



Junos[®] OS

Traffic Sampling, Forwarding, and Monitoring Feature Guide for Routing Devices

Release
15.1



Modified: 2016-09-14

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

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.

Junos[®] OS Traffic Sampling, Forwarding, and Monitoring Feature Guide for Routing Devices

15.1

Copyright © 2016, 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	xiii
	Documentation and Release Notes	xiii
	Supported Platforms	xiii
	Using the Examples in This Manual	xiii
	Merging a Full Example	xiv
	Merging a Snippet	xiv
	Documentation Conventions	xv
	Documentation Feedback	xvii
	Requesting Technical Support	xvii
	Self-Help Online Tools and Resources	xvii
	Opening a Case with JTAC	xviii
Chapter 1	Overview	19
	Traffic Sampling, Forwarding, and Monitoring Overview	19
Chapter 2	Collecting Traffic Samples for Network Monitoring	21
	Minimum Traffic Sampling Configuration	21
	Configuring Traffic Sampling	22
	Disabling Traffic Sampling	24
	Collecting Traffic Sampling Output in a File	24
	Traffic Sampling Output Format	25
	Directing Traffic Sampling Output to a Server Running the cflowd Application	26
	Debugging cflowd Flow Aggregation	28
	Collecting Traffic Sampling Output in the Cisco Systems NetFlow Services Export Version 9 Format	29
	Example: Configuring Active Flow Monitoring Using Version 9	30
	Example: Sampling a Single SONET/SDH Interface	30
	Example: Sampling All Traffic from a Single IP Address	31
	Example: Sampling All FTP Traffic	32
	Tracing Traffic-Sampling Operations	33
Chapter 3	Configuring Traffic Forwarding for Network Monitoring	35
	Configuring Traffic Forwarding and Monitoring	35
	Configuring IPv6 Accounting	39
	Configuring Discard Accounting	40
	Configuring Active Flow Monitoring on PTX Series Packet Transport Routers	42
	Configuring Passive Flow Monitoring	44
	Configuring Port Mirroring	45
	Port Mirroring Configuration Guidelines	46
	Configuring Port Mirroring	47
	Configuring the Port-Mirroring Address Family and Interface	47

	Configuring Multiple Port-Mirroring Instances	47
	Configuring Port-Mirroring Instances	48
	Associating a Port-Mirroring Instance on M320 Routers	48
	Associating a Port-Mirroring Instance on M120 Routers	49
	Configuring MX Series 3D Universal Edge Routers and M120 Routers to Mirror Traffic Only Once	49
	Configuring Next-Hop Groups to Use Multiple Interfaces to Forward Packets Used in Port Mirroring	49
	Defining a Port-Mirroring Firewall Filter	51
	Defining a Next-Hop Group for Port Mirroring	53
Chapter 4	Configuring Forwarding Table Filters to Efficiently Route Traffic	57
	Configuring Forwarding Table Filters	57
	Forwarding Table Filters for Routing Instances on ACX Series Routers	59
	Applying Forwarding Table Filters	60
Chapter 5	Configuring Forwarding Options for Load Balancing Traffic	63
	Configuring Load Balancing for Ethernet Pseudowires	63
	Configuring Load-Balance Groups	65
	Understanding Per-Packet Load Balancing	65
	Configuring Per-Packet Load Balancing	66
	Per-Packet Load Balancing Examples	68
	Per-Flow and Per-Prefix Load Balancing Overview	69
	Configuring Per-Prefix Load Balancing	69
	Configuring Per-Flow Load Balancing Based on Hash Values	70
	Understanding ECMP Flow-Based Forwarding	71
	Example: Configuring ECMP Flow-Based Forwarding	72
	Configuring Load Balancing Based on MAC Addresses	76
	Load Balancing VPLS Non-Unicast Traffic Across Member Links of an Aggregate Interface	77
	Example: Configuring Multicast Load Balancing over Aggregated Ethernet Links	78
Chapter 6	Configuring Other Forwarding Options	91
	Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents	91
	Configuring DNS and TFTP Packet Forwarding	94
	Tracing BOOTP, DNS, and TFTP Forwarding Operations	95
	Configuring the Log Filename	96
	Configuring the Number and Size of Log Files	96
	Configuring Access to the Log File	96
	Configuring a Regular Expression for Lines to Be Logged	96
	Example: Configuring DNS Packet Forwarding	97
	Preventing DHCP Spoofing on MX Series 3D Universal Edge Routers	97
Chapter 7	Configuration Statements	99
	accounting	102
	aggregation	103
	autonomous-system-type	104
	bootp	105

burn-hashing	106
cflowd (Discard Accounting)	107
cflowd (Flow Monitoring)	108
client-address	108
client-response-ttl	109
description (Forwarding Options)	109
dhcp-relay (DHCP Spoofing Prevention)	110
disable (Forwarding Options)	111
domain	112
export-format	112
enhanced-hash-key	113
family (Filtering)	117
family (Monitoring)	118
family (Port Mirroring)	119
family (Sampling)	121
family inet	123
family mpls	125
family multiservice	128
file (Extended DHCP Relay Agent and Helpers Trace Options)	130
file (Sampling)	130
file (Trace Options)	131
filename (Sampling)	131
files (Sampling and Traceoptions)	132
filter (IPv4, IPv6, and MPLS)	132
filter (VPLS)	133
flood	133
flow-active-timeout	134
flow-export-destination	134
flow-inactive-timeout	135
flow-server	136
group (DHCP Spoofing Prevention)	137
gtp-tunnel-endpoint-identifier	138
hash-key (Forwarding Options)	139
helpers	142
hosted-service-identifier	144
hosted-services	144
hyper-mode (forwarding-options)	145
indexed-load-balance	146
input (Forwarding Table)	147
input (Port Mirroring)	147
input (Sampling)	148
instance	149
interface (Accounting or Sampling)	150
interface (BOOTP)	151
interface (DHCP Spoofing Prevention)	152
interface (DNS and TFTP Packet Forwarding or Relay Agent)	153
interface (Monitoring)	154
interface (Next-Hop Group)	155
interface (Port Mirroring)	155

link-layer-broadcast-inet-check	156
load-balance (Forwarding Options)	157
load-balance-group	159
local-dump	159
max-packets-per-second	160
maximum-hop-count	160
maximum-packet-length	161
minimum-wait-time	162
mirror-once	163
monitoring	164
next-hop (Forwarding Options)	165
next-hop-group (Forwarding Options)	166
next-hop-group	167
no-filter-check	168
no-listen	168
output (Accounting)	169
output (Forwarding Table)	170
output (Monitoring)	171
output (Port Mirroring)	172
output (Sampling)	173
per-flow	174
per-prefix	175
port (cflowd)	175
port (Packet Forwarding)	176
port-mirroring	178
rate (Forwarding Options)	180
relay-agent-option	181
route-accounting	181
run-length	182
sampling (Forwarding Options)	183
server (DHCP and BOOTP Relay Agent)	186
server (DNS and TFTP Service)	187
server-address (Hosted Services)	187
server-profile	188
server-profile (Active Flow Monitoring)	188
size (Sampling and Traceoptions)	189
source-checking	190
stamp	191
tftp	191
traceoptions (DNS and TFTP Packet Forwarding)	192
traceoptions (Port Mirroring and Traffic Sampling)	194
version	194
version9	195
world-readable (Forwarding Options)	196
Chapter 8	
Operational Commands	197
clear passive-monitoring statistics	199
clear services flow-collector statistics	200
request services flow-collector change-destination primary interface	201

request services flow-collector change-destination secondary interface	202
request services flow-collector test-file-transfer	203
show chassis forwarding	204
show forwarding-options hyper-mode	205
show forwarding-options port-mirroring	206
show forwarding-options next-hop-group	208
show interfaces (Flow Monitoring)	211
show interfaces (M Series, MX Series, T Series Routers, and PTX Series Management and Internal Ethernet)	216
show interfaces statistics	232
show passive-monitoring error	244
show passive-monitoring flow	246
show passive-monitoring memory	248
show passive-monitoring status	250
show passive-monitoring usage	252
show route forwarding-table	254
show services accounting aggregation	268
show services accounting aggregation template	272
show services accounting errors	273
show services accounting flow	277
show services accounting flow-detail	282
show services accounting memory	287
show services accounting packet-size-distribution	289
show services accounting status	291
show services accounting usage	294
show services flow-collector file interface	296
show services flow-collector input interface	298
show services flow-collector interface	300
Chapter 9	
Index	307
Index	309

List of Figures

Chapter 2	Collecting Traffic Samples for Network Monitoring	21
	Figure 1: Configure Sampling Rate	23
Chapter 5	Configuring Forwarding Options for Load Balancing Traffic	63
	Figure 2: Simple Load Balancing Scenario	66
	Figure 3: ECMP Routes	73
	Figure 4: Multicast Load Balancing over Aggregated Ethernet Links	79

List of Tables

	About the Documentation	xiii
	Table 1: Notice Icons	xv
	Table 2: Text and Syntax Conventions	xvi
Chapter 8	Operational Commands	197
	Table 3: show chassis forwarding Output Fields	204
	Table 4: show forwarding-options hyper-mode Output Fields	205
	Table 5: show forwarding-options port-mirroring Output Fields	206
	Table 6: show forwarding-options next-hop-group Output Fields	208
	Table 7: show interfaces Output Fields (Flow Monitoring)	211
	Table 8: show interfaces Output Fields for M Series, MX Series, T Series, and PTX Series Routers Management Ethernet Interface	217
	Table 9: show passive-monitoring error Output Fields	244
	Table 10: show passive-monitoring flow Output Fields	246
	Table 11: show passive-monitoring memory Output Fields	248
	Table 12: show passive-monitoring status Output Fields	250
	Table 13: show passive-monitoring usage Output Fields	252
	Table 14: show route forwarding-table Output Fields	257
	Table 15: show services accounting aggregation Output Fields	269
	Table 16: show services accounting aggregation template Output Fields	272
	Table 17: show services accounting errors Output Fields	273
	Table 18: show services accounting flow Output Fields	277
	Table 19: show services accounting flow-detail Output Fields	283
	Table 20: show services accounting memory Output Fields	287
	Table 21: show services accounting packet-size-distribution Output Fields	289
	Table 22: show services accounting status Output Fields	291
	Table 23: show services accounting usage Output Fields	294
	Table 24: show services flow-collector file interface Output Fields	296
	Table 25: show services flow-collector input interface Output Fields	298
	Table 26: show services flow-collector interface Output Fields	300

About the Documentation

- [Documentation and Release Notes on page xiii](#)
- [Supported Platforms on page xiii](#)
- [Using the Examples in This Manual on page xiii](#)
- [Documentation Conventions on page xv](#)
- [Documentation Feedback on page xvii](#)
- [Requesting Technical Support on page xvii](#)

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](#)
- [T Series](#)
- [MX Series](#)
- [SRX 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 [CLI Explorer](#).

Documentation Conventions

[Table 1 on page xv](#) defines notice icons used in this guide.

Table 1: Notice Icons

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

[Table 2 on page xvi](#) defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

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

GUI Conventions

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

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

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <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: <http://kb.juniper.net/InfoCenter/>
- 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>.

CHAPTER 1

Overview

- [Traffic Sampling, Forwarding, and Monitoring Overview on page 19](#)

Traffic Sampling, Forwarding, and Monitoring Overview

Traffic sampling allows you to sample IP traffic based on particular input interfaces and various fields in the packet header. You can also use traffic sampling to monitor any combination of specific logical interfaces, specific protocols on one or more interfaces, a range of addresses on a logical interface, or individual IP addresses. Information about the sampled packets is saved to files on the router's hard disk.

Traffic sampling is not meant to capture all packets received by a router. We do not recommend excessive sampling (a rate greater than 1/1000 packets), because it can increase the load on your processor. If you need to set a higher sampling rate to diagnose a particular problem or type of traffic received, we recommend that you revert to a lower sampling rate after you discover the problem or troublesome traffic. In addition, traffic sampling and forwarding are supported only on routers equipped with an Internet Processor II application-specific integrated circuit (ASIC). To determine whether a routing platform has an Internet Processor II ASIC, use the **show chassis hardware** command.

Junos OS supports both per-packet and per-flow load balancing. In Junos OS Release 9.0 and later, you can configure per-prefix load balancing. This feature enables the router to elect the next hop independent of the route chosen by other routers. The result is a better utilization of available links. Likewise, you can configure Junos OS so that, for the active route, all next-hop addresses for a destination are installed in the forwarding table. This is called per-packet load balancing, which you can use to spread traffic across multiple paths between routers.

With forwarding policies, you can configure per-flow load balancing, port mirroring, and domain name system (DNS) or Trivial File Transfer Protocol (TFTP) forwarding.

CHAPTER 2

Collecting Traffic Samples for Network Monitoring

- [Minimum Traffic Sampling Configuration on page 21](#)
- [Configuring Traffic Sampling on page 22](#)
- [Disabling Traffic Sampling on page 24](#)
- [Collecting Traffic Sampling Output in a File on page 24](#)
- [Directing Traffic Sampling Output to a Server Running the cflowd Application on page 26](#)
- [Collecting Traffic Sampling Output in the Cisco Systems NetFlow Services Export Version 9 Format on page 29](#)
- [Example: Sampling a Single SONET/SDH Interface on page 30](#)
- [Example: Sampling All Traffic from a Single IP Address on page 31](#)
- [Example: Sampling All FTP Traffic on page 32](#)
- [Tracing Traffic-Sampling Operations on page 33](#)

Minimum Traffic Sampling Configuration

To configure traffic sampling, you must perform at least the following tasks:

1. Create a firewall filter to apply to the logical interfaces being sampled by including the **filter** statement at the **[edit firewall family *family-name*]** hierarchy level. In the filter **then** statement, you must specify the action modifier **sample** and the action **accept**.

```
[edit firewall family family-name]  
filter filter-name {  
  term term-name {  
    then {  
      sample;  
      accept;  
    }  
  }  
}
```

2. Apply the filter to the interfaces on which you want to sample traffic:

```
[edit interfaces]  
interface-name {  
  unit logical-unit-number {
```

```
family family-name {  
    filter {  
        input filter-name;  
    }  
    address address {  
        destination destination-address;  
    }  
}  
}
```

3. Enable sampling and specify a nonzero sampling rate:

```
[edit forwarding-options]  
sampling {  
    input {  
        rate number;  
    }  
}
```

Configuring Traffic Sampling

On routing platforms containing a Monitoring Services PIC or an Adaptive Services PIC, you can configure traffic sampling for traffic passing through the routing platform. In Junos OS Release 8.3 and later, you can also configure traffic sampling of MPLS traffic.

To configure traffic sampling on a logical interface:

1. Include the **input** statement at the **[edit forwarding-options sampling]** hierarchy level, for example:

```
[edit forwarding-options sampling]  
input {  
    max-packets-per-second number;  
    maximum-packet-length bytes  
    rate number;  
    run-length number;  
}
```

2. Specify the threshold traffic value by using the **max-packets-per-second** statement. The value is the maximum number of packets to be sampled, beyond which the sampling mechanism begins dropping packets. The range is 0 through 65,535. A value of 0 instructs the Packet Forwarding Engine not to sample any packets. The default value is 1000.



NOTE: This statement is not valid for port mirroring.

3. Specify the maximum length of the sampled packet by using the **maximum-packet-length** *bytes* statement. For *bytes*, specify a value.



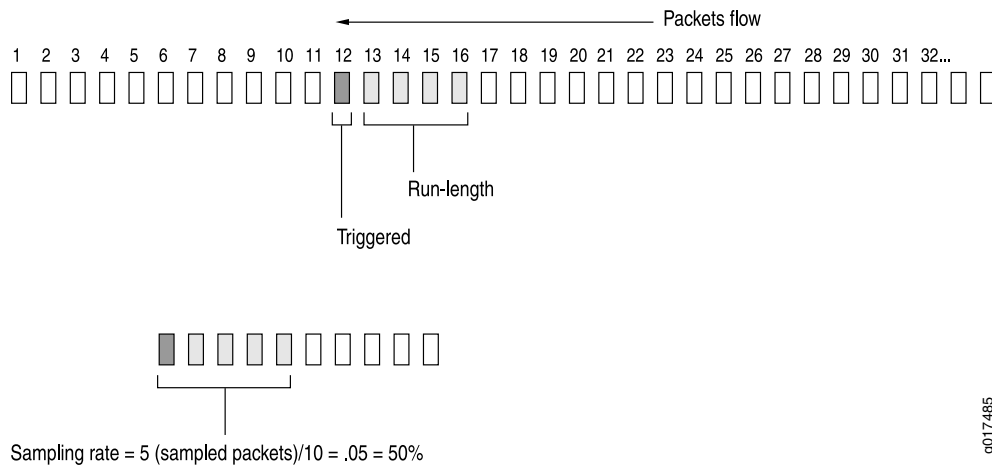
NOTE: For MX-Series devices with Modular Port Concentrators (MPCs) and T4000 router with Type 5 FPC, port-mirrored or sampled packets can be truncated (or clipped) to any length in the range of 1 to 255 bytes. Only 1 to 255 are valid values for packet truncation on these devices. For other devices, the range is from 0 to 9216. A maximum-packet-length value of zero represents that truncation is disabled, and the entire packet is mirrored or sampled.

4. Specify the sampling rate by setting the values for *rate* and *run-length* (see [Figure 1 on page 23](#)).

Figure 1: Configure Sampling Rate

Rate and Run-length

Case #1 Rate =10, run-length =4



The forwarding plane provides support for random sampling that can be configured through the *rate* or *run-length* statement. The *rate* statement sets the ratio of the number of packets to be sampled on an average. For example, if you configure a rate of 10, on average every tenth packet (1 packet out of 10) is sampled.

The *run-length* statement specifies the number of matching packets to sample following the initial one-packet trigger event. Configuring a run length greater than 0 allows you to sample packets following those already being sampled.



NOTE: The *run-length* statement is not supported on MX Series routers with Modular Port Concentrators (MPCs) and T4000 router with Type 5 FPC.

You can also send the sampled packets to a specified host using the cflowd version 5 and 8 formats or the version 9 format as defined in RFC 3954. For more information, see [“Directing Traffic Sampling Output to a Server Running the cflowd Application” on page 26](#) and [“Collecting Traffic Sampling Output in the Cisco Systems NetFlow Services Export Version 9 Format” on page 29](#).

Junos OS does not sample packets originating from the router. If you configure a sampling filter and apply it to the output side of an interface, then only the transit packets going through that interface are sampled. Packets that are sent from the Routing Engine to the Packet Forwarding Engine are not sampled.

When you apply a firewall filter to a loopback interface, the filter might block responses from the Monitoring Services PIC. To allow responses from the Monitoring Services PIC to pass through for sampling purposes, configure a term in the firewall filter to include the Monitoring Services PIC's IP address.



NOTE: Targeted broadcast does not work when the targeted broadcast option `forward-and-send-to-re` and the traffic sampling option `sampling` are configured on the same egress interface of an M320 router, a T640 router, or an MX960 router. To overcome this scenario, you must either disable one of these options or enable the sampling option with the targeted broadcast option `forward-only` on the egress interface. For information about targeted broadcast, see *Understanding Targeted Broadcast*.

**Related
Documentation**

- *Guidelines for Configuring Firewall Filters*
- *Guidelines for Applying Standard Firewall Filters*

Disabling Traffic Sampling

To explicitly disable traffic sampling on the router, include the **disable** statement at the **[edit forwarding-options sampling]** hierarchy level:

```
[edit forwarding-options sampling]
  disable;
```

Collecting Traffic Sampling Output in a File

You configure traffic sampling results to a file in the `/var/tmp` directory. To collect the sampled packets in a file, include the **file** statement at the **[edit forwarding-options sampling output]** hierarchy level:

```
[edit forwarding-options sampling family family-name output]
  file <disable> filename filename <files number> <size bytes> <stamp | no-stamp >
  <world-readable | no-world-readable>;
```

To configure the period of time before an active flow is exported, include the **flow-active-timeout** statement at the **[edit forwarding-options sampling output family (inet | inet6 | mpls)]** hierarchy level:

```
[edit forwarding-options sampling family (inet | inet6 | mpls) output]
  flow-active-timeout seconds;
```

To configure the period of time before a flow is considered inactive, include the **flow-inactive-timeout** statement at the **[edit forwarding-options sampling output]** hierarchy level:

```
[edit forwarding-options sampling family (inet | inet6 | mpls) output]
flow-inactive-timeout seconds;
```

To configure the interface that sends out monitored information, include the **interface** statement at the [edit forwarding-options **sampling output**] hierarchy level:

```
[edit forwarding-options sampling family (inet | inet6 | mpls) output]
interface interface-name {
    engine-id number;
    engine-type number;
    source-address address;
}
```



NOTE: This feature is not supported with the version 9 template format. You must send traffic flows collected using version 9 to a server. For more information see [“Collecting Traffic Sampling Output in the Cisco Systems NetFlow Services Export Version 9 Format”](#) on page 29.

Traffic Sampling Output Format

Traffic sampling output is saved to an ASCII text file. The following is an example of the traffic sampling output that is saved to a file in the `/var/tmp` directory. Each line in the output file contains information for one sampled packet. You can optionally display a timestamp for each line.

The column headers are repeated after each group of 1000 packets.

```
# Apr  7 15:48:50
Time                               Dest                Src Dest Src Proto TOS Pkt Intf  IP    TCP
                                addr                addr port port
                                len num frag flags
Apr 7 15:48:54 192.168.9.194 192.168.9.195  0  0  1  0x0 84 8  0x0  0x0
Apr 7 15:48:55 192.168.9.194 192.168.9.195  0  0  1  0x0 84 8  0x0  0x0
Apr 7 15:48:56 192.168.9.194 192.168.9.195  0  0  1  0x0 84 8  0x0  0x0
Apr 7 15:48:57 192.168.9.194 192.168.9.195  0  0  1  0x0 84 8  0x0  0x0
Apr 7 15:48:58 192.168.9.194 192.168.9.195  0  0  1  0x0 84 8  0x0  0x0
```

The output contains the following fields:

- **Time**—Time at which the packet was received (displayed only if you include the **stamp** statement in the configuration)
- **Dest addr**—Destination IP address in the packet
- **Src addr**—Source IP address in the packet
- **Dest port**—Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port for the destination address
- **Src port**—TCP or UDP port for the source address
- **Proto**—Packet’s protocol type
- **TOS**—Contents of the type-of-service (ToS) field in the IP header
- **Pkt len**—Length of the sampled packet, in bytes

- **Intf num**—Unique number that identifies the sampled logical interface
- **IP frag**—IP fragment number, if applicable
- **TCP flags**—Any TCP flags found in the IP header

To set the timestamp option for the file **my-sample**, enter the following:

```
[edit forwarding-options sampling family (inet | inet6 | mpls) output file]
user@host# set filename my-sample files 5 size 2m world-readable stamp;
```

Whenever you toggle the timestamp option, a new header is included in the file. If you set the **stamp** option, the **Time** field is displayed.

```
# Apr  7 15:48:50
# Time           Dest      Src  Dest  Src Proto  TOS   Pkt  Intf   IP   TCP
#                addr      addr port  port          len  num  frag flags
# Feb  1 20:31:21
#                Dest      Src  Dest  Src Proto  TOS   Pkt  Intf   IP   TCP
#                addr      addr port  port          len  num  frag flags
```

Directing Traffic Sampling Output to a Server Running the cflowd Application

You can collect an aggregate of sampled flows and send the aggregate to a specified host that runs the cflowd application available from the Cooperative Association for Internet Data Analysis (CAIDA) (<http://www.caida.org>). By using cflowd, you can obtain various types of byte and packet counts of flows through a router.

The cflowd application collects the sampled flows over a period of 1 minute. At the end of the minute, the number of samples to be exported are divided over the period of another minute and are exported over the course of the same minute.

Before you can perform flow aggregation, the routing protocol process must export the autonomous system (AS) path and routing information to the sampling process. To do this, include the **route-record** statement:

```
route-record;
```

You can include this statement at the following hierarchy levels:

- **[edit routing-options]**
- **[edit routing-instances *routing-instance-name* routing-options]**

By default, flow aggregation is disabled. To enable the collection of flow aggregates, include the **flow-server** statement at the **[edit forwarding-options sampling output]** hierarchy level:

```
[edit forwarding-options sampling family (inet | inet6 | mpls) output ]
flow-server hostname {
  aggregation {
    autonomous-system;
    destination-prefix;
    protocol-port;
    source-destination-prefix {
      caida-compliant;
```

```

    }
    source-prefix;
  }
  autonomous-system-type (origin | peer);
  (local-dump | no-local-dump);
  port port-number;
  source-address address;
  version format;
}

```

In the cflowd statement, specify the name, identifier, and source-address of the host that collects the flow aggregates. You must also include the UDP port number on the host and the **version**, which gives the format of the exported cflowd aggregates. To specify an IPv4 source address, include the **source-address** statement. To collect cflowd records in a log file before exporting, include the **local-dump** statement. To specify the cflowd version number, include the **version** statement. The cflowd version is either 5 or 8.

You can specify both host (cflowd) sampling and port mirroring in the same configuration. You can perform RE-sampling and port mirroring actions simultaneously. However, you cannot perform PIC-sampling and port mirroring actions simultaneously.

To specify aggregation of specific types of traffic, include the **aggregation** statement. This conserves memory and bandwidth enabling cflowd to export targeted flows rather than all the aggregated



NOTE: Aggregation is valid only if cflowd version 8 is specified.

To specify a flow type, include the **aggregation** statement at the **[edit forwarding-options sampling output cflowd hostname]** hierarchy level:

```

[edit forwarding-options sampling family (inet | inet6 | mpls) output hostname]
  aggregation {
    source-destination-prefix;
  }

```

You specify the aggregation type using one of the following options:

- **autonomous-system**—Aggregate by AS number; may require setting the separate cflowd **autonomous-system-type** statement to include either **origin** or **peer** AS numbers. The **origin** option specifies to use the origin AS of the packet source address in the Source Autonomous System cflowd field. The **peer** option specifies to use the peer AS through which the packet passed in the Source Autonomous System cflowd field. By default, cflowd exports the origin AS number.
- **destination-prefix**—Aggregate by destination prefix (only).
- **protocol-port**—Aggregate by protocol and port number; requires setting the separate cflowd **port** statement.
- **source-destination-prefix**—Aggregate by source and destination prefix. Version 2.1b1 of CAIDA's cflowd application does not record source and destination mask length values in compliance with CAIDA's *cflowd Configuration Guide*, dated August 30, 1999. If you configure the **caida-compliant** statement, Junos OS complies with Version 2.1b1

of cflowd. If you do not include the **caida-compliant** statement in the configuration, Junos OS records source and destination mask length values in compliance with the *cflowd Configuration Guide*.

- **source-prefix**—Aggregate by source prefix (only).

Collection of sampled packets in a local ASCII file is not affected by the **cflowd** statement.

Debugging cflowd Flow Aggregation

To collect the cflowd flows in a log file before they are exported, include the **local-dump** option at the **[edit forwarding-options sampling output cflowd hostname]** hierarchy level:

```
[edit forwarding-options sampling family (inet | inet6 | mpls) output flow-server hostname]
local-dump;
```

By default, the flows are collected in `/var/log/sampled`; to change the filename, include the **filename** statement at the **[edit forwarding-options sampling traceoptions]** hierarchy level. For more information about changing the filename, see “[Collecting Traffic Sampling Output in a File](#)” on page 24.



NOTE: Because the **local-dump** option adds extra overhead, you should use it only while debugging cflowd problems, not during normal operation.

The following is an example of the flow information. The AS number exported is the origin AS number. All flows that belong under a cflowd header are dumped, followed by the header itself:

```
Jun 27 18:35:43 v5 flow entry
Jun 27 18:35:43   Src addr: 10.53.127.1
Jun 27 18:35:43   Dst addr: 10.6.255.15
Jun 27 18:35:43   Nhop addr: 192.168.255.240
Jun 27 18:35:43   Input interface: 5
Jun 27 18:35:43   Output interface: 3
Jun 27 18:35:43   Pkts in flow: 15
Jun 27 18:35:43   Bytes in flow: 600
Jun 27 18:35:43   Start time of flow: 7230
Jun 27 18:35:43   End time of flow: 7271
Jun 27 18:35:43   Src port: 26629
Jun 27 18:35:43   Dst port: 179
Jun 27 18:35:43   TCP flags: 0x10
Jun 27 18:35:43   IP proto num: 6
Jun 27 18:35:43   TOS: 0xc0
Jun 27 18:35:43   Src AS: 7018
Jun 27 18:35:43   Dst AS: 11111
Jun 27 18:35:43   Src netmask len: 16
Jun 27 18:35:43   Dst netmask len: 0
```

[... 4] more v5 flow entries; then the following header:]

```
Jun 27 18:35:43 cflowd header:
Jun 27 18:35:43   Num-records: 42
Jun 27 18:35:43   Version: 5
Jun 27 18:35:43   Flow seq num: 118
Jun 27 18:35:43   Engine id: 0
Jun 27 18:35:43   Engine type: 3
```

Collecting Traffic Sampling Output in the Cisco Systems NetFlow Services Export Version 9 Format

In Junos OS Release 8.3 and later, you can collect a record of sampled flows using the version 9 format as defined in RFC 3954, *Cisco Systems NetFlow Services Export Version 9*. Version 9 uses templates to collect a set of sampled flows and send the record to a specified host.

You configure the version 9 template used to collect a record of sampled flows at the **[edit services monitoring]** hierarchy level. For more information, see the *Junos OS Services Interfaces Library for Routing Devices* and the *Flow Monitoring Feature Guide for Routing Devices*.

To enable the collection of traffic flows using the version 9 format, include the **version9** statement at the **[edit forwarding-options sampling family family-name output flow-server hostname]** hierarchy level:

```
[edit forwarding-options sampling family family-name output flow-server hostname]
version9 {
  template template-name;
}
```

template-name is the name of the version 9 template configured at the **[edit services monitoring]** hierarchy level.

You configure traffic sampling at the **[edit forwarding-options sampling input]** hierarchy level. In Junos OS Release 8.3 and later, you can configure sampling for MPLS traffic as well as IPv4 traffic. You can define a version 9 flow record template suitable for IPv4 traffic, MPLS traffic, or a combination of the two. In Junos OS Release 9.5 and later, you can sample packets from both the **inet** and **mpls** protocol families at the same time. In Junos OS Release 10.4 and later, you can configure sampling for peer AS billing traffic for the **inet** and **ipv6** protocols only. For more information about how to configure traffic sampling, see [“Configuring Traffic Sampling” on page 22](#).

The following restrictions apply to configuration of the version 9 format:

- You can configure only one host to collect traffic flows using the version 9 format. Configure the host at the **[edit forwarding-options sampling family family-name output flow-server hostname]** hierarchy level.
- You cannot specify both the version 9 format and cflowd versions 5 and 8 formats in the same configuration. For more information about how to configure flow monitoring using cflowd version 8, see [“Directing Traffic Sampling Output to a Server Running the cflowd Application” on page 26](#).
- Any values for **flow-active-timeout** and **flow-inactive-timeout** that you configure at the **[edit forwarding-options sampling output]** hierarchy level are overridden by the values configured in the version 9 template.
- Version 9 does not support Routing Engine-based sampling. You cannot configure version 9 to send traffic sampling result to a file in the **/var/tmp** directory.

Example: Configuring Active Flow Monitoring Using Version 9

In this example, you enable active flow monitoring using version 9. You specify a template **mpls** that you configure at the **[edit services monitoring]** hierarchy level. You also configure the traffic family **mpls** to sample MPLS packets.

```
[edit forwarding-options]
sampling {
  input {
    rate 1;
    run-length;
  }
  family inet {
    output {
      flow-server 10.60.2.1 { # The IP address and port of the host
        port 2055; # that collects the sampled traffic flows.
        source-address 3.3.3.1;
        version9 {
          template mpls; # Version 9 records are sent
        } # using the template named mpls
      }
    }
  }
}
```

Example: Sampling a Single SONET/SDH Interface

The following configuration gathers statistical sampling information from a small percentage of all traffic on a single SONET/SDH interface and collects it in a file named **sonet-samples.txt**.

Create the filter:

```
[edit firewall family inet]
filter {
  sample-sonet {
    then {
      sample;
      accept;
    }
  }
}
```

Apply the filter to the SONET/SDH interface:

```
[edit interfaces]
so-0/0/1 {
  unit 0 {
    family inet {
      filter {
        input sample-sonet;
      }
      address 10.127.68.254/32 {
        destination 10.127.74.7;
      }
    }
  }
}
```

```

    }
  }
}

```

Finally, configure traffic sampling:

```

[edit forwarding-options]
sampling {
  input {
    rate 100;
    run-length 2;
  }
  family inet {
    output {
      file {
        filename sonet-samples.txt;
        files 40;
        size 5m;
      }
    }
  }
}

```

Example: Sampling All Traffic from a Single IP Address

The following configuration gathers statistical information about every packet entering the router on a specific Gigabit Ethernet port originating from a single source IP address of **10.45.92.31**, and collects it in a file named **samples-10-45-92-31.txt**.

Create the filter:

```

[edit firewall family inet]
filter one-ip {
  term get-ip {
    from {
      source-address 10.45.92.31;
    }
    then {
      sample;
      accept;
    }
  }
}

```

Apply the filter to the Gigabit Ethernet interface:

```

[edit interfaces]
ge-4/1/1 {
  unit 0 {
    family inet {
      filter {
        input one-ip;
      }
      address 10.45.92.254;
    }
  }
}

```

Finally, gather statistics on all the candidate samples; in this case, gather all statistics:

```
[edit forwarding-options]
sampling {
  input {
    rate 1;
  }
  family inet {
    output {
      file {
        filename samples-215-45-92-31.txt;
        files 100;
        size 100k;
      }
    }
  }
}
```

Example: Sampling All FTP Traffic

The following configuration gathers statistical information about a moderate percentage of packets using FTP in the output path of a specific T3 interface, and collects the information in a file named **t3-ftp-traffic.txt**.

Create a filter:

```
[edit firewall family inet]
filter ftp-stats {
  term ftp-usage {
    from {
      destination-port [ftp ftp-data];
    }
    then {
      sample;
      accept;
    }
  }
}
```

Apply the filter to the T3 interface:

```
[edit interfaces]
t3-7/0/2 {
  unit 0 {
    family inet {
      filter {
        input ftp-stats;
      }
      address 10.35.78.254/32 {
        destination 10.35.78.4;
      }
    }
  }
}
```

Finally, gather statistics on 10 percent of the candidate samples:

```
[edit forwarding-options]
sampling {
  input {
    rate 10;
  }
  family inet {
    output {
      file {
        filename t3-ftp-traffic.txt;
        files 50;
        size 1m;
      }
    }
  }
}
```

Tracing Traffic-Sampling Operations

Tracing operations track all traffic-sampling operations and record them in a log file in the `/var/log` directory. By default, this file is named `/var/log/sampled`. The default file size is 128 KB, and 10 files are created before the first one gets overwritten.

To trace traffic-sampling operations, include the **traceoptions** statement at the **[edit forwarding-options sampling]** hierarchy level:

```
[edit forwarding-options sampling]
traceoptions {
  file <filename> <files number> <size bytes> <world-readable | no-world-readable>;
  no-remote-trace;
}
```


CHAPTER 3

Configuring Traffic Forwarding for Network Monitoring

- [Configuring Traffic Forwarding and Monitoring on page 35](#)
- [Configuring IPv6 Accounting on page 39](#)
- [Configuring Discard Accounting on page 40](#)
- [Configuring Active Flow Monitoring on PTX Series Packet Transport Routers on page 42](#)
- [Configuring Passive Flow Monitoring on page 44](#)
- [Configuring Port Mirroring on page 45](#)
- [Configuring Next-Hop Groups to Use Multiple Interfaces to Forward Packets Used in Port Mirroring on page 49](#)
- [Defining a Port-Mirroring Firewall Filter on page 51](#)
- [Defining a Next-Hop Group for Port Mirroring on page 53](#)

Configuring Traffic Forwarding and Monitoring

To configure forwarding options and traffic monitoring, include statements at the **[edit forwarding-options]** hierarchy level:

```
[edit forwarding-options]
accounting group-name {
  output {
    cflowd [ hostnames ] {
      aggregation {
        autonomous-system;
        destination-prefix;
        protocol-port;
        source-destination-prefix {
          caida-compliant;
        }
        source-prefix;
      }
      autonomous-system-type (origin | peer);
      port port-number;
      version format;
    }
    flow-active-timeout seconds;
    flow-inactive-timeout seconds;
```

```

    interface interface-name {
        engine-id number;
        engine-type number;
        source-address address;
    }
}
enhanced-hash-key {
    family inet {
        gtp-tunnel-endpoint-identifier;
        incoming-interface-index;
        no-destination-port;
        no-source-port;
        type-of-service;
    }
    family inet6 {
        gtp-tunnel-endpoint-identifier;
        incoming-interface-index;
        no-destination-port;
        no-source-port;
        traffic-class;
    }
    family mpls {
        incoming-interface-index;
        label-1-exp;
        no-payload;
    }
    family multiservice {
        incoming-interface-index;
        no-payload;
        outer-priority;
    }
    services-loadbalancing {
        family inet layer-3-services {
            incoming-interface-index;
            source-address;
        }
    }
}
family family-name {
    filter {
        input filter-name;
        output filter-name;
    }
    route-accounting;
}
flood {
    input filter-name;
}
hash-key {
    family inet {
        layer-3;
        layer-4;
    }
    family mpls {
        no-interface-index;
    }
}

```

```

label-1;
label-2;
label-3;
no-labels;
no-label-1-exp;
payload {
    ether-pseudowire;
    ip {
        layer-3-only;
        port-data {
            source-msb;
            source-lsb;
            destination-msb;
            destination-lsb;
        }
    }
}
}
}
family multiservice {
    destination-mac;
    label-1;
    label-2;
    payload {
        ip {
            layer-3-only;
        }
    }
    source-mac;
}
}
helpers {
    bootp {
        client-response-ttl;
        description text-description;
        interface interface-group {
            client-response-ttl number;
            description text-description;
            maximum-hop-count number;
            minimum-wait-time seconds;
            no-listen;
            server address {
                logical-system logical-system-name <routing-instance [ <default>
                    routing-instance-names ]>;
                routing-instance [ <default> routing-instance-names ];
            }
        }
        maximum-hop-count number;
        minimum-wait-time seconds;
        relay-agent-option;
        server [ addresses ];
    }
    domain {
        description text-description;
        server < [ routing-instance routing-instance-names ] >;
        interface interface-name {
            description text-description;

```

```

        no-listen;
        server < [ routing-instance routing-instance-names ] >;
    }
}
tftp {
    description text-description;
    server < [ routing-instance routing-instance-names ] >;
    interface interface-name {
        description text-description;
        no-listen;
        server < [ routing-instance routing-instance-names ] >;
    }
}
traceoptions {
    file <filename> <files number> <match regular-expression> <size size>
        <world-readable | no-world readable>;
    flag flag;
    level severity-level;
    no-remote-trace;
}
}
load-balance {
    indexed-load-balance;
    per-flow {
        hash-seed number;
    }
    per-prefix {
        hash-seed number;
    }
}
}
monitoring group-name {
    family inet {
        output {
            cflowd hostname {
                port port-number;
            }
            export-format cflowd-version-5;
            flow-active-timeout seconds;
            flow-export-destination {
                cflowd-collector;
            }
            flow-inactive-timeout seconds;
            interface interface-name {
                engine-id number;
                engine-type number;
                input-interface-index number;
                output-interface-index number;
                source-address address;
            }
        }
    }
}
}
next-hop-group [ group-names ] {
    interface interface-name {
        next-hop [ addresses ];
    }
}

```

```

}
port-mirroring {
  family (ccc | inet | inet6 | vpls) {
    output {
      interface interface-name {
        next-hop address;
      }
      no-filter-check;
    }
    input {
      maximum-packet-length bytes;
      rate number;
      run-length number;
    }
  }
}
traceoptions {
  file <filename> <files number> <match regular-expression> <size bytes>
  <world-readable | no-world-readable>;
  no-remote-trace;
}
}

```



NOTE: When a route pointing to more than one services PIC is available, and with application layer gateways (ALGs) configured, you must always configure the distribution of traffic across PICs based on the source IP address by including the `family inet layer-3-services source-address` statement at the `[edit forwarding-options enhanced-hash-key services-loadbalancing]` hierarchy level for IPv4 traffic and the `family inet6 layer-3-services source-address` statement at the `[edit forwarding-options enhanced-hash-key services-loadbalancing]` hierarchy level for IPv6 traffic. With ALGs used to manage a parent-child relationship of sessions, both the parent and the child sessions must be processed by the same type of services PIC.

Related Documentation

- [\[edit forwarding-options\] Hierarchy Level](#)

Configuring IPv6 Accounting

You can configure the routing platform to track IPv6-specific packets and bytes passing through the router.

To reset the IPv6 traffic counters and enable IPv6 accounting, include the **route-accounting** statement at the `[edit forwarding-options family inet6]` hierarchy level:

```

[edit]
forwarding-options {
  family inet6 {
    route-accounting;
  }
}

```

By default, IPv6 accounting is disabled.

To view IPv6 statistics for a device interface and for all logic units of that interface, use the **show interface statistics** operational mode command. In the command output, the **IPv6 transit statistics** counters display IPv6 transit traffic only. Traffic destined for or sent from the Routing Engine is not accounted for in any of the **Transit statistics** counters but in the **Local statistics** counters instead. Local traffic statistics are not protocol-aware and therefore keep track of all traffic types.

- Related Documentation
- [route-accounting on page 181](#)
 - [show interfaces statistics on page 232](#)

Configuring Discard Accounting

On routing platforms containing a Monitoring Services PIC or an Adaptive Services PIC, you can configure accounting for traffic passing through the routing platform.

To configure discard accounting, include the **accounting group group-name** statement at the **[edit forwarding-options]** hierarchy level:

```
[edit forwarding-options]
accounting group-name {
  output {
    cflowd [ hostnames ] {
      aggregation {
        autonomous-system;
        destination-prefix;
        protocol-port;
        source-destination-prefix {
          caida-compliant;
        }
        source-prefix;
      }
      autonomous-system-type (origin | peer);
      port port-number;
      version format;
    }
    flow-active-timeout seconds;
    flow-inactive-timeout seconds;
    interface {
      engine-id number;
      engine-type number;
      source-address address;
    }
  }
}
```

To configure the output flow aggregation, include the **cflowd** statement. For more information about flow aggregation, see [“Directing Traffic Sampling Output to a Server Running the cflowd Application” on page 26](#). To configure the interval before exporting an active flow, include the **flow-active-timeout** statement. The default value for **flow-active-timeout** is 1800 seconds. To configure the interval before a flow is considered inactive, include the **flow-inactive-timeout** statement. The default value for **flow-inactive-timeout** is 60 seconds. To configure the interface that sends out monitored

information, include the **interface** statement. Discard accounting is supported for the Monitoring Services PIC only.

When you apply a firewall filter to a loopback interface, the filter might block responses from the Monitoring Services PIC. To allow responses from the Monitoring Services PIC to pass through for accounting purposes, configure a term in the firewall filter to include the Monitoring Services PIC IP address. For more detailed information about configuring firewall filters, see *Guidelines for Configuring Firewall Filters* and *Guidelines for Applying Standard Firewall Filters*.

You can use discard accounting for passive and active flow monitoring.

**Related
Documentation**

- *Flow Monitoring Feature Guide for Routing Devices*
- *Class of Service Feature Guide for Routing Devices*

Configuring Active Flow Monitoring on PTX Series Packet Transport Routers

You can use flow monitoring to help with network administration. Active flow monitoring on PTX Series routers allows you to collect sampled packets, then the router does GRE encapsulation of the packets and sends them to a remote server for flow processing. The GRE encapsulation includes an interface index and GRE key field. The GRE encapsulation removes MPLS tags. You configure one or more port-mirroring instances to define which traffic to sample and configure a server to receive the GRE encapsulated packets. You configure a firewall filter on interfaces where you want to capture flows. You can configure as many as 48 port-mirroring instances.

To configure the router to do GRE encapsulation of sampled packets and send them to a remote server for flow processing:

1. Configure one or more server profiles that specify a host where GRE encapsulated sampled packets are sent, and optionally, a source address to include in the header of each sampled packet.

- a. Specify a name for each server profile and an IP address of the host where sampled packets are sent:

```
[edit services hosted-services]
user@host# set server-profile server-profile-name server-address ipv4-address
```

- b. (Optional) For each server profile, specify a source address to include in the header of each sampled packet:

```
[edit services hosted-services server-profile server-profile-name]
user@host# set client-address ipv4-address
```



NOTE: The default client address is 0.0.0.0. You must specify an IPv4 address as the client address. You can also specify the loopback address or management interface address as the client address.

2. Configure one or more port-mirroring instances.

- a. Specify a name for each port-mirroring instance:

```
[edit forwarding-options port-mirroring]
user@host# set instance instance-name
```



NOTE: You can configure a maximum of 48 port-mirroring instances.

- b. Specify a protocol family for each port-mirroring instance:

```
[edit forwarding-options port-mirroring instance instance-name]
user@host# set family (inet | inet6 )
```

3. To set the ratio of the number of packets to sample, specify a value from 1 through 65,535 for each port-mirroring instance:

```
[edit forwarding-options port-mirroring instance instance-name input]
user@host# set rate number
```



NOTE: You must specify a value for the `rate` statement. The default value is zero, which effectively disables sampling. If, for example, you specify a rate value of 4, every fourth packet (1 packet out of 4) is sampled.

4. (Optional) Specify the number of samples to collect after the initial trigger event for each port-mirroring instance:

```
[edit forwarding-options port-mirroring instance instance-name input]
user@host# set run-length number
```



NOTE: The default value is zero. You can specify a number up to 20.

5. To designate a host where sampled traffic is sent, specify the name of server profile configured at the `[edit services hosted-services]` hierarchy level for each port-mirroring instance:

```
[edit forwarding-options port-mirroring instance instance-name family ( inet | inet6)
output]
user@host# set server-profile server-profile-name
```

6. Configure one or more firewall filters.

- a. For each firewall filter, specify a protocol family, filter name, and match conditions:

```
[edit firewall]
user@host# set filter family (inet | inet6) filter filter-name term term-name from
match-conditions
```

- b. For each firewall filter you configure, specify the name of a port-mirroring instance you configured at the `[edit forwarding-options]` hierarchy level as a nonterminating action so that the traffic that matches that instance is sampled:

```
[edit firewall family (inet | inet6) filter filter-name term term-name]
user@host# set then port-mirroring instance instance-name
```

7. Apply each firewall filter to an interface to evaluate incoming traffic:

```
[edit interfaces interface-name unit logical-unit-number]
user@host# set family (inet | inet6) filter input firewall-filter-name
```



NOTE: Active flow monitoring is supported only on incoming traffic. You cannot apply firewall filters to evaluate outgoing traffic.

8. Configure the remote server, where GRE encapsulated packets are sent, to perform flow processing.

Related Documentation

- [Configuring Port Mirroring on page 45](#)

- [hosted-services on page 144](#)
- [port-mirroring on page 178](#)
- [server-profile \(Active Flow Monitoring\) on page 188](#)
- *Firewall Filter Nonterminating Actions*

Configuring Passive Flow Monitoring

On routing platforms containing the Monitoring Services PIC or the Monitoring Services II PIC, you can configure flow monitoring for traffic passing through the routing platform. This type of monitoring method is passive monitoring.

To configure flow monitoring, include the **monitoring** statement at the **[edit forwarding-options]** hierarchy level:

```
[edit forwarding-options]
monitoring group-name {
  family inet {
    output {
      cflowd hostname {
        port port-number;
      }
      export-format cflowd-version-5;
      flow-active-timeout seconds;
      flow-export-destination {
        cflowd-collector;
      }
      flow-inactive-timeout seconds;
    }
    interface interface-name {
      engine-id number;
      engine-type number;
      input-interface-index number;
      output-interface-index number;
      source-address address;
    }
  }
}
```

To configure a passive monitoring group, include the **monitoring** statement and specify a group name. To configure monitoring on a specified address family, include the **family** statement and specify an address family. To specify an interface to monitor incoming traffic, include the **input** statement. To configure the monitoring information that is sent out, include the **output** statement. To configure the output flow aggregation, include the **cflowd** statement. For more information about flow aggregation, see [“Directing Traffic Sampling Output to a Server Running the cflowd Application” on page 26](#). To specify the format of the monitoring information sent out, include the **export-format** statement and specify a version number. To configure the interval before exporting an active flow, include the **flow-active-timeout** statement. The default value for **flow-active-timeout** is 1800 seconds. To enable flow collection, include the **flow-export-destination** statement. To configure the interval before a flow is considered inactive, include the

flow-inactive-timeout statement. The default value for **flow-inactive-timeout** is 60 seconds. To configure the interface that sends out the monitored information, include the **interface** statement. Flow monitoring is supported for Monitoring Services PIC interfaces only.

When you apply a firewall filter to a loopback interface, the filter might block responses from the Monitoring Services PIC. To allow responses from the Monitoring Services PIC to pass through for monitoring purposes, configure a term in the firewall filter to include the Monitoring Services PIC's IP address. For more detailed information about configuring firewall filters, see *Guidelines for Configuring Firewall Filters* and *Guidelines for Applying Standard Firewall Filters*.

- Related Documentation**
- *Flow Monitoring Feature Guide for Routing Devices*
 - *Class of Service Feature Guide for Routing Devices*

Configuring Port Mirroring

Port mirroring is the ability of a router to send a copy of an IPv4 or IPv6 packet to an external host address or a packet analyzer for analysis. Port mirroring is different from traffic sampling. In traffic sampling, a sampling key based on the packet header is sent to the Routing Engine. There, the key can be placed in a file, or cflowd packets based on the key can be sent to a cflowd server. In port mirroring, the entire packet is copied and sent out through a next-hop interface.

One application for port mirroring sends a duplicate packet to a virtual tunnel. A next-hop group can then be configured to forward copies of this duplicate packet to several interfaces. For more information about next-hop groups, see [“Configuring Next-Hop Groups to Use Multiple Interfaces to Forward Packets Used in Port Mirroring” on page 49](#).

All M Series Multiservice Edge Routers, T Series Core Routers, and MX Series 3D Universal Edge Routers support port mirroring for IPv4 or IPv6. The M120, M320, and MX Series routers support port mirroring for IPv4 and IPv6 simultaneously.

Port mirroring for VPLS traffic is supported on M7i and M10i routers configured with an Enhanced CFEB (CFEB-E), on M120 routers, on M320 routers configured with an Enhanced III Flexible PIC Concentrators (FPCs), and MX Series routers.

In Junos OS Release 9.3 and later, port mirroring is supported for Layer 2 traffic on MX Series routers. For information about how to configure port mirroring for Layer 2 traffic, see the *Junos OS Layer 2 Switching and Bridging Library for Routing Devices*.

In Junos OS Release 9.6 and later, port mirroring is supported for Layer 2 VPN traffic on M120 routers and M320 routers configured with an Enhanced III FPC. You can also set the maximum length of the mirrored packet. When set, the mirrored packet is truncated to the specified length.

In the MPCs on M Series and MX Series routers, GRE and MPLS header information is not contained in the port-mirrored traffic corresponding to MPLS packets transmitted through IP-GRE tunnels.

Port Mirroring Configuration Guidelines

When configuring port mirroring, the following restrictions apply:

- Only transit data is supported.
- You can configure either IPv4 or IPv6 port mirroring but not both on M Series routers, except for the M120 and M320 routers, which support port mirroring for IPv4 and IPv6 simultaneously.
- You can configure port mirroring for IPv4 and IPv6 simultaneously on the M120 and M320 routers and the MX Series routers.
- Port mirroring in the ingress and egress direction is not supported for link services IQ (lsq-) interfaces.
- Ingress filtering of multicast packets is supported on all Dense Port Concentrators (DPCs) in MX Series routers. Egress filtering of multicast packets is supported for interfaces on MPCs in MX Series routers only. Filtering of multicast packets based on destination address is not supported on M Series routers or T Series routers and is not supported for interfaces on I-chip ASIC-based DPCs in MX Series routers.

