

Port Mirroring



Published: 2014-05-02

Juniper Networks, Inc.
1194 North Mathilda Avenue
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.

Port Mirroring

Copyright © 2014, 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	ix
	Documentation and Release Notes	ix
	Supported Platforms	ix
	Using the Examples in This Manual	ix
	Merging a Full Example	x
	Merging a Snippet	x
	Documentation Conventions	xi
	Documentation Feedback	xiii
	Requesting Technical Support	xiii
	Self-Help Online Tools and Resources	xiii
	Opening a Case with JTAC	xiv
Part 1	Overview	
Chapter 1	Port Mirroring	3
	Understanding Port Mirroring	3
Part 2	Configuration	
Chapter 2	Configuration Task	7
	Configuring Port Mirroring	7
	Configuring Tunnels	8
	Port Mirroring with Next-Hop Groups	9
	Configuring Inline Port Mirroring	10
	Filter-Based Forwarding with Multiple Monitoring Interfaces	11
	Restrictions	11
	Configuring Port Mirroring on Services Interfaces	12
	Examples: Configuring Port Mirroring	13
Chapter 3	Examples	21
	Example: Multiple Port Mirroring with Next-Hop Groups Configuration	21
Chapter 4	Configuration Statements	25
	[edit forwarding-options] Hierarchy Level	25
	[edit interfaces] Hierarchy Level	29
	family (Monitoring)	30
	file (Trace Options)	31
	filter	32
	host-outbound	33
	input (Port Mirroring)	33
	interface (Accounting or Sampling)	34
	next-hop (Forwarding Options)	34

	next-hop-group (Forwarding Options)	35
	no-filter-check	35
	output (Port Mirroring)	36
	rate (Forwarding Options)	36
	run-length	37
	size	38
	traceoptions (Forwarding Options)	39
	world-readable	39
Part 3	Administration	
Chapter 5	Port Mirroring Operational Mode Commands	43
	show forwarding-options next-hop-group	44
	show forwarding-options port-mirroring	47
Part 4	Index	
	Index	51

List of Figures

Part 2	Configuration	
Chapter 3	Examples	21
	Figure 1: Active Flow Monitoring—Multiple Port Mirroring with Next-Hop Groups	
	Topology Diagram	21

List of Tables

	About the Documentation ix
	Table 1: Notice Icons xi
	Table 2: Text and Syntax Conventions xii
Part 3	Administration
Chapter 5	Port Mirroring Operational Mode Commands 43
	Table 3: show forwarding-options next-hop-group Output Fields 44
	Table 4: show forwarding-options port-mirroring Output Fields 47

About the Documentation

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

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

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xi 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 xii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

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

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>

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

PART 1

Overview

- [Port Mirroring on page 3](#)

CHAPTER 1

Port Mirroring

- [Understanding Port Mirroring on page 3](#)

Understanding 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.

Related Documentation

- [Configuring Port Mirroring on page 7](#)
- [Example: Multiple Port Mirroring with Next-Hop Groups Configuration on page 21](#)

PART 2

Configuration

- [Configuration Task on page 7](#)
- [Examples on page 21](#)
- [Configuration Statements on page 25](#)

CHAPTER 2

Configuration Task

- [Configuring Port Mirroring on page 7](#)

Configuring Port Mirroring

To prepare traffic for port mirroring, include the **filter** statement at the **[edit firewall family inet]** 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 {  
      port-mirror;  
      accept;  
    }  
  }  
}
```

To configure port mirroring on a logical interface, configure the following statements at the **[edit forwarding-options port-mirroring]** hierarchy level:

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



NOTE: The `input` statement is deprecated at the `[edit forwarding-options port-mirroring family (inet | inet6)]` hierarchy level and is maintained only for backward compatibility. You must include the `input` statement at the `[edit forwarding-options port-mirroring]` hierarchy level.

Specify the port-mirroring destination by including the `next-hop` statement at the `[edit forwarding-options port-mirroring output interface interface-name]` hierarchy level:

`next-hop address;`



NOTE: For IPv4 port mirroring to reach a next-hop destination, you must manually include a static Address Resolution Protocol (ARP) entry in the router configuration.

The `no-filter-check` statement is required when you send port-mirrored traffic to a Tunnel PIC that has a filter applied to it. `en`

The interface used to send the packets to the analyzer is the output interface configured above at the `[edit forwarding-options port-mirroring family (inet | inet6) output]` hierarchy level. You can use any physical interface type, including generic routing encapsulation (GRE) tunnel interfaces. The next-hop address specifies the destination address; this statement is mandatory for non point-to-point interfaces, such as Ethernet interfaces.

To configure the sampling rate or duration, include the `rate` or `run-length` statement at the `[edit forwarding-options port-mirroring input]` hierarchy level.

You can trace port-mirroring operations the same way you trace sampling operations. For more information, see *Tracing Traffic Sampling Operations*.

For more information about port mirroring, see the following sections:

- [Configuring Tunnels on page 8](#)
- [Port Mirroring with Next-Hop Groups on page 9](#)
- [Configuring Inline Port Mirroring on page 10](#)
- [Filter-Based Forwarding with Multiple Monitoring Interfaces on page 11](#)
- [Restrictions on page 11](#)
- [Configuring Port Mirroring on Services Interfaces on page 12](#)
- [Examples: Configuring Port Mirroring on page 13](#)

Configuring Tunnels

In typical applications, you send the sampled packets to an analyzer or a workstation for analysis, rather than another router. If you must send this traffic over a network, you should use tunnels. For more information about tunnel interfaces, see *Tunnel Properties*.

If your router is equipped with a Tunnel PIC, you can forward duplicate packets to multiple interfaces by configuring a next-hop group. 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 address;
  }
}
```

The **interface** statement specifies the interface that sends out sampled information. The **next-hop** statement specifies the next-hop addresses to which to send the sampled information.

