Replication on page 43
- show ipv6 interface on page 135

Monitoring MLD Statistics

Purpose Display MLD information for interfaces on which you enabled MLD.

Action To display statistics, including hardware multicast packet replication status, for all IPv6 interfaces on which you enabled MLD:

```
host1:boston#show ipv6 mld interface
```

```
Interface ATM2/0.103 address 13.0.0.1/255.255.255.0
Administrative state enabled, Operational state enabled
Interface parameters:
    Version 2
    State Querier
    Query Interval 125 secs, 125 secs before the next query
    Other querier present interval 250 secs
    Maximum response time 255 (in 10ths of a second)
    Last member query interval 10 (in 10ths of a second)
    Robustness 3
    No inbound access group
    No inbound access source-group
    No inbound apply-oif-map
    Immediate Leave: disabled
Explicit Host Tracking: enabled
Max-Group limit: No Limit
Admission-Bandwidth limit: No limit
IOA Packet Replication: None
    Group Count: 1
Interface statistics:
    Rcvd: 2 reports, 0 leaves, 0 wrong version queries
    Sent: 2 queries
    Groups learnt: 1

Counts: 0 down, 0 init state, 1 querier, 0 non-querier, 1 Total
```

To display statistics, including hardware multicast packet replication status, for a particular IPv6 interface on which you enabled MLD:

```
host1#show ipv6 mld interface gigabitEthernet 3/0.0
Interface GigabitEthernet3/0.0 address 10.1.1.1/255.255.255.0
Administrative state enabled, Operational state enabled
Interface parameters:
    Version 1
    State Querier
    Query Interval 125 secs, 123 secs before the next query
    Other querier present interval 250 secs
    Maximum response time 100 (in 10ths of a second)
    Last member query interval 10 (in 10ths of a second)
    Robustness 3
    No inbound access group
    No inbound access source-group
    No inbound apply-oif-map
    Immediate Leave: disabled
Explicit Host Tracking: enabled
Max-Group limit: No Limit
    Group Count: 0
    IOA packet replication gigabitEthernet 3/8.1
Interface statistics:
    Rcvd: 0 reports, 0 leaves, 0 wrong version queries
    Sent: 14 queries
    Groups learnt: 0

Counts: 0 down, 0 init state, 1 querier, 0 non-querier, 1 Total
```

Meaning Table 9 on page 108 lists the **show ipv6 mld interface** command output fields.

Table 9: show ipv6 mld interface Output Fields

Field Name	Field Description
Interface	Type of interface and interface specifier. For details about interface types and specifiers, see *Interface Types and Specifiers* in *JunosE Command Reference Guide*.
address	IPv6 link-local address of the interface
Administrative state	Status of the interface in the software: enabled or disabled
Operational state	Physical status of the interface: enabled or disabled
Version	MLD version
State	Function of the interface: querier or nonquerier
Query Interval	Time interval at which this interface sends query messages
Other querier present interval	Time that the interface waits before declaring itself as the querier

Table 9: show ipv6 mld interface Output Fields *(continued)*

Field Name	Field Description
Maximum response time	Time interval during which this interface expects a host to respond
Graceful restart	Status of graceful restart: active or complete
Last member query interval	Time that this interface waits before sending a new query to a host that sends a group leave message
Robustness	Number of times this interface sends MLD messages
Inbound access group	Information about IPv6 access lists configured with the **ipv6 mld access-group** command
No inbound access group	No IPv6 access list configured with the **ipv6 mld access-group** command
Inbound access source-group	Information about IPv6 access lists configured with the **ipv6 mld access-source-group** command
No inbound access source-group	No IPv6 access list configured with the **ipv6 mld access-source-group** command
Inbound apply-oif-map	Information about OIF map names configured with the **ipv6 mld apply-oif-map** command
No inbound apply-oif-map	No OIF map name configured with the **ipv6 mld apply-oif-map** command
Immediate Leave	Setting of the **ipv6 mld immediate-leave** command: enabled or disabled
Explicit Host Tracking	Setting of the **ipv6 mld explicit-tracking** command: enabled or disabled
Max-Group limit	Number of MLD groups that the interface can accept, as configured with the **ipv6 mld group limit** command
Group Count	Number of MLD groups that the interface has accepted
IOA packet replication	Hardware multicast packet replication interface to which egress multicast packets on this interface are redirected

Table 9: show ipv6 mld interface Output Fields *(continued)*

Field Name	Field Description
Interface statistics Rcvd	Information about MLD messages received on this interface: • reports—Number of group multicast listener reports received • leaves—Number of group multicast listener done messages received • wrong version queries—Number of multicast listener queries received from devices running a different version of MLD • Interface statistics Sent—Number of MLD messages this interface has sent • Interface statistics Groups learnt—Number of groups this interface has discovered
Counts	Total number of MLD interfaces

Related Documentation

- Configuring IPv6 Hardware Multicast Packet Replication on page 43
- show ipv6 mld interface on page 136

CHAPTER 21

Verifying the Multicast Forwarding Entries in IPv6 Multicast Routing Table

Monitoring IPv6 Multicast Forwarding Entries

Purpose Displays information about all or specified multicast forwarding entries. You can specify a multicast group IPv6 address or both a multicast group IPv6 address and a multicast source IPv6 address to display information about particular multicast forwarding entries.

