



Junos[®] OS

Transport and Internet Protocols Feature Guide for Routing Devices



Modified: 2019-03-12

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos® OS Transport and Internet Protocols Feature Guide for Routing Devices
Copyright © 2019 Juniper Networks, Inc. All rights reserved.

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 <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xi
	Documentation and Release Notes	xi
	Using the Examples in This Manual	xi
	Merging a Full Example	xii
	Merging a Snippet	xii
	Documentation Conventions	xiii
	Documentation Feedback	xv
	Requesting Technical Support	xv
	Self-Help Online Tools and Resources	xvi
	Creating a Service Request with JTAC	xvi
Chapter 1	Understanding IP Support on Junos OS	17
	Junos OS Support for IPv4 Routing Protocols	17
	Junos OS Support for IPv6 Routing Protocols	18
Chapter 2	Configuring Path MTU Discovery	21
	Configuring Junos OS for Path MTU Discovery on Outgoing TCP Connections	21
	Configuring Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections	21
	Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections	22
	Configuring Junos OS for IPv6 Path MTU Discovery	22
	Configuring the Junos OS to Enable MTU Path Check for a Routing Instance on M Series Routers	23
	Enabling MTU Check for a Routing Instance	24
	Assigning an IP Address to an Interface in the Routing Instance	24
Chapter 3	Configuring ICMP Features	25
	Configuring Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages	25
	Configuring the Rate Limit for ICMPv4 Error Messages	25
	Configuring the Rate Limit for ICMPv6 Error Messages	26
	Configuring Junos OS to Ignore ICMP Source Quench Messages	26
	Configuring Junos OS to Disable Protocol Redirect Messages on the Router or Switch	27
	Configuring Junos OS to Disable the Routing Engine Response to Multicast Ping Packets	27

Chapter 4	Configuring Port Security	29
	System Settings	29
	Specifying the Physical Location of the Switch	29
	Modifying the Default Time Zone for a Router or Switch Running Junos OS	30
	Configuring Junos OS to Extend the Default Port Address Range	31
	Configuring Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets	32
	Configuring Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses	32
	Rebooting and Halting a Device	33
	Configuring Password Authentication for Console Access to PICs	34
	TCP Headers with SYN and FIN Flags Set	35
	Configuring Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set	35
Chapter 5	Configuring ARP and Neighbor Discovery Options	37
	Configuring Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses	37
	Configuring Passive ARP Learning for Backup VRRP Routers or Switches	37
	Configuring a Delay in Gratuitous ARP Requests	38
	Configuring a Gratuitous ARP Request When an Interface is Online	38
	Configuring the Purging of ARP Entries	38
	Adjusting the ARP Aging Timer	39
	Disabling MAC Address Learning of Neighbors Through ARP or Neighbor Discovery for IPv4 and IPv6 Neighbors	40
	Example: Configuring ARP Cache Protection	40
Chapter 6	Configuring TCP Options	49
	Configuring Junos OS to Disable TCP RFC 1323 Extensions	49
	Configuring Junos OS to Disable the TCP RFC 1323 PAWS Extension	49
	Configuring TCP MSS for Session Negotiation	50
	Configuring TCP MSS on T Series and M Series Routers, and MX Series Routers Using a Service Card	50
	Configuring TCP MSS Inline on MX Series Routers Using MPC Line Cards	51
	Configuring Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets	52
Chapter 7	Configuring IPv6 Features	55
	Configuring Junos OS for IPv6 Duplicate Address Detection Attempts	55
	Configuring Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit	55
	Configuring Junos OS to Enable Processing of IPv4-mapped IPv6 Addresses and 6PE Traceroutes	56
Chapter 8	Configuration Statements	57
	System Management Configuration Statements	58
	allow-6pe-traceroute	65
	allow-v4mapped-packets	66
	arp (Interfaces)	67
	arp-max-cache	70

arp-new-hold-limit	71
arp-system-cache-limit	72
auxiliary	73
console (System Ports)	74
default-address-selection	76
diag-port-authentication	77
extended-statistics	78
gratuitous-arp-delay	78
gratuitous-arp-on-ifup	79
gre-path-mtu-discovery	79
icmp (Error Message Rate Limit)	80
icmp6 (Error Message Rate Limit)	81
icmpv4-rate-limit	82
icmpv6-rate-limit	83
interfaces (ARP Aging Timer)	84
internet-options	85
ipip-path-mtu-discovery	86
ipv6-duplicate-addr-detection-transmits	87
ipv6-path-mtu-discovery	88
ipv6-path-mtu-discovery-timeout	88
ipv6-reject-zero-hop-limit	89
no-multicast-echo	89
non-subscriber-no-reply	90
no-ping-record-route	90
no-ping-time-stamp	91
no-redirects (IPv4 Traffic)	92
no-tcp-rfc1323-paws	93
no-tcp-rfc1323	93
passive-learning	94
purging	94
path-mtu-discovery	95
path-mtu-discovery (Tunnel)	96
source-quench	97
system	97
tcp-drop-synfin-set	98
tcp-mss	99
Chapter 9	
Operational Commands	101
clear arp	102
show arp	104
show system statistics arp	109
show system statistics icmp	116
show system statistics icmp6	121
show system statistics igmp	127
show system statistics ip	131
show system statistics ip6	139
show system statistics tcp	147

List of Figures

Chapter 4	Configuring Port Security	29
	Figure 1: TCP Header with SYN and FIN Flags Set	35
Chapter 5	Configuring ARP and Neighbor Discovery Options	37
	Figure 2: ARP Cache Protection	42

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xiii
	Table 2: Text and Syntax Conventions	xiv
Chapter 6	Configuring TCP Options	49
	Table 3: Source Address Selection	52
Chapter 9	Operational Commands	101
	Table 4: show arp Output Fields	106

About the Documentation

- Documentation and Release Notes on page xi
- Using the Examples in This Manual on page xi
- Documentation Conventions on page xiii
- Documentation Feedback on page xv
- Requesting Technical Support on page xv

Documentation and 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 <https://www.juniper.net/documentation/>.

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

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see [CLI Explorer](#).

Documentation Conventions

Table 1 on page xiii defines notice icons used in this guide.

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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xiv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	}

GUI Conventions

Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

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 Partner Support Service 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 <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- 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 <https://support.juniper.net/support/requesting-support/>.

CHAPTER 1

Understanding IP Support on Junos OS

- [Junos OS Support for IPv4 Routing Protocols on page 17](#)
- [Junos OS Support for IPv6 Routing Protocols on page 18](#)

Junos OS Support for IPv4 Routing Protocols

Junos OS implements full IP routing functionality, providing support for IP version 4 (IPv4). The routing protocols are fully interoperable with existing IP routing protocols, and they have been developed to provide the scale and control necessary for the Internet core.

Junos OS provides the following routing and Multiprotocol Label Switching (MPLS) applications protocols:

- Unicast routing protocols:
 - BGP—Border Gateway Protocol, version 4, is an exterior gateway protocol (EGP) that guarantees loop-free exchange of routing information between routing domains (also called autonomous systems). BGP, in conjunction with Junos routing policy, provides a system of administrative checks and balances that can be used to implement peering and transit agreements.
 - ICMP—Internet Control Message Protocol router discovery enables hosts to discover the addresses of operational routers on the subnet.
 - IS-IS—Intermediate System-to-Intermediate System is a link-state interior gateway protocol (IGP) for IP networks that uses the shortest-path-first (SPF) algorithm, which also is referred to as the Dijkstra algorithm, to determine routes. The Junos IS-IS software is a new and complete implementation of the protocol, addressing issues of scale, convergence, and resilience.
 - OSPF—Open Shortest Path First, version 2, is an IGP that was developed for IP networks by the Internet Engineering Task Force (IETF). OSPF is a link-state protocol that makes routing decisions based on the SPF algorithm. The Junos OSPF software is a new and complete implementation of the protocol, addressing issues of scale, convergence, and resilience.
 - RIP—Routing Information Protocol, version 2, is a distance-vector IGP for IP networks based on the Bellman-Ford algorithm. RIP dynamically routes packets between a subscriber and a service provider without the subscriber having to configure BGP or participate in the service provider's IGP discovery process.

- Multicast routing protocols:
 - DVMRP—Distance Vector Multicast Routing Protocol is a dense-mode (flood-and-prune) multicast routing protocol.
 - IGMP—Internet Group Management Protocol, versions 1 and 2, is used to manage membership in multicast groups.
 - MSDP—Multicast Source Discovery Protocol enables multiple Protocol Independent Multicast (PIM) sparse mode domains to be joined. A rendezvous point (RP) in a PIM sparse mode domain has a peer relationship with an RP in another domain, enabling it to discover multicast sources from other domains.
 - PIM sparse mode and dense mode—Protocol-Independent Multicast is a multicast routing protocol. PIM sparse mode routes to multicast groups that might span wide-area and interdomain internets. PIM dense mode is a flood-and-prune protocol.
 - SAP/SDP—Session Announcement Protocol and Session Description Protocol handle conference session announcements.
- MPLS applications protocols:
 - LDP—The Label Distribution Protocol provides a mechanism for distributing labels in non-traffic-engineered applications. LDP enables routers to establish label-switched paths (LSPs) through a network by mapping network layer routing information directly to data-link layer switched paths. LSPs created by LDP can also traverse LSPs created by the Resource Reservation Protocol (RSVP).
 - MPLS—Multiprotocol Label Switching, formerly known as tag switching, enables you to manually or dynamically configure LSPs through a network. It lets you direct traffic through particular paths rather than rely on the IGP's least-cost algorithm to choose a path.
 - RSVP—The Resource Reservation Protocol, version 1, provides a mechanism for engineering network traffic patterns that is independent of the shortest path decided upon by a routing protocol. RSVP itself is not a routing protocol; it operates with current and future unicast and multicast routing protocols. The primary purpose of the Junos RSVP software is to support dynamic signaling for MPLS LSPs.

**Related
Documentation**

- *Junos OS Overview*
- [Junos OS Support for IPv6 Routing Protocols on page 18](#)

Junos OS Support for IPv6 Routing Protocols

The Junos OS implements IP routing functionality, providing support for IP version 6 (IPv6). The routing protocols have been developed to provide the scale and control necessary for the Internet core.

The software supports the following unicast routing protocols:

- BGP—Border Gateway Protocol version 4, is an EGP that guarantees loop-free exchange of routing information between routing domains (also called autonomous systems). BGP, in conjunction with Junos routing policies, provides a system of administrative checks and balances that can be used to implement peering and transit agreements.
- ICMP—Internet Control Message Protocol router discovery enables hosts to discover the addresses of operational routers on the subnet.
- IS-IS—Intermediate System-to-Intermediate System is a link-state IGP for IP networks that uses the SPF algorithm, which also is referred to as the Dijkstra algorithm, to determine routes. The Junos OS supports a new and complete implementation of the protocol, addressing issues of scale, convergence, and resilience.
- OSPF version 3 (OSPFv3) supports IPv6. The fundamental mechanisms of OSPF such as flooding, designated router (DR) election, area-based topologies, and the SPF calculations remain unchanged. Some differences exist either because of changes in protocol semantics between IPv4 and IPv6, or because of the need to handle the increased address size of IPv6.
- RIP—Routing Information Protocol version 2 is a distance-vector IGP for IP networks based on the Bellman-Ford algorithm. RIP dynamically routes packets between a subscriber and a service provider without the subscriber having to configure BGP or to participate in the service provider's IGP discovery process.

**Related
Documentation**

- *Junos OS Overview*
- [Junos OS Support for IPv4 Routing Protocols on page 17](#)

CHAPTER 2

Configuring Path MTU Discovery

- [Configuring Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 21](#)
- [Configuring Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections on page 21](#)
- [Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 22](#)
- [Configuring Junos OS for IPv6 Path MTU Discovery on page 22](#)
- [Configuring the Junos OS to Enable MTU Path Check for a Routing Instance on M Series Routers on page 23](#)

Configuring Junos OS for Path MTU Discovery on Outgoing TCP Connections

By default, path MTU discovery on outgoing TCP connections is enabled. To disable path MTU discovery, include the **no-path-mtu-discovery** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]  
no-path-mtu-discovery;
```

To reenable path MTU discovery on outgoing TCP connections, include the **path-mtu-discovery** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]  
path-mtu-discovery;
```

Related Documentation

- [Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 22](#)
- [Configuring Junos OS to Ignore ICMP Source Quench Messages on page 26](#)

Configuring Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections

By default, path maximum transmission unit (MTU) discovery on outgoing IP-IP tunnel connections is enabled.

To disable IP-IP path MTU discovery, include the **no-ipip-path-mtu-discovery** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
no-ipip-path-mtu-discovery;
```

To reenable IP-IP path MTU discovery, include the **ipip-path-mtu-discovery** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
ipip-path-mtu-discovery;
```

**Related
Documentation**

- [Configuring Junos OS for IPv6 Path MTU Discovery on page 22](#)
- [Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 22](#)
- [Configuring Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 21](#)
- [ipip-path-mtu-discovery on page 86](#)

Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections

By default, path MTU discovery on outgoing GRE tunnel connections is enabled. To disable GRE path MTU discovery, include the **no-gre-path-mtu-discovery** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
no-gre-path-mtu-discovery;
```

To reenable GRE path MTU discovery, include the **gre-path-mtu-discovery** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
gre-path-mtu-discovery;
```



NOTE: To verify details of the path MTU on outgoing GRE tunnels use the command *show interfaces (GRE)*

**Related
Documentation**

- [Configuring Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 21](#)

Configuring Junos OS for IPv6 Path MTU Discovery

By default, path MTU (PMTU) discovery for IPv6 packets is enabled. To disable IPv6 PMTU discovery, include the **no-ipv6-path-mtu-discovery** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
no-ipv6-path-mtu-discovery;
```

To configure IPv6 PMTU discovery timeout in minutes, include the `ipv6-path-mtu-discovery-timeout` statement at the `[edit system internet-options]` hierarchy level:

```
[edit system internet-options]
ipv6-path-mtu-discovery-timeout minutes;
```

For details about IPv6 PMTU, see RFC 1981, *Path MTU Discovery for IP version 6*.

Related Documentation

- [Configuring Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections on page 21](#)
- [Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 22](#)
- [Configuring Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 21](#)

Configuring the Junos OS to Enable MTU Path Check for a Routing Instance on M Series Routers

By default, the maximum transmission unit (MTU) check for routing instance is disabled on M Series routers (except the M120 and M320 routers).



NOTE: The MTU check is automatically present for interfaces belonging to the main router.

On M Series routers (except the M120 and M320 routers) you can configure MTU path checks on the outgoing interface for unicast traffic routed on a virtual private network (VPN) routing and forwarding (VRF) routing instance. When you enable MTU check, the router sends an Internet Control Message Protocol (ICMP) message when the size of a unicast packet traversing a VRF routing instance or virtual-router routing instance has exceeded the MTU size and when an IP packet is set to "do not fragment". The ICMP message uses the routing instance local address as its source address.

For an MTU check to work in a routing instance, you must include the `vrf-mtu-check` statement at the `[edit chassis]` hierarchy level and assign at least one interface containing an IP address to the routing instance.

To configure path MTU checks, complete the following tasks:

1. [Enabling MTU Check for a Routing Instance on page 24](#)
2. [Assigning an IP Address to an Interface in the Routing Instance on page 24](#)

Enabling MTU Check for a Routing Instance

To enable MTU check for a routing instance, include the **vrf-mtu-check** statement at the **[edit chassis]** hierarchy level:

```
[edit chassis]
vrf-mtu-check;
```

Assigning an IP Address to an Interface in the Routing Instance

To assign an IP address to an interface in the VRF or virtual-router routing instance, configure the local address for that routing instance. A local address is any IP address derived from an interface that is assigned to the routing instance.

To assign an interface to a routing instance, include the **interface** statement at the **[edit routing-instances *routing-instance-name*]** hierarchy level:

```
[edit routing-instances routing-instance-name]
interface interface-name;
```

To configure an IP address for a loopback interface, include the **address** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet]** hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet]
address address;
```



NOTE: If you are assigning Internet Protocol Security (IPsec) or generic routing encapsulation (GRE) tunnel interfaces without IP addresses in the routing instance, include a loopback interface to the routing instance. To do this, include the **lo0.*n*** option at the **[edit routing-instances *routing-instance-name* interface]** hierarchy level. *n* cannot be 0, because lo0.0 is reserved for the main router (and not appropriate for use with routing instances). Also, an IP address must be assigned to this loopback interface in order to work. To set an IP address for a loopback interface, include the **address** statement at the **[edit interfaces lo0 unit *logical-unit-number* family inet]** hierarchy level.

See Also • [*vrf-mtu-check*](#)

CHAPTER 3

Configuring ICMP Features

- [Configuring Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 25](#)
- [Configuring the Rate Limit for ICMPv4 Error Messages on page 25](#)
- [Configuring the Rate Limit for ICMPv6 Error Messages on page 26](#)
- [Configuring Junos OS to Ignore ICMP Source Quench Messages on page 26](#)
- [Configuring Junos OS to Disable Protocol Redirect Messages on the Router or Switch on page 27](#)
- [Configuring Junos OS to Disable the Routing Engine Response to Multicast Ping Packets on page 27](#)

Configuring Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages

To limit the rate at which ICMPv6 messages are sent, include the **icmpv6-rate-limit** statement at the **[edit system internet-options]** hierarchy level:

```
icmpv6-rate-limit bucket-size bucket-size packet-rate packet-rate;
```

The bucket size is the the number of seconds in the rate-limiting bucket. The packet rate is the rate-limiting packets earned per second. Specify a **bucket-size** from 0 through 4294967295 seconds. The default value is 5 seconds. Specify a **packet-rate** from 0 through 4294967295. The default value is 1000.

Related Documentation

- [Rate Limiting ICMPv4 and ICMPv6 Traffic](#)

Configuring the Rate Limit for ICMPv4 Error Messages

By default, ICMP messages for IPv4 traffic errors are generated at the rate of 1 packet per second (pps).



NOTE: This statement applies only to ICMP error messages for non-ttl-expired IPv4 packets. It does not apply to ICMP error messages for ttl-expired IPv4 packets; for these errors, the rate is fixed at 50 pps.

Starting in Junos OS Release 19.1R1, the maximum rate increases to 1000 pps. In earlier releases, the maximum rate is 50 pps.

To configure this rate to any value from 1 pps through the maximum limit.

- Specify the rate.

```
[edit chassis]
user@host# set icmp rate-limit 10
```

Related Documentation

- [Configuring the Rate Limit for ICMPv6 Error Messages on page 26](#)

Configuring the Rate Limit for ICMPv6 Error Messages

By default, ICMP messages for IPv6 traffic errors are generated at the rate of 1 packet per second (pps).



NOTE: This statement applies only to ICMP error messages for non-ttl-expired IPv6 packets. It does not apply to ICMP error messages for ttl-expired IPv6 packets; for these errors, the rate is fixed at 50 pps.

Starting in Junos OS Release 19.1R1, the maximum rate increases to 1000 pps. In earlier releases, the maximum rate is 50 pps.

To configure this rate to any value from 1 through the maximum limit:

- Specify the rate.

```
[edit chassis]
user@host# set icmp6 rate-limit 10
```

Related Documentation

- [Configuring the Rate Limit for ICMPv4 Error Messages on page 25](#)

Configuring Junos OS to Ignore ICMP Source Quench Messages

By default, ignoring Internet Control Message Protocol (ICMP) source quench messages is disabled. To stop ignoring ICMP source quench messages, include the **source-quench** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
source-quench;
```

To disable ICMP source quench, include the **no-source-quench** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
no-source-quench;
```

**Related
Documentation**

- [Rate Limiting ICMPv4 and ICMPv6 Traffic](#)
- [Configuring Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 25](#)

Configuring Junos OS to Disable Protocol Redirect Messages on the Router or Switch

By default, the router or switch sends protocol redirect messages. To disable the sending of redirect messages by the router or switch, include the **no-redirects** statement at the **[edit system]** hierarchy level:

```
[edit system]
no-redirects;
```

To reenable the sending of redirect messages on the router or switch, delete the **no-redirects** statement from the configuration.

To disable the sending of redirect messages on a per-interface basis, include the **no-redirects** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family *family*]** hierarchy level.



NOTE: To make this change take effect, reboot the device.

**Related
Documentation**

- [Configuring Junos OS to Ignore ICMP Source Quench Messages on page 26](#)
- [Configuring Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets on page 52](#)
- [Junos OS Network Interfaces Library for Routing Devices](#)

Configuring Junos OS to Disable the Routing Engine Response to Multicast Ping Packets

By default, the Routing Engine responds to Internet Control Message Protocol (ICMP) echo requests sent to multicast group addresses. To disable the Routing Engine from responding to ICMP echo requests sent to multicast group addresses, include the **no-multicast-echo** statement at the **[edit system]** hierarchy level:

```
[edit system]
no-multicast-echo;
```

By configuring the Routing Engine to ignore multicast ping packets, you can prevent unauthorized persons from discovering the list of provider edge (PE) routers or switches in the network.

**Related
Documentation**

- [Configuring Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses on page 32](#)

CHAPTER 4

Configuring Port Security

- [System Settings on page 29](#)
- [Configuring Password Authentication for Console Access to PICs on page 34](#)
- [TCP Headers with SYN and FIN Flags Set on page 35](#)
- [Configuring Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set on page 35](#)

System Settings

- [Specifying the Physical Location of the Switch on page 29](#)
- [Modifying the Default Time Zone for a Router or Switch Running Junos OS on page 30](#)
- [Configuring Junos OS to Extend the Default Port Address Range on page 31](#)
- [Configuring Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets on page 32](#)
- [Configuring Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses on page 32](#)
- [Rebooting and Halting a Device on page 33](#)

Specifying the Physical Location of the Switch

To specify the physical location of the switch, specify the following options for the **location** statement at the **[edit system]** hierarchy level:

- **altitude *feet***—Number of feet above sea level.
- **building *name***—Name of the building, 1 to 28 characters in length. If the string contains spaces, enclose it in quotation marks (" ").
- **country-code *code***—Two-letter country code.
- **floor *number***—Floor in the building.
- **hcoord *horizontal-coordinate***—Bellcore Horizontal Coordinate.
- **lata *service-area***—Long-distance service area.
- **latitude *degrees***—Latitude in degree format.
- **longitude *degrees***—Longitude in degree format.