Next-hop groups have the following properties:

- Next-hop groups are supported for inet, inet6 and bridge family.
- Next-hop groups are supported on M Series and MX Series routers.
- Next-hop groups support up to 16 next-hop addresses.
- Up to 30 next-hop groups are supported.
- Each next-hop group is expected to have at least two next-hop addresses.

Port Mirroring with Next-Hop Groups

You can configure next-hop groups for MX, TX, and T Series routers using either IP addresses or Layer 2 addresses for the next hops. Use the **group-type [inet | layer-2]** statement at **[edit forwarding-options next-hop-group next-hop-group-name]** hierarchy level to establish the next-hop groups. You can reference more than one port mirroring instance in a filter on MX Series routers. Use the **port-mirror-instance instance-name** statement at the **[edit firewall family family-name filter filter-name term term-name]** to refer to one of several port mirroring instances. For more information about this configuration, see the *Layer 2 Port Mirroring Feature Guide for Routing Devices*.



NOTE: On the Trio chipset for MX series routers, port mirroring instances can only be bound to the FPC level and not up to the PIC level. For MX series routers with a DPC card, both levels are supported.

On MX, TX, and T Series routers only, you can configure port mirroring using next-hop groups, also known as *multipacket port mirroring*, without the presence of a Tunnel PIC. To configure this functionality, include the **next-hop-group** statement at the **[edit forwarding-options port-mirror family inet output]** or **[edit forwarding-options port-mirror instance instance-name family inet output]** hierarchy level:

```
[edit forwarding-options]
port-mirror {
  family inet {
    output {
      next-hop-group group-name;
```

```

    }
  }
}
or
[edit forwarding-options]
port-mirror {
  instance instance-name {
    family (inet | vpls) {
      output {
        next-hop-group group-name;
      }
    }
  }
}

```

You define the next-hop group by including the **next-hop-group** statement at the **[edit forwarding-options]** hierarchy level. For an example, see [“Examples: Configuring Port Mirroring” on page 13](#). This configuration is supported only with IPv4 addresses.

You can disable this configuration by including a **disable** or **disable-all-instances** statement at the **[edit forwarding-options port-mirror]** hierarchy level or by including a **disable** statement at the **[edit forwarding-options port-mirror instance *instance-name*]** hierarchy level. You can display the settings and network status by issuing the **show forwarding-options next-hop-group** and **show forwarding-options port-mirroring** operational commands.



NOTE: If you try to bind any derived instance to the FPC, a commit error will occur.

Configuring Inline Port Mirroring

Inline port mirroring provides you with the ability to specify instances that are not bound to the flexible PIC concentrator (FPC) in the firewall filter's **then port-mirror-instance** action. This way, you are not limited to only two port-mirror instances per FPC. Inline port mirroring decouples the port-mirror destination from the input parameters like **rate**. While the input parameters are programmed in the switch interface board, the next-hop destination of the mirrored packet is available in the packet itself. Inline port mirroring is supported only on Trio-based modular port concentrators (MPCs).

Using inline port mirroring, a port-mirror instance will have an option to inherit input parameters from another instance that specifies it, as shown in the following CLI configuration example:

```

instance pm2 {
  + input-parameters-instance pm1;
  family inet {
    output {
      interface ge-1/2/3.0 {
        next-hop 50.0.0.3;
      }
    }
  }
}

```



```

    }
  }
}

```

Multiple levels of inheritance are not allowed. One instance can be referred by multiple instances. An instance can refer to another instance that is defined before it. Forward references are not allowed and an instance cannot refer to itself, doing so will cause an error during configuration parsing.

The user can specify an instance that is not bound to the FPC in the firewall filter. The specified filter should inherit one of the two instances that have been bound to the FPC. If it does not, the packet is not marked for port-mirroring. If it does, then the packet will be sampled using the input parameters specified by the referred instance but the copy will be sent to the its own destination.

Filter-Based Forwarding with Multiple Monitoring Interfaces

If port-mirrored packets are to be distributed to multiple monitoring or collection interfaces based on patterns in packet headers, it is helpful to configure a filter-based forwarding (FBF) filter on the port-mirroring egress interface.

When an FBF filter is installed as an output filter, a packet that is forwarded to the filter has already undergone at least one route lookup. After the packet is classified at the egress interface by the FBF filter, it is redirected to another routing table for additional route lookup. Obviously, the route lookup in the latter routing table (designated by an FBF routing instance) must result in a different next hop from those from the previous tables the packet has passed through, to avoid packet looping inside the Packet Forwarding Engine.

For more information about FBF configuration, see the *Junos OS Routing Protocols Library for Routing Devices*. For an example of FBF applied to an output interface, see [“Examples: Configuring Port Mirroring” on page 13](#).

Restrictions

The following restrictions apply to port-mirroring configurations:

- 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 **10.68.9.10** and the port-mirrored traffic is sent to **10.68.20.15** for analysis, the device associated with the latter address should not know a route to **10.68.9.10**. Also, it should not send the sampled packets back to the source address.
- IPv4 and IPv6 traffic is supported. For IPv6 port mirroring, you must configure the next-hop router with an IPv6 neighbor before mirroring the traffic, similar to an ARP request for IPv4 traffic. All the restrictions applied to IPv4 configurations should also apply to IPv6.
- On M120 and M320 routers, multiple next-hop mirroring is not supported.