For Layer 3 port mirroring (**family inet** and **family inet6**), if the traffic being mirrored is multicast (in other words, if the packet's destination IP address is a multicast address), the destination MAC address in the mirrored copy corresponds to this multicast destination IP address and not to the unicast MAC address specified in the **[edit forwarding-options port-mirroring family (inet | inet6) output]** configuration.

- By default, firewall filters cannot be applied to port-mirroring destination interfaces. To enable port-mirroring destination interfaces to support firewall filters, use the **no-filter-check** statement to disable filter checking on the interfaces. You can include the **no-filter-check** statement at the following hierarchy levels:
 - **[edit forwarding-options port-mirroring family (inet | inet6 | ccc | vpls) output]**
 - **[edit forwarding-options port-mirroring instance *instance-name* family (inet | ccc | vpls) output]**
- You must include a firewall filter with both the **accept** action and the **port-mirror** action modifier on the inbound interface. Port mirroring does not work if you specify the **discard** action.
- The interface you configure for port mirroring should not participate in any kind of routing activity.
- The destination address you specify should not have a route to the ultimate traffic destination. For example, if the sampled IPv4 packets have a destination address of **192.68.9.10** and the port-mirrored traffic is sent to **192.68.20.15** for analysis, the device associated with the latter address should not know a route to **192.68.9.10**. Also, it should not send the sampled packets back to the source address.
- On all routers except the MX Series router, you can configure only one port-mirroring interface per router. If you include more than one interface in the **port-mirroring**

statement, the previous one is overwritten. MX Series routers support more than one port-mirroring interface per router.

- You can configure multiple port-mirroring instances on the M120, M320, and MX Series routers.
- You can specify both host (cflowd) sampling and port mirroring in the same configuration. You can perform RE-sampling and port mirroring actions simultaneously. However, you cannot perform PIC-sampling and port mirroring actions simultaneously.
- In typical applications, you send the sampled packets to an analyzer or a workstation for analysis, not to another router. If you must send this traffic over a network, you should use tunnels.

Configuring Port Mirroring

To configure port mirroring, include the **port-mirroring** statement at the **[edit forwarding-options]** hierarchy level:

```
[edit forwarding-options]
port-mirroring {
  family (ccc | inet | inet6 | vpls) {
    output {
      interface interface-name {
        next-hop address;
      }
      no-filter-check;
    }
    input {
      maximum-packet-length bytes;
      rate number;
      run-length number;
    }
  }
}
```

Configuring the Port-Mirroring Address Family and Interface

To configure port mirroring, include the **port-mirroring** statement. To configure the address family type of traffic to sample, include the **family** statement. To configure the rate of sampling, length of sampling, and the maximum size for the mirrored packet, include the **input** statement. To specify on which interface to send duplicate packets and the next-hop address to send packets, include the **output** statement. To determine whether there are any filters on the specified interface, include the **no-filter-check** statement.

For information about the **rate** and **run-length** statements, see “[Configuring Traffic Sampling](#)” on page 22 .

Configuring Multiple Port-Mirroring Instances

In Junos OS Release 9.5 and later, you can configure multiple port-mirroring instances on the M120, M320, and MX Series routers. On the M120 router, you can associate each instance with a specific Forwarding Engine Board (FEB). You cannot associate a port-mirroring instance with an FEB configured as a backup FEB. On the M320 router,

you can associate each instance with a specific Flexible PIC Concentrator (FPC). Associating a port-mirroring instance with an FPC or an FEB enables you to mirror packets to different destinations. Multiple port-mirroring instances are also supported on MX Series routers. For information about configuring multiple port-mirroring instances on MX Series routers, see the *Junos OS Layer 2 Switching and Bridging Library for Routing Devices*.



NOTE: In MX80 and MX104 routers, port-mirroring instances should always be associated with FPC 0, because associating port-mirroring instances to FPC 1 or FPC 2 can result in inconsistent behavior due to the underlying architecture.

To configure a port-mirroring instance, include the **instance *port-mirroring-instance*** statement at the **[edit forwarding-options port-mirroring]** hierarchy level:

```
[edit forwarding-options port-mirroring]
instance port-mirroring-instance-name {
  family (ccc | inet | inet6 | vpls) {
    output {
      interface interface-name {
        next-hop address;
      }
      no-filter-check;
    }
  }
  input {
    maximum-packet-length bytes;
    rate number;
    run-length number;
  }
}
```

Configuring Port-Mirroring Instances

You can configure multiple port-mirroring instances. Specify a unique **port-mirroring-instance-name** for each instance you configure.

Associating a Port-Mirroring Instance on M320 Routers

You can associate a port-mirroring instance with a specific FPC on an M320 router or with a specific FEB on an M120 router. You can associate only one port-mirroring instance with each FPC on an M320 router or with each FEB on an M120 router. On an M120 router, you cannot associate a port-mirroring instance with a FEB configured as a backup FEB.

To associate a port-mirroring instance with an FPC on an M320 router, include the **port-mirror-instance *port-mirroring-instance-name*** statement at the **[edit chassis fpc slot-number]** hierarchy level:

```
[edit chassis]
fpc slot-number {
  port-mirror-instance port-mirroring-instance-name;
}
```

For **slot-number**, specify the slot number of the FPC you want to associate with the port-mirroring instance. For **port-mirroring-instance-name**, specify the name of a port-mirroring instance you configured at the **[edit forwarding-options port-mirroring]** hierarchy level. For more information about configuring an FPC on an M320 router, see the *Junos OS Administration Library for Routing Devices*.

Associating a Port-Mirroring Instance on M120 Routers

To associate a port-mirroring instance with a FEB on an M120 router, include the **port-mirror-instance port-mirroring-instance-name** statement at the **[edit chassis feb slot-number]** hierarchy level:

```
[edit chassis]
feb slot-number {
  port-mirror-instance port-mirroring-instance-name;
}
```

For **slot-number**, specify the slot number of the FEB you want to associate with the port-mirroring instance. For **port-mirroring-instance-name**, specify the name of a port-mirroring instance you configured at the **[edit forwarding-options port-mirroring]** hierarchy level. For information about configuring FEB redundancy on an M120 router, see the *Junos OS High Availability Library for Routing Devices*. For information about configuring FPC-to-FEB connectivity on an M120 router, see the *Junos OS Administration Library for Routing Devices*.

Configuring MX Series 3D Universal Edge Routers and M120 Routers to Mirror Traffic Only Once

On MX Series and M120 routers only, you can configure port mirroring so that the router mirrors traffic only once. If you configure port mirroring on both ingress and egress interfaces, the same packet could be mirrored twice. To mirror packets only once and prevent the router from sending duplicate sampled packets to the same mirroring destination, include the **mirror-once** statement at the **[edit forwarding-options port-mirroring]** hierarchy level:

```
[edit forwarding-options port-mirroring]
mirror-once;
```



NOTE: The **mirror-once** statement is supported only in the global port-mirroring instance.

Configuring Next-Hop Groups to Use Multiple Interfaces to Forward Packets Used in Port Mirroring

Next-hop groups allow you to include multiple interfaces used to forward duplicate packets used in port mirroring.

To configure a next-hop group, include the **next-hop-group** statement at the **[edit forwarding-options]** hierarchy level:

```
[edit forwarding-options]
```

```

next-hop-group [ group-names ] {
    interface interface-name {
        next-hop [ addresses ];
    }
}
or
[edit forwarding-options port-mirroring family inet6 output]
next-hop-group group-name{
    group-type inet6;
    interface interface-name {
        next-hop ipv6-address;
    }
    next-hop-subgroup group-name{
        interface interface-name {
            next-hop ipv6-address;
        }
    }
}

```

You can specify one or more group names. To configure the interface that sends out sampled information, include the **interface** statement and specify an interface. To specify a next-hop address to send sampled information, include the **next-hop** statement and specify an IP address.

Next-hop groups have the following restrictions:

- Next-hop groups are supported for M Series and MX Series routers only.
- Next-hop groups support up to 16 next-hop addresses.
- You can configure up to 30 next-hop groups.
- Each next-hop group must have at least two next-hop addresses.
- When a firewall filter with next-hop-group action is applied on an interface in egress, the redirected copy does not retain any packet headers added while forwarding the packet to that interface. For example, if a filter with action next-hop-group is applied in egress of a GRE interface, the redirected copies received on the next-hop-group member interfaces do not contain a GRE header.



NOTE: When routes are exported, RIPv2 supports third-party next hops specified in policies, such as Virtual Router Redundancy Protocol (VRRP) groups.

Next-hop groups can be used for port mirroring.

Related Documentation

- [Configuring Port Mirroring on page 45](#)

Defining a Port-Mirroring Firewall Filter

On routers containing an Internet Processor II application-specific integrated circuit (ASIC) or T Series Internet Processor, you can send a copy of an IP version 4 (IPv4) or IP version 6 (IPv6) packet from the router to an external host address or a packet analyzer for analysis. This is known as *port mirroring*.

Port mirroring is different from traffic sampling. In traffic sampling, a sampling key based on the IPv4 header is sent to the Routing Engine. There, the key can be placed in a file, or cflowd packets based on the key can be sent to a cflowd server. In port mirroring, the entire packet is copied and sent out through a next-hop interface.

You can configure simultaneous use of sampling and port mirroring, and set an independent sampling rate and run-length for port-mirrored packets. However, if a packet is selected for both sampling and port mirroring, only one action can be performed and port mirroring takes precedence. For example, if you configure an interface to sample every packet input to the interface and a filter also selects the packet to be port mirrored to another interface, only the port mirroring would take effect. All other packets not matching the explicit filter port-mirroring criteria continue to be sampled when forwarded to their final destination.

Firewall filters provide a means of protecting your router from excessive traffic transiting the router to a network destination or destined for the Routing Engine. Firewall filters that control local packets can also protect your router from external incidents.

You can configure a firewall filter to do the following:

- Restrict traffic destined for the Routing Engine based on its source, protocol, and application.
- Limit the traffic rate of packets destined for the Routing Engine to protect against flood, or denial-of-service (DoS) attacks.
- Address special circumstances associated with fragmented packets destined for the Routing Engine. Because the device evaluates every packet against a firewall filter (including fragments), you must configure the filter to accommodate fragments that do not contain packet header information. Otherwise, the filter discards all but the first fragment of a fragmented packet.

For information about configuring firewall filters in general (including in a Layer 3 environment), see *Stateless Firewall Filter Overview* and *How Standard Firewall Filters Evaluate Packets* in the *Junos OS Firewall Filters and Traffic Policers Library for Routing Devices*.

To define a firewall filter with a port-mirroring action:

1. Prepare traffic for port mirroring by including the **filter** statement at the **[edit firewall family (inet | inet6)]** hierarchy level.

```
filter filter-name;
```

This filter at the **[edit firewall family (inet | inet6)]** hierarchy level selects traffic to be port-mirrored:

```
filter filter-name {  
  term term-name {  
    then {  
      next-hop-group group-name;  
    }  
  }  
}
```

2. Enable configuration of firewall filters.

```
[edit]  
user@host# set firewall family family
```

The value of the *family* option can be **inet** or **inet6**.

3. Enable configuration of a firewall filter *filter-name*.

```
[edit firewall family family]  
user@host# set filter filter-name
```

4. Enable configuration of a firewall filter term *filter-term-name*.

```
[edit firewall family family filter filter-name]  
user@host# edit term filter-term-name
```

For more information about firewall filter terms, see *Guidelines for Configuring Firewall Filters* in the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.

5. Specify the firewall filter match conditions based on the route source address to mirror a subset of the sampled packets.

For information about configuring firewall filter match conditions, see *Firewall Filter Match Conditions Based on Numbers or Text Aliases*, *Firewall Filter Match Conditions Based on Bit-Field Values*, *Firewall Filter Match Conditions Based on Address Fields*, and *Firewall Filter Match Conditions Based on Address Classes* in the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.

6. Enable configuration of the **action** and **action-modifier** to apply to the matching packets.

```
[edit firewall family family filter filter-name term filter-term-name]  
user@host# set then
```

7. Specify the actions to be taken on matching packets.

```
[edit firewall family family filter filter-name term filter-term-name then]  
user@host# set action
```

The recommended value for the **action** is **accept**. If you do not specify an action, or if you omit the **then** statement entirely, all packets that match the conditions in the **from** statement are accepted.

8. Specify a next-hop group as the **action-modifier**.

When the filter action is a **next-hop-group**, the packet no longer goes to its native destination, but rather is forwarded to interfaces as specified in the **next-hop-group** under the filter action.

To reference a next-hop group that specifies the next-hop addresses (for sending additional copies of packets to an analyzer), use the **next-hop-group *next-hop-group-name*** action modifier.

```
[edit firewall family family filter filter-name term filter-term-name then]
user@host# set next-hop-group next-hop-group-name
```

9. Verify the minimum configuration of the firewall filter.

```
[edit firewall ... ]
user@host# top
[edit]
user@host# show firewall

family (inet | inet6) { # Type of packets to mirror
  filter filter-name { # Firewall filter name
    term filter-term-name {
      from { # Do not specify match conditions based on route source address
      }
      then {
        next-hop-group next-hop-group-name;
      }
    }
  }
}
```

Related Documentation

- *Configuring Port Mirroring*
- *Example: Multiple Port Mirroring with Next-Hop Groups Configuration*
- *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*

Defining a Next-Hop Group for Port Mirroring

On routers containing an Internet Processor II application-specific integrated circuit (ASIC) or T Series Internet Processor, you can send a copy of an IP version 4 (IPv4) or IP version 6 (IPv6) packet from the router to an external host address or a packet analyzer for analysis. This is known as *port mirroring*.

Port mirroring is different from traffic sampling. In traffic sampling, a sampling key based on the IPv4 header is sent to the Routing Engine. There, the key can be placed in a file, or cflowd packets based on the key can be sent to a cflowd server. In port mirroring, the entire packet is copied and sent out through a next-hop interface.

You can configure simultaneous use of sampling and port mirroring, and set an independent sampling rate and run-length for port-mirrored packets. However, if a packet is selected for both sampling and port mirroring, only one action can be performed, and port mirroring takes precedence. For example, if you configure an interface to sample every packet input to the interface and a filter also selects the packet to be port mirrored to another interface, only the port mirroring would take effect. All other packets not matching the explicit filter port-mirroring criteria continue to be sampled when forwarded to their final destination.

Next-hop groups allow you to include port mirroring multiple interfaces used to forward duplicate packets used in port mirroring.

On MX Series routers, you can mirror tunnel interface input traffic to multiple destinations. To this form of multipacket port mirroring, you specify two or more additional destinations in a next-hop group, define a firewall filter that references the next-hop group as the filter action, and then apply the filter to a logical tunnel interface (lt-) or virtual tunnel interface (vt-) on the MX Series router.

To define a next-hop group for a Layer 2 port-mirroring firewall filter action:

1. Enable the configuration of forwarding options.

```
[edit]
user@host set forwarding-options port-mirroring family (inet | inet6) output
```

2. Enable configuration of a next-hop-group for Layer 2 port mirroring.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output]
user@host# set next-hop-group next-hop-group-name
```

3. Specify the type of addresses to be used in the next-hop group configuration.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group
next-hop-group-name]
user@host# set group-type inet6
```

4. Specify the interfaces of the next-hop route.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group
next-hop-group-name]
user@host# set interface logical-interface-name-1
user@host# set interface logical-interface-name-2
```

or

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group
next-hop-group-name]
user@host# set interface interface-name next-hop next-hop-address
```

The MX Series router supports up to 30 next-hop groups. Each next-hop group supports up to 16 next-hop addresses. Each next-hop group must specify at least two addresses. The *next-hop-address* can be an IPv4 or IPv6 address.

5. (Optional) Specify the next-hop subgroup.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group
next-hop-group-name]
user@host# set next-hop-subgroup subgroup-name interface interface-name next-hop
next-hop-address
```

6. Verify the configuration of the next-hop group.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group
next-hop-group-name]
user@host# top
[edit]
user@host# show forwarding-options
```

...

```
next-hop-group next-hop-group-name {  
  group-type inet6;  
  interface logical-interface-name-1;  
  interface interface-name{  
    next-hop next-hop-address;  
  }  
  next-hop-subgroup subgroup-name{  
    interface interface-name{  
      next-hop next-hop-address;  
    }  
  }  
}
```

**Related
Documentation**

- *Configuring Port Mirroring*
- *Example: Multiple Port Mirroring with Next-Hop Groups Configuration*
- *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*

CHAPTER 4

Configuring Forwarding Table Filters to Efficiently Route Traffic

- [Configuring Forwarding Table Filters on page 57](#)
- [Forwarding Table Filters for Routing Instances on ACX Series Routers on page 59](#)
- [Applying Forwarding Table Filters on page 60](#)

Configuring Forwarding Table Filters

Forwarding table filters are defined the same as other firewall filters, but you apply them differently:

- Instead of applying forwarding table filters to interfaces, you apply them to forwarding tables, each of which is associated with a routing instance and a virtual private network (VPN).
- Instead of applying input and output filters by default, you can apply an input forwarding table filter only.

All packets are subjected to the input forwarding table filter that applies to the forwarding table. A forwarding table filter controls which packets the router accepts and then performs a lookup for the forwarding table, thereby controlling which packets the router forwards on the interfaces.

When the router receives a packet, it determines the best route to the ultimate destination by looking in a forwarding table, which is associated with the VPN on which the packet is to be sent. The router then forwards the packet toward its destination through the appropriate interface.



NOTE: For transit packets exiting the router through the tunnel, forwarding table filtering is not supported on the interfaces you configure as the output interface for tunnel traffic.

A forwarding table filter allows you to filter data packets based on their components and to perform an action on packets that match the filter; it essentially controls which bearer packets the router accepts and forwards. To configure a forwarding table filter, include the **firewall** statement at the **[edit]** hierarchy level:

```
[edit]
firewall {
  family family-name {
    filter filter-name {
      term term-name {
        from {
          match-conditions;
        }
        then {
          action;
          action-modifiers;
        }
      }
    }
  }
}
```

family-name is the family address type: IPv4 (**inet**), IPv6 (**inet6**), Layer 2 traffic (**bridge**), or MPLS (**mpls**).

term-name is a named structure in which match conditions and actions are defined.

match-conditions are the criteria against which a bearer packet is compared; for example, the IP address of a source device or a destination device. You can specify multiple criteria in a match condition.

action specifies what happens if a packet matches all criteria; for example, the gateway GPRS support node (GGSN) accepting the bearer packet, performing a lookup in the forwarding table, and forwarding the packet to its destination; discarding the packet; and discarding the packet and returning a rejection message.

action-modifiers are actions that are taken in addition to the GGSN accepting or discarding a packet when all criteria match; for example, counting the packets and logging a packet.

To create a forwarding table, include the **instance-type** statement with the **forwarding** option at the **[edit routing-instances *instance-name*]** hierarchy level:

```
[edit]
routing-instances instance-name {
  instance-type forwarding;
}
```

To apply a forwarding table filter to a VPN routing and forwarding (VRF) table, include the **filter** and **input** statements at the **[edit routing-instance *instance-name* forwarding-options family *family-name*]** hierarchy level:

```
[edit routing-instances instance-name]
instance-type forwarding;
forwarding-options {
  family family-name {
```

```

    filter {
      input filter-name;
    }
  }
}

```

To apply a forwarding table filter to a forwarding table, include the **filter** and **input** statements at the **[edit forwarding-options family *family-name*]** hierarchy level:

```

[edit forwarding-options family family-name]
filter {
  input filter-name;
}

```

To apply a forwarding table filter to the default forwarding table **inet.0**, which is not associated with a specific routing instance, include the **filter** and **input** statements at the **[edit forwarding-options family inet]** hierarchy level:

```

[edit forwarding-options family inet]
filter {
  input filter-name;
}

```

Related Documentation

- [Guidelines for Configuring Firewall Filters](#)
- [Guidelines for Applying Standard Firewall Filters](#)
- [Applying Forwarding Table Filters on page 60](#)

Forwarding Table Filters for Routing Instances on ACX Series Routers

Forwarding table filter is a mechanism by which all the packets forwarded by a certain forwarding table are subjected to filtering and if a packet matches the filter condition, the configured action is applied on the packet. You can use the forwarding table filter mechanism to apply a filter on all interfaces associated with a single routing instance with a simple configuration. You can apply a forwarding table filter to a routing instance of type forwarding and also to the default routing instance **inet.0**. To configure a forwarding table filter, include the **filter *filter-name*** statement at the **[edit firewall family inet]** hierarchy level.

The following limitations apply to forwarding table filters configured on routing instances:

- You cannot attach the same filter to more than one routing instance.
- You cannot attach the same filter at both the **[edit interfaces *interface-name* family inet filter input *filter-name*]** and **[edit routing-instances *instance-name* forwarding-options family inet filter input *filter-name*]** hierarchy level.
- You cannot attach a filter that is either interface-specific or a physical interface filter.
- You cannot attach a filter to the egress direction of routing instances.

Related Documentation

- [Configuring Forwarding Table Filters on page 57](#)

Applying Forwarding Table Filters

A forwarding table filter allows you to filter data packets based on their components and perform an action on packets that match the filter. You can apply a filter on the ingress or egress packets of a forwarding table. You configure the filter at the **[edit firewall family *family-name*]** hierarchy level; for more information, see “[Configuring Forwarding Table Filters](#)” on page 57.

To apply a forwarding table filter on ingress packets of a forwarding table, include the **filter** and **input** statements at the **[edit forwarding-options family *family-name*]** hierarchy level:

```
[edit forwarding-options family family-name]
filter {
  input filter-name;
}
```

On the MX Series router only, to apply a forwarding table filter for a virtual switch, include the **filter** and **input** statements at the **[edit routing-instances *routing-instance-name* bridge-domains *bridge-domain-name* forwarding-options]** hierarchy level:

```
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name
 forwarding-options]
filter {
  input filter-name;
}
```

For more information about how to configure a virtual switch, see the *Junos OS Layer 2 Switching and Bridging Library for Routing Devices*.

You can filter based upon destination-class information by applying a firewall filter on the egress packets of the forwarding table. By applying firewall filters to packets that have been forwarded by a routing table, you can match based on certain parameters that are decided by the route lookup. For example, routes can be classified into specific destination and source classes. Firewall filters used for policing and mirroring are able to match based upon these classes.

To apply a firewall filter on egress packets of a forwarding table, include the **filter** and **output** statements at the **[edit forwarding-options family *family-name*]** hierarchy level:

```
[edit forwarding-options family family-name]
filter {
  output filter-name;
}
```



NOTE: The egress forwarding table filter is applied on the ingress interface of the Flexible PIC Concentrator (FPC). If different packets to the same destination arrive on different FPCs, they might encounter different policers.



NOTE: You cannot simultaneously attach to the same interface a firewall filter that includes the `interface-group` match condition and an egress forwarding table filter. The `interface-group` match condition matches the logical interface on which the packet was *received* to a specified interface group or set of interface groups. Forwarding table filters in general apply to local packets (host inbound or outbound traffic) in addition to data packets (or transit traffic), but *egress* forwarding table filters in particular apply to host *outbound* traffic and transit packets traffic only.



NOTE: In Junos OS Release 8.4 and later, you can no longer configure this output statement for VPLS. You can continue to configure ingress forwarding table filters with the input statement at the `[edit forwarding-options family vpls filter]` hierarchy level.



NOTE: For T Series routers other than T4000, a packet forwarded by the forwarding table reaches the egress forwarding table filter irrespective of whether the packet is actually forwarded by the forwarding table or not. The packet reaches the egress filter even if the route points to reject or discard next hops.

On T4000 Type 5 FPC, the packet reaches the egress filter only if it is forwarded by the forwarding table.

To apply a forwarding table filter to a flood table, include the **flood** and **input** statements at the `[edit forwarding-options family family-name]` hierarchy level:

```
[edit forwarding-options family vpls]
flood {
  input filter-name;
}
```



NOTE: The **flood** statement is valid for the vpls protocol family only.

On MX Series 3D Universal Edge Routers, you can apply a forwarding table filter by using the **source-checking** statement at the `[edit forwarding-options family inet6]` hierarchy level:

```
[edit forwarding-options family inet6]
family inet6 {
  source-checking;
}
```

This discards IPv6 packets when the source address type is unspecified, loopback, multicast or link-local.

RFC 4291, *IP Version 6 Addressing Architecture*, refers to four address types that require special treatment when they are used as source addresses. The four address types are:

- Unspecified
- Loopback
- Multicast
- Link-Local Unicast

The loopback and multicast addresses must never be used as a source address in IPv6 packets. The unspecified and link-local addresses can be used as source addresses but routers must never forward packets that have these addresses as source addresses. Typically, packets that contain unspecified or link-local addresses as source addresses are delivered to the local host. If the destination is not the local host, then the packet must not be forwarded. Configuring this statement filters or discards IPv6 packets of these four address types.

CHAPTER 5

Configuring Forwarding Options for Load Balancing Traffic

- [Configuring Load Balancing for Ethernet Pseudowires on page 63](#)
- [Configuring Load-Balance Groups on page 65](#)
- [Understanding Per-Packet Load Balancing on page 65](#)
- [Configuring Per-Packet Load Balancing on page 66](#)
- [Per-Flow and Per-Prefix Load Balancing Overview on page 69](#)
- [Configuring Per-Prefix Load Balancing on page 69](#)
- [Configuring Per-Flow Load Balancing Based on Hash Values on page 70](#)
- [Understanding ECMP Flow-Based Forwarding on page 71](#)
- [Example: Configuring ECMP Flow-Based Forwarding on page 72](#)
- [Configuring Load Balancing Based on MAC Addresses on page 76](#)
- [Load Balancing VPLS Non-Unicast Traffic Across Member Links of an Aggregate Interface on page 77](#)
- [Example: Configuring Multicast Load Balancing over Aggregated Ethernet Links on page 78](#)

Configuring Load Balancing for Ethernet Pseudowires

You can configure load balancing for IPv4 traffic over Layer 2 Ethernet pseudowires. You can also configure load balancing for Ethernet pseudowires based on IP information. The option to include IP information in the hash key provides support for Ethernet circuit cross-connect (CCC) connections.



NOTE: This feature is supported only on M120, M320, MX Series, and T Series routers.

To configure load balancing for IPv4 traffic over Layer 2 Ethernet pseudowires, include the **ether-pseudowire** statement at the **[edit forwarding-options hash-key family mpls payload]** hierarchy level:

[edit forwarding-options]

```

hash-key {
  family mpls {
    (label-1 | no-labels);
    payload {
      ether-pseudowire;
    }
  }
}

```



NOTE: You must also configure either the `label-1` or the `no-labels` statement at the `[edit forwarding-options hash-key family mpls]` hierarchy level.

You can also configure load balancing for Ethernet pseudowires based on IP information. This functionality provides support for load balancing for Ethernet cross-circuit connect (CCC) connections. To include IP information in the hash key, include the `ip` statement at the `[edit forwarding-options hash-key family mpls payload]` hierarchy level:

```

[edit forwarding-options]
hash-key {
  family mpls {
    (label-1 | no-labels);
    payload {
      ip;
    }
  }
}

```



NOTE: You must also configure either the `label-1` or `no-labels` statement at the `[edit forwarding-options hash-key family mpls]` hierarchy level.

You can configure load balancing for IPv4 traffic over Ethernet pseudowires to include only Layer 3 IP information in the hash key. To include only Layer 3 IP information, include the `layer-3-only` option at the `[edit forwarding-options family mpls hash-key payload ip]` hierarchy level:

```

[edit forwarding-options]
hash-key {
  family mpls {
    (label-1 | no-labels);
    payload {
      ip {
        layer-3-only;
      }
    }
  }
}

```



NOTE: You must also configure either the `label-1` or `no-labels` statement at the `[edit forwarding-options hash-key family mpls]` hierarchy level.

Configuring Load-Balance Groups

In addition to including policers in firewall filters, you can configure a load-balance group that is not part of a firewall filter configuration. A load-balance group contains interfaces that all use the same next-hop group characteristic to load-balance the traffic.

To configure a load-balance group, include the **load-balance-group** statement at the **[edit firewall]** hierarchy level:

```
[edit firewall]
load-balance-group group-name {
  next-hop-group[ group-names ];
}
```

Next-hop groups allow you to include multiple interfaces used to forward duplicate packets used in port mirroring. For more information about next-hop groups, see [“Configuring Next-Hop Groups to Use Multiple Interfaces to Forward Packets Used in Port Mirroring” on page 49](#).

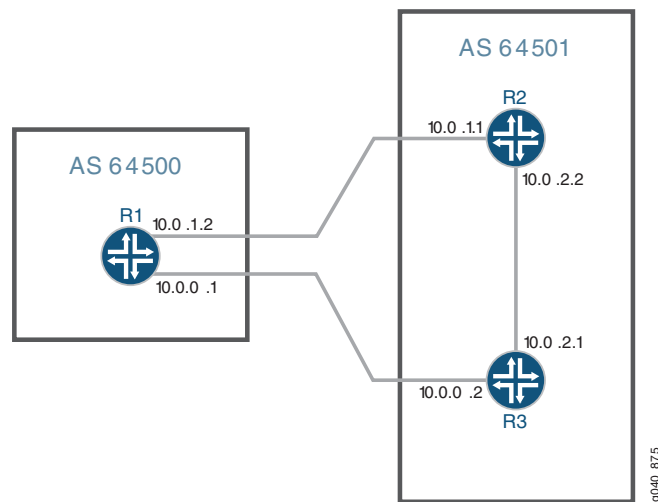
Understanding Per-Packet Load Balancing

By default, when there are multiple equal-cost paths to the same destination for the active route, Junos OS uses a hash algorithm to choose one of the next-hop addresses to install in the forwarding table. Whenever the set of next hops for a destination changes in any way, the next-hop address is rechosen using the hash algorithm.

You can configure Junos OS so that, for the active route, all next-hop addresses for a destination are installed in the forwarding table. This feature is called per-packet load balancing. You can use load balancing to spread traffic across multiple paths between routers.

[Figure 2 on page 66](#) shows a simple load balancing scenario. Device R1 is in AS 65000 and is connected to both Device R2 and Device R3, which are in AS 65001. Device R1 can be configured to load balance traffic across the two links.

Figure 2: Simple Load Balancing Scenario



Starting in Junos OS 13.3R3, for MX Series 3D Universal Edge routers with modular port concentrators (MPCs) only, you can configure consistent load balancing, which prevents the reordering of all flows to active paths in an equal-cost multipath (ECMP) group when one or more next-hop paths fail. Only flows for paths that are inactive are redirected to another active next-hop path. Flows mapped to servers that remain active are maintained. This feature applies only to external BGP peers.

Related Documentation

- *Example: Load Balancing BGP Traffic*
- [Configuring Per-Packet Load Balancing on page 66](#)
- *Configuring Load Balancing Based on MPLS Labels*
- [Configuring Load Balancing for Ethernet Pseudowires on page 63](#)
- [Configuring Load Balancing Based on MAC Addresses on page 76](#)
- *Configuring VPLS Load Balancing Based on IP and MPLS Information*
- *Configuring VPLS Load Balancing on MX Series 3D Universal Edge Routers*
- *Configuring Consistent Load Balancing for ECMP Groups*

Configuring Per-Packet Load Balancing

To configure per-packet load balancing as described in “[Understanding Per-Packet Load Balancing](#)” on page 65, include the **load-balance per-packet** statement either as an option of the **route-filter** statement at the **[edit policy-options policy-statement *policy-name* term *term-name* from]** hierarchy level:

```

[edit policy-options policy-statement policy-name term term-name from]
route-filter destination-prefix match-type {
  load-balance per-packet;
}
  
```

or at the `[edit policy-options policy-statement policy-name term term-name then]` hierarchy level:

```
[edit policy-options policy-statement policy-name term term-name then]
load-balance per-packet;
```

To complete the configuration you must apply the routing policy to routes exported from the routing table to the forwarding table, by including the policy name in the list specified by the **export** statement:

```
export [ policy-names ];
```

You can include this statement at the following hierarchy levels:

- `[edit routing-options forwarding-table]`
- `[edit logical-systems logical-system-name routing-options forwarding-table]`

By default, the software ignores port data when determining flows. To enable per-flow load balancing, you must set the **load-balance per-packet** action in the routing policy configuration.

To include port data in the flow determination, include the **family inet** statement at the `[edit forwarding-options hash-key]` hierarchy level:

```
[edit forwarding-options hash-key]
family inet {
    layer-3;
    layer-4;
}
```

If you include both the **layer-3** and **layer-4** statements, the router uses the following Layer 3 and Layer 4 information to load-balance:

- Source IP address
- Destination IP address
- Protocol
- Source port number
- Destination port number
- Incoming interface index
- IP type of service

The router recognizes packets in which all of these **layer-3** and **layer-4** parameters are identical, and ensures that these packets are sent out through the same interface. This prevents problems that might otherwise occur with packets arriving at their destination out of their original sequence.

This is appropriate behavior for Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packets. For Internet Control Message Protocol (ICMP) packets, the field location offset is the checksum field, which makes each ping packet a separate “flow.” There are other protocols that can be encapsulated in IP that may have a varying value

in the 32-bit offset. This may also be problematic because these protocols are seen as a separate flow.

With M Series (with the exception of the M120 router) and T Series routers, the first fragment is mapped to the same load-balanced destination as the unfragmented packets. The other fragments can be mapped to other load-balanced destinations.

For the M120 router only, all fragments are mapped to the same load-balanced destination. This destination is not necessarily the same as that for unfragmented packets.

By default, or if you include only the **layer-3** statement, the router uses the incoming interface index as well as the following Layer 3 information in the packet header to load balance traffic:

- Source IP address
- Destination IP address
- Protocol

By default, IP version 6 (IPv6) packets are automatically load-balanced based on the following Layer 3 and Layer 4 information:

- Source IP address
- Destination IP address
- Protocol
- Source port number
- Destination port number
- Incoming interface index
- Traffic class

Per-Packet Load Balancing Examples

Perform per-packet load balancing for all routes:

```
[edit]
policy-options {
  policy-statement load-balancing-policy {
    then {
      load-balance per-packet;
    }
  }
}
routing-options {
  forwarding-table {
    export load-balancing-policy;
  }
}
```

Perform per-packet load balancing only for a limited set of routes:

```
[edit]
policy-options {
  policy-statement load-balancing-policy {
    from {
      route-filter 192.168.10/24 orlonger;
      route-filter 10.114/16 orlonger;
    }
    then {
      load-balance per-packet;
    }
  }
}
routing-options {
  forwarding-table {
    export load-balancing-policy;
  }
}
```

Per-Flow and Per-Prefix Load Balancing Overview

By default, when there are multiple equal-cost paths to the same destination, Junos OS chooses one of the next-hop addresses at random.

On all M Series Multiservice Edge Routers, MX Series 3D Universal Edge Routers, and T Series Core Routers, you have the additional option of configuring per-prefix load balancing based on a specified hash value that enables the router to elect a next hop independently of the route chosen by other routers.

On the M120, M320, and MX Series routers only, you have the additional option of enabling per-flow load balancing based on a unique, load-balance hash value for each Packet Forwarding Engine slot.

- Related Documentation**
- [Configuring Per-Prefix Load Balancing on page 69](#)
 - [Configuring Per-Flow Load Balancing Based on Hash Values on page 70](#)

Configuring Per-Prefix Load Balancing

By default, Junos OS uses a hashing method based only on the destination address to elect a forwarding next hop when multiple equal-cost paths are available. As a result, when multiple routers or switches share the same set of forwarding next hops for a given destination, they can elect the same forwarding next hop.

You can enable router-specific or switch-specific load balancing by including a per-prefix hash value. However, this method applies only to indirect next hops. In other words, when we have a route with a protocol next hop that is not directly connected, it can be resolved over a set of equal-cost forwarding next hops. Only in this case, we use the hashing algorithm to elect a forwarding next hop. An example of this is routes learned from an IBGP neighbor. The protocol next hop for those routes might not be directly reachable and would be resolved through some IGP or static routes. The result could be a set of equal-cost forwarding next hops to reach that protocol next hop. Per-prefix load balancing thus leads to better utilization of the available links.

To configure per-prefix load balancing, include the **load-balance** statement at the **[edit forwarding-options]** hierarchy level:

```
[edit forwarding-options]
load-balance {
  indexed-load-balance;
  per-prefix {
    hash-seed number;
  }
}
```

To enable per-prefix load balancing, you must include the **hash-seed *number*** statement. The range that you can configure is 0 (the default) through 65,535. If no hash seed is configured, the elected forwarding next hop is the same as in previous releases.

If you notice an issue with the load-balance distribution, try including the **indexed-load-balance** statement at the **[edit forwarding-options load-balance]** hierarchy level to see if this resolves the issue. The **indexed-load-balance** statement causes the creation of a nexthop structure that is not a function of the hash only, but is also a function of the low-order bits of the IP address.



CAUTION: Including the **indexed-load-balance** statement causes an increase in memory usage on the device.

indexed-load-balance;

Configuring Per-Flow Load Balancing Based on Hash Values

By default, Junos OS uses a hashing method based only on the destination address to elect a forwarding next hop when multiple equal-cost paths are available. All Packet Forwarding Engine slots are assigned the same hash value by default.

You can enable router-specific or switch-specific load balancing by configuring the router or switch to assign a unique, load-balance hash value for each Packet Forwarding Engine slot.



NOTE: This feature is supported only on M120, M320, and MX Series routers.

To configure per-flow load balancing, include the **load-balance** statement at the **[edit forwarding-options]** hierarchy level:

```
[edit forwarding-options]
load-balance {
  indexed-load-balance;
  per-flow {
    hash-seed;
  }
}
```

To enable per-flow load balancing, you must include the **hash-seed** statement. Junos OS automatically chooses a value for the hashing algorithm. You cannot configure a specific value for the **hash-seed** statement when you enable per-flow load balancing.

Understanding ECMP Flow-Based Forwarding

An equal-cost multipath (ECMP) set is formed when the routing table contains multiple next-hop addresses for the same destination with equal cost. (Routes of equal cost have the same preference and metric values.) If there is an ECMP set for the active route, Junos OS uses a hash algorithm to choose *one* of the next-hop addresses in the ECMP set to install in the forwarding table.

You can configure Junos OS so that multiple next-hop entries in an ECMP set are installed in the forwarding table. On Juniper Networks devices, per-flow load balancing can be performed to spread traffic across multiple paths between routing devices. On Juniper Networks security devices, source and destination IP addresses and protocols are examined to determine individual traffic flows. Packets for the same flow are forwarded on the same interface; the interface does not change when there are additions or changes to the ECMP set. This is important for features such as source NAT, where the translation is performed only during the first path of session establishment; IDP; ALG; and route-based VPN tunnels. If a packet arrives on a given interface in an ECMP set, the security device ensures that reverse traffic is forwarded through the same interface.



NOTE: ECMP flow-based forwarding on security devices applies to IPv4 and IPv6 unicast traffic flows. Starting with 15.1X49-D60, ECMP flow-based forwarding of IPv6 unicast traffic is supported on all SRX Series devices and vSRX instances. Multicast flow is not supported.

On Juniper Networks security devices, the maximum number of next-hop addresses in an ECMP set that can be installed in the forwarding table is 16. If there are more than 16 next-hop addresses in an ECMP set, only the first 16 addresses are used.

In a chassis cluster deployment, a *local* interface is an interface that is on the same node as the interface on which a packet arrives, and a *remote* interface is an interface that is on the other chassis cluster node. If an ECMP route has both local and remote interfaces in a chassis cluster, then the local interface is favored for the next hop.

If a next-hop address is no longer part of the ECMP set or if it is removed from the routing table because of a route change, a flow that uses the next hop is rerouted and the session is not affected. Rerouting of the flow also occurs if there is a configuration change that takes away the next-hop address or if an administrator takes down the next-hop interface without deleting it. If a next-hop address is removed from the routing table because the interface is deleted or the session is intentionally cleared, the session is killed without being rerouted.



NOTE: We recommend that interfaces in an ECMP set be in the same security zone. If a flow is rerouted and the rerouted flow uses an interface in a different security zone than the original route, the session is killed.

To configure ECMP flow-based forwarding on Juniper Networks security devices, first define a load-balancing routing policy by including one or more **policy-statement** configuration statements at the **[edit policy-options]** hierarchy level, with the action **load-balance per-packet**. Then apply the routing policy to routes exported from the routing table to the forwarding table. To do this, include the **forwarding-table** and **export** configuration statements at the **[edit routing-options]** hierarchy level.

**Related
Documentation**

- [Example: Configuring ECMP Flow-Based Forwarding on page 72](#)
- [Understanding Routing Policies](#)
- [Categories of Routing Policy Match Conditions](#)
- [Summary of Routing Policy Actions](#)

Example: Configuring ECMP Flow-Based Forwarding

This example shows how to configure ECMP flow-based forwarding.

- [Requirements on page 72](#)
- [Overview on page 72](#)
- [Configuration on page 73](#)
- [Verification on page 76](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

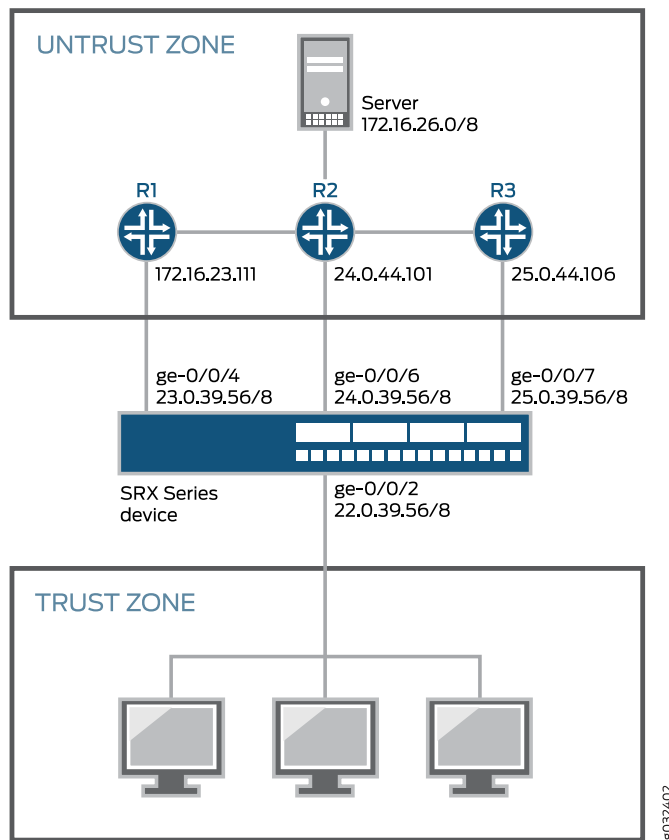
Overview

This example configures three static ECMP routes on an SRX Series device. Each static route uses a different router to reach the destination server. The interfaces to the routers are assigned to the untrust security zone. This example creates a load-balancing routing policy named **load-balancing-policy** and applies the policy to all routes exported from the routing table to the forwarding table.

Topology

[Figure 3 on page 73](#) shows the topology used in this example.

Figure 3: ECMP Routes



Configuration

CLI Quick Configuration

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

```
set interfaces ge-0/0/2 unit 0 family inet address 22.0.39.56/8
set interfaces ge-0/0/4 unit 0 family inet address 23.0.39.56/8
set interfaces ge-0/0/6 unit 0 family inet address 24.0.39.56/8
set interfaces ge-0/0/7 unit 0 family inet address 25.0.39.56/8
set routing-options static route 26.0.0.0/8 next-hop 23.0.54.111
set routing-options static route 26.0.0.0/8 next-hop 24.0.44.101
set routing-options static route 26.0.0.0/8 next-hop 25.0.44.106
set security zones security-zone trust interfaces ge-0/0/2
set security zones security-zone untrust interfaces ge-0/0/4 ge-0/0/6 ge-0/0/7
set security policies from-zone trust to-zone untrust policy permit-mail match
  source-address 22.0.39.56/8
set security policies from-zone trust to-zone untrust policy permit-mail match
  destination-address 26.0.0.0/8
set security policies from-zone trust to-zone untrust policy permit-mail match application
  junos-mail
set security policies from-zone trust to-zone untrust policy permit-mail then permit
```

```
set policy-options policy-statement load-balancing-policy then load-balance per-packet
set routing-options forwarding-table export load-balancing-policy
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure ECMP flow-based forwarding:

1. Configure interfaces.

```
[edit interaces]
user@host# set ge-0/0/2 unit 0 family inet address 22.0.39.56/8
user@host# set ge-0/0/4 unit 0 family inet address 23.0.39.56/8
user@host# set ge-0/0/6 unit 0 family inet address 24.0.39.56/8
user@host# set ge-0/0/7 unit 0 family inet address 25.0.39.56/8
```

2. Create security zones.

```
[edit security]
user@host# set zones security-zone trust interfaces ge-0/0/2
user@host# set zones security-zone untrust interfaces ge-0/0/4
user@host# set zones security-zone untrust interfaces ge-0/0/6
user@host# set zones security-zone untrust interfaces ge-0/0/7
```

3. Configure a security policy.

```
[edit security policies from-zone trust to-zone untrust]
user@host# set policy permit-mail match source-address 22.0.39.56/8
user@host# set policy permit-mail match destination-address 26.0.0.0/8
user@host# set policy permit-mail match application junos-mail
user@host# set policy permit-mail then permit
```

4. Configure ECMP routes.

```
[edit routing-options]
user@host# set static route 26.0.0.0/8 next-hop 23.0.54.111
user@host# set static route 26.0.0.0/8 next-hop 24.0.44.101
user@host# set static route 26.0.0.0/8 next-hop 25.0.44.106
```

5. Create a load-balancing routing policy.

```
[edit policy-options]
user@host# set policy-statement load-balancing-policy then load-balance per-packet
```

6. Apply the routing policy to all routes exported from the routing table to the forwarding table.

```
[edit routing-options]
user@host# set forwarding-table export load-balancing-policy
```

Results From configuration mode, confirm your configuration by issuing the **show interfaces**, **show security**, **show policy-options**, and **show routing-options** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# show interfaces
ge-0/0/2 {
```

```
    unit 0 {
      family inet {
        address 22.0.39.56/8;
      }
    }
  }
ge-0/0/4 {
  unit 0 {
    family inet {
      address 23.0.39.56/8;
    }
  }
}
ge-0/0/6 {
  unit 0 {
    family inet {
      address 24.0.39.56/8;
    }
  }
}
ge-0/0/7 {
  unit 0 {
    family inet {
      address 25.0.39.56/8;
    }
  }
}
}
user@host# show security
policies {
  from-zone trust to-zone untrust {
    policy permit-mail {
      match {
        source-address 22.0.39.56/8;
        destination-address 26.0.0.0/8;
        application junos-mail;
      }
      then {
        permit;
      }
    }
  }
}
zones {
  security-zone trust {
    interfaces {
      ge-0/0/2.0;
    }
  }
  security-zone untrust {
    interfaces {
      ge-0/0/4.0;
      ge-0/0/6.0;
      ge-0/0/7.0;
    }
  }
}
```

```

user@host# show policy-options
policy-statement load-balancing-policy {
    then {
        load-balance per-packet;
    }
}

[edit]
user@host# show routing-options
forwarding-table {
    export load-balancing-policy;
}
static {
    route 0.0.0.0/0 next-hop 10.100.37.1;
    route 26.0.0.0/8 next-hop [ 23.0.54.111 25.0.44.106 24.0.44.101 ];
}

```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying the Forwarding Table

Purpose Verify that the route information for all ECMP routes appears in the forwarding table.

Action From operational mode, enter the **show route forwarding-table** command.

```

user@host> show route forwarding-table
Routing table: default.inet
Internet:
Destination          Type RtRef Next hop          Type Index NhRef Netif
...
26.0.0.0/8           user    0 23.0.54.111    rslv    0    1 ge-0/0/4.0
26.0.0.0/8           user    0 24.0.44.101    rslv    0    1 ge-0/0/6.0
26.0.0.0/8           user    0 25.0.44.106    rslv    0    1 ge-0/0/7.0
...

```

Related Documentation

- [Understanding ECMP Flow-Based Forwarding on page 71](#)

Configuring Load Balancing Based on MAC Addresses

The hash key mechanism for load-balancing uses Layer 2 media access control (MAC) information such as frame source and destination address. To load-balance traffic based on Layer 2 MAC information, include the **family multiservice** statement at the **[edit forwarding-options hash-key]** hierarchy level:

```

family multiservice {
    destination-mac;
    source-mac;
}

```

To include the destination-address MAC information in the hash key, include the **destination-mac** option. To include the source-address MAC information in the hash key, include the **source-mac** option.



NOTE: Any packets that have the same source and destination address will be sent over the same path.



NOTE: You can configure per-packet load balancing to optimize VPLS traffic flows across multiple paths.



NOTE: Aggregated Ethernet member links will now use the physical MAC address as the source MAC address in 802.3ah OAM packets.

Related Documentation

- *Junos OS VPNs Library for Routing Devices*

Load Balancing VPLS Non-Unicast Traffic Across Member Links of an Aggregate Interface

By default, VPLS non-unicast (or BUM — broadcast, unknown, and multicast) traffic sent across aggregate Ethernet interfaces is sent across only one member link of the aggregate interface. Starting with Junos OS Release 14.1, you can configure each VPLS instance to load balance BUM traffic across all members of an aggregate interface. This is referred to as BUM hashing.

To enable BUM hashing for an VPLS instance, add **bum-hashing** to the routing instance at the **[edit routing-instances instance-name protocols vpls]** hierarchy level. For example:

```
[edit routing-instances]
instance-name {
  protocols {
    vpls {
      bum-hashing;
    }
  }
}
```



WARNING: Enabling or disabling BUM hashing on a VPLS routing instance causes the routing instance to be destroyed and re-created when the configuration change is committed.

You can also specify which forwarding class to use for forwarding BUM traffic. When CoS-based forwarding (CBF) is configured on a VPLS PE router, BUM traffic uses the default forwarding class to select the label-switched path (LSP). Starting with Junos OS Release 14.1, you can associate an LSP with the default forwarding class.

To associate an LSP with the default forwarding class, add the **forwarding-class-default** statement at the **[edit class-of-service forwarding-policy next-hop-map next-hop-map-name]** hierarchy level. For example:

```
[edit class-of-service forwarding-policy next-hop-map next-hop-map-name]
forwarding-class-default {
    lsp-next-hop value;
}
```

**Related
Documentation**

- [bum-hashing on page 106](#)
- [Example: Configuring Multicast Load Balancing over Aggregated Ethernet Links on page 78](#)

Example: Configuring Multicast Load Balancing over Aggregated Ethernet Links

This example shows how to configure point-to-multipoint LSPs to load balance across aggregated Ethernet links. The load balancing applies to all traffic types, including multicast. Feature parity for multicast load balancing of point-to-multipoint LSPs over aggregated Ethernet child links on the MX Series routers with MPCs or MICs is supported in Junos OS Releases 11.1R2, 11.2R2, and 11.4.



NOTE: VPLS multicast load balancing requires Junos OS Release 14.1 or later.

- [Requirements on page 78](#)
- [Overview on page 78](#)
- [Configuration on page 79](#)
- [Verification on page 89](#)

Requirements

Before you begin:

1. Configure the router interfaces.
2. Configure an interior gateway protocol or static routing. See the *Junos OS Routing Protocols Library for Routing Devices*.

