



Junos[®] OS

Transport and Internet Protocols Feature Guide for Routing Devices

Release
13.2



Published: 2013-07-30

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

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Junos® OS Transport and Internet Protocols Feature Guide for Routing Devices

13.2

Copyright © 2013, 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 <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xi
	Documentation and Release Notes	xi
	Supported Platforms	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	xv
	Opening a Case with JTAC	xvi
Part 1	Overview	
Chapter 1	Junos OS IP Support Overview	3
	Junos OS Support for IPv4 Routing Protocols	3
	Junos OS Support for IPv6 Routing Protocols	4
Part 2	Configuration	
Chapter 2	Configuring Path MTU Discovery	9
	Configuring the Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections	9
	Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections	10
	Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections	10
	Configuring the Junos OS for IPv6 Path MTU Discovery	10
Chapter 3	Configuring ICMP Features	13
	Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages	13
	Configuring the Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages	13
	Configuring the Junos OS to Ignore ICMP Source Quench Messages	14
	Configuring the Junos OS to Disable Protocol Redirect Messages on the Router or Switch	14
	Configuring the Junos OS to Disable the Routing Engine Response to Multicast Ping Packets	15

Chapter 4	Configuring IPv6 Features	17
	Configuring the Junos OS for IPv6 Duplicate Address Detection Attempts	17
	Configuring the Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit	17
	Configuring the Junos OS to Enable Processing of IPv4-mapped IPv6 Addresses and 6PE Traceroutes	18
Chapter 5	Configuring Junos OS Settings for Port Security	19
	Configuring the Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses	19
	Configuring Password Authentication for Console Access to PICs	20
	Configuring Password Authentication for the Diagnostics Port	20
	TCP Headers with SYN and FIN Flags Set	21
	Configuring the Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set	22
	Configuring the Junos OS to Extend the Default Port Address Range	22
Chapter 6	Configuring ARP and Neighbor Discovery Options	23
	Configuring the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses	23
	Configuring Passive ARP Learning for Backup VRRP Routers or Switches	23
	Configuring a Delay in Gratuitous ARP Requests	24
	Configuring a Gratuitous ARP Request When an Interface is Online	24
	Configuring the Purging of ARP Entries	24
	Adjusting the ARP Aging Timer	25
	Disabling MAC Address Learning of Neighbors Through ARP or Neighbor Discovery for IPv4 and IPv6 Neighbors	26
Chapter 7	Configuring TCP Options	27
	Configuring the Junos OS to Disable TCP RFC 1323 Extensions	27
	Configuring the Junos OS to Disable the TCP RFC 1323 PAWS Extension	27
	Configuring TCP MSS for Session Negotiation	28
	Configuring TCP MSS on T Series and M Series Routers	28
	Configuring TCP MSS on J Series Services Routers	29
	Configuring the Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets	29
Chapter 8	Configuration Statements	31
	System Management Configuration Statements	31
	allow-6pe-traceroute	38
	allow-v4mapped-packets	38
	arp (System)	39
	auxiliary	40
	console (System Ports)	41
	default-address-selection	42
	diag-port-authentication	43
	extended-statistics	44
	gratuitous-arp-delay	44
	gratuitous-arp-on-ifup	45
	gre-path-mtu-discovery	45

	icmpv4-rate-limit	46
	icmpv6-rate-limit	47
	interfaces (ARP Aging Timer)	48
	internet-options	49
	ipip-path-mtu-discovery	50
	ipv6-duplicate-addr-detection-transmits	51
	ipv6-path-mtu-discovery	51
	ipv6-path-mtu-discovery-timeout	52
	ipv6-reject-zero-hop-limit	52
	no-multicast-echo	53
	no-ping-record-route	54
	no-ping-time-stamp	54
	no-redirects (IPv4 Traffic)	55
	no-tcp-rfc1323-paws	56
	no-tcp-rfc1323	56
	passive-learning	57
	purging	57
	path-mtu-discovery	58
	source-quench	58
	system	59
	tcp-drop-synfin-set	59
	tcp-mss	60
Part 3	Administration	
Chapter 9	Monitoring Commands	63
	show system statistics arp	64
	show system statistics icmp	71
	show system statistics icmp6	76
	show system statistics igmp	82
	show system statistics ip	86
	show system statistics ip6	94
	show system statistics tcp	101
Part 4	Index	
	Index	111

