



Junos[®] OS

Layer 2 Port Mirroring Feature Guide for Routing Devices

Release
15.1



Modified: 2015-05-27

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 Layer 2 Port Mirroring Feature Guide for Routing Devices

15.1

Copyright © 2015, 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	Introduction to Layer 2 Port Mirroring	3
	Layer 2 Port Mirroring Overview	3
	Layer 2 Port Mirroring Properties	4
	Packet-Selection Properties	4
	Packet Address Family	4
	Mirror Destination Properties	5
	Mirror-Once Option	5
	Layer 2 Port Mirroring Global Instance	5
	Layer 2 Port Mirroring Named Instances	6
	Layer 2 Port Mirroring Named Instances Overview	6
	Mirroring at Ports Grouped at the FPC Level	7
	Mirroring at Ports Grouped at the PIC Level	7
	Mirroring at a Group of Ports Bound to Multiple Named Instances	7
	Layer 2 Port Mirroring Firewall Filters	8
	Layer 2 Port Mirroring Firewall Filters Overview	8
	Mirroring of Packets Received or Sent on a Logical Interface	9
	Mirroring of Packets Forwarded or Flooded to a Bridge Domain	9
	Mirroring of Packets Forwarded or Flooded to a VPLS Routing Instance	10
	Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups	10
Chapter 2	Behavior of Layer 2 Port Mirroring of Logical Interfaces on PE Routers	13
	Layer 2 Port Mirroring of PE Router Logical Interfaces	13
	Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces	15

Part 2	Configuration	
Chapter 3	Layer 2 Port Mirroring Configuration Guidelines	19
	Restrictions on Layer 2 Port Mirroring	19
	Application of Layer 2 Port Mirroring Types	20
	Precedence of Multiple Levels of Layer 2 Port Mirroring on a Physical Interface	23
Chapter 4	Layer 2 Port Mirroring Configuration for Physical Interfaces	25
	Configuring the Global Instance of Layer 2 Port Mirroring	25
	Defining a Named Instance of Layer 2 Port Mirroring	28
	Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level	32
	Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level	34
	Disabling Layer 2 Port Mirroring Instances	35
	Examples: Layer 2 Port-Mirroring at Multiple Levels of the Chassis	36
	Layer 2 Port Mirroring at the FPC Level	37
	Layer 2 Port Mirroring at the PIC Level	37
	Layer 2 Port Mirroring at the FPC and PIC Levels	37
	Example: Layer 2 Port Mirroring with Multiple Instances	38
	Example: Configuring Multiple Instances of Layer 2 Port Mirroring	38
	Explicit Reference of a Port Mirroring Instance	41
	Implicit Reference of Port Mirroring on the Underlying Physical Interface	41
Chapter 5	Layer 2 Port Mirroring Configuration for Logical Interfaces	43
	Defining a Layer 2 Port-Mirroring Firewall Filter	44
	Applying Layer 2 Port Mirroring to a Logical Interface	47
	Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain	50
	Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance	52
	Configuring Protocol-Independent Firewall Filter for Port Mirroring	54
	Example: Layer 2 Port Mirroring at a Logical Interface	55
	Example: Layer 2 Port Mirroring for a Layer 2 VPN	58
	Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links	60
Chapter 6	Layer 2 Port Mirroring Configuration for Multiple Destinations	63
	Defining a Next-Hop Group for Layer 2 Port Mirroring	63
	Example: Layer 2 Port Mirroring to Multiple Destinations	64
Chapter 7	Layer 2 Port Mirroring Configuration Statements	69
	family (Port Mirroring)	70
	interface (Port Mirroring)	71
	input (Port Mirroring)	71
	maximum-packet-length	72
	no-filter-check	73
	output (Port Mirroring)	74
	port-mirroring	75
	rate (Forwarding Options)	77
	run-length	78

Part 3	Administration	
Chapter 8	Displaying Information	81
	Displaying Information About DPCs or FPCs in an MX Series Router	81
	Displaying Layer 2 Port-Mirroring Instance Settings and Status	81
	Displaying Next-Hop Group Settings and Status	82
Chapter 9	Operational Mode Commands for Packet Forwarding Engine Components	83
	show chassis fabric fpcs	84
	show chassis fpc	122
	show chassis hardware	161
	show chassis pic	337
Chapter 10	Operational Mode Commands for Layer 2 Port-Mirroring Instances	353
	show forwarding-options port-mirroring	354
Chapter 11	Operational Mode Commands for Firewall Filter Statistics and Logs	357
	clear firewall	358
	show firewall	360
	show firewall log	367
Chapter 12	Operational Mode Commands for Next-Hop Groups for Layer 2 Port Mirroring	371
	show forwarding-options next-hop-group	372
Part 4	Index	
	Index	377

List of Tables

	About the Documentation ix
	Table 1: Notice Icons xi
	Table 2: Text and Syntax Conventions xi
Part 1	Overview
Chapter 2	Behavior of Layer 2 Port Mirroring of Logical Interfaces on PE Routers 13
	Table 3: Application of Layer 2 Port Mirroring Firewall Filters on PE Routers and PE Switches 14
Part 2	Configuration
Chapter 3	Layer 2 Port Mirroring Configuration Guidelines 19
	Table 4: Application of Layer 2 Port Mirroring Types 21
Part 3	Administration
Chapter 9	Operational Mode Commands for Packet Forwarding Engine Components 83
	Table 5: show chassis fabric fpcs Output Fields 87
	Table 6: show chassis fpc Output Fields 130
	Table 7: Routing Engines Displaying DIMM Information 164
	Table 8: show chassis hardware Output Fields 168
	Table 9: show chassis pic Output Fields 341
Chapter 10	Operational Mode Commands for Layer 2 Port-Mirroring Instances 353
	Table 10: show forwarding-options port-mirroring Output Fields 354
Chapter 11	Operational Mode Commands for Firewall Filter Statistics and Logs 357
	Table 11: show firewall Output Fields 362
	Table 12: show firewall log Output Fields 367
Chapter 12	Operational Mode Commands for Next-Hop Groups for Layer 2 Port Mirroring 371
	Table 13: show forwarding-options next-hop-group Output Fields 372

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:

- 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 xi 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

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

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	<pre>user@host> show chassis alarms</pre> <p>No alarms currently active</p>
<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.	<p>Configure the machine's domain name:</p> <pre>[edit] root@# set system domain-name domain-name</pre>
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 <code>[edit protocols ospf area area-id]</code> 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 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.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.