- **npa-nxx *number***—First six digits of the phone number (area code and exchange).
- **postal-code *postal-code***—Postal code.
- **rack *number***—Rack number.
- **vcoord *vertical-coordinate***—Bellcore Vertical Coordinate.

The following example shows how to specify the physical location of the switch:

```
[edit system]
location {
  altitude feet;
  building name;
  country-code code;
  floor number;
  hcoord horizontal-coordinate;
  lata service-area;
  latitude degrees;
  longitude degrees;
  npa-nxx number;
  postal-code postal-code;
  rack number;
  vcoord vertical-coordinate;
}
```

See Also • *Example: Configuring the Name of the Switch, IP Address, and System ID*

Modifying the Default Time Zone for a Router or Switch Running Junos OS

The default local time zone on the router or switch is UTC (Coordinated Universal Time, formerly known as Greenwich Mean Time, or GMT).

- To modify the local time zone, include the **time-zone** statement at the **[edit system]** hierarchy level:

```
[edit system]
time-zone (GMT hour-offset | time-zone);
```

You can use the **GMT *hour-offset*** option to set the time zone relative to UTC (GMT) time. By default, ***hour-offset*** is **0**. You can configure this to be a value from **-14** to **+12**.

You can also specify the ***time-zone*** value as a string such as PDT (Pacific Daylight Time) or WET (Western European Time), or specify the continent and major city.



NOTE: Junos OS complies with the POSIX time-zone standard, which is counter-intuitive to the way time zones are generally indicated relative to UTC. A time zone ahead of UTC (east of the Greenwich meridian) is commonly indicated as GMT +*n*; for example, the Central European Time (CET) zone is indicated as GMT +1. However, this is not true for POSIX time zone designations. POSIX indicates CET as GMT-1. If you include the `set system time-zone GMT+1` statement for a router in the CET zone, your router time will be set to one hour behind GMT, or two hours behind the actual CET time. For this reason, you might find it easier to use the POSIX time-zone strings, which you can list by entering `set system time-zone ?`.

For the time zone change to take effect for all processes running on the router or switch, you must reboot the router or switch.

The following example shows how to change the current time zone to **America/New_York**:

```
[edit]
user@host# set system time-zone America/New_York
[edit]
user@host# show
system {
    time-zone America/New_York;
}
```

- See Also**
- [Understanding NTP Time Servers](#)
 - [Updating the IANA Time Zone Database on Junos OS Devices](#)

Configuring Junos OS to Extend the Default Port Address Range

By default, the upper range of a port address is 5000. You can increase the range from which the port number can be selected to decrease the probability that someone can determine your port number.

- To configure Junos OS to extend the default port address range, include the **source-port** statement at the `[edit system internet-options]` hierarchy level:

```
[edit system internet-options]
source-port upper-limit upper-limit;
```

upper-limit *upper-limit* is the upper limit of a source port address and can be a value from 5000 through 65,355.

- See Also**
- [Configuring Junos OS to Disable TCP RFC 1323 Extensions on page 49](#)
 - [Configuring Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 37](#)
 - *source-port*

Configuring Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets

By default, the source address included in locally generated Transmission Control Protocol/IP (TCP/IP) packets, such as FTP traffic, and in User Datagram Protocol (UDP) and IP packets, such as Network Time Protocol (NTP) requests, is chosen as the local address for the interface on which the traffic is transmitted. This means that the local address chosen for packets to a particular destination might change from connection to connection based on the interface that the routing protocol has chosen to reach the destination when the connection is established. If multiple equal-cost next hops are present for a destination, locally generated packets use the **lo0** address as a source.

- To configure the software to select a fixed address to use as the source for locally generated IP packets, include the **default-address-selection** statement at the **[edit system]** hierarchy level:

```
[edit system]
default-address-selection;
```

If you include the **default-address-selection** statement in the configuration, the Junos OS chooses the system default address as the source for most locally generated IP packets. The default address is usually an address configured on the **lo0** loopback interface. For example, if you specified that SSH and telnet use a particular address, but you also have **default-address selection** configured, the system default address is used.

Configuring Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses

When you issue the **ping** command with the **record-route** option, the Routing Engine displays the path of the ICMP echo request packets and timestamps in the ICMP echo responses by default.

You can configure the Routing Engine to disable the setting of the **record-route** option in the IP header of the ping request packets. Disabling the **record-route** option prevents the Routing Engine from recording and displaying the path of the ICMP echo request packets in the response.

- To configure the Routing Engine to disable the setting of the **record route** option, include the **no-ping-record-route** statement at the **[edit system]** hierarchy level:

```
[edit system]
no-ping-record-route;
```

- To disable the reporting of timestamps in the ICMP echo responses, include the **no-ping-time-stamp** option at the **[edit system]** hierarchy level:

```
[edit system]
no-ping-time-stamp;
```

By configuring the **no-ping-record-route** and **no-ping-timestamp** options, you can prevent unauthorized persons from discovering information about the provider edge (PE) router or switch and its loopback address.

- See Also**
- [Configuring Junos OS to Disable the Routing Engine Response to Multicast Ping Packets on page 27](#)

Rebooting and Halting a Device

To reboot the switch, issue the **request system reboot** command.

```
user@switch> request system reboot ?
```

Possible completions:

<[Enter]>	Execute this command
all-members	Reboot all virtual chassis members
at	Time at which to perform the operation
both-routing-engines	Reboot both the Routing Engines
fast-boot	Enable fast reboot
hypervisor	Reboot Junos OS, host OS, and Hypervisor
in	Number of minutes to delay before operation
local	Reboot local virtual chassis member
member	Reboot specific virtual chassis member (0..9)
message	Message to display to all users
other-routing-engine	Reboot the other Routing Engine
	Pipe through a command

```
{master:0}
```

```
user@switch> request system reboot
```

```
Reboot the system ? [yes,no] (no) yes
Rebooting switch
```



NOTE: Not all options shown in the preceding command output are available on all QFX Series, OCX Series, and EX4600 switches. See the documentation for the *request system reboot* command for details about options.



NOTE: When you issue the *request system reboot hypervisor* command on QFX10000 switches, the reboot takes longer than a standard Junos OS reboot.

Similarly, to halt the switch, issue the **request system halt** command.



CAUTION: Before entering this command, you must have access to the switch's console port in order to bring up the Routing Engine.

```
user@switch> request system halt ?
```

Possible completions:

<[Enter]>	Execute this command
all-members	Halt all virtual chassis members
at	Time at which to perform the operation
backup-routing-engine	Halt backup Routing Engine
both-routing-engines	Halt both Routing Engines

<code>in</code>	Number of minutes to delay before operation
<code>local</code>	Halt local virtual chassis member
<code>member</code>	Halt specific virtual chassis member (0..9)
<code>message</code>	Message to display to all users
<code>other-routing-engine</code>	Halt other Routing Engine
<code> </code>	Pipe through a command



NOTE: When you issue this command on an individual component in a QFabric system, you will receive a warning that says “Hardware-based members will halt, Virtual Junos Routing Engines will reboot.” If you want to halt only one member, use the `member` option. You cannot issue this command from the QFabric CLI.

Issuing the **`request system halt`** command on the switch halts the Routing Engine. To reboot a Routing Engine that has been halted, you must connect through the console.

- See Also**
- *`clear system reboot`*
 - *`request system halt`*
 - *`request system power-off`*
 - *Connecting a QFX Series Device to a Management Console*

Configuring Password Authentication for Console Access to PICs

By default, there is no password setting for console access. To configure console access to the Physical Interface Cards (PICs), include the **`pic-console-authentication`** statement at the **`[edit system]`** hierarchy level:

```
[edit system]
pic-console-authentication {
  (encrypted-password "password" | plain-text-password);
}
```

encrypted-password "password"—Use Message Digest 5 (MD5) or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password.

You cannot configure a blank password for **encrypted-password** using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

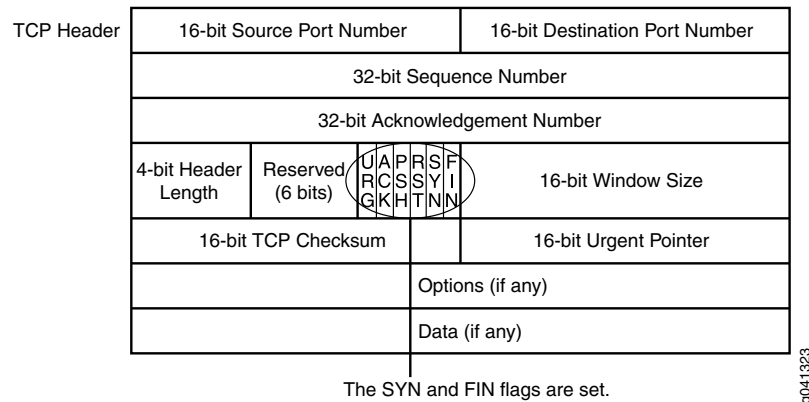
plain-text-password—Use a plain-text password. The command-line interface (CLI) prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password.

Related Documentation • [Configuring Junos OS to Set Console and Auxiliary Port Properties](#)

TCP Headers with SYN and FIN Flags Set

Both the SYN and FIN control flags are not normally set in the same TCP segment header. The SYN flag synchronizes sequence numbers to initiate a TCP connection. The FIN flag indicates the end of data transmission to finish a TCP connection. Their purposes are mutually exclusive. A TCP header with the SYN and FIN flags set is anomalous TCP behavior, causing various responses from the recipient, depending on the OS. See [Figure 1 on page 35](#).

Figure 1: TCP Header with SYN and FIN Flags Set



An attacker can send a segment with both flags set to see what kind of system reply is returned and thereby determine what kind of OS is on the receiving end. The attacker can then use any known system vulnerabilities for further attacks. When you enable the `tcp-drop-synfin-set` statement, Junos OS checks if the SYN and FIN flags are set in TCP headers. If it discovers such a header, it drops the packet.

Related Documentation • [tcp-drop-synfin-set on page 98](#)

Configuring Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set

By default, the router or switch accepts packets that have both the SYN and FIN bits set in the TCP flag. You can configure the router or switch to drop packets with both the SYN and FIN bits set. Accepting packets with the SYN and FIN bits set can result in security vulnerabilities, such as denial-of-service attacks. To configure the router or switch to drop such packets, include the `tcp-drop-synfin-set` statement at the `[edit system internet-options]` hierarchy level:

```
[edit system internet-options]
tcp-drop-synfin-set;
```

- Related Documentation**
- [Configuring Junos OS to Disable TCP RFC 1323 Extensions on page 49](#)
 - [Configuring Junos OS to Extend the Default Port Address Range on page 31](#)
[tcp-drop-synfin-set on page 98](#)

CHAPTER 5

Configuring ARP and Neighbor Discovery Options

- [Configuring Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 37](#)
- [Disabling MAC Address Learning of Neighbors Through ARP or Neighbor Discovery for IPv4 and IPv6 Neighbors on page 40](#)
- [Example: Configuring ARP Cache Protection on page 40](#)

Configuring Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses

The Address Resolution Protocol (ARP) is a protocol used by IPv4 to map IP network addresses to MAC addresses. This topic describes how to set passive ARP learning and ARP aging options for network devices. (A switch operates as a virtual router.)

Tasks for configuring ARP learning and aging are:

1. [Configuring Passive ARP Learning for Backup VRRP Routers or Switches on page 37](#)
2. [Configuring a Delay in Gratuitous ARP Requests on page 38](#)
3. [Configuring a Gratuitous ARP Request When an Interface is Online on page 38](#)
4. [Configuring the Purging of ARP Entries on page 38](#)
5. [Adjusting the ARP Aging Timer on page 39](#)

Configuring Passive ARP Learning for Backup VRRP Routers or Switches

By default, the backup VRRP router or switch drops ARP requests for the VRRP-IP to VRRP-MAC address translation. The backup router or switch does not learn the ARP (IP-to-MAC address) mappings for the hosts sending the requests. When it detects a failure of the master router or switch and becomes the new master, the backup router or switch must learn all the entries that were present in the ARP cache of the master router or switch. In environments with many directly attached hosts, such as metro Ethernet environments (this type of environment does not pertain to switches), the number of ARP entries to learn can be high. This can cause a significant transition delay, during which traffic transmitted to some of the hosts might be dropped.

Passive ARP learning enables the ARP cache in the backup router or switch to hold approximately the same contents as the ARP cache in the master router or switch, thus preventing the problem of learning ARP entries in a burst. To enable passive ARP learning, include the **passive-learning** statement at the **[edit system arp]** hierarchy level:

```
[edit system arp]  
passive-learning;
```

We recommend setting passive learning on both the backup and master VRRP routers or switches. This prevents the need to intervene manually when the master router or switch becomes the backup router or switch. While a router or switch is operating as the master, the passive learning configuration has no operational impact. The master (or a standalone) router always learns ARP entries from incoming requests. The configuration takes effect only when the router or switch is operating as a backup router or switch.

Configuring a Delay in Gratuitous ARP Requests

By default, the Junos OS sends gratuitous ARP requests immediately after network-related configuration changes are made on an interface, for example, a VLAN ID, MAC address, or IP address change. This might lead to the Packet Forwarding Engine dropping some initial request packets if the IP address configuration updates have not been fully processed. To avoid such request packets from being dropped, you can configure a delay in gratuitous ARP requests.

To configure a delay in gratuitous ARP requests, include the **gratuitous-arp-delay seconds** statement at the **[edit system arp]** hierarchy level:

```
[edit system arp]  
gratuitous-arp-delay seconds;
```

We recommend that you configure a value in the range of 3 through 6 seconds.

Configuring a Gratuitous ARP Request When an Interface is Online

To configure the Junos OS to automatically send a gratuitous ARP request when an interface is online, include the **gratuitous-arp-on-ifup** statement at the **[edit system arp]** hierarchy level:

```
[edit system arp]  
gratuitous-arp-on-ifup;
```

Configuring the Purging of ARP Entries

To configure the purging of obsolete ARP entries in the cache when an interface goes offline, include the **purging** statement at the **[edit system arp]** hierarchy level:

```
[edit system arp]  
purging;
```



NOTE: Purging is configured to delete ARP entries immediately after an interface that has gone offline is detected. If purging is not configured, ARP entries in the ARP table are retried after they have expired and are deleted if there is no ARP response within the default timeout value of 20 minutes. The default timeout value can be configured to other values using the `aging-timer` statement.

Adjusting the ARP Aging Timer

By default, the ARP aging timer is set at 20 minutes. In environments with many directly attached hosts, such as metro Ethernet environments, increasing the amount of time between ARP updates by configuring the ARP aging timer can improve performance in an event where having thousands of clients time out at the same time might impact packet forwarding performance. In environments where there are devices connected with lower ARP aging timers (less than 20 minutes), decreasing the ARP aging timer can improve performance by preventing the flooding of traffic toward next hops with expired ARP entries. In most environments, the default ARP aging timer value does not need to be adjusted.

The range of the ARP aging timer is from 1 through 240 minutes.

To configure a system-wide ARP aging timer, include the **aging-timer** statement at the **[edit system arp]** hierarchy level:

```
[edit system arp]
aging-timer minutes;
```

You can also configure the ARP aging timer for each logical interface of family type **inet**. To configure the ARP aging timer at the logical interface level, specify the **aging-timer** statement and the timer value in minutes at the **[edit system arp interfaces interface-name]** hierarchy level:

```
[edit system arp interfaces interface-name]
aging-timer minutes;
```

To configure the ARP aging timer for a specific interface in a logical system, include the **aging-timer** statement and the timer value in minutes at the **[edit logical-systems logical-system-name system arp interfaces interface-name]** hierarchy level:

```
[edit logical-systems logical-system-name system arp interfaces interface-name]
aging-timer minutes;
```



NOTE: If the aging timer value is configured both at the system and the logical interface levels, the value configured at the logical interface level takes precedence for the specific logical interface.

The timer value you configure takes effect as ARP entries expire. Each refreshed ARP entry receives the new timer value. The new timer value does not apply to ARP entries that exist at the time you commit the configuration.

- Related Documentation**
- [Disabling MAC Address Learning of Neighbors Through ARP or Neighbor Discovery for IPv4 and IPv6 Neighbors on page 40](#)

Disabling MAC Address Learning of Neighbors Through ARP or Neighbor Discovery for IPv4 and IPv6 Neighbors

The Junos OS provides the **no-neighbor-learn** configuration statement at the **[edit interfaces *interface-name* unit *interface-unit-number* family inet]** and **[edit interfaces *interface-name* unit *interface-unit-number* family inet6]** hierarchy levels.

To disable ARP address learning by not sending arp-requests and not learning from ARP replies for IPv4 neighbors, include the **no-neighbor-learn** statement at the **[edit interfaces *interface-name* unit *interface-unit-number* family inet]** hierarchy level:

```
[edit interfaces interface-name unit interface-unit-number family inet]
no-neighbor-learn;
```

To disable neighbor discovery for IPv6 neighbors, include the **no-neighbor-learn** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet6]** hierarchy level:

```
[edit interfaces interface-name unit interface-unit-number family inet6]
no-neighbor-learn;
```

- Related Documentation**
- *no-neighbor-learn*
 - [Configuring Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 37](#)
 - *Ethernet Interfaces Feature Guide for Routing Devices*

Example: Configuring ARP Cache Protection

Starting in Junos OS Release 16.1, you can configure an ARP cache limit for resolved and unresolved next-hop entries in the cache. This example shows how to configure ARP cache protection by specifying a maximum count and hold limit for resolved and unresolved next-hop entries in the ARP cache. This limit can be specified globally for all interfaces, or locally on a particular interface of the device. The benefit of configuring such a limit on the ARP cache is to protect the device from denial-of-service (DoS) attacks.

- [Requirements on page 41](#)
- [Overview on page 41](#)
- [Configuration on page 43](#)

- [Verification on page 45](#)
- [Troubleshooting on page 46](#)

Requirements

This example uses the following hardware and software components:

- Two routers that can be a combination of M, MX, and T Series routers.
- Two host devices connected to the routers.
- Junos OS Release 16.1 or later running on the routers.

Overview

Sending IP packets on a multiaccess network requires mapping from an IP address to a media access control (MAC) address (the physical or hardware address). In an Ethernet environment, ARP is used to map a MAC address to an IP address. Hosts that use ARP maintain a cache of discovered Internet-to-Ethernet address mappings to minimize the number of ARP broadcast messages.

To keep the cache from growing too large, by default, an entry is removed from the cache if it is not used within a certain period of time. In addition to this, starting in Junos OS Release 16.1, you can manage the number of ARP cache entries by configuring a limit on the resolved and unresolved next-hop entries.

The ARP cache feature supports two types of limits:

- **Count**—Count limit is the maximum number of next hops that can be created in the ARP cache.
- **Hold**—Hold limit is the maximum number of hold routes pointing to a particular interface that can be retained before getting added to the ARP cache.

The ARP cache limits are executed at two levels:

- **Local**—Local limits are configured per interface and are defined for resolved and unresolved entries in the ARP cache.
- **Global**—Global limits apply system-wide. A global limit is further defined separately for the public interfaces and management interfaces, for example, fxp0. The management interface has a single global limit and no local limit. The global limit enforces a system-wide cap on entries for the ARP cache, including private Internal routing interfaces (IRIs) for internal routing instances, for example, em0 and em1.

Small-sized platforms: ACX, EX22XX, EX3200, EX33XX, and SRX; default is 20,000.
Medium-sized platforms: EX4200, EX45XX, EX4300, EX62XX, and MX; default is 75,000.
All other platforms, default is 100,000. You can modify this limit by configuring the ARP next-hop cache protection feature.

- To configure the ARP cache count limit for resolved and unresolved next-hop entries globally, include the **arp-system-cache-limit** statement at the **[edit system]** hierarchy level.

- To configure the ARP cache count limit for resolved and unresolved next-hop entries locally, include the **arp-system-cache-limit** statement at the **[edit interfaces interface-name unit interface-unit-number family inet]** hierarchy level.
- To configure the ARP cache hold limit for unresolved next-hop entries locally, include the **arp-new-hold-limit** statement at the **[edit interfaces interface-name unit interface-unit-number family inet]** hierarchy level.



NOTE: The ARP cache hold limit is configured on a per-interface basis only, and cannot be configured at the system level.

The ARP cache next-hop entries get allotted to different types of interfaces differently, irrespective of the ARP cache protection feature configuration.

1. By default, 200 entries get allotted to IRIs.
2. 80 percent of the remaining entries get allotted to public interfaces.
3. 20 percent of the remaining entries get allotted to management interfaces.

When the ARP next-hop entries exceed the configured count limit, new entries are either discarded, or kept under the hold counter, if a hold limit is configured for that interface. The ARP next-hop hold limit specifies the maximum number of hold entries or hold routes that point to a particular interface. When the number of hold entries exceeds the configured hold limit, the drop counter for that interface is affected drastically, as the new hold entries create a loop and continue to increment until there is bandwidth to accommodate them.

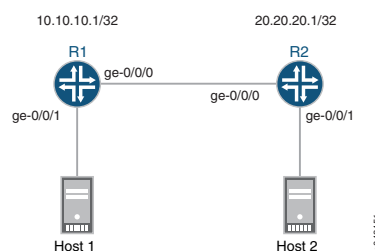


NOTE: After modifying the default ARP next-hop cache limit on an interface, the interface must be deactivated and reactivated for the newly configured values to take effect.

Topology

Figure 2 on page 42 illustrates a simple two-router topology with ARP cache protection enabled. Routers R1 and R2 are each connected to hosts, Host1 and Host2, respectively.