List of Figures

Part 2	Configuration	
Chapter 5	Configuring Junos OS Settings for Port Security	19
	Figure 1: TCP Header with SYN and FIN Flags Set	21

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xiii
	Table 2: Text and Syntax Conventions	xiii
Part 2	Configuration	
Chapter 7	Configuring TCP Options	27
	Table 3: Source Address Selection	30

About the Documentation

- Documentation and Release Notes on page xi
- Supported Platforms 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 <http://www.juniper.net/techpubs/>.

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 <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- M Series
- MX Series
- T Series
- J Series
- PTX Series

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.xsl;
    }
  }
}
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 the *CLI User Guide*.

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.

Table 2 on page xiii 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

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

Convention	Description	Examples
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies book 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 System Basics Configuration 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)	Enclose 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)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify 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		
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, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (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 JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>

- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

- [Junos OS IP Support Overview on page 3](#)

CHAPTER 1

Junos OS IP Support Overview

- [Junos OS Support for IPv4 Routing Protocols on page 3](#)
- [Junos OS Support for IPv6 Routing Protocols on page 4](#)

Junos OS Support for IPv4 Routing Protocols

The Junos operating system (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 4](#)

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 3](#)

PART 2

Configuration

- [Configuring Path MTU Discovery on page 9](#)
- [Configuring ICMP Features on page 13](#)
- [Configuring IPv6 Features on page 17](#)
- [Configuring Junos OS Settings for Port Security on page 19](#)
- [Configuring ARP and Neighbor Discovery Options on page 23](#)
- [Configuring TCP Options on page 27](#)
- [Configuration Statements on page 31](#)

CHAPTER 2

Configuring Path MTU Discovery

- [Configuring the Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections on page 9](#)
- [Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 10](#)
- [Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 10](#)
- [Configuring the Junos OS for IPv6 Path MTU Discovery on page 10](#)

Configuring the 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 the Junos OS for IPv6 Path MTU Discovery on page 10](#)
- [Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 10](#)
- [Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 10](#)
- [ipip-path-mtu-discovery on page 50](#)