Overview

This example shows a sample topology and configuration to perform the following tasks:

- Load balancing VPLS multicast traffic over link aggregation
- Load balancing point-to-multipoint multicast traffic over link aggregation
- Re-load balancing after a change in the next-hop topology

Next-hop topology changes might include but are not limited to:

- Layer 2 membership change in the link aggregation

- Indirect next-hop change
- Composite next-hop change

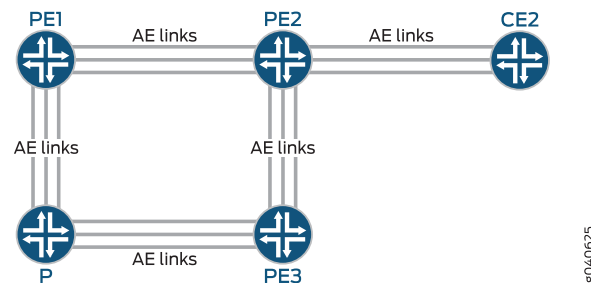
Load balancing is hash-based, so the higher the number of flows, the better. As is the case with unicast, you can also configure the hash key to be based on Layer 3 and Layer 4 information to achieve a better load-balancing result. There are a few exceptions that are specific to multicast traffic, which might lead to uneven load balancing—for example, when the outgoing interface list includes multiple aggregated interfaces with an unequal number of child links.



NOTE: For Draft Rosen multicast VPNs (MVPNs), load balancing over aggregated Ethernet interfaces is uneven when the LAGs are all core interfaces. In the case of Next-Generation MBGP MPVNs, multicast traffic is sent over point-to-multipoint and RSVP, and the hash is computed up to the IP headers. In the Draft Rosen case, multicast traffic is tunneled over GRE tunnels, and the hash is used only on GRE tunnel headers. This is why load balancing is not even for Draft Rosen when the LAGs are all core interfaces.

Figure 4 on page 79 shows the topology for this example. The example includes the configuration for Devices PE1 and PE2.

Figure 4: Multicast Load Balancing over Aggregated Ethernet Links



Configuration

CLI Quick Configuration

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

Device PE1

[edit]

```
set forwarding-options hash-key family multiservice source-mac
set forwarding-options hash-key family multiservice destination-mac
set forwarding-options hash-key family multiservice payload ip layer-3
set interfaces ge-0/0/6 gigether-options 802.3ad ae0
set interfaces ge-0/1/6 gigether-options 802.3ad ae0
set interfaces ge-0/2/2 encapsulation ethernet-vpls
set interfaces ge-0/2/2 unit 0 family vpls
set interfaces ge-0/2/3 gigether-options 802.3ad ae0
set interfaces ge-0/2/6 gigether-options 802.3ad ae0
set interfaces ge-0/3/0 gigether-options 802.3ad ae0
```

```
set interfaces ge-0/3/1 gigether-options 802.3ad ae0
set interfaces ge-0/3/6 gigether-options 802.3ad ae0
set interfaces ge-1/0/6 gigether-options 802.3ad ae0
set interfaces ge-1/2/6 unit 0 family inet address 13.1.1.2/30
set interfaces ae0 unit 0 family inet address 11.11.11.1/30
set interfaces ae0 unit 0 family iso
set interfaces ae0 unit 0 family mpls
set policy-options policy-statement exp-to-fwd term a from community grn-com
set policy-options policy-statement exp-to-fwd term a then install-nexthop lsp PE1-to-PE2
set policy-options policy-statement exp-to-fwd term a then accept
set policy-options community grn-com members target:65000:1
set protocols rsvp interface all
set protocols mpls interface fxp0.0 disable
set protocols mpls label-switched-path PE1-to-PE2 to 10.255.19.77
set protocols mpls label-switched-path PE1-to-PE3 to 10.255.19.79
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols bgp group int type internal
set protocols bgp group int local-address 10.255.71.214
set protocols bgp group int family inet any
set protocols bgp group int family l2vpn signaling
set protocols bgp group int neighbor 10.255.19.77
set protocols bgp group int neighbor 10.255.19.79
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set routing-instances vpls instance-type vpls
set routing-instances vpls interface ge-0/2/2.0
set routing-instances vpls route-distinguisher 65000:1
set routing-instances vpls vrf-target target:65000:1
set routing-instances vpls protocols vpls site-range 3
set routing-instances vpls protocols vpls no-tunnel-services
set routing-instances vpls protocols vpls site asia site-identifier 1
set routing-instances vpls protocols vpls site asia interface ge-0/2/2.0
set routing-instances vpls protocols vpls vpls-id 100
set routing-instances vpls protocols vpls burn-hashing
```

Device PE2

```
set interfaces ge-0/0/7 gigether-options 802.3ad ae0
set interfaces ge-0/1/7 gigether-options 802.3ad ae0
set interfaces ge-0/2/3 gigether-options 802.3ad ae0
set interfaces ge-0/2/7 gigether-options 802.3ad ae0
set interfaces ge-2/0/0 gigether-options 802.3ad ae1
set interfaces ge-2/0/1 gigether-options 802.3ad ae1
set interfaces ge-2/0/2 gigether-options 802.3ad ae1
set interfaces ge-2/0/4 encapsulation ethernet-vpls
set interfaces ge-2/0/4 unit 0 family vpls
set interfaces ge-2/0/7 gigether-options 802.3ad ae0
set interfaces ge-2/0/9 unit 0 family inet address 1.1.1.1/30
set interfaces ge-2/0/9 unit 0 family mpls
set interfaces ge-2/1/7 gigether-options 802.3ad ae0
set interfaces ge-2/2/7 gigether-options 802.3ad ae0
set interfaces ge-2/3/7 gigether-options 802.3ad ae0
set interfaces ae0 unit 0 family inet address 11.11.11.2/30
set interfaces ae0 unit 0 family iso
set interfaces ae0 unit 0 family mpls
set interfaces ae1 unit 0 family inet address 10.1.1.1/30
```

```

set interfaces ae1 unit 0 family mpls
set protocols rsvp interface all
set protocols rsvp interface fxp0.0 disable
set protocols mpls label-switched-path PE2-to-PE3 from 10.255.19.77
set protocols mpls label-switched-path PE2-to-PE3 to 10.255.19.79
set protocols mpls label-switched-path PE2-to-PE1 to 10.255.71.214
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols bgp group int type internal
set protocols bgp group int local-address 10.255.19.77
set protocols bgp group int family inet any
set protocols bgp group int family l2vpn signaling
set protocols bgp group int neighbor 10.255.71.214
set protocols bgp group int neighbor 10.255.19.79
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface ge-2/0/0.0
set protocols ospf area 0.0.0.0 interface ge-2/0/1.0
set protocols ospf area 0.0.0.0 interface ge-2/0/2.0
set protocols ospf area 0.0.0.0 interface ae0.0
set protocols ospf area 0.0.0.0 interface ae1.0
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set routing-instances vpls instance-type vpls
set routing-instances vpls interface ge-2/0/4.0
set routing-instances vpls route-distinguisher 65000:1
set routing-instances vpls vrf-target target:65000:1
set routing-instances vpls protocols vpls site-range 3
set routing-instances vpls protocols vpls no-tunnel-services
set routing-instances vpls protocols vpls site 2 site-identifier 2
set routing-instances vpls protocols vpls site 2 interface ge-2/0/4.0
set routing-instances vpls protocols vpls vpls-id 100
set routing-instances vpls protocols vpls bum-hashing

```

Step-by-Step Procedure To configure Device PE1:

1. Configure Device PE1 interfaces.

```

[edit interfaces]
user@PE1# set ge-0/0/6 gigether-options 802.3ad ae0
user@PE1# set ge-0/1/6 gigether-options 802.3ad ae0
user@PE1# set ge-0/2/2 encapsulation ethernet-vpls
user@PE1# set ge-0/2/2 unit 0 family vpls
user@PE1# set ge-0/2/3 gigether-options 802.3ad ae0
user@PE1# set ge-0/2/6 gigether-options 802.3ad ae0
user@PE1# set ge-0/3/0 gigether-options 802.3ad ae0
user@PE1# set ge-0/3/1 gigether-options 802.3ad ae0
user@PE1# set ge-0/3/6 gigether-options 802.3ad ae0
user@PE1# set ge-1/0/6 gigether-options 802.3ad ae0
user@PE1# set ge-1/2/6 unit 0 family inet address 13.1.1.2/30
user@PE1# set ae0 unit 0 family inet address 11.11.11.1/30
user@PE1# set ae0 unit 0 family iso
user@PE1# set ae0 unit 0 family mpls

```

2. On Device PE1, configure the packet header data to be used for per-flow load balancing.

```
[edit forwarding-options hash-key family multiservice]
user@PE1# set source-mac
user@PE1# set destination-mac
user@PE1# set payload ip layer-3
```

3. Configure the routing policy on Device PE1.

```
[edit policy-options]
user@PE1# set policy-statement exp-to-fwd term a from community grn-com
user@PE1# set policy-statement exp-to-fwd term a then install-nexthop lsp
PE1-to-PE2
user@PE1# set policy-statement exp-to-fwd term a then accept
user@PE1# set policy-options community grn-com members target:65000:1
```

4. Configure Device PE1 routing protocols and MPLS.

```
[edit protocols]
user@PE1# set rsvp interface all
user@PE1# set rsvp interface fxp0.0 disable
user@PE1# set mpls label-switched-path PE1-to-PE2 to 10.255.19.77
user@PE1# set mpls label-switched-path PE1-to-PE3 to 10.255.19.79
user@PE1# set mpls interface all
user@PE1# set mpls interface fxp0.0 disable
user@PE1# set bgp group int type internal
user@PE1# set bgp group int local-address 10.255.71.214
user@PE1# set bgp group int family inet any
user@PE1# set bgp group int family l2vpn signaling
user@PE1# set bgp group int neighbor 10.255.19.77
user@PE1# set bgp group int neighbor 10.255.19.79
user@PE1# set ospf traffic-engineering
user@PE1# set ospf area 0.0.0.0 interface all
user@PE1# set ospf area 0.0.0.0 interface fxp0.0 disable
```

5. Configure VPLS on Device PE1.

```
[edit routing-instances vpls]
user@PE1# set instance-type vpls
user@PE1# set interface ge-0/2/2.0
user@PE1# set route-distinguisher 65000:1
user@PE1# set vrf-target target:65000:1
user@PE1# set protocols vpls site-range 3
user@PE1# set protocols vpls no-tunnel-services
user@PE1# set protocols vpls site asia site-identifier 1
user@PE1# set protocols vpls site asia interface ge-0/2/2.0
user@PE1# set protocols vpls vpls-id 100
user@PE1# set protocols vpls bum-hashing
```

Step-by-Step Procedure To configure Device PE2:

1. Configure Device PE2 interfaces.

```
[edit interfaces]
user@PE2# set ge-0/0/7 gigether-options 802.3ad ae0
user@PE2# set ge-0/1/7 gigether-options 802.3ad ae0
```

```

user@PE2# set ge-0/2/3 gigether-options 802.3ad ae0
user@PE2# set ge-0/2/7 gigether-options 802.3ad ae0
user@PE2# set ge-2/0/0 gigether-options 802.3ad ae1
user@PE2# set ge-2/0/1 gigether-options 802.3ad ae1
user@PE2# set ge-2/0/2 gigether-options 802.3ad ae1
user@PE2# set ge-2/0/4 encapsulation ethernet-vpls
user@PE2# set ge-2/0/4 unit 0 family vpls
user@PE2# set ge-2/0/7 gigether-options 802.3ad ae0
user@PE2# set ge-2/0/9 unit 0 family inet address 1.1.1.1/30
user@PE2# set ge-2/0/9 unit 0 family mpls
user@PE2# set ge-2/1/7 gigether-options 802.3ad ae0
user@PE2# set ge-2/2/7 gigether-options 802.3ad ae0
user@PE2# set ge-2/3/7 gigether-options 802.3ad ae0
user@PE2# set ae0 unit 0 family inet address 11.11.11.2/30
user@PE2# set ae0 unit 0 family iso
user@PE2# set ae0 unit 0 family mpls
user@PE2# set ae1 unit 0 family inet address 10.1.1.1/30
user@PE2# set ae1 unit 0 family mpls

```

2. Configure Device PE2 routing protocols and MPLS.

```

[edit protocols]
user@PE2# set rsvp interface all
user@PE2# set rsvp interface fxp0.0 disable
user@PE2# set mpls label-switched-path PE2-to-PE3 from 10.255.19.77
user@PE2# set mpls label-switched-path PE2-to-PE3 to 10.255.19.79
user@PE2# set mpls label-switched-path PE2-to-PE1 to 10.255.71.214
user@PE2# set mpls interface all
user@PE2# set mpls interface fxp0.0 disable
user@PE2# set bgp group int type internal
user@PE2# set bgp group int local-address 10.255.19.77
user@PE2# set bgp group int family inet any
user@PE2# set bgp group int family l2vpn signaling
user@PE2# set bgp group int neighbor 10.255.71.214
user@PE2# set bgp group int neighbor 10.255.19.79
user@PE2# set ospf traffic-engineering
user@PE2# set ospf area 0.0.0.0 interface lo0.0
user@PE2# set ospf area 0.0.0.0 interface ge-2/0/0.0
user@PE2# set ospf area 0.0.0.0 interface ge-2/0/1.0
user@PE2# set ospf area 0.0.0.0 interface ge-2/0/2.0
user@PE2# set ospf area 0.0.0.0 interface ae0.0
user@PE2# set ospf area 0.0.0.0 interface ae1.0
user@PE2# set ospf area 0.0.0.0 interface all
user@PE2# set ospf area 0.0.0.0 interface fxp0.0 disable
user@PE2# set ldp interface all
user@PE2# set ldp interface fxp0.0 disable

```

3. Configure VPLS on Device PE2.

```

[edit routing-instances vpls]
user@PE2# set instance-type vpls
user@PE2# set interface ge-2/0/4.0
user@PE2# set route-distinguisher 65000:1
user@PE2# set vrf-target target:65000:1
user@PE2# set protocols vpls site-range 3
user@PE2# set protocols vpls no-tunnel-services
user@PE2# set protocols vpls site 2 site-identifier 2

```

```
user@PE2# set protocols vpls site 2 interface ge-2/0/4.0
user@PE2# set protocols vpls vpls-id 100
user@PE2# set protocols vpls bum-hashing
```

Results

From configuration mode, confirm your configuration by issuing the **show forwarding-options**, **show interfaces**, **show protocols**, **show policy-options**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Device PE1

```
user@PE1# show forwarding-options
hash-key {
  family multiservice {
    source-mac;
    destination-mac;
    payload {
      ip {
        layer-3;
      }
    }
  }
}
```

```
user@PE1# show interfaces
ge-0/0/6 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-0/1/6 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-0/2/2 {
  encapsulation ethernet-vpls;
  unit 0 {
    family vpls;
  }
}
ge-0/2/3 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-0/2/6 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-0/3/0 {
  gigether-options {
    802.3ad ae0;
  }
}
```

```

}
ge-0/3/1 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-0/3/6 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-1/0/6 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-1/2/6 {
  unit 0 {
    family inet {
      address 13.1.1.2/30;
    }
  }
}
ae0 {
  unit 0 {
    family inet {
      address 11.11.11.1/30;
    }
    family iso;
    family mpls;
  }
}

user@PE1# show protocols
mpls {
  interface all;
  interface fxp0.0 {
    disable;
  }
  label-switched-path PE1-to-PE2 {
    to 10.255.19.77;
  }
  label-switched-path PE1-to-PE3 {
    to 10.255.19.79;
  }
}
rsvp {
  interface all;
  interface fxp0.0 {
    disable;
  }
}
bgp {
  group int {
    type internal;
    local-address 10.255.71.214;
  }
}

```

```

        family inet {
            any;
        }
        family l2vpn {
            signaling;
        }
        neighbor 10.255.19.77;
        neighbor 10.255.19.79;
    }
}
ospf {
    traffic-engineering;
    area 0.0.0.0 {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
}

user@PE1# show policy-options
policy-statement exp-to-fwd {
    term a {
        from community grn-com;
        then {
            install-nexthop lsp PE1-to-PE2;
            accept;
        }
    }
}
community grn-com members target:65000:1;

user@PE1# show routing-instances
vpls {
    instance-type vpls;
    interface ge-0/2/2.0;
    route-distinguisher 65000:1;
    vrf-target target:65000:1;
    protocols {
        vpls {
            site-range 3;
            no-tunnel-services;
            site asia {
                site-identifier 1;
                interface ge-0/2/2.0;
            }
            vpls-id 100;
            bum-hashing;
        }
    }
}

Device PE2 user@PE2# show interfaces
ge-0/0/7 {
    gigether-options {
        802.3ad ae0;
    }
}

```

```
}
ge-0/1/7 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-0/2/3 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-0/2/7 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-2/0/0 {
  gigether-options {
    802.3ad ae1;
  }
}
ge-2/0/1 {
  gigether-options {
    802.3ad ae1;
  }
}
ge-2/0/2 {
  gigether-options {
    802.3ad ae1;
  }
}
ge-2/0/4 {
  encapsulation ethernet-vpls;
  unit 0 {
    family vpls;
  }
}
ge-2/0/7 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-2/0/9 {
  unit 0 {
    family inet {
      address 1.1.1.1/30;
    }
    family mpls;
  }
}
ge-2/1/7 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-2/2/7 {
```

```
    gigether-options {
      802.3ad ae0;
    }
  }
  ge-2/3/7 {
    gigether-options {
      802.3ad ae0;
    }
  }
  ae0 {
    unit 0 {
      family inet {
        address 11.11.11.2/30;
      }
      family iso;
      family mpls;
    }
  }
  ae1 {
    unit 0 {
      family inet {
        address 10.1.1.1/30;
      }
      family mpls;
    }
  }
}

user@PE2# show protocols
rsvp {
  interface all;
  interface fxp0.0 {
    disable;
  }
}
mpls {
  label-switched-path PE2-to-PE3 {
    from 10.255.19.77;
    to 10.255.19.79;
  }
  label-switched-path PE2-to-PE1 {
    to 10.255.71.214;
  }
  interface all;
  interface fxp0.0 {
    disable;
  }
}
bgp {
  group int {
    type internal;
    local-address 10.255.19.77;
    family inet {
      any;
    }
    family l2vpn {
      signaling;
    }
  }
}
```

```

    }
    neighbor 10.255.71.214;
    neighbor 10.255.19.79;
  }
}
ospf {
  traffic-engineering;
  area 0.0.0.0 {
    interface lo0.0;
    interface ge-2/0/0.0;
    interface ge-2/0/1.0;
    interface ge-2/0/2.0;
    interface ae0.0;
    interface ae1.0;
    interface all;
    interface fxp0.0 {
      disable;
    }
  }
}
ldp {
  interface all;
  interface fxp0.0 {
    disable;
  }
}

user@PE2# show routing-instances
vpls {
  instance-type vpls;
  interface ge-2/0/4.0;
  route-distinguisher 65000:1;
  vrf-target target:65000:1;
  protocols {
    vpls {
      site-range 3;
      no-tunnel-services;
      site 2 {
        site-identifier 2;
        interface ge-2/0/4.0;
      }
      vpls-id 100;
      bum-hashing;
    }
  }
}

```

Verification

You can monitor the operation of the routing instance by running the **show interfaces ae1.0 extensive** and **monitor interface traffic** commands.

For troubleshooting, you can configure tracing operations for all of the protocols.

- Related Documentation**
- *Configuring Point-to-Multipoint LSPs for an MBGP MVPN*
 - *Understanding Wildcards to Configure Selective Point-to-Multipoint LSPs for an MBGP MVPN*
 - *show interfaces (Aggregated Ethernet)*
 - [Load Balancing VPLS Non-Unicast Traffic Across Member Links of an Aggregate Interface on page 77](#)

CHAPTER 6

Configuring Other Forwarding Options

- [Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents on page 91](#)
- [Configuring DNS and TFTP Packet Forwarding on page 94](#)
- [Preventing DHCP Spoofing on MX Series 3D Universal Edge Routers on page 97](#)

Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents

You can configure the router, switch, or interface to act as a Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) relay agent. This means that a locally attached host can issue a DHCP or BOOTP request as a broadcast message. If the router, switch, or interface sees this broadcast message, it relays the message to a specified DHCP or BOOTP server.

You should configure the router, switch, or interface to be a DHCP and BOOTP relay agent if you have locally attached hosts and a distant DHCP or BOOTP server. For MX Series routers connected via IRB, see the note below to prevent BOOTP reply packets from being dropped.

To configure the router or switch to act as a DHCP and BOOTP relay agent, include the **bootp** statement at the **[edit forwarding-options helpers]** hierarchy level:

```
[edit forwarding-options helpers]
bootp {
  client-response-ttl number;
  description text-description;
  interface (interface-name | interface-group) {
    client-response-ttl number;
    description text-description;
    maximum-hop-count number;
    minimum-wait-time seconds;
    no-listen;
    server address {
      logical-system logical-system-name <routing-instance [ <default>
        routing-instance-names ]>;
      routing-instance [ <default> routing-instance-names ];
    }
  }
  maximum-hop-count number;
  minimum-wait-time seconds;
```

```
relay-agent-option;  
server server-identifier {  
    <logical-system logical-system-name>  
    <routing-instance [ routing-instance-names ]>;  
}
```

To set the description of the BOOTP service, DHCP service, or interface, include the **description** statement.

To set a logical interface or a group of logical interfaces with a specific DHCP relay or BOOTP configuration, include the **interface** statement.

To set the routing instance of the server to forward, include the **routing-instance** statement. You can include as many routing instances as necessary in the same statement.

To stop packets from being forwarded on a logical interface, a group of logical interfaces, or the router or switch, include the **no-listen** statement.

To set the maximum allowed number in the hops field of the BOOTP header, include the **maximum-hop-count** statement. Headers that have a larger number in the hops field are not forwarded. If you omit the **maximum-hop-count** statement, the default value is four hops.

To set the minimum allowed number of seconds in the **secs** field of the BOOTP header, include the **minimum-wait-time** statement. Headers that have a smaller number in the **secs** field are not forwarded. The default value for the minimum wait time is zero (0).

To set the IP address that specify the DHCP or BOOTP server for the router, switch, or interface, include the **server** statement. You can include multiple **server** statements.

To set an IP time-to-live (TTL) value for DHCP response packets sent to a DHCP client, include the **client-response-ttl** statement.

To use the DHCP relay agent option in relayed BOOTP/DHCP messages, include the **relay-agent-option** statement. This option is primarily useful for enabling DHCP forwarding between different VRF routing instances. This option is documented in RFC 3046, *DHCP Relay Agent Information Option*.

You can also configure an individual logical interface to be a DHCP and BOOTP relay agent if you have locally attached hosts and a remote DHCP or BOOTP server connected to one of the router's or switch's interfaces. For more information, see the *Junos OS Administration Library for Routing Devices*.

The following example demonstrates a BOOTP relay agent configuration.

```
user@host# show forwarding-options  
helpers {  
    bootp {  
        description "dhcp relay agent global parameters";  
        server 192.168.55.44;  
        server 172.16.0.3 routing-instance c3;  
        maximum-hop-count 10;  
        minimum-wait-time 8;
```

```

interface {
  fe-1/3/0 {
    description "use this info for this interface";
    server 10.10.10.10;
    server 192.168.14.14;
    maximum-hop-count 11;
    minimum-wait-time 3;
  }
  fe-1/3/1 {
    no-listen; ###ignore DHCPDISCOVER messages on this interface
  }
  all {
    description "globals apply to all other interfaces";
  }
}
}

```



BEST PRACTICE:

To use **bootp** helper on a MX Series router (MX80, MX240, MX480 and MX960) connected via IRB, you may need to take steps to ensure that DHCP discover packets (the bootp reply) are sent to clients and received as expected. Otherwise, bootp replies may be dropped because the DHCP client is clearing the broadcast bit in the discover packet, or because the DHCP server is stripping option-82 flags from the offer.

This happens when the IRB interface is a layer 3 (logical) interface associated with a bridge domain that has multiple layer 2 (physical) interfaces associated with it. In such cases, if the offer from the DHCP server is unicast and doesn't include an ingress interface identifying the physical interface on which the discovery packet was received, the MX router won't be able to determine an interface for sending out offers.

1. Enable broadcast on the IRB interface to flood discovery frames from all physical interfaces in the bridge domain. For example,

```

user@host# edit forwarding-options helpers bootp interface irb.0
broadcast;
server 202.67.4.1;
}

```

or,

2. Enable relay-agent-option on the bootp helper. For example,

```

user@host# edit forwarding-options helpers bootp
relay-agent-option;
server 202.67.4.1;
}

```

3. Configure the IRB interface connected to the DHCP server so it echoes option-82 flags back to the router. This will ensure that the option-82 string, which identifies the interface used by the router, is preserved.

Configuring DNS and TFTP Packet Forwarding

You can configure the router or switch to support Domain Name System (DNS) and Trivial File Transfer Protocol (TFTP) packet forwarding for IPv4 traffic, which allows clients to send DNS or TFTP requests to the router or switch. The responding DNS or TFTP server recognizes the client address and sends a response directly to that address. By default, the router or switch ignores DNS and TFTP request packets.

To enable DNS or TFTP packet forwarding, include the **helpers** statement at the **[edit forwarding-options]** hierarchy level:

```
[edit forwarding-options]
helpers {
  domain {
    description text-description;
    interface interface-name {
      description text-description;
      no-listen;
      server [ addresses {
        logical-system logical-system-name;
        routing-instance instance-name;
      }
    ]
  }
}
tftp {
  description text-description;
  interface interface-name {
    description text-description;
    no-listen;
    server address;
    server logical-system name < [ routing-instance routing-instance-names ] >;
    server < [ routing-instance routing-instance-names ] >;
  }
}
```

To set domain packet forwarding, include the **domain** statement.

To set the description of the DNS or TFTP service, include the **description** statement.

To set TFTP packet forwarding, include the **tftp** statement.

To set a DNS or TFTP server (with an IPv4 address), include the **server** statement. Use one address for either a global configuration or for each interface.

To set the routing instance of the server to forward, include the **routing-instance** statement. You can include as many routing instances as necessary in the same statement.

To disable recognition of DNS or TFTP requests on one or more interfaces, include the **no-listen** statement. If you do not specify at least one interface with this statement, the forwarding service is global to all interfaces on the router or switch.

The following sections discuss the following:

- [Tracing BOOTP, DNS, and TFTP Forwarding Operations on page 95](#)
- [Example: Configuring DNS Packet Forwarding on page 97](#)

Tracing BOOTP, DNS, and TFTP Forwarding Operations

BOOTP, DNS, and TFTP forwarding tracing operations track all BOOTP, DNS, and TFTP operations and record them in a log file. The logged error descriptions provide detailed information to help you solve problems faster.

By default, nothing is traced. If you include the **traceoptions** statement at the **[edit forwarding-options helpers]** hierarchy level, the default tracing behavior is the following:

- Important events are logged in a file called **fud** located in the **/var/log** directory.
- When the file **fud** reaches 128 kilobytes (KB), it is renamed **fud.0**, then **fud.1**, and so on, until there are 3 trace files. Then the oldest trace file (**fud.2**) is overwritten. (For more information about how log files are created, see the [System Log Explorer](#).)
- Log files can be accessed only by the user who configures the tracing operation.

You cannot change the directory (**/var/log**) in which trace files are located. However, you can customize the other trace file settings by including the following statements at the **[edit forwarding-options helpers]** hierarchy level:

```
[edit forwarding-options helpers]
traceoptions {
  file filename <files number> <match regular-expression> <size size> <world-readable |
    no-world-readable>;
  flag {
    address;
    all;
    config;
    domain;
    ifdb;
    io;
    main;
    port;
    rtsock;
    tftp;
    trace;
    ui;
    util;
  }
  level severity-level;
  no-remote-trace;
}
```

These statements are described in the following sections:

- [Configuring the Log Filename on page 96](#)
- [Configuring the Number and Size of Log Files on page 96](#)

- [Configuring Access to the Log File on page 96](#)
- [Configuring a Regular Expression for Lines to Be Logged on page 96](#)

Configuring the Log Filename

By default, the name of the file that records trace output is **fud**. You can specify a different name by including the **file filename** statement at the **[edit forwarding-options helpers traceoptions]** hierarchy level:

```
[edit forwarding-options helpers traceoptions]
file filename;
```

Configuring the Number and Size of Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed **filename.0**, then **filename.1**, and so on, until there are three trace files. Then the oldest trace file (**filename.2**) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit forwarding-options helpers traceoptions]** hierarchy level:

```
[edit forwarding-options helpers traceoptions]
file files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (**filename**) reaches 2 MB, **filename** is renamed **filename.0**, and a new file called **filename** is created. When the new **filename** reaches 2 MB, **filename.0** is renamed **filename.1** and **filename** is renamed **filename.0**. This process repeats until there are 20 trace files. Then the oldest file (**filename.19**) is overwritten by the newest file (**filename.0**).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10 KB through 1 gigabyte (GB).

Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the **world-readable** option with the **file** statement at the **[edit forwarding-options helpers traceoptions]** hierarchy level:

```
[edit forwarding-options helpers traceoptions]
file world-readable;
```

To explicitly set the default behavior, include the **no-world-readable** option with the **file** statement at the **[edit forwarding-options helpers traceoptions]** hierarchy level:

```
[edit forwarding-options helpers traceoptions]
file no-world-readable;
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including the **match** option with the **file** statement at the **[edit forwarding-options helpers traceoptions]** hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit forwarding-options helpers traceoptions]
file filename match regular-expression;
```

Example: Configuring DNS Packet Forwarding

Enable DNS packet request forwarding to all interfaces on a router except **t1-1/1/2** and **t1-1/1/3**:

```
[edit forwarding-options helpers]
dns {
  server 10.10.10.30;
  interface {
    t1-1/1/2 {
      no-listen;
      server 10.10.10.9;
    }
    t1-1/1/3 {
      no-listen;
      server 10.10.10.4;
    }
  }
}
```

Preventing DHCP Spoofing on MX Series 3D Universal Edge Routers

A problem that sometimes occurs with DHCP is *DHCP spoofing*, in which an untrusted client floods a network with DHCP messages. Often these attacks utilize source IP address spoofing to conceal the true source of the attack.

DHCP snooping helps prevent DHCP spoofing by copying DHCP messages to the control plane and using the information in the packets to create anti-spoofing filters. The anti-spoofing filters bind a client's MAC address to its DHCP-assigned IP address and use this information to filter spoofed DHCP messages. In a typical topology, a carrier edge router (in this function also referred to as the broadband services router [BSR]) connects the DHCP server and the MX Series router (or broadband services aggregator [BSA]) performing the snooping. The MX Series router connects to the client and the BSR.

DHCP snooping works as follows in the network topology mentioned above:

1. The client sends a DHCP discover message to obtain an IP address from the DHCP server.
2. The BSA intercepts the message and might add option 82 information specifying the slot, port, VPI/VCI, and so on.
3. The BSA then sends the DHCP discover message to the BSR, which converts it to a unicast packet and sends it to the DHCP server.

4. The DHCP server looks up the client's MAC address and option 82 information in its database. A valid client is assigned an IP address, which is returned to the client using a DHCP offer message. Both the BSR and BSA send this message upstream to the client.
5. The client examines the DHCP offer, and if it is acceptable, issues a DHCP request message that is sent to the DHCP server through the BSA and BSR.
6. The DHCP server confirms that the IP address is still available. If it is, the DHCP server updates its local tables and sends a DHCP ACK message to the client.
7. The BSR receives the DHCP ACK message and passes the message to the BSA.
8. The BSA creates an anti-spoofing filter by binding the IP address in the ACK message to the MAC address of the client. After this point, any DHCP messages from this IP address that are not bound to the client's MAC address are dropped.
9. The BSA sends the ACK message to the client so that the process of assigning a IP address can be completed.

You configure DHCP snooping by including within a DHCP group the appropriate interfaces of the BSA:

```
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name
  forwarding-options dhcp-relay group group-name]
interface interface-name;
```

In a VPLS environment, DHCP requests are forwarded over pseudowires. You can configure DHCP snooping over VPLS at the **[edit routing-instances *routing-instance-name*]** hierarchy level.

DHCP snooping works on a per learning bridge basis in bridge domains. Each learning domain must have an upstream interface configured. This interface acts as the flood port for DHCP requests coming from the client side. DHCP requests are be forwarded across learning domains in a bridge domain. You can configure DHCP snooping on bridge domains at the **[edit routing-instances *routing-instance-name* bridge-domains *bridge-domain-name*]** hierarchy level.

Related Documentation

- *Preventing DHCP Spoofing*

CHAPTER 7

Configuration Statements

- [accounting on page 102](#)
- [aggregation on page 103](#)
- [autonomous-system-type on page 104](#)
- [bootp on page 105](#)
- [burn-hashing on page 106](#)
- [cflowd \(Discard Accounting\) on page 107](#)
- [cflowd \(Flow Monitoring\) on page 108](#)
- [client-address on page 108](#)
- [client-response-ttl on page 109](#)
- [description \(Forwarding Options\) on page 109](#)
- [dhcp-relay \(DHCP Spoofing Prevention\) on page 110](#)
- [disable \(Forwarding Options\) on page 111](#)
- [domain on page 112](#)
- [export-format on page 112](#)
- [enhanced-hash-key on page 113](#)
- [family \(Filtering\) on page 117](#)
- [family \(Monitoring\) on page 118](#)
- [family \(Port Mirroring\) on page 119](#)
- [family \(Sampling\) on page 121](#)
- [family inet on page 123](#)
- [family mpls on page 125](#)
- [family multiservice on page 128](#)
- [file \(Extended DHCP Relay Agent and Helpers Trace Options\) on page 130](#)
- [file \(Sampling\) on page 130](#)
- [file \(Trace Options\) on page 131](#)
- [filename \(Sampling\) on page 131](#)
- [files \(Sampling and Traceoptions\) on page 132](#)
- [filter \(IPv4, IPv6, and MPLS\) on page 132](#)

- [filter \(VPLS\) on page 133](#)
- [flood on page 133](#)
- [flow-active-timeout on page 134](#)
- [flow-export-destination on page 134](#)
- [flow-inactive-timeout on page 135](#)
- [flow-server on page 136](#)
- [group \(DHCP Spoofing Prevention\) on page 137](#)
- [gtp-tunnel-endpoint-identifier on page 138](#)
- [hash-key \(Forwarding Options\) on page 139](#)
- [helpers on page 142](#)
- [hosted-service-identifier on page 144](#)
- [hosted-services on page 144](#)
- [hyper-mode \(forwarding-options\) on page 145](#)
- [indexed-load-balance on page 146](#)
- [input \(Forwarding Table\) on page 147](#)
- [input \(Port Mirroring\) on page 147](#)
- [input \(Sampling\) on page 148](#)
- [instance on page 149](#)
- [interface \(Accounting or Sampling\) on page 150](#)
- [interface \(BOOTP\) on page 151](#)
- [interface \(DHCP Spoofing Prevention\) on page 152](#)
- [interface \(DNS and TFTP Packet Forwarding or Relay Agent\) on page 153](#)
- [interface \(Monitoring\) on page 154](#)
- [interface \(Next-Hop Group\) on page 155](#)
- [interface \(Port Mirroring\) on page 155](#)
- [link-layer-broadcast-inet-check on page 156](#)
- [load-balance \(Forwarding Options\) on page 157](#)
- [load-balance-group on page 159](#)
- [local-dump on page 159](#)
- [max-packets-per-second on page 160](#)
- [maximum-hop-count on page 160](#)
- [maximum-packet-length on page 161](#)
- [minimum-wait-time on page 162](#)
- [mirror-once on page 163](#)
- [monitoring on page 164](#)
- [next-hop \(Forwarding Options\) on page 165](#)
- [next-hop-group \(Forwarding Options\) on page 166](#)

- [next-hop-group](#) on page 167
- [no-filter-check](#) on page 168
- [no-listen](#) on page 168
- [output \(Accounting\)](#) on page 169
- [output \(Forwarding Table\)](#) on page 170
- [output \(Monitoring\)](#) on page 171
- [output \(Port Mirroring\)](#) on page 172
- [output \(Sampling\)](#) on page 173
- [per-flow](#) on page 174
- [per-prefix](#) on page 175
- [port \(cflowd\)](#) on page 175
- [port \(Packet Forwarding\)](#) on page 176
- [port-mirroring](#) on page 178
- [rate \(Forwarding Options\)](#) on page 180
- [relay-agent-option](#) on page 181
- [route-accounting](#) on page 181
- [run-length](#) on page 182
- [sampling \(Forwarding Options\)](#) on page 183
- [server \(DHCP and BOOTP Relay Agent\)](#) on page 186
- [server \(DNS and TFTP Service\)](#) on page 187
- [server-address \(Hosted Services\)](#) on page 187
- [server-profile](#) on page 188
- [server-profile \(Active Flow Monitoring\)](#) on page 188
- [size \(Sampling and Traceoptions\)](#) on page 189
- [source-checking](#) on page 190
- [stamp](#) on page 191
- [tftp](#) on page 191
- [traceoptions \(DNS and TFTP Packet Forwarding\)](#) on page 192
- [traceoptions \(Port Mirroring and Traffic Sampling\)](#) on page 194
- [version](#) on page 194
- [version9](#) on page 195
- [world-readable \(Forwarding Options\)](#) on page 196

accounting

Syntax	<pre> accounting <i>group-name</i> { output { aggregate-export-interval <i>seconds</i>; cflowd [<i>hostnames</i>] { aggregation { autonomous-system; destination-prefix; protocol-port; source-destination-prefix { caida-compliant; } source-prefix; } autonomous-system-type (origin peer); port <i>port-number</i>; version <i>format</i>; } flow-active-timeout <i>seconds</i>; flow-inactive-timeout <i>seconds</i>; interface <i>interface-name</i> { engine-id <i>number</i>; engine-type <i>number</i>; source-address <i>address</i>; } } } </pre>
Hierarchy Level	[edit forwarding-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Specify discard accounting instance name and options.</p> <p>The statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Discard Accounting on page 40

aggregation

Syntax	<pre> aggregation { autonomous-system; destination-prefix; protocol-port; source-destination-prefix { caida-compliant; } source-prefix; } </pre>
Hierarchy Level	[edit forwarding-options accounting output hostname], [edit forwarding-options sampling family (inet inet6 mpls) output flow-server hostname]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	For cflowd version 8 only, specify the type of data to be aggregated; cflowd records and sends only those flows that match the specified criteria.
Options	<p>autonomous-system—Aggregate by autonomous system (AS) number.</p> <p>caida-compliant—Record source and destination mask length values in compliance with the Version 2.1b1 release of the cflowd application from the Cooperative Association for Internet Data Analysis (CAIDA). If this statement is not configured, Junos OS records source and destination mask length values in compliance with the <i>cflowd Configuration Guide</i>, dated August 30, 1999.</p> <p>destination-prefix—Aggregate by destination prefix.</p> <p>protocol-port—Aggregate by protocol and port number.</p> <p>source-destination-prefix—Aggregate by source and destination prefix.</p> <p>source-prefix—Aggregate by source prefix.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Directing Traffic Sampling Output to a Server Running the cflowd Application on page 26

autonomous-system-type

Syntax	<code>autonomous-system-type (origin peer);</code>
Hierarchy Level	[edit forwarding-options accountingoutput cflowd hostname], [edit forwarding-options sampling family (inet inet6 mpls) output flow-server hostname]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the type of AS numbers that cflowd exports.
Default	<code>origin</code>
Options	origin —Export origin AS numbers of the packet source address in the Source Autonomous System cflowd field. peer —Export peer AS numbers through which the packet passed in the Source Autonomous System cflowd field.
Required Privilege Level	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Directing Traffic Sampling Output to a Server Running the cflowd Application on page 26

bootp

Syntax	<pre> bootp { client-response-ttl <i>number</i>; description <i>text-description</i>; interface (<i>interface-name</i> <i>interface-group</i>) { client-response-ttl <i>number</i>; description <i>text-description</i>; maximum-hop-count <i>number</i>; minimum-wait-time <i>seconds</i>; no-listen; server address { logical-system <i>logical-system-name</i> <routing-instance [<default> <i>routing-instance-names</i>]>; routing-instance [<default> <i>routing-instance-names</i>]; } } maximum-hop-count <i>number</i>; minimum-wait-time <i>seconds</i>; relay-agent-option; server address { <logical-system <i>logical-system-name</i>> <routing-instance [<i>routing-instance-names</i>]>; } } </pre>
Hierarchy Level	[edit forwarding-options helpers]
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 11.3 for QFX Series switches.</p>
Description	<p>Configures a router, switch, or interface to act as a Dynamic Host Configuration Protocol (DHCP) or bootstrap protocol (BOOTP) relay agent. For MX Series (MX80, MX240, MX480 and MX960) routers connected via IRB, see “Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents” on page 91 for information on how to prevent BOOTP reply packets from being dropped.</p> <p>DHCP relaying is disabled.</p>
Options	The remaining statements are explained separately.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents on page 91

bum-hashing

Syntax	bum-hashing;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls], [edit routing-instances <i>routing-instance-name</i> protocols vpls]
Release Information	Statement introduced in Junos OS Release 14.1.
Description	Load balance VPLS BUM (broadcast, unknown, and multicast) traffic across all members of an aggregate interface for the routing instance.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Load Balancing VPLS Non-Unicast Traffic Across Member Links of an Aggregate Interface on page 77• Example: Configuring Multicast Load Balancing over Aggregated Ethernet Links on page 78

cflowd (Discard Accounting)

Syntax	<pre> cflowd <i>hostname</i> { aggregation { autonomous-system; destination-prefix; protocol-port; source-destination-prefix { caida-compliant; } source-prefix; } autonomous-system-type (origin peer); port <i>port-number</i>; version <i>format</i>; } </pre>
Hierarchy Level	[edit forwarding-options accounting <i>group-name</i> output]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Collect an aggregate of sampled flows and send the aggregate to a specified host system that runs the collection utility cfdcollect.</p> <p>You can configure up to one version 5 and one version 8 flow format at the [edit forwarding-options accounting <i>group-name</i> output] hierarchy level.</p>
Options	<p>hostname—The IP address or identifier of the host system (the workstation running the cflowd utility).</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Directing Traffic Sampling Output to a Server Running the cflowd Application on page 26

cflowd (Flow Monitoring)

Syntax	<code>cflowd hostname { port port-number; }</code>
Hierarchy Level	[edit forwarding-options monitoring group-name family inet output]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Collect an aggregate of sampled flows and send the aggregate to a specified host system that runs the collection utility cfdcollect.</p> <p>You can configure up to eight version 5 flow formats at the [edit forwarding-options monitoring group-name output] hierarchy level. Version 8 flow formats are not supported for flow-monitoring applications.</p>
Options	<p>hostname—The IP address or identifier of the host system (the workstation running the cflowd utility).</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Passive Flow Monitoring on page 44

client-address

Syntax	<code>client-address ipv4-address;</code>
Hierarchy Level	[edit services hosted-services server-profile server-profile-name]
Release Information	Statement introduced in Junos OS Release 13.2.
Description	<p>Configure the source address to include in the header of each sampled packet. You must specify an IPv4 address. You can also specify the loopback address or the management interface address as the client address.</p>
Options	<p>ipv4-address—IPv4 address of the client.</p> <p>Default: 0.0.0.0</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Active Flow Monitoring on PTX Series Packet Transport Routers on page 42

client-response-ttl

Syntax	<code>client-response-ttl <i>number</i>;</code>
Hierarchy Level	[edit forwarding-options helpers bootp], [edit forwarding-options helpers bootp interface (<i>interface-name</i> <i>interface-group</i>)]
Release Information	Statement introduced in Junos OS Release 8.1. Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Description	Set the IP time-to-live (TTL) value in BOOTP response messages sent to a BOOTP client. If you do not include the client-response-ttl statement, the default is to leave the TTL field unchanged.
Options	<i>number</i> —IP time-to-live (TTL) value. Range: 1 through 255 Default: Leave the TTL field in the BOOTP response message unchanged.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents on page 91

description (Forwarding Options)

Syntax	<code>description <i>text-description</i>;</code>
Hierarchy Level	[edit forwarding-options helpers bootp], [edit forwarding-options helpers bootp interface (<i>interface-name</i> <i>interface-group</i>)], [edit forwarding-options helpers domain], [edit forwarding-options helpers domain interface <i>interface-name</i>], [edit forwarding-options helpers tftp], [edit forwarding-options helpers tftp interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Description	Describe a BOOTP, DHCP, Domain Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or an interface that is configured for the service.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring DNS and TFTP Packet Forwarding on page 94 • Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents on page 91

dhcp-relay (DHCP Spoofing Prevention)

Syntax	<pre>dhcp-relay { group <i>group-name</i> { interface <i>interface-name</i>; } }</pre>
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> forwarding-options], [edit routing-instances <i>routing-instance-name</i> forwarding-options]
Release Information	Statement introduced in Junos OS Release 9.4 (MX Series routers only).
Description	<p>Configure Dynamic Host Configuration Protocol (DHCP) snooping on the router. When acting as a snooping agent, the MX Series router typically is located between the client and the DHCP relay agent. It creates filters by “snooping” DHCP messages and binding DHCP-issued IP addresses to the MAC address of the client. These filters help prevent DHCP spoofing.</p> <p>Configure DHCP snooping by including the appropriate interfaces in the DHCP relay configuration.</p> <p>The statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Preventing DHCP Spoofing on MX Series 3D Universal Edge Routers on page 97

disable (Forwarding Options)

Syntax	disable;
Hierarchy Level	[edit forwarding-options port-mirror], [edit forwarding-options port-mirror instance <i>instance-name</i>], [edit forwarding-options sampling], [edit forwarding-options sampling instance <i>instance-name</i>], [edit forwarding-options sampling family (inet inet6 mpls)], [edit forwarding-options sampling family (inet inet6 mpls) output file]
Release Information	Statement introduced before Junos OS Release 7.4. Statement added to port-mirror hierarchy in Junos OS Release 9.6.



NOTE: Beginning in Junos OS 15.1F5 and later 15.1 releases, the **disable** option has been deprecated at the forwarding-options **sampling** instance *instance-name* family (inet | inet6 | mpls) hierarchy level on PTX3000 routers. When configured, the option does not take effect, so packets continue to be sampled. Instead of the **disable** option, use the **deactivate forwarding-options sampling instance *instance-name* family (inet | inet6 | mpls)** command to prevent sampling.

Description	Disable traffic accounting, port mirroring, or sampling.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Traffic Sampling</i> • <i>Configuring Port Mirroring</i>

domain

Syntax	<pre>domain { description text-description; interface interface-name { broadcast; description text-description; no-listen; server address <logical-system logical-system-name> <routing-instance routing-instance-name>; } server address <logical-system logical-system-name> <routing-instance routing-instance-name>; }</pre>
Hierarchy Level	[edit forwarding-options helpers]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Enable DNS request packet forwarding. The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring DNS and TFTP Packet Forwarding on page 94

export-format

Syntax	<pre>export-format cflowd-version-5;</pre>
Hierarchy Level	[edit forwarding-options monitoring group-name family inet output]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Flow monitoring export format.
Options	cflowd-version-5 —cflowd version 5.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration
Related Documentation	<ul style="list-style-type: none">• Configuring Passive Flow Monitoring on page 44

enhanced-hash-key

```

Syntax  enhanced-hash-key {
            family inet {
                gtp-tunnel-endpoint-identifier;
                incoming-interface-index;
                no-destination-port;
                no-source-port;
                type-of-service;
            }
            family inet6 {
                gtp-tunnel-endpoint-identifier;
                incoming-interface-index;
                no-destination-port;
                no-source-port;
                traffic-class;
            }
            family mpls {
                incoming-interface-index;
                label-1-exp;
                no-ether-pseudowire;
                no-payload;
            }
            family multiservice {
                incoming-interface-index;
                no-mac-address;
                no-payload;
                outer-priority;
            }
            services-loadbalancing {
                family inet {
                    layer-3-services {
                        destination-address;
                        incoming-interface-index;
                        source-address;
                    }
                }
                family inet6 {
                    layer-3-services {
                        destination-address;
                        incoming-interface-index;
                        source-address;
                        src-prefix-len;
                    }
                }
            }
            symmetric;
        }

```

Hierarchy Level [edit forwarding-options],
 [edit logical-systems logical-system-name routing-instances instance-name
 forwarding-options],
 [edit routing-instances instance-name forwarding-options]

Release Information	Statement introduced in Junos OS Release 10.1. services-loadbalancing option introduced in Junos OS Release 11.2. gtp-tunnel-endpoint-identifier option introduced in Junos OS Release 13.2
Description	<p>For MX Series routers with MPCs, T4000 routers with Type 5 FPCs, and EX9200 switches, select data used in the hash key for enhanced IP forwarding engines.</p> <p>By default, MPCs use the following parameters for hashing:</p> <ul style="list-style-type: none">• Source IP address• Destination IP address• Layer 3 protocol• Source port• Destination port• Generic routing encapsulation (GRE) for GRE packets only. <p>You can modify the default hashing mechanism on MPCs and Type 5 FPCs by configuring statements at the [edit forwarding-options enhanced-hash-key] hierarchy level.</p>
Default	Not enabled.

Options **services-loadbalancing**—Distributes traffic across PICs based on source IP address when a route pointing to more than one services PICs is installed.

symmetric—Enable symmetric load balancing across aggregated Ethernet interfaces.
This option is needed on Trio-based MPCs only.

Data selections for **services-loadbalancing**:

- **inet**—IPv4 addressing protocol.
- **inet6**—IPv6 addressing protocol.
- **layer-3-services**—Include layer 3 IP data in the hash key.
- **incoming-interface-index**—Include incoming interface index in the hash key.
- **source-address**—Include source-address in the hash key.
- **destination-address**—Include destination-address in the hash key.
- **src-prefix-len**—Include the source prefix length in the hash key.

Data selections for family **inet**:

- **gtp-tunnel-endpoint-identifer**—Include the tunnel endpoint identifier (TEID) field in the hash key for GPRS tunneling protocol (GTP) traffic.



NOTE: This option is supported only on MX Series routers with MPCs and on the MX80 router.

- **incoming-interface-index**—Include incoming interface index in the hash key.
- **no-destination-port**—Omit IP destination port in the hash key.
- **no-source-port**—Omit IP source port in the hash key.
- **type-of-service**—Include type-of-service (TOS) byte in the hash key.

Data selections for family **inet6**:

- **gtp-tunnel-endpoint-identifer**—Include the tunnel endpoint identifier (TEID) field in the hash key for GPRS tunneling protocol (GTP) traffic.



NOTE: This option is supported only on MX Series routers with MPCs and on the MX80 router.

- **incoming-interface-index**—Include the incoming interface index in the hash key.
- **no-destination-port**—Omit the IP destination port in the hash key.
- **no-source-port**—Omit the IP source port in the hash key.
- **traffic-class**—Include the traffic class byte in the hash key.

Data selections for family **mpls**:

- **incoming-interface-index**—Include the incoming interface index in the hash key.
- **label-1-exp**—The EXP bit of the first label is used in the hash calculation.
- **no-ether-pseudowire**—Omit the Ethernet pseudowire payload data from the hash key (MX Series routers with MPCs only).
- **no-payload**—Omit the MPLS payload data from the hash key.

Data selections for family **multiservice**:

- **incoming-interface-index**—Include the incoming interface index in the hash key.
- **no-mac-address**—Omit source and destination MAC addresses from the hash key.
- **no-payload**—Omit the payload data from the hash key.
- **outer-priority**—Include the outer 802.1 priority bits in the hash key.

Required Privilege Level	interface—To view this statement in the configuration.
	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>[edit forwarding-options] Hierarchy Level</i>

family (Filtering)

Syntax