Action To display all multicast forwarding entries while bandwidth rate is constant:

```
host1#show ipv6 mroute
IPv6 Multicast Routing Table

(S, G) uptime d h:m:s[, expires d h:m:s]
  [Admission bandwidth: bps]
  [QoS bandwidth: bps]
  RPF route: addr/mask, incoming interface
             neighbor address, owner route-owner
  Incoming interface list:
      Interface (addr/mask), State/Owner [(RPF IIF)]
  Outgoing interface list:
      Interface (addr/mask), State/Owner, Uptime/Expires

(10:0:0:1:1::, ff0e::1) uptime 0 01:04:12
  RPF route: 10:0:0:1::/64, incoming interface ATM2/3.1001
             neighbor 10:0:0:1::1, owner Local
  Incoming interface list:
      ATM2/3.1001 (10:0:0:1::1/64), Accept/Pim (RPF IIF)
  Outgoing interface list:
      ATM2/0.200 (21:2:2:21::2:1/60), Forward/Pim, 0 01:04:12/never

(10:0:0:1:2::, ff0e::1) uptime 0 01:04:12
  RPF route: 10:0:0:1::/64, incoming interface ATM2/3.1001
             neighbor 10:0:0:1::1, owner Local
  Incoming interface list:
```

```
      ATM2/3.1001 (10:0:0:1::1/64), Accept/Pim (RPF IIF)
  Outgoing interface list:
      ATM2/0.200 (21:2:2:21::2:1/60), Forward/Pim, 0 01:04:12/never

Counts: 2 (S, G) entries
        0 (*, G) entries
```

To display all multicast forwarding entries when bandwidth limit of all the join interfaces exceeds configured CAC limits:

```
host1#show ipv6 mroute
IP Multicast Routing Table

(S, G) uptime d h:m:s[, expires d h:m:s]
  [Admission bandwidth: bps]
  [QoS bandwidth: bps]
  RPF route: addr/mask, incoming interface
             neighbor address, owner route-owner
  Incoming interface list:
      Interface (addr/mask), State/Owner [(RPF IIF)]
  Outgoing interface list:
      Interface (addr/mask), State/Owner, Uptime/Expires

(10:0:0:1:1::, ff0e::1) uptime 0 01:04:12
  RPF route: 10:0:0:1::/64, incoming interface ATM2/3.1001
             neighbor 10:0:0:1::1, owner Local
  Incoming interface list:
      ATM2/3.1001 (10:0:0:1::1/64), Accept/Pim (RPF IIF)
  Outgoing interface list:
      ATM2/0.200 (21:2:2:21::2:1/60), Forward/Pim, 0 01:04:12/never

(10:0:0:1:2::, ff0e::1) uptime 0 01:04:12
  RPF route: 10:0:0:1::/64, incoming interface ATM2/3.1001
             neighbor 10:0:0:1::1, owner Local
  Incoming interface list:
      ATM2/3.1001 (10:0:0:1::1/64), Accept/Pim (RPF IIF)
  Outgoing interface list:
      ATM2/0.200 (21:2:2:21::2:1/60), Blocked (join-intf-adm-limit)/IGMP, 0
01:04:12/never

Counts: 2 (S, G) entries
        0 (*, G) entries
```

Meaning Table 10 on page 112 lists the **show ipv6 mroute** command output fields.

Table 10: show ipv6 mroute Output Fields

Field Name	Field Description
(S,G)	IPv6 addresses of the multicast source and the multicast group
Uptime	Length of time that the (S,G) pair has been active, in *days hours:minutes:seconds* format
Expires	Length of time for which the (S,G) pair will be active, in *days hours:minutes:seconds* format
Admission bandwidth	Admission bandwidth (in bps)
QoS bandwidth	QoS bandwidth (in bps)

Table 10: show ipv6 mroute Output Fields *(continued)*

Field Name	Field Description
RPF Route	IPv6 address and prefix of the RPF route
Incoming interface	Type and specifier of the incoming interface for the RPF route
neighbor address	IPv6 address of the neighbor
owner	Owner of the route: • Local—route belonging to the local interface • Static—Static route • Other protocols—Route established by a protocol
Incoming interface list	List of incoming interfaces on the router. Details include: • Type of interface and its specifier • Action that the interface takes with packets: accept or discard • Multicast protocol that owns the interface • Time that the interface has been active in this multicast forwarding entry, in *days hours:minutes:seconds* format • Time that the interface will cease to be active in this multicast forwarding entry, in *days hours:minutes:seconds* format
Outgoing interface list	List of outgoing interfaces on the router. Details include: • Type of interface and its specifier • Action that the interface takes with packets: Forward or Blocked (intf-adm-limit, join-intf-adm-limit, port-adm-limit, port-limit, port-priority-limit) • Protocol running on the interface: PIM or MLD • Time that the interface has been active in this multicast forwarding entry, in *days hours:minutes:seconds* format • Time that the interface will cease to be active in this multicast forwarding entry, in *days hours:minutes:seconds* format
Counts	Numbers of types of source group mappings: • (S,G)—Number of (S,G) entries • (*,G)—Number of (*,G) entries

Related Documentation

- Defining IPv6 Static Routes for Reverse-Path Forwarding on page 37

- show ipv6 mroute on page 137

Monitoring Active IPv6 Multicast Routes

Purpose Display the active multicast routes.