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;
```

Related Documentation

- [Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 10](#)

Configuring the 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 10](#)
- [Configuring the Junos OS to Ignore ICMP Source Quench Messages on page 14](#)

Configuring the 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 the Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections on page 9](#)
- [Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 10](#)
- [Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 10](#)

CHAPTER 3

Configuring ICMP Features

- [Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages on page 13](#)
- [Configuring the Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 13](#)
- [Configuring the Junos OS to Ignore ICMP Source Quench Messages on page 14](#)
- [Configuring the Junos OS to Disable Protocol Redirect Messages on the Router or Switch on page 14](#)
- [Configuring the Junos OS to Disable the Routing Engine Response to Multicast Ping Packets on page 15](#)

Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages

To limit the rate at which ICMPv4 messages can be generated by the Routing Engine and sent to the Routing Engine, include the **icmpv4-rate-limit** statement at the **[edit system internet-options]** hierarchy level:

icmpv4-rate-limit bucket-size *bucket-size* packet-rate *packet-rate*;

The bucket size is 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 4,294,967,295. The default value is 1000.

Related Documentation

- [Configuring the Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 13](#)

Configuring the 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**
- [Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages on page 13](#)

Configuring the 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**
- [Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages on page 13](#)
 - [Configuring the Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 13](#)

Configuring the 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.

- Related Documentation**
- [Configuring the Junos OS to Ignore ICMP Source Quench Messages on page 14](#)
 - [Configuring the Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets](#)
 - [Junos OS Network Interfaces Library for Routing Devices](#)

Configuring the 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 the Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses on page 19](#)

CHAPTER 4

Configuring IPv6 Features

- [Configuring the Junos OS for IPv6 Duplicate Address Detection Attempts on page 17](#)
- [Configuring the Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit on page 17](#)
- [Configuring the Junos OS to Enable Processing of IPv4-mapped IPv6 Addresses and 6PE Traceroutes on page 18](#)

Configuring the 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 4](#)
- [Configuring the Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit on page 17](#)
- [Configuring the Junos OS for IPv6 Path MTU Discovery on page 10](#)

Configuring the 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 10](#)
- [Configuring the Junos OS for IPv6 Duplicate Address Detection Attempts on page 17](#)

Configuring the 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 38](#)
 - [allow-6pe-traceroute on page 38](#)

CHAPTER 5

Configuring Junos OS Settings for Port Security

- [Configuring the Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses on page 19](#)
- [Configuring Password Authentication for Console Access to PICs on page 20](#)
- [Configuring Password Authentication for the Diagnostics Port on page 20](#)
- [TCP Headers with SYN and FIN Flags Set on page 21](#)
- [Configuring the Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set on page 22](#)
- [Configuring the Junos OS to Extend the Default Port Address Range on page 22](#)

Configuring the 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.

- Related Documentation**
- [Configuring the Junos OS to Disable the Routing Engine Response to Multicast Ping Packets on page 15](#)

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 the Junos OS to Set Console and Auxiliary Port Properties](#)
 - [Configuring Password Authentication for the Diagnostics Port on page 20](#)

Configuring Password Authentication for the Diagnostics Port

If you have been asked by Customer Support personnel to connect a physical console to a control board or forwarding component on the router (such as the System Control Board [SCB], System and Switch Board [SSB], or Switching and Forwarding Module [SFM]) to perform diagnostics, you can configure a password on the diagnostics port. This password provides an extra level of security.

To configure a password on the diagnostics port, include the **diag-port-authentication** statement at the **[edit system]** hierarchy level:

```
[edit system]
diag-port-authentication (encrypted-password "password" | plain-text-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.

You can use an MD5 password, or you can enter a plain-text password that the Junos OS encrypts (using MD5-style encryption) before it places it into the password database. For an MD5 password, specify the password in the configuration. Null-password (empty) is not permitted.

If you configure the **plain-text-password** option, the CLI prompts you for the password.

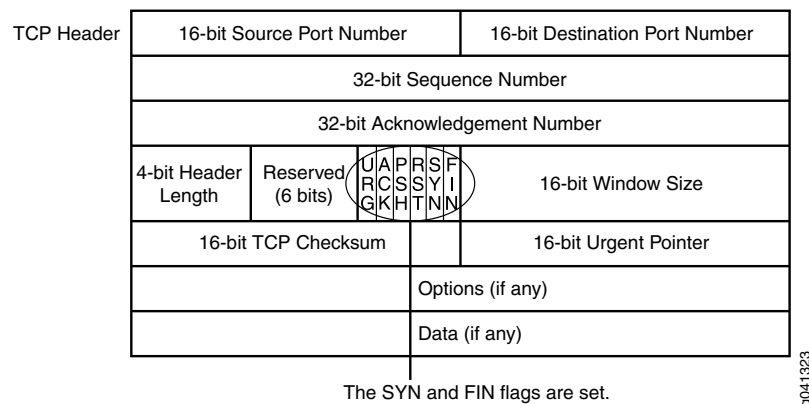
For routers that have more than one SSB, the same password is used for both SSBs.

Related Documentation • [Configuring Password Authentication for Console Access to PICs on page 20](#)

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 21](#).

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 59](#)

Configuring the 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 the Junos OS to Disable TCP RFC 1323 Extensions on page 27](#)
- [Configuring the Junos OS to Extend the Default Port Address Range on page 22](#)
[tcp-drop-synfin-set on page 59](#)

Configuring the 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 the 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.