```
family family-name {
    filter {
        input input-filter-name;
        output output-filter-name;
    }
    flood {
        input filter-name;
    }
    route-accounting;
    source-checking;
}
```

Hierarchy Level [edit forwarding-options]

Release Information Statement introduced before Junos OS Release 7.4.
route-accounting option introduced in Junos OS Release 8.3; supported only with IPv6.
source-checking option introduced in Junos OS Release 12.3 on MX Series Universal Edge Routers; supported only with IPv6.

Description Specify address family for filters.

Options *family-name*—Address family. Specify **inet** for IP version 4 (IPv4), **inet6** for IP version 6 (IPv6), **mpls** for MPLS, or **vpls** for virtual private LAN service (VPLS).



NOTE: In Junos OS Release 8.4 and later, the **output** statement is not valid at the [edit forwarding-options family vpls filter] hierarchy level.

The remaining statements are explained separately.

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

Related Documentation

- [Applying Forwarding Table Filters on page 60](#)

family (Monitoring)

Syntax

```
family inet {  
  output {  
    cflowd\hostname {  
      port port-number;  
    }  
    export-format cflowd-version-5;  
    flow-active-timeout seconds;  
    flow-export-destination {  
      (cflowd-collector | collector-pic);  
    }  
    flow-inactive-timeout seconds;  
    interface interface-name {  
      engine-id number;  
      engine-type number;  
      input-interface-index number;  
      output-interface-index number;  
      source-address address;  
    }  
  }  
}
```

Hierarchy Level [edit forwarding-options [monitoring](#) group-name]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure flow monitoring for an address family. Only the IPv4 protocol is supported.

The remaining statements are explained separately.

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

Related Documentation

- [Configuring Passive Flow Monitoring on page 44](#)

family (Port Mirroring)

Syntax	<pre> family (ccc inet inet6 vpls) { output { interface interface-name { next-hop address; } next-hop-group group-name { group-type inet6; interface interface-name { next-hop ipv6-address; } next-hop-subgroup group-name { interface interface-name { next-hop ipv6-address; } } } no-filter-check; server-profile server-profile-name; } } </pre>
Hierarchy Level	[edit forwarding-options port-mirroring], [edit forwarding-options port-mirroring instance instance-name]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>vpls and ccc options introduced in Junos OS Release 9.3 for MX Series routers only.</p> <p>vpls support extended to M7i, M10i, M120, and M320 routers in Junos OS Release 9.5.</p> <p>ccc option introduced in Junos OS Release 9.6 for M120 and M320 routers only.</p> <p>Statement introduced in Junos OS Release 12.1 for PTX Series Packet Transport Switches.</p> <p>ccc option introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>next-hop-group option for family inet6 introduced in Junos OS Release 14.2 for MX Series routers only.</p>
Description	Configure the address type family to sample for port mirroring.
Options	<p>ccc—Sample Layer 2 VPN traffic.</p> <p>inet—Sample IPv4 traffic.</p> <p>inet6—Sample IPv6 traffic.</p> <p>vpls—Sample VPLS traffic.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Port Mirroring on page 45

- [Configuring Active Flow Monitoring on PTX Series Packet Transport Routers on page 42](#)

family (Sampling)

```
Syntax  family (inet | inet6 | mpls) {
        disable;
        output {
            aggregate-export-interval seconds;
            extension-service service-name;
            file {
                disable;
                filename filename;
                files number;
                size bytes;
                (stamp | no-stamp);
                (world-readable | no-world-readable);
            }
            flow-active-timeout seconds;
            flow-inactive-timeout seconds;
            flow-server hostname {
                aggregation {
                    autonomous-system;
                    destination-prefix;
                    protocol-port;
                    source-destination-prefix {
                        caida-compliant;
                    }
                    source-prefix;
                }
                autonomous-system-type (origin | peer);
                (local-dump | no-local-dump);
                port port-number;
                source-address address;
                version format;
                version9 {
                    template template-name;
                }
            }
            interface interface-name {
                engine-id number;
                engine-type number;
                source-address address;
            }
        }
    }
```

Hierarchy Level [edit forwarding-options [sampling](#)]

Release Information Statement introduced before Junos OS Release 7.4.
mpls option introduced in Junos OS Release 8.3.

Description Configure the protocol family to be sampled.

Options **inet**—IP version 4 (IPv4)
inet6—IP version 6 (IPv6)

mpls—MPLS

The remaining statements are explained separately.

Required Privilege Level	interface—To view this statement in the configuration.
	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Traffic Sampling on page 22

family inet

Syntax	<pre>family inet { layer-3; layer-4; session-id; symmetric-hash { complement; } }</pre>
Hierarchy Level	[edit forwarding-options hash-key]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure layer information for the load-balancing specification. Only the IPv4 protocol is supported.
Options	<p>family inet—Incorporate port data into the hash key for flow determination. By default, port data is ignored when determining flows.</p> <ul style="list-style-type: none"> • layer-3—Incorporate Layer 3 (IP) data into the hash key. You must include the layer-3 statement. If you omit the layer-3 statement, the management process removes the hash-key statement from the configuration and the router behaves as if you specified layer-3. <p>By default, or if you specify only the layer-3 statement, the router uses the following Layer 3 information in the packet header for per-flow load balancing:</p> <ul style="list-style-type: none"> • Source IP address • Destination IP address • Protocol • Incoming interface index <ul style="list-style-type: none"> • layer-4—Incorporate Layer 4 Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) data into the hash key. <p>If you include the layer-4 statement, the router uses the following Layer 4 information to load-balance:</p> <ul style="list-style-type: none"> • Source port number • Destination port number • IP type of service <ul style="list-style-type: none"> • session-id—Include the session ID in the hash key. • symmetric-hash—Create the symmetric hash key with source and destination ports. <ul style="list-style-type: none"> • complement—Create the complement of the symmetric hash key.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Per-Packet Load Balancing on page 66

family mpls

```
Syntax  family mpls {
        all-labels;
        label-1;
        label-2;
        label-3;
        no-labels;
        no-label-1-exp;
        payload {
            ether-pseudowire;
            ip {
                disable;
                layer-3-only;
                port-data {
                    source-msb;
                    source-lsb;
                    destination-msb;
                    destination-lsb;
                }
            }
        }
    }
```

Hierarchy Level [edit forwarding-options [hash-key](#)]

Release Information Statement introduced before Junos OS Release 7.4.
no-label-1-exp option introduced in Junos OS Release 8.0.
label-3 and **no-labels** options introduced in Junos OS Release 8.1.
ether-pseudowire option introduced in Junos OS Release 9.1 (M320 and T Series routers only); support extended to M120 and MX Series routers in Junos OS Release 9.4.
all-labels and **payload ip disable** options introduced in Junos OS Release 12.1X48R2. (PTX Series Packet Transport Routers only).

Description For aggregated Ethernet and SONET/SDH interfaces only, configure load balancing based on MPLS labels and payload. Only the IPv4 protocol is supported.

Options **family mpls**—(Aggregated Ethernet interfaces, aggregated SONET/SDH interfaces, and multiple equal-cost MPLS next hops only) Incorporate MPLS label and payload information into the hash key for per-flow load balancing. Only the IPv4 protocol is supported.

- **all-labels**—(PTX Series Packet Transport Routers only) Up to eight MPLS labels are included in the hash key to identify the uniqueness of a flow in the Packet Forwarding Engine. This is the default setting.
- **label-1**—(M120, M320, MX Series, and T Series routers only) Include the first MPLS label into the hash key. This is used for a one-label packet for per-flow load balancing IPv4 VPLS traffic based on IP information and MPLS labels.
- **label-2**—(M120, M320, MX Series, and T Series routers only) Include the second MPLS label into the hash key. This is used for a two-label packet for per-flow load balancing

IPv4 VPLS traffic based on IP information and MPLS labels. To use the second MPLS label in the hash key, include both the **label-1** and **label-2** statements at the **[edit forwarding-options hash-key family mpls]** hierarchy level. By default, the router provides hashing on the first and second labels. If both labels are specified, the entire first label and the first 16 bits of the second label are hashed.

- **label-3**—(M120, M320, MX Series, and T Series routers only) Include the third MPLS label into the hash key. To use the third MPLS label, include the **label-1**, **label-2**, and **label-3** statements at the **[edit forwarding-options hash-key family mpls]** hierarchy level.
- **no-labels**—Include no MPLS labels into the hash key.
- **no-label-1-exp**—(M120, M320, MX Series, and T Series routers only) The EXP bit of the first label is not used in the hash calculation to avoid reordering complications.
- **payload**—Incorporate bits from the IP payload into the hash key for per-flow load balancing Layer 2 information based on MPLS labels.
 - **disable**—(PTX Series Packet Transport Routers only) Exclude IP payload from the hash key.
 - **ether-pseudowire**—(M120, M320, MX Series, and T Series routers only) Load-balance IPv4 traffic over Layer 2 Ethernet pseudowires.
 - **ip**—Include the IP address of the IPv4 or IPv6 payload into the hash key for per-flow load balancing Layer 2 information based on MPLS labels. For the PTX Series Packet Transport Routers, this is the default setting with both Layer 3 and Layer 4 IP information included in the hash key.
 - **disable**—(PTX Series Packet Transport Routers only) Exclude IP payload from the hash key.
 - **layer-3-only**—Include only Layer 3 IP information from the IP payload data into the hash key for per-flow load balancing Layer 2 information based on MPLS labels.
 - **port-data**—(M120, M320, MX Series, and T Series routers only) Include the source and destination port field information into the hash key. By default, the most significant byte and least significant byte of the source and destination port fields are hashed. To select specific bytes to be hashed, include one or more of the **source-msb**, **source-lsb**, **destination-msb**, and **destination-lsb** options at the **[edit forwarding-options hash-key family mpls payload ip port-data]** hierarchy level. To prevent all four bytes from being hashed, include the **layer-3-only** statement at the **[edit forwarding-options hash-key family mpls payload ip]** hierarchy level.
 - **destination-lsb**—Include the least-significant byte of the destination port.
 - **destination-msb**—Include the most-significant byte of the destination port.
 - **source-lsb**—Include the least-significant byte of the source port.
 - **source-msb**—Include the most-significant byte of the source port.

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

- Related Documentation**
- *Configuring Load Balancing Based on MPLS Labels*
 - [Configuring Load Balancing for Ethernet Pseudowires on page 63](#)

family multiservice

Syntax

```
family multiservice {
    destination-mac;
    label-1;
    label-2;
    payload {
        ip {
            layer-3 {
                (source-ip-only | destination-ip-only);
            }
            layer-3-only;
            layer-4;
        }
    }
    source-mac;
    symmetric-hash {
        complement;
    }
}
```

Hierarchy Level [edit forwarding-options [hash-key](#)]

Release Information Statement introduced in Junos OS Release 8.0.
ip, **label-1**, **label-2**, **layer-3-only**, and **payload** options introduced in Junos OS Release 9.4.
layer-3, **layer-4**, **source-ip-only**, and **destination-ip-only** options introduced in Junos OS Release 9.5.
symmetric-hash and **complement** options introduced in Junos OS Release 9.6.

Description Configure load balancing based on Layer 2 media access control information. On MX Series routers, configure VPLS load balancing. On M120 and M320 routers only, configure VPLS load balancing based on MPLS labels and IP information. For IPv4 traffic, only the IP source and destination addresses are included in the hash key. For MPLS and IPv4 traffic, one or two MPLS labels and IPv4 source and destination addresses are included. For MPLS Ethernet pseudowires, only one or two MPLS labels are included in the hash key.

Options You can configure one or more options to load-balance using the packet information that you specify.

destination-mac—Include the destination-address MAC information in the hash key for Layer 2 load balancing.

label-1 (M120 and M320 routers only)—Include the first MPLS label in the hash key. Used for including a one-label packet for per-flow load balancing of IPv4 VPLS traffic based on IP information and MPLS labels.

label-2 (M120 and M320 routers only)—Include the second MPLS label in the hash key. If both **label-1** and **label-2** are specified, the entire first label and the first 16 bits of the second label are hashed.

payload (MX Series, M120, and M320 routers only)—Include the packet's IP payload in the hash key.

- **ip** (MX Series, M120, and M320 routers only)—Include the IP address of the IPv4 or IPv6 payload in the hash key.
- **layer-3** (MX Series routers only)—Use this to include Layer 3 information from the packet's IP payload in the hash key.
 - **destination-ip-only** (MX Series routers only)—Use this to include only the destination IP address in the payload in the hash key.
 - **source-ip-only** (MX Series routers only)—Use this to include only the source IP address in the payload in the hash key.



NOTE: You can include either the **source-ip-only** or the **destination-ip-only** statement, not both. They are mutually exclusive.

- **layer-3-only** (M120, and M320 routers only)—Include only the Layer 3 information from the packet's IP payload in the hash key.
- **layer-4** (MX Series routers only)—Include Layer 4 information from the packet's IP payload in the hash key.



NOTE: On MX Series routers only, you can configure either Layer 3 or Layer 4 load balancing, or both at the same time.



NOTE: On I chip platforms, an unknown Layer 4 header is excluded from load-balance hashing to avoid undesired packet reordering.

source-mac—Include the source-address MAC information in the hash key.

symmetric-hash (MX Series routers only)—Configure the symmetric hash or symmetric hash complement for configuring symmetrical load balancing on an 802.3ad Link Aggregation Group.

- **complement** —Include the complement of the symmetric hash in the hash key.

**Required Privilege
Level**

interface—To view this statement in the configuration.

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

- Related Documentation**
- [Configuring Load Balancing Based on MAC Addresses on page 76](#)
 - [Configuring VPLS Load Balancing Based on IP and MPLS Information](#)
 - [Configuring VPLS Load Balancing on MX Series 3D Universal Edge Routers](#)
 - [Configuring VPLS Load Balancing](#)

file (Extended DHCP Relay Agent and Helpers Trace Options)

Syntax	file <i>filename</i> <files <i>number</i> > <match <i>regular-expression</i> > <size <i>bytes</i> > <world-readable no-world-readable>;
Hierarchy Level	[edit forwarding-options dhcp-relay traceoptions], [edit forwarding-options helpers traceoptions]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure information about the DNS and TFTP packet-forwarding files that contain trace logging information.
Options	<i>filename</i> —Name of the file containing the trace information. Default: /var/log/sampled The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	• Tracing BOOTP, DNS, and TFTP Forwarding Operations on page 95

file (Sampling)

Syntax	file <i>filename filename</i> <disable> <files <i>number</i> > <stamp no-stamp> <size <i>bytes</i> > <world-readable no-world-readable>;
Hierarchy Level	[edit forwarding-options sampling family <i>family-name</i> output]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Collect the traffic samples in a file. The statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	• Collecting Traffic Sampling Output in a File on page 24

file (Trace Options)

Syntax	file <i>filename</i> < files number > < size bytes > < world-readable no- world-readable >;
Hierarchy Level	[edit forwarding-options port-mirroring traceoptions], [edit forwarding-options sampling traceoptions]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure information about the files that contain trace logging information.
Options	<i>filename</i> —The name of the file containing the trace information. Default: /var/log/sampled The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Tracing Traffic-Sampling Operations on page 33

filename (Sampling)

Syntax	filename <i>filename</i> ;
Hierarchy Level	[edit forwarding-options sampling family family-name output file]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the name of the output file.
Options	<i>filename</i> —Name of the file in which to place the traffic samples. All files are placed in the directory /var/tmp.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Collecting Traffic Sampling Output in a File on page 24

files (Sampling and Traceoptions)

Syntax	<code>files <i>number</i>;</code>
Hierarchy Level	[edit forwarding-options helpertraceoptions file], [edit forwarding-options port-mirroring traceoptions file], [edit forwarding-options sampling family <i>family-name</i> output file], [edit forwarding-options sampling traceoptions file]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
Description	Configure the total number of files to be saved with samples or trace data.
Options	<i>number</i> —Maximum number of traffic sampling or trace log files. When a file named <i>sampling-file</i> reaches its maximum size, it is renamed <i>sampling-file.0</i> , then <i>sampling-file.1</i> , and so on, until the maximum number of traffic sampling files is reached. Then the oldest sampling file is overwritten. Range: 1 through 100 files Default: 5 files for sampling output; 10 files for trace log information
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Collecting Traffic Sampling Output in a File on page 24• Tracing Traffic-Sampling Operations on page 33

filter (IPv4, IPv6, and MPLS)

Syntax	<pre>filter { input <i>input-filter-name</i>; output <i>output-filter-name</i>; }</pre>
Hierarchy Level	[edit forwarding-options family (inet inet6 mpls)]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Apply a forwarding table filter to a forwarding table.
Options	The statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Applying Forwarding Table Filters on page 60

filter (VPLS)

Syntax	filter input <i>filter-name</i> ;
Hierarchy Level	[edit forwarding-options family vpls], [edit logical-systems <i>logical-system-name</i> forwarding-options family vpls], [edit logical-systems <i>logical-system-name</i> routing -instances <i>instance-name</i> forwarding-options family vpls], [edit routing -instances <i>instance-name</i> forwarding-options family vpls]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Apply a forwarding table filter for VPLS.
Options	The other statement is explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Applying Forwarding Table Filters on page 60

flood

Syntax	flood { input <i>filter-name</i> ; }
Hierarchy Level	[edit forwarding-options family vpls], [edit routing -instances <i>instance-name</i> forwarding-options family vpls]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Apply a forwarding table filter to a flood table.
Options	input <i>filter-name</i> —Name of the forwarding table filter.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Applying Forwarding Table Filters on page 60

flow-active-timeout

Syntax	<code>flow-active-timeout seconds;</code>
Hierarchy Level	[edit forwarding-options accounting group-name output], [edit forwarding-options monitoring group-name family inet output], [edit forwarding-options sampling family family-name output]
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 time that elapses before another active flow is exported.
Options	seconds —Timeout, in seconds. Range: 60 through 1800 Default: 1800
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Discard Accounting on page 40• Configuring Passive Flow Monitoring on page 44• Collecting Traffic Sampling Output in a File on page 24

flow-export-destination

Syntax	<code>flow-export-destination { (cflowd-collector collector-pic); }</code>
Hierarchy Level	[edit forwarding-options monitoring group-name family inet output]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure flow collection.
Options	cflowd-collector —cflowd collector. collector-pic —Collector PIC.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Passive Flow Monitoring on page 44

flow-inactive-timeout

Syntax	<code>flow-inactive-timeout <i>seconds</i>;</code>
Hierarchy Level	[edit forwarding-options accounting <i>group-name</i> output], [edit forwarding-options monitoring <i>group-name</i> family inet output], [edit forwarding-options sampling <i>family</i> <i>family-name</i> output]
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 time that elapses before a flow is considered inactive.
Options	<i>seconds</i> —Timeout, in seconds. Range: 15 through 1800 Default: 60
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Discard Accounting on page 40• Configuring Passive Flow Monitoring on page 44• Collecting Traffic Sampling Output in a File on page 24

flow-server

Syntax	<pre> flow-server <i>hostname</i> { aggregation { autonomous-system; destination-prefix; protocol-port; routing-instance <i>instance-name</i>; source-destination-prefix { caida-compliant; } source-prefix; } autonomous-system-type (origin peer); (local-dump no-local-dump); port <i>port-number</i>; source-address <i>address</i>; version <i>format</i>; version9 { template <i>template-name</i>; } } </pre>
Hierarchy Level	<p>[edit forwarding-options sampling family {<i>inet</i> <i>inet6</i> <i>mpls</i> <i>vpls</i>} output]</p> <p>[edit routing-instance <i>instance-name</i> forwarding-options sampling family {<i>inet</i> <i>inet6</i> <i>mpls</i> <i>vpls</i>} output]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>version9 statement introduced in Junos OS Release 8.3.</p>
Description	<p>Collect an aggregate of sampled flows and send the aggregate to a specified host system or flow server that runs the collection utility. Specify a host system or flow server to collect sampled flows using the version 9 format.</p> <p>You can configure up to one version 5 and one version 8 flow format at the [edit forwarding-options sampling output flow-server <i>hostname</i>] hierarchy level. For the same configuration, you can specify only either version 9 flow record formats or formats using versions 5 and 8, not both types of formats.</p>



NOTE: Starting with Junos OS Release 13.3, you can configure flow collectors to be reachable through non default VPN routing and forwarding (VRF) instances by including the `routing-instance instance-name` statement at the **[edit forwarding-options sampling instance *instance-name* family {*inet* | *inet6* | *mpls* | *vpls*} output]** hierarchy level for inline flow monitoring. You cannot configure a flow collector to be reachable through non default VRF instances for version 5 and version 8 flows. You must configure the routing instance to be a VRF instance by including the `instance-type vrf` statement at the **[edit routing-instances *instance-name*]** hierarchy level.

Options *hostname*—The IP address or identifier of the host system (the workstation either running the cflowd utility or collecting traffic flows using version 9).

You can configure only one host system for version 9.

The remaining statements are explained separately.

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

Related Documentation

- [Collecting Traffic Sampling Output in the Cisco Systems NetFlow Services Export Version 9 Format on page 29](#)
- [Directing Traffic Sampling Output to a Server Running the cflowd Application on page 26](#)

group (DHCP Spoofing Prevention)

Syntax `group group-name {
 interface interface-name;
}`

Hierarchy Level [edit routing-instances *routing-instance-name* bridge-domains *bridge-domain-name* forwarding-options [dhcp-relay](#)],
[edit routing-instances *routing-instance-name* forwarding-options [dhcp-relay](#)]

Release Information Statement introduced in Junos OS Release 9.4 (MX Series routers only).

Description Configure Dynamic Host Configuration Protocol (DHCP) snooping on the router. When acting as a snooping agent, the MX Series router typically is located between the client and the DHCP relay agent. It creates filters by “snooping” DHCP messages and binding DHCP-issued IP addresses with the MAC address of the client. These filters help prevent DHCP spoofing.

Configure DHCP snooping by including the appropriate interfaces under the **group** statement.

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

Related Documentation

- [Preventing DHCP Spoofing on MX Series 3D Universal Edge Routers on page 97](#)

gtp-tunnel-endpoint-identifier

Syntax	<code>gtp-tunnel-endpoint-identifier</code>
Hierarchy Level	[edit forwarding-options hash-key family inet layer-4], [edit forwarding-options hash-key family inet6 layer-4]
Release Information	Statement introduced in Junos OS Release 15.1F3 for PTX Series Routers with third generation FPCs.
Description	When you configure gtp-tunnel-endpoint-identifier , the hash calculation of IPv4 or IPv6 packets are included in the GPRS tunneling protocol–tunnel endpoint ID (GTP-TEID) field hash calculations.



NOTE: The **gtp-tunnel-endpoint-identifier** configuration statement is supported on PTX Series routers only when network services is set to **enhanced-mode**. For more information, see **enhanced-mode**.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• hash-key on page 139• Understanding Per-Packet Load Balancing on page 65• Configuring Per-Packet Load Balancing on page 66

hash-key (Forwarding Options)

```

Syntax  hash-key {
        family inet {
            layer-3;
            layer-4;
            session-id;
            symmetric-hash {
                complement;
            }
        }
        family mpls {
            all-labels;
            bottom-label-1;
            bottom-label-2;
            bottom-label-3;
            label-1;
            label-2;
            label-3;
            no-labels;
            no-label-1-exp;
            payload {
                ether-pseudowire;
                ip {
                    disable;
                    layer-3-only;
                    port-data {
                        destination-lsb;
                        destination-msb;
                        source-lsb;
                        source-msb;
                    }
                }
            }
        }
    }
    family multiservice {
        destination-mac;
        label-1;
        label-2;
        payload {
            ip {
                layer-3-only;
                layer-3 {
                    (source-ip-only | destination-ip-only);
                }
                layer-4;
            }
        }
        source-mac;
    }
}

```

Hierarchy Level [edit forwarding-options]

Release Information Statement introduced before Junos OS Release 7.4.
family multiservice and **no-label-1-exp** options introduced in Junos OS Release 8.0.
label-3 and **no-labels** options introduced in Junos OS Release 8.1.
ether-pseudowire statement introduced in Junos OS Release 9.1 (M320 and T Series routers only); support extended to M120 and MX Series routers in Junos OS Release 9.4.
ip, **label-1**, **label-2**, **layer-3-only**, and **payload** options for the **family multiservice** statement introduced in Junos OS Release 9.4 (M120 and M320 routers only). For MX Series routers, only the **ip** and **payload** statements apply.
layer-3, **source-ip-only**, **destination-ip-only**, and **layer-4** statements introduced for the **family multiservice** statement in Junos OS Release 9.5. (MX Series routers only).
all-labels and **payload ip disable** statements introduced for the **family mpls** statement in Junos OS Release 12.1X48R2. (PTX Series Packet Transport Routers only).
bottom-label statements introduced for the **family mpls** statement in Junos OS Release 14.1 for MX Series routers with DPCs (excluding M7i, M10i, and M120).

Description Select which packet header data to use for per-flow load balancing.

The options are explained separately.



NOTE: To modify the default hashing mechanism on Modular Port Concentrators (MPCs) and Type 5 FPCs, you need to configure the statements at the [edit forwarding-options **enhanced-hash-key**] hierarchy level. Statements at the [edit forwarding-options hash-key] hierarchy level do not support MPCs and Type 5 FPCs.



NOTE:

The following statements are not supported on T Series routers:

- The **symmetric-hash** and the **session-id** statements at the [edit forwarding-options hash-key family inet] hierarchy level and all statements at the [edit forwarding-options hash-key family multiservice] hierarchy level.
- The **label-1** and **label-2** statements, and the IP configuration at the [edit forwarding-options hash-key family multiservice] hierarchy level.



NOTE: The following statements are not supported on Q Series switches:

- The **symmetric-hash** and the **session-id** statements at the [edit forwarding-options hash-key family inet] hierarchy level.

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

- Related Documentation**
- [Configuring Per-Packet Load Balancing on page 66](#)
 - *Configuring Load Balancing Based on MPLS Labels*
 - [Configuring Load Balancing Based on MAC Addresses on page 76](#)

helpers

```
Syntax  helpers {
        bootp {
            client-response-ttl number;
            description text-description;
            interface interface-group {
                client-response-ttl number;
                description text-description;
                maximum-hop-count number;
                minimum-wait-time seconds;
                no-listen;
                server address {
                    logical-system logical-system-name <routing-instance [ <default>
                        routing-instance-names ]>;
                    routing-instance [ <default> routing-instance-names ];
                }
            }
            maximum-hop-count number;
            minimum-wait-time seconds;
            relay-agent-option;
            server address {
                logical-system logical-system-name <routing-instance [ <default>
                    routing-instance-names ]>;
                routing-instance [ <default> routing-instance-names ];
            }
        }
        domain {
            description text-description;
            interface interface-name {
                broadcast;
                description text-description;
                no-listen;
                server address <logical-system logical-system-name> <routing-instance
                    routing-instance-name>;
            }
            server address <logical-system logical-system-name> <routing-instance
                routing-instance-name>;
        }
        port (Packet Forwarding) port-number {
            description text-description;
            interface interface-name {
                broadcast;
                description text-description;
                no-listen;
                server address <logical-system logical-system-name> <routing-instance
                    routing-instance-name>;
            }
            server address <logical-system logical-system-name> <routing-instance
                routing-instance-name>;
        }
        tftp {
            description text-description;
            interface interface-name {
```

```

broadcast;
description text-description;
no-listen;
server address <logical-system logical-system-name> <routing-instance
routing-instance-name>;
}
server address <logical-system logical-system-name> <routing-instance
routing-instance-name>;
}
traceoptions {
file filename <files number> <match regular-expression> <size bytes> <world-readable |
no-world-readable>;
flag flag;
level level;
no-remote-trace level;
}
}

```

Hierarchy Level [edit forwarding-options]

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

Description Enable TFTP or DNS request packet forwarding, or configure the router, switch, or interface to act as a DHCP/BOOTP relay agent. Use only one server address per interface or global configuration.

In addition to TFTP and DNS, you can use the helpers statement to enable LAN-Broadcast forwarding. To do this, you must manually define which UDP port is forwarded, as shown here:

```

user@ host# show forwarding-options
helpers {
  port 3000 {
    interface {
      fe-0/0/1.0 {
        server 111.0.0.2;
      }
    }
  }
  port 3001 {
    interface {
      fe-0/0/0.0 {
        server 100.0.0.2;
      }
    }
  }
}

```

The remaining statements are explained separately.

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

- Related Documentation**
- [Configuring DNS and TFTP Packet Forwarding on page 94](#)
 - [Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents on page 91](#)


hosted-service-identifier

Syntax	hosted-service-identifier <i>identifier</i> ;
Hierarchy Level	[edit services hosted-services server-profile <i>server-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2.
Description	Configure the identifier for the service performed on the remote server
Options	<i>identifier</i> —Identifier for the service performed on the remote server. Range: 1 through 63
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	• Configuring Active Flow Monitoring on PTX Series Packet Transport Routers on page 42



hosted-services

Syntax	hosted-services { server-profile <i>server-profile-name</i> { client-address <i>ipv4-address</i> ; server-address <i>ipv4-address</i> ; } }
Hierarchy Level	[edit services]
Release Information	Statement introduced in Junos OS Release 13.2.
Description	Configure services performed on the remote server.
Options	The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	• Configuring Active Flow Monitoring on PTX Series Packet Transport Routers on page 42

hyper-mode (forwarding-options)

Syntax	hyper-mode
Hierarchy Level	[edit forwarding-options]
Release Information	Statement introduced in Junos OS Release 13.3R4 for MX Series routers.
Description	Configure the hyper mode feature to increase the rate at which a data packet is processed. This configuration results in the optimization of the lifetime of a data packet, which further enables the router to provide better performance and throughput. This feature is supported on enhanced MPCs such as MPC3E, MPC4E, MPC5E, and MPC6E.
<div>  <p>NOTE: The hyper mode feature is configured at the global level and requires a system reboot. You can enable the feature only if the network-service mode on the router is configured as either enhanced-ip or enhanced-ethernet.</p> </div>	
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Hyper Mode on Enhanced MPCs to Speed Up Packet Processing</i> • <i>Understanding the Hyper Mode Feature on Enhanced MPCs for MX Series Routers</i> • show forwarding-options hyper-mode on page 205

indexed-load-balance

Syntax	indexed-load-balance;
Hierarchy Level	[edit forwarding-options load-balance], [edit logical-systems <i>logical-system-name</i> forwarding-options load-balance], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options load-balance], [edit routing-instances <i>routing-instance-name</i> forwarding-options load-balance]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<div>  <p>NOTE: Starting with Junos OS Release 12.1, the indexed-next-hop statement has been renamed as the indexed-load-balance statement.</p> </div> <p>Improve load-balance distribution for unicast and aggregated next hops. Include this statement if you notice issues with load-balance distribution for IPv4 traffic. The indexed-load-balance statement causes the creation of a nexthop structure that is not a function of the hash only, but is also a function of the low-order bits of the IP address.</p> <div>  <p>CAUTION: Including the indexed-load-balance statement causes an increase in memory usage on the device.</p> </div>
Default	Disabled
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring Per-Prefix Load Balancing on page 69

input (Forwarding Table)

Syntax	<code>input <i>filter-name</i>;</code>
Hierarchy Level	[edit forwarding-options family (inet inet6 mpls vpls) filter], [edit routing-instances <i>routing-instance-name</i> forwarding-options family (inet inet6 mpls vpls) filter]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 15.1X53-D10 for QFX10000 switches..
Description	Apply a forwarding table filter to ingress traffic of the forwarding table.
Options	<i>filter-name</i> —Name of the applied filter.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Applying Forwarding Table Filters on page 60

input (Port Mirroring)

Syntax	<pre>input { maximum-packet-length <i>bytes</i>; rate <i>number</i>; run-length <i>number</i>; }</pre>
Hierarchy Level	[edit forwarding-options port-mirroring], [edit forwarding-options port-mirroring instance <i>instance-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. maximum-packet-length option introduced in Junos OS Release 9.6 for M120 and M320 routers only. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
Description	Configure input packet properties for port mirroring. The statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Port Mirroring on page 45

input (Sampling)

Syntax	<pre>input { max-packets-per-second <i>number</i>; maximum-packet-length <i>bytes</i>; rate <i>number</i>; run-length <i>number</i>; }</pre>
Hierarchy Level	[edit forwarding-options sampling]
Release Information	Statement introduced before Junos OS Release 7.4. Support for sampling of MPLS traffic introduced in Junos OS Release 8.3.
Description	Configure traffic sampling on a logical interface. The statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Obsolete Configuring Traffic Sampling</i>

instance

Syntax	<pre> instance { instance-name { input { maximum-packet-length bytes; rate number; run-length number; } family (ccc inet inet6 mpls vpls) { output { interface interface-name { next-hop address; } no-filter-check; server-profile server-profile-name; } } } } </pre>
Hierarchy Level	<p>[edit forwarding-options port-mirroring],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options port-mirroring]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3 (MX Series routers only). Support extended to M120 and M320 routers in Junos OS Release 9.5.</p> <p>maximum-packet-length and ccc options introduced in Junos OS Release 9.6 for M120 and M320 routers only.</p> <p>server-profile option introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers only.</p>
Description	Configure a port-mirroring instance.
Options	<p><i>port-mirroring-instance-name</i>—Name of the port-mirroring instance.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control-level—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Port Mirroring on page 45 • Configuring Active Flow Monitoring on PTX Series Packet Transport Routers on page 42

interface (Accounting or Sampling)

Syntax	<pre>interface <i>interface-name</i> { engine-id <i>number</i>; engine-type <i>number</i>; source-address <i>address</i>; }</pre>
Hierarchy Level	[edit forwarding-options accounting group-name output], [edit forwarding-options sampling family family-name output]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the output interface for sending copies of packets elsewhere to be analyzed.
Options	<p>engine-id <i>number</i>—Identity of the accounting interface.</p> <p>engine-type <i>number</i>—Type of this accounting interface.</p> <p><i>interface-name</i>—Name of the accounting interface.</p> <p>source-address <i>address</i>—Address used for generating packets.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Discard Accounting on page 40• Collecting Traffic Sampling Output in a File on page 24

interface (BOOTP)

Syntax	<pre> interface (<i>interface-name</i> <i>interface-group</i>) { apply-secondary-as-giaddr; broadcast; client-response-ttl <i>number</i>; description <i>text-description</i>; maximum-hop-count <i>number</i>; minimum-wait-time <i>seconds</i>; no-listen; server <i>address</i> { logical-system <i>logical-system-name</i> <routing-instance [<default> <i>routing-instance-names</i>]>; routing-instance [<default> <i>routing-instance-names</i>]; } } </pre>
Hierarchy Level	[edit forwarding-options helpers bootp]
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 11.3 for QFX Series switches.</p>
Description	Specify the interface for a DHCP and BOOTP relay agent.
Options	<p><i>interface-group</i>—Set a logical interface or group of logical interfaces with a specific DHCP relay configuration.</p> <p><i>apply-secondary-as-giaddr</i>—Enable DHCP relay to use secondary gateway IP on this interface.</p> <p><i>broadcast</i>—If the layer 2 interface is unknown, then broadcast.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents on page 91

interface (DHCP Spoofing Prevention)

Syntax	<code>interface <i>interface-name</i>;</code>
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-relay group group-name], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group group-name]
Release Information	Statement introduced in Junos OS Release 9.4 (MX Series routers only).
Description	<p>Configure Dynamic Host Configuration Protocol (DHCP) snooping on the router. When acting as a snooping agent, the MX Series router typically is located between the client and the DHCP relay agent. It creates filters by “snooping” DHCP messages and binding DHCP-issued IP addresses with the MAC address of the client. These filters help prevent DHCP spoofing.</p> <p>DHCP snooping is configured by including the appropriate interfaces.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Preventing DHCP Spoofing on MX Series 3D Universal Edge Routers on page 97

interface (DNS and TFTP Packet Forwarding or Relay Agent)

Syntax	<pre>interface <i>interface-name</i> { broadcast; <i>description</i> <i>text-description</i>; no-listen; <i>server</i> <i>address</i> <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>; }</pre>
Hierarchy Level	[edit forwarding-options helpers domain], [edit forwarding-options helpers tftp]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the interface for monitoring and forwarding DNS or TFTP requests.
Options	<p><i>interface-name</i>—Name of the interface.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring DNS and TFTP Packet Forwarding on page 94

interface (Monitoring)

Syntax	<pre>interface <i>interface-name</i> { engine-id <i>number</i>; engine-type <i>number</i>; input-interface-index <i>number</i>; output-interface-index <i>number</i>; source-address <i>address</i>; }</pre>
Hierarchy Level	[edit forwarding-options monitoring group-name inet output]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the output interface for monitored traffic.
Options	<p><i>interface-name</i>—Name of the interface.</p> <p><i>engine-id number</i>—Identity of the monitoring interface.</p> <p><i>engine-type number</i>—Type of the monitoring interface.</p> <p><i>input-interface-index number</i>—Input interface index for records from the interface.</p> <p><i>output-interface-index number</i>—Output interface index for records from the interface.</p> <p><i>source-address address</i>—Address used for generating packets.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Passive Flow Monitoring on page 44

interface (Next-Hop Group)

Syntax	<pre>interface <i>interface-name</i> { <i>next-hop</i> <i>address</i>; }</pre>
Hierarchy Level	[edit forwarding-options <i>next-hop-group</i> <i>group-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Specify the output interface for sending copies of packets elsewhere to be analyzed.</p> <p>The commit operation fails when a next-hop group has only one interface configured. It is implicitly assumed that a subgroup is up only if more than one interface in the subgroup is up.</p>
Options	<p><i>interface-name</i>—Name of the interface.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Next-Hop Groups to Use Multiple Interfaces to Forward Packets Used in Port Mirroring on page 49

interface (Port Mirroring)

Syntax	<pre>interface <i>interface-name</i> { <i>next-hop</i> <i>address</i>; }</pre>
Hierarchy Level	<p>[edit forwarding-options <i>port-mirroring</i> <i>output</i>],</p> <p>[edit forwarding-options <i>port-mirroring</i> <i>family</i> (inet inet6) <i>output</i>]</p>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the output interface for sending copies of packets elsewhere to be analyzed.
Options	<p><i>interface-name</i>—Name of the interface.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Port Mirroring on page 45

link-layer-broadcast-inet-check

Syntax	link-layer-broadcast-inet-check;
Hierarchy Level	[edit forwarding-options]
Release Information	Statement introduced in Junos OS Release 14.2.
Description	Enable destination MAC and IP address check to prevent the Router from forwarding IPV4 packets, which have link layer destination address set to broadcast or multicast , unless it is directed to an <i>IPV4 multicast</i> address.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>[edit forwarding-options] Hierarchy Level</i>

load-balance (Forwarding Options)

Syntax	<pre>load-balance { indexed-load-balance; per-flow { hash-seed; } per-prefix { hash-seed <i>number</i>; } }</pre>
Hierarchy Level	<p>[edit forwarding-options], [edit logical-systems <i>logical-system-name</i> forwarding-options], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options], [edit routing-instances <i>routing-instance-name</i> forwarding-options]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.0. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for per-flow load balancing introduced in Junos OS Release 9.3.</p>
Description	<p>Enable per-prefix or per-flow load balancing so that the router or switch elects a next hop independently of the route selected by other routers or switches.</p> <p>For the active route, when there are multiple equal-cost paths to the same destination, by default, Junos OS chooses in a random fashion one of the next-hop addresses to install into the forwarding table. Whenever the set of next hops for a destination changes in any way, the next-hop address is chosen again, also in a random fashion.</p> <p>You can configure Junos OS so that, for the active route, all next-hop addresses for a destination are installed in the forwarding table. This is called per-packet load balancing. You can use load balancing to spread traffic across multiple paths between routing devices. The behavior of the per-packet load-balancing function varies according to the version of the Internet Processor ASIC in the routing device.</p> <p>On routing devices with an Internet Processor I ASIC, when per-packet load balancing is configured, traffic between routing devices with multiple paths is spread in a random fashion across the available interfaces. The forwarding table balances the traffic headed to a destination, transmitting packets in round-robin fashion among the multiple next hops (up to a maximum of eight equal-cost load-balanced paths). The traffic is load-balanced on a per-packet basis.</p> <p>Per-packet load distribution uses a hashing algorithm that distributes packets over equal-cost links. The algorithm is designed to distribute packets to prevent any single link from being saturated. However, per-packet load balancing offers no guarantee of equal distribution of traffic over equal-cost links, nor does it guarantee that increasing the number of Internet flows creates a better hash distribution.</p> <p>On routing devices with the Internet Processor II ASIC and T Series Internet Processor II ASIC, when per-packet load balancing is configured, traffic between routing devices with multiple paths is divided into individual traffic flows (up to a maximum of 16 equal-cost</p>

load-balanced paths). On some platforms, you can increase the number of paths by using the **chassis maximum-ecmp** statement. With this statement, you can change the maximum number of equal-cost load-balanced paths to 32 or 64. Packets for each individual flow are kept on a single interface. To recognize individual flows in the transit traffic, the routing device examines each of the following:

- Source IP address
- Destination IP address
- Protocol
- Source port number
- Destination port number
- Source interface index
- Type of service (ToS)

The routing device recognizes packets in which all of these parameters are identical, and it ensures that these packets are sent out through the same interface. This prevents problems that might otherwise occur with packets arriving at their destination out of their original sequence.

Load balancing is not supported on management and internal Ethernet (**fxo**) interfaces because this type of interface cannot handle the routing process. On **fxp** interfaces, you cannot configure multiple next hops and enable load balancing.

Options The statements are explained separately.

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

Related Documentation

- *Example: Load Balancing BGP Traffic*
- [Configuring Per-Flow Load Balancing Based on Hash Values on page 70](#)
- [Configuring Per-Prefix Load Balancing on page 69](#)

load-balance-group

Syntax	<code>load-balance-group <i>group-name</i> { next-hop-group [<i>group-names</i>]; }</code>
Hierarchy Level	[edit firewall]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure a load-balance group.
Options	<p><i>group-name</i>—Name of load-balance group.</p> <p><i>group-names</i>—Name of next-hop groups to include in the load-balance group set.</p>
Required Privilege Level	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Load-Balance Groups on page 65 in the <i>Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices</i>

local-dump

Syntax	<code>(local-dump no-local-dump);</code>
Hierarchy Level	[edit forwarding-options sampling family (inet inet6 mpls) output flow-server <i>hostname</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Enable collection of cflowd records in a log file.
Options	<p>no-local-dump—Do not dump cflowd records to a log file before exporting.</p> <p>local-dump—Dump cflowd records to a log file before exporting.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Debugging cflowd Flow Aggregation on page 28

max-packets-per-second

Syntax	<code>max-packets-per-second <i>number</i>;</code>
Hierarchy Level	[edit forwarding-options sampling input]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify that the traffic threshold that must be exceeded before packets are dropped. A value of 0 instructs the Packet Forwarding Engine not to sample any traffic.
Options	<i>number</i> —Maximum number of packets per second. Range: 0 through 65,535 Default: 1000
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">See Configuring Traffic Sampling on page 22.

maximum-hop-count

Syntax	<code>maximum-hop-count <i>number</i>;</code>
Hierarchy Level	[edit forwarding-options helpers bootp], [edit forwarding-options helpers bootp interface (<i>interface-name</i> <i>interface-group</i>)]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Description	Set the maximum allowed number of hops. This value is compared against the hops field in the BOOTP request message. BOOTP request messages that have a number in the hops field that exceeds maximum-hop-count are not forwarded. If you omit the maximum-hop-count statement, the default value is four hops.
Options	<i>number</i> —Maximum number of hops for BOOTP request messages. Range: 1 through 16 Default: 4
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents on page 91

maximum-packet-length

Syntax	<code>maximum-packet-length bytes;</code>
Hierarchy Level	[edit forwarding-options analyzer analyzer-name input], [edit forwarding-options port-mirroring input], [edit forwarding-options port-mirroring instance instance-name input], [edit forwarding-options sampling input], [edit forwarding-options sampling instance instance-name input]
Release Information	Statement introduced in Junos OS Release 9.6. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers. The [edit forwarding-options analyzer analyzer-name input] hierarchy level for MX Series routers introduced in Junos OS Release 14.1.
Description	Set the maximum length of the packet used for port mirroring or traffic sampling. Packets with lengths greater than the specified maximum are truncated.



NOTE: The `maximum-packet-length` statement is not supported on MX80 routers or PTX Series routers with third-generation FPCs installed.



NOTE: For MX Series routers with Modular Port Interface Concentrators (MPCs), when `maximum-packet-length` (clip length) is configured for port-mirrored packets and the mirror-destination interface is a next-hop-group, the clip length would be effective only for the first member interface of the next-hop-group. The mirrored packet copy sent to the rest of the interfaces would not be clipped.

Native analyzer sessions (that is, the [edit forwarding-options analyzer analyzer-name input] hierarchy level for MX Series routers) can be configured without specifying input parameters, which would mean that the instance uses default input values: `rate = 1` and `maximum-packet-length = 0`.

Options	<i>bytes</i> —Maximum length (in bytes) of the mirrored packet or the sampled packet. Range: 0 through 9216 Default: 0
----------------	--------------------------------------------------------------------------------------------------------------------------------------------

For MX Series routers with Modular Port Concentrators (MPCs), port-mirrored or sampled packets can be truncated (or clipped) to any length in the range of 1 to 255 bytes. Only 1 to 255 are valid values for packet truncation on these devices. For other devices, the range is from 0 to 9216. A `maximum-packet-length` value of zero represents that truncation is disabled, and the entire packet is mirrored or sampled.

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

Related Documentation

- [Configuring Port Mirroring on page 45](#)
- [Configuring Traffic Sampling](#)

minimum-wait-time

Syntax minimum-wait-time *seconds*;

Hierarchy Level [edit forwarding-options [helpers bootp](#)],
[edit forwarding-options [helpers bootp interface](#) (*interface-name* | *interface-group*)]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

Description Set the minimum allowed number of seconds that the BOOTP client has waited before packets are forwarded, based on the secs field in the BOOTP request message. If the value of **minimum-wait-time** is less than the value of the secs field in the BOOTP request message, the packet is not forwarded to the BOOTP servers and relay agents that are configured at the hierarchy level of this statement. You can use the **minimum-wait-time** statement to determine which servers the device should forward packets to based on how long the BOOTP client has been waiting to receive a BOOTP reply from a server. The BOOTP client sets the secs field in the BOOTP request to reflect the number of seconds elapsed since the client began address acquisition or a renewal process.

The default value for the minimum wait time is zero (0) seconds. If the minimum wait time is 0 and the secs field in the BOOTP request message is 0, the device forwards the packet.

Options *seconds*—Minimum wait time the BOOTP client has waited before packets are forwarded.
Range: 0 to 30,000
Default: 0

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

Related Documentation

- [Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents on page 91](#)

mirror-once

Syntax	mirror-once;
Hierarchy Level	[edit forwarding-options port-mirroring]
Release Information	Statement introduced in Junos OS Release 9.3 (MX Series routers only). Support extended to M120 routers in Junos OS Release 9.5. Statement introduced in Junos OS Release 12.1X48 for PTX Packet Transport Routers.
Description	Configure the router to mirror packets only once. This feature is useful if you configure port mirroring on both ingress and egress interfaces, which could result in the same packet being mirrored twice.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Port Mirroring on page 45

monitoring

Syntax `monitoring group-name {
 family inet {
 output {
 cflowd hostname {
 port port-number;
 }
 export-format cflowd-version-5;
 flow-active-timeout seconds;
 flow-export-destination {
 (cflowd-collector | collector-pic);
 }
 flow-inactive-timeout seconds;
 interface interface-name {
 engine-id number;
 engine-type number;
 input-interface-index number;
 output-interface-index number;
 source-address address;
 }
 }
 }
 }`

Hierarchy Level [edit forwarding-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify flow monitoring instance name and properties.

 The statements are explained separately.

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

Related Documentation • [Configuring Passive Flow Monitoring on page 44](#)

next-hop (Forwarding Options)

Syntax	<code>next-hop <i>address</i>;</code>
Hierarchy Level	[edit forwarding-options port-mirroring <code>output interface <i>interface-name</i></code>], [edit forwarding-options port-mirroring family (inet inet6 ccc vpls) <code>output interface <i>interface-name</i></code>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
Description	Specify the next-hop address for sending copies of packets to an analyzer.
Options	<i>address</i> —IP address of the next-hop router.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Port Mirroring on page 45

next-hop-group (Forwarding Options)

Syntax	<pre>next-hop-group <i>group-name</i> { interface <i>interface-name</i> { next-hop <i>address</i>; } next-hop-subgroup <i>subgroup-name</i> { interface <i>interface-name</i> { next-hop <i>address</i>; } } }</pre>
Hierarchy Level	[edit forwarding-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Specify the next-hop address for sending copies of packets to an analyzer.</p> <p>The commit operation fails when a next-hop group has only one interface configured. It is implicitly assumed that a subgroup is up only if more than one interface in the subgroup is up.</p>
Options	<p><i>addresses</i>—IP address of the next-hop router. Each next-hop group supports up to 16 next-hop addresses. Up to 30 next-hop groups are supported. Each next-hop group must have at least two next-hop addresses.</p> <p><i>group-names</i>—Name of next-hop group. Up to 30 next-hop groups are supported for the router. Each next-hop group must have at least two next-hop addresses.</p> <p><i>interface-name</i>—Interface used to reach the next-hop destination.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Next-Hop Groups to Use Multiple Interfaces to Forward Packets Used in Port Mirroring on page 49

next-hop-group

Syntax	<pre> next-hop-group <i>group-name</i>{ group-type inet6; interface <i>interface-name</i> { next-hop <i>ipv6-address</i>; } next-hop-subgroup <i>group-name</i>{ interface <i>interface-name</i> { next-hop <i>ipv6-address</i>; } } } </pre>
Hierarchy Level	[edit forwarding-options port-mirroring family inet6 output]
Release Information	Statement introduced in Junos OS Release 14.2 for IPv6.
Description	Specify the next-hop group through which to send port-mirror traffic to an analyzer. This configuration enables multipacket port mirroring on MX Series routers with or without the use of a Tunnel PIC. It is implicitly assumed that a subgroup is up only if more than one interface in the subgroup is up.
Options	<p><i>group-name</i>—Name of the next-hop group. Up to 30 next-hop groups are supported for the router. Each next-hop group must have at least two next-hop addresses.</p> <p><i>interface-name</i>—Name of the interface used to reach the next-hop destination.</p> <p><i>ipv6-address</i>—IPv6 address of the next-hop router. Each next-hop group supports up to 16 next-hop addresses. Each next-hop subgroup can have up to 16 next-hop groups.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Port Mirroring

no-filter-check

Syntax	no-filter-check;
Hierarchy Level	[edit forwarding-options port-mirroring output], [edit forwarding-options port-mirroring family (inet inet6 ccc vpls) output]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
Description	Disable filter checking on the port-mirroring interface. This statement is required when you send port-mirrored traffic to a Tunnel Services PIC that has a filter applied to it.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Port Mirroring on page 45

no-listen

Syntax	no-listen;
Hierarchy Level	[edit forwarding-options helpers bootp interface (<i>interface-name</i> <i>interface-group</i>)], [edit forwarding-options helpers domain interface <i>interface-name</i>], [edit forwarding-options helpers tftp interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Description	Disable recognition of DNS requests or stop packets from being forwarded on a logical interface, a group of logical interfaces, a router, or a switch.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring DNS and TFTP Packet Forwarding on page 94• Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents on page 91

output (Accounting)