- You can specify a multicast group IPv6 address or both a multicast group IPv6 address and a multicast source IPv6 address to display information about particular multicast forwarding entries.
- You can specify the bandwidth threshold to display the active multicast routes with admission bandwidth greater than the specified bandwidth threshold. The default bandwidth threshold is 4000 bps.
- You can use the **summary** option to see a summary rather than a detailed description.
- You can use the **count** option to display the number of active multicast forwarding entries.
- You can use the **oif-detail** option to display the details of the join interfaces corresponding to the mapped interface when oif-mapping is configured.
- You can use the **statistics** option to display statistics for packets received through all active multicast forwarding entries that the router has added to the multicast routing table and established on the appropriate line modules.

Action To display the active multicast routes with admission bandwidth above 10000 bps:

```
host1#show ipv6 mroute active 10000
Active IP Multicast Routes >=10000 bps

(S, G) uptime d h:m:s[, expires d h:m:s]

[Admission bandwidth: bps]

[QoS bandwidth: bps]

RPF route: addr/mask, incoming interface

neighbor address, owner route-owner

Incoming interface list:

Interface (addr/mask), State/Owner [(RPF IIF)]

Outgoing interface list:

Interface (addr/mask), State/Owner, Uptime/Expires

(52::1, ff3e::1) uptime 0 00:01:07

Admission bandwidth: 47000 bps (adaptive)

QoS bandwidth: 47000 bps (adaptive)

RPF route: 52::/112, incoming interface ATM2/1.17

neighbor 17::2, owner NetmgmtRpf

Incoming interface list:

ATM2/1.17 (fe80::90:1a00:3140:1ff8/128), Accept/MLD (RPF IIF)

Outgoing interface list:
```



```
NULL
Counts: 1 (S, G) entries
0 (*, G) entries
```

To display the summary of active multicast routes:

```
host1#show ipv6 mroute summary active
Active IP Multicast Routes >=4000 bps
Group Address Source Address  RPF route RPF Iif   #Oifs
--------------- ------------ ----------- --------- -----
232.0.0.1     51.0.0.1      51.0.0.0/24  ATM3/1.17  0
232.0.0.2     51.0.0.1      51.0.0.0/24  ATM3/1.17  0
232.0.0.3     51.0.0.1      51.0.0.0/24  ATM3/1.17  0
Counts: 3 (S, G) entries
0 (*, G) entries
```

Meaning Table 11 on page 115 lists the **show ipv6 mroute active** and **show ipv6 mroute summary active** commands output fields.

Table 11: show ipv6 mroute active and show ipv6 mroute summary active Output Fields

Field Name	Field Description
(S,G)	IPv6 addresses of the multicast source and the multicast group
Uptime	Length of time that the (S,G) pair has been active, in *days hours:minutes:seconds* format
Expires	Length of time for which the (S,G) pair will be active, in *days hours:minutes:seconds* format
Admission bandwidth	Admission bandwidth (in bps)
QoS bandwidth	QoS bandwidth (in bps)
RPF Route	IPv6 address and prefix of the RPF route
Incoming interface	Type and specifier of the incoming interface for the RPF route
neighbor address	IPv6 address of the neighbor
owner	Owner of the route: • Local—route belonging to the local interface • Static—Static route • Other protocols—Route established by a protocol

Table 11: show ipv6 mroute active and show ipv6 mroute summary active Output Fields *(continued)*

Field Name	Field Description
Incoming interface list	List of incoming interfaces on the router. Details include: • Type of interface and its specifier • Action that the interface takes with packets: accept or discard • Multicast protocol that owns the interface • Time that the interface has been active in this multicast forwarding entry, in *days hours:minutes:seconds* format • Time that the interface will cease to be active in this multicast forwarding entry, in *days hours:minutes:seconds* format
Outgoing interface list	List of outgoing interfaces on the router. Details include: • Type of interface and its specifier • Action that the interface takes with packets: Forward or Blocked (intf-adm-limit, join-intf-adm-limit, port-adm-limit, port-limit, port-priority-limit) • Protocol running on the interface: PIM or MLD • Time that the interface has been active in this multicast forwarding entry, in *days hours:minutes:seconds* format • Time that the interface will cease to be active in this multicast forwarding entry, in *days hours:minutes:seconds* format
Counts	Numbers of types of source group mappings: • (S,G)—Number of (S,G) entries • (*,G)—Number of (*,G) entries
Group Address	IP address of the multicast group
Source Address	IP address of the multicast source
RPF Iif	Type and identifier for the incoming interface for the RPF route
#Oifs	Number of outgoing interfaces

Related Documentation

- Defining IPv6 Static Routes for Reverse-Path Forwarding on page 37
- show ipv6 mroute on page 137

Monitoring IPv6 Multicast Entries in a Source or Group

Purpose Display information about the number of groups and sources.

- You can specify a multicast group address or both a multicast group address and a multicast source address to display information about a particular multicast forwarding entry.
- You can use the **active** option to display information for the active multicast routes.
- You can specify the bandwidth threshold along with the **active** option to display information for the active multicast routes with admission bandwidth greater than the specified bandwidth threshold. The default bandwidth threshold is 4000 bps.

Action To display the number of groups and sources:

```
host1#show ipv6 mroute count
IPv6 Multicast Routing Table

Counts: 2000 (S, G) entries
        0 (*, G) entries
```

Meaning Table 12 on page 117 lists the **show ipv6 mroute count** command output fields.