Related Documentation

- [Configuring the Junos OS to Disable TCP RFC 1323 Extensions on page 27](#)
- [Configuring the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 23](#)
- *source-port*

CHAPTER 6

Configuring ARP and Neighbor Discovery Options

- [Configuring the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 23](#)
- [Disabling MAC Address Learning of Neighbors Through ARP or Neighbor Discovery for IPv4 and IPv6 Neighbors on page 26](#)

Configuring the 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 23](#)
2. [Configuring a Delay in Gratuitous ARP Requests on page 24](#)
3. [Configuring a Gratuitous ARP Request When an Interface is Online on page 24](#)
4. [Configuring the Purging of ARP Entries on page 24](#)
5. [Adjusting the ARP Aging Timer on page 25](#)

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 26](#)

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

- [Configuring the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 23](#)
- [Ethernet Interfaces](#)

CHAPTER 7

Configuring TCP Options

- [Configuring the Junos OS to Disable TCP RFC 1323 Extensions on page 27](#)
- [Configuring the Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 27](#)
- [Configuring TCP MSS for Session Negotiation on page 28](#)
- [Configuring the Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets on page 29](#)

Configuring the 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 the Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 27](#)
- [Configuring the Junos OS to Extend the Default Port Address Range on page 22](#)
- [no-tcp-rfc1323-paws on page 56](#)

Configuring the 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 the Junos OS to Disable TCP RFC 1323 Extensions on page 27](#)
- [Configuring the Junos OS to Extend the Default Port Address Range on page 22](#)
- [no-tcp-rfc1323 on page 56](#)

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 could 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 sections describe how to configure TCP MSS on T Series and M Series routers and J Series Services Routers, respectively:

1. [Configuring TCP MSS on T Series and M Series Routers on page 28](#)
2. [Configuring TCP MSS on J Series Services Routers on page 29](#)

Configuring TCP MSS on T Series and M Series Routers

To specify a TCP MSS value on T Series and M Series routers, 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.

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 on J Series Services Routers

To specify a TCP MSS value on a J Series Services Router, include the following statement at the **[edit system internet-options]** hierarchy level:

```
[edit system internet-options]
tcp-mss {
  mss-value;
}
```

The range of the **mss-value** parameter is from 64 through 65535 bytes.

To remove the TCP MSS specification, use the following command:

```
delete system internet-options tcp-mss
```

For more information about configuring TCP MSS and session negotiation on J Series Services Routers, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

Related Documentation

- [Configuring the Junos OS to Disable TCP RFC 1323 Extensions on page 27](#)
- [Configuring the Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 27](#)

Configuring the 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 the Junos OS to Disable Protocol Redirect Messages on the Router or Switch on page 14](#)
- [default-address-selection on page 42](#)

Configuration Statements

- [System Management Configuration Statements on page 31](#)

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 {
    events [ login change-log interactive-commands ];
    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;
        }
      }
    }
  }
  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 {
    commit 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 ];
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 {
  password-protocol mschap-v2;
}
attributes {
  nas-ip-address ip-address;
}
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;
    }
    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";
        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 {  
    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 (GMThour-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	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 the Junos OS to Enable Processing of IPv4-mapped IPv6 Addresses and 6PE Traceroutes on page 18• allow-v4mapped-packets on page 38

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 the Junos OS to Enable Processing of IPv4-mapped IPv6 Addresses and 6PE Traceroutes on page 18• allow-6pe-traceroute on page 38

arp (System)


Syntax	<pre>arp { aging-timer <i>minutes</i>; gratuitous-arp-delay <i>seconds</i>; gratuitous-arp-on-ifup; interfaces { interface-name { aging-timer <i>minutes</i>; } } passive-learning; purging; }</pre> <p>For EX-Series switches:</p> <pre>arp { aging-timer <i>minutes</i>; }</pre>
Hierarchy Level	[edit system]
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> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
Description	<p>Specify ARP options. 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.</p> <p>For EX-Series switches, set only the time interval between ARP updates.</p>
Options	<p>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.</p> <p>passive-learning (QFX-Series only)—Configure switches to learn the ARP mappings (IP-to-MAC address) for hosts sending the requests.</p> <p>Default: 20 minutes</p> <p>Range: 1 to 240 minutes</p> <p>The remaining statements are explained separately.</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 the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 23 • <i>Junos OS Network Interfaces Library for Routing Devices</i>