- Because M320 routers do not support multiple bindings of port-mirror instances per FPC, the **port-mirror-instance** action is not supported in firewall filters for these routers.
- On M Series routers other than the M120 and M320 routers, only one family protocol (either IPv4 or IPv6) is supported at a time.
- Port mirroring supports up to 16 next hops, but there is no next-hop group support for **inet6**.
- Only transit data is supported.
- You can configure multiple port-mirroring interfaces per router.
- On routers containing an Internet Processor II application-specific integrated circuit (ASIC), you must include a firewall filter with both the **accept** action and the **port-mirror** action modifier on the inbound interface. Do not include the **discard** action, or port mirroring will not work.
- If the port-mirroring interface is a non-point-to-point interface, you must include an IP address under the **port-mirroring** statement to identify the other end of the link. This IP address must be reachable for you to see the sampled traffic. If the port-mirroring interface is an Ethernet interface, the router should have an Address Resolution Protocol (ARP) entry for it. The following sample configuration sets up a static ARP entry.
- You do not need to configure firewall filters on both inbound and outbound interfaces, but at least one is necessary on the inbound interface to provide the copies of the packets to send to an analyzer.
- Inline port mirroring is supported only on Trio-based MPCs.
- Configuration for both port mirroring and traffic sampling are handled by the same daemon, so in order to view a trace log file for port mirroring, you must configure the **traceoptions** option under traffic sampling.

Configuring Port Mirroring on Services Interfaces

A special situation arises when you configure unit **0** of a services interface (AS or Multiservices PIC) to be the port-mirroring logical interface, as in the following example:

```
[edit forwarding-options]
port-mirroring {
  input {
    rate 1;
  }
  family inet {
    output {
      interface sp-1/0/0.0;
    }
  }
}
```

Since any traffic directed to unit **0** on a services interface is targeted for monitoring (cflowd packets are generated for it), the sample port-mirroring configuration indicates that the customer would like to have cflowd records generated for the port-mirrored traffic.

However, generation of cflowd records requires the following additional configuration; if it is missing, the port-mirrored traffic is simply dropped by the services interface without generating any cflowd packets.

```
[edit forwarding-options]
sampling {
  instance instance1 { # named instances of sampling parameters
    input {
      rate 1;
    }
    family inet {
      output {
        flow-server 172.16.28.65 {
          port 1230;
        }
      }
      interface sp-1/0/0 { # If the port-mirrored traffic requires monitoring, this
                           # interface must be same as that specified in the
                           # port-mirroring configuration.
        source-address 3.1.2.3;
      }
    }
  }
}
```



NOTE: Another way to configure sp-1/0/0 to generate cflowd records is to use only the sampling configuration, but include a firewall filter `sample` action instead of a `port-mirror` action.

Examples: Configuring Port Mirroring

The following example sends port-mirrored traffic to multiple cflowd servers or packet analyzers:

```
[edit interfaces]
ge-1/0/0 { # This is the input interface where packets enter the router.
  unit 0 {
    family inet {
      filter {
        input mirror_pkts; # Here is where you apply the first filter.
      }
      address 10.11.0.1/24;
    }
  }
}
ge-1/1/0 { # This is an exit interface for HTTP packets.
  unit 0 {
    family inet {
      address 10.12.0.1/24;
    }
  }
}
ge-1/2/0 { # This is an exit interface for HTTP packets.
```

```
    unit 0 {
        family inet {
            address 10.13.0.1/24;
        }
    }
}
so-0/3/0 { # This is an exit interface for FTP packets.
    unit 0 {
        family inet {
            address 10.1.1.1/30;
        }
    }
}
so-4/3/0 { # This is an exit interface for FTP packets.
    unit 0 {
        family inet {
            address 10.2.2.2/30;
        }
    }
}
so-7/0/0 { # This is an exit interface for all remaining packets.
    unit 0 {
        family inet {
            address 10.5.5.5/30;
        }
    }
}
so-7/0/1 { # This is an exit interface for all remaining packets.
    unit 0 {
        family inet {
            address 10.6.6.6/30;
        }
    }
}
vt-3/3/0 { # The tunnel interface is where you send the port mirrored traffic.
    unit 0 {
        family inet;
    }
    unit 1 {
        family inet {
            filter {
                input collect_pkts; # This is where you apply the second firewall filter.
            }
        }
    }
}
[edit forwarding-options]
port-mirroring { # This is required when you configure next-hop groups.
    input {
        rate 1; # This rate port mirrors one packet for every one received (1:1 = all
                # packets).
    }
    family inet {
        output { # This sends traffic to a tunnel interface to prepare for multiport mirroring.
            interface vt-3/3/0.1;
            no-filter-check;
        }
    }
}
```

```

    }
  }
}
next-hop-group ftp-traffic { # Point-to-point interfaces require you to specify the interface
  # name only.
  interface so-4/3/0.0;
  interface so-0/3/0.0;
}
next-hop-group http-traffic { # You need to configure a next hop for multipoint interfaces
  # (Ethernet).
  interface ge-1/1/0.0 {
    next-hop 10.12.0.2;
  }
  interface ge-1/2/0.0 {
    next-hop 10.13.0.2;
  }
}
next-hop-group default-collect {
  interface so-7/0/0.0;
  interface so-7/0/1.0;
}
[edit firewall]
family inet {
  filter mirror_pkts { # Apply this filter to the input interface.
    term catch_all {
      then {
        count input_mirror_pkts;
        port-mirror; # This action sends traffic to be copied and port mirrored.
        accept;
      }
    }
  }
  filter collect_pkts { # Apply this filter to the tunnel interface.
    term ftp-term { # This term sends FTP traffic to an FTP next-hop group.
      from {
        protocol ftp;
      }
      then next-hop-group ftp-traffic;
    }
    term http-term { # This term sends HTTP traffic to an HTTP next-hop group.
      from {
        protocol http;
      }
      then next-hop-group http-traffic;
    }
    term default { # This term sends all remaining traffic to a final next-hop group.
      then next-hop-group default-collectors;
    }
  }
}
}