```
Syntax  output {
        cflowd [ hostnames ] {
            aggregation {
                autonomous-system;
                destination-prefix;
                protocol-port;
                source-destination-prefix {
                    caida-compliant;
                }
                source-prefix;
            }
            autonomous-system-type (origin | peer);
            port port-number;
            version format;
        }
        flow-active-timeout seconds;
        flow-inactive-timeout seconds;
        interface interface-name {
            engine-id number;
            engine-type number;
            source-address address;
        }
    }
```

Hierarchy Level [edit forwarding-options [accounting](#) *group-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure cflowd, output interfaces, and flow properties.

The statements are explained separately.

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

Related Documentation

- [Configuring Discard Accounting on page 40](#)

output (Forwarding Table)

Syntax	<code>output <i>filter-name</i>;</code>
Hierarchy Level	[edit forwarding-options family (inet inet6 mpls) filter], [edit routing-instances <i>routing-instance-name</i> forwarding-options family (inet inet6 mpls) filter]
Release Information	Statement introduced in Junos OS Release 7.5. Statement introduced in Junos OS Release 15.1X53-D10 for QFX10000 switches..
Description	Configure filtering on the egress traffic of the forwarding table.
Options	<i>filter-name</i> —Name of the applied filter.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Applying Forwarding Table Filters on page 60

output (Monitoring)

Syntax	<pre> output { cflowd hostname { port port-number; } export-format cflowd-version-5; flow-active-timeout seconds; flow-export-destination { (cflowd-collector collector-pic); } flow-inactive-timeout seconds; interface interface-name { engine-id number; engine-type number; input-interface-index number; output-interface-index number; source-address address; } } </pre>
Hierarchy Level	[edit forwarding-options monitoring group-name family inet]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure cflowd, output interfaces, and flow properties.</p> <p>The statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Passive Flow Monitoring on page 44

output (Port Mirroring)

Syntax	<pre> output { interface interface-name { next-hop address; } next-hop-group group-name { group-type inet6; interface interface-name { next-hop ipv6-address; } next-hop-subgroup group-name { interface interface-name { next-hop ipv6-address; } } } no-filter-check; server-profile server-profile-name; } </pre>
Hierarchy Level	<p>[edit forwarding-options port-mirroring family (ccc inet inet6 mpls vpls)],</p> <p>[edit forwarding-options port-mirroring instance instance-name family (ccc inet inet6 mpls vpls)]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>vpls option introduced in Junos OS Release 9.3 for MX Series routers only; support extended to M7i, M10i, M120, and M320 routers in Junos OS Release 9.5.</p> <p>ccc option introduced in Junos OS Release 9.6 for M120 and M320 routers only.</p> <p>server-profile option introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers only.</p> <p>next-hop-group option introduced for family inet6 in Junos OS Release 14.2 for MX Series routers only.</p>
Description	<p>Configure the port mirroring destination properties.</p> <p>The statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Port Mirroring on page 45 • Configuring Active Flow Monitoring on PTX Series Packet Transport Routers on page 42

output (Sampling)

```
Syntax  output {
        aggregate-export-interval seconds;
        flow-server hostname {
            aggregation {
                autonomous-system;
                destination-prefix;
                protocol-port;
                source-destination-prefix {
                    caida-compliant;
                }
                source-prefix;
            }
            autonomous-system-type (origin | peer);
            (local-dump | no-local-dump);
            port port-number;
            source-address address;
            version format;
            version9 {
                template template-name;
            }
        }
        extension-service service-name;
        file filename filename <disable> <files number> <stamp | no-stamp> <size bytes>
            <world-readable | no-world-readable>;
        flow-active-timeout seconds;
        flow-inactive-timeout seconds;
        flow-server host-name {
            aggregation;
            autonomous-system-type (origin | peer);
            (local-dump | no-local-dump);
            port number;
            source-address address;
            version (5 | 8);
            version9;
        }
        interface interface-name {
            engine-id number;
            engine-type number;
            source-address address;
        }
    }
```

Hierarchy Level [edit forwarding-options **sampling family** (inet | inet6 | mpls)]

Release Information Statement introduced before Junos OS Release 7.4.
version9 statement introduced in Junos OS Release 8.3.

Description Configure cflowd, output files and interfaces, and flow properties. Enable the collection of traffic flows using the version 9 format.

The statements are explained separately.

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

Related Documentation

- [Collecting Traffic Sampling Output in the Cisco Systems NetFlow Services Export Version 9 Format on page 29](#)
- [Collecting Traffic Sampling Output in a File on page 24](#)

per-flow

Syntax

```
per-flow {  
    hash-seed;  
}
```

Hierarchy Level [edit forwarding-options [load-balance](#)],
[edit logical-systems *logical-system-name* forwarding-options [load-balance](#)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options [load-balance](#)],
[edit routing-instances *routing-instance-name* forwarding-options [load-balance](#)]

Release Information Statement introduced in Junos OS Release 9.3 (M120, M320, and MX Series routers only).

Description Enable per-flow load balancing based on hash values.

Options **hash-seed**—Configure the hash value. Junos OS automatically chooses a value for the hashing algorithm used. You cannot configure a specific hash value for per-flow load balancing.

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

Related Documentation

- [Configuring Per-Flow Load Balancing Based on Hash Values on page 70](#)
- [load-balance \(Forwarding Options\) on page 157](#)

per-prefix

Syntax	<code>per-prefix { hash-seed <i>number</i>; }</code>
Hierarchy Level	[edit forwarding-options load-balance], [edit logical-systems <i>logical-system-name</i> forwarding-options load-balance], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options load-balance], [edit routing-instances <i>routing-instance-name</i> forwarding-options load-balance]
Release Information	Statement introduced in Junos OS Release 9.0. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the hash parameter for per-prefix load balancing.
Options	hash-seed —Per-prefix load-balancing hash function. <i>number</i> —Hash value. Range: 0 through 65,534 Default: 0
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Per-Prefix Load Balancing on page 69 • load-balance (Forwarding Options) on page 157

port (cflowd)

Syntax	<code>port <i>port-number</i>;</code>
Hierarchy Level	[edit forwarding-options accounting group-name output cflowd <i>hostname</i>], [edit forwarding-options monitoring group-name family inet output flow-server <i>hostname</i>], [edit forwarding-options sampling family (inet inet6 mpls) output flow-server <i>hostname</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the UDP port number on the cflowd host system.
Options	<i>port-number</i> —Any valid UDP port number on the host system.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Directing Traffic Sampling Output to a Server Running the cflowd Application on page 26

port (Packet Forwarding)

Syntax `port port-number {
 description text-description;
 interface interface-name {
 broadcast;
 description text-description;
 no-listen;
 server address <logical-system logical-system-name> <routing-instance routing-instance-name>;
 }
 server address <logical-system logical-system-name> <routing-instance routing-instance-name>;
 }`

Hierarchy Level [edit forwarding-options helpers]

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 UDP or TCP port number for listening.

In addition to TFTP and DNS, you can use the helpers statement to enable LAN broadcast forwarding. To do this, you must manually define which UDP port is forwarded, as shown here:

```
user@ host# show forwarding-options
helpers {
  port 3000 {
    interface {
      fe-0/0/1.0 {
        server 111.0.0.2;
      }
    }
  }
  port 3001 {
    interface {
      fe-0/0/0.0 {
        server 100.0.0.2;
      }
    }
  }
}
```

The remaining statements are explained separately.

Options *port-number*—UDP or TCP port number for listening.
Range: 1 through 65535

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

- Related Documentation**
- [Configuring DNS and TFTP Packet Forwarding on page 94](#)
 - [Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents on page 91](#)

port-mirroring

```

Syntax  port-mirroring {
        input {
            maximum-packet-length bytes;
            rate number;
            run-length number;
        }
        family (ccc | inet | inet6 | vpls) {
            output {
                interface interface-name {
                    next-hop address;
                }
                next-hop-group group-name {
                    group-type inet6;
                    interface interface-name {
                        next-hop ipv6-address;
                    }
                }
                next-hop-subgroup group-name {
                    interface interface-name {
                        next-hop ipv6-address;
                    }
                }
            }
            no-filter-check;
        }
    }
    instance {
        instance-name {
            input {
                maximum-packet-length bytes;
                rate number;
                run-length number;
            }
            family (ccc | inet | inet6 | vpls) {
                output {
                    interface interface-name {
                        next-hop address;
                    }
                }
                no-filter-check;
                server-profile server-profile-name;
            }
        }
    }
    mirror-once;
    traceoptions {
        file filename <files number> <size bytes> <world-readable | no-world-readable>;
    }
}

```

Hierarchy Level [edit forwarding-options]

Release Information Statement introduced before Junos OS Release 7.4.

family vpls statement introduced in Junos OS Release 9.3 (MX Series routers only); support extended to M7i, M10, M120, and M320 routers in Junos OS Release 9.5.

instance port-mirroring-instance-name statement introduced in Junos OS Release 9.3 (MX Series routers only); support extended to M120 and M320 routers in Junos OS Release 9.5.

mirror-once statement introduced in Junos OS Release 9.3 (MX Series routers only); support extended to M120 routers in Junos OS Release 9.5.

family ccc statement introduced in Junos OS Release 9.6 (M120 and M320 routers only). Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.

family inet6 and **next-hop-group** statements introduced in Junos OS Release 14.2 (MX Series routers only).

Description	Specify the address family, rate, run length, interface, and next-hop address for sending copies of packets to an analyzer. The statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Port Mirroring on page 45• Configuring Active Flow Monitoring on PTX Series Packet Transport Routers on page 42

rate (Forwarding Options)

Syntax	<code>rate number;</code>
Hierarchy Level	[edit forwarding-options analyzer <i>analyzer-name</i> input], [edit forwarding-options port-mirroring family (inet inet6) input], [edit forwarding-options port-mirroring input], [edit forwarding-options sampling input], [edit forwarding-options sampling instance <i>instance-name</i> input]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers. Support at the [edit forwarding-options analyzer <i>analyzer-name</i> input] hierarchy level for MX Series routers introduced in Junos OS Release 14.1.
Description	<p>Set the ratio of the number of packets to be sampled. For example, if you specify a rate of 10, every tenth packet (1 packet out of 10) is sampled.</p> <p>Native analyzer sessions (that is, the [edit forwarding-options analyzer <i>analyzer-name</i> input] hierarchy level for MX Series routers) can be configured without specifying input parameters, which would mean that the instance uses default input values: rate = 1 and maximum-packet-length = 0.</p>
Options	<p><i>number</i>—Denominator of the ratio.</p> <p>Range: 1 through 65,535</p>
Usage Guidelines	See <i>Configuring Port Mirroring</i> or <i>Configuring Traffic Sampling</i> .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Port Mirroring on page 45• Configuring Traffic Sampling on page 22

relay-agent-option

Syntax	relay-agent-option;
Hierarchy Level	[edit forwarding-options helpers bootp], [edit logical-systems routing-instances <i>instance-name</i> forwarding-options helpers bootp], [edit routing-instances <i>instance-name</i> forwarding-options helpers bootp]
Release Information	Statement introduced in Junos OS Release 8.0.
Description	Enable the DHCP relay agent information option which allows DHCP to forward information from clients on different VRF routing instances. The functionality is described in RFC 3046, <i>DHCP Relay Agent Information Option</i> . For the Junos OS implementation, the DHCP option number is 82, and the suboption ID is 1. The suboption length is the length required to contain an interface name in addition to the terminating null character. The overall option length is the suboption length plus 2 bytes (for the option header). The DHCP relay agent information option is only present on packets sent between the relay and the DHCP server.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents on page 91

route-accounting

Syntax	route-accounting;
Hierarchy Level	[edit forwarding-options family inet6]
Release Information	Statement introduced in Junos OS Release 8.3.
Description	Configure the routing platform to track IPv6 traffic passing through the router.
Default	Disabled
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring IPv6 Accounting on page 39

run-length

Syntax	<code>run-length <i>number</i>;</code>
Hierarchy Level	[edit forwarding-options port-mirroring input], [edit forwarding-options port-mirroring instance <i>port-mirroring-instance-name</i> input], [edit forwarding-options port-mirroring family (inet inet6) input], [edit forwarding-options sampling input], [edit forwarding-options sampling instance <i>instance-name</i> input]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
Description	Set the number of samples following the initial trigger event. The configuration enables you to sample packets following those already being sampled.
Options	<i>number</i> —Number of samples. Range: 0 through 20 Default: 0
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Applying Forwarding Table Filters on page 60• <i>Configuring Port Mirroring</i>• <i>Configuring Traffic Sampling</i>

sampling (Forwarding Options)

```
Syntax  sampling {
    disable;
    sample-once;
    family (inet | inet6 | mpls) {
        disable;
        output {
            aggregate-export-interval seconds;
            extension-service service-name;
            file {
                disable;
                filename filename;
                files number;
                size bytes;
                (stamp | no-stamp);
                (world-readable | no-world-readable);
            }
            flow-active-timeout seconds;
            flow-inactive-timeout seconds;
            flow-server hostname {
                aggregation {
                    autonomous-system;
                    destination-prefix;
                    protocol-port;
                    source-destination-prefix {
                        caida-compliant;
                    }
                    source-prefix;
                }
                autonomous-system-type (origin | peer);
                (local-dump | no-local-dump);
                port port-number;
                source-address address;
                version format;
                version9 {
                    template template-name;
                }
            }
            interface interface-name {
                engine-id number;
                engine-type number;
                source-address address;
            }
        }
    }
    input {
        max-packets-per-second number;
        maximum-packet-length bytes;
        rate number;
        run-length number;
    }
    instance instance-name {
        disable;
    }
}
```

```

family (inet | inet6 | mpls) {
  disable;
  output {
    aggregate-export-interval seconds;
    extension-service service-name;
    flow-server hostname {
      aggregation {
        autonomous-system;
        destination-prefix;
        protocol-port;
        source-destination-prefix {
          caida-compliant;
        }
        source-prefix;
      }
      autonomous-system-type (origin | peer);
      (local-dump | no-local-dump);
      port port-number;
      source-address address;
      version format;
      version-ipfix {
        template template-name;
      }
      version9 {
        template template-name;
      }
    }
    inline-jflow {
      source-address address;
      flow-export-rate rate;
    }
    interface interface-name {
      engine-id number;
      engine-type number;
      source-address address;
    }
  }
}
input {
  max-packets-per-second number;
  maximum-packet-length bytes;
  rate number;
  run-length number;
}
}
pre-rewrite-tos;
traceoptions {
  no-remote-trace;
  file filename <files number> <size bytes> <match expression> <world-readable |
  no-world-readable>;
}
}

```

Hierarchy Level [edit forwarding-options]

Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Configure traffic sampling. The statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Traffic Sampling</i>• Applying Forwarding Table Filters on page 60• Collecting Traffic Sampling Output in the Cisco Systems NetFlow Services Export Version 9 Format on page 29• Directing Traffic Sampling Output to a Server Running the cflowd Application on page 26• Configuring Port Mirroring on page 45• Tracing Traffic-Sampling Operations on page 33

server (DHCP and BOOTP Relay Agent)

Syntax	<pre>server address { logical-system <i>logical-system-name</i> <routing-instance [<default> <i>routing-instance-names</i>]>; routing-instance [<default> <i>routing-instance-names</i>]; }</pre>
Hierarchy Level	[edit forwarding-options helpers bootp], [edit forwarding-options helpers bootp interface (<i>interface-name</i> <i>interface-group</i>)]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Description	Configure the router or switch to act as a DHCP and BOOTP relay agent. The device forwards all broadcast requests within the configured subnet to all configured servers in parallel. To support clients on different VRFs, see the relay-agent-option statement.
Options	<ul style="list-style-type: none">• address—One or more addresses of the server.• logical-system <i>logical-system-name</i>—(Optional) Logical system of the server.• routing-instance <i>routing-instance-names</i>—(Optional) Routing instance name that belong to the DHCP or BOOTP relay agent.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents on page 91• relay-agent-option on page 181

server (DNS and TFTP Service)

Syntax	<code>server address <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>;</code>
Hierarchy Level	[edit forwarding-options helpers domain], [edit forwarding-options helpers domain interface <i>interface-name</i>], [edit forwarding-options helpers tftp], [edit forwarding-options helpers tftp interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the DNS or TFTP server for forwarding DNS or TFTP requests. Only one server can be specified for each interface.
Options	address —Address of the server. logical-system <i>logical-system-name</i> —(Optional) Logical system of the server. routing-instance [<i>routing-instance-names</i>] —(Optional) Set the routing instance name or names that belong to the DNS server or TFTP server.
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring DNS and TFTP Packet Forwarding on page 94

server-address (Hosted Services)

Syntax	<code>server-address <i>ipv4-address</i>;</code>
Hierarchy Level	[edit services hosted-services server-profile <i>server-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2.
Description	Configure the server address where sampled packets are sent.
Options	<i>ipv4-address</i> —IPv4 address of the server.
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Active Flow Monitoring on PTX Series Packet Transport Routers on page 42

server-profile

Syntax	<code>server-profile <i>server-profile-name</i> { <i>client-address</i> <i>ipv4-address</i>; <i>server-address</i> <i>ipv4-address</i>; }</code>
Hierarchy Level	[edit services hosted-services]
Release Information	Statement introduced in Junos OS Release 13.2.
Description	Configure the server profile.
Options	<i>server-profile-name</i> —Name to apply to this server profile. The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Active Flow Monitoring on PTX Series Packet Transport Routers on page 42

server-profile (Active Flow Monitoring)

Syntax	<code>server-profile <i>server-profile-name</i>;</code>
Hierarchy Level	[edit forwarding-options port-mirroring instance <i>instance-name</i> family (inet inet6 mpls) output]
Description	Specify the name of a server profile. This profile specifies a host where sampled traffic is sent.
Options	<i>server-profile-name</i> —Specify the name of a server profile configured at the [edit services hosted-services server-profile <i>server-profile-name</i>] hierarchy level.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• hosted-services on page 144• Configuring Active Flow Monitoring on PTX Series Packet Transport Routers on page 42

size (Sampling and Traceoptions)

Syntax	<code>size bytes;</code>
Hierarchy Level	<p>[edit forwarding-options helpertraceoptions file], [edit forwarding-options port-mirroring traceoptions file], [edit forwarding-options sampling family family-name output file], [edit forwarding-options sampling traceoptions file]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.</p>
Description	<p>Specify the maximum size of each file containing sample or log data. The file size is limited by the number of files to be created and the available hard disk space.</p> <p>When a traffic sampling file named sampling-file reaches the maximum size, it is renamed sampling-file.0. When the sampling-file file again reaches its maximum size, sampling-file.0 is renamed sampling-file.1 and sampling-file is renamed sampling-file.0. This renaming scheme continues until the maximum number of traffic sampling files is reached. Then the oldest traffic sampling file is overwritten.</p>
Options	<p>bytes—Maximum size of each traffic sampling file or trace log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).</p> <p>Syntax: <i>xk</i> to specify KB, <i>xm</i> to specify MB, or <i>xg</i> to specify GB</p> <p>Range: 10 KB through the maximum file size supported on your router</p> <p>Default: 1 MB for sampling data; 128 KB for log information</p>
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Collecting Traffic Sampling Output in a File on page 24 • Tracing Traffic-Sampling Operations on page 33

source-checking

Syntax	source-checking;
Hierarchy Level	[edit forwarding-options family inet6]
Release Information	Statement introduced in Junos OS Release 12.3.
Description	<p>(MX Series 3D Universal Edge Routers Only) Discard IPv6 packets when the source address type is unspecified, loopback, multicast or link-local</p> <p>RFC 4291, <i>IP Version 6 Addressing Architecture</i>, refers to four address types that require special treatment when they are used as source addresses. The four address types are:</p> <ul style="list-style-type: none">• Unspecified• Loopback• Multicast• Link-Local Unicast <p>The loopback and multicast addresses must never be used as a source address in IPv6 packets. The unspecified and link-local addresses can be used as source addresses but routers must never forward packets that have these addresses as source addresses. Typically, packets that contain unspecified or link-local addresses as source addresses are delivered to the local host. If the destination is not the local host, then the packet must not be forwarded. Configuring this statement filters or discards IPv6 packets of these four address types.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Applying Forwarding Table Filters on page 60

stamp

Syntax	(stamp no-stamp);
Hierarchy Level	[edit forwarding-options sampling family family-name output file]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Include a timestamp with each line in the output file.
Default	no-stamp
Options	<p>no-stamp—Do not include timestamps.</p> <p>stamp—Include a timestamp with each line of packet sampling information.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Collecting Traffic Sampling Output in a File on page 24

tftp

Syntax	<pre>tftp { description text-description; interface interface-name { broadcast; description text-description; no-listen; server address <logical-system logical-system-name> <routing-instance routing-instance-name>; } server address <logical-system logical-system-name> <routing-instance routing-instance-name>; }</pre>
Hierarchy Level	[edit forwarding-options helpers]
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>Enable TFTP request packet forwarding.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring DNS and TFTP Packet Forwarding on page 94

traceoptions (DNS and TFTP Packet Forwarding)

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i>> <size <i>bytes</i>> <world-readable no-world-readable>; flag <i>flag</i>; level <i>level</i>; <no-remote-trace>; }</pre>
Hierarchy Level	[edit forwarding-options helpers]
Release Information	Statement introduced before Junos OS Release 7.4. Statement standardized and match option introduced in Junos OS Release 8.0. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure tracing operations for BOOTP, DNS and TFTP packet forwarding.
Default	If you do not include this statement, no tracing operations are performed.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" "). All files are placed in a file named fud in the directory /var/log. If you include the file statement, you must specify a filename.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000 Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none">• address—Trace address management events• all—Trace all events• bootp—Trace BOOTP or DHCP services events• config—Trace configuration events• domain—Trace DNS service events• ifdb—Trace interface database operations• io—Trace I/O operations• main—Trace main loop events• port—Trace arbitrary protocol events

- **rtsock**—Trace routing socket operations
- **tftp**—Trace TFTP service events
- **trace**—Trace tracing operations
- **ui**—Trace user interface operations
- **util**—Trace miscellaneous utility operations

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—(Optional) Disable remote tracing globally or for a specific tracing operation.

no-world-readable—(Optional) Restrict file access to the owner.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** file again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and filename.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB

Range: 0 bytes through 4,294,967,295 KB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Tracing BOOTP, DNS, and TFTP Forwarding Operations on page 95

traceoptions (Port Mirroring and Traffic Sampling)

Syntax	<code>traceoptions { file <i>filename</i> <files number> <size bytes> <world-readable no-world-readable>; }</code>
Hierarchy Level	[edit forwarding-options port-mirroring], [edit forwarding-options sampling]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure traffic sampling tracing operations. The statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Tracing Traffic-Sampling Operations on page 33

version

Syntax	<code>version <i>format</i>;</code>
Hierarchy Level	[edit forwarding-options accounting group-name output cflowd hostname], [edit forwarding-options sampling family (inet inet6 mpls) output flow-server hostname]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the version format of the aggregated flows exported to a cflowd server.
Options	format —Export format of the flows. Values: 5 or 8 Default: 5
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Directing Traffic Sampling Output to a Server Running the cflowd Application on page 26

version9

Syntax	<pre>version9 { template <i>template-name</i>; }</pre>
Hierarchy Level	[edit forwarding-options sampling family <i>family-name</i> output flow-server <i>hostname</i>]
Release Information	Statement introduced in Junos OS Release 8.3.
Description	Enable active flow monitoring using the version 9 template format to collect traffic flows.
Options	template <i>template-name</i> —Name of a version 9 record flow format template configured at the [edit services monitoring] hierarchy level.
Required Privilege Level	interface—To view this statement in the configuration. interface-level—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Collecting Traffic Sampling Output in the Cisco Systems NetFlow Services Export Version 9 Format on page 29• <i>Flow Monitoring Feature Guide for Routing Devices</i>• <i>Junos OS Services Interfaces Library for Routing Devices</i>

world-readable (Forwarding Options)

Syntax	(world-readable no-world-readable);
Hierarchy Level	[edit forwarding-options helpers traceoptions file], [edit forwarding-options port-mirroring traceoptions file], [edit forwarding-options sampling family <i>family-name</i> output file], [edit forwarding-options sampling traceoptions file]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
Description	Enable unrestricted file access.
Default	no-world-readable
Options	no-world-readable —Restrict file access to the owner. world-readable —Enable unrestricted file access.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Collecting Traffic Sampling Output in a File on page 24• Tracing Traffic-Sampling Operations on page 33

CHAPTER 8

Operational Commands

- clear passive-monitoring statistics
- clear services flow-collector statistics
- request services flow-collector change-destination primary interface
- request services flow-collector change-destination secondary interface
- request services flow-collector test-file-transfer
- show chassis forwarding
- show forwarding-options hyper-mode
- show forwarding-options port-mirroring
- show forwarding-options next-hop-group
- show interfaces (Flow Monitoring)
- show interfaces (M Series, MX Series, T Series Routers, and PTX Series Management and Internal Ethernet)
- show interfaces statistics
- show passive-monitoring error
- show passive-monitoring flow
- show passive-monitoring memory
- show passive-monitoring status
- show passive-monitoring usage
- show route forwarding-table
- show services accounting aggregation
- show services accounting aggregation template
- show services accounting errors
- show services accounting flow
- show services accounting flow-detail
- show services accounting memory
- show services accounting packet-size-distribution
- show services accounting status
- show services accounting usage

- `show services flow-collector file interface`
- `show services flow-collector input interface`
- `show services flow-collector interface`

clear passive-monitoring statistics

Syntax	clear passive-monitoring statistics (all interface <i>interface-name</i>)
Release Information	Command introduced in Junos OS Release 7.6.
Description	(M40e, M160, and M320 routers and T Series routers only) Clear statistics for one passive monitoring interface or for all passive monitoring interfaces.
Options	all —Clear statistics for all configured passive monitoring interfaces. interface <i>interface-name</i> —Clear statistics for the specified passive monitoring interface (<i>mo-fpc/pic/port</i>).
Required Privilege Level	network
List of Sample Output	clear passive-monitoring statistics on page 199
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear passive-monitoring statistics

```
user@host> clear passive-monitoring statistics interface mo-5/0/0
```

clear services flow-collector statistics

Syntax	clear services flow-collector statistics (all interface <i>interface-name</i>)
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M40e, M160, and M320 routers and T Series routers only) Clear statistics for one flow collector interface or for all flow collector interfaces.
Options	all —Clear statistics for all configured flow collector interfaces. interface <i>interface-name</i> —Clear statistics for the specified flow collector interface (<i>cp-fpc/pic/port</i>).
Required Privilege Level	network
List of Sample Output	clear services flow-collector statistics on page 200
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services flow-collector statistics

```
user@host> clear services flow-collector statistics interface cp-5/0/0
Flow collector interface: cp-5/0/0
Interface state: Collecting flows
Statistics cleared successfully
```

request services flow-collector change-destination primary interface

Syntax	request services flow-collector change-destination primary interface <i>cp-fpc/pic/port</i> <clear-files> <clear-logs> <immediately gracefully>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M40e, M160, and M320 routers and T Series routers only) Switch to the primary File Transfer Protocol (FTP) server that is configured as a flow collector.
Options	<p>none—Switch to the primary FTP server.</p> <p>cp-fpc/pic/port—Specify the flow collector interface name for the primary destination.</p> <p>clear-files—(Optional) Request clearing of existing data files in the FTP wait queue when the switch takes place.</p> <p>clear-logs—(Optional) Request clearing of existing logs when the switch takes place.</p> <p>immediately gracefully—(Optional) Specify whether you want the switch to take place immediately, or to affect only newly created files.</p>
Required Privilege Level	maintenance
List of Sample Output	request services flow-collector change-destination primary interface on page 201
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request services flow-collector change-destination primary interface

```

user@host> request services flow-collector change-destination primary interface cp-6/0/0
Flow collector interface: cp-6/0/0
Interface state: Collecting flows
Destination change successful

```

request services flow-collector change-destination secondary interface

Syntax	<code>request services flow-collector change-destination secondary interface <i>cp-fpc/pic/port</i></code> <code><clear-files></code> <code><clear-logs></code> <code><immediately gracefully></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M40e, M160, and M320 routers and T Series routers only) Switch to the secondary File Transfer Protocol (FTP) server that is configured as a flow collector.
Options	<p>none—Switch to the secondary FTP server.</p> <p><i>cp-fpc/pic/port</i>—Specify the flow collector interface name (<i>cp-fpc/pic/port</i>) for the secondary destination.</p> <p>clear-files—(Optional) Request clearing of existing data files in the FTP wait queue when the switch takes place.</p> <p>clear-logs—(Optional) Request clearing of existing logs when the switch takes place.</p> <p>immediately gracefully—(Optional) Specify whether you want the switch to take place immediately, or to affect only newly created files.</p>
Required Privilege Level	maintenance
List of Sample Output	request services flow-collector change-destination secondary interface on page 202
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request services flow-collector change-destination secondary interface

```
user@host> request services flow-collector change-destination secondary interface cp-6/0/0
Flow collector interface: cp-6/0/0
Interface state: Collecting flows
Destination change successful
```

request services flow-collector test-file-transfer

Syntax	<code>request services flow-collector test-file-transfer <i>filename</i> interface (all <i>cp-fpc/pic/port</i>) (channel-zero channel-one) (primary secondary)</code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M40e, M160, and M320 routers, PTX Series, and T Series routers only) Transfer a test file to the primary or secondary File Transfer Protocol (FTP) server that is configured as a flow collector. This command verifies that the output side of the flow collector interface is operating properly.
Options	<p><i>filename</i>—Name of the test file to transfer.</p> <p>interface all <i>cp-fpc/pic/port</i>—Transfer a test file of flows from all configured flow collector interfaces or from only the specified interface.</p> <p>channel-zero channel-one—Transfer a file from export channel 0 (unit 0) or channel 1 (unit 1) of the PIC.</p> <p>primary secondary—Transfer a file to the primary or secondary server configured as a flow collector.</p>
Required Privilege Level	network
List of Sample Output	request services flow-collector test-file-transfer on page 203
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request services flow-collector test-file-transfer

```
user@host> request services flow-collector test-file-transfer test_file interface cp-7/1/0
channel-one primary
```

```
Flow collector interface: cp-7/1/0
Interface state: Collecting flows
Response: Test file transfer successfully scheduled
```

show chassis forwarding

Syntax	show chassis forwarding
Release Information	Current—Command introduced before Junos OS Release 7.4. Now—Command introduced in Junos OS Release 7.4. Support for Branch SRX Series added in Junos OS Release 10.1
Description	Display status of the forwarding process (fwdd). This command is supported on Branch SRX Series Services Gateways.
Options	This command has no options.
Required Privilege Level	view
List of Sample Output	show chassis forwarding on page 204
Output Fields	Table 3 on page 204 lists the output fields for the show chassis forwarding command. Output fields are listed in the approximate order in which they appear.

Table 3: show chassis forwarding Output Fields

Field Name	Field Description
FWWD status	<p>Forwarding status:</p> <ul style="list-style-type: none"> • State: <ul style="list-style-type: none"> • Online—FWDD is operational and running. • Offline—FWDD is not running. • Microkernel CPU utilization—Percentage of microkernel CPU being used by the forwarding process. • Real-time threads CPU utilization—Percentage of CPU being used by the forwarding process. • Heap utilization—Percentage of heap space (dynamic memory) being used by the forwarding process. If this number exceeds 80 percent, there may be a software problem (memory leak). • Buffer utilization—Percentage of buffer space being used by the forwarding process for buffering internal messages. • Uptime—How long the forwarding process has been up and running.

Sample Output

show chassis forwarding

```

user@host> show chassis forwarding
FWDD status:
  State                               Online
  Microkernel CPU utilization         10 percent
  Real-time threads CPU utilization    4 percent
  Heap utilization                     26 percent
  Buffer utilization                   0 percent
  Uptime:                             1 day, 1 hour, 30 minutes, 11 seconds

```

show forwarding-options hyper-mode

Syntax	show forwarding-options hyper-mode
Release Information	Command introduced in Junos OS Release 13.3R4 for MX Series routers.
Description	Display information about the hyper mode feature. After you configure the hyper mode feature, you must reboot the system for the router to reflect the change. For instance, if you have configured hyper mode but not rebooted the system, the Current mode field displays normal while the Configured mode field displays hyper mode .
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Hyper Mode on Enhanced MPCs to Speed Up Packet Processing</i> • <i>Understanding the Hyper Mode Feature on Enhanced MPCs for MX Series Routers</i> • hyper-mode (forwarding-options) on page 145
List of Sample Output	show forwarding-options hyper-mode on page 205
Output Fields	Table 4 on page 205 lists the output fields for the show forwarding-options hyper-mode command. Output fields are listed in the order in which they appear.

Table 4: show forwarding-options hyper-mode Output Fields

Field Name	Field Description
Current mode	Displays the current mode, either normal or hyper mode .
Configured mode	Displays the configured mode, either normal or hyper mode .

Sample Output

show forwarding-options hyper-mode

```
user@host> show forwarding-options hyper-mode
Current mode: hyper mode
Configured mode: hyper mode
```

show forwarding-options port-mirroring

Syntax	show forwarding-options port-mirroring <terse detail> <instance-name>
Release Information	Command introduced in Junos OS Release 9.6. Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Display current state of port-mirroring instances.
Options	terse detail —(Optional) Display the specified level of output. instance-name —(Optional) Display a single port-mirroring instance.
Required Privilege Level	view
Related Documentation	
List of Sample Output	show forwarding-options port-mirroring terse on page 207 show forwarding-options port-mirroring detail on page 207
Output Fields	Table 5 on page 206 lists the output fields for the show forwarding-options port-mirroring command. Output fields are listed in the approximate order in which they appear.

Table 5: show forwarding-options port-mirroring Output Fields

Field Name	Field Description	Level of Output
Instance Name	Name of port-mirroring instance.	All levels
Instance Id	Instance identification number.	All levels
State	Instance state, either up or down .	All levels
Input parameters		
Rate	Rate (ratio of packets sampled).	detail
Run-length	Run length (number of consecutive packets sampled).	detail
Maximum-packet-length	Maximum packet length.	detail
Output parameters		
Family	Protocol family.	detail
State	Instance state, either up or down .	detail
Destination	Destination (next-hop group name).	detail

Sample Output

show forwarding-options port-mirroring terse

```
user@host> show forwarding-options port-mirroring terse
Instance Name      Instance Id  State
&global_instance   1           up
inst1               2           up
```

show forwarding-options port-mirroring detail

```
user@host> show forwarding-options port-mirroring detail
Instance Name: &global_instance
Instance Id: 1      State: up
  Input parameters:
    Rate:           10
    Run-length:      4
    Maximum-packet-length: 0
  Output parameters:
    Family: inet     State: up Destination: inet_nhg
    Family: vpls/eth-switch State: up Destination: vpls_nhg

Instance Name: inst1
Instance Id: 2      State: up
  Input parameters:
    Rate:           1
    Run-length:      0
    Maximum-packet-length: 200
  Output parameters:
    Family: inet     State: up Destination: inet_nhg
    Family: vpls/eth-switch State: down Destination: vpls_nhg_2
```

show forwarding-options next-hop-group

Syntax	show forwarding-options next-hop-group <terse brief detail> <group-name>
Release Information	Command introduced in Junos OS Release 9.6. Command introduced in Junos OS Release 12.3R2 for EX Series switches. Support for IPv6 introduced in Junos OS Release 14.2 for the MX Series routers.
Description	Display current state of next-hop groups.
Options	terse brief detail —(Optional) Display the specified level of output. group-name —(Optional) Display a single next-hop group.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show forwarding-options port-mirroring on page 206
List of Sample Output	show forwarding-options next-hop-group terse on page 209 show forwarding-options next-hop-group brief on page 209 show forwarding-options next-hop-group detail on page 209
Output Fields	Table 6 on page 208 lists the output fields for the show forwarding-options next-hop-group command. Output fields are listed in the approximate order in which they appear.

Table 6: show forwarding-options next-hop-group Output Fields

Field Name	Field Description	Level of Output
Next-hop-group	Name of next-hop group.	All levels
Type	Next-hop group type, such as inet , inet6 or layer-2 .	All levels
State	Next-hop group state, either up or down .	All levels
Members Interfaces	Names of interfaces to which next-hop group members belong.	brief detail
Member Subgroup	Names of subgroups to which next-hop group members belong.	brief detail
Number of members configured	Number of next-hop group members configured.	detail
Number of members that are up	Number of next-hop group members that are up.	detail

Table 6: show forwarding-options next-hop-group Output Fields (*continued*)

Field Name	Field Description	Level of Output
Number of subgroups configured	Number of subgroups configured.	detail
Number of subgroups that are up	Number of subgroups that are up.	detail

Sample Output

show forwarding-options next-hop-group terse

```

user@host> show forwarding-options next-hop-group terse
Next-hop-group      Type      State
nhg                  inet      up
nhg6                 inet6     up
vpls_nhg_2          layer-2   down

```

show forwarding-options next-hop-group brief

```

user@host> show forwarding-options next-hop-group brief

Next-hop-group: nhg
Type: inet
State: up
Members Interfaces:
  ge-0/2/8.0      next-hop 30.1.1.10
  ge-5/1/8.0      next-hop 10.1.1.10
  ge-5/1/9.0      next-hop 20.1.1.10

Next-hop-group: nhg6
Type: inet6
State: up
Members Interfaces:
  ge-5/1/5.0      next-hop 10::1:1:10
  ge-5/1/6.0      next-hop 20::1:1:10
Member Subgroup: nhsg6
Members Interfaces:
  ge-5/0/4.0      next-hop 3::1:1:1
  ge-5/1/4.0      next-hop 4::1:1:1

Next-hop-group: vpls_nhg_2
Type: layer-2      State: down

```

show forwarding-options next-hop-group detail

```

user@host> show forwarding-options next-hop-group detail

Next-hop-group: nhg
Type: inet
State: up
Number of members configured      : 3
Number of members that are up    : 3
Number of subgroups configured    : 0
Number of subgroups that are up  : 0

```

Members Interfaces:		State
ge-0/2/8.0	next-hop 30.1.1.10	up
ge-5/1/8.0	next-hop 10.1.1.10	up
ge-5/1/9.0	next-hop 20.1.1.10	up

Next-hop-group: nhg6

Type: inet6

State: up

Number of members configured : 2

Number of members that are up : 2

Number of subgroups configured : 1

Number of subgroups that are up : 1

Members Interfaces:		State
ge-5/1/5.0	next-hop 10::1:1:10	up
ge-5/1/6.0	next-hop 20::1:1:10	up

Member Subgroup: nhsg6

Number of members configured : 2

Number of members that are up : 2

Members Interfaces:		State
ge-5/0/4.0	next-hop 3::1:1:1	up
ge-5/1/4.0	next-hop 4::1:1:1	up

Next-hop-group: vpls_nhg_2

Number of members configured : 2

Number of members that are up : 0

Number of subgroups configured : 0

Number of subgroups that are up : 0

Type: layer-2 State: down

Members Interfaces: State

ge-2/2/1.100 down

ge-2/3/9.0 down

show interfaces (Flow Monitoring)

Syntax	<pre>show interfaces mo-fpc/pic/port:channel <brief detail extensive terse> <descriptions> <media> <snmp-index snmp-index> <statistics></pre>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M Series and T Series routers only) Display status information about the specified flow monitoring interface.
Options	<p>mo-fpc/pic/port:channel—Display standard status information about the specified flow monitoring interface.</p> <p>brief detail extensive terse—(Optional) Display the specified level of output.</p> <p>descriptions—(Optional) Display interface description strings.</p> <p>media—(Optional) Display media-specific information about network interfaces.</p> <p>snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.</p> <p>statistics—(Optional) Display static interface statistics.</p>
Required Privilege Level	view
List of Sample Output	show interfaces extensive (Flow Monitoring) on page 214
Output Fields	Table 7 on page 211 lists the output fields for the show interfaces (Flow Monitoring) command. Output fields are listed in the approximate order in which they appear.

Table 7: show interfaces Output Fields (Flow Monitoring)

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Link	Status of the link: up or down .	All levels
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Physical interface index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none

Table 7: show interfaces Output Fields (Flow Monitoring) (*continued*)

Field Name	Field Description	Level of Output
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Description	Description and name of the interface.	All levels
Type	Type of interface.	All levels
Link-level type	Encapsulation type used on the physical interface.	All levels
MTU	Maximum Transmit Unit (MTU). Size of the largest packet to be transmitted.	All levels
Clocking	Reference clock source of the interface.	All levels
Speed	Network speed on the interface.	All levels
Device flags	Information about the physical device. Possible values are described in the "Device Flags" section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the "Interface Flags" section under <i>Common Output Fields Description</i> .	All levels
Link type	Data transmission type.	All levels
Link flags	Information about the link. Possible values are described in the "Link Flags" section under <i>Common Output Fields Description</i> .	All levels
Physical info	Information about the physical interface.	All levels
Hold-times	Current interface hold-time up and hold-time down. Value is in milliseconds.	detail extensive
Current address	Configured MAC address.	detail extensive none
Hardware address	Media access control (MAC) address of the interface.	detail extensive none
Alternate link address	Backup link address.	detail extensive none
Last flapped	Date, time, and how long ago the interface went from down to up. The format is Last flapped: <i>year-month-day hour:minute:second timezone (hour:minute:second ago)</i> . For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)	detail extensive
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive

Table 7: show interfaces Output Fields (Flow Monitoring) (*continued*)

Field Name	Field Description	Level of Output
Traffic statistics	<p>Number and rate of bytes and packets received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> • Input bytes, Output bytes—Number of bytes received and transmitted on the interface. • Input packets, Output packets—Number of packets received and transmitted on the interface. 	detail extensive
Input errors	<ul style="list-style-type: none"> • Errors—Input errors on the interface. • Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. • Framing errors—Number of packets received with an invalid frame checksum (FCS). • Runts—Frames received smaller than the runt threshold. • Giants—Frames received larger than the giant threshold. • Policed Discards—Frames that the incoming packet match code discarded because the frames did not recognize them or were not of interest. Usually, this field reports protocols that Junos does not support. • Resource errors—Sum of transmit drops. 	extensive
Output errors	<ul style="list-style-type: none"> • Carrier transitions—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly, possibly once every 10 seconds, the cable, the remote system, or the interface is malfunctioning. • Errors—Sum of outgoing frame aborts and FCS errors. • Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet dropped by the ASIC Red mechanism. • Resource errors—Sum of transmit drops. 	extensive
Logical Interface		
Logical interface	Name of the logical interface.	All levels
Index	Logical interface index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	Logical interface SNMP interface index number.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Flags	Information about the logical interface; values are described in the “Logical Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
Encapsulation	Encapsulation on the logical interface.	All levels

Table 7: show interfaces Output Fields (Flow Monitoring) (*continued*)

Field Name	Field Description	Level of Output
Traffic statistics	<p>Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</p> <ul style="list-style-type: none"> • Input bytes, Output bytes—Number of bytes received and transmitted on the interface. • Input packets, Output packets—Number of packets received and transmitted on the interface. 	detail extensive
Local statistics	Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
Transit statistics	Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
Protocol	Protocol family configured on the logical interface (such as iso or inet6).	detail extensive none
MTU	MTU size on the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route table	Route table in which this address exists; for example, Route table:0 refers to inet.0 .	detail extensive
Flags	Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive none

Sample Output

show interfaces extensive (Flow Monitoring)

```

user@host> show interfaces mo-4/0/0 extensive
Physical interface: mo-4/0/0, Enabled, Physical link is Up
  Interface index: 144, SNMP ifIndex: 42, Generation: 28
  Description: monitor pic 2
  Type: Adaptive-Services, Link-level type: Adaptive-Services, MTU: Unlimited,
  Clocking: Unspecified, Speed: 800mbps
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps 16384
  Link type      : Full-Duplex
  Link flags     : None
  Physical info  : Unspecified
  Hold-times    : Up 0 ms, Down 0 ms
  Current address: Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped  : 2005-05-24 16:43:12 PDT (00:17:46 ago)
  Statistics last cleared: Never

```

```
Traffic statistics:
Input bytes :          756824218          8328536 bps
Output bytes :          872916185          8400160 bps
Input packets:           508452           697 pps
Output packets:        15577196          18750 pps
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
  Policed discards: 0, Resource errors: 0
Output errors:
  Carrier transitions: 2, Errors: 0, Drops: 0, MTU errors: 0,
  Resource errors: 0

Logical interface mo-4/0/0.0 (Index 83) (SNMP ifIndex 43) (Generation 26)
Flags: Point-To-Point SNMP-Traps Encapsulation: Adaptive-Services
Traffic statistics:
  Input bytes :          756781796
  Output bytes :          872255328
  Input packets:           507233
  Output packets:        15575988
Local statistics:
  Input bytes :              0
  Output bytes :              0
  Input packets:              0
  Output packets:             0
Transit statistics:
  Input bytes :          756781796          8328536 bps
  Output bytes :          872255328          8400160 bps
  Input packets:           507233           697 pps
  Output packets:        15575988          18750 pps
Protocol inet, MTU: Unlimited, Generation: 38, Route table: 0
Flags: None

Logical interface mo-4/0/0.16383 (Index 84) (SNMP ifIndex 58) (Generation 27)
...
```

show interfaces (M Series, MX Series, T Series Routers, and PTX Series Management and Internal Ethernet)

List of Syntax	Syntax (M Series, MX Series, T Series, and PTX Series Routers Management Ethernet Interface) on page 216 Syntax (M Series, MX Series, T Series, and PTX Series Routers Internal Ethernet Interface) on page 216
Syntax (M Series, MX Series, T Series, and PTX Series Routers Management Ethernet Interface)	<pre>show interfaces em0 fxp0 <brief detail extensive terse> <descriptions> <media> <snmp-index <i>snmp-index</i>> <statistics></pre>
Syntax (M Series, MX Series, T Series, and PTX Series Routers Internal Ethernet Interface)	<pre>show interfaces bcm0 em0 em1 fxp1 fxp2 ixgbe0 ixgbe1 <brief detail extensive terse> <descriptions> <media> <snmp-index <i>snmp-index</i>> <statistics></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced on PTX Series Packet Transport Routers for Junos OS Release 12.1.</p>
Description	(M Series, T Series, TX Matrix Plus, and PTX Series devices only) Display status information about the management Ethernet and internal Ethernet interfaces.
Options	<p>em0 fxp0—(M Series, MX Series, T Series, and PTX Series) Display standard information about the management Ethernet interface. For supported Ethernet interface by chassis and Routing Engine, see <i>Supported Routing Engines by Router</i>.</p> <p>bcm0 em0 em1 fxp1 fxp2 ixgbe0 ixgbe1—(M Series, MX Series, T Series, and PTX Series) Display standard information about the internal Ethernet interfaces. See <i>Supported Routing Engines by Router</i> for the internal Ethernet interface names for each Routing Engine by hardware platform.</p> <p>brief detail extensive terse—(Optional) Display the specified level of output.</p> <p>descriptions—(Optional) Display interface description strings.</p> <p>media—(Optional) Display media-specific information.</p> <p>snmp-index <i>snmp-index</i>—(Optional) Display information for the specified SNMP index of the interface.</p> <p>statistics—(Optional) Display static interface statistics.</p>
Required Privilege Level	view

- List of Sample Output**
- [show interfaces brief \(Management Ethernet\) on page 220](#)
 - [show interfaces \(Management Ethernet\) on page 220](#)
 - [show interfaces \(Management Ethernet \[TX Matrix Plus Router\]\) on page 221](#)
 - [show interfaces \(Management Ethernet \[PTX Series Packet Transport Routers\]\) on page 221](#)
 - [show interfaces detail \(Management Ethernet\) on page 221](#)
 - [show interfaces detail \(Management Ethernet \[TX Matrix Plus Router\]\) on page 222](#)
 - [show interfaces detail \(Management Ethernet \[PTX Packet Transport Routers\]\) on page 223](#)
 - [show interfaces extensive \(Management Ethernet\) on page 223](#)
 - [show interfaces extensive \(Management Ethernet \[TX Matrix Plus Router\]\) on page 224](#)
 - [show interfaces extensive \(Management Ethernet \[PTX Series Packet Transport Routers\]\) on page 225](#)
 - [show interfaces brief \(Management Ethernet\) on page 226](#)
 - [show interfaces brief \(Management Ethernet \[TX Matrix Plus Router\]\) on page 226](#)
 - [show interfaces brief \(Management Ethernet \[PTX Series Packet Transport Routers\]\) on page 226](#)
 - [show interfaces \(Internal Ethernet\) on page 226](#)
 - [show interfaces \(Internal Ethernet \[TX Matrix Plus Router\]\) on page 227](#)
 - [show interfaces detail \(Internal Ethernet\) on page 227](#)
 - [show interfaces detail \(Internal Ethernet \[TX Matrix Plus Router\]\) on page 228](#)
 - [show interfaces extensive \(internal Ethernet\) on page 229](#)
 - [show interfaces extensive \(internal Ethernet \[TX Matrix Plus Router\]\) on page 230](#)

Output Fields Table 8 on page 217 lists the output fields for the **show interfaces** (management) command on the M Series routers, T Series routers, TX Matrix Plus routers, and PTX Series. Output fields are listed in the approximate order in which they appear.

Table 8: show interfaces Output Fields for M Series, MX Series, T Series, and PTX Series Routers Management Ethernet Interface

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Physical interface index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Type	Type of interface.	All levels
Link-level type	Encapsulation type used on the physical interface.	All levels
MTU	Maximum transmission unit (MTU)—Size of the largest packet to be transmitted.	All levels

Table 8: show interfaces Output Fields for M Series, MX Series, T Series, and PTX Series Routers Management Ethernet Interface (*continued*)

Field Name	Field Description	Level of Output
Clocking	Reference clock source of the interface.	All levels
Speed	Network speed on the interface.	All levels
Device flags	Information about the physical device. Possible values are described in the “Device Flags” section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the “Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
Link type	Data transmission type.	detail extensive none
Link flags	Information about the link. Possible values are described in the “Link Flags” section under <i>Common Output Fields Description</i> .	detail extensive
Physical info	Information about the physical interface.	detail extensive
Hold-times	Current interface hold-time up and hold-time down. Value is in milliseconds.	detail extensive
Current address	Configured MAC address.	detail extensive none
Hardware address	Media access control (MAC) address of the interface.	detail extensive none
Alternate link address	Backup link address.	detail extensive
Last flapped	Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago) . For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago) .	detail extensive none
Input packets	Number of packets received on the physical interface.	None specified
Output packets	Number of packets transmitted on the physical interface.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive
Traffic statistics	Number and rate of bytes and packets received and transmitted on the logical and physical interface. <ul style="list-style-type: none"> • Input bytes, Output bytes—Number of bytes received and transmitted on the interface. • Input packets, Output packets—Number of packets received and transmitted on the interface. 	detail extensive

Table 8: show interfaces Output Fields for M Series, MX Series, T Series, and PTX Series Routers Management Ethernet Interface (*continued*)

Field Name	Field Description	Level of Output
Input errors	<ul style="list-style-type: none"> • Errors—Input errors on the interface. • Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. • Framing errors—Number of packets received with an invalid frame checksum (FCS). • Runts—Frames received smaller than the runt threshold. • Giants—Frames received larger than the giant threshold. • Policed Discards—Frames that the incoming packet match code discarded because they were not recognized or were not of interest. Usually, this field reports protocols that Junos does not support. • Resource errors—Sum of transmit drops. 	extensive
Output errors	<ul style="list-style-type: none"> • Carrier transitions—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly, possibly once every 10 seconds, the cable, the remote system, or the interface is malfunctioning. • Errors—Sum of outgoing frame aborts and FCS errors. • Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet dropped by the ASIC RED mechanism. • Resource errors—Sum of transmit drops. 	extensive
Logical Interface		
Logical interface	Name of the logical interface	All levels
Index	Logical interface index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	Logical interface SNMP interface index number.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Flags	Information about the logical interface; values are described in the “Device Flags” section under <i>Common Output Fields Description</i> .	All levels
Encapsulation	Encapsulation on the logical interface.	detail extensive none
inet	IP address of the logical interface.	brief
Protocol	Protocol family configured on the logical interface (such as iso or inet6).	detail extensive none
MTU	MTU size on the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive

Table 8: show interfaces Output Fields for M Series, MX Series, T Series, and PTX Series Routers Management Ethernet Interface (*continued*)

Field Name	Field Description	Level of Output
Route table	Route table in which this address exists. For example, Route table:0 refers to inet.0.	detail extensive
Flags	Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Addresses, Flags	Information about address flags. Possible values are described in the “Addresses Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Destination	IP address of the remote side of the connection.	detail extensive none
Local	IP address of the logical interface.	detail extensive none
Broadcast	Broadcast address.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive

Sample Output

show interfaces brief (Management Ethernet)