- For more information about ARP updates, see the [Junos OS System Basics Configuration Guide](#).

auxiliary

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


console (System Ports)

Syntax	<pre>console { 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>
Description	Configure the characteristics of the console port.
Default	The console port is enabled and its speed is 9600 baud.
Options	<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>
	<div>  <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.</p> </div>
	<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.</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 the Junos OS to Set Console and Auxiliary Port Properties</i>

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, but not 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	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 to Select a Fixed Source Address for Locally Generated TCP/IP Packets on page 29• <i>Junos OS Network Interfaces Library for Routing Devices</i>

diag-port-authentication

Syntax	diag-port-authentication (encrypted-password " <i>password</i> " plain-text-password);
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="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	<ul style="list-style-type: none"> • Configuring Password Authentication for the Diagnostics Port on page 20

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	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

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, 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 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	system—To view this statement in the configuration.
Level	system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 23

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 the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 23

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	<p>Configure path MTU discovery for outgoing GRE tunnel connections:</p> <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 10

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">• Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages on page 13

icmpv6-rate-limit

Syntax	icmpv6-rate-limit { bucket-size <i>seconds</i> ; packet-rate <i>packet-rate</i> ; }
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 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	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 the Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 13

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 240
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 25

internet-options

Syntax	<pre> internet-options { (gre-path-mtu-discovery no-gre-path-mtu-discovery); icmpv4-rate-limit bucket-size <i>bucket-size</i> packet-rate <i>packet-rate</i>; icmpv6-rate-limit bucket-size <i>bucket-size</i> packet-rate <i>packet-rate</i>; (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-rfc1323; no-tcp-rfc1323-paws; (path-mtu-discovery no-path-mtu-discovery); source-port upper-limit <<i>upper-limit</i>>; (source-quench no-source-quench); tcp-drop-synfin-set; tcp-mss <i>mss-value</i>; } </pre>
Hierarchy Level	[edit system]
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 system IP options to protect against certain types of DoS attacks.</p> <p>The remaining statements are explained separately.</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 the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages on page 13 • Configuring the Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages on page 13 • Configuring the Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections on page 9 • Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections on page 10 • Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 10 • Configuring the Junos OS for IPv6 Duplicate Address Detection Attempts on page 17 • Configuring the Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit on page 17 • Configuring the Junos OS to Ignore ICMP Source Quench Messages on page 14

- [Configuring the Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set on page 22](#)
- [Configuring the Junos OS to Disable TCP RFC 1323 Extensions on page 27](#)
- [Configuring the Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 27](#)
- [Configuring the Junos OS to Extend the Default Port Address Range on page 22](#)
- [Configuring TCP MSS on J Series Services Routers on page 29](#)

ipip-path-mtu-discovery

Syntax	(<code>ipip-path-mtu-discovery</code> <code>no-ipip-path-mtu-discovery</code>);
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 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 the Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections on page 9• internet-options on page 49

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 17

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 the Junos OS for IPv6 Path MTU Discovery on page 10

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	<i>minutes</i> —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 the Junos OS for IPv6 Path MTU Discovery on page 10

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 the Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit on page 17

no-multicast-echo

```

Syntax  no-multicast-echo {
            arp {
                aging-timer minutes;
                gratuitous-arp-delay seconds;
                gratuitous-arp-on-ifup;
                interfaces {
                    interface-name {
                        aging-timer minutes;
                    }
                }
            }
            passive-learning;
            purging;
        }
        host-name hostname;
        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;
        }
    }
    license {
        autoupdate URL;
    }
    renew before-expiration (number | interval number)
}

```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 8.1.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