Table 12: show ipv6 mroute count Output Fields

Field Name	Field Description
Counts	Number of types of source group mappings: • (S,G)—Number of (S,G) entries • (*,G)—Number of (*,G) entries

Related Documentation

- show ipv6 mroute on page 137

Monitoring Join Interface Details When IPv6 OIF Mapping Is Configured

Purpose Display details of the join interfaces corresponding to the mapped interfaces when OIF mapping is configured.

- You can specify a multicast group address or both a multicast group address and a multicast source address to display information about a particular multicast forwarding entry.
- You can use the **active** option to display information for the active multicast routes.
- You can specify the bandwidth threshold along with the **active** option to display information for the active multicast routes with admission bandwidth greater than the specified bandwidth threshold. The default bandwidth threshold is 4000 bps.

Action To display details of the join interfaces:

```
host1#show ipv6 mroute oif-detail
                  IPv6 Multicast Routing Table

(S, G) uptime d h:m:s[, expires d h:m:s]
[Data rate: Kbps] [SPT threshold: Kbps]
[Threshold: Kbps]
  [Admission bandwidth: bps]
  [QoS bandwidth: bps]
  RPF route: addr/mask, incoming interface
             neighbor address, owner route-owner
  Incoming interface list:
      Interface (addr/mask), State/Owner [(RPF IIF)]
  Outgoing interface list:
      Interface (addr/mask), State/Owner, Uptime/Expires
  Join interface list:
  Interface (addr/mask)[, State/Owner]

 (2000::1, ff1e::1) uptime 0 00:00:04
  Admission bandwidth: 60000000 bps
  QoS bandwidth: 0 bps (adaptive)
  RPF route: 2000::1/128, incoming interface GigabitEthernet13/1/1
             neighbor 2000::1, owner Local
  Incoming interface list:
      GigabitEthernet13/1/1 (fe80::290:1aff:fe42:8e5a/128), Accept/Mld (RPF IIF)

  Outgoing interface list:
      GigabitEthernet13/1/4 (fe80::290:1aff:fe42:8e5d/128), Blocked
(intf-adm-limit)/Mld, 0 00:00:04/never
     Join interface list:
      GigabitEthernet15/0/1.10 (fe80::290:1aff:fe42:2731/128)

Counts: 1 (S, G) entries
        0 (*, G) entries
```

Meaning Table 13 on page 118 lists the **show ipv6 mroute oif-detail** command output fields.

Table 13: show ipv6 mroute oif-detail Output Fields

Field Name	Field Description
(S,G)	IPv6 addresses of the multicast source and the multicast group
Uptime	Length of time that the (S,G) pair has been active, in *days hours:minutes:seconds* format
Expires	Length of time for which the (S,G) pair will be active, in *days hours:minutes:seconds* format
Admission bandwidth	Admission bandwidth (in bps)
QoS bandwidth	QoS bandwidth (in bps)
RPF Route	IPv6 address and prefix of the RPF route
Incoming interface	Type and specifier of the incoming interface for the RPF route

Table 13: show ipv6 mroute oif-detail Output Fields *(continued)*

Field Name	Field Description
neighbor address	IPv6 address of the neighbor
owner	Owner of the route: • Local—route belonging to the local interface • Static—Static route • Other protocols—Route established by a protocol
Incoming interface list	List of incoming interfaces on the router. Details include: • Type of interface and its specifier • Action that the interface takes with packets: accept or discard • Multicast protocol that owns the interface • Time that the interface has been active in this multicast forwarding entry, in *days hours:minutes:seconds* format • Time that the interface will cease to be active in this multicast forwarding entry, in *days hours:minutes:seconds* format
Outgoing interface list	List of outgoing interfaces on the router. Details include: • Type of interface and its specifier • Action that the interface takes with packets: Forward or Blocked (intf-adm-limit, join-intf-adm-limit, port-adm-limit, port-limit, port-priority-limit) • Protocol running on the interface: PIM or MLD • Time that the interface has been active in this multicast forwarding entry, in *days hours:minutes:seconds* format • Time that the interface will cease to be active in this multicast forwarding entry, in *days hours:minutes:seconds* format

Table 13: show ipv6 mroute oif-detail Output Fields *(continued)*

Field Name	Field Description
Join interface list	List of join interfaces on the router. Details include: • Type of interface and its specifier • Action that the interface takes with packets: Forward or Blocked (intf-adm-limit, join-intf-adm-limit, port-adm-limit, port-limit, port-priority-adm-limit) • Protocol running on the interface: PIM, DVMRP, or IGMP • Amount of time that the interface has been active in this multicast forwarding entry, in *days hours:minutes:seconds* format • Length of time that the interface can remain active in this multicast forwarding entry, in *days hours:minutes:seconds* format or *never*
Counts	Numbers of types of source group mappings: • (S,G)—Number of (S,G) entries • (*,G)—Number of (*,G) entries

Related Documentation

- Blocking IPv6 Mroutes on page 45
- Creating IPv6 Mroute Port Limits on page 47
- **show ipv6 mroute on page 137**

Monitoring IPv6 Multicast Statistics

Purpose Display statistics for packets received through multicast routes that the router has added to the multicast routing table and established on the appropriate line modules.