Figure 2: ARP Cache Protection



For example, if Router R1 is configured with an **arp-system-cache-limit** of 220 globally, and it receives 230 ARP entries, on the first interface receiving the entries (say, ge-0/0/0), the following actions are performed:

1. When 230 entries are received, the global limit of 220 entries is applied to the system, where the configured limit is divided among the different types of interfaces, and the remaining entries received on a particular interface get discarded.
2. Out of the 220 cached entries, by default, 200 entries are allocated for IRI interfaces.
3. Out of the remaining 20 entries, 80 percent of the entries (16 entries) are sent to public interfaces and 20 percent of the entries (4 entries) are sent to the management interface. If the 230 ARP entries are received on the public interface, only the cache limit of 16 entries is retained, and the remaining 214 entries get discarded.

In addition, if ge-0/0/0 on Router R1 is configured with an **arp-new-hold-limit** value of 8, the following actions are performed:

1. Out of the 230 received entries, only 220 entries are cached in the ARP table. However, instead of discarding the remaining entries, the hold entries are sent to the hold counter of ge-0/0/0, and then the remaining entries are sent to the drop counter of ge-0/0/0.
2. Depending on availability of bandwidth, the eight hold entries are cached in the ARP table of ge-0/0/0 before taking any newly received entries into account.
3. The drop counter of ge-0/0/0, however, does not increment by single entries. The discarded hold entries in the drop counter form a loop and add to the entries count until there is bandwidth on the interface to accommodate all the entries. Therefore, additions to the drop counter have a drastic effect on the interface performance.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
R1
set interfaces ge-0/0/0 unit 0 family inet address 1.1.1/30
set interfaces ge-0/0/0 unit 0 family inet arp-new-hold-limit 8
set interfaces ge-0/0/1 unit 0 family inet address 2.2.2/30
set interfaces lo0 unit 0 family inet address 10.10.10/32
set system arp-system-cache-limit 220

R2
set interfaces ge-0/0/0 unit 0 family inet address 1.1.2/30
set interfaces ge-0/0/1 unit 0 family inet address 3.3.3/30
set interfaces lo0 unit 0 family inet address 20.20.20/32
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode*.

To configure Router R1 with ARP cache protection:

1. Configure the interfaces of Router R1.

```
[edit interfaces]
user@R1# set ge-0/0/0 unit 0 family inet address 1.1.1.1/30
user@R1# set ge-0/0/1 unit 0 family inet address 2.2.2.1/30
user@R1# set lo0 unit 0 family inet address 10.10.10.1/32
```

2. Configure ARP cache protection globally for all the interfaces of Router R1.

```
[edit system]
user@R1# set arp-system-cache-limit 220
```

3. Configure a hold limit on the ARP cache entries of interface ge-0/0/0 of Router R1.

```
[edit interfaces]
user@R1# set ge-0/0/0 unit 0 family inet arp-new-hold-limit 8
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces** and **show system** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@R1# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet {
      address 1.1.1.1/30;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family inet {
      address 2.2.2.1/30;
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.10.10.1/32;
    }
  }
}
```

```
}
```

```
user@R1# show system
arp-system-cache-limit 220 ;
```

Verification

Confirm that the configuration is working properly.

- [Verifying Global ARP Next-Hop Cache Limit on page 45](#)
- [Verifying Local ARP Next-Hop Cache Limit on page 45](#)

Verifying Global ARP Next-Hop Cache Limit

Purpose Verify the system-wide ARP next-hop cache limits and the allocation of next-hop entries for different interfaces.

Action From operational mode, run the **show system statistics arp** command.

```
user@R1> show system statistics arp
```

```
arp:
    717253 datagrams received
    47 ARP requests received
    31 ARP replies received
    285 resolution request received
    0 unrestricted proxy requests
    0 restricted proxy requests
    0 received proxy requests
    0 unrestricted proxy requests not proxied
*****
    220 Max System ARP nh cache limit
    16 Max Public ARP nh cache limit
    200 Max IRI ARP nh cache limit
    4 Max Management intf ARP nh cache limit
    16 Current Public ARP next-hops present
    1 Current IRI ARP next-hops present
    2 Current Management ARP next-hops present
    2457 Total ARP next-hops creation failed as limit reached
    2454 Public ARP next-hops creation failed as public limit reached
    3 IRI ARP next-hops creation failed as iri limit reached
    0 Management ARP next-hops creation failed as mgt limit reached
```

Meaning The global ARP next-hop cache limits are displayed in the output, along with the allocation of next-hop entries for IRI, public, and management interfaces.

Verifying Local ARP Next-Hop Cache Limit

Purpose Verify the interface ARP next-hop cache limit.

Action From operational mode, run the **show interfaces *interface-name*** command.

```
user@R1> show interface fxp0

fxp0
Physical interface: fxp0, Enabled, Physical link is Up
  Interface index: 1, SNMP ifIndex: 1
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 100mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Full-Duplex
  Current address: 00:a0:a5:62:8e:39, Hardware address: 00:a0:a5:62:8e:39
  Last flapped   : 2014-10-16 10:23:29 PDT (16:27:21 ago)
    Input packets : 0
    Output packets: 0

Logical interface fxp0.0 (Index 3) (SNMP ifIndex 13)
  Flags: Up SNMP-Traps Encapsulation: ENET2
  Bandwidth: 0
  Input packets : 23
  Output packets: 4
  Protocol inet, MTU: 1500
  Max nh cache: 220 New hold nh limit: 8, Curr nh cnt: 2, Curr new hold cnt: 0,
  NH drop cnt: 0
  Flags: Sendbcst-pkt-to-re, Is-Primary
  Addresses, Flags: Is-Default Is-Preferred Is-Primary
    Destination: 10.209.0/18, Local: 10.209.3.69, Broadcast: 10.209.63.255
```

Meaning The local ARP next-hop cache count and hold limits for the management interface is displayed in the output.

Troubleshooting

To troubleshoot the ARP cache protection configuration, see:

- [Troubleshooting System Log Messages on page 46](#)

[Troubleshooting System Log Messages](#)

Problem System log messages are generated to record events when the ARP cache limits are exceeded.

Solution To interpret the system log messages, refer to the following:

- **Feb 08 17:12:39 [TRACE] [R1]: Public intf soft (80%) arp nh cache limit reached**—Router R1 has reached 80 percent of the allowed ARP next-hop cache limit for public interfaces.
- **Feb 08 17:07:43 [TRACE] [R1]: Public intf hard arp nh cache limit reached**—Router R1 has reached the maximum allowed limit for ARP next-hop cache entries on the public interface.

- **Feb 08 17:15:14 [TRACE] [R1]: Max cache soft (80%) arp nh cache limit for intf idx 325 reached**—Router R1 has reached 80 percent of the configured global ARP next-hop cache limit for all its interfaces.
- **Feb 08 17:19:41 [TRACE] [R1]: Max cache hard arp nh cache limit for intf idx 325 reached**—Router R1 has reached the maximum configured global ARP next-hop cache limit for all its interfaces.

Release History Table

Release	Description
16.1	Starting in Junos OS Release 16.1, you can configure an ARP cache limit for resolved and unresolved next-hop entries in the cache.

Related Documentation

- [arp-system-cache-limit on page 72](#)
- [arp-new-hold-limit on page 71](#)

CHAPTER 6

Configuring TCP Options

- [Configuring Junos OS to Disable TCP RFC 1323 Extensions on page 49](#)
- [Configuring Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 49](#)
- [Configuring TCP MSS for Session Negotiation on page 50](#)
- [Configuring Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets on page 52](#)

Configuring Junos OS to Disable TCP RFC 1323 Extensions

To disable RFC 1323 TCP extensions, include the **no-tcp-rfc1323** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
no-tcp-rfc1323;
```

Related Documentation

- [Configuring Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 49](#)
- [Configuring Junos OS to Extend the Default Port Address Range on page 31](#)
- [no-tcp-rfc1323-paws on page 93](#)

Configuring Junos OS to Disable the TCP RFC 1323 PAWS Extension

To configure the Junos OS to disable Protection Against Wrapped Sequence (PAWS) number extension (described in RFC 1323, *TCP Extensions for High Performance*), include the **no-tcp-rfc1323-paws** statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
no-tcp-rfc1323-paws;
```

Related Documentation

- [Configuring Junos OS to Disable TCP RFC 1323 Extensions on page 49](#)
- [Configuring Junos OS to Extend the Default Port Address Range on page 31](#)
- [no-tcp-rfc1323 on page 93](#)

Configuring TCP MSS for Session Negotiation

During session connection establishment, two peers agree in negotiations to determine the IP segment size of packets that they will exchange during their communication. The TCP MSS (maximum segment size) value in TCP SYN packets specifies the maximum number of bytes that a TCP packet's data field, or segment, can contain. An MSS value that is set too high can result in an IP datagram that is too large to send and that must be fragmented. Fragmentation can incur additional overhead cost and packet loss.

To diminish the likelihood of fragmentation and to protect against packet loss, you can use the **tcp-mss** statement to specify a lower TCP MSS value. The **tcp-mss** statement applies to all IPv4 TCP SYN packets traversing all the router's ingress interfaces whose MSS value is higher than the one you specify. You cannot exempt particular ports from its effects.

The following section describes how to configure TCP MSS on T Series, M Series, and MX Series routers:

1. [Configuring TCP MSS on T Series and M Series Routers, and MX Series Routers Using a Service Card on page 50](#)
2. [Configuring TCP MSS Inline on MX Series Routers Using MPC Line Cards on page 51](#)

Configuring TCP MSS on T Series and M Series Routers, and MX Series Routers Using a Service Card

To specify a TCP MSS value on T Series and M Series routers as well as MX Series routers using a service card, include the **tcp-mss** statement at the **[edit services service-set service-set-name]** hierarchy level:

```
[edit services]
service-set service-set-name {
  tcp-mss mss-value;
  stateful-firewall-rules rule-name;
  interface-service {
    service-interface sp-fpc/pic/port;
  }
}
stateful-firewall {
  rule rule-name {
    match-direction input-output;
    term 1 {
      then {
        accept;
      }
    }
  }
}
```

The range of the **tcp-mss mss-value** parameter is from 536 through 65535 bytes.

Add the service set to any interface for which you want to adjust the TCP-MSS value:

```
[edit interfaces interface-name]
unit 0 {
  family inet | inet6 {
    service {
      input {
        service-set service-set-name;
      }
      output {
        service-set service-set-name;
      }
    }
    address ip-address;
  }
}
```

To view statistics of SYN packets received and SYN packets whose MSS value is modified, issue the **show services service-sets statistics tcp-mss** operational mode command.

For further information about configuring TCP MSS on T Series and M Series routers, see the *Junos OS Services Interfaces Library for Routing Devices*.

Configuring TCP MSS Inline on MX Series Routers Using MPC Line Cards

To specify a TCP MSS value on MX Series routers that use MPC line cards, include the **tcp-mss** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family *family*]** hierarchy level:

```
[edit interfaces]
interfaces interface-name {
  unit 0 {
    family inet | inet6 {
      tcp-mss {
        mss-value;
      }
    }
  }
}
```

The range of the *mss-value* parameter is from 64 through 65,535 bytes.

The TCP MSS value must be lower than the MTU of the interface.

This statement is supported on the following interfaces: gr- (GRE), ge- (Gigabit Ethernet), xe- (10-Gigabit Ethernet), and et- (40-Gigabit and 100-Gigabit Ethernet). Families supported are **inet** and **inet6**.



NOTE: Configuring TCP MSS inline on MX Series routers using MPC line cards works only for traffic exiting/egressing the interface, not traffic entering/ingressing the interface.

- Related Documentation**
- [Configuring Junos OS to Disable TCP RFC 1323 Extensions on page 49](#)
 - [Configuring Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 49](#)

Configuring Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets

Locally generated IP packets are the packets that are produced by applications running on the Routing Engine. Junos OS chooses a source address for these packets so that the application peers can respond. It also enables you to specify the source address on a per application basis. To serve this purpose, the Telnet CLI command contains the **source-address** argument.

This section introduces the **default-address-selection** statement:

```
[edit system]
default-address-selection;
```

If you specifically choose the source address, as in the case of Telnet, **default-address-selection** does not influence the source address selection. The source address becomes the one that is specified with the **source-address** argument (provided the address is a valid address specified on the interface of a router). If the source address is not specified or if the specified address is invalid, **default-address-selection** influences the default source address selection.

If the source address is not explicitly specified as in the case of Telnet, then by default (when **default-address-selection** is not specified) the source address chosen for locally generated IP packets is the IP address of the outgoing interface. This indicates that depending on the chosen outgoing interface, the source address might be different for different invocations of a given application.

If the interface is unnumbered (no IP address is specified on an interface), Junos OS uses a predictable algorithm to determine the default source address. If **default-address-selection** is specified, Junos OS uses the algorithm to choose the source address irrespective of whether the outgoing interface is numbered. This indicates that with **default-address-selection**, you can influence Junos OS to provide the same source address in locally generated IP packets regardless of the outgoing interface.

The behavior of source address selection by Junos OS can be summed up as shown in the following table:

Table 3: Source Address Selection

Outgoing Interface	When default-address-selection Is Specified	When default-address-selection Is Not Specified
Unnumbered	Use default-address-selection	Use default-address-selection
Numbered	Use default-address-selection	Use IP address of outgoing interface

See *Configuring Default, Primary, and Preferred Addresses and Interfaces* for more information about the default address source selection algorithm.



NOTE: For IP packets sent by IP routing protocols (including OSPF, RIP, RSVP, and the multicast protocols, but not including IS-IS), the local address selection is often constrained by the protocol specification so that the protocol operates correctly. When this constraint exists in the routing protocol, the packet's source address is unaffected by the presence of the `default-address-selection` statement in the configuration. For protocols in which the local address is unconstrained by the protocol specification, for example, IBGP and multihop EBGP, if you do not configure a specific local address when configuring the protocol, the local address is chosen using the same method as other locally generated IP packets.

**Related
Documentation**

- [Configuring Junos OS to Disable Protocol Redirect Messages on the Router or Switch on page 27](#)
- [default-address-selection on page 76](#)

CHAPTER 7

Configuring IPv6 Features

- [Configuring Junos OS for IPv6 Duplicate Address Detection Attempts on page 55](#)
- [Configuring Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit on page 55](#)
- [Configuring Junos OS to Enable Processing of IPv4-mapped IPv6 Addresses and 6PE Traceroutes on page 56](#)

Configuring Junos OS for IPv6 Duplicate Address Detection Attempts

The `ipv6-duplicate-addr-detection-transmits` statement at the `[edit system internet-options]` hierarchy level controls the number of attempts for IPv6 duplicate address detection. The default value is 3.

Related Documentation

- [Junos OS Support for IPv6 Routing Protocols on page 18](#)
- [Configuring the Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit on page 55](#)
- [Configuring the Junos OS for IPv6 Path MTU Discovery on page 22](#)

Configuring Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit

The `ipv6-reject-zero-hop-limit` and `no-ipv6-reject-zero-hop-limit` statements are used to enable and disable rejection of incoming IPv6 packets that have a zero hop limit value in their header.

By default, such packets are rejected both when they are addressed to the local host and when they are transiting the router or switch. To accept zero hop-limit packets addressed to the local host, include the `no-ipv6-reject-zero-hop-limit` statement at the `[edit system internet-options]` hierarchy level. Transit packets are still dropped.

```
[edit system internet-options]  
no-ipv6-reject-zero-hop-limit;
```

Related Documentation

- [Configuring the Junos OS for IPv6 Path MTU Discovery on page 22](#)
- [Configuring the Junos OS for IPv6 Duplicate Address Detection Attempts on page 55](#)

Configuring Junos OS to Enable Processing of IPv4-mapped IPv6 Addresses and 6PE Traceroutes

By default, the Junos OS disables the processing of IPv4-mapped IPv6 packets to protect against malicious packets from entering the network. This might result in IPv6 packets from being dropped in a pure IPv4 routing environment. In a mixed routing environment of IPv4 and IPv6 networks, you might want to enable the processing of IPv4-mapped IPv6 packets to ensure smooth packet flow. In addition, this might also be helpful when you are in the process of transitioning your routing environment from IPv4 to IPv6 networks.

To enable the processing of such IPv4-mapped IPv6 packets, include the **allow-v4mapped-packets** statement at the **[edit system]** hierarchy level:

```
[edit system]
allow-v4mapped-packets;
```



NOTE: We recommend that you configure this statement only after fully understanding the security implications of allowing IPv4-mapped IPv6 packets in your network.

In a dual-stack IPv6 network connected over an IPv4 MPLS network, the P routers in the IPv4 MPLS backbone do not have an IPv6 family. Consequently, the transit P routers are not shown in the output when you do an IPv6 traceroute. To generate an ICMPv6 echo request and a TTL expired response packet to and from the intermediate transit routers in the 6PE network, include the **allow-6pe-traceroute** statement at the **[edit system]** hierarchy level:

```
[edit system]
allow-6pe-traceroute;
```

- Related Documentation
- [allow-v4mapped-packets on page 66](#)
 - [allow-6pe-traceroute on page 65](#)

CHAPTER 8

Configuration Statements

- [System Management Configuration Statements on page 58](#)
- [allow-6pe-traceroute on page 65](#)
- [allow-v4mapped-packets on page 66](#)
- [arp \(Interfaces\) on page 67](#)
- [arp-max-cache on page 70](#)
- [arp-new-hold-limit on page 71](#)
- [arp-system-cache-limit on page 72](#)
- [auxiliary on page 73](#)
- [console \(System Ports\) on page 74](#)
- [default-address-selection on page 76](#)
- [diag-port-authentication on page 77](#)
- [extended-statistics on page 78](#)
- [gratuitous-arp-delay on page 78](#)
- [gratuitous-arp-on-ifup on page 79](#)
- [gre-path-mtu-discovery on page 79](#)
- [icmp \(Error Message Rate Limit\) on page 80](#)
- [icmp6 \(Error Message Rate Limit\) on page 81](#)
- [icmpv4-rate-limit on page 82](#)
- [icmpv6-rate-limit on page 83](#)
- [interfaces \(ARP Aging Timer\) on page 84](#)
- [internet-options on page 85](#)
- [ipip-path-mtu-discovery on page 86](#)
- [ipv6-duplicate-addr-detection-transmits on page 87](#)
- [ipv6-path-mtu-discovery on page 88](#)
- [ipv6-path-mtu-discovery-timeout on page 88](#)
- [ipv6-reject-zero-hop-limit on page 89](#)
- [no-multicast-echo on page 89](#)
- [non-subscriber-no-reply on page 90](#)

- [no-ping-record-route](#) on page 90
- [no-ping-time-stamp](#) on page 91
- [no-redirects \(IPv4 Traffic\)](#) on page 92
- [no-tcp-rfc1323-paws](#) on page 93
- [no-tcp-rfc1323](#) on page 93
- [passive-learning](#) on page 94
- [purging](#) on page 94
- [path-mtu-discovery](#) on page 95
- [path-mtu-discovery \(Tunnel\)](#) on page 96
- [source-quench](#) on page 97
- [system](#) on page 97
- [tcp-drop-synfin-set](#) on page 98
- [tcp-mss](#) on page 99

System Management Configuration Statements

This topic lists all the configuration statements that you can include at the **[edit system]** hierarchy level to configure system management features:

```
system {
  accounting {
    destination {
      radius {
        server {
          server-address {
            accounting-port port-number;
            retry number;
            secret password;
            source-address address;
            timeout seconds;
          }
        }
      }
    }
    tacplus {
      server {
        server-address {
          port port-number;
          secret password;
          single-connection;
          timeout seconds;
        }
      }
    }
  }
  enhanced-avs-max;
  events [ login change-log interactive-commands ];
}
archival {
```

```

configuration {
  archive-sites {
    ftp://<username>:<password>@<host>:<port>/<url-path>;
    ftp://<username>:<password>@<host>:<port>/<url-path>;
  }
  transfer-interval interval;
  transfer-on-commit;
}
allow-v4mapped-packets;
arp {
  aging-timer minutes;
  gratuitous-arp-delay;
  gratuitous-arp-on-ifup;
  interfaces;
  passive-learning;
  purging;
}
authentication-order [ authentication-methods ];
backup-router address <destination destination-address>;
commit {
  delta-export;
  fast-synchronize;
  persist-groups-inheritance ;
  server;
  synchronize
}
synchronize;
(compress-configuration-files | no-compress-configuration-files);
default-address-selection;
dump-device (compact-flash | remove-compact | usb);
diag-port-authentication (encrypted-password "password" | plain-text-password);
dynamic-profile-options {
  versioning;
}
domain-name domain-name;
domain-search [ domain-list ];
fips {
  level level;
}
host-name hostname;
inet6-backup-router address <destination destination-address>;
internet-options {
  tcp-mss mss-value;
  (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
  icmpv4-rate-limit bucket-size bucket-size packet-rate packet-rate;
  icmpv6-rate-limit bucket-size bucket-size packet-rate packet-rate;
  (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
  (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
  ipv6-path-mtu-discovery-timeout;
  no-tcp-rfc1323-paws;
  no-tcp-rfc1323;
  (path-mtu-discovery | no-path-mtu-discovery);
  source-port upper-limit <upper-limit>;
  (source-quench | no-source-quench);
}

```

```

tcp-drop-synfin-set;
}
location {
  altitude feet;
  building name;
  country-code code;
  floor number;
  hcoord horizontal-coordinate;
  lata service-area;
  latitude degrees;
  longitude degrees;
  npa-nxx number;
  postal-code postal-code;
  rack number;
  vcoord vertical-coordinate;
}
login {
  announcement text;
  class class-name {
    access-end;
    access-start;
    allow-commands "regular-expression";
    ( allow-configuration | allow-configuration-regexps ) "regular expression 1" "regular expression 2";
    allowed-days;
    deny-commands "regular-expression";
    ( deny-configuration | deny-configuration-regexps ) "regular expression 1" "regular expression 2";
    idle-timeout minutes;
    login-script;
    login-tip;
    permissions [ permissions ];
  }
  message text;
  password {
    change-type (set-transitions | character-set);
    format (md5 | sha1 | des);
    maximum-length length;
    minimum-changes number;
    minimum-length length;
  }
  retry-options {
    backoff-threshold number;
    backoff-factor seconds;
    minimum-time seconds;
    tries-before-disconnect number;
  }
  user username {
    full-name complete-name;
    uid uid-value;
    class class-name;
    authentication {
      (encrypted-password "password" | plain-text-password);
      ssh-rsa "public-key";
      ssh-dsa "public-key";
    }
  }
}