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**
- [Configuring the Junos OS to Disable the Routing Engine Response to Multicast Ping Packets on page 15](#)

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.
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	• Configuring the Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses on page 19

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.
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	• Configuring the Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses on page 19

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.
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 the Junos OS to Disable Protocol Redirect Messages on the Router or Switch on page 14 • <i>Understanding the Protocol Redirect Mechanism on EX Series Switches</i> • <i>Configuring Junos OS to Disable Sending Protocol Redirect Messages on EX Series 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 the Junos OS to Disable the TCP RFC 1323 PAWS Extension on page 27

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 the Junos OS to Disable TCP RFC 1323 Extensions on page 27

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.
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 ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 23

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 the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses on page 23

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 the Junos OS for Path MTU Discovery on Outgoing TCP Connections on page 10

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	Configure how the Junos OS handles Internet Control Message Protocol (ICMP) source quench messages: <ul style="list-style-type: none">• source-quench—The Junos OS ignores ICMP source quench messages.• no-source-quench—The Junos OS does not ignore ICMP source quench messages.
Default	The Junos OS does not ignore ICMP source quench 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 the Junos OS to Ignore ICMP Source Quench Messages on page 14

system

Syntax	system { ... }
Hierarchy Level	[edit]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure system management properties.
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"> • System Management Configuration Statements on page 31

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 the Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set on page 22 • TCP Headers with SYN and FIN Flags Set on page 21

tcp-mss

Syntax	<code>tcp-mss mss-value;</code>
Hierarchy Level	[edit system internet-options]
Release Information	Statement introduced in Junos OS Release 9.2 of J Series Services Routers software.
Description	<p>(J Series Services Routers only) 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>
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 on J Series Services Routers on page 29

PART 3

Administration

- [Monitoring Commands on page 63](#)

CHAPTER 9

Monitoring Commands

show system statistics arp

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> <p>Replace <i>number</i> with the following values depending on the LCC configuration:</p> <ul style="list-style-type: none">• 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 65](#)
[show system statistics arp \(EX Series Switches\) on page 66](#)
[show system statistics arp \(TX Matrix Plus Router\) on page 66](#)

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 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
```

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 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
```

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

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. Replace <i>number</i> with the following values depending on the LCC configuration:</p> <ul style="list-style-type: none"> • 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 72](#)
[show system statistics icmp \(EX Series Switches\) on page 73](#)
[show system statistics icmp \(TX Matrix Plus Router\) on page 73](#)

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

Syntax	show system statistics icmp6
Syntax (EX Series Switches)	show system statistics icmp6 <all-members> <local> <member <i>member-id</i> >
Syntax (TX Matrix Router)	show system statistics icmp6 <all-chassis all-lcc lcc <i>number</i> scc>
Syntax (TX Matrix Plus Router)	show system statistics icmp6 <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 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> <p>Replace <i>number</i> with the following values depending on the LCC configuration:</p> <ul style="list-style-type: none">• 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 on page 77](#)
[show system statistics icmp6 \(EX Series Switches\) on page 78](#)
[show system statistics icmp6 \(TX Matrix Plus Router\) on page 79](#)

Sample Output

show system statistics icmp6

```
user@host> show system statistics icmp6
icmp6:
  23224 Calls to icmp_error
  0 Errors not generated because old message was icmp error
  24491 Errors not generated because rate limitation
  Output histogram:
    12 unreachable
    15500 parameter problem
    206 echo
    33863 echo reply
    2413 multicast listener query
    12 multicast listener report
    302 router advertisement
    192 neighbor solicitation
    58 neighbor advertisement
  0 Messages with bad code fields
  0 Messages < minimum length
  0 Bad checksums
  0 Messages with bad length
  Input histogram:
    5012 unreachable
    5000 packet too big
```



```

5000 time exceeded
5000 parameter problem
33863 echo
5091 echo reply
5010 multicast listener query
5020 multicast listener report
5000 multicast listener done
5000 router solicitation
5000 router advertisement
5030 neighbor solicitation
5060 neighbor advertisement
5000 redirect
5000 router renumbering
5000 node information request
5000 node information reply
5000 Version 2 Multicast Listener Report
0 No route
0 Administratively prohibited
0 Beyond scope
12 Address unreachable
0 Port unreachable
0 packet too big
0 Time exceed transit
0 Time exceed reassembly
0 Erroneous header field
23212 Unrecognized next header
0 Unrecognized option
0 redirect
0 Unknown
33863 Message responses generated
0 Messages with too many ND options