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

Convention	Description	Examples
> (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 at the Juniper Networks Technical Documentation 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 <https://www.juniper.net/cgi-bin/docbugreport/>.
- 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 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

- [Introduction to Layer 2 Port Mirroring on page 3](#)
- [Behavior of Layer 2 Port Mirroring of Logical Interfaces on PE Routers on page 13](#)

CHAPTER 1

Introduction to Layer 2 Port Mirroring

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Properties on page 4](#)
- [Layer 2 Port Mirroring Global Instance on page 5](#)
- [Layer 2 Port Mirroring Named Instances on page 6](#)
- [Layer 2 Port Mirroring Firewall Filters on page 8](#)
- [Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups on page 10](#)

Layer 2 Port Mirroring Overview

On routing platforms and switches that contain an Internet Processor II ASIC, you can send a copy of any incoming packet from the routing platform or switch to an external host address or a packet analyzer for analysis. This is known as *port mirroring*. In Junos OS Release 9.3 and later, Juniper Networks MX Series 3D Universal Edge Routers in a Layer 2 environment support port mirroring for Layer 2 bridging traffic and virtual private LAN service (VPLS) traffic. In Junos OS Release 9.4 and later, MX Series routers in a Layer 2 environment also support port mirroring for Layer 2 VPN traffic over a circuit cross-connect (CCC) that transparently connects logical interfaces of the same type. In Junos OS Release 12.3R2, Juniper Networks EX Series switches support port mirroring for Layer 2 bridging traffic.

Layer 2 port mirroring enables you to specify the manner in which incoming and outgoing packets at specified ports are monitored and the manner in which copies of selected packets are forwarded to another destination, where the packets can be analyzed. MX Series routers and EX Series switches support Layer 2 port mirroring by performing flow monitoring functions using a class-of-service (CoS) architecture that is in concept similar to, but in particulars different from, other routing platforms and switches.

Like the M120 Multiservice Edge Router and M320 Multiservice Edge Routers, MX Series routers and EX Series switches support port mirroring of IPv4, IPv6, and VPLS packets simultaneously. However, the *Junos OS Layer 2 Switching and Bridging Library for Routing Devices* describes port mirroring only for Layer 2 bridging traffic (**family ethernet-switching**), Layer 2 VPLS traffic (**family vpls**) through an MX Series router, and Layer 2 VPN traffic that passes through a CCC (**family ccc**).

For general information about packet flow within MX Series routers and other routers, see the *Class of Service Feature Guide for Routing Devices*.

In a Layer 3 environment, MX Series routers and EX Series switches support port mirroring of IPv4 (**family inet**) and IPv6 (**family inet6**) traffic. For information about Layer 3 port mirroring, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.

**Related
Documentation**

- [Layer 2 Port Mirroring Properties on page 4](#)
- [Restrictions on Layer 2 Port Mirroring on page 19](#)
- [Application of Layer 2 Port Mirroring Types on page 20](#)
- [Application of Layer 2 Port Mirroring Types on page 20](#)

Layer 2 Port Mirroring Properties

Port mirroring specifies the following types of properties:

- [Packet-Selection Properties on page 4](#)
- [Packet Address Family on page 4](#)
- [Mirror Destination Properties on page 5](#)
- [Mirror-Once Option on page 5](#)

Packet-Selection Properties

The packet-selection properties of Layer 2 port-mirroring specify how the sampled packets are to be selected for mirroring:

- The number of packets in each sample.
- The number of packets to mirror from each sample.
- The length to which mirrored packets are to be truncated.

Packet Address Family

The packet address family type specifies the type of traffic to be mirrored. In a Layer 2 environment, MX Series routers and EX Series switches support port mirroring for the following packet address families:

- Family type **ethernet-switching**—For mirroring VPLS traffic when the physical interface is configured with encapsulation type **ethernet-bridge**.
- Family type **ccc**—For mirroring Layer 2 VPN traffic.
- Family type **vpls**—For mirroring VPLS traffic.



NOTE: In typical applications, you send mirrored packets directly to an analyzer or a workstation for analysis, not to another router or switch. If you must send mirrored packets over a network, you should use tunnels. For Layer 2 VPN implementations, you can use the Layer 2 VPN routing instance type **l2vpn** to tunnel the packets to a remote destination.

For information about configuring a routing instance for Layer 2 VPN, see the *Junos OS VPNs Library for Routing Devices*. For a detailed Layer 2 VPN example configuration, see the *Junos OS, Release 15.1*. For information about tunnel interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*.

Mirror Destination Properties

For a given packet address family, the mirror destination properties of a Layer 2 port-mirroring instance specify how the selected packets are to be sent on a particular physical interface:

- The physical interface on which to send the selected packets.
- Whether filter checking is to be disabled for the mirror destination interface. By default, filter checking is enabled on all



NOTE: If you apply a filter to an interface that is also a Layer 2 port-mirroring destination, a commit failure occurs unless you have disabled filter checking for that mirror destination interface.