- You can specify a multicast group address or both a multicast group address and a multicast source address to display information about a particular multicast forwarding entry.
- You can use the **active** option to display information for the active multicast routes.
- You can specify the bandwidth threshold along with the **active** option to display information for the active multicast routes with admission bandwidth greater than the specified bandwidth threshold. The default bandwidth threshold is 4000 bps.

Action To display the statistics of the multicast routes added to the multicast routing table:

```
host#show ipv6 mroute statistics
IPv6 Multicast Routing Table

(S, G) uptime d h:m:s[, expires d h:m:s]
  [Admission bandwidth: bps]
  [QoS bandwidth: bps]
  RPF route: addr/mask, incoming interface
```

```
            neighbor address, owner route-owner
  Incoming interface list:
      Interface (addr/mask), State/Owner [(RPF IIF)]
  Outgoing interface list:
      Interface (addr/mask), State/Owner, Uptime/Expires

(10:0:0:1:1::, ff0e::1) uptime 0 01:05:23
  Admission bandwidth:
  RPF route: 10:0:0:1::/64, incoming interface ATM2/3.1001
            neighbor 10:0:0:1::1, owner Local
  Incoming interface list:
      ATM2/3.1001 (10:0:0:1::1/64), Accept/Pim (RPF IIF)
  Outgoing interface list:
      ATM2/0.200 (21:2:2:21::2:1/60), Forward/Pim, 0 01:05:23/never
  Statistics:
      Received   : 346 pkts, 22144 bytes
      Forwarded  : 346 pkts, 22144 bytes
      Rcvd on OIF: 0 pkts

(10:0:0:1:2::, ff0e::1) uptime 0 01:05:23
  RPF route: 10:0:0:1::/64, incoming interface ATM2/3.1001
            neighbor 10:0:0:1::1, owner Local
  Incoming interface list:
      ATM2/3.1001 (10:0:0:1::1/64), Accept/Pim (RPF IIF)
  Outgoing interface list:
      ATM2/0.200 (21:2:2:21::2:1/60), Forward/Pim, 0 01:05:26/never
  Statistics:
      Received   : 346 pkts, 22144 bytes
      Forwarded  : 346 pkts, 22144 bytes
      Rcvd on OIF: 0 pkts
```

Meaning Table 14 on page 121 lists the **show ipv6 mroute statistics** command output fields.

Table 14: show ipv6 mroute statistics Output Fields

Field Name	Field Description
(S,G)	IPv6 addresses of the multicast source and the multicast group
Uptime	Length of time that the (S,G) pair has been active, in *days hours:minutes:seconds* format
Expires	Length of time for which the (S,G) pair will be active, in *days hours:minutes:seconds* format
Admission bandwidth	Admission bandwidth (in bps)
QoS bandwidth	QoS bandwidth (in bps)
RPF Route	IPv6 address and prefix of the RPF route
Incoming interface	Type and specifier of the incoming interface for the RPF route
neighbor address	IPv6 address of the neighbor

Table 14: show ipv6 mroute statistics Output Fields *(continued)*

Field Name	Field Description
owner	Owner of the route: • Local—route belonging to the local interface • Static—Static route • Other protocols—Route established by a protocol
Incoming interface list	List of incoming interfaces on the router. Details include: • Type of interface and its specifier • Action that the interface takes with packets: accept or discard • Multicast protocol that owns the interface • Time that the interface has been active in this multicast forwarding entry, in *days hours:minutes:seconds* format • Time that the interface will cease to be active in this multicast forwarding entry, in *days hours:minutes:seconds* format
Outgoing interface list	List of outgoing interfaces on the router. Details include: • Type of interface and its specifier • Action that the interface takes with packets: Forward or Blocked (intf-adm-limit, join-intf-adm-limit, port-adm-limit, port-limit, port-priority-limit) • Protocol running on the interface: PIM or MLD • Time that the interface has been active in this multicast forwarding entry, in *days hours:minutes:seconds* format • Time that the interface will cease to be active in this multicast forwarding entry, in *days hours:minutes:seconds* format
Statistics	• Received—Number of packets and bytes that the virtual router received for this multicast route • Forwarded—Number of packets and statistics that the virtual router has forwarded for this multicast route • Rcvd on OIF—Number of packets and statistics that the virtual router has received on the OIF for this multicast route NOTE: The display shows statistics after the virtual router has added the multicast route to the multicast routing table and established the route on the appropriate line module. Statistics for interactions before the route is established on the line module are not displayed.

Related Documentation

- Blocking IPv6 Mroutes on page 45
- Creating IPv6 Mroute Port Limits on page 47
- show ipv6 mroute on page 137

Monitoring Summary Information of IPv6 Multicast Routes

Purpose Display a summary of all or specified multicast routes.

- You can specify a multicast group address or both a multicast group address and a multicast source address to display information about a particular multicast forwarding entry.
- You can use the **active** option to display information for the active multicast routes.
- You can specify the bandwidth threshold along with the **active** option to display information for the active multicast routes with admission bandwidth greater than the specified bandwidth threshold. The default bandwidth threshold is 4000 bps.