```

The following example demonstrates configuration of filter-based forwarding at the output interface. In this example, the packet flow follows this path:

1. A packet arrives at interface **fe-1/2/0.0** with source and destination addresses **10.50.200.1** and **10.50.100.1**, respectively.
2. The route lookup in routing table **inet.0** points to the egress interface **so-0/0/3.0**.
3. The output filter installed at **so-0/0/3.0** redirects the packet to routing table **fbf.inet.0**.
4. The packet matches the entry **10.50.100.0/25**, and finally leaves the router from interface **so-2/0/0.0**.

```
[edit interfaces]
so-0/0/3 {
  unit 0 {
    family inet {
      filter {
        output fbf;
      }
      address 10.50.10.2/25;
    }
  }
}
fe-1/2/0 {
  unit 0 {
    family inet {
      address 10.50.50.2/25;
    }
  }
}
so-2/0/0 {
  unit 0 {
    family inet {
      address 10.50.20.2/25;
    }
  }
}
[edit firewall]
filter fbf {
  term 0 {
    from {
      source-address {
        10.50.200.0/25;
      }
    }
    then routing-instance fbf;
  }
  term d {
    then count d;
  }
}
[edit routing-instances]
fbf {
  instance-type forwarding;
  routing-options {
```

```

        static {
            route 10.50.100.0/25 next-hop so-2/0/0.0;
        }
    }
}
[edit routing-options]
interface-routes {
    rib-group inet fbf-group;
}
static {
    route 10.50.100.0/25 next-hop 10.50.10.1;
}
rib-groups {
    fbf-group {
        import-rib [ inet.0 fbf.inet.0 ];
    }
}

```

The following example shows configuration of port mirroring using next-hops groups or multipacket port mirroring:

```

forwarding-options {
    next-hop-group inet_nhgc {
        group-type inet;
        interface ge-2/0/2.101 {
            next-hop 10.2.0.2;
        }
        interface ge-2/2/8.2 {
            next-hop 10.8.0.2;
        }
    }
    next-hop-group vpls_nhgc {
        group-type layer-2;
        interface ge-2/0/1.100;
        interface ge-2/2/9.0;
        inactive: next-hop-subgroup vpls_subgc {
            interface ge-2/0/1.101;
            interface ge-2/2/9.1;
        }
    }
    next-hop-group vpls_nhgc_2 {
        group-type layer-2;
        interface ge-2/2/1.100;
        interface ge-2/3/9.0;
    }
}
port-mirror {
    disable-all-instances; /* Disable all port-mirroring instances */
    disable; /* Disable the global instance */
    input {
        rate 10; # start mirroring every 10th packet
        run-length 4; # mirror 4 additional packets
    }
    family inet {
        output {
            next-hop-group inet_nhgc;
        }
    }
}

```

```
}
family vpls {
  output {
    next-hop-group vpls_nhg;
  }
}
instance {
  inst1 {
    disable; /* Disable this instance */
    input {
      rate 1;
      maximum-packet-length 200;
    }
    family inet {
      output {
        next-hop-group inet_nhg;
      }
    }
    family vpls {
      output {
        next-hop-group vpls_nhg_2;
      }
    }
  }
}
}
```

The following example shows configuration of port mirroring using next-hops groups or multipacket port mirroring on a T series router:

```
forwarding-options {
  next-hop-group inet_nhg {
    group-type inet;
    interface so-0/0/0.0; # There is no need for the nexthop address on T series routers
    interface ge-2/0/2.0 {
      next-hop 1.2.3.4
    }
  }
  next-hop-subgroup sub_inet {
    interface so-1/2/0.0;
    interface ge-6/1/2.0 {
      next-hop 6.7.8.9;
    }
  }
  next-hop-group vpls_nhg_2 {
    group-type layer-2;
    interface ge-2/2/1.100;
    interface ge-2/3/9.0;
  }
}
port-mirroring {
  disable-all-instances; /*Disable all port-mirroring instances */
  disable; /* Disable the global instance */
  input {
    rate 10;
    run-length 4;
  }
}
```



```

    }
    family inet {
        output {
            next-hop-group inet_nhg;
        }
    }
    family vpls {
        output {
            next-hop-group vpls_nhg;
        }
    }
    instance {
        inst1 {
            disable; /* Disable this instance */
            input {
                rate 1;
                maximum-packet-length 200;
            }
            family inet {
                output {
                    next-hop-group inet_nhg;
                }
            }
            family vpls {
                output {
                    next-hop-group vpls_nhg_2;
                }
            }
        }
    }
}

```

The following example shows configuration of inline port mirroring using PM1 and PM2 as our port mirror instances.

```

instance {
    pm1 {
        input {
            rate 3;
        }
        family inet {
            output {
                interface ge-1/2/2.0 {
                    next-hop 40.0.0.2;
                }
            }
        }
    }
    pm2 {
        input-parameters-instance pm1;
        family inet {
            output {
                interface ge-1/2/3.0 {
                    next-hop 50.0.0.3;
                }
            }
        }
    }
}

```

```
    }  
  }  
}  
}  
firewall {  
  filter pm_filter {  
    term t1 {  
      then port-mirror-instance pm2;  
    }  
  }  
}  
chassis {  
  fpc 1 {  
    port-mirror-instance pm1;  
  }  
}
```

The packets will be sampled at a rate of 3 and the copy is sent to 50.0.0.3.