Mirror-Once Option

If port mirroring is enabled at both ingress and egress interfaces, you can prevent the MX Series router and an EX Series switch from sending duplicate packets to the same destination (which would complicate the analysis of the mirrored traffic).



NOTE: The mirror-once port-mirroring option is a global setting. The option is independent of the packet selection properties and the packet family type-specific mirror destination properties.

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Restrictions on Layer 2 Port Mirroring on page 19](#)
- [Application of Layer 2 Port Mirroring Types on page 20](#)

Layer 2 Port Mirroring Global Instance

On an MX Series router and on an EX Series switch, you can configure a set of port-mirroring properties that implicitly apply to packets received on all ports in the router (or switch) chassis. This set of port-mirroring properties is the *global instance* of Layer 2 port mirroring for the router or switch.

Within the global instance configuration, you can specify a set of mirror destination properties for each packet address family supported by Layer 2 port mirroring.

For a general description of Layer 2 port-mirroring properties, see “[Layer 2 Port Mirroring Properties](#)” on page 4. For a comparison of the types of Layer 2 port mirroring available

on an MX Series router and on an EX Series switch, see [“Application of Layer 2 Port Mirroring Types” on page 20](#).

**Related
Documentation**

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Configuring the Global Instance of Layer 2 Port Mirroring on page 25](#)
- [Examples: Layer 2 Port-Mirroring at Multiple Levels of the Chassis on page 36](#)
- [Example: Layer 2 Port Mirroring with Multiple Instances on page 38](#)
- [Example: Layer 2 Port Mirroring to Multiple Destinations on page 64](#)

Layer 2 Port Mirroring Named Instances

This topic describes the following information:

- [Layer 2 Port Mirroring Named Instances Overview on page 6](#)
- [Mirroring at Ports Grouped at the FPC Level on page 7](#)
- [Mirroring at Ports Grouped at the PIC Level on page 7](#)
- [Mirroring at a Group of Ports Bound to Multiple Named Instances on page 7](#)

Layer 2 Port Mirroring Named Instances Overview

On an MX Series router, you can define a set of port-mirroring properties that you can explicitly bind to physical ports on the router. This set of port mirroring properties is known as a *named instance* of Layer 2 port mirroring.

You can bind a named instance of Layer 2 port mirroring to physical ports associated with MX Series router Packet Forwarding Engine components at different levels of the router chassis:

- At the FPC level—You can bind a named instance to the physical ports associated with a specific Dense Port Concentrator (DPC) or to the physical ports associated with a specific Flexible Port Concentrator (FPC).
- At the PIC level—You can bind a named instance of port mirroring to a specific Packet Forwarding Engine (on a specific DPC) or to a specific PIC.



NOTE: MX Series routers support DPCs as well as FPCs and PICs. Unlike FPCs, DPCs do not support PICs. In the Junos OS CLI, however, you use FPC and PIC syntax to configure or display information about DPCs and the Packet Forwarding Engines on the DPCs.

The following points summarize the behavior of Layer 2 port mirroring based on named instances:

- The scope of packet selection is determined by the target of the binding—At the ports (or port) bound to a named instance of Layer 2 port mirroring, the router selects input packets according to the packet-selection properties in the named instance.

- The destination of a selected packet is determined by the packet address family—Of the packets selected, the router mirrors only the packets belonging to an address family for which the named instance of Layer 2 port mirroring specifies a set of mirror destination properties. In a Layer 2 environment, MX Series routers support port mirroring of VPLS (**family bridge** or **family vpls**) traffic and Layer 2 VPN traffic with **family ccc**.

For a general description of Layer 2 port-mirroring properties, see “[Layer 2 Port Mirroring Properties](#)” on page 4. For a comparison of the types of Layer 2 port mirroring available on an MX Series router, see “[Application of Layer 2 Port Mirroring Types](#)” on page 20.

Mirroring at Ports Grouped at the FPC Level

On an MX Series router, you can bind a named instance of Layer 2 port mirroring to a specific DPC or FPC installed in the router chassis. The port mirroring properties in the instance are applied to all Packet Forwarding Engines (and their associated ports) on the specified DPC or to all PICs (and their associated ports) installed in the specified FPC. Port mirroring properties that are bound to a DPC or FPC override any port-mirroring properties bound at the global level or the MX Series router chassis.

Mirroring at Ports Grouped at the PIC Level

On an MX Series router, you can bind a named instance of Layer 2 port mirroring to a specific Packet Forwarding Engine or PIC. The port-mirroring properties in that instance are applied to all ports associated with the specified Packet Forwarding Engine or PIC. Port-mirroring properties that are bound to a Packet Forwarding Engine or PIC override any port-mirroring properties bound at the DPC or FPC that contains them.



NOTE: For MX960 routers, there is a one-to-one mapping of Packet Forwarding Engines to Ethernet ports. Therefore, on MX960 routers only, you can configure port-specific bindings of port-mirroring instances.

Mirroring at a Group of Ports Bound to Multiple Named Instances

On an MX Series router, you can apply up to two named instances of Layer 2 port mirroring to the same group of ports within the router chassis. By applying two different port-mirroring instances to the same DPC, FPC, Packet Forwarding Engine, or PIC, you can bind two distinct Layer 2 port mirroring specifications to a single group of ports.



NOTE: You can configure only one global instance of Layer 2 port mirroring on an MX Series router.