```

user@host> show interfaces fxp0 brief
Physical interface: fxp0, Enabled, Physical link is Up
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
  Speed: 100mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps

Logical interface fxp0.0
  Flags: SNMP-Traps Encapsulation: ENET2
  inet  192.168.70.143/21

```

show interfaces (Management Ethernet)

```

user@host> show interfaces fxp0
Physical interface: fxp0, Enabled, Physical link is Up
  Interface index: 1, SNMP ifIndex: 1
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 100mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Half-Duplex
  Current address: 00:a0:a5:56:01:89, Hardware address: 00:a0:a5:56:01:89
  Last flapped   : Never
    Input packets : 80804
    Output packets: 1105

Logical interface fxp0.0 (Index 2) (SNMP ifIndex 13)
  Flags: SNMP-Traps Encapsulation: ENET2
  Protocol inet, MTU: 1500
    Flags: Is-Primary
    Addresses, Flags: Is-Preferred Is-Primary

```

```
Destination: 192.168.64/21, Local: 192.168.70.143,
Broadcast: 192.168.71.255
```

show interfaces (Management Ethernet [TX Matrix Plus Router])

```
user@host> show interfaces em0
Physical interface: em0, Enabled, Physical link is Up
  Interface index: 8, SNMP ifIndex: 17
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 100mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Full-Duplex
  Current address: 00:80:f9:26:00:c0, Hardware address: 00:80:f9:26:00:c0
  Last flapped   : Never
    Input packets : 1424
    Output packets: 5282

Logical interface em0.0 (Index 3) (SNMP ifIndex 18)
  Flags: SNMP-Traps Encapsulation: ENET2
  Input packets : 1424
  Output packets: 5282
  Protocol inet, MTU: 1500
    Flags: Is-Primary
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 192.168.178.0/25, Local: 192.168.178.11, Broadcast:
192.168.178.127
```

show interfaces (Management Ethernet [PTX Series Packet Transport Routers])

```
user@host> show interfaces em0
Physical interface: em0, Enabled, Physical link is Up
  Interface index: 8, SNMP ifIndex: 0
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Full-Duplex
  Current address: 00:80:f9:25:00:1b, Hardware address: 00:80:f9:25:00:1b
  Last flapped   : Never
    Input packets : 212581
    Output packets: 71

Logical interface em0.0 (Index 3) (SNMP ifIndex 0)
  Flags: SNMP-Traps Encapsulation: ENET2
  Input packets : 212551
  Output packets: 71
  Protocol inet, MTU: 1500
    Flags: Is-Primary
  Addresses, Flags: Is-Default Is-Preferred Is-Primary
    Destination: 192.168.3/24, Local: 192.168.3.30,
Broadcast: 192.168.3.255
```

show interfaces detail (Management Ethernet)

```
user@host> show interfaces fxp0 detail
Physical interface: fxp0, Enabled, Physical link is Up
  Interface index: 1, SNMP ifIndex: 1, Generation: 0
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
Speed: 100mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Half-Duplex
  Physical info   : Unspecified
```

```

Hold-times      : Up 0 ms, Down 0 ms
Current address: 00:a0:a5:56:01:89, Hardware address: 00:a0:a5:56:01:89
Alternate link address: Unspecified
Last flapped    : Never
Statistics last cleared: Never
Traffic statistics:
  Input bytes   :          6484031
  Output bytes  :          167503
  Input packets :          81008
  Output packets:          1110

Logical interface fxp0.0 (Index 2) (SNMP ifIndex 13) (Generation 1)
  Flags: SNMP-Traps Encapsulation: ENET2
  Protocol inet, MTU: 1500, Generation: 6, Route table: 0
  Flags: Is-Primary
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 192.168.64/21, Local: 192.168.70.143,
    Broadcast: 192.168.71.255, Generation: 1

```

show interfaces detail (Management Ethernet [TX Matrix Plus Router])

```

user@host> show interfaces em0 detail
Physical interface: em0, Enabled, Physical link is Up
  Interface index: 8, SNMP ifIndex: 17, Generation: 2
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
  Speed: 100mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Full-Duplex
  Physical info  : Unspecified
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 00:80:f9:26:00:c0, Hardware address: 00:80:f9:26:00:c0
  Alternate link address: Unspecified
  Last flapped   : Never
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes   :          124351
    Output bytes  :          1353212
    Input packets :          1804
    Output packets:          5344
  IPv6 transit statistics:
    Input bytes   :          0
    Output bytes  :          0
    Input packets :          0
    Output packets:          0

Logical interface em0.0 (Index 3) (SNMP ifIndex 18) (Generation 1)
  Flags: SNMP-Traps Encapsulation: ENET2
  Traffic statistics:
    Input bytes   :          117135
    Output bytes  :          1331647
    Input packets :          1804
    Output packets:          5344
  Local statistics:
    Input bytes   :          117135
    Output bytes  :          1331647
    Input packets :          1804
    Output packets:          5344
  Protocol inet, MTU: 1500, Generation: 1, Route table: 0
  Flags: Is-Primary
  Addresses, Flags: Is-Preferred Is-Primary

```

Destination: 192.168.178.0/25, Local: 192.168.178.11, Broadcast:
192.168.178.127, Generation: 1

show interfaces detail (Management Ethernet [PTX Packet Transport Routers])

```
user@host> show interfaces detail em0
Physical interface: em0, Enabled, Physical link is Up
  Interface index: 8, SNMP ifIndex: 0, Generation: 3
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,

  Speed: 1000mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Full-Duplex
  Physical info  : Unspecified
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 00:80:f9:25:00:1b, Hardware address: 00:80:f9:25:00:1b
  Alternate link address: Unspecified
  Last flapped   : Never
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes   :          15255909
    Output bytes  :           4608
    Input packets :         214753
    Output packets:           72
  IPv6 transit statistics:
    Input bytes   :           0
    Output bytes  :           0
    Input packets :           0
    Output packets:           0

  Logical interface em0.0 (Index 3) (SNMP ifIndex 0) (Generation 1)
  Flags: SNMP-Traps Encapsulation: ENET2
  Traffic statistics:
    Input bytes   :         14394630
    Output bytes  :           3024
    Input packets :         214723
    Output packets:           72
  Local statistics:
    Input bytes   :         14394630
    Output bytes  :           3024
    Input packets :         214723
    Output packets:           72
  Protocol inet, MTU: 1500, Generation: 1, Route table: 0
  Flags: Is-Primary
  Addresses, Flags: Is-Default Is-Preferred Is-Primary
    Destination: 192.168.3/24, Local: 192.168.3.30,
    Broadcast: 192.168.3.255, Generation: 1
```

show interfaces extensive (Management Ethernet)

```
user@host> show interfaces fxp0 extensive
Physical interface: fxp0, Enabled, Physical link is Up
  Interface index: 1, SNMP ifIndex: 1, Generation: 0
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
  Speed: 100mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Half-Duplex
  Physical info  : Unspecified
  Hold-times     : Up 0 ms, Down 0 ms
```

```

Current address: 00:a0:a5:56:01:89, Hardware address: 00:a0:a5:56:01:89
Alternate link address: Unspecified
Last flapped   : Never
Statistics last cleared: Never
Traffic statistics:
  Input bytes   :          6678904
  Output bytes  :          169657
  Input packets :          83946
  Output packets:          1127
Input errors:
  Errors: 12, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
  Policed discards: 0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
  Resource errors: 0

Logical interface fxp0.0 (Index 2) (SNMP ifIndex 13) (Generation 1)
Flags: SNMP-Traps Encapsulation: ENET2
Protocol inet, MTU: 1500, Generation: 6, Route table: 0
Flags: Is-Primary
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 192.168.64/21, Local: 192.168.70.143,
  Broadcast: 192.168.71.255, Generation: 1

```

show interfaces extensive (Management Ethernet [TX Matrix Plus Router])

```
user@host> show interfaces em0 extensive
```

```

Physical interface: em0, Enabled, Physical link is Up
  Interface index: 8, SNMP ifIndex: 17, Generation: 2
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
  Speed: 100mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Full-Duplex
  Physical info  : Unspecified
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 00:80:f9:26:00:c0, Hardware address: 00:80:f9:26:00:c0
  Alternate link address: Unspecified
  Last flapped   : Never
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes   :          127120
    Output bytes  :          1357414
    Input packets :          1843
    Output packets:          5372
  IPv6 transit statistics:
    Input bytes   :          0
    Output bytes  :          0
    Input packets :          0
    Output packets:          0
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
    0, Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
    0

Logical interface em0.0 (Index 3) (SNMP ifIndex 18) (Generation 1)
Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:

```

```

Input bytes : 119748
Output bytes : 1335719
Input packets: 1843
Output packets: 5372
Local statistics:
Input bytes : 119748
Output bytes : 1335719
Input packets: 1843
Output packets: 5372
Protocol inet, MTU: 1500, Generation: 1, Route table: 0
Flags: Is-Primary
Addresses, Flags: Is-Preferred Is-Primary
Destination: 192.168.178.0/25, Local: 192.168.178.11, Broadcast:
192.168.178.127, Generation: 1

```

show interfaces extensive (Management Ethernet [PTX Series Packet Transport Routers])

```

user@host> show interfaces extensive em0
Physical interface: em0, Enabled, Physical link is Up
  Interface index: 8, SNMP ifIndex: 0, Generation: 3
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,

  Speed: 1000mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Full-Duplex
  Physical info  : Unspecified
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 00:80:f9:25:00:1b, Hardware address: 00:80:f9:25:00:1b
  Alternate link address: Unspecified
  Last flapped   : Never
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes : 15236459
    Output bytes : 4608
    Input packets: 214482
    Output packets: 72
  IPv6 transit statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
    Policed discards: 0, Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
    Resource errors: 0

  Logical interface em0.0 (Index 3) (SNMP ifIndex 0) (Generation 1)
  Flags: SNMP-Traps Encapsulation: ENET2
  Traffic statistics:
    Input bytes : 14376264
    Output bytes : 3024
    Input packets: 214452
    Output packets: 72
  Local statistics:
    Input bytes : 14376264
    Output bytes : 3024
    Input packets: 214452
    Output packets: 72

```

```
Protocol inet, MTU: 1500, Generation: 1, Route table: 0
Flags: Is-Primary
Addresses, Flags: Is-Default Is-Preferred Is-Primary
  Destination: 192.168.3/24, Local: 192.168.3.30,
  Broadcast: 192.168.3.255, Generation: 1
```

show interfaces brief (Management Ethernet)

```
user@host> show interfaces fxp1 brief
Physical interface: fxp1, Enabled, Physical link is Up
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
  Speed: 100mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps

Logical interface fxp1.0
  Flags: SNMP-Traps Encapsulation: ENET2
  inet  10.0.0.4/8
  inet6 fe80::200:ff:fe00:4/64
        fec0::10:0:0:4/64
  tnp   4
```

show interfaces brief (Management Ethernet [TX Matrix Plus Router])

```
user@host> show interfaces em0 brief
Physical interface: em0, Enabled, Physical link is Up
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
  Speed: 100mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps

Logical interface em0.0
  Flags: SNMP-Traps Encapsulation: ENET2
  inet  192.168.178.11/25
```

show interfaces brief (Management Ethernet [PTX Series Packet Transport Routers])

```
user@host> show interfaces em0 brief
Physical interface: em0, Enabled, Physical link is Up
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,

  Speed: 1000mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps

  Logical interface em0.0
  Flags: SNMP-Traps Encapsulation: ENET2
  inet  192.168.3.30/24
```

```
root@absolutely> show interfaces em0 terse
Interface      Admin Link Proto  Local      Remote
em0            up    up
em0.0          up    up  inet    192.168.3.30/24
```

show interfaces (Internal Ethernet)

```
user@host> show interfaces fxp1
Physical interface: fxp1, Enabled, Physical link is Up
  Interface index: 2, SNMP ifIndex: 2
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 100mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
```

```

Link type      : Full-Duplex
Current address: 02:00:00:00:00:04, Hardware address: 02:00:00:00:00:04
Last flapped   : Never
  Input packets : 30655
  Output packets: 33323

Logical interface fxp1.0 (Index 3) (SNMP ifIndex 14)
  Flags: SNMP-Traps Encapsulation: ENET2
  Protocol inet, MTU: 1500
    Flags: Is-Primary
    Addresses, Flags: Is-Default Is-Preferred Is-Primary
      Destination: 10/8, Local: 10.0.0.4, Broadcast: 10.255.255.255
  Protocol inet6, MTU: 1500
    Flags: Is-Primary
    Addresses, Flags: Is-Preferred
      Destination: fe80::/64, Local: fe80::200:ff:fe00:4
    Addresses, Flags: Is-Default Is-Preferred Is-Primary
      Destination: fec0::/64, Local: fec0::10:0:0:4
  Protocol tnp, MTU: 1500
    Flags: Primary, Is-Primary
    Addresses
      Local: 4

```

show interfaces (Internal Ethernet [TX Matrix Plus Router])

```

user@host> show interfaces ixgbe0
Physical interface: ixgbe0, Enabled, Physical link is Up
  Interface index: 2, SNMP ifIndex: 116
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Full-Duplex
  Current address: 02:00:00:22:00:04, Hardware address: 02:00:00:22:00:04
  Last flapped   : Never
    Input packets : 2301738
    Output packets: 3951155

Logical interface ixgbe0.0 (Index 4) (SNMP ifIndex 117)
  Flags: SNMP-Traps Encapsulation: ENET2
  Input packets : 2301595
  Output packets: 3951155
  Protocol inet, MTU: 1500
    Flags: Is-Primary
    Addresses, Flags: Is-Preferred
      Destination: 10/8, Local: 10.34.0.4, Broadcast: 10.255.255.255
    Addresses, Flags: Primary Is-Default Is-Preferred Is-Primary
      Destination: 128/2, Local: 162.0.0.4, Broadcast: 191.255.255.255
  Protocol inet6, MTU: 1500
    Flags: Is-Primary
    Addresses, Flags: Is-Preferred
      Destination: fe80::/64, Local: fe80::200:ff:fe22:4
    Addresses, Flags: Is-Default Is-Preferred Is-Primary
      Destination: fec0::/64, Local: fec0::a:22:0:4
  Protocol tnp, MTU: 1500
    Flags: Primary, Is-Primary
    Addresses
      Local: 0x22000004

```

show interfaces detail (Internal Ethernet)

```

user@host> show interfaces fxp1 detail

```

```

Physical interface: fxp1, Enabled, Physical link is Up
Interface index: 2, SNMP ifIndex: 2, Generation: 1
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
Speed: 100mbps
Device flags : Present Running
Interface flags: SNMP-Traps
Link type : Full-Duplex
Physical info : Unspecified
Hold-times : Up 0 ms, Down 0 ms
Current address: 02:00:00:00:00:04, Hardware address: 02:00:00:00:00:04
Alternate link address: Unspecified
Last flapped : Never
Statistics last cleared: Never
Traffic statistics:
Input bytes : 2339969
Output bytes : 15880707
Input packets: 30758
Output packets: 33443

Logical interface fxp1.0 (Index 3) (SNMP ifIndex 14) (Generation 2)
Flags: SNMP-Traps Encapsulation: ENET2
Protocol inet, MTU: 1500, Generation: 7, Route table: 1
Flags: Is-Primary
Addresses, Flags: Is-Default Is-Preferred Is-Primary
Destination: 10/8, Local: 10.0.0.4, Broadcast: 10.255.255.255,
Generation: 3
Protocol inet6, MTU: 1500, Generation: 8, Route table: 1
Flags: Is-Primary
Addresses, Flags: Is-Preferred
Destination: fe80::/64, Local: fe80::200:ff:fe00:4,
Broadcast: Unspecified, Generation: 5
Addresses, Flags: Is-Default Is-Preferred Is-Primary
Destination: fec0::/64, Local: fec0::10:0:0:4, Broadcast: Unspecified,
Generation: 7
Protocol tnp, MTU: 1500, Generation: 9, Route table: 1
Flags: Primary, Is-Primary
Addresses, Flags: None
Destination: Unspecified, Local: 4, Broadcast: Unspecified,
Generation: 8

```

show interfaces detail (Internal Ethernet [TX Matrix Plus Router])

```

user@host> show interfaces ixgbe0 detail
Physical interface: ixgbe0, Enabled, Physical link is Up
Interface index: 2, SNMP ifIndex: 116, Generation: 3
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
Speed: 1000mbps
Device flags : Present Running
Interface flags: SNMP-Traps
Link type : Full-Duplex
Physical info : Unspecified
Hold-times : Up 0 ms, Down 0 ms
Current address: 02:00:00:22:00:04, Hardware address: 02:00:00:22:00:04
Alternate link address: Unspecified
Last flapped : Never
Statistics last cleared: Never
Traffic statistics:
Input bytes : 238172825
Output bytes : 1338948955
Input packets: 2360984
Output packets: 4061512

```

```

IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Logical interface ixgbe0.0 (Index 4) (SNMP ifIndex 117) (Generation 2)
Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:
Input bytes : 228720309
Output bytes : 1261387447
Input packets: 2360841
Output packets: 4061512
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 228720309
Output bytes : 1261387447
Input packets: 2360841
Output packets: 4061512
Protocol inet, MTU: 1500, Generation: 2, Route table: 1
Flags: Is-Primary
Addresses, Flags: Is-Preferred
Destination: 10/8, Local: 10.34.0.4, Broadcast: 10.255.255.255, Generation:
2
Addresses, Flags: Primary Is-Default Is-Preferred Is-Primary
Destination: 128/2, Local: 162.0.0.4, Broadcast: 191.255.255.255,
Generation: 3
Protocol inet6, MTU: 1500, Generation: 3, Route table: 1
Flags: Is-Primary
Addresses, Flags: Is-Preferred
Destination: fe80::/64, Local: fe80::200:ff:fe22:4
Generation: 4
Addresses, Flags: Is-Default Is-Preferred Is-Primary
Destination: fec0::/64, Local: fec0::a:22:0:4
Protocol tnp, MTU: 1500, Generation: 5
Generation: 4, Route table: 1
Flags: Primary, Is-Primary
Addresses, Flags: None
Destination: Unspecified, Local: 0x22000004, Broadcast: Unspecified,
Generation: 6

```

show interfaces extensive (internal Ethernet)

```

user@host> show interfaces fxp1 extensive
Physical interface: fxp1, Enabled, Physical link is Up
Interface index: 2, SNMP ifIndex: 2, Generation: 1
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
Speed: 100mbps
Device flags : Present Running
Interface flags: SNMP-Traps
Link type : Full-Duplex
Physical info : Unspecified
Hold-times : Up 0 ms, Down 0 ms
Current address: 02:00:00:00:00:04, Hardware address: 02:00:00:00:00:04
Alternate link address: Unspecified
Last flapped : Never
Statistics last cleared: Never

```

```

Traffic statistics:
Input bytes :          2349897
Output bytes :        15888605
Input packets:         30896
Output packets:        33607
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
Policed discards: 0, Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
Resource errors: 0

Logical interface fxp1.0 (Index 3) (SNMP ifIndex 14) (Generation 2)
Flags: SNMP-Traps Encapsulation: ENET2
Protocol inet, MTU: 1500, Generation: 7, Route table: 1
Flags: Is-Primary
Addresses, Flags: Is-Default Is-Preferred Is-Primary
Destination: 10/8, Local: 10.0.0.4, Broadcast: 10.255.255.255,
Generation: 3
Protocol inet6, MTU: 1500, Generation: 8, Route table: 1
Flags: Is-Primary
Addresses, Flags: Is-Preferred
Destination: fe80::/64, Local: fe80::200:ff:fe00:4,
Broadcast: Unspecified, Generation: 5
Addresses, Flags: Is-Default Is-Preferred Is-Primary
Destination: fec0::/64, Local: fec0::10:0:0:4, Broadcast: Unspecified,
Generation: 7
Protocol tnp, MTU: 1500, Generation: 9, Route table: 1
Flags: Primary, Is-Primary
Addresses, Flags: None
Destination: Unspecified, Local: 4, Broadcast: Unspecified,
Generation: 8

```

show interfaces extensive (internal Ethernet [TX Matrix Plus Router])

```

user@host> show interfaces ixgbe0 extensive
Physical interface: ixgbe0, Enabled, Physical link is Up
Interface index: 2, SNMP ifIndex: 116, Generation: 3
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
Speed: 1000mbps
Device flags : Present Running
Interface flags: SNMP-Traps
Link type : Full-Duplex
Physical info : Unspecified
Hold-times : Up 0 ms, Down 0 ms
Current address: 02:00:00:22:00:04, Hardware address: 02:00:00:22:00:04
Alternate link address: Unspecified
Last flapped : Never
Statistics last cleared: Never
Traffic statistics:
Input bytes :          242730780
Output bytes :        1348312269
Input packets:         2398737
Output packets:        4133510
IPv6 transit statistics:
Input bytes :          0
Output bytes :          0
Input packets:          0
Output packets:         0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:

```

```

0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0


```

```

Logical interface ixgbe0.0 (Index 4) (SNMP ifIndex 117) (Generation 2)
  Flags: SNMP-Traps Encapsulation: ENET2
  Traffic statistics:
    Input bytes :          233127252
    Output bytes :         1269350897
    Input packets:         2398594
    Output packets:        4133510
  IPv6 transit statistics:
    Input bytes :          0
    Output bytes :          0
    Input packets:         0
    Output packets:        0
  Local statistics:
    Input bytes :          233127252
    Output bytes :         1269350897
    Input packets:         2398594
    Output packets:        4133510
  Protocol inet, MTU: 1500, Generation: 2, Route table: 1
    Flags: Is-Primary
    Addresses, Flags: Is-Preferred
      Destination: 10/8, Local: 10.34.0.4, Broadcast: 10.255.255.255, Generation:
2
      Addresses, Flags: Primary Is-Default Is-Preferred Is-Primary
        Destination: 128/2, Local: 162.0.0.4, Broadcast: 191.255.255.255,
Generation: 3
    Protocol inet6, MTU: 1500, Generation: 3, Route table: 1
      Flags: Is-Primary
      Addresses, Flags: Is-Preferred
        Destination: fe80::/64, Local: fe80::200:ff:fe22:4
Generation: 4
      Addresses, Flags: Is-Default Is-Preferred Is-Primary
        Destination: fec0::/64, Local: fec0::a:22:0:4
    Protocol tnp, MTU: 1500, Generation: 5
    Generation: 4, Route table: 1
      Flags: Primary, Is-Primary
      Addresses, Flags: None
        Destination: Unspecified, Local: 0x22000004, Broadcast: Unspecified,
Generation: 6

```

show interfaces statistics

Syntax	<code>show interfaces statistics <i>interface-name</i> <detail></code>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 12.1 for PTX Series Packet Transport Switches.</p> <p>Command introduced in Junos OS Release 12.2 for ACX Series Routers.</p>
Description	Display static interface statistics, such as errors.
	<div>  <p>NOTE: When the <code>show interfaces statistics</code> command is executed on an interface that is configured on T4000 Type 5 FPC, the <i>IPv6 transit statistics</i> field displays:</p> <ul style="list-style-type: none"> • Total statistics (sum of transit and local statistics) at the physical interface level • Transit statistics at the logical interface level </div>
Options	<p><i>interface-name</i>—Name of an interface.</p> <p><i>detail</i>—(Optional) Display detail output.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>clear interfaces statistics</i>
List of Sample Output	<p>show interfaces statistics (Fast Ethernet) on page 233</p> <p>show interfaces statistics (Gigabit Ethernet PIC—Egress) on page 233</p> <p>show interfaces statistics detail (Aggregated Ethernet) on page 235</p> <p>show interfaces statistics detail (Aggregated Ethernet—Ingress) on page 236</p> <p>show interfaces statistics detail (Aggregated Ethernet—Egress) on page 237</p> <p>show interfaces statistics (SONET/SDH) on page 239</p> <p>show interfaces statistics (Aggregated SONET/SDH—Ingress) on page 240</p> <p>show interfaces statistics (Aggregated SONET/SDH—Egress) on page 241</p> <p>show interfaces statistics (PTX Series Packet Transport Switches) on page 242</p> <p>show interfaces statistics (ACX Series routers) on page 242</p>
Output Fields	<p>Output from both the <code>show interfaces <i>interface-name</i> detail</code> and the <code>show interfaces <i>interface-name</i> extensive</code> commands include all the information displayed in the output from the <code>show interfaces statistics</code> command. For more information, see the particular interface type in which you are interested. For information about destination class and source class statistics, see the “Destination Class Field” section and the “Source Class Field” section under <i>Common Output Fields Description</i>. For information about the input errors and output errors, see <i>Fast Ethernet and Gigabit Ethernet Counters</i>.</p>

Sample Output

show interfaces statistics (Fast Ethernet)

```

user@host> show interfaces fe-1/3/1 statistics
Physical interface: fe-1/3/1, Enabled, Physical link is Up
  Interface index: 144, SNMP ifIndex: 1042
  Description: ford fe-1/3/1
  Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  CoS queues     : 4 supported, 4 maximum usable queues
  Current address: 00:90:69:93:04:dc, Hardware address: 00:90:69:93:04:dc
  Last flapped   : 2006-04-18 03:08:59 PDT (00:01:24 ago)
  Statistics last cleared: Never
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Input errors: 0, Output errors: 0
  Active alarms  : None
  Active defects : None
Logical interface fe-1/3/1.0 (Index 69) (SNMP ifIndex 50)
  Flags: SNMP-Traps Encapsulation: ENET2
  Protocol inet, MTU: 1500
    Flags: Is-Primary, DCU, SCU-in

      Destination class      Packets          Bytes
                        (packet-per-second)  (bits-per-second)
      silver1                0                0
      (                      0) (                0)
      silver2                0                0
      (                      0) (                0)
      silver3                0                0
      (                      0) (                0)
  Addresses, Flags: Is-Default Is-Preferred Is-Primary
    Destination: 10.27.245/24, Local: 10.27.245.2,
    Broadcast: 10.27.245.255
  Protocol iso, MTU: 1497
    Flags: Is-Primary

```

show interfaces statistics (Gigabit Ethernet PIC—Egress)

```

user@host> show interfaces ge-5/2/0 statistics detail
Physical interface: ge-5/2/0, Enabled, Physical link is Up
  Interface index: 146, SNMP ifIndex: 519, Generation: 149
  Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps, BPDU Error: None,
  MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 00:1d:b5:61:d9:74, Hardware address: 00:1d:b5:61:d9:74
  Last flapped   : 2009-11-11 11:24:00 PST (09:23:08 ago)
  Statistics last cleared: 2009-11-11 17:50:58 PST (02:56:10 ago)
  Traffic statistics:
    Input bytes :          271524          0 bps
    Output bytes :        37769598        352 bps
    Input packets:           3664          0 pps
    Output packets:        885790          0 pps

```

```

IPv6 transit statistics:
Input bytes : 0
Output bytes : 16681118
Input packets: 0
Output packets: 362633
Multicast statistics:
IPv4 multicast statistics:
Input bytes : 112048 0 bps
Output bytes : 20779920 0 bps
Input packets: 1801 0 pps
Output packets: 519498 0 pps
IPv6 multicast statistics:
Input bytes : 156500 0 bps
Output bytes : 16681118 0 bps
Input packets: 1818 0 pps
Output packets: 362633 0 pps
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3
incompletes: 0, L2 channel errors: 0,
L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0,
Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

0 best-effort      882558      882558      0

1 expedited-fo      0      0      0

2 assured-forw      0      0      0

3 network-cont      3232      3232      0

Active alarms : None
Active defects : None

Logical interface ge-5/2/0.0 (Index 71) (SNMP ifIndex 573) (Generation 135)
Flags: SNMP-Traps 0x4000 Encapsulation: ENET2
Egress accounting overhead: 100
Ingress accounting overhead: 90
Traffic statistics:
Input bytes : 271524
Output bytes : 37769598
Input packets: 3664
Output packets: 885790
IPv6 transit statistics:
Input bytes : 0
Output bytes : 16681118
Input packets: 0
Output packets: 362633
Local statistics:
Input bytes : 271524
Output bytes : 308560
Input packets: 3664
Output packets: 3659
Transit statistics:
Input bytes : 0 0 bps
Output bytes : 37461038 0 bps
Input packets: 0 0 pps

```

```

Output packets:          882131          0 pps
IPv6 transit statistics:
  Input bytes :           0
  Output bytes :        16681118
  Input packets:          0
  Output packets:       362633
Multicast statistics:
IPv4 multicast statistics:
  Input bytes :        112048          0 bps
  Output bytes :       20779920          0 bps
  Input packets:        1801          0 pps
  Output packets:       519498          0 pps
IPv6 multicast statistics:
  Input bytes :        156500          0 bps
  Output bytes :       16681118          0 bps
  Input packets:        1818          0 pps
  Output packets:       362633          0 pps
Protocol inet, MTU: 1500, Generation: 151, Route table: 0
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 40.40.40.0/30, Local: 40.40.40.2, Broadcast: 40.40.40.3,
Generation: 167
Protocol inet6, MTU: 1500, Generation: 152, Route table: 0
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: ::40.40.40.0/126, Local: ::40.40.40.2
Generation: 169
  Addresses, Flags: Is-Preferred
    Destination: fe80::/64, Local: fe80::21d:b5ff:fe61:d974
Protocol multiservice, MTU: Unlimited, Generation: 171
Generation: 153, Route table: 0
  Policer: Input: __default_arp_policer__

```

show interfaces statistics detail (Aggregated Ethernet)

```

user@host> show interfaces ae0 detail
Physical interface: ae0, Enabled, Physical link is Up
  Interface index: 186, SNMP ifIndex: 111, Generation: 187
  Link-level type: Ethernet, MTU: 1514, Speed: 2000mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Disabled, Minimum links needed: 1,
  Minimum bandwidth needed: 0
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Current address: 00:90:69:0b:2f:f0, Hardware address: 00:90:69:0b:2f:f0
  Last flapped   : Never
  Statistics last cleared: 2006-12-23 03:04:16 PST (01:16:24 ago)
Traffic statistics:
  Input bytes :          28544          0 bps
  Output bytes :         39770          0 bps
  Input packets:           508          0 pps
  Output packets:          509          0 pps
  Input bytes :         IPv6 28544
  Output bytes :         IPv6 0
  Input packets:         IPv6 508
  Output packets:         IPv6 0
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
  Policed discards: 0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
  Resource errors: 0

```

```

Logical interface ae0.0 (Index 67) (SNMP ifIndex 139) (Generation 145)
Flags: SNMP-Traps Encapsulation: ENET2
Statistics          Packets          pps          Bytes          bps
Bundle:
  Input :           508             0          28544           0
  Output:           509             0          35698           0
Link:
  ge-3/3/8.0
    Input :           508             0          28544           0
    Output:            0             0            0           0
  ge-3/3/9.0
    Input :            0             0            0           0
    Output:            0             0            0           0
Marker Statistics:  Marker Rx      Resp Tx    Unknown Rx    Illegal Rx
  ge-3/3/8.0           0          0          0           0
  ge-3/3/9.0           0          0          0           0
Egress queues: 8 supported, 8 in use
Queue counters:      Queued packets  Transmitted packets  Dropped packets

  0 best-effort              0              0              0
  1 expedited-fo             0              0              0
  2 assured-forw             0              0              0
  3 network-cont             0              0              0

Protocol inet, MTU: 1500, Generation: 166, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 10.1.1/24, Local: 10.1.1.1, Broadcast: 10.1.1.255,
  Generation: 159
Protocol inet6, MTU: 1500, Generation: 163, Route table: 0
Flags: Is-Primary
Addresses, Flags: Is-Preferred
  Destination: fe80::/64, Local: fe80::206:5bff:fe05:c321,
  Broadcast: Unspecified, Generation: 161

```

show interfaces statistics detail (Aggregated Ethernet—Ingress)

```

user@host> show interfaces statistics detail ae0 | no-more
Physical interface: ae0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 504, Generation: 278
Link-level type: Ethernet, MTU: 1514, Speed: 1Gbps, BPDU Error: None, MAC-REWRITE
Error: None, Loopback: Disabled,
Source filtering: Disabled, Flow control: Disabled, Minimum links needed: 1,
Minimum bandwidth needed: 0
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Current address: 00:1d:b5:61:db:f0, Hardware address: 00:1d:b5:61:db:f0
Last flapped   : 2009-11-09 03:30:23 PST (00:01:28 ago)
Statistics last cleared: 2009-11-09 03:26:18 PST (00:05:33 ago)
Traffic statistics:
  Input bytes :           544009602          54761856 bps
  Output bytes :             3396             0 bps
  Input packets:          11826292          148809 pps
  Output packets:              42             0 pps
IPv6 transit statistics:
  Input bytes :          350818604
  Output bytes :              0
  Input packets:          7626488

```

```

    Output packets:                                0
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0
Ingress queues: 8 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

  0 best-effort              0              0              0
  1 expedited-fo             0              0              0
  2 assured-forw             0              0              0
  3 network-cont             0              0              0

Egress queues: 8 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

  0 best-effort             21              21              0
  1 expedited-fo             0              0              0
  2 assured-forw             0              0              0
  3 network-cont            451              451              0

Logical interface ae0.0 (Index 70) (SNMP ifIndex 574) (Generation 177)
Flags: SNMP-Traps 0x4000 Encapsulation: ENET2
Statistics      Packets      pps      Bytes      bps
Bundle:
  Input :      11826292      148809      544009602      54761856
  Output:         42         0         3396         0
Link:
  ge-5/2/0.0
  Input :      11826292      148809      544009602      54761856
  Output:         42         0         3396         0
Marker Statistics:  Marker Rx      Resp Tx      Unknown Rx      Illegal Rx
ge-5/2/0.0              0              0              0              0
Protocol inet, MTU: 1500, Generation: 236, Route table: 0
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 30.30.30.0/30, Local: 30.30.30.2, Broadcast: 30.30.30.3,
Generation: 310
  Protocol inet6, MTU: 1500, Generation: 237, Route table: 0
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: ::30.30.30.0/126, Local: ::30.30.30.2
Generation: 312
    Addresses, Flags: Is-Preferred
      Destination: fe80::/64, Local: fe80::21d:b5ff:fe61:dbf0
Protocol multiservice, MTU: Unlimited, Generation: 314
Generation: 238, Route table: 0
  Policer: Input: __default_arp_policer__

```

show interfaces statistics detail (Aggregated Ethernet—Egress)

```

user@host> show interfaces statistics detail ae0 | no-more
Physical interface: ae0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 501, Generation: 319

```

```

Link-level type: Ethernet, MTU: 1514, Speed: 1Gbps, BPDU Error: None, MAC-REWRITE
Error: None, Loopback: Disabled,
Source filtering: Disabled, Flow control: Disabled, Minimum links needed: 1,
Minimum bandwidth needed: 0
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Current address: 00:1f:12:c2:37:f0, Hardware address: 00:1f:12:c2:37:f0
Last flapped : 2009-11-09 03:30:24 PST (00:02:42 ago)
Statistics last cleared: 2009-11-09 03:26:42 PST (00:06:24 ago)
Traffic statistics:
Input bytes :                440                0 bps
Output bytes :            1047338120            54635848 bps
Input packets:                7                0 pps
Output packets:          22768200            148466 pps
IPv6 transit statistics:
Input bytes :                288
Output bytes :            723202616
Input packets:                4
Output packets:          15721796
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
0, Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0
Ingress queues: 8 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

0 best-effort                0                0                0
1 expedited-fo                0                0                0
2 assured-forw                0                0                0
3 network-cont                0                0                0

Egress queues: 8 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

0 best-effort          201985796          201985796                0
1 expedited-fo                0                0                0
2 assured-forw                0                0                0
3 network-cont           65                65                0

Logical interface ae0.0 (Index 72) (SNMP ifIndex 505) (Generation 204)
Flags: SNMP-Traps 0x4000 Encapsulation: ENET2
Statistics      Packets      pps      Bytes      bps
Bundle:
Input :          7          0          440          0
Output:        22768200      148466      1047338120      54635848
Link:
ge-2/1/6.0
Input :          7          0          440          0
Output:        22768200      148466      1047338120      54635848
Marker Statistics: Marker Rx      Resp Tx      Unknown Rx      Illegal Rx
ge-2/1/6.0          0          0          0          0
Protocol inet, MTU: 1500, Generation: 291, Route table: 0

```

```

    Addresses, Flags: Is-Preferred Is-Primary
    Destination: 30.30.30.0/30, Local: 30.30.30.1, Broadcast: 30.30.30.3,
Generation: 420
    Protocol inet6, MTU: 1500, Generation: 292, Route table: 0
    Addresses, Flags: Is-Preferred Is-Primary
    Destination: ::/26, Local: ::30.30.30.1
Generation: 422
    Addresses, Flags: Is-Preferred
    Destination: fe80::/64, Local: fe80::21f:12ff:fec2:37f0
    Protocol multiservice, MTU: Unlimited, Generation: 424
    Generation: 293, Route table: 0
    Policer: Input: __default_arp_policer__

```

show interfaces statistics (SONET/SDH)

```

user@host> show interfaces statistics detail so-3/0/0 | no-more
Physical interface: so-3/0/0, Enabled, Physical link is Up
Interface index: 133, SNMP ifIndex: 538, Generation: 283
Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC192,
Loopback: None, FCS: 16, Payload scrambler: Enabled
Device flags   : Present Running
Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
Link flags     : Keepalives
Hold-times     : Up 0 ms, Down 0 ms
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive statistics:
  Input : 13 (last seen 00:00:04 ago)
  Output: 14 (last sent 00:00:02 ago)
LCP state: Opened
NCP state: inet: Opened, inet6: Opened, iso: Not-configured, mpls: Not-configured

CHAP state: Closed
PAP state: Closed
CoS queues   : 8 supported, 8 maximum usable queues
Last flapped : 2009-11-09 02:52:34 PST (01:12:39 ago)
Statistics last cleared: 2009-11-09 03:58:54 PST (00:06:19 ago)
Traffic statistics:
Input bytes   :          2559160294          54761720 bps
Output bytes  :           10640          48 bps
Input packets:          55633975          148809 pps
Output packets:           216           0 pps
IPv6 transit statistics:
Input bytes   :          647922328
Output bytes  :           0
Input packets:          14085269
Output packets:           0
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Bucket drops:
0, Policed discards: 0, L3 incompletes: 0,
  L2 channel errors: 0, L2 mismatch timeouts: 0, HS link CRC errors: 0, HS link
FIFO overflows: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, Aged packets: 0, HS link FIFO
underflows: 0, MTU errors: 0
Egress queues: 8 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

  0 best-effort          4              4              0

  1 expedited-fo         0              0              0

```

```

2 assured-forw          0          0          0
3 network-cont          213        213          0

SONET alarms   : None
SONET defects  : None

Logical interface so-3/0/0.0 (Index 72) (SNMP ifIndex 578) (Generation 182)
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
  Protocol inet, MTU: 4470, Generation: 244, Route table: 0
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 30.30.30.0/30, Local: 30.30.30.2, Broadcast: 30.30.30.3,
Generation: 322
    Protocol inet6, MTU: 4470, Generation: 245, Route table: 0
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: ::30.30.30.0/126, Local: ::30.30.30.2
Generation: 324
      Addresses, Flags: Is-Preferred
        Destination: fe80::/64, Local: fe80::2a0:a5ff:fe61:9264
Generation: 326

```

show interfaces statistics (Aggregated SONET/SDH—Ingress)

```

user@host> show interfaces statistics detail as0 | no-more
Physical interface: as0, Enabled, Physical link is Up
  Interface index: 132, SNMP ifIndex: 534, Generation: 282
  Link-level type: PPP, MTU: 4474, Speed: OC192, Minimum links needed: 1, Minimum
bandwidth needed: 0
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : Keepalives
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Last flapped   : 2009-11-09 03:45:53 PST (00:09:38 ago)
  Statistics last cleared: 2009-11-09 03:48:17 PST (00:07:14 ago)
  Traffic statistics:
    Input bytes :          2969786332          54761688 bps
    Output bytes :           11601           0 bps
    Input packets:          64560636          148808 pps
    Output packets:           225           0 pps
  IPv6 transit statistics:
    Input bytes :          2086013152
    Output bytes :              0
    Input packets:          45348114
    Output packets:              0
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
0, Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0
  Egress queues: 8 supported, 4 in use
  Queue counters:
    Queued packets  Transmitted packets  Dropped packets

0 best-effort          3              3              0
1 expedited-fo         0              0              0
2 assured-forw         0              0              0
3 network-cont        222            222              0

```

```

Logical interface as0.0 (Index 71) (SNMP ifIndex 576) (Generation 179)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
Statistics          Packets          pps          Bytes          bps
Bundle:
  Input :          64560550          148808          2969785300          54761688
  Output:           139           0           10344           0
Link:
  so-3/0/0.0
  Input :          64560550          148808          2969785300          54761688
  Output:           139           0           10344           0
Protocol inet, MTU: 4470, Generation: 240, Route table: 0
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 30.30.30.0/30, Local: 30.30.30.2, Broadcast: 30.30.30.3,
Generation: 316
Protocol inet6, MTU: 4470, Generation: 241, Route table: 0
Addresses, Flags: Is-Preferred Is-Primary
  Destination: ::30.30.30.0/126, Local: ::30.30.30.2
Generation: 318
Addresses, Flags: Is-Preferred
  Destination: fe80::/64, Local: fe80::2a0:a5ff:fe61:9264
Generation: 320

```

show interfaces statistics (Aggregated SONET/SDH—Egress)

```

user@host> show interfaces statistics detail as0 | no-more
Physical interface: as0, Enabled, Physical link is Up
Interface index: 132, SNMP ifIndex: 565, Generation: 323
Link-level type: PPP, MTU: 4474, Speed: OC192, Minimum links needed: 1, Minimum
bandwidth needed: 0
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags     : Keepalives
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Last flapped   : 2009-11-09 03:43:37 PST (00:12:48 ago)
Statistics last cleared: 2009-11-09 03:48:54 PST (00:07:31 ago)
Traffic statistics:
Input bytes :          11198          392 bps
Output bytes :        3101452132        54783448 bps
Input packets:           234           0 pps
Output packets:        67422937        148868 pps
IPv6 transit statistics:
Input bytes :          5780
Output bytes :        2171015678
Input packets:           72
Output packets:        47195993
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
0, Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0
Egress queues: 8 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

0 best-effort          67422830          67422830          0

1 expedited-fo           0           0          0

2 assured-forw           0           0          0

```

3 network-cont	90	90	0
----------------	----	----	---

```

Logical interface as0.0 (Index 71) (SNMP ifIndex 548) (Generation 206)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
Statistics          Packets          pps          Bytes          bps
Bundle:
  Input :           144             0          10118          392
  Output:        67422847        148868      3101450962      54783448
Link:
  so-0/1/0.0
    Input :           144             0          10118          392
    Output:        67422847        148868      3101450962      54783448
Protocol inet, MTU: 4470, Generation: 295, Route table: 0
Addresses, Flags: Is-Preferred Is-Primary
Destination: 30.30.30.0/30, Local: 30.30.30.1, Broadcast: 30.30.30.3,
Generation: 426
Protocol inet6, MTU: 4470, Generation: 296, Route table: 0
Addresses, Flags: Is-Preferred Is-Primary
Destination: ::/26, Local: ::30.30.30.1
Generation: 428
Addresses, Flags: Is-Preferred
Destination: fe80::/64, Local: fe80::2a0:a5ff:fe63:1d0a
Generation: 429

```

show interfaces statistics (PTX Series Packet Transport Switches)

```

user@host> show interfaces statistics em0
Physical interface: em0, Enabled, Physical link is Up
  Interface index: 8, SNMP ifIndex: 0
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Full-Duplex
  Current address: 00:80:f9:25:00:1b, Hardware address: 00:80:f9:25:00:1b
  Last flapped   : Never
  Statistics last cleared: Never
Input packets : 212620
Output packets: 71
  Input errors: 0, Output errors: 0

  Logical interface em0.0 (Index 3) (SNMP ifIndex 0)
Flags: SNMP-Traps Encapsulation: ENET2
Input packets : 212590
Output packets: 71
Protocol inet, MTU: 1500
Flags: Is-Primary
Addresses, Flags: Is-Default Is-Preferred Is-Primary
Destination: 192.168.3/24, Local: 192.168.3.30,
Broadcast: 192.168.3.255

```

show interfaces statistics (ACX Series routers)

```

user@host> show interfaces statistics ge-0/1/7
Physical interface: ge-0/1/7, Enabled, Physical link is Down
  Interface index: 151, SNMP ifIndex: 524
  Link-level type: Ethernet, Media type: Copper, MTU: 1514, Link-mode: Full-duplex,
  Speed: 1000mbps, BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,

  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online

```

```
Device flags   : Present Running Down
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Link flags     : None
CoS queues     : 8 supported, 8 maximum usable queues
Current address: 84:18:88:c1:49:a3, Hardware address: 84:18:88:c1:49:a3
Last flapped   : 2012-05-11 04:25:28 PDT (2d 20:23 ago)
Statistics last cleared: 2012-05-13 23:07:23 PDT (01:41:25 ago)
Input rate     : 0 bps (0 pps)
Output rate    : 0 bps (0 pps)
Input errors: 0, Output errors: 0
Active alarms  : LINK
Active defects : LINK
Interface transmit statistics: Disabled
```

show passive-monitoring error

Syntax	<code>show passive-monitoring error (* all mo-fpc/pic/port)</code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M40e, M160, and M320 routers and T Series routers only) Display passive monitoring error statistics.
Options	<code>* all mo-fpc/pic/port</code> —Display error statistics for monitoring interfaces. Use a wildcard character, specify all interfaces, or provide a specific interface name.
Required Privilege Level	view
List of Sample Output	show passive-monitoring error all on page 245
Output Fields	Table 9 on page 244 lists the output fields for the <code>show passive-monitoring error</code> command. Output fields are listed in the approximate order in which they appear.

Table 9: show passive-monitoring error Output Fields

Field Name	Field Description
Passive monitoring interface	Name of the passive monitoring interface.
Local interface index	Index counter of the local interface.
Interface state	State of the passive monitoring interface: <ul style="list-style-type: none"> • Monitoring—Specified interface is actively monitoring. • Disabled—Specified interface has been disabled from the CLI. • Not monitoring—The interface is operational, but not monitoring. This condition occurs when an interface first comes online, or when the interface is operational, but no logical unit has been configured under the physical interface. • Unknown—Unknown state. • Error—An error occurred during the process of determining the state of the interface.
Error information	
Packets dropped (no memory)	Number of packets dropped because of memory shortage.
Packets dropped (not IP)	Number of non-IP packets dropped.
Packets dropped (not IPv4)	Number of packets dropped because they failed the IPv4 version check.
Packets dropped (header too small)	Number of packets dropped because the packet length or IP header length was too small.

Table 9: show passive-monitoring error Output Fields (*continued*)

Field Name	Field Description
Memory allocation failures	Number of flow record memory allocation failures. A small number reflects failures to replenish the free list. A large number indicates the monitoring station is almost out of memory space.
Memory free failures	Number of flow record memory free failures.
Memory free list failures	Number of flow records received from free list that failed. Memory is nearly exhausted or too many new flows greater than 128 KB are being created per second.
Memory warning	Whether the flows have exceeded 1 million packets per second (Mpps) on a Monitoring Services PIC or 2 Mpps on a Monitoring Services II PIC. The response can be Yes or No .
Memory overload	Whether the memory has been overloaded. The response can be Yes or No .
PPS overload	Whether the PIC is receiving more packets per second than the configured threshold. The response can be Yes or No .
BPS overload	Whether the PIC is receiving more bits per second than the configured threshold. The response can be Yes or No .

Sample Output

show passive-monitoring error all

```

user@host> show passive-monitoring error all
Passive monitoring interface: mo-4/0/0, Local interface index: 44
Interface state: Monitoring
Error information
  Packets dropped (no memory): 0, Packets dropped (not IP): 0
  Packets dropped (not IPv4): 0, Packets dropped (header too small): 0
  Memory allocation failures: 0, Memory free failures: 0
  Memory free list failures: 0
  Memory warning: No, Memory overload: No, PPS overload: No, BPS overload: No

Passive monitoring interface: mo-4/1/0, Local interface index: 45
Interface state: Not monitoring
Error information
  Packets dropped (no memory): 0, Packets dropped (not IP): 0
  Packets dropped (not IPv4): 0, Packets dropped (header too small): 0
  Memory allocation failures: 0, Memory free failures: 0
  Memory free list failures: 0
  Memory warning: No, Memory overload: No, PPS overload: No, BPS overload: No

```

show passive-monitoring flow

Syntax	<code>show passive-monitoring flow (* all mo-fpc/pic/port)</code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M40e, M160, and M320 routers and T Series routers only) Display passive flow statistics.
Options	<code>* all mo-fpc/pic/port</code> —Display passive flow statistics for monitoring interfaces. Use a wildcard character, specify all interfaces, or provide a specific interface name.
Required Privilege Level	view
List of Sample Output	show passive-monitoring flow all on page 247
Output Fields	Table 10 on page 246 lists the output fields for the <code>show passive-monitoring flow</code> command. Output fields are listed in the approximate order in which they appear.

Table 10: show passive-monitoring flow Output Fields

Field Name	Field Description
Passive monitoring interface	Name of the passive monitoring interface.
Local interface index	Index counter of the local interface.
Interface state	State of the passive monitoring interface: <ul style="list-style-type: none"> • Monitoring—Specified interface is actively monitoring. • Disabled—Specified interface has been disabled from the CLI. • Not monitoring—The interface is operational, but not monitoring. This condition occurs when an interface first comes online, or when the interface is operational, but no logical unit has been configured under the physical interface. • Unknown—Unknown state. • Error—An error occurred during the process of determining the state of the interface.
Flow information	
Flow packets	Number of packets received by an operational PIC.
Flow bytes	Number of bytes received by an operational PIC.
Flow packets 10-second rate	Number of packets per second handled by the PIC and displayed as a 10-second average.
Flow bytes 10-second rate	Number of bytes per second handled by the PIC and displayed as a 10-second average.
Active flows	Number of currently active flows tracked by the PIC.
Total flows	Total number of flows received by an operational PIC.

Table 10: show passive-monitoring flow Output Fields (*continued*)

Field Name	Field Description
Flows exported	Total number of flows exported by an operational PIC.
Flows packets exported	Total number of cflowd packets exported by an operational PIC.
Flows inactive timed out	Total number of flows that are exported because of inactivity.
Flows active timed out	Total number of long-lived flows that are exported because of an active timeout.

Sample Output

show passive-monitoring flow all

```

user@host> show passive-monitoring flow all
Passive monitoring interface: mo-4/0/0, Local interface index: 44
Interface state: Monitoring
Flow information
  Flow packets: 6533434, Flow bytes: 653343400
  Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
  Active flows: 0, Total flows: 1599
  Flows exported: 1599, Flows packets exported: 55
  Flows inactive timed out: 1599, Flows active timed out: 0

Passive monitoring interface: mo-4/1/0, Local interface index: 45
Interface state: Monitoring
Flow information
  Flow packets: 6537780, Flow bytes: 653778000
  Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
  Active flows: 0, Total flows: 1601
  Flows exported: 1601, Flows packets exported: 55
  Flows inactive timed out: 1601, Flows active timed out: 0

```

show passive-monitoring memory

Syntax	<code>show passive-monitoring memory (* all mo-fpc/pic/port)</code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M40e, M160, and M320 routers and T Series routers only) Display passive monitoring memory and flow record statistics
Options	<code>* all mo-fpc/pic/port</code> —Display memory and flow record statistics for monitoring interfaces. Use a wildcard character, specify all interfaces, or provide a specific interface name.
Required Privilege Level	view
List of Sample Output	show passive-monitoring memory all on page 248
Output Fields	Table 11 on page 248 lists the output fields for the <code>show passive-monitoring memory</code> command. Output fields are listed in the approximate order in which they appear.

Table 11: show passive-monitoring memory Output Fields

Field Name	Field Description
Passive monitoring interface	Name of the passive monitoring interface.
Local interface index	Index counter of the local interface.
Memory utilization	
Allocation count	Number of flow records allocated.
Free count	Number of flow records freed.
Maximum allocated	Maximum number of flow records allocated since the monitoring station booted. This number represents the peak number of flow records allocated at a time.
Allocations per second	Flow records allocated per second during the last statistics interval on the PIC.
Frees per second	Flow records freed per second during the last statistics interval on the PIC.
Total memory used, Total memory free	Total memory currently used and total amount of memory currently free (in bytes).

Sample Output

show passive-monitoring memory all