**Related
Documentation**

- [Understanding Port Mirroring on page 3](#)
- [Example: Multiple Port Mirroring with Next-Hop Groups Configuration on page 21](#)

CHAPTER 3

Examples

- [Example: Multiple Port Mirroring with Next-Hop Groups Configuration on page 21](#)

Example: Multiple Port Mirroring with Next-Hop Groups Configuration

When you need to analyze traffic containing more than one packet type, or you wish to perform multiple types of analysis on a single type of traffic, you can implement multiple port mirroring and next-hop groups. You can make up to 16 copies of traffic per group and send the traffic to next-hop group members. A maximum of 30 groups can be configured on a router at any given time. The port-mirrored traffic can be sent to any interface, except aggregated SONET/SDH, aggregated Ethernet, loopback (**lo0**), or administrative (**fxp0**) interfaces. To send port-mirrored traffic to multiple flow servers or packet analyzers, you can use the **next-hop-group** statement at the **[edit forwarding-options]** hierarchy level.

Figure 1: Active Flow Monitoring—Multiple Port Mirroring with Next-Hop Groups Topology Diagram

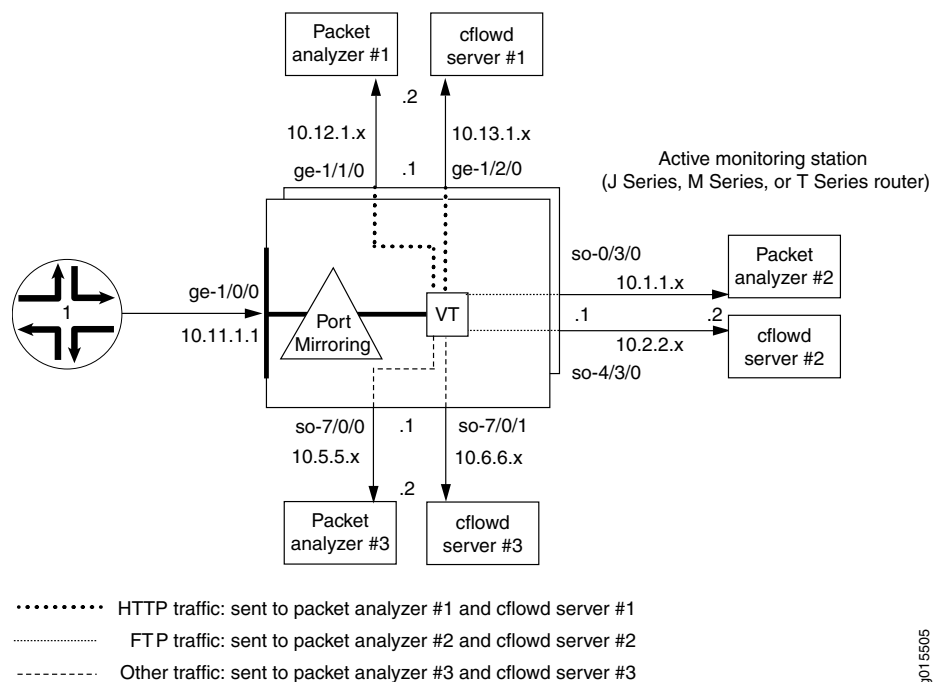


Figure 1 on page 21 shows an example of how to configure multiple port mirroring with next-hop groups. All traffic enters the monitoring router at interface **ge-1/0/0**. A firewall filter counts and port-mirrors all incoming packets to a Tunnel Services PIC. A second filter is applied to the tunnel interface and splits the traffic into three categories: HTTP traffic, FTP traffic, and all other traffic. The three types of traffic are assigned to three separate next-hop groups. Each next-hop group contains a unique pair of exit interfaces that lead to different groups of packet analyzers and flow servers.



NOTE: Instances enabled to mirror packets to different destinations from the same PFE, also use different sampling parameters for each instance. When we configure Layer2 Port-mirroring with both global port-mirroring and instance based port-mirroring, PIC level instances will override FPC level and the FPC level will override the Global instance.

```
[edit]
interfaces {
  ge-1/0/0 { # This is the input interface where packets enter the router.
    unit 0 {
      family inet {
        filter {
          input mirror_pkts; # Here is where you apply the first filter.
        }
        address 10.11.1.1/24;
      }
    }
  }
  ge-1/1/0 { # This is an exit interface for HTTP packets.
    unit 0 {
      family inet {
        address 10.12.1.1/24;
      }
    }
  }
  ge-1/2/0 { # This is an exit interface for HTTP packets.
    unit 0 {
      family inet {
        address 10.13.1.1/24;
      }
    }
  }
  so-0/3/0 { # This is an exit interface for FTP packets.
    unit 0 {
      family inet {
        address 10.1.1.1/30;
      }
    }
  }
  so-4/3/0 { # This is an exit interface for FTP packets.
    unit 0 {
      family inet {
        address 10.2.2.1/30;
      }
    }
  }
}
```

```

    }
  }
  so-7/0/0 { # This is an exit interface for all remaining packets.
    unit 0 {
      family inet {
        address 10.5.5.1/30;
      }
    }
  }
  so-7/0/1 { # This is an exit interface for all remaining packets.
    unit 0 {
      family inet {
        address 10.6.6.1/30;
      }
    }
  }
  vt-3/3/0 { # The tunnel interface is where you send the port-mirrored traffic.
    unit 0 {
      family inet;
    }
    unit 1 {
      family inet {
        filter {
          input collect_pkts; # This is where you apply the second firewall filter.
        }
      }
    }
  }
}
forwarding-options {
  port-mirroring { # This is required when you configure next-hop groups.
    family inet {
      input {
        rate 1; # This port-mirrors all packets (one copy for every packet received).
      }
      output { # Sends traffic to a tunnel interface to enable multipoint mirroring.
        interface vt-3/3/0.1;
        no-filter-check;
      }
    }
  }
  next-hop-group ftp-traffic { # Point-to-point interfaces require you to specify the
    interface so-4/3/0.0; # interface name.
    interface so-0/3/0.0;
  }
  next-hop-group http-traffic { # Configure a next hop for all multipoint interfaces.
    interface ge-1/1/0.0 {
      next-hop 10.12.1.2;
    }
    interface ge-1/2/0.0 {
      next-hop 10.13.1.2;
    }
  }
  next-hop-group default-collect {
    interface so-7/0/0.0;
    interface so-7/0/1.0;
  }
}