```

```

    }
  }
}
login-tip number;
mirror-flash-on-disk;
name-server {
  address;
}
no-multicast-echo;
no-redirects;
no-ping-record-route;
no-ping-time-stamp;
ntp {
  authentication-key key-number type type value password;
  boot-server address;
  broadcast <address> <key key-number> <version value> <ttl value>;
  broadcast-client;
  multicast-client <address>;
  peer address <key key-number> <version value> <prefer>;
  source-address source-address;
  server address <key key-number> <version value> <prefer>;
  trusted-key [ key-numbers ];
}
ports {
  auxiliary {
    type terminal-type;
  }
  pic-console-authentication {
    encrypted-password encrypted-password;
    plain-text-password;
    console {
      insecure;
      log-out-on-disconnect;
      type terminal-type;
      disable;
    }
  }
}
processes {
  process--name (enable | disable) failover (alternate-media | other-routing-engine);
  timeout seconds;
}
}
radius-server server-address {
  accounting-port port-number;
  port port-number;
  retry number;
  secret password;
  source-address source-address;
  timeout seconds;
}
radius-options {
  enhanced-accounting
  password-protocol mschap-v2;
}
attributes {

```

```

    nas-ip-address ip-address;
  }
  enhanced-accounting;
  password-protocol mschap-v2;
}
root-authentication {
  (encrypted-password "password" | plain-text-password);
  ssh-rsa "public-key";
  ssh-dsa "public-key";
}
(saved-core-context | no-saved-core-context);
saved-core-files saved-core-files;
scripts {
  commit {
    allow-transients;
    file filename {
      optional;
      refresh;
      refresh-from url;
      source url;
    }
    traceoptions {
      file <filename> <files number> <size size> <world-readable | no-world-readable>;
      flag flag;
      no-remote-trace;
    }
  }
  op {
    file filename {
      arguments {
        argument-name {
          description descriptive-text;
        }
      }
      command filename-alias;
      description descriptive-text;
      refresh;
      refresh-from url;
      source url;
    }
    refresh;
    refresh-from url;
    traceoptions {
      file <filename> <files number> <size size> <world-readable | no-world-readable>;
      flag flag;
      no-remote-trace;
    }
  }
}
}
services {
  finger {
    connection-limit limit;
    rate-limit limit;
  }
  flow-tap-dtcp {
    ssh {

```

```

        connection-limit limit;
        rate-limit limit;
    }
}
ftp {
    connection-limit limit;
    rate-limit limit;
}
rest {
    control {
        allowed-sources [ value-list ];
        connection-limit limit;
    }
    enable-explorer;
    http {
        addresses [ addresses ];
        port port-number;
    }
    https {
        addresses [ addresses ];
        cipher-list [ cipher-1 cipher-2 cipher-3 ... ];
        mutual-authentication {
            certificate-authority certificate-authority-profile-name;
        }
        port port-number;
        server-certificate local-certificate-identifier;
    }
    traceoptions {
        flag flag;
    }
}
service-deployment {
    servers server-address {
        port port-number;
    }
    source-address source-address;
}
ssh {
    root-login (allow | deny | deny-password);
    protocol-version [v1 v2];
    connection-limit limit;
    rate-limit limit;
}
telnet {
    connection-limit limit;
    rate-limit limit;
}
web-management {
    http {
        interfaces [ interface-names ];
        port port;
    }
    https {
        interfaces [ interface-names ];
        local-certificate name;
    }
}

```

```

    port port;
  }
  session {
    idle-timeout [ minutes ];
    session-limit [ session-limit ];
  }
}
xnm-clear-text {
  connection-limit limit;
  rate-limit limit;
}
xnm-ssl {
  connection-limit limit;
  local-certificate name;
  rate-limit limit;
}
}
static-host-mapping {
  hostname {
    alias [ alias ];
    inet [ address ];
    sysid system-identifier;
  }
}
syslog {
  archive <files number> <size size> <world-readable | no-world-readable>;
  console {
    facility severity;
  }
  file filename {
    facility severity;
    archive <archive-sites {ftp-url <password password>}> <files number> <size size>
      <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
      no-world-readable>;
    explicit-priority;
    match "regular-expression";
    match-string string-name;
    structured-data {
      brief;
    }
  }
}
host (hostname | other-routing-engine | scc-master) {
  facility severity;
  explicit-priority;
  facility-override facility;
  log-prefix string;
  match "regular-expression";
  source-address source-address;
  structured-data {
    brief;
  }
}
source-address source-address;
time-format (year | millisecond | year millisecond);
user (username | *) {

```



```

    facility severity;
    match "regular-expression";
  }
}
tacplus-options {
  enhanced-accounting;
  service-name service-name;
  (no-cmd-attribute-value | exclude-cmd-attribute);
}
tacplus-server server-address {
  secret password;
  single-connection;
  source-address source-address;
  timeout seconds;
}
time-zone (GMT hour-offset | time-zone);
}
tracing {
  destination-override {
    syslog host;
  }
}
use-imported-time-zones;
}

```

allow-6pe-traceroute

Syntax	allow-6pe-traceroute;
Hierarchy Level	[edit system]
Description	<p>Allow IPv4-mapped IPv6 source addresses in an ICMPv6 echo request TTL expired packets.</p> <p>In a dual-stack IPv6 network connected over an IPv4 MPLS network, the P routers in the IPv4 MPLS backbone do not have an IPv6 family. Consequently, the transit P routers are not shown in the output when you do an IPv6 traceroute. To generate an ICMPv6 echo request and a TTL expired response packet to and from the intermediate transit routers in the 6PE network, you must configure this statement along with the allow-v4-mapped statement.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Junos OS to Enable Processing of IPv4-mapped IPv6 Addresses and 6PE Traceroutes on page 56 • allow-v4mapped-packets on page 66

allow-v4mapped-packets

Syntax	allow-v4mapped-packets;
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Enable the processing of IPv4-mapped IPv6 packets.
Options	None Default: IPv4-mapped IPv6 address processing is disabled.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Junos OS to Enable Processing of IPv4-mapped IPv6 Addresses and 6PE Traceroutes on page 56• allow-6pe-traceroute on page 65

arp (Interfaces)

Syntax `arp ip-address (mac | multicast-mac) mac-address publish;`

```
arp {
  aging-timer minutes;
  gratuitous-arp-delay seconds;
  gratuitous-arp-on-ifup;
  interfaces {
    interface-name {
      aging-timer minutes;
    }
  }
  passive-learning;
  purging;
}
```

Syntax (EX Series) `arp {
 aging-timer minutes;
}`

Hierarchy Level [edit [system](#)]

[edit interfaces *interface-name* unit *logical-unit-number* family inet address *address*],

[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet address *address*]



NOTE: The edit logical-systems hierarchy is not available on QFabric systems.

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description For Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces only, configure Address Resolution Protocol (ARP) table entries, mapping IP addresses to MAC addresses. You can enable backup VRRP routers to learn ARP requests for VRRP-IP to VRRP-MAC address translation. You can also set the time interval between ARP updates.



NOTE: By default, an ARP policer is installed that is shared among all the Ethernet interfaces on which you have configured the family inet statement. By including the arp statement at the [edit interfaces *interface-name* unit

logical-unit-number family inet policer] hierarchy level, you can apply a specific ARP-packet policer to an interface. This feature is not available on EX Series switches.

When you need to conserve IP addresses, you can configure an Ethernet interface to be unnumbered by including the `unnumbered-address` statement at the [edit interfaces *interface-name* unit *logical-unit-number* family inet] hierarchy level.



NOTE: For EX-Series switches, set only the time interval between ARP updates.

Options **ip-address**—IP address to map to the MAC address. The IP address specified must be part of the subnet defined in the enclosing **address** statement.

mac mac-address—MAC address to map to the IP address. Specify the MAC address as six hexadecimal bytes in one of the following formats: *nnnn.nnnn.nnnn* or *nn:nn:nn:nn:nn:nn*. For example, **0000.5e00.5355** or **00:00:5e:00:53:55**.

multicast-mac mac-address—Multicast MAC address to map to the IP address. Specify the multicast MAC address as six hexadecimal bytes in one of the following formats: *nnnn.nnnn.nnnn* or *nn:nn:nn:nn:nn:nn*. For example, **0000.5e00.5355** or **00:00:5e:00:53:55**.

publish—(Optional) Have the router or switch reply to ARP requests for the specified IP address. If you omit this option, the router or switch uses the entry to reach the destination but does not reply to ARP requests.




NOTE: For unicast MAC addresses only, if you include the **publish** option, the router or switch replies to proxy ARP requests.

aging-timer—Time interval in minutes between ARP updates. In environments where the number of ARP entries to update is high (for example, on routers only, metro Ethernet environments), increasing the time between updates can improve system performance.

passive-learning (QFX-Series only)—Configure backup VRRP routers or switches to learn the ARP mappings (IP-to-MAC address) for hosts sending the requests. By default, the backup VRRP router drops these requests; therefore, if the master router fails, the backup router must learn all entries present in the ARP cache of the master router. Configuring passive learning reduces transition delay when the backup router is activated.

Required Privilege Level	interface—To view this statement in the configuration.
	interface-control—To add this statement to the configuration.
	system—To view this statement in the configuration.
	system-control—To add this statement to the configuration.
Related Documentation	• <i>Configuring Static ARP Table Entries For Mapping IP Addresses to MAC Addresses</i>
	• Configuring Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 37
	• <i>Junos OS Network Interfaces Library for Routing Devices</i>
	• Junos OS System Basics Configuration Guide .

arp-max-cache

Syntax	<code>arp-max-cache <i>arp-max-cache</i>;</code>
Hierarchy Level	<code>[edit interfaces <i>name</i> unit <i>name</i> family inet]</code>
Release Information	Statement introduced in Junos OS Release 16.1.
Description	The ARP cache limit for resolved next hops can be configured at an interface level. The benefit of configuring the ARP cache limit is to protect the device from DoS attacks.
	<div>  <p>NOTE: After modifying the default ARP next-hop cache limit on an interface, you must deactivate and then reactivate the interface for the newly configured values to take effect.</p> </div>
Options	<p><i>arp-max-cache</i>—Indicates the maximum number of routes to be held in the ARP cache.</p> <p>Default: (ACX Series routers, EX2200, EX2200-C, EX3200, and EX3300 switches, SRX Series services gateways) 20,000 (EX4200, EX4300, EX4500, EX4550, and EX6210 switches, MX Series routers) 75,000 (Other platforms) 100,000</p> <p>Range: 1 through 2,000,000</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring ARP Cache Protection on page 40 • arp (Interfaces) on page 67 • arp on page 67 • arp-inspection (MX Series) • arp-new-hold-limit on page 71 • arp-system-cache-limit on page 72

arp-new-hold-limit

Syntax	<code>arp-new-hold-limit <i>arp-new-hold-limit</i>;</code>
Hierarchy Level	[edit interfaces <i>name</i> unit <i>name</i> family inet]
Release Information	Statement introduced in Junos OS Release 16.1.
Description	The ARP cache limit for unresolved next hops can be configured at an interface level. The benefit of configuring the ARP cache limit is to protect the device from DoS attacks.
Options	<p><i>arp-new-hold-limit</i>—Indicates the new or maximum routes to be held, before getting added to the ARP cache.</p> <p>Default: (ACX Series routers, EX2200, EX2200-C, EX3200, and EX3300 switches, SRX Series services gateways) 20,000 (EX4200, EX4300, EX4500, EX4550, and EX6210 switches, MX Series routers) 75,000 (Other platforms) 100,000</p> <p>Range: 1 through 2,000,000</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring ARP Cache Protection on page 40 • arp on page 67 • <i>arp-inspection (MX Series)</i> • arp-system-cache-limit on page 72 • arp-max-cache on page 70

arp-system-cache-limit

Syntax	<code>arp-system-cache-limit <i>number</i>;</code>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 16.1.
Description	Specify the ARP cache next-hop limit at the system (global) level to restrict the number of next-hop routes. To configure the limit at the interface level, use the arp-max-cache statement.
Default	The default behavior of ARP is to remove the cache entry if it is not used within a certain period of time, and not to allow the cache to grow too large. You can also manage the number of ARP cache next-hop entries by configuring a limit to the maximum number of next hops that can be created.
Options	<i>number</i> —Indicates the maximum number of routes to be held in the ARP cache. Range: 1 through 2,000,000 Default: (ACX Series routers, EX2200, EX2200-C, EX3200, and EX3300 switches, SRX Series services gateways) 20,000 (EX4200, EX4300, EX4500, EX4550, and EX6210 switches, MX Series routers) 75,000 (Other platforms) 100,000
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring ARP Cache Protection on page 40• arp (Interfaces) on page 67• arp on page 67• arp-inspection (MX Series)• arp-max-cache on page 70• arp-new-hold-limit on page 71

auxiliary

Syntax	<pre> auxiliary { disable; insecure; type <i>terminal-type</i>; port-type (mini-usb rj45); } </pre>
Hierarchy Level	[edit system ports]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	<p>Configure the characteristics of the auxiliary port.</p> <p>Remaining statement is explained separately.</p>
Default	disable is the default option.
Options	<p>disable—Disable the port.</p> <p>insecure—Disable super user access or root logins to establish terminal connection.</p> <p>type <i>terminal-type</i>—Type of terminal that is connected to the port.</p> <p>Range: ansi, vt100, small-xterm, xterm</p> <p>Default: The terminal type is unknown, and the user is prompted for the terminal type. The remaining statement is explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> <i>Configuring Junos OS to Set Console and Auxiliary Port Properties</i>

console (System Ports)

Syntax	<pre>console { authentication-order [<i>authentication-methods</i>]; disable; insecure; log-out-on-disconnect; type <i>terminal-type</i>; }</pre>
Hierarchy Level	[edit system ports]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>disable option added in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>authentication-order option added in Junos OS Release 12.2R3.</p>
Description	Configure the characteristics of the console port.
Default	The console port is enabled and its speed is 9600 baud.
Options	<p>authentication-order Specify the order in which the authentication methods such as password (for local password authentication), radius (for RADIUS server authentication), or tacplus (for TACACS+ server authentication) should be attempted.</p> <p>authentication-methods—One or more authentication methods, listed in the order in which they should be tried. The method can be one or more of the following:</p> <ul style="list-style-type: none"> • password—Use the password configured for the user with the authentication statement at the [edit system login user] hierarchy level. • radius—Use RADIUS authentication services. • tacplus—Use TACACS+ authentication services. <p>disable—Disable console login connections.</p> <p>insecure—Disable root login connections to the console and auxiliary ports. Configuring the console port as insecure also prevents superusers and anyone with a user identifier (UID) of 0 from establishing terminal connections in multiuser mode. This option can be used to prevent a user from attempting password recovery by booting into single-user mode, if the user does not know the root password.</p> <p>log-out-on-disconnect—Log out the session when the data carrier on the console port is lost.</p>



NOTE:

- The log-out-on-disconnect option is not operational on MX80 routers. On MX80 routers you must manually log out from the console with the request system logout u0 command.
- The log-out-on-disconnect option is not operational on guest network functions (GNFs), which are managed using Juniper Device Manager (JDM). You must use the exit command to log out from the GNF console. For more information, see [Junos Node Slicing feature guide](#).

type *terminal-type*—Type of terminal that is connected to the port.

Range: ansi, vt100, small-xterm, xterm

Default: The terminal type is unknown, and the user is prompted for the terminal type.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.


Related Documentation

- *Configuring Junos OS to Set Console and Auxiliary Port Properties*
- *Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication*

default-address-selection

Syntax	default-address-selection;
Hierarchy Level	[edit system]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Use the loopback interface, lo0 , as the source address for all locally generated IP packets when the packet is sent through a routed interface, and also when the packet is sent through a local interface such as fxp0 . The lo0 interface is the interface to the router's or switch's Routing Engine.
Default	<p>The default address is used as the source address for all locally generated IP packets on outgoing interfaces that are unnumbered. If an outgoing interface is numbered, the default address is chosen using the following sequence:</p> <ul style="list-style-type: none"> • The primary address on the loopback interface lo0 that is <i>not</i> 127.0.0.1 is used. • The primary address for the primary interface or the preferred address (if configured) for the primary interface is used. <p>By default, the primary address on an interface is selected as the numerically lowest local address configured on the interface.</p> <p>An interface's <i>primary address</i> is used by default as the local address for broadcast and multicast packets sourced locally and sent out through the interface. An interface's <i>preferred address</i> is the default local address used for packets sourced by the local router or switch to destinations on the subnet. By default, the numerically lowest local address configured for the interface is chosen as the preferred address on the subnet.</p> <p>To configure a different primary address or preferred address, include the primary or preferred statement at the [edit interfaces interface-name unit logical-unit-number family family address address or [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address address hierarchy levels.</p> <p>For more information about default, primary, and preferred addresses for an interface, see “Configuring Default, Primary, and Preferred Addresses and Interfaces” in the <i>Junos OS Network Interfaces Library for Routing Devices</i>.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets on page 52 • <i>Junos OS Network Interfaces Library for Routing Devices</i>

diag-port-authentication

Syntax	<code>diag-port-authentication (encrypted-password "<i>password</i>" plain-text-password);</code>
Hierarchy Level	[edit system]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure a password for performing diagnostics on the router's System Control Board (SCB), System and Switch Board (SSB), Switching and Forwarding Module (SFM), or Forwarding Engine Board (FEB) port.</p> <p>For routers that have more than one SSB, the same password is used for both SSBs.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> NOTE: Do not run diagnostics on the SCB, SSB, SFM, or FEB unless you have been instructed to do so by Customer Support personnel.</p> </div>
Default	No password is configured on the diagnostics port.
Options	<p>encrypted-password <i>password</i>—Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.</p> <p>You cannot configure a blank password for encrypted-password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.</p> <p>plain-text-password—Use a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password for each user.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	

extended-statistics

Syntax	extended-statistics;
Hierarchy Level	[edit chassis]
Release Information	Statement introduced in Junos OS Release 12.3.
Description	(MX Series routers only) Enable accounting of system statistics for IPv4 and IPv6 traffic.
Default	Accounting of system statistics is disabled.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>show system statistics</i>

gratuitous-arp-delay

Syntax	gratuitous-arp-delay;
Hierarchy Level	[edit system arp]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Configure a delay for gratuitous ARP requests at the system level. By default, Junos OS sends gratuitous ARP requests immediately after network-related configuration changes are made on an interface, for example, a VLAN ID, MAC address, or IP address change. This might lead to the Packet Forwarding Engine dropping some initial request packets if the configuration updates have not been fully processed. To avoid such request packets from being dropped, you can configure a delay in gratuitous ARP requests.
Options	seconds —Configure the ARP request delay in seconds. We recommend configuring a value in the range of 3 through 6 seconds.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 37


gratuitous-arp-on-ifup

Syntax	gratuitous-arp-on-ifup;
Hierarchy Level	[edit system arp]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Add this statement to the [edit system arp] hierarchy to configure Junos OS to automatically issue a gratuitous ARP announcement when an interface is online.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 37


gre-path-mtu-discovery

Syntax	(gre-path-mtu-discovery no-gre-path-mtu-discovery);
Hierarchy Level	[edit system internet-options]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure path MTU discovery for outgoing GRE tunnel connections: <ul style="list-style-type: none"> • gre-path-mtu-discovery—Path MTU discovery is enabled. • no-gre-path-mtu-discovery—Path MTU discovery is disabled.
Default	Path MTU discovery is enabled.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 22

icmp (Error Message Rate Limit)

Syntax	<pre>icmp { rate-limit <i>rate-limit</i>; }</pre>
Hierarchy Level	[edit chassis]
Release Information	Statement introduced in Junos OS Release 16.1.
Description	Configure the rate at which ICMP messages are generated for IPv4 packet errors for non-ttl-expired packets. <div> NOTE: This statement does not apply to ICMP messages for ttl-expired packets; for these errors, the rate is fixed at 50 pps.</div>
Options	<p>rate-limit <i>rate-limit</i>—Rate in packets per second (pps). Starting in Junos OS Release 18.4R1, the maximum rate is 1000 pps. In earlier releases, the maximum rate is 50 pps.</p> <p>Range: 1 through 1000</p> <p>Default: 1</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Rate Limit for ICMPv4 Error Messages on page 25

icmp6 (Error Message Rate Limit)

Syntax	<pre>icmp6 { rate-limit <i>rate-limit</i>; }</pre>
Hierarchy Level	[edit chassis]
Release Information	Statement introduced in Junos OS Release 16.1.
Description	Configure the rate at which ICMP messages are generated for IPv6 packet errors for non-ttl-expired packets.
	<div>  <p>NOTE: This statement does not apply to ICMP messages for ttl-expired packets; for these errors, the rate is fixed at 50 pps.</p> </div>
Options	<p>rate-limit <i>rate-limit</i>—Rate in packets per second (pps). Starting in Junos OS Release 18.4R1, the maximum rate is 1000 pps. In earlier releases, the maximum rate is 50 pps.</p> <p>Range: 1 through 1000</p> <p>Default: 1</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring the Rate Limit for ICMPv6 Error Messages on page 26

icmpv4-rate-limit

Syntax	<pre>icmpv4-rate-limit { bucket-size <i>seconds</i>; packet-rate <i>pps</i>; }</pre>
Hierarchy Level	[edit system internet-options]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure rate-limiting parameters for ICMPv4 messages sent.
Options	<p>bucket-size <i>seconds</i>—Number of seconds in the rate-limiting bucket. Range: 0 through 4294967295 seconds Default: 5</p> <p>packet-rate <i>pps</i>—Rate-limiting packets earned per second. Range: 0 through 4294967295 pps Default: 1000</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Rate Limiting ICMPv4 and ICMPv6 Traffic</i>

icmpv6-rate-limit

Syntax	<pre>icmpv6-rate-limit { bucket-size <i>seconds</i>; packet-rate <i>packet-rate</i>; }</pre>
Hierarchy Level	[edit system internet-options]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Configure rate-limiting parameters for ICMPv6 messages sent.
Options	<p>bucket-size <i>seconds</i>—Number of seconds in the rate-limiting bucket. Range: 0 through 4294967295 seconds Default: 5</p> <p>packet-rate <i>pps</i>—Rate-limiting packets earned per second. Range: 0 through 4294967295 pps Default: 1000</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 25

interfaces (ARP Aging Timer)