```
user@host> show passive-monitoring memory all
```

```
Passive monitoring interface: mo-4/0/0, Local interface index: 44
Memory utilization
  Allocation count: 1600, Free count: 1599, Maximum allocated: 1600
  Allocations per second: 3200, Frees per second: 1438
  Total memory used (in bytes): 103579176, Total memory free (in bytes):
  163914184
```

show passive-monitoring status

Syntax	show passive-monitoring status (* all mo-fpc/pic/port)
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M40e, M160, and M320 routers and T Series routers only) Display passive monitoring status.
Options	* all mo-fpc/pic/port—Display status for monitoring interfaces. Use a wildcard character, specify all interfaces, or provide a specific interface name.
Required Privilege Level	view
List of Sample Output	show passive-monitoring status all on page 251
Output Fields	Table 12 on page 250 lists the output fields for the show passive-monitoring status command. Output fields are listed in the approximate order in which they appear.

Table 12: show passive-monitoring status Output Fields

Output Field	Output Field Description
Passive monitoring interface	Name of the passive monitoring interface.
Local interface index	Index counter of the local interface.
Interface state	Monitoring state of the passive monitoring interface. <ul style="list-style-type: none"> • Monitoring—PIC is actively monitoring. • Disabled—PIC has been disabled using the CLI. • Not monitoring—PIC is operational, but not monitoring. This condition can happen while the PIC is coming online, or when the PIC is operational but has no logical unit configured under the physical interface. • Unknown
Group index	Integer that represents the monitoring group of which the PIC is a member. Group index is a mapping from the group name to an index. It is not related to the number of monitoring groups.
Export interval	Configured export interval for cflowd records, in seconds.
Export format	Configured export format (only cflowd version 5 is supported).
Protocol	Protocol the PIC is configured to monitor (only IPv4 is supported).
Engine type	Configured engine type that is inserted in output cflowd packets.
Engine ID	Configured engine ID that is inserted in output cflowd packets.

Sample Output

show passive-monitoring status all

```
user@host> show passive-monitoring status all
Passive monitoring interface: mo-4/0/0, Local interface index: 44
Interface state: Monitoring
  Group index: 0
  Export interval: 15 secs, Export format: cflowd v5
  Protocol: IPv4, Engine type: 1, Engine ID: 1

Passive monitoring interface: mo-4/1/0, Local interface index: 45
Interface state: Disabled

Passive monitoring interface: mo-4/2/0, Local interface index: 46
Interface state: Not monitoring
```

show passive-monitoring usage

Syntax	<code>show passive-monitoring usage (* all mo-fpc/pic/port)</code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M40e, M160, and M320 routers and T Series routers only) Display passive monitoring usage statistics.
Options	<code>* all mo-fpc/pic/port</code> —Display usage statistics for monitoring interfaces. Use a wildcard character, specify all interfaces, or provide a specific interface name.
Required Privilege Level	view
List of Sample Output	show passive-monitoring usage all on page 252
Output Fields	Table 13 on page 252 lists the output fields for the <code>show passive-monitoring usage</code> command. Output fields are listed in the approximate order in which they appear.

Table 13: show passive-monitoring usage Output Fields

Output Field	Output Field Description
Passive monitoring interface	Name of the passive monitoring interface.
Local interface index	Index counter of the local interface.
CPU utilization	
Uptime	Time, in milliseconds, that the PIC has been operational.
Interrupt time	Total time that the PIC has spent processing packets since the last PIC reset.
Load (5 second)	CPU load on the PIC, averaged more than 5 seconds. The number is a percentage obtained by dividing the time spent on active tasks by the total elapsed time.
Load (1 minute)	CPU load on the PIC, averaged more than 1 minute. The number is a percentage obtained by dividing the time spent on active tasks by the total elapsed time.

Sample Output

show passive-monitoring usage all

```

user@host> show passive-monitoring usage
Passive monitoring interface: mo-4/0/0, Local interface index: 44
CPU utilization
  Uptime: 653155 milliseconds, Interrupt time: 40213754 microseconds
  Load (5 second): 20%, Load (1 minute): 17%

Passive monitoring interface: mo-4/1/0, Local interface index: 45
CPU utilization

```

Uptime: 652292 milliseconds, Interrupt time: 40223178 microseconds
Load (5 second): 22%, Load (1 minute): 15%

Passive monitoring interface: mo-4/2/0, Local interface index: 46
CPU utilization

Uptime: 649491 milliseconds, Interrupt time: 40173645 microseconds
Load (5 second): 22%, Load (1 minute): 10098862%

show route forwarding-table

List of Syntax	Syntax on page 254 Syntax (MX Series Routers) on page 254 Syntax (TX Matrix and TX Matrix Plus Routers) on page 254
Syntax	<pre>show route forwarding-table <detail extensive summary> <all> <ccc interface-name> <destination destination-prefix> <family family matching matching> <interface-name interface-name> <label name> <matching matching> <multicast> <table (default logical-system-name/routing-instance-name routing-instance-name)> <vlan (all vlan-name)> <vpn vpn></pre>
Syntax (MX Series Routers)	<pre>show route forwarding-table <detail extensive summary> <all> <bridge-domain (all domain-name)> <ccc interface-name> <destination destination-prefix> <family family matching matching> <interface-name interface-name> <label name> <learning-vlan-id learning-vlan-id> <matching matching> <multicast> <table (default logical-system-name/routing-instance-name routing-instance-name)> <vlan (all vlan-name)> <vpn vpn></pre>
Syntax (TX Matrix and TX Matrix Plus Routers)	<pre>show route forwarding-table <detail extensive summary> <all> <ccc interface-name> <destination destination-prefix> <family family matching matching> <interface-name interface-name> <matching matching> <label name> <lcc number> <multicast> <table routing-instance-name> <vpn vpn></pre>
Release Information	Command introduced before Junos OS Release 7.4. Option bridge-domain introduced in Junos OS Release 7.5 Option learning-vlan-id introduced in Junos OS Release 8.4

Options **all** and **vlan** introduced in Junos OS Release 9.6.

Command introduced in Junos OS Release 11.3 for the QFX Series.

Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Display the Routing Engine's forwarding table, including the network-layer prefixes and their next hops. This command is used to help verify that the routing protocol process has relayed the correction information to the forwarding table. The Routing Engine constructs and maintains one or more routing tables. From the routing tables, the Routing Engine derives a table of active routes, called the forwarding table.



NOTE: The Routing Engine copies the forwarding table to the Packet Forwarding Engine, the part of the router that is responsible for forwarding packets. To display the entries in the Packet Forwarding Engine's forwarding table, use the **show pfe route** command.

Options **none**—Display the routes in the forwarding tables. By default, the **show route forwarding-table** command does not display information about private, or internal, forwarding tables.

detail | extensive | summary—(Optional) Display the specified level of output.

all—(Optional) Display routing table entries for all forwarding tables, including private, or internal, tables.

bridge-domain (all | bridge-domain-name)—(MX Series routers only) (Optional) Display route entries for all bridge domains or the specified bridge domain.

ccc interface-name—(Optional) Display route entries for the specified circuit cross-connect interface.

destination destination-prefix—(Optional) Destination prefix.

family family—(Optional) Display routing table entries for the specified family: **fibre-channel**, **fmembers**, **inet**, **inet6**, **iso**, **mpls**, **tnp**, **unix**, **vpls**, or **vlan-classification**.

interface-name interface-name—(Optional) Display routing table entries for the specified interface.

label name—(Optional) Display route entries for the specified label.

lcc number—(TX Matrix and TX matrix Plus routers only) (Optional) On a routing matrix composed of a TX Matrix router and T640 routers, display information for the specified T640 router (or line-card chassis) connected to the TX Matrix router. On a routing matrix composed of the TX Matrix Plus router and T1600 or T4000 routers, display information for the specified router (line-card chassis) connected to the TX Matrix Plus router.

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

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

learning-vlan-id *learning-vlan-id*—(MX Series routers only) (Optional) Display learned information for all VLANs or for the specified VLAN.

matching *matching*—(Optional) Display routing table entries matching the specified prefix or prefix length.

multicast—(Optional) Display routing table entries for multicast routes.

table (**default** | *logical-system-name/routing-instance-name* | *routing-instance-name*)—(Optional) Display route entries for all the routing tables in the main routing instance or for the specified routing instance. If your device supports logical systems, you can also display route entries for the specified logical system and routing instance. To view the routing instances on your device, use the **show route instance** command.

vlan (**all** | *vlan-name*)—(Optional) Display information for all VLANs or for the specified VLAN.

vpn *vpn*—(Optional) Display routing table entries for a specified VPN.

Required Privilege Level

view

List of Sample Output

[show route forwarding-table on page 259](#)
[show route forwarding-table detail on page 260](#)
[show route forwarding-table destination extensive \(Weights and Balances\) on page 260](#)
[show route forwarding-table extensive on page 261](#)
[show route forwarding-table extensive \(RPF\) on page 262](#)
[show route forwarding-table family mpls on page 263](#)
[show route forwarding-table family vpls on page 263](#)
[show route forwarding-table vpls \(Broadcast, unknown unicast, and multicast \(BUM\) hashing is enabled\) on page 263](#)
[show route forwarding-table vpls \(Broadcast, unknown unicast, and multicast \(BUM\) hashing is enabled with MAC Statistics\) on page 264](#)
[show route forwarding-table family vpls extensive on page 264](#)
[show route forwarding-table table default on page 265](#)
[show route forwarding-table table logical-system-name/routing-instance-name on page 266](#)

[show route forwarding-table vpn on page 267](#)

Output Fields [Table 14 on page 257](#) lists the output fields for the **show route forwarding-table** command. Output fields are listed in the approximate order in which they appear. Field names might be abbreviated (as shown in parentheses) when no level of output is specified, or when the **detail** keyword is used instead of the **extensive** keyword.

Table 14: show route forwarding-table Output Fields

Field Name	Field Description	Level of Output
Logical system	Name of the logical system. This field is displayed if you specify the table logical-system-name/routing-instance-name option on a device that is configured for and supports logical systems.	All levels
Routing table	Name of the routing table (for example, inet, inet6, mpls).	All levels
Address family	Address family (for example, IP, IPv6, ISO, MPLS, and VPLS).	All levels
Destination	Destination of the route.	detail extensive
Route Type (Type)	How the route was placed into the forwarding table. When the detail keyword is used, the route type might be abbreviated (as shown in parentheses): <ul style="list-style-type: none"> cloned (clon)—(TCP or multicast only) Cloned route. destination (dest)—Remote addresses directly reachable through an interface. destination down (iddn)—Destination route for which the interface is unreachable. interface cloned (ifcl)—Cloned route for which the interface is unreachable. route down (ifdn)—Interface route for which the interface is unreachable. ignore (ignr)—Ignore this route. interface (intf)—Installed as a result of configuring an interface. permanent (perm)—Routes installed by the kernel when the routing table is initialized. user—Routes installed by the routing protocol process or as a result of the configuration. 	All levels
Route Reference (RtRef)	Number of routes to reference.	detail extensive
Flags	Route type flags: <ul style="list-style-type: none"> none—No flags are enabled. accounting—Route has accounting enabled. cached—Cache route. incoming-iface interface-number—Check against incoming interface. prefix load balance—Load balancing is enabled for this prefix. rt nh decoupled—Route has been decoupled from the next hop to the destination. sent to PFE—Route has been sent to the Packet Forwarding Engine. static—Static route. 	extensive
Next hop	IP address of the next hop to the destination.	detail extensive

Table 14: show route forwarding-table Output Fields (*continued*)

Field Name	Field Description	Level of Output
Next hop Type (Type)	<p>Next-hop type. When the detail keyword is used, the next-hop type might be abbreviated (as indicated in parentheses):</p> <ul style="list-style-type: none"> • broadcast (bcst)—Broadcast. • deny—Deny. • discard (dscd) —Discard. • hold—Next hop is waiting to be resolved into a unicast or multicast type. • indexed (idxd)—Indexed next hop. • indirect (indr)—Indirect next hop. • local (locl)—Local address on an interface. • routed multicast (mcrst)—Regular multicast next hop. • multicast (mcst)—Wire multicast next hop (limited to the LAN). • multicast discard (mdsc)—Multicast discard. • multicast group (mgrp)—Multicast group member. • receive (rcv)—Receive. • reject (rjct)—Discard. An ICMP unreachable message was sent. • resolve (rslv)—Resolving the next hop. • unicast (ucst)—Unicast. • unilist (ulst)—List of unicast next hops. A packet sent to this next hop goes to any next hop in the list. 	detail extensive
Index	Software index of the next hop that is used to route the traffic for a given prefix.	detail extensive none
Route interface-index	Logical interface index from which the route is learned. For example, for interface routes, this is the logical interface index of the route itself. For static routes, this field is zero. For routes learned through routing protocols, this is the logical interface index from which the route is learned.	extensive
Reference (NhRef)	Number of routes that refer to this next hop.	detail extensive none
Next-hop interface (Netif)	Interface used to reach the next hop.	detail extensive none
Weight	Value used to distinguish primary, secondary, and fast reroute backup routes. Weight information is available when MPLS label-switched path (LSP) link protection, node-link protection, or fast reroute is enabled, or when the standby state is enabled for secondary paths. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible (see the Balance field description).	extensive
Balance	Balance coefficient indicating how traffic of unequal cost is distributed among next hops when a router is performing unequal-cost load balancing. This information is available when you enable BGP multipath load balancing.	extensive
RPF interface	List of interfaces from which the prefix can be accepted. Reverse path forwarding (RPF) information is displayed only when rpf-check is configured on the interface.	extensive

Sample Output

show route forwarding-table

```

user@host> show route forwarding-table
Routing table: default.inet
Internet:
Destination      Type RtRef Next hop          Type Index NhRef Netif
default          perm  0                               rjct  46   4
0.0.0.0/32       perm  0                               dscd  44   1
1.1.1.0/24       ifdn  0                               rslv  608  1 ge-2/0/1.0
1.1.1.0/32       iddn  0 1.1.1.0          recv  606  1 ge-2/0/1.0
1.1.1.1/32       user  0                               rjct  46   4
1.1.1.1/32       intf  0 1.1.1.1          locl  607  2
1.1.1.1/32       iddn  0 1.1.1.1          locl  607  2
1.1.1.255/32     iddn  0 ff:ff:ff:ff:ff:ff bcst  605  1 ge-2/0/1.0
10.0.0.0/24      intf  0                               rslv  616  1 ge-2/0/0.0
10.0.0.0/32      dest  0 10.0.0.0         recv  614  1 ge-2/0/0.0
10.0.0.1/32      intf  0 10.0.0.1         locl  615  2
10.0.0.1/32      dest  0 10.0.0.1         locl  615  2
10.0.0.255/32    dest  0 10.0.0.255       bcst  613  1 ge-2/0/0.0
10.1.1.0/24      ifdn  0                               rslv  612  1 ge-2/0/1.0
10.1.1.0/32      iddn  0 10.1.1.0         recv  610  1 ge-2/0/1.0
10.1.1.1/32      user  0                               rjct  46   4
10.1.1.1/32      intf  0 10.1.1.1         locl  611  2
10.1.1.1/32      iddn  0 10.1.1.1         locl  611  2
10.1.1.255/32    iddn  0 ff:ff:ff:ff:ff:ff bcst  609  1 ge-2/0/1.0
10.209.0.0/16    user  0 10.209.63.254    ucst  419  20 fxp0.0
10.209.0.0/16    user  1 0:12:1e:ca:98:0  ucst  419  20 fxp0.0
10.209.0.0/18    intf  0                               rslv  418  1 fxp0.0
10.209.0.0/32    dest  0 10.209.0.0       recv  416  1 fxp0.0
10.209.2.131/32  intf  0 10.209.2.131     locl  417  2
10.209.2.131/32  dest  0 10.209.2.131     locl  417  2
10.209.17.55/32  dest  0 0:30:48:5b:78:d2 ucst  435  1 fxp0.0
10.209.63.42/32  dest  0 0:23:7d:58:92:ca ucst  434  1 fxp0.0
10.209.63.254/32 dest  0 0:12:1e:ca:98:0  ucst  419  20 fxp0.0
10.209.63.255/32 dest  0 10.209.63.255    bcst  415  1 fxp0.0
10.227.0.0/16    user  0 10.209.63.254    ucst  419  20 fxp0.0

...

Routing table: iso
ISO:
Destination      Type RtRef Next hop          Type Index NhRef Netif
default          perm  0                               rjct  27   1
47.0005.80ff.f800.0000.0108.0003.0102.5524.5220.00
intf  0                               locl  28   1

Routing table: inet6
Internet6:
Destination      Type RtRef Next hop          Type Index NhRef Netif
default          perm  0                               rjct   6   1
ff00::/8         perm  0                               mdsc   4   1
ff02::1/128      perm  0 ff02::1          mcst   3   1

Routing table: ccc
MPLS:
Interface.Label  Type RtRef Next hop          Type Index NhRef Netif
default          perm  0                               rjct  16   1
100004(top)fe-0/0/1.0

```

show route forwarding-table detail

```

user@host> show route forwarding-table detail
Routing table: inet
Internet:
Destination      Type RtRef Next hop          Type Index NhRef Netif
default          user   2 0:90:69:8e:b1:1b ucst  132   4 fxp0.0
default          perm   0                               rjct   14    1
10.1.1.0/24      intf   0 ff.3.0.21         ucst  322   1 so-5/3/0.0
10.1.1.0/32      dest   0 10.1.1.0          recv  324   1 so-5/3/0.0
10.1.1.1/32      intf   0 10.1.1.1          locl  321   1
10.1.1.255/32    dest   0 10.1.1.255        bcst  323   1 so-5/3/0.0
10.21.21.0/24    intf   0 ff.3.0.21         ucst  326   1 so-5/3/0.0
10.21.21.0/32    dest   0 10.21.21.0        recv  328   1 so-5/3/0.0
10.21.21.1/32    intf   0 10.21.21.1        locl  325   1
10.21.21.255/32  dest   0 10.21.21.255      bcst  327   1 so-5/3/0.0
127.0.0.1/32     intf   0 127.0.0.1         locl  320   1
172.17.28.19/32  clon   1 192.168.4.254     ucst  132   4 fxp0.0
172.17.28.44/32  clon   1 192.168.4.254     ucst  132   4 fxp0.0

...

Routing table: private1__inet
Internet:
Destination      Type RtRef Next hop          Type Index NhRef Netif
default          perm   0                               rjct   46    1
10.0.0.0/8       intf   0                               rslv  136   1 fxp1.0
10.0.0.0/32      dest   0 10.0.0.0          recv  134   1 fxp1.0
10.0.0.4/32      intf   0 10.0.0.4          locl  135   2
10.0.0.4/32      dest   0 10.0.0.4          locl  135   2

...

Routing table: iso
ISO:
Destination      Type RtRef Next hop          Type Index NhRef Netif
default          perm   0                               rjct   38    1

Routing table: inet6
Internet6:
Destination      Type RtRef Next hop          Type Index NhRef Netif
default          perm   0                               rjct   22    1
ff00::/8         perm   0                               mdsc   21    1
ff02::1/128      perm   0 ff02::1          mcst   17    1

...

Routing table: mpls
MPLS:
Destination      Type RtRef Next hop          Type Index NhRef Netif
default          perm   0                               rjct  28    1

```

show route forwarding-table destination extensive (Weights and Balances)

```

user@host> show route forwarding-table destination 3.4.2.1 extensive
Routing table: inet [Index 0]
Internet:

Destination: 3.4.2.1/32
Route type: user
Route reference: 0                               Route interface-index: 0

```

```

Flags: sent to PFE
Next-hop type: unicast          Index: 262143  Reference: 1
Nexthop: 4.4.4.4
Next-hop type: unicast          Index: 335      Reference: 2
Next-hop interface: so-1/1/0.0  Weight: 22    Balance: 3
Nexthop: 145.12.1.2
Next-hop type: unicast          Index: 337      Reference: 2
Next-hop interface: so-0/1/2.0  Weight: 33    Balance: 33

```

show route forwarding-table extensive

```

user@host> show route forwarding-table extensive
Routing table: inet [Index 0]
Internet:

Destination: default
Route type: user
Route reference: 2                      Route interface-index: 0
Flags: sent to PFE
Nexthop: 0:90:69:8e:b1:1b
Next-hop type: unicast                  Index: 132      Reference: 4
Next-hop interface: fxp0.0

Destination: default
Route type: permanent
Route reference: 0                      Route interface-index: 0
Flags: none
Next-hop type: reject                   Index: 14       Reference: 1

Destination: 127.0.0.1/32
Route type: interface
Route reference: 0                      Route interface-index: 0
Flags: sent to PFE
Nexthop: 127.0.0.1
Next-hop type: local                     Index: 320      Reference: 1

...

Routing table: private1__inet [Index 1]
Internet:

Destination: default
Route type: permanent
Route reference: 0                      Route interface-index: 0
Flags: sent to PFE
Next-hop type: reject                   Index: 46       Reference: 1

Destination: 10.0.0.0/8
Route type: interface
Route reference: 0                      Route interface-index: 3
Flags: sent to PFE
Next-hop type: resolve                   Index: 136      Reference: 1
Next-hop interface: fxp1.0

...

Routing table: iso [Index 0]
ISO:

Destination: default
Route type: permanent

```

```

Route reference: 0
Flags: sent to PFE
Next-hop type: reject
Route interface-index: 0
Index: 38      Reference: 1

Routing table: inet6 [Index 0]
Internet6:

Destination: default
Route type: permanent
Route reference: 0
Flags: sent to PFE
Next-hop type: reject
Route interface-index: 0
Index: 22      Reference: 1

Destination: ff00::/8
Route type: permanent
Route reference: 0
Flags: sent to PFE
Next-hop type: multicast discard
Route interface-index: 0
Index: 21      Reference: 1

...

Routing table: private1__inet6 [Index 1]
Internet6:

Destination: default
Route type: permanent
Route reference: 0
Flags: sent to PFE
Next-hop type: reject
Route interface-index: 0
Index: 54      Reference: 1

Destination: fe80::2a0:a5ff:fe3d:375/128
Route type: interface
Route reference: 0
Flags: sent to PFE
Next-hop: fe80::2a0:a5ff:fe3d:375
Next-hop type: local
Route interface-index: 0
Index: 75      Reference: 1

...

```

show route forwarding-table extensive (RPF)

The next example is based on the following configuration, which enables an RPF check on all routes that are learned from this interface, including the interface route:

```

so-1/1/0 {
  unit 0 {
    family inet {
      rpf-check;
      address 15.95.1.2/30;
    }
  }
}

```

```

user@host> show route forwarding-table extensive
Routing table: inet [Index 0]
Internet:
...
...
Destination: 15.95.1.3/32
Route type: destination
Route reference: 0
Route interface-index: 67

```

```

Flags: sent to PFE
Nexthop: 15.95.1.3
Next-hop type: broadcast          Index: 328      Reference: 1
Next-hop interface: so-1/1/0.0
RPF interface: so-1/1/0.0

```

show route forwarding-table family mpls

```

user@host> show route forwarding-table family mpls
Routing table: mpls
MPLS:
Destination      Type RtRef Next hop          Type Index NhRef Netif
default          perm  0
0                user  0
1                user  0
2                user  0
100000           user  0 10.31.1.6          swap 100001 fe-1/1/0.0
800002           user  0                  Pop      vt-0/3/0.32770

vt-0/3/0.32770 (VPLS)
                  user  0                  indr  351    4
                  Push 800000, Push 100002(top)

so-0/0/0.0

```

show route forwarding-table family vpls

```

user@host> show route forwarding-table family vpls
Routing table: green.vpls
VPLS:
Destination      Type RtRef Next hop          Type Index NhRef Netif
default          dymn  0
default          perm  0
fe-0/1/0.0       dymn  0
00:90:69:0c:20:1f/48 <<<<<Remote CE
                  dymn  0                  indr  351    4
                  Push 800000, Push 100002(top)

so-0/0/0.0
00:90:69:85:b0:1f/48 <<<<<Local CE
                  dymn  0                  ucst  354    2 fe-0/1/0.0

```

show route forwarding-table vpls (Broadcast, unknown unicast, and multicast (BUM) hashing is enabled)

```

user@host> show route forwarding-table vpls
Routing table: green.vpls
VPLS:
Enabled protocols: BUM hashing
Destination      Type RtRef Next hop          Type Index NhRef Netif
default          perm  0
lsi.1048832      intf  0
                  4.4.3.2          indr 1048574 4
                  Push 262145      621    2

ge-3/0/0.0
00:19:e2:25:d0:01/48 user  0                  ucst  590    5 ge-2/3/9.0
0x30003/51       user  0                  comp  627    2
ge-2/3/9.0       intf  0                  ucst  590    5 ge-2/3/9.0
ge-3/1/3.0       intf  0                  ucst  619    4 ge-3/1/3.0
0x30002/51       user  0                  comp  600    2
0x30001/51       user  0                  comp  597    2

```

show route forwarding-table vpls (Broadcast, unknown unicast, and multicast (BUM) hashing is enabled with MAC Statistics)

```

user@host> show route forwarding-table vpls
Routing table: green.vpls
VPLS:
Enabled protocols: BUM hashing, MAC Stats

```

Destination	Type	RtRef	Next hop	Type	Index	NhRef	Netif
default	perm	0		dscd	519	1	
1si.1048834	intf	0		indr	1048574	4	
			4.4.3.2	Push	262145	592	2
ge-3/0/0.0							
00:19:e2:25:d0:01/48	user	0		ucst	590	5	ge-2/3/9.0
0x30003/51	user	0		comp	630	2	
ge-2/3/9.0	intf	0		ucst	590	5	ge-2/3/9.0
ge-3/1/3.0	intf	0		ucst	591	4	ge-3/1/3.0
0x30002/51	user	0		comp	627	2	
0x30001/51	user	0		comp	624	2	

show route forwarding-table family vpls extensive

```

user@host> show route forwarding-table family vpls extensive
Routing table: green.vpls [Index 2]
VPLS:

Destination: default
  Route type: dynamic
  Route reference: 0
  Flags: sent to PFE
  Next-hop type: flood
  Next-hop type: unicast
  Next-hop interface: fe-0/1/3.0
  Next-hop type: unicast
  Next-hop interface: fe-0/1/2.0
  Route interface-index: 72
  Index: 289
  Reference: 1
  Index: 291
  Reference: 3
  Index: 290
  Reference: 3

Destination: default
  Route type: permanent
  Route reference: 0
  Flags: none
  Next-hop type: discard
  Route interface-index: 0
  Index: 341
  Reference: 1

Destination: fe-0/1/2.0
  Route type: dynamic
  Route reference: 0
  Flags: sent to PFE
  Next-hop type: flood
  Next-hop type: indirect
  Next-hop type: Push 800016
  Next-hop interface: at-1/0/1.0
  Next-hop type: indirect
  Next hop: 10.31.3.2
  Next-hop type: Push 800000
  Next-hop interface: fe-0/1/1.0
  Next-hop type: unicast
  Next-hop interface: fe-0/1/3.0
  Route interface-index: 69
  Index: 293
  Reference: 1
  Index: 363
  Reference: 4
  Index: 301
  Reference: 5
  Index: 291
  Reference: 3

Destination: fe-0/1/3.0
  Route type: dynamic
  Route reference: 0
  Flags: sent to PFE
  Next-hop type: flood
  Route interface-index: 70
  Index: 292
  Reference: 1

```

```

Next-hop type: indirect          Index: 363      Reference: 4
Next-hop type: Push 800016
Next-hop interface: at-1/0/1.0
Next-hop type: indirect          Index: 301      Reference: 5
Next hop: 10.31.3.2
Next-hop type: Push 800000
Next-hop interface: fe-0/1/1.0
Next-hop type: unicast           Index: 290      Reference: 3
Next-hop interface: fe-0/1/2.0

Destination: 10:00:00:01:01:01/48
Route type: dynamic
Route reference: 0               Route interface-index: 70
Flags: sent to PFE, prefix load balance
Next-hop type: unicast           Index: 291      Reference: 3
Next-hop interface: fe-0/1/3.0
Route used as destination:
  Packet count:      6640    Byte count:      675786
Route used as source
  Packet count:      6894    Byte count:      696424

Destination: 10:00:00:01:01:04/48
Route type: dynamic
Route reference: 0               Route interface-index: 69
Flags: sent to PFE, prefix load balance
Next-hop type: unicast           Index: 290      Reference: 3
Next-hop interface: fe-0/1/2.0
Route used as destination:
  Packet count:      96     Byte count:      8079
Route used as source:
  Packet count:      296    Byte count:      24955

Destination: 10:00:00:01:03:05/48
Route type: dynamic
Route reference: 0               Route interface-index: 74
Flags: sent to PFE, prefix load balance
Next-hop type: indirect          Index: 301      Reference: 5
Next hop: 10.31.3.2
Next-hop type: Push 800000
Next-hop interface: fe-0/1/1.0

```

show route forwarding-table table default

```

user@host> show route forwarding-table table default
Routing table: default.inet
Internet:
Destination      Type RtRef Next hop          Type Index NhRef Netif
default          perm  0
0.0.0.0/32       perm  0
10.0.60.0/30     user  0 10.0.60.13          ucst  713  5 fe-0/1/3.0
10.0.60.12/30    intf  0
10.0.60.12/32    dest  0 10.0.60.12          recv  686  1 fe-0/1/3.0
10.0.60.13/32    dest  0 0:5:85:8b:bc:22     ucst  713  5 fe-0/1/3.0
10.0.60.14/32    intf  0 10.0.60.14          locl  687  2
10.0.60.14/32    dest  0 10.0.60.14          locl  687  2
10.0.60.15/32    dest  0 10.0.60.15          bcst  685  1 fe-0/1/3.0
10.0.67.12/30    user  0 10.0.60.13          ucst  713  5 fe-0/1/3.0
10.0.80.0/30     ifdn  0 ff.3.0.21          ucst  676  1 so-0/0/1.0
10.0.80.0/32     dest  0 10.0.80.0          recv  678  1 so-0/0/1.0
10.0.80.2/32     user  0
10.0.80.2/32     intf  0 10.0.80.2          locl  675  1

```



```

Logical system: R4
Routing table: vpn-red.inet6
Internet6:
Destination      Type RtRef Next hop      Type Index NhRef Netif
default          perm  0              rjct  708    1
::/128           perm  0              dscd  706    1
ff00::/8         perm  0              mdsc  707    1
ff02::1/128      perm  0 ff02::1      mcst  704    1

```

```

Logical system: R4
Routing table: vpn-red.mpls
MPLS:
Destination      Type RtRef Next hop      Type Index NhRef Netif
default          perm  0              dscd  638

```

show route forwarding-table vpn

```

user@host> show route forwarding-table vpn VPN-A
Routing table:: VPN-A.inet
Internet:
Destination      Type RtRef Nexthop      Type Index NhRef Netif
default          perm  0              rjct   4    4
10.39.10.20/30    intf  0 ff.3.0.21      ucst   40    1
so-0/0/0.0
10.39.10.21/32    intf  0 10.39.10.21     locl   36    1
10.255.14.172/32  user  0              ucst   69    2
so-0/0/0.0
10.255.14.175/32  user  0              indr   81    3
Push 100004, Push
100004(top) so-1/0/0.0
224.0.0.0/4       perm  2              mdsc   5    3
224.0.0.1/32      perm  0 224.0.0.1       mcst   1    8
224.0.0.5/32      user  1 224.0.0.5       mcst   1    8
255.255.255.255/32 perm  0              bcst   2    3

```

show services accounting aggregation

Syntax	<pre>show services accounting aggregation <i>aggregation-type</i> <<i>aggregation-value</i>> <detail extensive terse> <limit <i>limit-value</i>> < name <i>service-name</i>> <order (bytes packets)></pre>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display information about the aggregated active flows being processed by the accounting service.
Options	<p><i>aggregation-type</i> <<i>aggregation-value</i>>—Display information for a particular aggregation type and optional value:</p> <ul style="list-style-type: none"> as <<i>source-as-value</i> <i>destination-as-value</i> <i>input-snmp-interface-index-value</i> <i>output-snmp-interface-index-value</i>>—Aggregate by autonomous system (AS). destination-prefix <<i>destination-prefix-value</i> <i>destination-as-value</i> <i>output-snmp-interface-index-value</i>>—Aggregate by destination prefix. protocol-port <<i>protocol-value</i> <i>source-port-value</i> <i>destination-port-value</i>>—Aggregate by protocol and port. source-destination-prefix <<i>source-prefix-value</i> <i>destination-prefix-value</i> <i>destination-as-value</i> <i>source-as-value</i> <i>input-snmp-interface-index-value</i> <i>output-snmp-interface-index-value</i>>—Aggregate by source and destination prefix. source-prefix <<i>source-prefix-value</i> <i>source-as-value</i> <i>input-snmp-interface-index-value</i>>—Aggregate by source prefix. <p>detail extensive terse—(Optional) Display the specified level of output.</p> <p>limit <i>limit-value</i>—(Optional) Limit the display output to this number of flows. The default is no limit.</p> <p>name <i>service-name</i>—(Optional) Display information about the aggregated flows for a particular service name.</p> <p>order (bytes packets)—(Optional) Display the flow with the ordering of the highest number, either by byte count or by packet count.</p>
Additional Information	For information about aggregation configuration options, see the <i>Junos OS Services Interfaces Library for Routing Devices</i> .
Required Privilege Level	view
List of Sample Output	show services accounting aggregation protocol-port detail on page 270 show services accounting aggregation source-destination-prefix on page 270

[show services accounting aggregation source-destination- prefix order packet detail on page 270](#)

[show services accounting aggregation source-destination- prefix extensive limit on page 271](#)

[show services accounting aggregation source-destination-prefix name terse on page 271](#)

Output Fields Table 15 on page 269 lists the output fields for the **show services accounting aggregation** command. Output fields are listed in the approximate order in which they appear.

Table 15: show services accounting aggregation Output Fields

Field Name	Field Description
Service Accounting interface	Name of the service accounting interface.
Local interface index	Index corresponding to the service accounting interface.
Service name	Name of a service that was configured at the [edit forwarding-options accounting] hierarchy level. The default display, (default sampling), indicates the service was configured at the [edit forwarding-options sampling-level] hierarchy level.
Protocol	Protocol identifier and number.
Source Port	Source port identifier and number.
Destination Port	Destination port identifier and number.
Source-AS	Source autonomous system (AS) number.
Destination-AS	Destination AS number.
Source Prefix	Source prefix.
Destination Prefix	Destination prefix.
Source address	Source address.
Source prefix length	Source prefix length.
Destination address	Destination address.
Destination prefix length	Destination prefix length.
Input SNMP interface index	SNMP index of the interface the packet came in on.
Output SNMP interface index	SNMP index of the interface the packet went out on.

Table 15: show services accounting aggregation Output Fields (*continued*)

Field Name	Field Description
Start time	Actual time when the packet in this aggregation was first seen.
End time	Actual time when the packet in this aggregation was last seen.
Flow count	Number of flows in the aggregation.
Packet count	Number of packets in the aggregation.
Byte count	Number of bytes in the aggregation.

Sample Output

show services accounting aggregation protocol-port detail

```

user@host> show service accounting aggregation protocol-port detail
Service Accounting interface: mo-2/0/0, Local interface index: 468
Service name: (default sampling)
  Protocol: 6, Source port: 20, Destination port: 20
  Start time: 442349, End time: 6425714
  Flow count: 194, Packet count: 4294964388, Byte count: 4294781184

  Protocol: 0, Source port: 0, Destination port: 0
  Start time: 442349, End time: 6425749
  Flow count: 204, Packet count: 4294964324, Byte count: 4294777088

  Protocol: 17, Source port: 123, Destination port: 123
  Start time: 442364, End time: 6425784
  Flow count: 186, Packet count: 4294964152, Byte count: 4294766080

```

show services accounting aggregation source-destination-prefix

```

user@host> show service accounting aggregation source-destination-prefix
Service Accounting interface: rsp0, Local interface index: 171
Service name: (default sampling)
Interface state: Accounting
Source          Destination    Input          Output          Flow    Packet
Byte           prefix        interface      interface      count   count
prefix        count
11.1.0.0/20    40.0.0.0/24   ge-5/0/1.0    ge-5/0/0.0     256     491761
31472704
11.1.0.0/20    40.0.1.36/32  ge-5/0/1.0    ge-5/0/0.0     1
1926          123264
11.1.0.0/20    40.0.1.59/32  ge-5/0/1.0    ge-5/0/0.0     1
1926          123264
11.1.0.0/20    40.0.3.63/32  ge-5/0/1.0    ge-5/0/0.0     1
1925          123200
11.1.0.0/20    40.0.3.32/32  ge-5/0/1.0    ge-5/0/0.0     1
1925

```

show services accounting aggregation source-destination- prefix order packet detail

```

user@host> show service accounting aggregation source-destination-prefix order packet detail
name t2 input-snmp-interface-index 538

```

```

Service Accounting interface: mo-2/0/0, Local interface index: 468
Service name: t2
Source      Destination  Input SNMP  Output SNMP  Flow  Packet  Byte
Prefix      Prefix      Index      Index      Count Count   Count
11.1.1.2/20 30.0.167.1/0 538        432         1     60     46483
11.1.1.2/20 30.0.168.1/0 538        432         1     60     5191
11.1.1.2/20 30.0.154.1/0 538        432         2     60     45504
11.1.1.2/20 30.0.76.1/0  538        432         1     60     42177
11.1.1.2/20 30.0.149.1/0 538        432         1     60     49184
11.1.1.2/20 30.0.113.1/0 538        432         2     60     48757

```

show services accounting aggregation source-destination- prefix extensive limit

```

user@host> show service accounting aggregation source-destination-prefix name t2 extensive
limit 3

```

```

Service Accounting interface: mo-2/0/0, Local interface index: 542
Service name: t2

Source address: 11.1.1.2, Source prefix length: 20
Destination address: 44.200.176.1, Destination prefix length: 0
Input SNMP interface index: 24, Output SNMP interface index: 26
Source-AS: 69, Destination-AS: 69
Start time: Fri Feb 21 14:16:57 2003, End time: Fri Feb 21 14:22:50 2003
Flow count: 0, Packet count: 6, Byte count: 5340

```

```

Source address: 11.1.1.2, Source prefix length: 20
Destination address: 45.243.160.1, Destination prefix length: 0
Input SNMP interface index: 24, Output SNMP interface index: 26
Source-AS: 69, Destination-AS: 69
Start time: Fri Feb 21 14:16:57 2003, End time: Fri Feb 21 14:22:50 2003
Flow count: 0, Packet count: 6, Byte count: 5490

```

```

Source address: 11.1.1.2, Source prefix length: 20
Destination address: 45.162.160.1, Destination prefix length: 0
Input SNMP interface index: 24, Output SNMP interface index: 26
Source-AS: 69, Destination-AS: 69
Start time: Fri Feb 21 14:16:57 2003, End time: Fri Feb 21 14:22:50 2003
Flow count: 0, Packet count: 6, Byte count: 4079

```

show services accounting aggregation source-destination-prefix name terse

```

user@host> show service accounting aggregation source-destination-prefix name T3 terse
Service Accounting interface: rsp0, Local interface index: 171
Service name: T3
Interface state: Accounting
Source      Destination  Input      Output      Flow  Packet
prefix      prefix      interface  interface   count count
              count
11.1.0.0/20 50.0.0.0/24 ge-5/0/1.0 ge-5/0/0.0 256   639822
              40948608
11.1.0.0/20 50.0.2.67/32 ge-5/0/1.0 ge-5/0/0.0 1
2485        159040
11.1.0.0/20 50.0.2.92/32 ge-5/0/1.0 ge-5/0/0.0 1
2485

```

show services accounting aggregation template

Syntax	show services accounting aggregation template <template-name <i>template-name</i>>
Release Information	Command introduced in Junos OS Release 8.3.
Description	Display information for flow aggregation version 9 templates.
Options	<template-name <i>template-name</i>> —(Optional) Display information for the specified template only.
Required Privilege Level	view
List of Sample Output	show services accounting aggregation template on page 272
Output Fields	Table 16 on page 272 lists the output fields for the show services accounting aggregation template command. Output fields are listed in the approximate order in which they appear.

Table 16: show services accounting aggregation template Output Fields

Field Name	Field Description
MPLS Label 1	Position of first MPLS label.
MPLS Label 2	Position of second MPLS label.
MPLS Label 3	Position of third MPLS label.
MPLS Top Level Address	Outer top label FEC IP address.
Packet Count	Number of packets sent.

Sample Output

show services accounting aggregation template

```

user@host> show services accounting aggregation template template-name mpls
MPLS label 1: 299808, MPLS label 2: 0, MPLS label 3: 0
Source address: 11.1.1.2, Destination address: 10.255.15.22, Top Label Address:
22.15.255.10
Source port: 0, Destination port: 0
Protocol: 61, TOS: 0, TCP flags: 0
Source mask: 24, Destination mask: 32
Input SNMP interface index: 503, Output SNMP interface index: 505
Start time: 40780, End time: 157330
Packet count: 3949198, Byte count: 181663062

```

show services accounting errors

Syntax	show services accounting errors <inline-jflow name (* all <i>service-name</i>)>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display active flow error statistics.
Options	<p>none—Display error statistics for all services accounting instances.</p> <p>inline-jflow fpc-slot <i>slot-number</i>—(Optional) Display error statistics for inline jflow.</p> <p>name (* all <i>service-name</i>)—(Optional) Display active flow error statistics. Use a wildcard character, specify all services, or provide a specific service name.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> show services accounting flow on page 277
List of Sample Output	<p>show services accounting errors (Monitoring PIC interface) on page 274</p> <p>show services accounting errors (Service PIC interface) on page 275</p> <p>show services accounting errors inline-jflow fpc-slot slot-number (when only IPv6 is configured) on page 275</p> <p>show services accounting errors inline-jflow fpc-slot slot-number (when both IPv4 and IPv6 are configured) on page 275</p> <p>show services accounting errors inline-jflow (MX80 Router when both IPv4 and IPv6 are configured) on page 275</p>
Output Fields	Table 17 on page 273 lists the output fields for the show services accounting errors command. Output fields are listed in the approximate order in which they appear.

Table 17: show services accounting errors Output Fields

Field	Field Description
Service Accounting interface	Name of the service accounting interface.
Local interface index	Index counter of the local interface.
FPC slot	Slot number of the FPC for which the flow information is displayed. (Available only when the inline-jflow fpc-slot slot-number option is used.)
Service name	Name of a service that was configured at the [edit forwarding-options accounting] hierarchy level. The default display, (default sampling) , indicates the service was configured at the [edit forwarding-options sampling-level] hierarchy level.

Error Information

Table 17: show services accounting errors Output Fields (*continued*)

Field	Field Description
Packets dropped (no memory)	Number of packets dropped because of memory shortage.
Packets dropped (not IP)	Number of non-IP packets dropped.
Packets dropped (not IPv4)	Number of packets dropped because they failed the IPv4 version check.
Packets dropped (header too small)	Number of packets dropped because the packet length or IP header length was too small.
Memory allocation failures	Number of flow record memory allocation failures. A small number reflects failures to replenish the free list. A large number indicates the monitoring station is almost out of memory space.
Memory free failures	Number of flow record memory free failures.
Memory free list failures	Number of flow records received from the free list that failed. Memory is nearly exhausted, or too many new flows greater than 128 KB are being created per second.
Memory overload	Whether the memory has been overloaded. The response can be Yes or No .
PPS overload	Whether the PIC is receiving more packets per second than the configured threshold. The response can be Yes or No .
BPS overload	Whether the PIC is receiving more bits per second than the configured threshold. The response can be Yes or No .
Flow Creation Failures	Number of times flow creation failed.
Route Record Lookup Failures	Number of times the route record lookup failed.
AS Lookup Failures	Number of times autonomous system lookup failed.
Export Packet Failures	Number of times packet export failed.

Sample Output

show services accounting errors (Monitoring PIC interface)

```

user@host> show services accounting errors
Service Accounting interface: mo-1/1/0, Local interface index: 15
Service name: (default sampling)
Error information
  Packets dropped (no memory): 0, Packets dropped (not IP): 0
  Packets dropped (not IPv4): 0, Packets dropped (header too small): 0
  Memory allocation failures: 0, Memory free failures: 0
  Memory free list failures: 0
  Memory overload: No, PPS overload: No, BPS overload: No

```

Sample Output

show services accounting errors (Service PIC interface)

```
user@host> show services accounting errors
Service Accounting interface: sp-0/1/0
Service name: (default sampling)
Error information
  Service sets dropped: 0, Active timeout failures: 0
  Export packet failures: 0, Flow creation failures: 0
  Memory overload: No

Service Accounting interface: sp-1/0/0
Service name: (default sampling)
Error information
  Service sets dropped: 0, Active timeout failures: 0
  Export packet failures: 0, Flow creation failures: 0
  Memory overload: No
```

show services accounting errors inline-jflow fpc-slot slot-number (when only IPv6 is configured)

```
user@host> show services accounting errors inline-jflow fpc-slot 5
Error information
  FPC Slot: 5
  Flow Creation Failures: 0
  Route Record Lookup Failures: 0, AS Lookup Failures: 0
  Export Packet Failures: 0
  Memory Overload: No, Memory Alloc Fail Count: 0
```

show services accounting errors inline-jflow fpc-slot slot-number (when both IPv4 and IPv6 are configured)

```
user@host> show services accounting errors inline-jflow fpc-slot 5
Error information
  FPC Slot: 5
  Flow Creation Failures: 0
  Route Record Lookup Failures: 0, AS Lookup Failures: 0
  Export Packet Failures: 0
  Memory Overload: No, Memory Alloc Fail Count: 0

IPv4:
IPv4 Flow Creation Failures: 0
IPv4 Route Record Lookup Failures: 0, IPv4 AS Lookup Failures: 0
IPv4 Export Packet Failures: 0

IPv6:
IPv6 Flow Creation Failures: 0
IPv6 Route Record Lookup Failures: 0, IPv6 AS Lookup Failures: 0
IPv6 Export Packet Failures: 0
```

show services accounting errors inline-jflow (MX80 Router when both IPv4 and IPv6 are configured)

```
user@host> show services accounting errors inline-jflow
Error information
  TFEB Slot: 0
  Flow Creation Failures: 0
  Route Record Lookup Failures: 0, AS Lookup Failures: 0
  Export Packet Failures: 0
  Memory Overload: No

IPv4:
IPv4 Flow Creation Failures: 0
```

IPv4 Route Record Lookup Failures: 0, IPv4 AS Lookup Failures: 0
IPv4 Export Packet Failures: 0

IPv6:

IPv6 Flow Creation Failures: 0
IPv6 Route Record Lookup Failures: 0, IPv6 AS Lookup Failures: 0
IPv6 Export Packet Failures: 0

show services accounting flow

Syntax	<code>show services accounting flow</code> <code><inline-jflow logical-system name (* all service-name)></code>
Release Information	Command introduced before Junos OS Release 7.4. Junos OS Release 10.0 added the capability to display output from multiple sampling instances.
Description	Display active flow statistics.
Options	<p>none—Display active flow statistics for all service instances.</p> <p>logical-system (all logical-system)—(Optional) Display active flow statistics for the specified logical system or all logical systems on the device.</p> <p>inline-jflow (fpc-slot slot-number)—(Optional) Display inline flow statistics for the specified FPC.</p> <p>name (* all service-name)—(Optional) Display services accounting active flow statistics. Use a wildcard character, specify all services, or provide a specific service name.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show services accounting status on page 291
List of Sample Output	show services accounting flow (flow aggregation v5/v8 configuration) on page 278 show services accounting flow (flow aggregation v9 configuration) on page 278 show services accounting flow name on page 279 show services accounting flow name all on page 279 show services accounting flow (multiple sampling instances) on page 280 show services accounting flow inline-jflow fpc-slot slot-number (for IPv4 flow) on page 280 show services accounting flow inline-jflow fpc-slot slot-number (with IPv4 and IPv6 Configuration) on page 280 show services accounting flow inline-jflow (MX80 Router with IPv4 and IPv6 Configuration) on page 280
Output Fields	Table 18 on page 277 lists the output fields for the show services accounting flow command. Output fields are listed in the approximate order in which they appear.

Table 18: show services accounting flow Output Fields

Output Field	Output Field Description
Service Accounting interface	Name of the service accounting interface.
Local interface index	Index counter of the local interface.

Table 18: show services accounting flow Output Fields (*continued*)

Output Field	Output Field Description
Service name	Name of a service that was configured at the [edit forwarding-options accounting] hierarchy level. The default display, (default sampling), indicates the service was configured at the [edit forwarding-options sampling-level] hierarchy level.
Flow Information	
FPC Slot	Slot number of the FPC for which the flow information is displayed. (Available only when the inline-jflow fpc-slot slot-number option is used.)
Flow packets	Number of packets received by an operational PIC.
Flow bytes	Number of bytes received by an operational PIC.
Flow packets 10-second rate	Number of packets per second handled by the PIC and displayed as a 10-second average.
Flow bytes 10-second rate	Number of bytes per second handled by the PIC and displayed as a 10-second average.
Active flows	Number of currently active flows tracked by the PIC.
Total flows	Total number of flows received by an operational PIC.
Flows exported	Total number of flows exported by an operational PIC.
Flows packets exported	Total number of cflowd packets exported by an operational PIC.
Flows inactive timed out	Total number of flows that are exported because of inactivity.
Flows active timed out	Total number of long-lived flows that are exported because of an active timeout.

Sample Output

show services accounting flow (flow aggregation v5/v8 configuration)

```

user@host> show services accounting flow
Service Accounting interface: rsp0, Local interface index: 171
Service name: (default sampling)
Interface state: Accounting
Flow information
  Flow packets: 87168293, Flow bytes: 5578770752
  Flow packets 10-second rate: 45762, Flow bytes 10-second rate: 2928962
  Active flows: 1000, Total flows: 2000
  Flows exported: 19960, Flows packets exported: 582
  Flows inactive timed out: 1000, Flows active timed out: 29000

```

show services accounting flow (flow aggregation v9 configuration)

```

user@host> show services accounting flow
Flow information
  Service Accounting interface: sp-7/1/0, Local interface index: 149

```

```

Flow packets: 0, Flow bytes: 0
Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
Active flows: 0, Total flows: 0
Flows exported: 0, Flows packets exported: 1
Flows inactive timed out: 0, Flows active timed out: 0

```

show services accounting flow name

```

user@host> show services accounting flow count2
Service Accounting interface: mo-1/1/0, Local interface index: 15
Service name: count2
Flow information
  Flow packets: 0, Flow bytes: 0
  Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
  Active flows: 0, Total flows: 0
  Flows exported: 0, Flows packets exported: 0
  Flows inactive timed out: 0, Flows active timed out: 0

```

show services accounting flow name all

```

user@host> show services accounting flow name all
Service Accounting interface: rsp0, Local interface index: 171
Service name: T2
Interface state: Accounting
Flow information
  Flow packets: 37609891, Flow bytes: 2407033024
  Flow packets 10-second rate: 45762, Flow bytes 10-second rate: 2928953
  Active flows: 1000, Total flows: 1000
  Flows exported: 6705, Flows packets exported: 198
  Flows inactive timed out: 0, Flows active timed out: 13000