```

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

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.
Description	Display system-wide Internet Group Management Protocol (IGMP) statistics.
Options	<p>none—Display system statistics for IGMP.</p> <p>all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display system statistics for IGMP 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 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.</p> <p>all-members—(EX4200 switches only) (Optional) Display IGMP 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 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 <i>number</i> with the following values depending on the LCC configuration:</p> <ul style="list-style-type: none">• 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 83](#)
[show system statistics igmp \(EX Series Switches\) on page 83](#)
[show system statistics igmp \(TX Matrix Plus Router\) on page 84](#)

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

Syntax	show system statistics ip
Syntax (EX Series Switches)	show system statistics ip <all-members> <local> <member <i>member-id</i> >
Syntax (TX Matrix Router)	show system statistics ip <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 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. Replace <i>number</i> with the following values depending on the LCC configuration:</p> <ul style="list-style-type: none">• 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 87](#)
[show system statistics ip \(EX Series Switches\) on page 88](#)
[show system statistics ip \(TX Matrix Plus Router\) on page 89](#)

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 fragments dropped (queue overflow)
    0 fragments dropped after timeout
    0 fragments dropped due to over limit
    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 fragments dropped (queue overflow)
0 fragments dropped after timeout
0 fragments dropped due to over limit
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 fragments dropped (queue overflow)
0 fragments dropped after timeout
0 fragments dropped due to over limit
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 fragments dropped (queue overflow)
0 fragments dropped after timeout
0 fragments dropped due to over limit
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 recv 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 fragments dropped (queue overflow)
0 fragments dropped after timeout
0 fragments dropped due to over limit
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 fragments dropped (queue overflow)
0 fragments dropped after timeout
0 fragments dropped due to over limit
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 fragments dropped (queue overflow)
0 fragments dropped after timeout
0 fragments dropped due to over limit
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 rcv buffer

show system statistics ip6

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. Replace <i>number</i> with the following values depending on the LCC configuration:</p> <ul style="list-style-type: none">• 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 95](#)
[show system statistics ip6 \(EX Series Switches\) on page 96](#)
[show system statistics ip6 \(TX Matrix Router\) on page 96](#)

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 fragments that exceeded limit
  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
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 fragments that exceeded limit
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 fragments that exceeded limit
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

```

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 fragments that exceeded limit
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
```

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 fragments that exceeded limit
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 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

```

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 fragments that exceeded limit
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 fragments that exceeded limit
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

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> <p>Replace <i>number</i> with the following values depending on the LCC configuration:</p> <ul style="list-style-type: none"> • 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 102](#)
[show system statistics tcp \(EX Series Switches\) on page 103](#)
[show system statistics tcp lcc \(TX Matrix Router\) on page 105](#)
[show system statistics tcp \(TX Matrix Plus Router\) on page 106](#)

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
```


PART 4

Index

- [Index on page 111](#)

Index

Symbols

#, comments in configuration statements.....	xiv
(), in syntax descriptions.....	xiv
< >, in syntax descriptions.....	xiv
[], in configuration statements.....	xiv
{ }, in configuration statements.....	xiv
(pipe), in syntax descriptions.....	xiv

A

addresses	
router source addresses.....	29, 42
aging timer	
ARP.....	25
allow-v4mapped-packets statement.....	38
ARP	
aging timer.....	25
arp.....	39
arp statement.....	39
usage guidelines.....	23
authentication	
diagnostics port.....	20
diagnostics port password.....	43
auxiliary statement.....	40