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Defining a Named Instance of Layer 2 Port Mirroring on page 28](#)
- [Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level on page 32](#)
- [Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level on page 34](#)

- [Examples: Layer 2 Port-Mirroring at Multiple Levels of the Chassis on page 36](#)
- [Example: Layer 2 Port Mirroring with Multiple Instances on page 38](#)

Layer 2 Port Mirroring Firewall Filters ---

This topic describes the following information:

- [Layer 2 Port Mirroring Firewall Filters Overview on page 8](#)
- [Mirroring of Packets Received or Sent on a Logical Interface on page 9](#)
- [Mirroring of Packets Forwarded or Flooded to a Bridge Domain on page 9](#)
- [Mirroring of Packets Forwarded or Flooded to a VPLS Routing Instance on page 10](#)

Layer 2 Port Mirroring Firewall Filters Overview

On an MX Series router, you can configure a firewall filter *term* to specify that Layer 2 port mirroring is to be applied to all packets at the interface to which the firewall filter is applied.

You can apply a Layer 2 port-mirroring firewall filter to the input or output logical interfaces (including aggregated Ethernet logical interfaces), to traffic forwarded or flooded to a bridge domain, or traffic forwarded or flooded to a VPLS routing instance.

MX Series routers support Layer 2 port mirroring of VPLS (**family bridge** or **family vpls**) traffic and Layer 2 VPN traffic with **family ccc** in a Layer 2 environment

Within a firewall filter **term**, you can specify the Layer 2 port-mirroring properties under the **then** statement in either of the following ways:

- Implicitly reference the Layer 2 port mirroring properties in effect on the port.
- Explicitly reference a particular named instance of Layer 2 port mirroring.



.....
NOTE: When configuring a Layer 2 port-mirroring firewall filter, do not include the optional **from** statement that specifies match conditions based on the route source address. Omit this statement so that all packets are considered to match and all *actions* and *action-modifiers* specified in the **then** statement are taken.

If you want to mirror all incoming packets, then you must not use the **from** statement; /* comment: one configure filter terms with **from** if they are interested in mirroring only a subset of packet.

.....
For a general description of Layer 2 port-mirroring properties, see “[Layer 2 Port Mirroring Properties](#)” on [page 4](#). For a comparison of the types of Layer 2 port mirroring available on an MX Series router, see “[Application of Layer 2 Port Mirroring Types](#)” on [page 20](#).



NOTE: If you associate integrated routing and bridging (IRB) with the bridge domain (or VPLS routing instance), and also configure within the bridge domain (or VPLS routing instance) a forwarding table filter with the `port-mirror` or `port-mirror-instance` action, then the IRB packet is mirrored as a Layer 2 packet. You can disable this behavior by configuring the `no-irb-layer-2-copy` statement in the bridge-domain (or VPLS routing instance).

For a detailed description of how to configure a Layer 2 port-mirroring firewall filter, see [“Defining a Layer 2 Port-Mirroring Firewall Filter” on page 44](#).

For detailed information about how you can use Layer 2 port-mirroring firewall filters with MX Routers configured as provider edge (PE) routers, see [“Layer 2 Port Mirroring of PE Router Logical Interfaces” on page 13](#). For detailed information about configuring firewall filters in general (including in a Layer 3 environment), see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.

Mirroring of Packets Received or Sent on a Logical Interface

To mirror Layer 2 traffic received or sent on a logical interface, apply a port-mirroring firewall filter to the input or output of the interface.

A port-mirroring firewall filter can also be applied to an aggregated-Ethernet logical interface. For details, see [“Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces” on page 15](#).



NOTE: If port-mirroring firewall filters are applied at both the input and output of a logical interface, two copies of each packet are mirrored. To prevent the router from forwarding duplicate packets to the same destination, you can enable the “mirror-once” option for Layer 2 port mirroring in the global instance for the Layer 2 packet address family.

Mirroring of Packets Forwarded or Flooded to a Bridge Domain

To mirror Layer 2 traffic forwarded to or flooded to a bridge domain, apply a port-mirroring firewall filter to the input to the forwarding table or flood table. Any packet received for the bridge domain forwarding or flood table and that matches the filter conditions is mirrored.

For more information about bridge domains, see *Layer 2 Bridge Domains Overview*. For information about flooding behavior in a bridge domain, see *Layer 2 Learning and Forwarding for Bridge Domains Overview*.



NOTE: When you configure port mirroring on any interface under one bridge domain, the mirrored packet can move to an external analyzer located under different bridge domains.

Mirroring of Packets Forwarded or Flooded to a VPLS Routing Instance

To mirror Layer 2 traffic forwarded to or flooded to a VPLS routing instance, apply a port-mirroring firewall filter to the input to the forwarding table or flood table. Any packet received for the VPLS routing instance forwarding or flood table and that matches the filter condition is mirrored.

For more information about VPLS routing instances, see *Configuring a VPLS Routing Instance* and *Configuring VLAN Identifiers for Bridge Domains and VPLS Routing Instances*. For information about flooding behavior in VPLS, see the *Junos OS VPNs Library for Routing Devices*.

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)
- [Example: Layer 2 Port Mirroring at a Logical Interface on page 55](#)
- [Example: Layer 2 Port Mirroring for a Layer 2 VPN on page 58](#)
- [Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links on page 60](#)
- [Example: Layer 2 Port Mirroring to Multiple Destinations on page 64](#)

Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups

On an MX Series router and on an EX Series switch, you can mirror traffic to multiple destinations by configuring next-hop groups in Layer 2 port-mirroring firewall filters applied to tunnel interfaces. The mirroring of packets to multiple destinations is also known as *multipacket port mirroring*.



NOTE: Junos OS Release 9.5 introduced support for Layer 2 port mirroring using next-hop groups on MX Series routers, but required installation of a Tunnel PIC. Beginning in Junos OS Release 9.6, Layer 2 port mirroring using next-hop groups on MX Series routers does not require Tunnel PICs.