Syntax	<pre>interfaces { <i>interface-name</i> { aging-timer <i>minutes</i>; } }</pre>
Hierarchy Level	[edit system arp] [edit logical-systems <i>logical-system-name</i> system arp]
Release Information	Statement introduced in Junos OS Release 9.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the ARP aging timer in minutes for a logical interface of family type inet .
Options	aging-timer <i>minutes</i> —Time between ARP updates, in minutes. Default: 20 Range: 1 through 6,00,000
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Adjusting the ARP Aging Timer on page 39

internet-options

Syntax

```
internet-options {
  (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
  icmpv4-rate-limit bucket-size bucket-size packet-rate packet-rate;
  icmpv6-rate-limit bucket-size bucket-size packet-rate packet-rate;
  (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
  ipv6-duplicate-addr-detection-transmits;
  (ipv6-reject-zero-hop-limit | no-ipv6-reject-zero-hop-limit);
  (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
  ipv6-path-mtu-discovery-timeout;
  no-tcp-reset
  no-tcp-rfc1323;
  no-tcp-rfc1323-paws;
  (path-mtu-discovery | no-path-mtu-discovery);
  source-port upper-limit <upper-limit>;
  (source-quench | no-source-quench);
  tcp-drop-synfin-set;
  tcp-mss mss-value;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for SRX Series devices.

Description Configure system IP options to protect against certain types of DoS attacks.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages](#)
- [Configuring Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 25](#)
- [Configuring Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections on page 21](#)
- [Configuring Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 22](#)
- [Configuring Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 21](#)
- [Configuring Junos OS for IPv6 Duplicate Address Detection Attempts on page 55](#)
- [Configuring Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit on page 55](#)

- [Configuring Junos OS to Ignore ICMP Source Quench Messages on page 26](#)
- [Configuring Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set on page 35](#)
- [Configuring Junos OS to Disable TCP RFC 1323 Extensions on page 49](#)
- [Configuring Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 49](#)
- [Configuring Junos OS to Extend the Default Port Address Range on page 31](#)
- [Configuring TCP MSS for Session Negotiation on page 50](#)

ipip-path-mtu-discovery

Syntax	(<code>ipip-path-mtu-discovery</code> <code>no-ipip-path-mtu-discovery</code>);
Hierarchy Level	[<code>edit system internet-options</code>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure path MTU discovery for outgoing IP-IP tunnel connections: <ul style="list-style-type: none">• <code>ipip-path-mtu-discovery</code>—Path MTU discovery is enabled.• <code>no-ipip-path-mtu-discovery</code>—Path MTU discovery is disabled.
Default	Path MTU discovery is enabled.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections on page 21• internet-options on page 85

ipv6-duplicate-addr-detection-transmits

Syntax	ipv6-duplicate-addr-detection-transmits;
Hierarchy Level	[edit system internet-options]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Control the number of attempts for IPv6 duplicate address detection. The range of values supported for ipv6-duplicate-addr-detection-transmits is from 0 to 20.
Default	The default value is 3.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Junos OS for IPv6 Duplicate Address Detection Attempts on page 55

ipv6-path-mtu-discovery

Syntax	(ipv6-path-mtu-discovery no-ipv6-path-mtu-discovery);
Hierarchy Level	[edit system internet-options]
Release Information	Statement introduced in Junos OS Release 9.2. Statement introduced in Junos OS Release 9.2 for EX Series switches.
Description	Configure path MTU discovery for IPv6 packets: <ul style="list-style-type: none">• ipv6-path-mtu-discovery—IPv6 path MTU discovery is enabled.• no-ipv6-path-mtu-discovery—IPv6 path MTU discovery is disabled.
Default	IPv6 path MTU discovery is enabled.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Junos OS for IPv6 Path MTU Discovery on page 22

ipv6-path-mtu-discovery-timeout

Syntax	ipv6-path-mtu-discovery-timeout <i>minutes</i> ;
Hierarchy Level	[edit system internet-options]
Release Information	Statement introduced in Junos OS Release 9.2. Statement introduced in Junos OS Release 9.2 for EX Series switches.
Description	Set the IPv6 path MTU discovery timeout interval.
Options	minutes —IPv6 path MTU discovery timeout. Default: 10 minutes
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Junos OS for IPv6 Path MTU Discovery on page 22

ipv6-reject-zero-hop-limit

Syntax	(ipv6-reject-zero-hop-limit no-ipv6-reject-zero-hop-limit);
Hierarchy Level	[edit system internet-options]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Enable and disable rejecting incoming IPv6 packets with a zero hop limit value in their header.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit on page 55

no-multicast-echo

Syntax	no-multicast-echo
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 8.1.
Description	Disable the Routing Engine from responding to ICMP echo requests sent to multicast group addresses.
Default	The Routing Engine responds to ICMP echo requests sent to multicast group addresses.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Junos OS to Disable the Routing Engine Response to Multicast Ping Packets on page 27

non-subscriber-no-reply

Syntax	non-subscriber-no-reply;
Hierarchy Level	[edit system arp]
Release Information	Statement introduced in Junos OS Release 13.3R9 for the MX Series.
Description	Enable this option to drop ARP requests from non-subscribers when a user route is dynamically added for a subscriber. Configuring this statement suppresses the ARP response from the kernel when there is an ARP request for a loopback interface from static DHCP subscribers using a common LAN segment between two devices. However, this configuration might not be effective if the subscriber configuration has suppressed either a destination Layer 2 route or an access Layer 3 route.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• gratuitous-arp-delay on page 78• interfaces on page 84

no-ping-record-route

Syntax	no-ping-record-route;
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 9.4. Statement introduced in Junos OS Release 9.4 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the Junos OS to disable the reporting of the IP address in ping responses.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses on page 32

no-ping-time-stamp

Syntax	no-ping-time-stamp;
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 9.4. Statement introduced in Junos OS Release 9.4 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the Junos OS to disable the recording of timestamps in ping responses.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses on page 32

no-redirects (IPv4 Traffic)

Syntax	no-redirects;
Hierarchy Level	[edit system], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 12.3 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<p>Stop protocol redirect messages for IPv4 traffic from being sent on the entire switch or on an interface on the router or switch.</p> <p>To disable the sending of protocol redirect messages for the entire router or switch, include the no-redirects statement at the [edit system] hierarchy level.</p> <p>To disable the sending of protocol redirect messages on a specific interface, include the no-redirects statement at the [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>] hierarchy level.</p>
Default	The router or switch sends redirect messages.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Junos OS to Disable Protocol Redirect Messages on the Router or Switch on page 27 • <i>Understanding the Protocol Redirect Mechanism on Switches</i> • <i>Configuring Junos OS to Disable Sending Protocol Redirect Messages on Switches (CLI Procedure)</i> • <i>Junos OS Network Interfaces Library for Routing Devices</i>

no-tcp-rfc1323-paws

Syntax	no-tcp-rfc1323-paws;
Hierarchy Level	[edit system internet-options]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the Junos OS to disable the RFC 1323 Protection Against Wrapped Sequence (PAWS) number extension.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 49

no-tcp-rfc1323

Syntax	no-tcp-rfc1323;
Hierarchy Level	[edit system internet-options]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the Junos OS to disable RFC 1323 TCP extensions.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Junos OS to Disable TCP RFC 1323 Extensions on page 49

passive-learning

Syntax	passive-learning;
Hierarchy Level	[edit system arp]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure backup VRRP routers or switches to learn the ARP mappings (IP-to-MAC address) for hosts sending the requests.
Default	Learning of ARP mappings (IP-to-MAC address) by backup VRRP routers or switches for hosts sending the requests is disabled unless this statement is configured.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 37


purging

Syntax	purging;
Hierarchy Level	[edit system arp]
Release Information	Statement introduced in Junos OS Release 9.6. Statement introduced in Junos OS Release 9.6 for EX Series switches.
Description	Purge obsolete ARP entries from the cache when an interface or link goes offline.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 37

path-mtu-discovery

Syntax	(path-mtu-discovery no-path-mtu-discovery);
Hierarchy Level	[edit system internet-options]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure path MTU discovery for outgoing Transmission Control Protocol (TCP) connections: <ul style="list-style-type: none">• path-mtu-discovery—Path MTU discovery is enabled.• no-path-mtu-discovery—Path MTU discovery is disabled.
Default	Path MTU discovery is enabled.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 21

path-mtu-discovery (Tunnel)

Syntax	(path-mtu-discovery no-path-mtu-discovery);
Hierarchy Level	[edit interfaces ip-fpc/pic/port unit logical-unit-number tunnel] [edit interfaces gr-fpc/pic/port unit logical-unit-number tunnel]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure path MTU discovery for outgoing tunnel connections:</p> <ul style="list-style-type: none"> • path-mtu-discovery—Path MTU discovery is enabled. • no-path-mtu-discovery—Path MTU discovery is disabled.
	<p> NOTE: Starting in Junos OS Release 17.2R1, the no-path-mtu-discovery configuration statement in the [edit interfaces ip-fpc/pic/port unit logical-unit-number tunnel] and [edit interfaces gr-fpc/pic/port unit logical-unit-number tunnel] hierarchies is no longer available for ipip6 tunnels.</p>
Default	Path MTU discovery is enabled.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 21

source-quench

Syntax	(source-quench no-source-quench);
Hierarchy Level	[edit system internet-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure how the Junos OS handles Internet Control Message Protocol (ICMP) source quench messages:</p> <ul style="list-style-type: none"> • source-quench—React to incoming ICMP source quench messages. • no-source-quench—Do not react to incoming ICMP source quench messages.
Default	The Junos OS does not ignore ICMP source quench messages.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Junos OS to Ignore ICMP Source Quench Messages on page 26


system

Syntax	system { ... }
Hierarchy Level	[edit]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Configure system management properties.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • System Management Configuration Statements on page 58

tcp-drop-synfin-set

Syntax	tcp-drop-synfin-set;
Hierarchy Level	[edit system internet-options]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the router or switch to drop packets that have both the SYN and FIN bits set.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set on page 35• TCP Headers with SYN and FIN Flags Set on page 35

tcp-mss

Syntax	<code>tcp-mss <i>mss-value</i>;</code>
Hierarchy Level	[edit system internet-options] [edit interfaces <i>name</i> unit <i>number</i> family <i>protocol</i>]
Release Information	Statement introduced in Junos OS Release 9.2 of J Series Services Routers software. Statement introduced in Junos OS Release 9.5 for M Series and T Series routers. Statement introduced in Junos OS Release 14.2 for MX Series routers.
Description	<p>Enable and specify the TCP maximum segment size (TCP MSS) to be used to replace that of TCP SYN packets whose MSS option is set to a higher value than the value you choose.</p> <p>If the router receives a TCP packet with the SYN bit and MSS option set and the MSS option specified in the packet is larger than the MSS specified by the tcp-mss command, the router replaces the MSS value in the packet with the lower value specified by the tcp-mss statement.</p> <p>This statement enables you to specify the MSS size in TCP SYN packets used during session establishment. Decreasing the MSS size helps to limit packet fragmentation and to protect against packet loss that can occur when a packet must be fragmented to meet the MTU size but the packet's DF (don't fragment) bit is set.</p> <p>Use the tcp-mss statement to specify a lower TCP MSS value than the value in the TCP SYN packets.</p>
	<div>  <p>NOTE: We recommend not to configure TCP MSS because it is not supported when an SRX Series device is running in packet mode with MPLS.</p> </div>
Options	<p>mss-value—TCP MSS value for SYN packets with a higher MSS value set.</p> <p>Range: 64 through 65535 bytes.</p> <p>Default: TCP MSS is disabled.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring TCP MSS for Session Negotiation on page 50

CHAPTER 9

Operational Commands

- `clear arp`
- `show arp`
- `show system statistics arp`
- `show system statistics icmp`
- `show system statistics icmp6`
- `show system statistics igmp`
- `show system statistics ip`
- `show system statistics ip6`
- `show system statistics tcp`

clear arp

Syntax	<pre>clear arp <all> <hostname <i>hostname</i>> <interface <i>interface-name</i>> <logical-system <i>logical-system-name</i>> <tenant <i>name</i>> <vpn <i>vpn</i>></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 14.1 for the MX Series.</p> <p>all option introduced in Junos OS Release 14.2.</p> <p>tenant option added in Junos OS Release 18.3.</p>
Description	<p>Remove entries from the Address Resolution Protocol (ARP) table for the current CLI view. To clear entries for a specific logical system, you must first enter the set cli logical-system <i>logical-system-name</i> command, and then issue the clear arp command.</p>
Options	<p>all— Clear all entries from the ARP table.</p> <p>hostname <i>hostname</i>—(Optional) Clear only the specified host entry from the ARP table.</p> <p>interface <i>interface-name</i>—(Optional) Clear entries only for the specified interface from the ARP table.</p> <p>logical-system <i>logical-system-name</i>—(Optional) Clear entries for only the specified logical system from the ARP table (only available in main router context).</p> <p>tenant <i>name</i>—(Optional) Display the name of the tenant.</p> <p>vpn <i>vpn</i>—(Optional) Clear entries from the ARP table for the specified virtual private network (VPN).</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • set cli logical-system • show arp on page 104 • show dhcp-security arp inspection statistics • Port Security Features
List of Sample Output	<p>clear arp all on page 103</p> <p>clear arp logical-system ls1 on page 103</p>
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear arp all

```
user@host> clear arp all
192.168.71.254    deleted
192.168.65.46    deleted
192.168.64.10    deleted
10.0.12.14       deleted
10.0.17.14       deleted
```

clear arp logical-system ls1

```
user@host> clear arp logical-system ls1
192.168.71.254    deleted
192.168.65.46    deleted
192.168.64.10    deleted
10.0.12.14       deleted
10.0.17.14       deleted
```

show arp

Syntax `show arp`
 `<expiration-time>`
 `<hostname host-name>`
 `<interface interface-name>`
 `<logical-system logical-system-name>`
 `<no-resolve>`
 `<reference-count count>`
 `<tenant name>`
 `<state state>`
 `<vpn vpn-name>`

Release Information Command introduced before Junos OS Release 7.4.
 `expiration-time` option added in Junos OS Release 8.1.
 `logical-system` and `vpn` options added in Junos OS Release 10.1.
 `reference-count`, `tenant`, and `state` options added in Junos OS Release 18.3.

Description Display all entries in the Address Resolution Protocol (ARP) table. To display entries for a particular logical system only, first enter the **set cli logical-system *logical-system-name*** command, and then enter the **show arp** command.



NOTE: Starting with Junos OS Release 14.2, the following enhancements have been made to the output of the `show arp interfaces` command:

- For integrated routing and bridging (IRB) interfaces, in the output of the `show arp` command, the IRB interface name is displayed under the Interface field of the output and the Layer 2 interface identifier is specified in square brackets following the IRB name. Until Release 14.1 and earlier, only the layer 2 interface name and not the IRB name was displayed.
- Starting with release 14.2, if you do not specify a subinterface or a logical unit of the interface with the `show arp interface interface-name` command, an error message is shown. Until Release 14.1 and earlier, if you did not specify the subinterface for a physical interface, the system considered the supplied command to be for subinterface 0 and displayed the output. For example, if you entered `ge-2/2/5`, it was processed by the system as `ge-2/2/5.0`.
- When IRB interfaces are configured and if you attempt to specify an interface name that is not configured on the system, an error message is displayed stating the particular interface is not defined on the system. Until release 14.1 and earlier, unrelated and incorrect entries were displayed even for interface names that did not exist.
- Starting with Release 14.2, you can enter the `show arp interface` command with the IRB name and retrieve the statistical details for the IRB interface. This functionality was not available previously. However, you could previously obtain the ARP details of an IRB interface that had a Layer 2 interface configured.



NOTE: Starting with Junos OS Release 16.1, `show arp no-resolve` command does not display the underlying ifl information if `enhanced-convergence` statement at `[edit irb unit unit-number hierarchy level` and `enhanced-ip` statement at `[edit chassis network-services]` hierarchy level is configured for the destination interface IRB.

Options **none**—Display the entries in the ARP table.

expiration-time—(Optional) Display the amount of time, in seconds, until each ARP entry is set to expire.

hostname *host-name*—(Optional) Display the hostname.

interface *interface-name*—(Optional) Display information about ARP for the specified logical interface

logical-system *logical-system-name*—(Optional) Display ARP entries for the specified logical system; only available on the main router context.

no-resolve—(Optional) Do not attempt to determine the hostname that corresponds to the IP address.

reference-count *count*—(Optional) Display the next-hop reference count.

state *state*—(Optional) Display the next-hop current state.

tenant *name*—(Optional) Display the name of the tenant.

vpn *vpn-name*—(Optional) Display entries in the ARP table for the specified virtual private network's (VPN) routing table.

Required Privilege Level

view

Related Documentation

- [clear arp on page 102](#)
- [set cli logical-system](#)

List of Sample Output

[show arp on page 107](#)
[show arp no-resolve on page 107](#)
[show arp expiration-time on page 107](#)

Output Fields

[Table 4 on page 106](#) describes the output fields for the **show arp** command. Output fields are listed in the approximate order in which they appear.

Table 4: show arp Output Fields

Field Name	Field Description
MAC Address	Media access control (MAC) address that corresponds to the IP address.
Address	IP address that corresponds to the hostname.
Name	Hostname.
Interface	Interface name.
Flags	<p>(no-resolve option only) Indicates how mappings between IP and MAC addresses are defined:</p> <ul style="list-style-type: none"> • Permanent—Static mapping. • Permanent and published—Static mapping that is published. • None—Dynamic mapping.
TTE	(expiration-time option only) Amount of time, in seconds, until ARP entry is set to expire.

Sample Output

show arp

```
user@host> show arp
```

MAC Address	Address	Name	Interface
00:e0:81:22:fd:74	192.168.64.10	firewall.my.net	fxp0.0
00:04:5a:65:78:e1	192.168.65.13	lab.my.net	fxp0.0

show arp no-resolve

```
user@host> show arp no-resolve
```

MAC Address	Address	Interface	Flags
00:90:69:96:00:01	10.10.45.5	fe-0/0/1.0	none
00:00:00:00:00:01	200.200.200.1	fe-0/0/0.0	permanent published
00:00:00:00:00:02	200.200.200.2	fe-0/0/0.0	permanent
00:90:69:91:b0:00	200.200.200.3	fe-0/0/0.0	none

Total entries: 4

```
user@host> show arp no-resolve
```

The command displaying the underlying l2 ifl information when **enhanced-convergence** statement and **enhanced-ip** statement is not configured.