Action To display a summary of all multicast routes:

```
host1#show ipv6 mroute summary
IPv6 Multicast Routing Table

Group Address   Source Address  RPF route          RPF Iif         #Oifs
--------------- --------------- ------------------ --------------- -----
ff0e::1         10:0:0:1:1::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:2::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:3::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:4::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:5::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:6::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:7::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:8::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:9::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:a::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:b::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:c::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:d::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:e::    10:0:0:1::/64      ATM2/3.1001     1
ff0e::1         10:0:0:1:f::    10:0:0:1::/64      ATM2/3.1001     1

Counts: 16 (S, G) entries
        0 (*, G) entries
```

Meaning Table 15 on page 123 lists the **show ipv6 mroute summary** command output fields.

Table 15: show ipv6 mroute summary Output Fields

Field Name	Field Description
Group Address	IP address of the multicast group
Source Address	IP address of the multicast source
RPF Route	IP address and network mask of the RPF route

Table 15: show ipv6 mroute summary Output Fields *(continued)*

Field Name	Field Description
RPF Iif	Type and identifier for the incoming interface for the RPF route
#Oifs	Number of outgoing interfaces
Counts	Numbers of types of (S,G) mappings: • (S,G)—Number of (S,G) entries • (*,G)—Number of (*,G) entries

Related Documentation

- Defining IPv6 Static Routes for Reverse-Path Forwarding on page 37
- show ipv6 mroute on page 137

CHAPTER 22

Displaying the IPv6 Multicast Protocols Enabled on the Router

Monitoring IPv6 Multicast Protocols Enabled on the Router

Purpose Display information about multicast protocols enabled on the router.

Action To display information about enabled multicast protocols:

```
host1:2#show ipv6 multicast protocols
Multicast protocols:

Protocol Pim
    Type: Sparse
    Interfaces: 1 registered, 1 owned
    Registered interfaces:
        ATM2/1.103 (21:2:2:22::1:2/60) owner Pim
Protocol Mld
    Type: Local
    Interfaces: 1000 registered, 1000 owned
    Registered interfaces:
        ATM2/0.131 (31:2:2:22::2:2/604) local Mld owner Mld
            Admission-bandwidth 2000000/10000000 bps
            QoS Adjust 2000 bps
        ATM2/0.132 (31:2:2:22::2:3/60) local Mld owner Mld
            Admission-bandwidth 0/10000000 bps
            QoS Adjust 0 bps
        ATM2/0.133 (31:2:2:22::2:4/60) local Mld owner Mld
            Admission-bandwidth 8000000/10000000 bps, 2 Blocked OIFs
            QoS Adjust 0 bps
...
Count: 2  protocols
```

Meaning Table 16 on page 125 lists the **show ipv6 multicast protocols** command output fields.

Table 16: show ipv6 multicast protocols Output Fields

Field Name	Field Description
Protocol	Name of the multicast protocol

Table 16: show ipv6 multicast protocols Output Fields *(continued)*

Field Name	Field Description
Type	Mode of the multicast protocol: • For PIM—Sparse • For MLD—Local
Interfaces	• registered—Number of interfaces on which the protocol is configured • owned—Number of interfaces that a protocol owns. If you configure only MLD on an interface, MLD owns the interface. However, if you configure MLD and PIM on the same interface, PIM owns the interface.
Registered interfaces	Includes the following information about interfaces on which the protocol is configured: • Types and identifiers of interfaces. For details about interface types and specifiers, see *Interface Types and Specifiers* in *JunosE Command Reference Guide* . • Protocols configured on the interface and the protocol that owns the interface. If you configure only MLD on an interface, MLD owns the interface. However, if you configure MLD and PIM on the same interface, PIM owns the interface. • Admitted bandwidth / configured admission bandwidth (in bps) • Number of blocked OIFs • QoS adjustment bandwidth (in bps)
Count	Number of multicast protocols on the virtual router

Related Documentation

- Example: Configuring an IPv6 Multicast Bandwidth Map on page 49
- Activating IPv6 Multicast QoS Adjustment Functions on page 41
- Enabling Interface-Level Admission Bandwidth Limitation for IPv6 on page 45
- Enabling Port-Level Admission Bandwidth Limitation for IPv6 on page 47
- **show ipv6 multicast protocols on page 138**

Monitoring Summary Information of IPv6 Multicast Protocols Enabled on the Router

Purpose Display information about multicast protocols enabled on the router.

Action To display a summary of information about multicast protocols enabled on the router:

```
host1#show ipv6 multicast protocols brief
Protocol  Registered Owned       Type
          Interfaces Interfaces
```

```
--------- ---------- ---------- -------------------
Pim             1          1    Sparse
Mld             1          1    Local

Count: 2 protocols
```

Meaning Table 17 on page 127 lists the **show ipv6 multicast protocols brief** command output fields.

Table 17: show ipv6 multicast protocols brief Output Fields

Field Name	Field Description
Protocol	Name of the multicast protocol
Registered Interfaces	Number of interfaces on which the protocol is configured
Owned Interfaces	Number of interfaces that a protocol owns. If you configure only MLD on an interface, MLD owns the interface. However, if you configure MLD and PIM on the same interface, PIM owns the interface
Type	Mode of the multicast protocol: • For PIM—Sparse • For MLD—Local
Count	Number of multicast protocols on the virtual router

Related Documentation

- show ipv6 multicast protocols on page 138

CHAPTER 23

Verifying the Status of IPv6 Multicast Routing

Monitoring IPv6 Multicast Status on a Virtual Router

Purpose Display information about the status of IPv6 multicast on the virtual router.