On MX Series routers and on EX Series switches, you can define a firewall filter for mirroring packets to a next-hop group. The next-hop group can contain Layer 2 members, Layer 3 members, and subgroups that are either unit list (mirroring packets to each interface) or load-balanced (mirroring packets to one of several interfaces). The MX Series router and the EX Series switch 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.

To enable port mirroring to the members of a next-hop group, you specify the next-hop group as the filter action of a firewall filter, and then you apply the firewall filter to logical tunnel interfaces (**lt-**) or virtual tunnel interfaces (**vt-**) on the MX Series router or on the EX Series switch.



NOTE: The use of subgroups for load-balancing mirrored traffic is not supported.

**Related
Documentation**

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Overview on page 3](#)
- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)
- [Defining a Next-Hop Group for Layer 2 Port Mirroring on page 63](#)
- [Example: Layer 2 Port Mirroring to Multiple Destinations on page 64](#)

CHAPTER 2

Behavior of Layer 2 Port Mirroring of Logical Interfaces on PE Routers

- [Layer 2 Port Mirroring of PE Router Logical Interfaces on page 13](#)
- [Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces on page 15](#)

Layer 2 Port Mirroring of PE Router Logical Interfaces

For an MX Series router or an EX Series switch configured as a provider edge (PE) router or PE switch on the customer-facing edge of a service provider network, you can apply a Layer 2 port-mirroring firewall filter at the following ingress and egress points to mirror the traffic between the MX Series router (or an EX Series switch) and customer edge (CE) devices, such as routers and Ethernet switches.

[Table 3 on page 14](#) describes the ways in which you can apply Layer 2 port-mirroring firewall filters to an MX Series router or an EX Series switch configured as a PE router or PE switch.

Table 3: Application of Layer 2 Port Mirroring Firewall Filters on PE Routers and PE Switches

Point of Application	Scope of Mirroring	Notes	Configuration Details
Ingress Customer-Facing Logical Interface	Packets originating within a service provider customer's network, sent first to a CE device, and sent next to an MX Series router or an EX Series switch acting as a PE router or PE switch.	<p>You can also configure aggregated Ethernet interfaces between CE devices and PE routers or PE switches for VPLS routing instances. Traffic is load-balanced across all of the links in the aggregated interface.</p> <p>Traffic received on an aggregated Ethernet interface is forwarded over a different interface based on a lookup of the destination MAC (DMAC) address:</p> <ul style="list-style-type: none"> • Packets destined for a local site are sent out of the load-balanced child interface. • Packets destined for the remote site are encapsulated and forwarded over a label-switched path (LSP). 	<p>See “Applying Layer 2 Port Mirroring to a Logical Interface” on page 47.</p> <p>For more information about VPLS routing instances, see <i>Configuring a VPLS Routing Instance</i> and <i>Configuring VLAN Identifiers for Bridge Domains and VPLS Routing Instances</i>.</p>
Egress Customer-Facing Logical Interface	<p>Unicast packets being forwarded by the MX Series router or the EX Series switch to another PE router or PE switch.</p> <p>NOTE: If you apply a port-mirroring filter to the output for a logical interface, only unicast packets are mirrored. To mirror multicast, unknown unicast, and broadcast packets, apply a filter to the input to the flood table of a bridge domain or VPLS routing instance.</p>		See “Applying Layer 2 Port Mirroring to a Logical Interface” on page 47.
Input to a Bridge Domain Forwarding Table or Flood Table	Forwarding traffic or flood traffic sent to the bridge domain from a CE device.	Forwarding and flood traffic typically consists of broadcast packets, multicast packets, unicast packets with an unknown destination MAC address, or packets with a MAC entry in the DMAC routing table.	See “Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain” on page 50. For information about flooding behavior in VPLS, see the <i>Junos OS VPNs Library for Routing Devices</i> .
Input to a VPLS Routing Instance Forwarding Table or Flood Table	Forwarding traffic or flood traffic sent to the VPLS routing instance from a CE device.		See “Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance” on page 52. For information about flooding behavior in VPLS, see the <i>Junos OS VPNs Library for Routing Devices</i> .

Related Documentation

- [Layer 2 Port Mirroring Overview](#) on page 3
- [Layer 2 Port Mirroring Firewall Filters](#) on page 8
- [Defining a Layer 2 Port-Mirroring Firewall Filter](#) on page 44
- [Example: Layer 2 Port Mirroring at a Logical Interface](#) on page 55

Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces

An aggregated Ethernet interface is a virtual aggregated link that consists of a set of physical interfaces of the same speed and operating in full-duplex link connection mode. You can configure aggregated Ethernet interfaces between CE devices and PE routers for VPLS routing instances. Traffic is load-balanced across all of the links in the aggregated interface. If one or more links in the aggregated interface fails, the traffic is switched to the remaining links.

You can apply a Layer 2 port-mirroring firewall filter to an aggregated Ethernet interface to configure port-mirroring at the parent interface. However, if any child interfaces are bound to different Layer 2 port-mirroring instances, packets received at the child interfaces will be mirrored to the destinations specified by their respective port-mirroring instances. Thus, multiple child interfaces can mirror packets to multiple destinations.

For example, suppose the parent aggregated Ethernet interface instance **ae0** has two child interfaces:

- **xe-2/0/0**
- **xe-3/1/2**

Suppose that these child interfaces on **ae0** are bound to two different Layer 2 port-mirroring instances:

- **pm_instance_A**—A named instance of Layer 2 port-mirroring, bound to child interface **xe-2/0/0**.
- **pm_instance_B**—A named instance of Layer 2 port-mirroring, bound to child interface **xe-3/1/2**.