```
show arp no-resolve
```

MAC Address	Address	Interface	Flags
02:01:00:00:00:05	10.0.0.5	em1.0	none
00:00:5e:00:01:1b	91.91.91.50	irb.0[xe-2/1/0.0]	none >>> underlying
l2 ifl associated			
02:01:00:00:00:05	128.0.0.5	em1.0	none
02:01:00:00:00:05	128.0.0.6	em1.0	none
02:00:00:00:00:12	128.0.0.18	em0.0	none
00:26:88:6a:c6:80	192.168.237.126	fxp0.0	none

Total entries: 6

The command not displaying the underlying l2 ifl information when **enhanced-convergence** statement and **enhanced-ip** statement is configured.

MAC Address	Address	Interface	Flags
02:01:00:00:00:05	10.0.0.5	em1.0	none
00:00:5e:00:01:1b	91.91.91.50	irb.0	none >>> underlying
l2 ifl association is removed.			
02:01:00:00:00:05	128.0.0.5	em1.0	none
02:01:00:00:00:05	128.0.0.6	em1.0	none
02:00:00:00:00:12	128.0.0.18	em0.0	none
00:26:88:6a:c6:80	192.168.237.126	fxp0.0	none

Total entries: 6

show arp expiration-time

```
user@host> show arp expiration-time
```

MAC Address	Address	Name	Interface	Flags	TTE
00:a0:a5:12:3e:d4	10.0.0.5	10.0.0.5	fxp1.0	none	

```
00:e0:81:22:fd:74 192.168.64.10 supernova.englab.juniper. fxp0.0 none 1491
00:30:48:84:03:56 192.168.65.46 kgb.englab.juniper.net fxp0.0 none 1279
00:03:ba:12:f7:5e 192.168.65.226 nmssun1-eri0.englab.junip fxp0.0 none 452
00:90:69:8e:b0:fc 192.168.71.254 stonewall-ge-200.englab.j fxp0.0 none 1421
Total entries: 5
```

show system statistics arp

List of Syntax	Syntax on page 109 Syntax (EX Series Switches) on page 109 Syntax (TX Matrix Router) on page 109 Syntax (TX Matrix Plus Router) on page 109
Syntax	show system statistics arp
Syntax (EX Series Switches)	show system statistics arp <all-members> <local> <member <i>member-id</i> >
Syntax (TX Matrix Router)	show system statistics arp <all-chassis all-lcc lcc <i>number</i> scc>
Syntax (TX Matrix Plus Router)	show system statistics arp <all-chassis all-lcc lcc <i>number</i> sfc <i>number</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Description	Display system-wide Address Resolution Protocol (ARP) statistics.
Options	<p>none—Display system-wide ARP statistics.</p> <p>all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display ARP statistics for all the routers in the chassis.</p> <p>all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system-wide ARP statistics for all T640 routers connected to the TX Matrix router. On a TX Matrix Plus router, display system-wide ARP statistics for all routers connected to the TX Matrix Plus router</p> <p>all-members—(EX4200 switches only) (Optional) Display ARP statistics for all members of the Virtual Chassis configuration.</p> <p>lcc <i>number</i>—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display ARP statistics for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display ARP statistics for a specific router that is connected to the TX Matrix Plus router.</p>

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches only) (Optional) Display ARP statistics for the local Virtual Chassis member.

member *member-id*—(EX4200 switches only) (Optional) Display ARP statistics for the specified member of the Virtual Chassis configuration. Replace *member-id* with a value from 0 through 9.

scc—(TX Matrix routers only) (Optional) Display ARP statistics for the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers only) (Optional) Display ARP statistics for the TX Matrix Plus router. Replace *number* with 0.

Additional Information By default, when you issue the **show system statistics arp** command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

Required Privilege Level view

Related Documentation

- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output [show system statistics arp on page 110](#)
[show system statistics arp \(EX Series Switches\) on page 111](#)
[show system statistics arp \(TX Matrix Plus Router\) on page 112](#)

Sample Output

show system statistics arp

```
user@host> show system statistics arp
```

```

arp:
184710 datagrams received
2886 ARP requests received
684 ARP replies received
0 resolution request received
0 unrestricted proxy requests
0 restricted proxy requests
0 received proxy requests
0 unrestricted proxy requests not proxied
0 restricted proxy requests not proxied
0 datagrams with bogus interface
0 datagrams with incorrect length
0 datagrams for non-IP protocol
0 datagrams with unsupported op code
0 datagrams with bad protocol address length
0 datagrams with bad hardware address length
0 datagrams with multicast source address
0 datagrams with multicast target address
0 datagrams with my own hardware address
0 datagrams for an address not on the interface
0 datagrams with a broadcast source address
0 datagrams with source address duplicate to mine
181140 datagrams which were not for me
0 packets discarded waiting for resolution
4 packets sent after waiting for resolution
703 ARP requests sent
2886 ARP replies sent
0 requests for memory denied
0 requests dropped on entry
0 requests dropped during retry
0 requests dropped due to interface deletion
0 requests on unnumbered interfaces
0 new requests on unnumbered interfaces
0 replies for from unnumbered interfaces
0 requests on unnumbered interface with non-subnetted donor
0 replies from unnumbered interface with non-subnetted donor

```

show system statistics arp (EX Series Switches)

```
user@host> show system statistics arp
```

```

arp:
186423 datagrams received
88 ARP requests received
88 ARP replies received
0 resolution request received
0 unrestricted proxy requests
0 restricted proxy requests
0 received proxy requests
0 proxy requests not proxied
0 restricted proxy requests not proxied
0 datagrams with bogus interface
0 datagrams with incorrect length
0 datagrams for non-IP protocol
0 datagrams with unsupported op code
0 datagrams with bad protocol address length
0 datagrams with bad hardware address length
0 datagrams with multicast source address
0 datagrams with multicast source address
0 datagrams with my own hardware address

```

```

164 datagrams for an address not on the interface
0 datagrams with a broadcast source address
0 datagrams with source address duplicate to mine
186075 datagrams which were not for me
0 packets discarded waiting for resolution
0 packets sent after waiting for resolution
50 ARP requests sent
88 ARP replies sent
0 requests for memory denied
0 requests dropped on entry
0 requests dropped during retry
0 requests dropped due to interface deletion
0 requests on unnumbered interfaces
0 new requests on unnumbered interfaces
0 replies for from unnumbered interfaces
0 requests on unnumbered interface with non-subnetted donor
0 replies from unnumbered interface with non-subnetted donor

```

show system statistics arp (TX Matrix Plus Router)

```
user@host> show system statistics arp
```

```
sfc0-re0:
```

```
-----
```

```
arp:
```

```

487 datagrams received
8 ARP requests received
438 ARP replys received
438 resolution requests received
0 unrestricted proxy requests
0 restricted proxy requests
0 received proxy requests
0 proxy requestss not proxied
0 restricted-proxy requestss not proxied
0 with bogus interface
0 with incorrect length
0 for non-IP protocol
0 with unsupported op code
0 with bad protocol address length
0 with bad hardware address length
0 with multicast source address
0 with multicast target address
0 with my own hardware address
0 for an address not on the interface
0 with a broadcast source address
0 with source address duplicate to mine
41 which were not for me
0 packets discarded waiting for resolution
438 packets sent after waiting for resolution
1282 ARP requests sent
8 ARP replys sent
0 requests for memory denied
0 requests dropped on entry
0 requests dropped during retry
0 requests dropped due to interface deletion
0 requests on unnumbered interfaces
0 new requests on unnumbered interfaces
0 replies for from unnumbered interfaces
0 requests on unnumbered interface with non-subnetted donor
0 replies from unnumbered interface with non-subnetted donor

```



```
lcc0-re0:
```

```
-----
arp:
```

```

 19 datagrams received
 0 ARP requests received
 1 ARP reply received
 0 resolution requests received
 0 unrestricted proxy requests
 0 restricted proxy requests
 0 received proxy requests
 0 proxy requestss not proxied
 0 restricted-proxy requestss not proxied
 0 with bogus interface
 0 with incorrect length
 0 for non-IP protocol
 0 with unsupported op code
 0 with bad protocol address length
 0 with bad hardware address length
 0 with multicast source address
 0 with multicast target address
 0 with my own hardware address
 0 for an address not on the interface
 0 with a broadcast source address
 0 with source address duplicate to mine
18 which were not for me
 0 packets discarded waiting for resolution
 0 packets sent after waiting for resolution
 8 ARP requests sent
 0 ARP replies sent
 0 requests for memory denied
 0 requests dropped on entry
 0 requests dropped during retry
 0 requests dropped due to interface deletion
 0 requests on unnumbered interfaces
 0 new requests on unnumbered interfaces
 0 replies for from unnumbered interfaces
 0 requests on unnumbered interface with non-subnetted donor
 0 replies from unnumbered interface with non-subnetted donor
```

```
lcc1-re0:
```

```
-----
arp:
```

```

17 datagrams received
 0 ARP requests received
 1 ARP reply received
 0 resolution requests received
 0 unrestricted proxy requests
 0 restricted proxy requests
 0 received proxy requests
 0 proxy requestss not proxied
 0 restricted-proxy requestss not proxied
 0 with bogus interface
 0 with incorrect length
 0 for non-IP protocol
 0 with unsupported op code
 0 with bad protocol address length
 0 with bad hardware address length
 0 with multicast source address
 0 with multicast target address
```

```

0 with my own hardware address
0 for an address not on the interface
0 with a broadcast source address
0 with source address duplicate to mine
16 which were not for me
0 packets discarded waiting for resolution
0 packets sent after waiting for resolution
9 ARP requests sent
0 ARP replies sent
0 requests for memory denied
0 requests dropped on entry
0 requests dropped during retry
0 requests dropped due to interface deletion
0 requests on unnumbered interfaces
0 new requests on unnumbered interfaces
0 replies for from unnumbered interfaces
0 requests on unnumbered interface with non-subnetted donor
0 replies from unnumbered interface with non-subnetted donor

```

```
lcc2-re0:
```

```
-----
arp:
```

```

18 datagrams received
1 ARP request received
1 ARP reply received
0 resolution requests received
0 unrestricted proxy requests
0 restricted proxy requests
0 received proxy requests
0 proxy requestss not proxied
0 restricted-proxy requestss not proxied
0 with bogus interface
0 with incorrect length
0 for non-IP protocol
0 with unsupported op code
0 with bad protocol address length
0 with bad hardware address length
0 with multicast source address
0 with multicast target address
0 with my own hardware address
0 for an address not on the interface
0 with a broadcast source address
0 with source address duplicate to mine
16 which were not for me
0 packets discarded waiting for resolution
0 packets sent after waiting for resolution
9 ARP requests sent
1 ARP reply sent
0 requests for memory denied
0 requests dropped on entry
0 requests dropped during retry
0 requests dropped due to interface deletion
0 requests on unnumbered interfaces
0 new requests on unnumbered interfaces
0 replies for from unnumbered interfaces
0 requests on unnumbered interface with non-subnetted donor
0 replies from unnumbered interface with non-subnetted donor

```

```
lcc3-re0:
```

```
arp:
  13 datagrams received
  0 ARP requests received
  1 ARP reply received
  0 resolution requests received
  0 unrestricted proxy requests
  0 restricted proxy requests
  0 received proxy requests
  0 proxy requestss not proxied
  0 restricted-proxy requestss not proxied
  0 with bogus interface
  0 with incorrect length
  0 for non-IP protocol
  0 with unsupported op code
  0 with bad protocol address length
  0 with bad hardware address length
  0 with multicast source address
  0 with multicast target address
  0 with my own hardware address
  0 for an address not on the interface
  0 with a broadcast source address
  0 with source address duplicate to mine
  12 which were not for me
  0 packets discarded waiting for resolution
  0 packets sent after waiting for resolution
  8 ARP requests sent
  0 ARP replys sent
  0 requests for memory denied
  0 requests dropped on entry
  0 requests dropped during retry
  0 requests dropped due to interface deletion
  0 requests on unnumbered interfaces
  0 new requests on unnumbered interfaces
  0 replies for from unnumbered interfaces
  0 requests on unnumbered interface with non-subnetted donor
  0 replies from unnumbered interface with non-subnetted donor
```

show system statistics icmp

List of Syntax	Syntax on page 116 Syntax (EX Series Switches) on page 116 Syntax (TX Matrix Router) on page 116 Syntax (TX Matrix Plus Router) on page 116
Syntax	show system statistics icmp
Syntax (EX Series Switches)	show system statistics icmp <all-members> <local> <member <i>member-id</i> >
Syntax (TX Matrix Router)	show system statistics icmp <all-chassis all-lcc lcc <i>number</i> scc>
Syntax (TX Matrix Plus Router)	show system statistics icmp <all-chassis all-lcc lcc <i>number</i> sfc <i>number</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Description	Display system-wide Internet Control Message Protocol (ICMP) statistics.
Options	<p>none—Display system statistics for ICMP.</p> <p>all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display system statistics for ICMP for all the routers in the chassis.</p> <p>all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system statistics for ICMP for all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, display system statistics for ICMP for all connected T1600 or T4000 LCCs.</p> <p>all-members—(EX4200 switches only) (Optional) Display ICMP statistics for all members of the Virtual Chassis configuration.</p> <p>lcc <i>number</i>—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system statistics for ICMP for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display system statistics for ICMP for a specific router that is connected to the TX Matrix Plus router.</p>

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches only) (Optional) Display ICMP statistics for the local Virtual Chassis member.

member *member-id*—(EX4200 switches only) (Optional) Display ICMP statistics for the specified member of the Virtual Chassis configuration. Replace *member-id* with a value from 0 through 9.

scc—(TX Matrix routers only) (Optional) Display system statistics for ICMP for the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers and TX Matrix Plus routers with 3D SIBs only) (Optional) Display system statistics for ICMP for the TX Matrix Plus router. Replace *number* with 0.

Additional Information By default, when you issue the **show system statistics icmp** command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

Required Privilege Level view

Related Documentation [• Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output [show system statistics icmp on page 117](#)
[show system statistics icmp \(EX Series Switches\) on page 118](#)
[show system statistics icmp \(TX Matrix Plus Router\) on page 119](#)

Sample Output

show system statistics icmp

```
user@host> show system statistics icmp
```

```

icmp:
  16783 drops due to rate limit
  9998 calls to icmp_error
  0 errors not generated because old message was icmp
  Output Histogram
    38877 echo reply
    1 destination unreachable
    1 routing redirect
    163 echo
    5000 time exceeded
    4996 parameter problem
    5000 time stamp reply
  0 messages with bad code fields
  0 messages less than the minimum length
  0 messages with bad checksum
  0 messages with bad source address
  20000 messages with bad length
  0 echo drops with broadcast or multicast destination address
  0 timestamp drops with broadcast or multicast destination address
  Input Histogram
    5093 echo reply
    5000 destination unreachable
    5000 source quench
    5000 routing redirect
    5000 alternate host address
    38877 echo
    5000 router advertisement
    5000 router solicitation
    5000 time exceeded
    5000 parameter problem
    5000 time stamp
    5000 time stamp reply
    5000 information request
    5000 information request reply
    5000 address mask request
    5000 address mask reply
    5000 traceroute
    5000 data conversion error
    5000 mobile host redirect
    5000 IPv6 where-are-you
    5000 IPv6 i-am-here
    5000 mobile registration request
    5000 mobile registration reply
    5000 skip
    5000 photuris
  43877 message responses generated

```

show system statistics icmp (EX Series Switches)

```

user@host> show system statistics icmp

icmp:
  0 drops due to rate limit
  12 calls to icmp_error
  0 errors not generated because old message was icmp
  Output histogram:
    297 echo reply
    12 destination unreachable
  0 messages with bad code fields
  0 messages less than the minimum length

```

```

0 messages with bad checksum
0 messages with bad source address
0 messages with bad length
0 echo drops with broadcast or multicast destination address
0 timestamp drops with broadcast or multicast destination address
Input histogram:
    297 echo
297 message responses generated

```

show system statistics icmp (TX Matrix Plus Router)

```
user@host> show system statistics icmp
```

```
sfc0-re0:
```

```
-----
icmp:
    0 drops due to rate limit
    0 calls to icmp_error
    0 errors not generated because old message was icmp
Output histogram:
    echo reply: 21
    0 messages with bad code fields
    0 messages less than the minimum length
    0 messages with bad checksum
    0 messages with bad source address
    0 messages with bad length
    0 echo drops with broadcast or multicast destination address
    0 timestamp drops with broadcast or multicast destination address
Input histogram:
    echo: 21
21 message responses generated

```

```
lcc0-re0:
```

```
-----
icmp:
    0 drops due to rate limit
    1 call to icmp_error
    0 errors not generated because old message was icmp
Output histogram:
    echo reply: 24
    destination unreachable: 1
    0 messages with bad code fields
    0 messages less than the minimum length
    0 messages with bad checksum
    0 messages with bad source address
    0 messages with bad length
    0 echo drops with broadcast or multicast destination address
    0 timestamp drops with broadcast or multicast destination address
Input histogram:
    echo: 24
24 message responses generated

```

```
lcc1-re0:
```

```
-----
icmp:
    0 drops due to rate limit
    0 calls to icmp_error
    0 errors not generated because old message was icmp
Output histogram:
    echo reply: 23

```

```
0 messages with bad code fields
0 messages less than the minimum length
0 messages with bad checksum
0 messages with bad source address
0 messages with bad length
0 echo drops with broadcast or multicast destination address
0 timestamp drops with broadcast or multicast destination address
Input histogram:
    echo: 23
23 message responses generated
```

lcc2-re0:

icmp:

```
0 drops due to rate limit
0 calls to icmp_error
0 errors not generated because old message was icmp
Output histogram:
    echo reply: 22
0 messages with bad code fields
0 messages less than the minimum length
0 messages with bad checksum
0 messages with bad source address
0 messages with bad length
0 echo drops with broadcast or multicast destination address
0 timestamp drops with broadcast or multicast destination address
Input histogram:
    echo: 22
22 message responses generated
```

lcc3-re0:

icmp:

```
0 drops due to rate limit
0 calls to icmp_error
0 errors not generated because old message was icmp
Output histogram:
    echo reply: 22
0 messages with bad code fields
0 messages less than the minimum length
0 messages with bad checksum
0 messages with bad source address
0 messages with bad length
0 echo drops with broadcast or multicast destination address
0 timestamp drops with broadcast or multicast destination address
Input histogram:
    echo: 22
22 message responses generated
```


show system statistics icmp6

List of Syntax	Syntax (EX Series Switches) on page 121 Syntax (MX Series Routers) on page 121 Syntax (TX Matrix Router) on page 121 Syntax (TX Matrix Plus Router) on page 121
Syntax (EX Series Switches)	<pre>show system statistics icmp6 <all-members> <local> <member <i>member-id</i>></pre>
Syntax (MX Series Routers)	<pre>show system statistics icmp6</pre>
Syntax (TX Matrix Router)	<pre>show system statistics icmp6 <all-chassis all-lcc lcc <i>number</i> scc></pre>
Syntax (TX Matrix Plus Router)	<pre>show system statistics icmp6 <all-chassis all-lcc lcc <i>number</i> sfc <i>number</i>></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.</p>
Description	Display system-wide Internet Control Message Protocol for IPv6 (ICMPv6) statistics.
Options	<p>none—Display system statistics for ICMPv6.</p> <p>all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display system statistics for ICMPv6 for all the routers in the chassis.</p> <p>all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system statistics for ICMPv6 for all T640 routers connected to the TX Matrix router. On a TX Matrix Plus router, display system statistics for ICMPv6 for all connected T1600 or T4000 LCCs.</p> <p>all-members—(EX4200 switches only) (Optional) Display ICMPv6 statistics for all members of the Virtual Chassis configuration.</p> <p>lcc <i>number</i>—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system statistics for ICMPv6 for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display system statistics for ICMPv6 for a specific router that is connected to the TX Matrix Plus router.</p>

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches only) (Optional) Display ICMPv6 statistics for the local Virtual Chassis member.

member *member-id*—(EX4200 switches only) (Optional) Display ICMPv6 statistics for the specified member of the Virtual Chassis configuration. Replace *member-id* with a value from 0 through 9.

scc—(TX Matrix routers only) (Optional) Display system statistics for ICMPv6 for the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers only) (Optional) Display system statistics for ICMPv6 for the TX Matrix Plus router. Replace *number* with 0.

Additional Information By default, when you issue the **show system statistics icmp6** command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

Required Privilege Level view

Related Documentation

- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output [show system statistics icmp6 \(MX Series Routers\) on page 122](#)
[show system statistics icmp6 \(EX Series Switches\) on page 123](#)
[show system statistics icmp6 \(TX Matrix Plus Router\) on page 124](#)

Sample Output

show system statistics icmp6 (MX Series Routers)

```
user@host> show system statistics icmp6
```

```

icmp6:
  79 Calls to icmp_error
  0 Errors not generated because old message was icmp error
  0 Errors not generated because rate limitation
  Output histogram:
    79 unreachable
    30 echo
    163 multicast listener query
    6 multicast listener report
    940 neighbor solicitation
    694184 neighbor advertisement
  0 Messages with bad code fields
  0 Messages < minimum length
  0 Bad checksums
  0 Messages with bad length
  Input histogram:
    10 echo reply
    6 multicast listener report
    693975 neighbor solicitation
  Histogram of error messages to be generated:
    0 No route
    0 Administratively prohibited
    0 Beyond scope
    79 Address unreachable
    0 Port unreachable
    0 Time exceed transit
    0 Time exceed reassembly
    0 Erroneous header field
    0 Unrecognized next header
    0 Unrecognized option
    0 Unknown
  0 Message responses generated
  0 Messages with too many ND options
  100000 Max System ND nh cache limit
  79840 Max Public ND nh cache limit
  200 Max IRI ND nh cache limit
  19960 Max Management intf ND nh cache limit
  79840 Current Public ND nexthops present
  4 Current IRI ND nexthops present
  0 Current Management ND nexthops present
  909266 Total ND nexthops creation failed as limit reached
  909266 Public ND nexthops creation failed as public limit reached
  0 IRI ND nexthops creation failed as iri limit reached
  0 Management ND nexthops creation failed as mgt limit reached

```

show system statistics icmp6 (EX Series Switches)

```
user@host> show system statistics icmp6
```

```

icmp6:
  0 Calls to icmp_error
  0 Errors not generated because old message was icmp error
  0 Errors not generated because rate limitation
  0 Messages with bad code fields
  0 Messages < minimum length
  0 Bad checksums
  0 Messages with bad length
    0 No route
    0 Administratively prohibited
    0 Beyond scope

```

```

0 Address unreachable
0 Port unreachable
0 packet too big
0 Time exceed transit
0 Time exceed reassembly
0 Erroneous header field
0 Unrecognized next header
0 Unrecognized option
0 redirect
0 Unknown
0 Message responses generated
0 Messages with too many ND options

```

Sample Output

show system statistics icmp6 (TX Matrix Plus Router)

```

user@host> show system statistics icmp6

sfc0-re0:
-----
icmp6:
  0 calls to icmp_error
  0 errors not generated because old message was icmp error or so
  0 errors not generated because rate limitation
  Output histogram:
    neighbor solicitation: 12
    neighbor advertisement: 4
  0 messages with bad code fields
  0 messages < minimum length
  0 bad checksums
  0 messages with bad length
  Histogram of error messages to be generated:
    0 no route
    0 administratively prohibited
    0 beyond scope
    0 address unreachable
    0 port unreachable
    0 packet too big
    0 time exceed transit
    0 time exceed reassembly
    0 erroneous header field
    0 unrecognized next header
    0 unrecognized option
    0 redirect
    0 unknown
  0 message responses generated
  0 messages with too many ND options

lcc0-re0:
-----
icmp6:
  0 calls to icmp_error
  0 errors not generated because old message was icmp error or so
  0 errors not generated because rate limitation
  Output histogram:
    neighbor solicitation: 12
    neighbor advertisement: 4
  0 messages with bad code fields
  0 messages < minimum length

```

```

0 bad checksums
0 messages with bad length
Histogram of error messages to be generated:
  0 no route
  0 administratively prohibited
  0 beyond scope
  0 address unreachable
  0 port unreachable
  0 packet too big
  0 time exceed transit
  0 time exceed reassembly
  0 erroneous header field
  0 unrecognized next header
  0 unrecognized option
  0 redirect
  0 unknown
0 message responses generated
0 messages with too many ND options

```

```
lcc1-re0:
```

```
-----
icmp6:
```

```

0 calls to icmp_error
0 errors not generated because old message was icmp error or so
0 errors not generated because rate limitation
Output histogram:
  neighbor solicitation: 12
  neighbor advertisement: 4
0 messages with bad code fields
0 messages < minimum length
0 bad checksums
0 messages with bad length
Input histogram:
  neighbor advertisement: 2
Histogram of error messages to be generated:
  0 no route
  0 administratively prohibited
  0 beyond scope
  0 address unreachable
  0 port unreachable
  0 packet too big
  0 time exceed transit
  0 time exceed reassembly
  0 erroneous header field
  0 unrecognized next header
  0 unrecognized option
  0 redirect
  0 unknown
0 message responses generated
0 messages with too many ND options

```