```

```
    }
  }
  firewall {
    family inet {
      filter mirror_pkts { # Apply this filter to the input interface.
        term catch_all {
          then {
            count input_mirror_pkts;
            port-mirror; # This action sends traffic to be copied and port-mirrored.
          }
        }
      }
      filter collect_pkts { # Apply this filter to the tunnel interface.
        term ftp-term { # This term sends FTP traffic to an FTP next-hop group.
          from {
            protocol ftp;
          }
          then next-hop-group ftp-traffic;
        }
        term http-term { # This term sends HTTP traffic to an HTTP next-hop group.
          from {
            protocol http;
          }
          then next-hop-group http-traffic;
        }
        term default { # This sends all remaining traffic to a final next-hop group.
          then next-hop-group default-collectors;
        }
      }
    }
  }
}
```

- Related Documentation**
- [Understanding Port Mirroring on page 3](#)
 - [Configuring Port Mirroring on page 7](#)

CHAPTER 4

Configuration Statements

- [\[edit forwarding-options\] Hierarchy Level](#) on page 25
- [\[edit interfaces\] Hierarchy Level](#) on page 29
- [family \(Monitoring\)](#) on page 30
- [file \(Trace Options\)](#) on page 31
- [filter](#) on page 32
- [host-outbound](#) on page 33
- [input \(Port Mirroring\)](#) on page 33
- [interface \(Accounting or Sampling\)](#) on page 34
- [next-hop \(Forwarding Options\)](#) on page 34
- [next-hop-group \(Forwarding Options\)](#) on page 35
- [no-filter-check](#) on page 35
- [output \(Port Mirroring\)](#) on page 36
- [rate \(Forwarding Options\)](#) on page 36
- [run-length](#) on page 37
- [size](#) on page 38
- [traceoptions \(Forwarding Options\)](#) on page 39
- [world-readable](#) on page 39

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

To configure flow monitoring and accounting properties, include the following statements at the **[edit forwarding-options]** hierarchy level:

```
[edit forwarding-options]
accounting name {
  output {
    aggregate-export-interval seconds;
    cflowd hostname {
      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;
}
}
}
monitoring name {
    family family {
        output {
            cflowd hostname port port-number;
            export-format format;
            flow-active-timeout seconds;
            flow-export-destination {
                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;
            }
        }
    }
}
next-hop-group group-names {
    interface interface-name {
        next-hop address;
    }
}
port-mirroring {
    input {
        rate rate;
        run-length number;
        maximum-packet-length bytes
    }
    family (inet | inet6) {
        output {
            interface interface-name {
                next-hop address;
            }
            no-filter-check;
        }
    }
}
traceoptions {
```



```

    file filename {
        files number;
        size bytes;
        (world-readable | no-world-readable);
    }
}
sampling {
    disable;
    sample-once;
    input {
        rate number;
        run-length number;
        max-packets-per-second number;
        maximum-packet-length bytes;
    }
    traceoptions {
        no-remote-trace;
        file filename <files number> <size bytes> <match expression> <world-readable |
        no-world-readable>;
    }
}
family (inet | inet6 | mpls) {
    disable;
    output {
        aggregate-export-interval seconds;
        flow-active-timeout seconds;
        flow-inactive-timeout 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;
            version9 {
                template template-name;
            }
        }
    }
    interface interface-name {
        engine-id number;
        engine-type number;
        source-address address;
    }
    file {
        disable;
        filename filename;
        files number;
    }
}

```

```

        size bytes;
        (stamp | no-stamp);
        (world-readable | no-world-readable);
    }
}
instance instance-name {
    disable;
    input {
        rate number;
        run-length number;
        max-packets-per-second number;
        maximum-packet-length bytes;
    }
    family (inet | inet6 | mpls) {
        disable;
        output {
            aggregate-export-interval seconds;
            flow-active-timeout seconds;
            flow-inactive-timeout 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;
                version9 {
                    template template-name;
                }
            }
        }
        interface interface-name {
            engine-id number;
            engine-type number;
            source-address address;
        }
        inline-jflow {
            source-address address;
            flow-export-rate rate;
        }
    }
}
}
}

```



NOTE: For the complete [edit forwarding-options] hierarchy, see the *Routing Policy Feature Guide for Routing Devices*. This section documents only the statements used in flow monitoring and accounting services.

**Related
Documentation**

- [\[edit interfaces\] Hierarchy Level on page 29](#)
- [\[edit services flow-monitoring\] Hierarchy Level](#)

[edit interfaces] Hierarchy Level

To configure flow monitoring and accounting interfaces, include the following statements at the [edit interfaces] hierarchy level:

```
[edit interfaces]
mo-fpc/pic/port {
  unit logical-unit-number {
    family inet {
      accounting {
        destination-class-usage;
        source-class-usage direction;
      }
    }
    address address {
      destination address;
    }
    filter {
      group filter-group-number;
      input filter-name;
      output filter-name;
    }
    receive-options-packets;
    receive-ttl-exceeded;
    sampling direction;
  }
}
multiservice-options {
  (core-dump | no-core-dump);
  (syslog | no-syslog);
  flow-control-options {
    down-on-flow-control;
    dump-on-flow-control;
    reset-on-flow-control;
  }
}
(at-fpc/pic/port | fe-fpc/pic/port | ge-fpc/pic/port) {
  passive-monitor-mode;
}
so-fpc/pic/port {
  unit logical-unit-number {
    passive-monitor-mode;
  }
}
```