Action To display information about the status of IPv6 multicast on the virtual router:

```
host1#show ipv6 multicast routing
Multicast forwarding is enabled on this router
Multicast graceful restart is complete (timer 0 seconds) on this router
Multicast cache-miss processing is enabled on this router


Multicast forwarding is enabled on this router
Multicast graceful restart is complete (timer 0 seconds) on this router
Multicast cache-miss processing is enabled on this router
```

Related Documentation

- Enabling IPv6 Multicast on page 35
- show ipv6 multicast routing on page 139

CHAPTER 24

Verifying the Multicast Routes

Monitoring Multicast Routes on Virtual Router Ports

Purpose Display information for multicast routes on a port across all virtual routers.

NOTE: This command displays information for mroutes on a port across all virtual routers.

Action To display the multicast route port outgoing interface, limits, counts, bandwidth settings, and bandwidth accepted:

```
host1#show mroute port count

BW     Priority
Port    Limit   Count    bps     BW bps    Hysteresis   Admitted
-----   -----   -----   -----   --------   ----------   --------
1/1/0   None    1       None    None       85           0
1/1/1   None    2       15000   10000      85           2000
```

Meaning Table 18 on page 131 lists the output fields of the **show mroute port count** command.

Table 18: show mroute port count Output Fields

Field Name	Field Description
Port	Slot or port value on the router
Limit	None (reserved for future functionality)
Count	Number of multicast route outgoing interfaces on the specified port
BW bps	Bandwidth limit (in bits per second)
Priority BW bps	Priority bandwidth limit (in bits per second)
Admitted	Bandwidth admitted on the port (in bits per second)

Related Documentation

- *Defining a Multicast Bandwidth Map*
- *Creating Mroute Port Limits*
- *Enabling Port-Level Admission Bandwidth Control*
- show mroute port count on page 142

CHAPTER 25

Monitoring Commands

show interfaces

Syntax show interfaces *interfaceType interfaceSpecifier* [delta] [brief] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the current state of the interface you specify.

Options

- *interfaceType*—Interface type; see *Interface Types and Specifiers*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*; for ATM, subinterfaces are not supported by the syntax
- delta—Displays baselined statistics
- brief—Displays a brief summary of the interface
- *filter*—See *Filtering show Commands*

Mode Privileged Exec, User Exec

Related Documentation

- *Monitoring the QoS Configuration of ATM Interfaces*
- *Monitoring the QoS Configuration of Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet Interfaces*
- *Monitoring Interfaces and Policy Lists*

show ipv6 interface

Syntax

show ipv6 interface [vrf *vrfName*] [brief | detail]
[*interfaceType interfaceSpecifier*][delta] [*filter*]

To display summary information:

show ipv6 interface summary [vrf *vrfName*] [*filter*]

Release Information

Command introduced before JunosE Release 7.1.0.
vrf keyword and *vrfName* variable added in JunosE Release 7.2.0.

Description

Displays current state of all IPv6 interfaces or the IPv6 interfaces that you specify. The default is all interface types and all interfaces.

Options

- *vrfName*—Name of the VRF
- brief—Displays a brief summary of IPv6 status and configuration information
- detail—Shows a detailed display of IP status and configuration information
- *interfaceType*—Interface type; see *Interface Types and Specifiers*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*
- delta—Displays baselined statistics
- *filter*—See *Filtering show Commands*
- summary—Shows a detailed summary of IP status and configuration

Mode

Privileged Exec, User Exec

Related Documentation

- *Monitoring the Policy Configuration of IPv6 Interfaces*
- Monitoring IPv6 Statistics on page 92

show ipv6 mld interface

Syntax show ipv6 mld interface [brief | count] [delta]
[*interfaceType interfaceSpecifier*] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays MLD information for interfaces on which you enabled MLD.

Options

- brief—Displays a summary of the information
- count—Displays the total number of interfaces on which you enabled MLD
- delta—Displays baselined statistics
- *interfaceType*—Interface type; see *Interface Types and Specifiers*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*
- *filter*—See *Filtering show Commands*

Mode Privileged Exec, User Exec

Related Documentation

- Monitoring MLD Statistics on page 107

show ipv6 mroute

Syntax show ipv6 mroute [*groupIpAddress* [*sourceIpAddress*]]
[summary | count | oif-detail | statistics] [active [*bandwidth*]] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.
active keyword added in JunosE Release 8.1.0.
oif-detail keyword added in JunosE Release 12.0.0.

Description Displays information about all or specified multicast routes.

Options
- *groupIpAddress*—IPv6 address of a multicast group
- *sourceIpAddress*—IPv6 address of a multicast source
- summary—Displays brief information about the multicast routes
- count—Displays the number of groups and sources
- oif-detail—Displays details of the join interfaces corresponding to the mapped interface when OIF-mapping is configured
- statistics—Displays statistics for packets received through multicast routes that the router has added to the multicast routing table and established on the appropriate line modules
- active—Displays active mroutes
- *bandwidth*—Admission bandwidth for active multicast routes that is greater than the specified bandwidth threshold; default is 4000 bps
- *filter*—See *Filtering show Commands*

Mode Privileged Exec, User Exec

Related Documentation
- Monitoring IPv6 Multicast Forwarding Entries on page 111
- Monitoring Active IPv6 Multicast Routes on page 114
- Monitoring IPv6 Multicast Entries in a Source or Group on page 117
- Monitoring Join Interface Details When IPv6 OIF Mapping Is Configured on page 117
- Monitoring IPv6 Multicast Statistics on page 120
- Monitoring Summary Information of IPv6 Multicast Routes on page 123

show ipv6 multicast protocols

Syntax show ipv6 multicast protocols [brief] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about the multicast protocols enabled on the router.