Now suppose you apply a Layer 2 port-mirroring firewall filter to the Layer 2 traffic sent on **ae0.0** (logical unit **0** on the aggregated Ethernet interface instance **0**). This enables port mirroring on **ae0.0**, which has the following effect on the processing of traffic received on the child interfaces for which Layer 2 port-mirroring properties are specified:

- The packets received on **xe-2/0/0.0** are mirrored to the output interfaces configured in port-mirroring instance **pm_instance_A**.
- The packets received on **xe-3/1/2.0** are mirrored to the output interfaces configured in port-mirroring instance **pm_instance_B**.

Because **pm_instance_A** and **pm_instance_B** can specify different packet-selection properties or mirror destination properties, the packets received on **xe-2/0/0.0** and **xe-3/1/2.0** can mirror different packets to different destinations.

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Firewall Filters on page 8](#)
- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)
- [Example: Layer 2 Port Mirroring for a Layer 2 VPN on page 58](#)

PART 2

Configuration

- [Layer 2 Port Mirroring Configuration Guidelines on page 19](#)
- [Layer 2 Port Mirroring Configuration for Physical Interfaces on page 25](#)
- [Layer 2 Port Mirroring Configuration for Logical Interfaces on page 43](#)
- [Layer 2 Port Mirroring Configuration for Multiple Destinations on page 63](#)
- [Layer 2 Port Mirroring Configuration Statements on page 69](#)

CHAPTER 3

Layer 2 Port Mirroring Configuration Guidelines

- [Restrictions on Layer 2 Port Mirroring on page 19](#)
- [Application of Layer 2 Port Mirroring Types on page 20](#)
- [Precedence of Multiple Levels of Layer 2 Port Mirroring on a Physical Interface on page 23](#)

Restrictions on Layer 2 Port Mirroring

The following restrictions apply to Layer 2 port mirroring:

- Only Layer 2 transit data (packets that contain chunks of data transiting the routing platform as they are forwarded from a source to a destination) can be mirrored. Layer 2 local data (packets that contain chunks of data that are destined for or sent by the Routing Engine, such as Layer 2 control packets) can be mirrored by configuring **set chassis host-outbound media-interface**.
- If you apply a port-mirroring filter to the output of a logical interface, only unicast packets are mirrored. To mirror broadcast packets, multicast packets, unicast packets with an unknown destination media access control (MAC) address, or packets with MAC entry in the destination MAC (DMAC) routing table, apply a filter to the input to the flood table of a bridge domain or virtual private LAN service (VPLS) routing instance.



NOTE: This is restricted only for DPCs. For MX Series routers with MPCs and MICs, both unicast and multicast packets can be mirrored.

- The **family** any mirroring is supported in logical systems starting with Junos OS 13.2 and can be achieved by creating a **port-mirroring** instance under the **[edit forwarding-options]** hierarchy and applying **family** any filter on an interface belonging to logical systems.
- The mirror destination device should be on a dedicated bridge domain and should not participate in any bridging activity: The mirror destination device should not have a bridge to the ultimate traffic destination, and the mirror destination device should not send the mirrored packets back to the source address.

- For either the global port-mirroring instance or a named port-mirroring instance, you can configure only one mirror output interface per port-mirroring instance and packet address family. If you include more than one **interface** statement under the **family (bridge | ccc | vpls) output** statement, the previous **interface** statement is overridden.

- Layer 2 port-mirroring firewall filtering is supported for logical systems.

In a Layer 2 port-mirroring firewall filter definition, the filter **action-modifier (port-mirror)** relies on port-mirroring properties defined in the global instance or named instances of Layer 2 port mirroring, which are configured under the **[edit forwarding-options port-mirroring]** hierarchy. However, the firewall filter with a port-mirror action can be applied to an interface belonging to a logical system, thereby enabling port mirroring of the interface within the logical system.

- For a Layer 2 port mirroring firewall filter in which you implicitly reference Layer 2 port mirroring properties by including the **port-mirror** statement, if multiple named instances of Layer 2 port mirroring are bound to the underlying physical interface, then only the first binding in the stanza (or the only binding) is used at the logical interface. This is done mainly for backward compatibility.
- Layer 2 port-mirroring firewall filters support the use of next-hop subgroups for load-balancing mirrored traffic.
- If a **family ccc** mirror destination is a Logical Tunnel (**lt-**) interface hosted on a DPC and that **lt-** interface also has a **firewall filter** with action **next-hop-group** applied that redirects packets to MPC interfaces, then port-mirror instances must be created at the **[edit forwarding options port-mirroring instance]** with **family ccc output interface** destination of a **next-hop-group** member interface. One port-mirroring instance will be needed for each member interface in the **next-hop-group**. These port-mirroring instances do not need to be used anywhere in the configuration.

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Application of Layer 2 Port Mirroring Types on page 20](#)
- [Precedence of Multiple Levels of Layer 2 Port Mirroring on a Physical Interface on page 23](#)
- [Layer 2 Port Mirroring of PE Router Logical Interfaces on page 13](#)
- [Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces on page 15](#)

Application of Layer 2 Port Mirroring Types

You can apply different sets of Layer 2 port-mirroring properties to the VPLS packets at different ingress or egress points of an MX Series route.

[Table 4 on page 21](#) describes the three types of Layer 2 port mirroring you can configure on an MX Series router: the global instance, named instances, and firewall filters.