```
lcc2-re0:
```

```
-----
icmp6:
```

```

0 calls to icmp_error
0 errors not generated because old message was icmp error or so
0 errors not generated because rate limitation
Output histogram:
  neighbor solicitation: 12
  neighbor advertisement: 4

```

```
0 messages with bad code fields
0 messages < minimum length
0 bad checksums
0 messages with bad length
Input histogram:
  neighbor advertisement: 2
Histogram of error messages to be generated:
  0 no route
  0 administratively prohibited
  0 beyond scope
  0 address unreachable
  0 port unreachable
  0 packet too big
  0 time exceed transit
  0 time exceed reassembly
  0 erroneous header field
  0 unrecognized next header
  0 unrecognized option
  0 redirect
  0 unknown
0 message responses generated
0 messages with too many ND options
```

lcc3-re0:

icmp6:

```
0 calls to icmp_error
0 errors not generated because old message was icmp error or so
0 errors not generated because rate limitation
Output histogram:
  neighbor solicitation: 12
  neighbor advertisement: 4
0 messages with bad code fields
0 messages < minimum length
0 bad checksums
0 messages with bad length
Input histogram:
  neighbor advertisement: 2
Histogram of error messages to be generated:
  0 no route
  0 administratively prohibited
  0 beyond scope
  0 address unreachable
  0 port unreachable
  0 packet too big
  0 time exceed transit
  0 time exceed reassembly
  0 erroneous header field
  0 unrecognized next header
  0 unrecognized option
  0 redirect
  0 unknown
0 message responses generated
0 messages with too many ND options
```

show system statistics igmp

List of Syntax	Syntax on page 127 Syntax (EX Series Switches) on page 127 Syntax (TX Matrix Router) on page 127 Syntax (TX Matrix Plus Router) on page 127
Syntax	show system statistics igmp
Syntax (EX Series Switches)	show system statistics igmp <all-members> <local> <member <i>member-id</i> >
Syntax (TX Matrix Router)	show system statistics igmp <all-chassis all-lcc lcc <i>number</i> scc>
Syntax (TX Matrix Plus Router)	show system statistics igmp <all-chassis all-lcc lcc <i>number</i> sfc <i>number</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6. Command introduced in Junos OS Release 12.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Display system-wide Internet Group Management Protocol (IGMP) statistics.
Options	none —Display system statistics for IGMP. all-chassis —(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display system statistics for IGMP for all the routers in the chassis. all-lcc —(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system statistics for IGMP for all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, display system statistics for IGMP for all connected T1600 or T4000 LCCs. all-members —(EX4200 switches only) (Optional) Display IGMP statistics for all members of the Virtual Chassis configuration. lcc <i>number</i> —(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system statistics for IGMP for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display system statistics for IGMP for a specific router that is connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches only) (Optional) Display IGMP statistics for the local Virtual Chassis member.

member *member-id*—(EX4200 switches only) (Optional) Display IGMP statistics for the specified member of the Virtual Chassis configuration. Replace *member-id* with a value from 0 through 9.

scc—(TX Matrix routers only) (Optional) Display system statistics for IGMP for the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers only) (Optional) Display system statistics for IGMP for the TX Matrix Plus router. Replace *number* with 0.

Additional Information By default, when you issue the **show system statistics igmp** command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

Required Privilege Level view

Related Documentation

- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output [show system statistics igmp on page 128](#)
[show system statistics igmp \(EX Series Switches\) on page 129](#)
[show system statistics igmp \(TX Matrix Plus Router\) on page 129](#)

Sample Output

show system statistics igmp

```
user@host> show system statistics igmp
```



```
igmp:
  17178 messages received
  0 messages received with too few bytes
  0 messages received with bad checksum
  0 membership queries received
  0 membership queries received with invalid field(s)
  0 membership reports received
  0 membership reports received with invalid field(s)
  0 membership reports received for groups to which we belong
  0 membership reports sent
```

show system statistics igmp (EX Series Switches)

```
user@host> show system statistics igmp
```

```
igmp:
  0 messages received
  0 messages received with too few bytes
  0 messages received with bad checksum
  0 membership queries received
  0 membership queries received with invalid fields
  0 membership reports received
  0 membership reports received with invalid fields
  0 membership reports received for groups to which we belong
  0 Membership reports sent
```

show system statistics igmp (TX Matrix Plus Router)

```
user@host> show system statistics igmp
```

```
sfc0-re0:
```

```
-----
igmp:
  0 messages received
  0 messages received with too few bytes
  0 messages received with bad checksum
  0 membership queries received
  0 membership queries received with invalid field(s)
  0 membership reports received
  0 membership reports received with invalid field(s)
  0 membership reports received for groups to which we belong
  0 membership reports sent
```

```
lcc0-re0:
```

```
-----
igmp:
  0 messages received
  0 messages received with too few bytes
  0 messages received with bad checksum
  0 membership queries received
  0 membership queries received with invalid field(s)
  0 membership reports received
  0 membership reports received with invalid field(s)
  0 membership reports received for groups to which we belong
  0 membership reports sent
```

```
lcc1-re0:
```

```
-----
igmp:
```

```
0 messages received
0 messages received with too few bytes
0 messages received with bad checksum
0 membership queries received
0 membership queries received with invalid field(s)
0 membership reports received
0 membership reports received with invalid field(s)
0 membership reports received for groups to which we belong
0 membership reports sent
```

lcc2-re0:

igmp:

```
0 messages received
0 messages received with too few bytes
0 messages received with bad checksum
0 membership queries received
0 membership queries received with invalid field(s)
0 membership reports received
0 membership reports received with invalid field(s)
0 membership reports received for groups to which we belong
0 membership reports sent
```

lcc3-re0:

igmp:

```
0 messages received
0 messages received with too few bytes
0 messages received with bad checksum
0 membership queries received
0 membership queries received with invalid field(s)
0 membership reports received
0 membership reports received with invalid field(s)
0 membership reports received for groups to which we belong
0 membership reports sent
```

show system statistics ip

List of Syntax	Syntax on page 131 Syntax (EX Series Switches) on page 131 Syntax (TX Matrix Router) on page 131 Syntax (TX Matrix Plus Router) on page 131
Syntax	<code>show system statistics ip</code>
Syntax (EX Series Switches)	<code>show system statistics ip</code> <code><all-members></code> <code><local></code> <code><member <i>member-id</i>></code>
Syntax (TX Matrix Router)	<code>show system statistics ip</code> <code><all-chassis all-lcc lcc <i>number</i> scc></code>
Syntax (TX Matrix Plus Router)	<code>show system statistics ip</code> <code><all-chassis all-lcc lcc <i>number</i> sfc <i>number</i>></code>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.</p>
Description	Display system-wide IPv4 statistics.
Options	<p>none—Display system statistics for IPv4.</p> <p>all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display system statistics for IPv4 for all the routers in the chassis.</p> <p>all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system statistics for IPv4 for all T640 routers connected to the TX Matrix router. On a TX Matrix Plus router, display system statistics for IPv4 for all T1600 or T4000 routers connected to the TX Matrix Plus router.</p> <p>all-members—(EX4200 switches only) (Optional) Display IPv4 statistics for all members of the Virtual Chassis configuration.</p> <p>lcc <i>number</i>—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system statistics for IPv4 for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display system statistics for IPv4 for a specific router that is connected to the TX Matrix Plus router.</p>

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches only) (Optional) Display IPv4 statistics for the local Virtual Chassis member.

member *member-id*—(EX4200 switches only) (Optional) Display IPv4 statistics for the specified member of the Virtual Chassis configuration. Replace *member-id* with a value from 0 through 9.

scc—(TX Matrix routers only) (Optional) Display system statistics for IPv4 for the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers only) (Optional) Display system statistics for IPv4 for the TX Matrix Plus router. Replace *number* with 0.

Additional Information By default, when you issue the **show system statistics ip** command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

Required Privilege Level view

Related Documentation

- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output [show system statistics ip on page 132](#)
[show system statistics ip \(EX Series Switches\) on page 133](#)
[show system statistics ip \(TX Matrix Plus Router\) on page 134](#)

Sample Output

show system statistics ip

```
user@host> show system statistics ip
```

```

ip:
1752658 total packets received
0 bad header checksums
0 with size smaller than minimum
0 with data size < data length
0 with header length < data size
0 with data length < header length
0 with incorrect version number
0 packets destined to dead next hop
0 fragments received
0 fragments dropped (dup or out of space)
0 fragment sessions dropped (queue overflow)
0 fragments dropped after timeout
0 packets reassembled ok
1709456 packets for this host
10494 packets for unknown/unsupported protocol
546 packets forwarded
0 packets not forwardable
546 redirects sent
1340179 packets sent from this host
0 packets sent with fabricated ip header
0 output packets dropped due to no bufs
0 output packets discarded due to no route
0 output datagrams fragmented
0 fragments created
0 datagrams that can't be fragmented
0 packets with bad options
10494 packets with options handled without error
0 strict source and record route options
0 loose source and record route options
0 record route options
0 timestamp options
0 timestamp and address options
0 timestamp and prespecified address options
0 option packets dropped due to rate limit
10494 router alert options
0 multicast packets dropped (no iflist)
0 packets dropped (src and int don't match)
0 transit re packets dropped on mgmt i/f
0 packets used first nexthop in ecmp unilist
0 incoming ttpoip packets received
0 incoming ttpoip packets dropped
0 outgoing TTPoIP packets sent
0 outgoing TTPoIP packets dropped
0 raw packets dropped. no space in socket recv buffer

```

show system statistics ip (EX Series Switches)

```
user@host> show system statistics ip
```

```

ip:
74121 total packets received
0 bad header checksums
0 with size smaller than minimum
0 with data size < data length
0 with header length < data size
0 with data length < header length
0 with incorrect version number
0 packets destined to dead next hop
0 fragments received

```

```

0 fragments dropped (dup or out of space)
0 fragment sessions dropped (queue overflow)
0 fragments dropped after timeout
0 packets reassembled ok
1134061 packets for this host
0 packets for unknown/unsupported protocol
40177 packets forwarded
0 packets not forwardable
40177 redirects sent
1122558 packets sent from this host
0 packets sent with fabricated ip header
0 output packets dropped due to no bufs
0 output packets discarded due to no route
0 output datagrams fragmented
0 fragments created
0 datagrams that can't be fragmented
0 packets with bad options
0 packets with options handled without error
0 strict source and record route options
0 loose source and record route options
0 record route options
0 timestamp options
0 timestamp and address options
0 timestamp and prespecified address options
0 option packets dropped due to rate limit
0 router alert options
0 multicast packets dropped (no iflist)
0 packets dropped (src and int don't match)
0 transit re packets dropped on mgmt i/f
0 packets used first nexthop in ecmp unilist
0 incoming ttpoip packets received
0 incoming ttpoip packets dropped
0 outgoing TTPoIP packets sent
0 outgoing TTPoIP packets dropped

```

show system statistics ip (TX Matrix Plus Router)

```
user@host> show system statistics ip
```

```
sfc0-re0:
```

```
-----
ip:
```

```

47695035 total packets received
0 bad header checksums
0 with size smaller than minimum
0 with data size < data length
0 with header length < data size
0 with data length < header length
0 with incorrect version number
0 packets destined to dead next hop
42350 fragments received
0 fragments dropped (dup or out of space)
0 fragment sessions dropped (queue overflow)
0 fragments dropped after timeout
21175 packets reassembled ok
47674941 packets for this host
146 packets for unknown/unsupported protocol
0 packets forwarded
0 packets not forwardable
0 redirects sent

```

```

61304579 packets sent from this host
8496 packets sent with fabricated ip header
0 output packets dropped due to no bufs
0 output packets discarded due to no route
6746344 output datagrams fragmented
0 fragments created
0 datagrams that can't be fragmented
0 packets with bad options
2400 packets with options handled without error
0 strict source and record route options
0 loose source and record route options
0 record route options
0 timestamp options
0 timestamp and address options
0 timestamp and prespecified address options
0 option packets dropped due to rate limit
2400 router alert options
0 multicast packets dropped (no iflist)
0 packets dropped (src and int don't match)
0 transit re packets dropped on mgmt i/f
0 packets used first nexthop in ecmp unilist
12995412 incoming ttpoip packets received
0 incoming ttpoip packets dropped
16959177 outgoing TTPoIP packets sent
0 outgoing TTPoIP packets dropped
0 raw packets dropped. no space in socket recv buffer

```

lcc0-re0:

ip:

```

12990061 total packets received
0 bad header checksums
0 with size smaller than minimum
0 with data size < data length
0 with header length < data size
0 with data length < header length
0 with incorrect version number
0 packets destined to dead next hop
0 fragments received
0 fragments dropped (dup or out of space)
0 fragment sessions dropped (queue overflow)
0 fragments dropped after timeout
0 packets reassembled ok
12989979 packets for this host
82 packets for unknown/unsupported protocol
0 packets forwarded
0 packets not forwardable
0 redirects sent
9318381 packets sent from this host
0 packets sent with fabricated ip header
0 output packets dropped due to no bufs
0 output packets discarded due to no route
3440 output datagrams fragmented
0 fragments created
0 datagrams that can't be fragmented
0 packets with bad options
82 packets with options handled without error
0 strict source and record route options
0 loose source and record route options
0 record route options

```

```

0 timestamp options
0 timestamp and address options
0 timestamp and prespecified address options
0 option packets dropped due to rate limit
82 router alert options
0 multicast packets dropped (no iflist)
0 packets dropped (src and int don't match)
0 transit re packets dropped on mgmt i/f
0 packets used first nexthop in ecmp unilist
0 incoming ttpoip packets received
0 incoming ttpoip packets dropped
548071 outgoing TTPoIP packets sent
0 outgoing TTPoIP packets dropped
0 raw packets dropped. no space in socket rcv buffer

```

lcc1-re0:

ip:

```

12849723 total packets received
0 bad header checksums
0 with size smaller than minimum
0 with data size < data length
0 with header length < data size
0 with data length < header length
0 with incorrect version number
0 packets destined to dead next hop
0 fragments received
0 fragments dropped (dup or out of space)
0 fragment sessions dropped (queue overflow)
0 fragments dropped after timeout
0 packets reassembled ok
12849641 packets for this host
82 packets for unknown/unsupported protocol
0 packets forwarded
0 packets not forwardable
0 redirects sent
7676351 packets sent from this host
0 packets sent with fabricated ip header
0 output packets dropped due to no bufs
0 output packets discarded due to no route
0 output datagrams fragmented
0 fragments created
0 datagrams that can't be fragmented
0 packets with bad options
82 packets with options handled without error
0 strict source and record route options
0 loose source and record route options
0 record route options
0 timestamp options
0 timestamp and address options
0 timestamp and prespecified address options
0 option packets dropped due to rate limit
82 router alert options
0 multicast packets dropped (no iflist)
0 packets dropped (src and int don't match)
0 transit re packets dropped on mgmt i/f
0 packets used first nexthop in ecmp unilist
0 incoming ttpoip packets received
0 incoming ttpoip packets dropped
0 outgoing TTPoIP packets sent

```



```

0 outgoing TTPoIP packets dropped
0 raw packets dropped. no space in socket recv buffer

```

```
lcc2-re0:
```

```
-----
ip:
```

```

16926850 total packets received
0 bad header checksums
0 with size smaller than minimum
0 with data size < data length
0 with header length < data size
0 with data length < header length
0 with incorrect version number
0 packets destined to dead next hop
0 fragments received
0 fragments dropped (dup or out of space)
0 fragment sessions dropped (queue overflow)
0 fragments dropped after timeout
0 packets reassembled ok
16926768 packets for this host
82 packets for unknown/unsupported protocol
0 packets forwarded
0 packets not forwardable
0 redirects sent
10039747 packets sent from this host
0 packets sent with fabricated ip header
0 output packets dropped due to no bufs
0 output packets discarded due to no route
0 output datagrams fragmented
0 fragments created
0 datagrams that can't be fragmented
0 packets with bad options
82 packets with options handled without error
0 strict source and record route options
0 loose source and record route options
0 record route options
0 timestamp options
0 timestamp and address options
0 timestamp and prespecified address options
0 option packets dropped due to rate limit
82 router alert options
0 multicast packets dropped (no iflist)
0 packets dropped (src and int don't match)
0 transit re packets dropped on mgmt i/f
0 packets used first nexthop in ecmp unilist
0 incoming ttpoip packets received
0 incoming ttpoip packets dropped
0 outgoing TTPoIP packets sent
0 outgoing TTPoIP packets dropped
0 raw packets dropped. no space in socket recv buffer

```

```
lcc3-re0:
```

```
-----
ip:
```

```

18025026 total packets received
0 bad header checksums
0 with size smaller than minimum
0 with data size < data length
0 with header length < data size
0 with data length < header length

```

```
0 with incorrect version number
0 packets destined to dead next hop
0 fragments received
0 fragments dropped (dup or out of space)
0 fragment sessions dropped (queue overflow)
0 fragments dropped after timeout
0 packets reassembled ok
18024944 packets for this host
82 packets for unknown/unsupported protocol
0 packets forwarded
0 packets not forwardable
0 redirects sent
10456545 packets sent from this host
0 packets sent with fabricated ip header
0 output packets dropped due to no bufs
0 output packets discarded due to no route
0 output datagrams fragmented
0 fragments created
0 datagrams that can't be fragmented
0 packets with bad options
82 packets with options handled without error
0 strict source and record route options
0 loose source and record route options
0 record route options
0 timestamp options
0 timestamp and address options
0 timestamp and prespecified address options
0 option packets dropped due to rate limit
82 router alert options
0 multicast packets dropped (no iflist)
0 packets dropped (src and int don't match)
0 transit re packets dropped on mgmt i/f
0 packets used first nexthop in ecmp unilist
0 incoming ttpoip packets received
0 incoming ttpoip packets dropped
0 outgoing TTPoIP packets sent
0 outgoing TTPoIP packets dropped
0 raw packets dropped. no space in socket recv buffer
```

show system statistics ip6

List of Syntax	Syntax on page 139 Syntax (EX Series Switches) on page 139 Syntax (TX Matrix Router) on page 139 Syntax (TX Matrix Plus Router) on page 139
Syntax	show system statistics ip6
Syntax (EX Series Switches)	show system statistics ip6 <all-members> <local> <member <i>member-id</i> >
Syntax (TX Matrix Router)	show system statistics ip6 <all-chassis all-lcc lcc <i>number</i> scc>
Syntax (TX Matrix Plus Router)	show system statistics ip <all-chassis all-lcc lcc <i>number</i> sfc <i>number</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Description	Display system-wide IPv6 statistics.
Options	<p>none—Display system statistics for IPv6.</p> <p>all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display system statistics for IPv6 for all the routers in the chassis.</p> <p>all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system statistics for IPv6 for all T640 routers connected to the TX Matrix router. On a TX Matrix Plus router, display system statistics for IPv6 for all connected T1600 or T4000 LCCs.</p> <p>all-members—(EX4200 switches only) (Optional) Display IPv6 statistics for all members of the Virtual Chassis configuration.</p> <p>lcc <i>number</i>—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system statistics for IPv6 for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display system statistics for IPv6 for a specific router that is connected to the TX Matrix Plus router.</p>

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches only) (Optional) Display IPv6 statistics for the local Virtual Chassis member.

member *member-id*—(EX4200 switches only) (Optional) Display IPv6 statistics for the specified member of the Virtual Chassis configuration. Replace *member-id* with a value from 0 through 9.

scc—(TX Matrix routers only) (Optional) Display system statistics for IPv6 for the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers only) (Optional) Display system statistics for IPv6 for the TX Matrix Plus router. Replace *number* with 0.

Additional Information By default, when you issue the **show system statistics ip6** command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

Required Privilege Level view

Related Documentation

- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output [show system statistics ip6 on page 140](#)
[show system statistics ip6 \(EX Series Switches\) on page 141](#)
[show system statistics ip6 \(TX Matrix Router\) on page 142](#)

Sample Output

show system statistics ip6

```
user@host> show system statistics ip6
```

```

ip6:
  0 total packets received
  0 with size smaller than minimum
  0 with data size < data length
  0 with bad options
  0 with incorrect version number
  0 fragments received
  0 fragments dropped (dup or out of space)
  0 fragments dropped after timeout
  0 fragment sessions dropped (queue overflow)
  0 packets reassembled ok
  0 packets for this host
  0 packets forwarded
  0 packets not forwardable
  0 redirects sent
  0 packets sent from this host
  0 packets sent with fabricated ip header
  0 output packets dropped due to no bufs, etc.
  0 output packets discarded due to no route
  0 output datagrams fragmented
  0 fragments created
  0 datagrams that can't be fragmented
  0 packets that violated scope rules
  0 multicast packets which we don't join
Mbuf statistics:
  0 packets whose headers are not continuous
  0 tunneling packets that can't find gif
  0 packets discarded due to too many headers
  0 failures of source address selection
  0 forward cache hit
  0 forward cache miss
  0 packets destined to dead next hop
  0 option packets dropped due to rate limit
  0 packets dropped (src and int don't match)
  0 packets dropped due to bad protocol

```

show system statistics ip6 (EX Series Switches)

```
user@host> show system statistics ip6
```

```

ip6:
  0 total packets received
  0 packets with size smaller than minimum
  0 packets with data size < data length
  0 packets with bad options
  0 packets with incorrect version number
  0 fragments received
  0 fragments dropped (dup or out of space)
  0 fragments dropped after timeout
  0 fragment sessions dropped (queue overflow)
  0 packets reassembled ok
  0 packets for this host
  0 packets forwarded
  0 packets not forwardable
  0 redirects sent
  0 packets sent from this host
  0 packets sent with fabricated ip header
  0 output packets dropped due to no bufs, etc.
  0 output datagrams fragmented
  0 fragments created

```