B

braces, in configuration statements.....	xiv
brackets	
angle, in syntax descriptions.....	xiv
square, in configuration statements.....	xiv
bucket-size statement	
ICMPv4.....	46
usage guidelines.....	13
ICMPv6.....	47
usage guidelines.....	13

C

comments, in configuration statements.....	xiv
console statement	
physical port.....	41
conventions	
text and syntax.....	xiii

curly braces, in configuration statements.....	xiv
customer support.....	xv
contacting JTAC.....	xv

D

default-address-selection statement.....	42
usage guidelines.....	29
diag-port-authentication statement.....	43
usage guidelines.....	20
diagnostics port password.....	20, 43
documentation	
comments on.....	xv

F

font conventions.....	xiii
-----------------------	------

G

gratuitous-arp-delay statement.....	44
gratuitous-arp-on-ifup statement.....	45
gre-path-mtu-discovery statement.....	45
usage guidelines.....	10

I

icmpv4-rate-limit statement.....	46
usage guidelines.....	13
icmpv6-rate-limit statement.....	47
usage guidelines.....	13
insecure statement.....	41
interfaces statement	
ARP.....	48
internet-options statement.....	49
usage guidelines.....	9, 10, 13, 27, 28
IP packets	
router source addresses.....	29, 42
ipip-path-mtu-discovery statement.....	50
usage guidelines.....	9
ipv6-duplicate-addr-detection-transmits	
statement.....	51
usage guidelines.....	17
ipv6-path-mtu-discovery statement.....	51
usage guidelines.....	10
ipv6-path-mtu-discovery-timeout statement.....	52
ipv6-reject-zero-hop-limit statement.....	52
usage guidelines.....	17

L

lo0 interface.....	29, 42
log-out-on-disconnect statement.....	41

M

manuals	
comments on.....	xv
messages	
redirect.....	14

N

no-gre-path-mtu-discovery statement.....	45
no-ipip-path-mtu-discovery statement.....	50
no-multicast-echo statement.....	53
usage guidelines.....	15
no-path-mtu-discovery statement.....	58
no-ping-record-route statement.....	54
no-ping-time-stamp statement.....	54
no-redirects statement.....	55
usage guidelines.....	14
no-source-quench statement.....	58
no-tcp-rfc1323 statement.....	56
usage guidelines.....	27
no-tcp-rfc1323-paws statement.....	56
usage guidelines.....	27

P

packet-rate statement	
ICMPv4.....	46
usage guidelines.....	13
ICMPv6.....	47
usage guidelines.....	13
packets	
router source addresses.....	29, 42
parentheses, in syntax descriptions.....	xiv
passive ARP learning	
VRRP.....	23
passive-learning statement.....	57
passwords	
diagnostics port	20, 43
path-mtu-discovery statement.....	58
usage guidelines.....	10
pic-console-authentication statement	
usage guidelines.....	20
plain-text passwords	
for a diagnostic port.....	20
ports	
diagnostics port.....	20, 43
protocols	
redirect messages.....	14
purging statement.....	57

R

redirect messages	
disabling.....	14
routers	
ports	
diagnostics port.....	20, 43
redirect	14
source addresses.....	29, 42
routing protocol process	
IPv6 routing protocols.....	4

S

show system statistics arp command.....	64
show system statistics icmp command.....	71
show system statistics icmp6 command.....	76
show system statistics igmp command.....	82
show system statistics ip command.....	86
show system statistics ip6 command.....	94
show system statistics tcp command.....	101
source-port statement	
usage guidelines.....	22
source-quench statement.....	58
usage guidelines.....	14
support, technical See technical support	
syntax conventions.....	xiii
system statement.....	59
usage guidelines.....	31

T

tcp-drop-synfin-set statement.....	59
usage guidelines.....	22
tcp-mss statement.....	60
usage guidelines.....	28
technical support	
contacting JTAC.....	xv
type statement	
console port.....	41

V

VRRP	
passive ARP learning.....	23