Service Accounting interface: rsp0, Local interface index: 171
Service name: T3
Interface state: Accounting
Flow information
  Flow packets: 37750807, Flow bytes: 2416051712
  Flow packets 10-second rate: 45762, Flow bytes 10-second rate: 2928940
  Active flows: 1000, Total flows: 1000
  Flows exported: 13437, Flows packets exported: 378
  Flows inactive timed out: 0, Flows active timed out: 13000

Service Accounting interface: rsp0, Local interface index: 171
Service name: T4
Interface state: Accounting
Flow information
  Flow packets: 0, Flow bytes: 0
  Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
  Active flows: 0, Total flows: 0
  Flows exported: 0, Flows packets exported: 0
  Flows inactive timed out: 0, Flows active timed out: 0

Service Accounting interface: rsp0, Local interface index: 171
Service name: count1
Interface state: Accounting
Flow information
  Flow packets: 0, Flow bytes: 0
  Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
  Active flows: 0, Total flows: 0
  Flows exported: 0, Flows packets exported: 0
  Flows inactive timed out: 0, Flows active timed out: 0

```

show services accounting flow (multiple sampling instances)

```
user@host> show services accounting flow
Flow information
  Service Accounting interface: sp-2/0/0, Local interface index: 215
  Flow packets: 9867, Flow bytes: 631488
  Flow packets 10-second rate: 0, Flow bytes 10-second rate: 628
  Active flows: 2, Total flows: 10
  Flows exported: 4028, Flows packets exported: 6150
  Flows inactive timed out: 8, Flows active timed out: 4026

  Service Accounting interface: sp-2/1/0, Local interface index: 223
  Flow packets: 0, Flow bytes: 0
  Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
  Active flows: 0, Total flows: 0
  Flows exported: 0, Flows packets exported: 1
  Flows inactive timed out: 0, Flows active timed out: 0
```

show services accounting flow inline-jflow fpc-slot slot-number (for IPv4 flow)

```
user@host> show services accounting flow inline-jflow fpc-slot 5
Flow information
  FPC Slot: 5
  Flow Packets: 0, Flow Bytes: 0
  Active Flows: 0, Total Flows: 0
  Flows Exported: 0, Flow Packets Exported: 0
  Flows Inactive Timed Out: 0, Flows Active Timed Out: 0
```

show services accounting flow inline-jflow fpc-slot slot-number (with IPv4 and IPv6 Configuration)

```
user@host> show services accounting flow inline-jflow fpc-slot 5
Flow information
  FPC Slot: 5
  Flow Packets: 0, Flow Bytes: 0
  Active Flows: 0, Total Flows: 0
  Flows Exported: 0, Flow Packets Exported: 0
  Flows Inactive Timed Out: 0, Flows Active Timed Out: 0

  IPv4 Flows:
  IPv4 Flow Packets: 0, IPv4 Flow Bytes: 0
  IPv4 Active Flows: 0, IPv4 Total Flows: 0
  IPv4 Flows Exported: 0, IPv4 Flow Packets exported: 0
  IPv4 Flows Inactive Timed Out: 0, IPv4 Flows Active Timed Out: 0

  IPv6 Flows:
  IPv6 Flow Packets: 0, IPv6 Flow Bytes: 0
  IPv6 Active Flows: 0, IPv6 Total Flows: 0
  IPv6 Flows Exported: 0, IPv6 Flow Packets Exported: 0
  IPv6 Flows Inactive Timed Out: 0, IPv6 Flows Active Timed Out: 0
```

show services accounting flow inline-jflow (MX80 Router with IPv4 and IPv6 Configuration)

```
user@host> show services accounting flow inline-jflow
Flow information
  TFEB Slot: 0
  Flow Packets: 0, Flow Bytes: 0
  Active Flows: 0, Total Flows: 0
  Flows Exported: 0, Flow Packets Exported: 0
  Flows Inactive Timed Out: 0, Flows Active Timed Out: 0

  IPv4 Flows:
```

IPv4 Flow Packets: 0, IPv4 Flow Bytes: 0
IPv4 Active Flows: 0, IPv4 Total Flows: 0
IPv4 Flows Exported: 0, IPv4 Flow Packets exported: 0
IPv4 Flows Inactive Timed Out: 0, IPv4 Flows Active Timed Out: 0

IPv6 Flows:
IPv6 Flow Packets: 0, IPv6 Flow Bytes: 0
IPv6 Active Flows: 0, IPv6 Total Flows: 0
IPv6 Flows Exported: 0, IPv6 Flow Packets Exported: 0
IPv6 Flows Inactive Timed Out: 0, IPv6 Flows Active Timed Out: 0

show services accounting flow-detail

Syntax `show services accounting flow-detail`
 `<detail | extensive | terse>`
 `<filters>`
 `<limit limit-value>`
 `<name (* | all | service-name)>`
 `<order (bytes | packets)>`

Release Information Command introduced before Junos OS Release 7.4.

Description Display information about the flows being processed by the accounting service.

Options `detail | extensive | terse`—(Optional) Display the specified level of output.

filters—(Optional) Filter the display output of the currently active flow records. The following filters query actively changing data structures and result in different results for multiple invocations:

- **destination-as**—Display flow records filtered by destination autonomous system information.
- **destination-port**—Display flow records filtered by destination port information.
- **destination-prefix**—Display flow records filtered by destination prefix information.
- **input-snmp-interface-index**—Display flow records filtered by SNMP input interface index information.
- **output-snmp-interface-index**—Display flow records filtered by SNMP output interface index information.
- **proto**—Display flow records filtered by protocol type.
- **source-as**—Display flow records filtered by source autonomous system information.
- **source-port**—Display flow records filtered by source port information.
- **source-prefix**—Display flow records filtered by source prefix information.
- **tos**—Display flow records filtered by type of service classification.

limit *limit-value*—(Optional) Limit the display output to the specified number of flows. The default is no limit.

name (* | all | *service-name*)—(Optional) Display information about the flows being processed. Use a wildcard character, specify all services, or provide a specific services name.

order (bytes | packets)—(Optional) Display the flow with the ordering of the highest number, either by byte count or by packet count.

Additional Information When no PIC is active, or when no route record has been downloaded from the PIC, this command reports no flows, even though packets are being sampled. This command

displays information about two concurrent sessions only. If a third session is attempted, the command pauses with no output until one of the previous sessions is completed.

Required Privilege Level view

List of Sample Output [show services accounting flow-detail on page 284](#)
[show services accounting flow-detail limit on page 285](#)
[show services accounting flow-detail name extensive on page 285](#)
[show services accounting flow-detail limit order bytes on page 285](#)
[show services accounting flow-detail source-port on page 286](#)

Output Fields [Table 19 on page 283](#) lists the output fields for the **show services accounting flow-detail** command. Output fields are listed in the approximate order in which they appear.

Table 19: show services accounting flow-detail Output Fields

Field Name	Field Description	Output Level
Service Accounting interface	Name of the service accounting interface.	All levels
Service name	Name of a service that was configured at the [edit forwarding-options accounting] hierarchy level. The default display, (default sampling) , indicates the service was configured at the [edit forwarding-options sampling] hierarchy level.	All levels
Local interface index	Index counter of the local interface.	All levels
TOS	Type-of-service value from the IP header.	extensive
Input SNMP interface index	SNMP index of the interface on which the packet came in.	extensive
Output SNMP interface index	SNMP index of the interface on which the packet went out.	extensive
Source-AS	Source AS number.	extensive
Destination-AS	Destination AS number.	extensive
Protocol	Name of the protocol used for the packet flow from the corresponding source address.	All levels
Input interface	Interface on which the packets were received.	All levels
Output interface	Interface on which the packets were transmitted.	All levels
TCP flags	Number of TCP header flags detected in the flow.	extensive
Source address	Address where the flow originated.	All levels
Source port	Name of the source port.	All levels

Table 19: show services accounting flow-detail Output Fields (*continued*)

Field Name	Field Description	Output Level
Source prefix length	Source prefix length.	extensive
Destination address	Address where the flow is sent.	All levels
Destination prefix length	Destination prefix length.	extensive
Destination port	Name of the destination port.	All levels
Start time	Actual time when the packet in this aggregation was first seen.	detail extensive
End time	Actual time when the packet in this aggregation was last seen.	detail extensive
Packet count	Number of packets in the aggregation.	All levels
Byte count	Number of bytes in the aggregation.	All levels
Time since last active timeout	Amount of time elapsed since the last active timeout, in the format <i>hh:mm:ss</i> .	None specified
Packet count for last active timeout	Number of packets in the aggregation since the last active timeout.	None specified
Byte count for last active timeout	Number of bytes in the aggregation since the last active timeout.	None specified

Sample Output

show services accounting flow-detail

In this sample, the output is split into three sections, with ellipses (...) indicating where the sections are continued.

```

user@host> show services accounting flow-detail
Service Accounting interface: rsp0, Local interface index: 171
Service name: (default sampling)
Interface state: Accounting

```

Protocol	Input interface	Source address	Source port	Output interface...
tcp(6)	ge-5/0/1.0	11.1.1.2	0	ge-5/0/0.0
tcp(6)	ge-5/0/1.0	11.1.1.2	0	ge-5/0/0.0

Destination address	Destination port	Packet count	Byte count	Time since last active timeout...
40.0.3.149	0	2660	170240	00:00:58
40.0.3.138	0	2660	170240	00:00:58

Packet count for last active timeout	Byte count for last active timeout
2805	179520
2805	179520

show services accounting flow-detail limit

In this sample, the output is split into three sections, with ellipses (...) indicating where the sections are continued.

```
user@host> show services accounting flow-detail limit 1
Service Accounting interface: rsp0, Local interface index: 171
Service name: (default sampling)
Interface state: Accounting
Protocol   Input          Source          Source   Output
           interface    address         port     interface...
tcp(6)     ge-5/0/1.0     11.1.1.2        0        ge-5/0/0.0

Destination      Destination      Packet   Byte   Time since last
address          port            count    count  active timeout...
40.0.3.149              0             2158    138112 00:00:47

Packet count for   Byte count for
last active timeout last active timeout
                2827                180928
```

show services accounting flow-detail name extensive

```
user@host> show services accounting flow-detail name cf-2 extensive
Service Accounting interface: mo-0/2/0, Local interface index: 145
Service name: cf-2
  TOS: 0, Protocol: udp(17), TCP flags: 0
  Source address: 10.10.10.1, Source prefix length: 0, Destination address:
20.20.20.20,
  Destination prefix length: 0, Source port: 1173, Destination port: 69
  Input SNMP interface index: 65, Output SNMP interface index: 0, Source-AS: 0,
  Destination-AS: 0
  Start time: 62425, End time: 635265, Packet count: 165845, Byte count: 9453165
```

show services accounting flow-detail limit order bytes

The output of the following command is displayed over 141 columns, not the standard 80 columns. In this sample, the output is split into three sections, with ellipses (...) indicating where the sections are continued.

```
user@host> show services accounting flow-detail limit 5 order bytes
Service Accounting interface: mo-2/0/0, Local interface index: 356
Service name: (default sampling)
Protocol   Input          Source          Source   Output
           interface    address         port     interface...
icmp(1)    ge-2/3/0.0     11.1.1.2        0        .local.
icmp(1)    ge-2/3/0.0     11.1.1.2        0        .local.
icmp(1)    ge-2/3/0.0     11.1.1.2        0        .local.
icmp(1)    ge-2/3/0.0     11.1.1.2        0        .local.
icmp(1)    ge-2/3/0.0     11.1.1.2        0        .local.

Destination      Destination      Packet   Byte   Time since last
address          port            count    count  active timeout...
51.88.128.2              0             16     12148  Not applicable
52.78.144.2              0             16     15229  Not applicable
51.147.192.2             0             16     13296  Not applicable
51.136.16.2              0             16     13924  Not applicable
50.214.48.2              0             16     13428  Not applicable

Packet count for   Byte count for
```

last active timeout	last active timeout
Not applicable	Not applicable
Not applicable	Not applicable
Not applicable	Not applicable
Not applicable	Not applicable
Not applicable	Not applicable

show services accounting flow-detail source-port

```
user@host> show services accounting flow-detail name cf-2 detail source-port 1173
Service Accounting interface: mo-0/2/0, Local interface index: 145
Service name: cf-2
  Protocol: udp(17), Source address: 10.10.10.1, Source port: 1173, Destination
address:
20.20.20.20, Destination port: 69
  Start time: 62425, End time: 811115, Packet count: 142438, Byte count: 8118966
```

show services accounting memory

Syntax	show services accounting memory
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display memory and flow record statistics.
Options	This command has no options.
Required Privilege Level	view
List of Sample Output	show services accounting memory (Monitoring PIC interface) on page 287 show services accounting memory (Service PIC interface) on page 288
Output Fields	Table 20 on page 287 lists the output fields for the show services accounting memory command. Output fields are listed in the approximate order in which they appear.

Table 20: show services accounting memory Output Fields

Output Field	Output Field Description
Service Accounting interface	Name of the service accounting interface.
Memory Utilization	
Local interface index	Index counter of the local interface.
Allocation count	Number of flow records allocated.
Free count	Number of flow records freed.
Maximum allocated	Maximum number of flow records allocated since the monitoring station booted. This number represents the peak number of flow records allocated at a time.
Allocations per second	Flow records allocated per second during the last statistics interval on the PIC.
Frees per second	Flow records freed per second during the last statistics interval on the PIC.
Total memory used	Total amount of memory currently used (in bytes).
Total memory free	Total amount of memory currently free (in bytes).

Sample Output

show services accounting memory (Monitoring PIC interface)

```

user@host> show services accounting memory
Service Accounting interface: mo-2/0/0, Local interface index: 468
Memory utilization

```

```
Allocation count: 437340, Free count: 433699, Maximum allocated: 6782
Allocations per second: 3366, Frees per second: 6412
Total memory used (in bytes): 133460320,
Total memory free (in bytes): 133918352
```

Sample Output

show services accounting memory (Service PIC interface)

```
user@host> show services accounting memory
Service Accounting interface: sp-0/1/0
Memory utilization
  Allocation count: 1000, Free count: 0
  Allocations per second: 0, Frees per second: 0
  Total memory used (in bytes): 218158272
  Total memory free (in bytes): 587147696

Service Accounting interface: sp-1/0/0
Memory utilization
  Allocation count: 1000, Free count: 0
  Allocations per second: 0, Frees per second: 0
  Total memory used (in bytes): 218157592
  Total memory free (in bytes): 587148376
```

show services accounting packet-size-distribution

Syntax	show services accounting packet-size-distribution <name (* all <i>service-name</i>)>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display a packet size distribution histogram.
Options	<p>none—Display a packet size distribution histogram of all accounting services.</p> <p>name (* all <i>service-name</i>)—(Optional) Display a packet size distribution histogram. Use a wildcard character, specify all services, or provide a specific services name.</p>
Required Privilege Level	view
List of Sample Output	show services accounting packet-size-distribution name on page 289
Output Fields	Table 21 on page 289 lists the output fields for the show services accounting packet-size-distribution command. Output fields are listed in the approximate order in which they appear.

Table 21: show services accounting packet-size-distribution Output Fields

Field Name	Field Description
Service Accounting interface	Name of the service accounting interface.
Service name	Name of a service that was configured at the [edit-forwarding-options accounting] hierarchy level. The default display, (default sampling), indicates the service was configured at the [edit-forwarding-options sampling-level] hierarchy level.
Local interface index	Index counter of the local interface.
Range start	Smallest packet length (in bytes) to count.
Range end	Largest packet length (in bytes) to count.
Number of packets	Count of packets detected in the size between Range start and Range end.
Percentage packets	Percentage of the total number of packets that are in this size range.

Sample Output

show services accounting packet-size-distribution name

```
user@host> show services accounting packet-size-distribution name test3
Service Accounting interface: mo-0/2/0, Local interface index: 163
Service name: test3
```

Range start	Range end	Number of packets	Percentage packets
32	64	2924	100

show services accounting status

Syntax	show services accounting status <inline-jflow fpc-slot <i>slot-number</i> name (* all <i>service-name</i>)>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 13.2R2 for EX Series switches.
Description	Display available Physical Interface Cards (PICs) for accounting services.
Options	<p>none—Display available PICs for all accounting services.</p> <p>inline-jflow fpc-slot <i>slot-number</i>—(Optional) Display inline flow accounting status for the specified FPC. For a two-member MX Series Virtual Chassis or EX9200 Virtual Chassis, the master router or switch uses FPC slot numbers 0 through 11 with no offset; the backup router or switch uses FPC slot numbers 12 through 23, with an offset of 12.</p> <p>name (* all <i>service-name</i>)—(Optional) Display available PICs. Use a wildcard character, specify all services, or provide a specific services name.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> show services accounting flow on page 277 Inline Flow Monitoring for Virtual Chassis Overview
List of Sample Output	show services accounting status name (Monitoring PIC interface) on page 292 show services accounting status name (Service PIC interface) on page 292 show services accounting status inline-jflow fpc-slot (when both IPv4 and IPv6 are configured) on page 293 show services accounting status inline-jflow (MX80 Router when both IPv4 and IPv6 are configured) on page 293
Output Fields	Table 22 on page 291 lists the output fields for the show services accounting status command. Output fields are listed in the approximate order in which they appear.

Table 22: show services accounting status Output Fields

Field	Field Description
Service Accounting interface	Name of the service accounting interface.
Service name	Name of a service that was configured at the [edit-forwarding-options accounting] hierarchy level. The default display, (default sampling), indicates the service was configured at the [edit-forwarding-options sampling-level] hierarchy level.
FPC Slot	Slot number of the FPC for which the flow information is displayed.

Table 22: show services accounting status Output Fields (*continued*)

Field	Field Description
Local interface index	Index counter of the local interface.
Interface state	Accounting state of the passive monitoring interface. <ul style="list-style-type: none"> • Accounting—PIC is actively accounting. • Disabled—PIC has been disabled from the CLI. • Not accounting—PIC is up but not accounting. This can happen while the PIC is coming online, or when the PIC is up but has no logical unit configured under the physical interface. • Unknown
Group index	Integer that represents the monitoring group of which the PIC is a member. Group index is a mapping from the group name to an index. It is not related to the number of monitoring groups.
Export interval (in seconds)	Configured export interval for cflowd records, in seconds.
Export format	Configured export format.
Protocol	Protocol the PIC is configured to monitor.
Engine type	Configured engine type that is inserted in output cflowd packets.
Engine ID	Configured engine ID that is inserted in output cflowd packets.
Route Record Count	Number of routes recorded.
AS Record Count	Number of autonomous systems recorded.
Route Records Set	Status of route recording; whether routes are recorded or not.
Configuration Set	Status of monitoring configuration; whether monitoring configuration is set or not.

Sample Output

show services accounting status name (Monitoring PIC interface)

```

user@host> show services accounting status name count1
Service Accounting interface: mo-2/0/0, Local interface index: 468
Service name: count1
Interface state: Accounting
  Group index: 0
  Export interval (in seconds): 60, Export format: cflowd v8
  Protocol: IPv4, Engine type: 55, Engine ID: 5

```

Sample Output

show services accounting status name (Service PIC interface)

```

user@host> show services accounting status name

```

```

Service Accounting interface: sp-0/1/0
Interface state: Accounting
  Export format: 9, Route record count: 0
  IFL to SNMP index count: 7, AS count: 0
  Configuration set: Yes, Route record set: No, IFL SNMP map set: Yes

Service Accounting interface: sp-1/0/0
Interface state: Accounting
  Export format: 9, Route record count: 33
  IFL to SNMP index count: 7, AS count: 1
  Configuration set: Yes, Route record set: Yes, IFL SNMP map set: Yes

```

show services accounting status inline-jflow fpc-slot (when both IPv4 and IPv6 are configured)

```

user@host> show services accounting status inline-jflow fpc-slot 5
FPC Slot: 5
  IPv4 export format: Version-IPFIX, IPv6 export format: Version-IPFIX
  VPLS export format: Not set
  IPv4 Route Record Count: 5, IPv6 Route Record Count: 7
  Route Record Count: 12, AS Record Count: 1
  Route-Records Set: Yes, Config Set: Yes

```

show services accounting status inline-jflow (MX80 Router when both IPv4 and IPv6 are configured)

```

user@host> show services accounting status inline-jflow

Status information
TFEB Slot: 0
Export format: IP-FIX
IPv4 Route Record Count: 6, IPv6 Route Record Count: 8
Route Record Count: 14, AS Record Count: 1
Route-Records Set: Yes, Config Set: Yes

```

show services accounting usage

Syntax	<code>show services accounting usage</code> <code><name service-name></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display the CPU usage of PIC used for active flow monitoring.
Options	<p>none—Display CPU usage for all service names.</p> <p>name service-name—(Optional) Display CPU usage for the specified service name.</p>
Additional Information	When no route record has been downloaded from the PIC, this command reports no flows, even though packets are being sampled.
Required Privilege Level	view
List of Sample Output	show services accounting usage (Monitoring PIC interface) on page 295 show services accounting usage (Service PIC interface) on page 295
Output Fields	Table 23 on page 294 lists the output fields for the show services accounting usage command. Output fields are listed in the approximate order in which they appear.

Table 23: show services accounting usage Output Fields

Output Field	Output Field Description
Service Accounting interface	Name of the service accounting interface.
Service name	Name of a service that was configured at the <code>[edit-forwarding-options accounting]</code> hierarchy level. The default display, (default sampling) , indicates the service was configured at the <code>[edit-forwarding-options sampling-level]</code> hierarchy level.
Local interface index	Index counter of the local interface.
Uptime	Time that the PIC has been operational (in milliseconds).
Interrupt time	Total time that the PIC has spent processing packets since the last PIC reset (in microseconds).
Load (5 second)	CPU load on the PIC, averaged more than 5 seconds. The number is a percentage obtained by dividing the time spent on active tasks by the total elapsed time.
Load (1 minute)	CPU load on the PIC, averaged more than 1 minute. The number is a percentage obtained by dividing the time spent on active tasks by the total elapsed time.

Sample Output

show services accounting usage (Monitoring PIC interface)

```
user@host> show services accounting usage
Service Accounting interface: mo-1/1/0, Local interface index: 15
Service name: (default sampling)
CPU utilization
  Uptime: 600413856 milliseconds, Interrupt time: 2403 microseconds
  Load (5 second): 43%, Load (1 minute): 24%
```

Sample Output

show services accounting usage (Service PIC interface)

```
user@host> show services accounting usage
Service Accounting interface: sp-0/1/0
Service name: (default sampling)
CPU utilization
  Uptime: 7853940 milliseconds, Interrupt time: 0 microseconds
  Load (5 second): 2%, Load (1 minute): 0%

Service Accounting interface: sp-0/1/0
Service name: (default sampling)
CPU utilization
  Uptime: 331160 milliseconds, Interrupt time: 0 microseconds
  Load (5 second): 2%, Load (1 minute): 0%
```

show services flow-collector file interface

Syntax	show services flow-collector file interface (all cp-fpc/pic/port) <detail extensive terse>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M40e, M160, and M320 routers and T Series routers only) Display information about flow collector files.
Options	<p>all cp-fpc/pic/port—Display file information for all configured flow collector interfaces or for the specified interface.</p> <p>detail extensive terse—(Optional) Display the specified level of output.</p>
Additional Information	No entries are displayed for files that have been successfully transferred.
Required Privilege Level	view
List of Sample Output	show services flow-collector file interface extensive on page 297
Output Fields	Table 24 on page 296 lists the output fields for the show services flow-collector file interface command. Output fields are listed in the approximate order in which they appear.

Table 24: show services flow-collector file interface Output Fields

Output Field	Output Field Description	Level of Output
Filename	Name of the file created on the flow collector interface.	All levels
Flows	Total number of collector flows for which records are present in the file.	none specified
Throughput	Throughput statistics: <ul style="list-style-type: none"> • Flow records—Number of flow records in the file. <ul style="list-style-type: none"> • per second—Average number of flow records per second. • peak per second—Peak number of flow records per second. • Uncompressed bytes—Total file size before compression. <ul style="list-style-type: none"> • per second—Average number of uncompressed bytes per second. • peak per second—Peak number of uncompressed bytes per second. • Compressed bytes—Total file size after compression. <ul style="list-style-type: none"> • per second—Average number of compressed bytes per second. • peak per second—Peak number of compressed bytes per second. 	extensive

Table 24: show services flow-collector file interface Output Fields (*continued*)

Output Field	Output Field Description	Level of Output
Status	<p>File statistics:</p> <ul style="list-style-type: none"> • Compressed blocks—(extensive output only) Data blocks in the file that have been compressed. The file is exported only when the compressed block count and block count become the same. • Block count—(extensive output only) Total number of data blocks in the file. • State—Processing state of the file. <ul style="list-style-type: none"> • Active—The flow collector interface is writing to the file. • Export 1—File export is in progress to the primary server. • Export 2—File export is in progress to the secondary server. • Wait—File is pending export. • Transfer attempts 0—Number of attempts made to transfer the file. If the file is successfully transferred in the first attempt, this field is 0. 	All levels

Sample Output

show services flow-collector file interface extensive

```

user@host> show services flow-collector file interface cp-3/2/0 extensive
Filename: cFlowd-py69Ni69-0-20031112_014301-so_3_0_0_0.bcp.bi.gz
Throughput:
  Flow records: 188365, per second: 238, peak per second: 287
  Uncompressed bytes: 21267756, per second: 27007, peak per second: 32526
  Compressed bytes: 2965643, per second: 0, peak per second: 22999
Status:
  Compressed blocks: 156, Block count: 156
  State: Active, Transfer attempts: 0

```

show services flow-collector input interface

Syntax	show services flow-collector input interface (all cp-fpc/pic/port) <detail extensive terse>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M40e, M160, and M320 routers and T Series routers only) Display the number of packets received by collector interfaces from monitoring interfaces.
Options	<p>all cp-fpc/pic/port—Display packets received by all configured flow collector interfaces or by the specified interface.</p> <p>detail extensive terse—(Optional) Display the specified level of output.</p>
Required Privilege Level	view
List of Sample Output	show services flow-collector input interface on page 298 show services flow-collector input interface all on page 298
Output Fields	Table 25 on page 298 lists the output fields for the show services flow-collector input interface command. Output fields are listed in the approximate order in which they appear.

Table 25: show services flow-collector input interface Output Fields

Output Field	Output Field Description
Interface	Name of the monitoring interface.
Packets	Number of packets traveling from the monitoring interface to the flow collector interface.
Bytes	Number of bytes traveling from the monitoring interface to the flow collector interface.

Sample Output

show services flow-collector input interface

```

user@host> show services flow-collector input interface cp-3/2/0
Interface                Packets    Bytes
mo-3/0/0.0                21706     32328568
mo-3/1/0.0                21706     32329096

```

show services flow-collector input interface all

```

user@host> show services flow-collector input interface all
Flow collector interface: cp-6/1/0
Interface state: Collecting flows
Interface                Packets    Bytes
mo-3/0/0.0                274        416232
mo-3/3/0.0                274        416184

```

mo-1/0/0.0	274	416232
mo-1/1/0.0	274	416232
mo-1/2/0.0	274	416232
mo-1/3/0.0	274	416232
mo-3/1/0.0	274	416232
mo-4/0/0.0	274	416232
mo-4/1/0.0	274	416232
mo-4/2/0.0	274	416184
mo-4/3/0.0	274	416232
mo-5/0/0.0	274	416232
mo-5/1/0.0	274	416232
mo-5/2/0.0	274	416232
mo-5/3/0.0	274	416232
mo-6/0/0.0	274	416232

Flow collector interface: cp-6/3/0
Interface state: Collecting flows

show services flow-collector interface

Syntax	show services flow-collector interface (all <i>cp-fpc/pic/port</i>) <detail extensive terse>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M40e, M160, and M320 routers and T Series routers only) Display overall statistics for the flow collector application.
Options	<p>all <i>cp-fpc/pic/port</i>—Display statistics for flow collector applications on all interfaces or for the specified interface.</p> <p>detail extensive terse—(Optional) Display the specified level of output.</p>
Required Privilege Level	view
List of Sample Output	show services flow-collector interface all detail on page 302 show services flow-collector interface all extensive on page 303 show services flow-collector interface all terse on page 305 show services flow-collector interface extensive on page 305
Output Fields	Table 26 on page 300 lists the output fields for the show services flow-collector interface command. Output fields are listed in the approximate order in which they appear.

Table 26: show services flow-collector interface Output Fields

Output Field	Output Field Description	Level of Output
Flow collector interface	Name of the flow collector interface.	All levels
Interface state	Collecting flow state for the interface.	All levels
Packets	Total number of packets received.	none specified
Flows Uncompressed Bytes	Total uncompressed data size for all files created on this PIC.	none specified
Compressed Bytes	Total compressed data size for all files created on this PIC.	none specified
FTP bytes	Total number of bytes transferred to the FTP server, including those dropped during transfer.	none specified
FTP files	Total number of FTP transfers attempted by the server.	none specified
Memory	Bytes used on the PIC and bytes free.	detail extensive

Table 26: show services flow-collector interface Output Fields (*continued*)

Output Field	Output Field Description	Level of Output
Input	Incoming flow collector packet statistics: <ul style="list-style-type: none"> • Packets—Number of packets received on the unit. <ul style="list-style-type: none"> • per second—Average number of packets per second. • peak per second—Peak number of packets per second. • Bytes—Number of bytes received on the unit. <ul style="list-style-type: none"> • per second—Average number of bytes per second. • peak per second—Peak number of bytes per second. • Flow records processed—Number of records in the flow collector packets that were processed by the flow-collector interface. <ul style="list-style-type: none"> • per second—Average number of flow records processed per second. • peak per second—Peak number of flow records per second. 	detail extensive
Allocation	Data block statistics: <ul style="list-style-type: none"> • Blocks allocated—Total number of data blocks (containing flow records) allocated to the files created on this PIC. <ul style="list-style-type: none"> • per second—Average number of blocks allocated per second. • peak per second—Peak number of blocks allocated per second. • Blocks freed—Total number of data blocks freed. <ul style="list-style-type: none"> • per second—Average number of blocks freed per second. • peak per second—Peak number of blocks freed per second. • Blocks unavailable—Total number of data block requests denied, typically because of a memory shortage. <ul style="list-style-type: none"> • per second—Average number of blocks unavailable per second. • peak per second—Peak number of blocks unavailable per second. 	extensive
Files	File statistics, incremented since the PIC last booted: <ul style="list-style-type: none"> • Files created—Total number of files created on this PIC. • Files exported— Number of files successfully created and exported. • Files destroyed— (extensive output only) Number of files successfully exported and files dropped by the flow collection interface. 	detail extensive
Throughput	Throughput statistics: <ul style="list-style-type: none"> • Uncompressed bytes—Total uncompressed data size for all files created on this PIC. <ul style="list-style-type: none"> • per second—Average number of uncompressed bytes per second. • peak per second—Peak number of uncompressed bytes per second. • Compressed bytes—Total compressed data size for all files created on this PIC. <ul style="list-style-type: none"> • per second—Average number of compressed bytes per second. • peak per second—Peak number of compressed bytes per second. 	detail extensive

Table 26: show services flow-collector interface Output Fields (*continued*)

Output Field	Output Field Description	Level of Output
Packet drops	<p>Number of packets dropped for the following causes:</p> <ul style="list-style-type: none"> • No memory—Packets dropped because of insufficient memory. • Not IP—Packets dropped because they are not IP packets. • Not IPv4—Packets dropped because they are not IP version 4 packets. • Too small—Packets dropped because each packet was smaller than the size reported in its header. • Fragments—Packets dropped because of fragmentation. Fragments are not reassembled. • ICMP—Packets dropped because they are not ICMP packets. • TCP—Packets dropped because they are not TCP packets. • Unknown—Packets dropped because of undetermined causes. • Not Junos flow—Packets dropped because they are not interpreted by Junos OS. Junos OS interprets only IPv4, UDP cflowd version 5 packets. 	extensive
File transfer	<p>File transfer statistics:</p> <ul style="list-style-type: none"> • FTP bytes—Total number of bytes transferred to the FTP server, including those dropped during transfer. • FTP files—Total number of FTP transfers attempted by the server. • FTP failure—Total number of FTP failures encountered by the server. 	detail extensive
Flow collector interface	Physical interface acting as a flow collector.	detail
Export channel	<p>Export channel 0 is unit 0. Export channel 1 is unit 1. Flow receive channel is unit 2. Server status statistics are the following:</p> <ul style="list-style-type: none"> • Current server Primary or Secondary—Current FTP server being used. Value is • Primary server state—State of the server: <ul style="list-style-type: none"> • OK—Server is operating without problems. • FTP error—Server encountered an FTP protocol error while sending files. • Network error—Flow-collector interface has errors when contacting the primary FTP server. • Unknown—First file transfer has not been sent to the primary server. • Secondary server state—State of the server: <ul style="list-style-type: none"> • OK—Server is operating without errors. • FTP error—Server encountered an FTP protocol error while sending files. • Network error—Flow-collector interface has errors when contacting the secondary FTP server. • Unknown—First file transfer has not been sent to the secondary server. • Not configured—Secondary server is not configured. 	detail extensive

Sample Output

show services flow-collector interface all detail

```
user@host> show services flow-collector interface all detail
```

```

Flow collector interface: cp-6/1/0
Interface state: Collecting flows
Memory:
  Used: 51452732, Free: 440329088
Input:
  Packets: 4384, per second: 0, peak per second: 156
  Bytes: 6659616, per second: 0, peak per second: 249695
  Flow records processed: 131070, per second: 0, peak per second: 4914
Files:
  Files created: 1, per second: 0, peak per second: 0
  Files exported: 1, per second: 0, peak per second: 0
Throughput:
  Uncompressed bytes: 13742307, per second: 0, peak per second: 593564
  Compressed bytes: 3786177, per second: 0, peak per second: 162826
File Transfer:
  FTP bytes: 3786247, per second: 0, peak per second: 378620
  FTP files: 1, per second: 0, peak per second: 0
  FTP failure: 0
Export channel: 0
  Current server: Primary
  Primary server state: OK, Secondary server state: OK
Export channel: 1
  Current server: Primary
  Primary server state: Unknown, Secondary server state: OK

Flow collector interface: cp-6/3/0
Interface state: Collecting flows
Memory:
  Used: 51452732, Free: 440329088
Input:
  Packets: 0, per second: 0, peak per second: 0
  Bytes: 0, per second: 0, peak per second: 0
  Flow records processed: 0, per second: 0, peak per second: 0
Files:
  Files created: 0, per second: 0, peak per second: 0
  Files exported: 0, per second: 0, peak per second: 0
Throughput:
  Uncompressed bytes: 0, per second: 0, peak per second: 0
  Compressed bytes: 0, per second: 0, peak per second: 0
File Transfer:
  FTP bytes: 70, per second: 0, peak per second: 6
  FTP files: 0, per second: 0, peak per second: 0
  FTP failure: 0
Export channel: 0
  Current server: Primary
  Primary server state: Unknown, Secondary server state: OK
Export channel: 1
  Current server: Primary
  Primary server state: Unknown, Secondary server state: OK

```

show services flow-collector interface all extensive

```

user@host> show services flow-collector interface all extensive
Flow collector interface: cp-6/1/0
Interface state: Collecting flows
Memory:
  Used: 51452732, Free: 440329088
Input:
  Packets: 4384, per second: 0, peak per second: 156
  Bytes: 6659616, per second: 0, peak per second: 249695
  Flow records processed: 131070, per second: 0, peak per second: 4914

```

Allocation:
Blocks allocated: 108, per second: 0, peak per second: 0
Blocks freed: 108, per second: 0, peak per second: 10
Blocks unavailable: 0, per second: 0, peak per second: 0

Files:
Files created: 1, per second: 0, peak per second: 0
Files exported: 1, per second: 0, peak per second: 0
Files destroyed: 1, per second: 0, peak per second: 0

Throughput:
Uncompressed bytes: 13742307, per second: 0, peak per second: 593564
Compressed bytes: 3786177, per second: 0, peak per second: 162826

Packet drops:
No memory: 0, Not IP: 0
Not IPv4: 0, Too small: 0
Fragments: 0, ICMP: 0
TCP: 0, Unknown: 0
Not JUNOS flow: 0

File Transfer:
FTP bytes: 3786247, per second: 0, peak per second: 378620
FTP files: 1, per second: 0, peak per second: 0
FTP failure: 0

Export channel: 0
Current server: Primary
Primary server state: OK, Secondary server state: OK

Export channel: 1
Current server: Primary
Primary server state: Unknown, Secondary server state: OK

Flow collector interface: cp-6/3/0
Interface state: Collecting flows

Memory:
Used: 51452732, Free: 440329088

Input:
Packets: 0, per second: 0, peak per second: 0
Bytes: 0, per second: 0, peak per second: 0
Flow records processed: 0, per second: 0, peak per second: 0

Allocation:
Blocks allocated: 0, per second: 0, peak per second: 0
Blocks freed: 0, per second: 0, peak per second: 0
Blocks unavailable: 0, per second: 0, peak per second: 0

Files:
Files created: 0, per second: 0, peak per second: 0
Files exported: 0, per second: 0, peak per second: 0
Files destroyed: 0, per second: 0, peak per second: 0

Throughput:
Uncompressed bytes: 0, per second: 0, peak per second: 0
Compressed bytes: 0, per second: 0, peak per second: 0

Packet drops:
No memory: 0, Not IP: 0
Not IPv4: 0, Too small: 0
Fragments: 0, ICMP: 0
TCP: 0, Unknown: 0
Not JUNOS flow: 0

File Transfer:
FTP bytes: 70, per second: 0, peak per second: 6
FTP files: 0, per second: 0, peak per second: 0
FTP failure: 0

Export channel: 0
Current server: Primary
Primary server state: Unknown, Secondary server state: OK

Export channel: 1

Current server: Primary
 Primary server state: Unknown, Secondary server state: OK

show services flow-collector interface all terse

```
user@host> show services flow-collector interface all terse
Flow collector interface: cp-6/1/0
Interface state: Collecting flows
  Packets      Bytes      Flows Uncompressed   Compressed   FTP bytes FTP files
                Bytes      Bytes      Bytes      Bytes
      4384    6659616    131070    13742307    3786177      3786247        1

Flow collector interface: cp-6/3/0
Interface state: Collecting flows
  Packets      Bytes      Flows Uncompressed   Compressed   FTP bytes FTP files
                Bytes      Bytes      Bytes      Bytes
         0         0         0         0         0         70         0
```

show services flow-collector interface extensive

```
user@host> show services flow-collector interface cp-5/2/0 extensive
Flow collector interface: cp-5/2/0
Interface state: Collecting flows
Memory:
  Used: 458311860, Free: 40810008
Input:
  Packets: 922629, per second: 2069, peak per second: 3266
  Bytes: 1376559252, per second: 3096940, peak per second: 4880051
  Flow records processed: 25764957, per second: 42564, peak per second: 98124
Allocation:
  Blocks allocated: 20862, per second: 31, peak per second: 72
  Blocks freed: 17161, per second: 40, peak per second: 202
  Blocks unavailable: 58786, per second: 652, peak per second: 1120
Files:
  Files created: 52, per second: 0, peak per second: 0
  Files exported: 42, per second: 0, peak per second: 0
  Files destroyed: 42, per second: 0, peak per second: 0
Throughput:
  Uncompressed bytes: 2592070401, per second: 7297307,
  peak per second: 8630023
  Compressed bytes: 659600068, per second: 1858458, peak per second: 2198471
Packet drops:
  No memory: 58786, Not IP: 0
  Not IPv4: 0, Too small: 0
  Fragments: 0, ICMP: 0
  TCP: 0, Unknown: 0
  Not JUNOS flow: 0
File Transfer:
  FTP bytes: 585981447, per second: 1313320, peak per second: 4857798
  FTP files: 48, per second: 0, peak per second: 0
  FTP failure: 8
Export channel: 0
  Current server: Primary
  Primary server state: FTP error, Secondary server state: Not configured
Export channel: 1
  Current server: Primary
  Primary server state: OK, Secondary server state: Not configured
```


CHAPTER 9

Index

- [Index on page 309](#)

Index

Symbols

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

A

accept	
firewall filters	
action.....	21
accounting statement.....	102
usage guidelines.....	40
active flow monitoring	
aggregated flows, displaying.....	268
available PICs, displaying.....	291
CPU usage, displaying.....	294
error statistics, displaying.....	273
flow statistics, displaying.....	277
flows, detailed information, displaying.....	282
memory statistics, displaying.....	287
packet size distribution, displaying.....	289
active flow monitoring, version 9	
PTX series	
configuring.....	42
aggregated Ethernet	
load balancing.....	77, 78
aggregated flows, displaying.....	268
aggregation statement.....	103
usage guidelines.....	40
autonomous-system-type statement.....	104
usage guidelines.....	26

B

BOOTP relay agent.....	91
bootp statement.....	105
usage guidelines.....	91
braces, in configuration statements.....	xvi

brackets	
angle, in syntax descriptions.....	xvi
square, in configuration statements.....	xvi
bum-hashing statement	
routing-instances.....	106

C

cflowd.....	107, 108
chassis	
forwarding process, displaying.....	204
clear passive-monitoring statistics command.....	199
clear services flow-collector statistics	
command.....	200
client-address.....	108
client-response-ttl statement.....	109
comments, in configuration statements.....	xvi
conventions	
text and syntax.....	xv
curly braces, in configuration statements.....	xvi
customer support.....	xvii
contacting JTAC.....	xvii

D

description statement	
helper service or interface.....	109
service	
usage guidelines.....	91, 94
DHCP	
relay agent.....	91
snopping.....	97
dhcp-relay statement	
DHCP snooping.....	110
disable statement	
flow monitoring.....	111
traffic sampling	
usage guidelines.....	24
Discard Accounting	
cflowd.....	107
DNS	
packet forwarding.....	94
requests, disabling recognition.....	94
documentation	
comments on.....	xvii
domain statement.....	112

E

ECMP	
flow-based forwarding.....	71, 72

enhanced-hash-key		
forwarding-options.....	113	
equal-cost multi-path See ECMP		
equal-cost multipath See ECMP		
ether-pseudowire statement.....	125	
usage guidelines.....	63	
Ethernet interfaces		
status information, displaying		
internal.....	216	
management.....	216	
export-format	112	
export-format statement		
usage guidelines.....	44	
F		
family		
monitoring.....	118	
family inet statement (load balancing).....	123	
usage guidelines.....	35	
family mpls statement.....	125	
usage guidelines.....	63	
family multiservice statement.....	128	
usage guidelines.....	76	
family statement		
forwarding table filters.....	117	
port mirroring.....	119	
sampling.....	121	
file statement		
helpers trace options.....	130	
sampling.....	130	
traceoptions.....	131	
traffic sampling output		
usage guidelines.....	24, 33, 95	
filename		
Sampling.....	131	
files		
logging information output file.....	33, 95	
traffic sampling output files.....	24	
var/log/sampled file.....	33, 95	
var/tmp/sampled.pkts file.....	24	
files statement		
sampling.....	132	
usage guidelines.....	24	
filter statement		
forwarding table.....	132	
VPLS.....	133	
firewall filters		
applying.....	57	
in traffic sampling.....	21	
flood statement.....	133	
usage guidelines.....	60	
flow aggregation.....	26	
templates.....	272	
flow collector services		
interface files, displaying.....	296	
packets received, displaying.....	298	
primary server, switching to.....	201	
secondary server, switching to.....	202	
statistics		
displaying.....	300	
interface, clearing.....	200	
test file, transferring.....	203	
Flow Monitoring		
cflowd.....	108	
flow monitoring		
active		
aggregated flows, displaying.....	268	
CPU usage, displaying.....	294	
detailed information, displaying.....	282	
error statistics, displaying.....	273	
flow statistics, displaying.....	277	
memory statistics, displaying.....	287	
packet size distribution, displaying.....	289	
PICs, displaying available.....	291	
passive		
flow statistics, displaying.....	246	
memory and flow statistics,		
displaying.....	248	
status, displaying.....	250	
usage statistics, displaying.....	252	
flow monitoring interfaces		
status information, displaying.....	211	
flow-active-timeout statement.....	134	
accounting		
usage guidelines.....	40	
sampling		
usage guidelines.....	24	
flow-based forwarding		
ECMP.....	71, 72	
flow-export-destination statement.....	134	
usage guidelines.....	44	
flow-inactive-timeout statement.....	135	
accounting		
usage guidelines.....	40	
sampling		
usage guidelines.....	24	
flow-server statement		
usage guidelines.....	26	

-
- font conventions.....xv
 - forwarding process, displaying.....204
 - forwarding table
 - filters.....60
 - route entries, displaying.....254
 - forwarding-options
 - enhanced-hash-key113
 - forwarding-options statement
 - usage guidelines.....35
 - FTP traffic, sampling.....32
- G**
- group statement
 - DHCP snooping.....137
- H**
- hash-key statement.....139
 - usage guidelines.....35
 - hash-seed statement
 - load balancing.....174, 175
 - helpers statement.....142
 - hosted-service-identifier.....144
 - hosted-services statement.....108, 144, 187, 188
 - hyper-mode statement.....145
- I**
- indexed-load-balance.....146
 - input statement
 - firewall filters
 - usage guidelines.....57
 - forwarding table.....147
 - port mirroring.....147
 - sampling.....148
 - traffic sampling
 - usage guidelines.....22
 - usage guidelines.....60
 - instance statement
 - port mirroring.....149
 - interface statement
 - accounting or sampling.....150
 - BOOTP.....151
 - DNS or TFTP packet forwarding or relay
 - agent.....153
 - monitoring.....154
 - next-hop group.....155
 - port mirroring.....155
 - snooping.....152
 - usage guidelines.....91
 - internal Ethernet interface
 - status information, displaying.....216
 - IP addresses
 - sampling traffic from single IP addresses.....31
 - IPv6 accounting, configuring.....39
- L**
- link-layer-broadcast-inet-check.....156
 - load balancing
 - configuring.....78
 - Ethernet pseudowires.....63
 - per-flow.....69, 70
 - per-packet.....65
 - IPv4.....66
 - per-prefix.....69
 - load-balance group.....65
 - load-balance statement.....157
 - usage guidelines.....69, 70
 - load-balance-group statement.....159
 - usage guidelines.....65
 - local-dump statement.....159
 - usage guidelines.....26, 28
 - log output
 - traffic sampling.....33, 95
- M**
- manuals
 - comments on.....xvii
 - max-packets-per-second statement.....160
 - maximum-hop-count statement.....160
 - usage guidelines.....91
 - maximum-packet-length statement.....161
 - minimum-wait-time statement.....162
 - mirror-once statement.....163
 - monitoring
 - family.....118
 - monitoring statement.....164
 - usage guidelines.....44
- N**
- next-hop group for port mirroring.....53
 - next-hop groups.....49
 - next-hop statement.....165
 - next-hop groups
 - usage guidelines.....49
 - next-hop-group
 - port-mirroring for IPv6.....167
 - next-hop-group statement.....166
 - usage guidelines.....49

no-filter-check statement.....	168
no-listen statement	
usage guidelines.....	91
no-local-dump statement.....	159
usage guidelines.....	26
no-stamp statement.....	191
usage guidelines.....	24
no-world-readable statement.....	196
usage guidelines.....	33

O

output files	
logging information output file.....	33, 95
traffic sampling output files.....	24
output statement	
accounting.....	169
firewall filters	
usage guidelines.....	57
forwarding table.....	170
monitoring.....	171
port mirroring.....	172
sampling.....	173
usage guidelines.....	60

P

P2MP.....	78
packet size distribution, displaying.....	289
parentheses, in syntax descriptions.....	xvi
passive flow monitoring	
error statistics, displaying.....	244
flow statistics, displaying.....	246
memory statistics, displaying.....	248
PICs, displaying available.....	250
statistics, clearing.....	199
usage statistics, displaying.....	252
per-flow load balancing.....	70
per-flow statement.....	174
per-prefix load balancing.....	69
per-prefix statement.....	175
PICs	
active flow monitoring	
available PICs, displaying.....	291
CPU usage, displaying.....	294
port mirroring.....	45
disabling.....	111
displaying.....	206
mirror-once statement.....	163

multiple instances.....	149
PTX series	
configuring.....	42
port statement.....	175, 176
usage guidelines.....	26
port-mirroring firewall filter.....	51
port-mirroring statement.....	178
usage guidelines.....	45

R

rate statement.....	180
usage guidelines.....	22
relay agents	
DHCP and BOOTP.....	91
relay-agent-option statement.....	181
usage guidelines.....	91
request services flow-collector change-destination	
primary interface command.....	201
request services flow-collector change-destination	
secondary interface command.....	202
request services flow-collector test-file-transfer	
command.....	203
route recording.....	26
route-accounting statement.....	181
usage guidelines.....	39
routers	
DHCP relay agents.....	91
routes, displaying	
in the forwarding table.....	254
routing policies	
configuration tasks.....	72
ECMP flow-based forwarding.....	71, 72
routing-instance statement	
usage guidelines.....	91
run-length statement.....	182
usage guidelines.....	22

S

sample (firewall filter action).....	21
sampled file.....	33, 95
sampled.pkts file.....	24
Sampling	
filename	131
sampling	
next-hop-groups, displaying.....	208
port-mirroring instances, displaying.....	206
sampling statement.....	183
usage guidelines.....	21

server statement	
DHCP and BOOTP service	186
DNS and TFTP service	187
usage guidelines.....	91
server-profile statement	
port mirroring.....	188
show chassis forwarding command.....	204
show chassis hardware command	
usage guidelines.....	19
show forwarding-options next-hop-group	
command.....	208
show forwarding-options port-mirroring	
command.....	206
show interfaces (Flow Monitoring) command.....	211
show interfaces (M Series, MX Series, T Series	
Routers, PTX Series Management and Internal	
Ethernet) command.....	216
show interfaces statistics command.....	232
show passive-monitoring error command.....	244
show passive-monitoring flow command.....	246
show passive-monitoring memory command.....	248
show passive-monitoring status command.....	250
show passive-monitoring usage command.....	252
show route forwarding-table command.....	254
show services accounting aggregation	
command.....	268
show services accounting aggregation template	
command.....	272
show services accounting errors command.....	273
show services accounting flow command.....	277
show services accounting flow-detail	
command.....	282
show services accounting memory command.....	287
show services accounting packet-size-distribution	
command.....	289
show services accounting status command.....	291
show services accounting usage command.....	294
show services flow-collector file interface	
command.....	296
show services flow-collector input interface	
command.....	298
show services flow-collector interface	
command.....	300
size statement	
sampling.....	189
snooping, DHCP.....	97
SONET interfaces	
sampling.....	30
source-checking statement.....	190
stamp option.....	25
stamp statement.....	191
usage guidelines.....	24
statistics	
active flow error.....	273
active flow instances.....	277
active flow memory utilization.....	287
aggregated active flow.....	268
interfaces	
displaying.....	232
support, technical See technical support	
syntax conventions.....	xv
T	
technical support	
contacting JTAC.....	xvii
templates	
flow aggregation.....	272
TFTP	
packet forwarding.....	94
requests, disabling recognition.....	94
tftp statement.....	191
timestamp option.....	25
traceoptions statement	
DNS and TFTP packet forwarding.....	192
port mirroring and traffic sampling.....	194
usage guidelines.....	38
traffic	
accounting.....	40
forwarding	
configuration statements.....	35
overview.....	35
monitoring.....	44
sampling	
disabling.....	24
DNS and TFTP packet forwarding.....	94
flow aggregation.....	26
FTP traffic.....	32
logging information output file.....	33, 60, 95
output files.....	24
run-length parameter.....	22
sampling rate parameter.....	22
SONET interfaces.....	30
traffic from single IP addresses.....	31
traffic sampling	
configuring.....	21
disabling.....	111

V

var/log/sampled file.....	33, 60, 95
var/tmp/sampled.pkts file.....	24
version statement.....	194
usage guidelines.....	26
version9 statement.....	195
usage guidelines.....	29
VPLS.....	78
load balancing across aggregated Ethernet.....	77

W

world-readable statement.....	196
usage guidelines.....	33