```

0 datagrams that can't be fragmented
0 packets that violated scope rules
0 multicast packets which we don't join
0 packets whose headers are not continuous
0 tunneling packets that can't find gif
0 packets discarded due to too may headers
0 failures of source address selection
0 forward cache hit
0 forward cache miss
0 Packets destined to dead next hop
0 option packets dropped due to rate limit
0 Packets dropped (src and int don't match)
0 packets dropped due to bad protocol
0 transit re packet(null) dropped on mgmt i/f

```

show system statistics ip6 (TX Matrix Router)

```
user@host> show system statistics ip6
```

```
sfc0-re0:
```

```
-----
ip6:
```

```

0 total packets received
0 with size smaller than minimum
0 with data size < data length
0 with bad options
0 with incorrect version number
0 fragments received
0 fragments dropped (dup or out of space)
0 fragments dropped after timeout
0 fragment sessions dropped (queue overflow)
0 packets reassembled ok
0 packets for this host
0 packets forwarded
0 packets not forwardable
0 redirects sent
0 packets sent from this host
0 packets sent with fabricated ip header
0 output packets dropped due to no bufs, etc.
0 output packets discarded due to no route
0 output datagrams fragmented
0 fragments created
0 datagrams that can't be fragmented
0 packets that violated scope rules
0 multicast packets which we don't join
Mbuf statistics:
0 packets whose headers are not continuous
0 tunneling packets that can't find gif
0 packets discarded due to too may headers
0 failures of source address selection
source addresses on an outgoing I/F
    4 link-locals
source addresses of same scope
    4 link-locals
0 forward cache hit
0 forward cache miss
0 packets destined to dead next hop
0 option packets dropped due to rate limit
0 packets dropped (src and int don't match)
0 packets dropped due to bad protocol

```

```

0 transit re packet(null) dropped on mgmt i/f
0 packet(null) used first nexthop in ecmp unilist

```

```
lcc0-re0:
```

```
-----
ip6:
```

```

0 total packets received
0 with size smaller than minimum
0 with data size < data length
0 with bad options
0 with incorrect version number
0 fragments received
0 fragments dropped (dup or out of space)
0 fragments dropped after timeout
0 fragment sessions dropped (queue overflow)
0 packets reassembled ok
0 packets for this host
0 packets forwarded
0 packets not forwardable
0 redirects sent
0 packets sent from this host
0 packets sent with fabricated ip header
0 output packets dropped due to no bufs, etc.
0 output packets discarded due to no route
0 output datagrams fragmented
0 fragments created
0 datagrams that can't be fragmented
0 packets that violated scope rules
0 multicast packets which we don't join
Mbuf statistics:
0 packets whose headers are not continuous
0 tunneling packets that can't find gif
0 packets discarded due to too many headers
0 failures of source address selection
source addresses on an outgoing I/F
    4 link-locals
source addresses of same scope
    4 link-locals
0 forward cache hit
0 forward cache miss
0 packets destined to dead next hop
0 option packets dropped due to rate limit
0 packets dropped (src and int don't match)
0 packets dropped due to bad protocol
0 transit re packet(null) dropped on mgmt i/f
0 packet(null) used first nexthop in ecmp unilist

```

```
lcc1-re0:
```

```
-----
ip6:
```

```

2 total packets received
0 with size smaller than minimum
0 with data size < data length
0 with bad options
0 with incorrect version number
0 fragments received
0 fragments dropped (dup or out of space)
0 fragments dropped after timeout
0 fragment sessions dropped (queue overflow)
0 packets reassembled ok

```

```

0 packets for this host
0 packets forwarded
0 packets not forwardable
0 redirects sent
0 packets sent from this host
0 packets sent with fabricated ip header
0 output packets dropped due to no bufs, etc.
0 output packets discarded due to no route
0 output datagrams fragmented
0 fragments created
0 datagrams that can't be fragmented
0 packets that violated scope rules
0 multicast packets which we don't join
Input histogram:
    ICMP6: 2
Mbuf statistics:
0 packets whose headers are not continuous
0 tunneling packets that can't find gif
0 packets discarded due to too many headers
0 failures of source address selection
source addresses on an outgoing I/F
    4 link-locals
source addresses of same scope
    4 link-locals
0 forward cache hit
0 forward cache miss
0 packets destined to dead next hop
0 option packets dropped due to rate limit
0 packets dropped (src and int don't match)
0 packets dropped due to bad protocol
0 transit re packet(null) dropped on mgmt i/f
0 packet(null) used first nexthop in ecmp unilist

```

lcc2-re0:

ip6:

```

2 total packets received
0 with size smaller than minimum
0 with data size < data length
0 with bad options
0 with incorrect version number
0 fragments received
0 fragments dropped (dup or out of space)
0 fragments dropped after timeout
0 fragment sessions dropped (queue overflow)
0 packets reassembled ok
0 packets for this host
0 packets forwarded
0 packets not forwardable
0 redirects sent
0 packets sent from this host
0 packets sent with fabricated ip header
0 output packets dropped due to no bufs, etc.
0 output packets discarded due to no route
0 output datagrams fragmented
0 fragments created
0 datagrams that can't be fragmented
0 packets that violated scope rules
0 multicast packets which we don't join
Input histogram:

```



```

        ICMP6: 2
Mbuf statistics:
0 packets whose headers are not continuous
0 tunneling packets that can't find gif
0 packets discarded due to too many headers
0 failures of source address selection
source addresses on an outgoing I/F
    4 link-locals
source addresses of same scope
    4 link-locals
0 forward cache hit
0 forward cache miss
0 packets destined to dead next hop
0 option packets dropped due to rate limit
0 packets dropped (src and int don't match)
0 packets dropped due to bad protocol
0 transit re packet(null) dropped on mgmt i/f
0 packet(null) used first nexthop in ecmp unilist

```

```
lcc3-re0:
```

```
-----
ip6:
```

```

2 total packets received
0 with size smaller than minimum
0 with data size < data length
0 with bad options
0 with incorrect version number
0 fragments received
0 fragments dropped (dup or out of space)
0 fragments dropped after timeout
0 fragment sessions dropped (queue overflow)
0 packets reassembled ok
0 packets for this host
0 packets forwarded
0 packets not forwardable
0 redirects sent
0 packets sent from this host
0 packets sent with fabricated ip header
0 output packets dropped due to no bufs, etc.
0 output packets discarded due to no route
0 output datagrams fragmented
0 fragments created
0 datagrams that can't be fragmented
0 packets that violated scope rules
0 multicast packets which we don't join
Input histogram:
    ICMP6: 2
Mbuf statistics:
0 packets whose headers are not continuous
0 tunneling packets that can't find gif
0 packets discarded due to too many headers
0 failures of source address selection
source addresses on an outgoing I/F
    4 link-locals
source addresses of same scope
    4 link-locals
0 forward cache hit
0 forward cache miss
0 packets destined to dead next hop
0 option packets dropped due to rate limit

```

```
0 packets dropped (src and int don't match)
0 packets dropped due to bad protocol
0 transit re packet(null) dropped on mgmt i/f
0 packet(null) used first nexthop in ecmp unilist
```

show system statistics tcp

List of Syntax	Syntax on page 147 Syntax (EX Series Switches) on page 147 Syntax (TX Matrix Router) on page 147 Syntax (TX Matrix Plus Router) on page 147
Syntax	show system statistics tcp
Syntax (EX Series Switches)	show system statistics tcp <all-members> <local> <member <i>member-id</i> >
Syntax (TX Matrix Router)	show system statistics tcp <all-chassis all-lcc lcc <i>number</i> scc>
Syntax (TX Matrix Plus Router)	show system statistics tcp <all-chassis all-lcc lcc <i>number</i> sfc <i>number</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Description	Display system-wide Transmission Control Protocol (TCP) statistics.
Options	<p>none—Display system statistics for TCP.</p> <p>all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display system statistics for TCP for all the routers in the chassis.</p> <p>all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system statistics for TCP for all T640 routers connected to the TX Matrix router. On a TX Matrix Plus router, display system statistics for TCP for all connected T1600 or T4000 LCCs.</p> <p>all-members—(EX4200 switches only) (Optional) Display TCP statistics for all members of the Virtual Chassis configuration.</p> <p>lcc <i>number</i>—(TX Matrix routers, TX Matrix Plus routers, and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system statistics for TCP for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display system statistics for TCP for a specific router that is connected to the TX Matrix Plus router.</p>

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches only) (Optional) Display TCP statistics for the local Virtual Chassis member.

member *member-id*—(EX4200 switches only) (Optional) Display TCP statistics for the specified member of the Virtual Chassis configuration. Replace *member-id* with a value from 0 through 9.

scc—(TX Matrix routers only) (Optional) Display system statistics for TCP for the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers and TX Matrix Plus routers only) (Optional) Display system statistics for TCP for the TX Matrix Plus router. Replace *number* with 0.

Additional Information By default, when you issue the **show system statistics tcp** command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

Required Privilege Level view

Related Documentation

- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output [show system statistics tcp on page 149](#)
[show system statistics tcp \(EX Series Switches\) on page 150](#)
[show system statistics tcp lcc \(TX Matrix Router\) on page 151](#)
[show system statistics tcp \(TX Matrix Plus Router\) on page 152](#)
[show system statistics tcp \(Junos OS Evolved\) on page 155](#)

Sample Output

show system statistics tcp

```
user@host> show system statistics tcp
```

```
tcp:
```

```

  3844 packets sent
    3618 data packets (1055596 bytes)
    0 data packets (0 bytes) retransmitted
    0 resends initiated by MTU discovery
    205 ack-only packets (148 packets delayed)
    0 URG only packets
    0 window probe packets
    0 window update packets
    1079 control packets
  5815 packets received
    3377 acks (for 1055657 bytes)
    24 duplicate acks
    0 acks for unsent data
    2655 packets (15004 bytes) received in-sequence
    1 completely duplicate packet (0 bytes)
    0 old duplicate packets
    0 packets with some dup. data (0 bytes duped)
    0 out-of-order packets (0 bytes)
    0 packets (0 bytes) of data after window
    0 window probes
    7 window update packets
    0 packets received after close
    0 discarded for bad checksums
    0 discarded for bad header offset fields
    0 discarded because packet too short
  1 connection request
  32 connection accepts
  0 bad connection attempts
  0 listen queue overflows
  33 connections established (including accepts)
  30 connections closed (including 0 drops)
    27 connections updated cached RTT on close
    27 connections updated cached RTT variance on close
    0 connections updated cached ssthresh on close
  0 embryonic connections dropped
  3374 segments updated rtt (of 3220 attempts)
  0 retransmit timeouts
    0 connections dropped by rexmit timeout
  0 persist timeouts
    0 connections dropped by persist timeout
  344 keepalive timeouts
    0 keepalive probes sent
    0 connections dropped by keepalive
  1096 correct ACK header predictions
  1314 correct data packet header predictions
  32 syncache entries added
    0 retransmitted
    0 dupsyn
    0 dropped
    32 completed
    0 bucket overflow
    0 cache overflow
    0 reset

```

```

    0 stale
    0 aborted
    0 badack
    0 unreach
    0 zone failures
0 cookies sent
0 cookies received
0 ACKs sent in response to in-window but not exact RSTs
0 ACKs sent in response to in-window SYNs on established connections
0 rcv packets dropped by TCP due to bad address
0 out-of-sequence segment drops due to insufficient memory
1058 RST packets
0 ICMP packets ignored by TCP
0 send packets dropped by TCP due to auth errors
0 rcv packets dropped by TCP due to auth errors

```

show system statistics tcp (EX Series Switches)

```
user@host> show system statistics tcp
```

Tcp:

```

572724 packets sent
    21936 data packets (1887657 bytes)
    2 data packets retransmitted (20 bytes)
    0 resends initiated by MTU discovery
    3724 ack only packets (537 packets delayed)
    0 URG only packets
    1 window probe packets
    1 window update packets
    1094083 control packets
1134258 packets received
    21371 acks(for 1886660 bytes)
    5870 duplicate acks
    0 acks for unsent data
    19908 packets received in-sequence(267794 bytes)
    3022 completely duplicate packets(0 bytes)
    0 old duplicate packets
    4 packets with some duplicate data(4 bytes duped)
    2 out-of-order packets(2 bytes)
    0 packets of data after window(0 bytes)
    0 window probes
    40 window update packets
    0 packets received after close
    0 discarded for bad checksums
    0 discarded for bad header offset fields
    0 discarded because packet too short
547027 connection requests
80 connection accepts
0 bad connection attempts
0 listen queue overflows
103 connections established (including accepts)
547106 connections closed (including 6 drops)
    47 connections updated cached RTT on close
    47 connections updated cached RTT variance on close
    0 connections updated cached ssthresh on close
547004 embryonic connections dropped
20862 segments updated rtt(of 567830 attempts)
2 retransmit timeouts
    0 connections dropped by retransmit timeout
0 persist timeouts

```

```

        0 connections dropped by persist timeout
3032 keepalive timeouts
        3031 keepalive probes sent
        1 connections dropped by keepalive
7823 correct ACK header predictions
12533 correct data packet header predictions
80 syncache entries added
        0 retransmitted
        0 dupsyn
        4 dropped
        80 completed
        0 bucket overflow
        0 cache overflow
        0 reset
        0 stale
        0 aborted
        0 badack
        0 unreach
        0 zone failures
0 cookies sent
0 cookies received
1 SACK recovery episodes
1 segment retransmits in SACK recovery episodes
1 byte retransmits in SACK recovery episodes
71 SACK options (SACK blocks) received
1 SACK options (SACK blocks) sent
0 SACK scoreboard overflow
0 ACKs sent in response to in-window but not exact RSTs
0 ACKs sent in response to in-window SYNs on established connections
0 rcv packets dropped by TCP due to bad address
0 out-of-sequence segment drops due to insufficient memory
547024 RST packets
0 ICMP packets ignored by TCP
0 send packets dropped by TCP due to auth errors
0 rcv packets dropped by TCP due to auth errors
0 outgoing segments dropped due to policing

```

show system statistics tcp lcc (TX Matrix Router)

```
user@host> show system statistics tcp lcc 2
```

```
lcc2-re0:
```

```
-----
tcp:
```

```

21271 packets sent
    11069 data packets (12044 bytes)
    0 data packets (0 bytes) retransmitted
    0 resends initiated by MTU discovery
    10198 ack-only packets (10194 packets delayed)
    0 URG only packets
    0 window probe packets
    0 window update packets
    4 control packets
13363 packets received
    11073 acks (for 12044 bytes)
    0 duplicate acks
    0 acks for unsent data
    12895 packets (2400874 bytes) received in-sequence
    0 completely duplicate packets (0 bytes)
    0 old duplicate packets

```

```

        0 packets with some dup. data (0 bytes duped)
        0 out-of-order packets (0 bytes)
        0 packets (0 bytes) of data after window
        0 window probes
        0 window update packets
        0 packets received after close
        0 discarded for bad checksums
        0 discarded for bad header offset fields
        0 discarded because packet too short
    4 connection requests
    0 connection accepts
    0 bad connection attempts
    0 listen queue overflows
    4 connections established (including accepts)
    33 connections closed (including 0 drops)
        0 connections updated cached RTT on close
        0 connections updated cached RTT variance on close
        0 connections updated cached ssthresh on close
    0 embryonic connections dropped
    11073 segments updated rtt (of 11073 attempts)
0 retransmit timeouts
    0 connections dropped by rexmit timeout
    0 persist timeouts
    0 connections dropped by persist timeout
    0 keepalive timeouts
        0 keepalive probes sent
        0 connections dropped by keepalive
    464 correct ACK header predictions
    2172 correct data packet header predictions
    0 ACKs sent in response to in-window but not exact RSTs
    0 ACKs sent in response to in-window SYNs on established connections
    0 out-of-sequence segment drops due to insufficient memory
    0 RST packets
    0 ICMP packets ignored by TCP

```

show system statistics tcp (TX Matrix Plus Router)

```
user@host> show system statistics tcp
```

```
sfc0-re0:
```

```
-----
Tcp:
```

```

    10420 packets sent
        10203 data packets (2374613 bytes)
        0 data packets retransmitted (0 bytes)
        0 resends initiated by MTU discovery
        202 ack only packets (120 packets delayed)
        0 URG only packets
        0 window probe packets
        0 window update packets
        30 control packets
    16635 packets received
        9468 acks(for 2374674 bytes)
        32 duplicate acks
        0 acks for unsent data
        7764 packets received in-sequence(38286 bytes)
        20 completely duplicate packets(0 bytes)
        0 old duplicate packets
        0 packets with some duplicate data(0 bytes duped)
        0 out-of-order packets(0 bytes)

```



```

        0 packets of data after window(0 bytes)
        0 window probes
        356 window update packets
        0 packets received after close
        0 discarded for bad checksums
        0 discarded for bad header offset fields
        0 discarded because packet too short
    10 connection requests
    33 connection accepts
    0 bad connection attempts
    0 listen queue overflows
    34 connections established (including accepts)
    50 connections closed (including 0 drops)
        24 connections updated cached RTT on close
        24 connections updated cached RTT variance on close
        0 connections updated cached ssthresh on close
    9 embryonic connections dropped
    9468 segments updated rtt(of 9256 attempts)
    0 retransmit timeouts
        0 connections dropped by retransmit timeout
    0 persist timeouts
        0 connections dropped by persist timeout
    14 keepalive timeouts
        14 keepalive probes sent
        0 connections dropped by keepalive
    6220 correct ACK header predictions
    6625 correct data packet header predictions
    33 syncache entries added
        0 retransmitted
        0 dupsyn
        0 dropped
        33 completed
        0 bucket overflow
        0 cache overflow
        0 reset
        0 stale
        0 aborted
        0 badack
        0 unreach
        0 zone failures
    0 cookies sent
    0 cookies received
    0 SACK recovery episodes
    0 segment retransmits in SACK recovery episodes
    0 byte retransmits in SACK recovery episodes
    0 SACK options (SACK blocks) received
    0 SACK options (SACK blocks) sent
    0 SACK scoreboard overflow
    0 ACKs sent in response to in-window but not exact RSTs
    0 ACKs sent in response to in-window SYNs on established connections
    0 rcv packets dropped by TCP due to bad address
    0 out-of-sequence segment drops due to insufficient memory
    15 RST packets
    0 ICMP packets ignored by TCP
    0 send packets dropped by TCP due to auth errors
    0 rcv packets dropped by TCP due to auth errors
    0 outgoing segments dropped due to policing

```

```
1cc0-re0:
-----
```

Tcp:

```

1306 packets sent
    1251 data packets (161855 bytes)
    0 data packets retransmitted (0 bytes)
    0 resends initiated by MTU discovery
    51 ack only packets (1 packets delayed)
    0 URG only packets
    0 window probe packets
    0 window update packets
    6 control packets
1397 packets received
    1218 acks(for 161904 bytes)
    2 duplicate acks
    0 acks for unsent data
    612 packets received in-sequence(12495 bytes)
    0 completely duplicate packets(0 bytes)
    0 old duplicate packets
    0 packets with some duplicate data(0 bytes duped)
    0 out-of-order packets(0 bytes)
    0 packets of data after window(0 bytes)
    0 window probes
    22 window update packets
    0 packets received after close
    0 discarded for bad checksums
    0 discarded for bad header offset fields
    0 discarded because packet too short
1 connection requests
24 connection accepts
0 bad connection attempts
0 listen queue overflows
25 connections established (including accepts)
27 connections closed (including 0 drops)
    24 connections updated cached RTT on close
    24 connections updated cached RTT variance on close
    0 connections updated cached ssthresh on close
0 embryonic connections dropped
1218 segments updated rtt(of 1192 attempts)
0 retransmit timeouts
    0 connections dropped by retransmit timeout
0 persist timeouts
    0 connections dropped by persist timeout
0 keepalive timeouts
    0 keepalive probes sent
    0 connections dropped by keepalive
196 correct ACK header predictions
119 correct data packet header predictions
24 syncache entries added
    0 retransmitted
    0 dupsyn
    0 dropped
    24 completed
    0 bucket overflow
    0 cache overflow
    0 reset
    0 stale
    0 aborted
    0 badack
    0 unreach
    0 zone failures
0 cookies sent

```

```

0 cookies received
0 SACK recovery episodes
0 segment retransmits in SACK recovery episodes
0 byte retransmits in SACK recovery episodes
0 SACK options (SACK blocks) received
0 SACK options (SACK blocks) sent
0 SACK scoreboard overflow
0 ACKs sent in response to in-window but not exact RSTs
0 ACKs sent in response to in-window SYNs on established connections
0 rcv packets dropped by TCP due to bad address
0 out-of-sequence segment drops due to insufficient memory
2 RST packets
0 ICMP packets ignored by TCP
0 send packets dropped by TCP due to auth errors
0 rcv packets dropped by TCP due to auth errors
0 outgoing segments dropped due to policing

lcc1-re0:
-----
Tcp:
    1118 packets sent
        1066 data packets (131896 bytes)
        0 data packets retransmitted (0 bytes)
        0 resends initiated by MTU discovery
        48 ack only packets (2 packets delayed)
        0 URG only packets
        0 window probe packets
        0 window update packets
        6 control packets
    1215 packets received

```

show system statistics tcp (Junos OS Evolved)

```
user@host> show system statistics tcp
```

```

Tcp:
    2635574 packets sent
        0 window probe packets
    1124324 packets received
        0 discarded for bad checksums
        0 discarded for bad header offset fields
    3495 connection requests
    2371 bad connection attempts
    0 listen queue overflows
    1574 connections established (including accepts)
    1 embryonic connections dropped
        22 connections dropped by retransmit timeout
        3677 keepalive probes sent
        8 retransmitted
        17 reset
        0 aborted
    0 cookies sent
    0 cookies received
    199 SACK recovery episodes
    13743 segment retransmits in SACK recovery episodes
    0 out-of-sequence segment drops due to insufficient memory
    2365 RST packets

```