Options
- brief—Displays a summary rather than detailed information
- *filter*—See *Filtering show Commands*

Mode Privileged Exec, User Exec

Related Documentation
- Monitoring IPv6 Multicast Protocols Enabled on the Router on page 125
- Monitoring Summary Information of IPv6 Multicast Protocols Enabled on the Router on page 126

show ipv6 multicast routing

Syntax show ipv6 multicast routing [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about the status of multicast routing on the router.

Options
- *filter*—See *Filtering show Commands*

Mode Privileged Exec, User Exec

Related Documentation
- Monitoring IPv6 Multicast Status on a Virtual Router on page 129

show ipv6 rpf-route

Syntax show ipv6 rpf-route [vrf *vrfName*] [*ipv6Address* [detail] | *ipv6Prefix* [detail]] [all] [*protocol*] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.
vrf keyword and *vrfName* variable added in JunosE Release 7.2.0.

Description Displays IPv6 routes that the router can use to verify source addresses in multicast packets.

Options

- *vrfName*—Name of the VRF
- *ipv6Address*—Specific IPv6 address to show
- *ipv6Mask*—IPv6 mask of the specific address to show
- detail—displays detailed information about the specified route
- all—Displays routes from all sources to a prefix
- *protocol*—One of the following protocols for which you want to display the best routes in the routing table; no routes are displayed if routes for the specified protocol are not present in the routing table
  - access—Displays the best access-server routes (BGP) in the routing table
  - access-internal—Displays the best access-internal routes in the routing table
  - bgp—Displays the best BGP routes in the routing table
  - bgp-tunnel—Displays the best BGP tunnel routes in the routing table
  - dvmrp—Displays the best DVMRP routes in the routing table
  - isis—Displays the best IS-IS routes in the routing table
  - ldp—Displays the best LDP tunnel routes in the routing table
  - local—Displays the best locally connected routes in the routing table
  - mbgp—Displays the best MBGP routes in the routing table
  - ospf—Displays the best OSPF routes owned by in the routing table
  - other—Displays the best internal control routes in the routing table
  - rip—Displays the best RIP routes in the routing table
  - rsvp—Displays the best RSVP tunnel routes in the routing table
  - static—Displays the best static routes added by network management to the routing table
  - static-rpf—Displays the best static RPF routes added by network management to the routing table
- *filter*—See *Filtering show Commands*

Mode Privileged Exec, User Exec

Related Documentation
- Monitoring Available IPv6 Routes for Reverse-Path Forwarding on page 83

show mroute port count

Syntax show mroute port [*portNumber*] count [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the mroute port outgoing interface limits and counts.

Options
- *portNumber*—Port number (in the form *slot/port*) for which you want to display information; if you omit the port number, the router displays information for all ports belonging to the bridge group
- *filter*—See *Filtering show Commands*

Mode Privileged Exec, User Exec

Related Documentation
- Monitoring Multicast Routes on Virtual Router Ports on page 131

show vlan subinterface

Syntax show vlan subinterface [*interfaceType interfaceSpecifier*] [mac-address] [*filter*]

To display summary information:

show vlan subinterface summary

To display by VLAN ID or S-VLAN ID:

show vlan subinterface { svlan *s-vlanIdValue* | vlan } { *vlanIdValue* | any }
[mac-address] [*filter*]

To display VLAN subinterfaces that are created based on agent-circuit-identifier information:

show vlan subinterface [*interfaceType interfaceSpecifier* | svlan *s-vlanIdValue*]
agent-circuit-identifier [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.
s-vlan keyword and *s-vlanIdValue* variable added in JunosE Release 7.1.0.
vlan keyword and *vlanIdValue* variable added in JunosE Release 7.1.0.
any and **mac-address** keywords added in JunosE Release 7.1.0.
agent-circuit-identifier keyword added in JunosE Release 7.3.0.

Description Displays configuration and status information for a specified VLAN subinterface or for all VLAN subinterfaces configured on the router. Alternatively, you can use the **summary** keyword to display only brief summary information for all VLAN interfaces. You can also display information about the VLAN IDs or S-VLAN IDs for the specified VLAN subinterface.

Options

- *interfaceType*—One of the following interface types listed in *Interface Types and Specifiers:*
  - atm
  - fastEthernet
  - gigabitEthernet
  - lag
  - tenGigabitEthernet
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*
- mac-address—Displays VLAN subinterfaces configured with unique MAC addresses
- *filter*—See *Filtering show Commands*
- summary—Displays only the total number of VLAN subinterfaces and the total number of VLAN major interfaces configured on the router
- *s-vlanIdValue*—S-VLAN ID number in the range 0–4095

- *vlanIdValue*—VLAN ID number in the range 0–4095
- any—Specifies the VLAN ID as a wildcard
- agent-circuit-identifier—Specifies VLAN subinterfaces that are created based on agent-circuit-identifier information

Mode Privileged Exec, User Exec

Related Documentation
- Monitoring VLAN Statistics on page 90

PART 4

Index

Index