- Related Documentation**
- [\[edit forwarding-options\] Hierarchy Level on page 25](#)
 - [\[edit services flow-monitoring\] Hierarchy Level](#)

family (Monitoring)

Syntax

```
family inet {
  output {
    flow-active-timeout seconds;
    flow-inactive-timeout seconds;
    export-format format;
    cflowd hostname {
      aggregation {
        autonomous-system;
        destination-prefix;
        protocol-port;
        source-destination-prefix {
          caida-compliant;
        }
        source-prefix;
      }
      port port-number;
    }
    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 *name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify input and output interfaces and properties for flow monitoring. Only IPv4 (**inet**) is supported.

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 Flow Monitoring](#)

file (Trace Options)

Syntax	file <i>filename</i> <files <i>number</i> < <i>size bytes</i> > <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">• <i>Tracing Traffic Sampling Operations</i>

filter

Syntax	<pre>filter { input <i>filter-name</i>; output <i>filter-name</i>; group <i>filter-group-number</i>; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Apply a firewall filter to an interface. You can also use filters for encrypted traffic.
Options	<p>group <i>filter-group-number</i>—Define an interface to be part of a filter group. The default filter group number is 0.</p> <p>input <i>filter-name</i>—Name of one filter to evaluate when packets are received on the interface.</p> <p>output <i>filter-name</i>—Name of one filter to evaluate when packets are transmitted on the interface.</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">• <i>Routing Policy Feature Guide for Routing Devices</i> or the <i>Junos OS Administration Library for Routing Devices</i>• <i>Configuring Flow Monitoring</i>

host-outbound

Syntax	host-outbound media-interface;
Hierarchy Level	[edit chassis]
Release Information	Statement introduced in Junos OS Release 13.2 on MX Series 3D Universal Edge Routers.
Description	<p>Enable Layer 2 port mirroring of host-generated outbound packets only on MPCs on MX Series 3D Universal Edge routers.</p> <p>This statement enables all Routing Engine-generated Layer 2 injections to execute egress logical interface filters.</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"> • <i>Examples: Layer 2 Port-Mirroring at Multiple Levels of the Chassis</i> • <i>Configuring Port Mirroring</i> • <i>Layer 2 Port Mirroring Overview</i>

input (Port Mirroring)

Syntax	<pre>input { maximum-packet-length bytes rate number; run-length number; }</pre>
Hierarchy Level	<p>[edit forwarding-options port-mirroring],</p> <p>[edit forwarding-options port-mirroring instance <i>instance-name</i>]</p> <p>[edit forwarding-options port-mirroring family (inet inet6)]</p>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure port mirroring on a logical interface.</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 7

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 <i>name</i> output], [edit forwarding-options sampling family (inet inet6 mpls) output], [edit forwarding-options sampling instance <i>instance-name</i> family (inet inet6 mpls) output]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the output interface for monitored traffic.
Options	<i>interface-name</i> —Name of the interface. 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 Discard Accounting• Configuring Traffic Sampling

next-hop (Forwarding Options)

Syntax	<pre>next-hop <i>address</i>;</pre>
Hierarchy Level	[edit forwarding-options port-mirroring <i>family</i> (inet inet6) output <i>interface interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
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 7

next-hop-group (Forwarding Options)

Syntax	<pre> next-hop-group <i>group-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>It is implicitly assumed that a subgroup is up only if more than one interface in the subgroup is up.</p>
Options	<p><i>address</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-name</i>—Name of next-hop group. Up to 30 next-hop groups are supported for the router. Each next-hop group is expected to have at least two next-hop addresses.</p> <p><i>interface-name</i>—Name of 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 Port Mirroring on page 7

no-filter-check

Syntax	no-filter-check;
Hierarchy Level	[edit forwarding-options port-mirroring family (inet inet6) output]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Disable filter checking on the port-mirroring interface.</p> <p>This statement is required when you send port-mirrored traffic to a Tunnel PIC that has a filter applied to it.</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 7

output (Port Mirroring)

Syntax	<pre>output { interface interface-name { next-hop address; } no-filter-check; }</pre>
Hierarchy Level	[edit forwarding-options port-mirroring family (inet inet6)]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure 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	<ul style="list-style-type: none">• Configuring Port Mirroring on page 7

rate (Forwarding Options)

Syntax	<pre>rate number;</pre>
Hierarchy Level	[edit forwarding-options port-mirroring input], [edit forwarding-options sampling input], [edit forwarding-options sampling instance <i>instance-name</i> input], [edit forwarding-options port-mirroring family (inet inet6) 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 a 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.
Options	number —Denominator of the ratio. Range: 1 through 65,535
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• Configuring Traffic Sampling

run-length

Syntax	<code>run-length <i>number</i>;</code>
Hierarchy Level	<p>[edit forwarding-options port-mirroring input],</p> <p>[edit forwarding-options port-mirroring instance <i>port-mirroring-instance-name</i> input],</p> <p>[edit forwarding-options port-mirroring family (inet inet6) input],</p> <p>[edit forwarding-options sampling input],</p> <p>[edit forwarding-options sampling instance <i>instance-name</i> input]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.</p>
Description	Set the number of samples following the initial trigger event. The configuration enables you to sample packets following those already being sampled.
Options	<p><i>number</i>—Number of samples.</p> <p>Range: 0 through 20</p> <p>Default: 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"> • <i>Applying Filters to Forwarding Tables</i> • Configuring Port Mirroring on page 7 • <i>Configuring Traffic Sampling</i>

size

Syntax	<code>size bytes;</code>
Hierarchy Level	[edit forwarding-options port-mirroring traceoptions file], [edit forwarding-options sampling family (inet inet6 mpls) output file], [edit forwarding-options sampling traceoptions file]
Release Information	Statement introduced before Junos OS Release 7.4.
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 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	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 7• Configuring Traffic Sampling

traceoptions (Forwarding Options)

Syntax	<pre> traceoptions { no-remote-trace; file filename <files number> <size bytes> <match expression> <world-readable no-world-readable>; } </pre>
Hierarchy Level	[edit forwarding-options port-mirroring], [edit forwarding-options sampling]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure traffic sampling tracing operations.</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"> • <i>Tracing Traffic Sampling Operations</i>

world-readable

Syntax	(world-readable no-world-readable);
Hierarchy Level	<p>[edit forwarding-options port-mirroring traceoptions file],</p> <p>[edit forwarding-options sampling family (inet inet6 mpls) output file],</p> <p>[edit forwarding-options sampling traceoptionsfile]</p>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Enable unrestricted file access.
Options	<p>no-world-readable—Restrict file access to owner. This is the default.</p> <p>world-readable—Enable unrestricted file access.</p> <p>Default: no-world-readable</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 7 • <i>Configuring Traffic Sampling</i>

PART 3

Administration

- [Port Mirroring Operational Mode Commands on page 43](#)

CHAPTER 5

Port Mirroring Operational Mode Commands

- `show forwarding-options next-hop-group`
- `show forwarding-options port-mirroring`

show forwarding-options next-hop-group

Syntax	<code>show forwarding-options next-hop-group</code> <code><terse brief detail></code> <code><group-name></code>
Release Information	Command introduced in Junos OS Release 9.6. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Display current state of next-hop groups.
Options	<code>terse brief detail</code> —(Optional) Display the specified level of output. <code>group-name</code> —(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 47
List of Sample Output	show forwarding-options next-hop-group terse on page 45 show forwarding-options next-hop-group brief on page 45 show forwarding-options next-hop-group detail on page 45
Output Fields	Table 3 on page 44 lists the output fields for the <code>show forwarding-options next-hop-group</code> command. Output fields are listed in the approximate order in which they appear.

Table 3: 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 <code>inet</code> or <code>layer-2</code> .	All levels
State	Next-hop group state, either <code>up</code> or <code>down</code> .	All levels
Members Interfaces	Names of interfaces to which next-hop group members belong.	brief detail
Members 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 3: 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
inet_nhg            inet      up
vpls_nhg            layer-2   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: inet_nhg
Type: inet      State: up
Members Interfaces:
  ge-2/0/2.101 next-hop 101.2.0.2

Next-hop-group: vpls_nhg
Type: layer-2   State: up
Members Interfaces:
  ge-2/0/1.100
  ge-2/2/9.0
Members Subgroup: vpls_subg
Members Interfaces:
  ge-2/0/1.101
  ge-2/2/9.1

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: inet_nhg
Type: inet      State: up
Number of members configured      : 2
Number of members that are up    : 1
Number of subgroups configured    : 0
Number of subgroups that are up  : 0
Members Interfaces:              State
  ge-2/0/2.101 next-hop 101.2.0.2  up
  ge-2/2/8.2   next-hop 2.8.0.2    down

Next-hop-group: vpls_nhg
Type: layer-2   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-2/0/1.100                up
    ge-2/2/9.0                  up
Members Subgroup: vpls_subg     up
    Number of members configured : 2
    Number of members that are up : 2
Members Interfaces:
    ge-2/0/1.101                up
    ge-2/2/9.1                  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 forwarding-options port-mirroring

Syntax	show forwarding-options port-mirroring <terse detail> <instance-name>
Release Information	Command introduced in Junos OS Release 9.6. Statement 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	<ul style="list-style-type: none"> • [edit forwarding-options port-mirroring] Hierarchy Level
List of Sample Output	show forwarding-options port-mirroring terse on page 48 show forwarding-options port-mirroring detail on page 48
Output Fields	Table 4 on page 47 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 4: 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
```