Table 4: Application of Layer 2 Port Mirroring Types

Type of Layer2PortMirroring Definition	Point of Application	Scope of Mirroring	Description	Configuration Details
Global Instance of Layer2PortMirroring	All ports in the MX Series router chassis	VPLS packets received on all ports in the MX Series router chassis	If configured, the global port-mirroring properties implicitly apply to all VPLS packets received on all ports in the router chassis.	See “Configuring the Global Instance of Layer 2 Port Mirroring” on page 25
Named Instance of Layer2PortMirroring	Ports grouped at the FPC level See “Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level” on page 32.	VPLS packets received on ports associated with a specific DPC or FPC and its Packet Forwarding Engines.	Overrides any port-mirroring properties configured by the global port-mirroring instance.	See “Defining a Named Instance of Layer 2 Port Mirroring” on page 28. NOTE: The number of port-mirroring destinations supported for an MX Series router is limited to the number of Packet Forwarding Engines contained on the DPCs installed in the router chassis.
	Ports grouped at the PIC level See “Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level” on page 34.	VPLS packets received on ports associated with a specific Packet Forwarding Engine.	Overrides any port-mirroring properties configured at the FPC level or in the global port-mirroring instance.	

Table 4: Application of Layer 2 Port Mirroring Types (*continued*)

Type of Layer2PortMirroring Definition	Point of Application	Scope of Mirroring	Description	Configuration Details
Layer2Port-Mirroring Firewall Filter	Logical interface (including an aggregated Ethernet interface)	VPLS packets received or sent on a logical interface.	In the firewall filter configuration, include <i>action</i> and <i>action-modifier</i> terms to apply to the packets selected for mirroring: <ol style="list-style-type: none"> The accept action is recommended. Specify port mirroring by Including one of the following modifiers: <ul style="list-style-type: none"> The port-mirror modifier implicitly references the port-mirroring properties currently bound to the underlying physical interfaces. The port-mirror-instance <i>pm-instance-name</i> modifier explicitly references a named instance of port mirroring. (Optional) For tunnel interface input packets only, to mirror the packets to additional destinations, include the next-hop-group <i>next-hop-group-name</i> modifier. This modifier references a next-hop-group that specifies the next-hop addresses (for sending additional copies of packets to an analyzer). 	See “ Defining a Layer 2 Port-Mirroring Firewall Filter ” on page 44. NOTE: Layer 2 port-mirroring firewall filters are not supported for logical systems. For mirroring tunnel interface input packets to multiple destinations, also see “ Defining a Next-Hop Group for Layer 2 Port Mirroring ” on page 63.
	Bridge domain forwarding table or flood table	Layer 2 traffic forwarded or flooded to a bridge domain		
	VPLS routing instance forwarding table or flood table	Layer 2 traffic forwarded or flooded to a VPLS routing instance		

- Related Documentation**
- [Layer 2 Port Mirroring Overview on page 3](#)
 - [Restrictions on Layer 2 Port Mirroring on page 19](#)
 - [Precedence of Multiple Levels of Layer 2 Port Mirroring on a Physical Interface on page 23](#)
 - [Layer 2 Port Mirroring of PE Router Logical Interfaces on page 13](#)
 - [Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces on page 15](#)

Precedence of Multiple Levels of Layer 2 Port Mirroring on a Physical Interface

You can bind different sets of Layer 2 port mirroring properties (the global instance and one or more named instances) at various levels of an MX Series router or of an EX Series switch chassis (at the chassis level, at the FPC level, or at the PIC level). Therefore, it is possible for a single group of physical interfaces to be bound to multiple Layer 2 port mirroring definitions.

If a group of ports (or, in the case of a PIC-level binding in an MX960 router, a single port) is bound to multiple Layer 2 port mirroring definitions, the router (or switch) applies the Layer 2 port-mirroring properties to those ports as follows:

1. **Chassis-level port-mirroring properties implicitly apply to all ports in the chassis.** If an MX Series router or an EX Series switch is configured with the global port-mirroring instance, those port mirroring properties apply to all ports. See [“Configuring the Global Instance of Layer 2 Port Mirroring” on page 25](#).
2. **FPC-level port-mirroring properties override chassis-level properties.** If a DPC or FPC is bound to a named instance of port mirroring, those port mirroring properties apply to all ports associated with that DPC or FPC, overriding any port mirroring properties bound at the chassis level. See [“Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level” on page 32](#).
3. **PIC-level port-mirroring properties override FPC-level properties.** If a Packet Forwarding Engine or PIC is bound to a named instance of port mirroring, those port mirroring properties apply to all ports associated with the Packet Forwarding Engine or PIC, overriding any port mirroring properties bound to those ports at the FPC level. See [“Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level” on page 34](#).

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Restrictions on Layer 2 Port Mirroring on page 19](#)
- [Application of Layer 2 Port Mirroring Types on page 20](#)
- [Layer 2 Port Mirroring of PE Router Logical Interfaces on page 13](#)
- [Layer 2 Port Mirroring of PE Router Aggregated Ethernet Interfaces on page 15](#)

CHAPTER 4

Layer 2 Port Mirroring Configuration for Physical Interfaces

- [Configuring the Global Instance of Layer 2 Port Mirroring on page 25](#)
- [Defining a Named Instance of Layer 2 Port Mirroring on page 28](#)
- [Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level on page 32](#)
- [Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level on page 34](#)
- [Disabling Layer 2 Port Mirroring Instances on page 35](#)
- [Examples: Layer 2 Port-Mirroring at Multiple Levels of the Chassis on page 36](#)
- [Example: Layer 2 Port Mirroring with Multiple Instances on page 38](#)

Configuring the Global Instance of Layer 2 Port Mirroring

On an MX Series router, you can configure a set of Layer 2 port-mirroring properties that implicitly apply to packets received on all ports in the router chassis.