PART 4

Index

- [Index on page 51](#)

Index

Symbols

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

B

braces, in configuration statements.....	xii
brackets	
angle, in syntax descriptions.....	xii
square, in configuration statements.....	xii

C

comments, in configuration statements.....	xii
conventions	
text and syntax.....	xi
curly braces, in configuration statements.....	xii
customer support.....	xiii
contacting JTAC.....	xiii

D

documentation	
comments on.....	xiii

F

file statement.....	31
filter statement	
flow monitoring.....	32
flow monitoring	
example configuration	
multiple port mirroring.....	13, 21
next-hop groups.....	13, 21
font conventions.....	xi
forwarding-options statement	
usage guidelines.....	25

H

host-outbound statement.....	33
------------------------------	----

I

interface statement	
flow monitoring	
usage guidelines.....	8

M

manuals	
comments on.....	xiii

N

next-hop groups.....	7
next-hop statement.....	34
next-hop groups	
usage guidelines.....	8
usage guidelines.....	7
next-hop-group statement	
forwarding-options.....	35
usage guidelines.....	7, 8
no-filter-check statement.....	35
usage guidelines.....	7
no-world-readable statement	
flow monitoring.....	39

O

output statement	
port mirroring.....	36

P

parentheses, in syntax descriptions.....	xii
port mirroring.....	7
displaying.....	47
port-mirroring statement	
usage guidelines.....	7

R

rate statement.....	36
usage guidelines.....	7
run-length statement.....	37
usage guidelines.....	7

S

sampling	
next-hop-groups, displaying.....	44
port-mirroring instances, displaying.....	47
show forwarding-options next-hop-group	
command.....	44
show forwarding-options port-mirroring	
command.....	47
size statement.....	38

support, technical See technical support
syntax conventions.....xi

T

technical support
 contacting JTAC.....xiii
traceoptions statement
 flow monitoring.....39

W

world-readable statement
 flow monitoring.....39