To configure the global instance of Layer 2 port mirroring on an MX Series router:

1. Enable configuration of the Layer 2 port mirroring:

```
[edit]  
user@host# edit forwarding-options port-mirroring
```
2. Enable configuration of the packet-selection properties:

```
[edit forwarding-options port-mirroring]  
user@host# edit input
```

3. Specify global-level packet-selection properties.

a. Specify the number of packets to select:

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

The valid range is 1 through 65535.

b. Specify the number of packets to mirror from each selection:

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

The valid range is 0 through 20. The default value is 0.

c. Specify the length to which mirrored packets are to be truncated:

```
[edit forwarding-options port-mirroring input]  
user@host# set maximum-packet-length number
```

For MX-Series devices 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.

4. Specify the global-level Layer 2 address-type family from which traffic is to be selected for mirroring:

```
[edit forwarding-options port-mirroring input]  
user@host# up  
[edit forwarding-options port-mirroring]  
user@host# edit family family
```

The value of the *family* option can be **bridge**, **ccc**, or **vpls**.



NOTE: Under the [edit forwarding-options port-mirroring] hierarchy level, the protocol family statement **family bridge** is an alias for **family vpls**. The command-line interface (CLI) displays Layer 2 port-mirroring configurations as **family vpls**, even for Layer 2 port-mirroring configured as **family bridge**. Use **family bridge** when the physical interface is configured with **encapsulation ethernet-bridge**.

5. Enable configuration of global-level mirror destination properties for this address family:

```
[edit forwarding-options port-mirroring family family]  
user@host# edit output
```

6. Specify global-level mirror destination properties for this address family.

- a. Specify the physical interface on which to send the mirrored packets:

```
[edit forwarding-options port-mirroring family family output]
user@host# set interface interface-name
```

You can also specify an integrated routing and bridging (IRB) interface as the output interface.

- b. (Optional) Allow configuration of filters on the destination interface for the named port-mirroring instance:

```
[edit forwarding-options port-mirroring family family output]
user@host# set no-filter-check
```

7. (Optional) Specify that any packets selected for mirroring are to be mirrored only once to any mirroring destination:

```
[edit forwarding-options port-mirroring family family output]
user@host# up 2
[edit forwarding-options port-mirroring]
user@host# set mirror-once
```



TIP: Enable the mirror-once option when an MX Series router is configured to perform Layer 2 port mirroring at both ingress and egress interfaces, which could result in sending duplicate packets to the same destination (which would complicate the analysis of the mirrored traffic).

8. Verify the minimum configuration of the global instance of Layer 2 port mirroring:

```
[edit forwarding-options ... ]
user@host# top
[edit]
user@host# show forwarding-options
```

```
forwarding-options {
  port-mirroring {
    input { # Global packet-selection properties.
      maximum-packet-length number; # Default is 0.
      rate number;
      run-length number;
    }
    family (ccc | vpls) { # Address- type 'bridge' displays as 'vpls'.
      output { # Global mirror destination properties.
        interface interface-name;
        no-filter-check; # Optional. Allow filters on interface.
      }
    }
    mirror-once; # Optional. Mirror destinations do not receive duplicate packets.
  }
}
```

**Related
Documentation**

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Global Instance on page 5](#)
- [Examples: Layer 2 Port-Mirroring at Multiple Levels of the Chassis on page 36](#)
- [Example: Layer 2 Port Mirroring with Multiple Instances on page 38](#)

Defining a Named Instance of Layer 2 Port Mirroring

On an MX Series router, you can define a set of Layer 2 port-mirroring properties that you can bind to a particular Packet Forwarding Engine (at the PIC level of the router chassis) or to group of Packet Forwarding Engines (at the DPC or FPC level of the route chassis).

To define a named instance of Layer 2 port mirroring on an MX Series router:

1. Enable configuration of a named instance of Layer 2 port mirroring :

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

2. Enable configuration of the packet-sampling properties:

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

3. Specify packet-selection properties:

a. Specify the number of packets to select:

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

The valid range is 1 through 65535.

b. Specify the number of packets to mirror from each selection:

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

The valid range is 0 through 20. The default value is 0.



NOTE: The `run-length` statement is not supported on MX80 routers.

c. Specify the length to which mirrored packets are to be truncated:

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

For MX-Series devices 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.



NOTE: The `maximum-packet-length` statement is not supported on MX80 routers.

4. Enable configuration of the mirror destination properties for Layer 2 packets that are part of bridging domain, Layer 2 switching cross-connects, or virtual private LAN service (VPLS):

a. Specify the Layer 2 address family type of traffic to be mirrored:

```
[edit forwarding-options port-mirroring instance pm-instance-name input]
user@host# up
[edit forwarding-options port-mirroring instance pm-instance-name]
user@host# edit family family
```

The value of the *family* option can be **bridge**, **ccc**, or **vpls**.



NOTE: Under the [edit forwarding-options port-mirroring] hierarchy level, the protocol family statement family bridge is an alias for family vpls. The command-line interface (CLI) displays Layer 2 port-mirroring configurations as family vpls, even for Layer 2 port-mirroring configured as family bridge. Use family bridge when the physical interface is configured with encapsulation ethernet-bridge.

- b. Enable configuration of the mirror destination properties:

```
[edit forwarding-options port-mirroring instance pm-instance-name family family]  
user@host# edit output
```

5. Specify mirror destination properties.

- a. Specify the physical interface on which to send the mirrored packets:

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

- b. (Optional) Allow configuration of filters on the destination interface for the global port-mirroring instance:

```
[edit forwarding-options port-mirroring instance pm-instance-name family family  
output]  
user@host# set no-filter-check
```



NOTE: You cannot configure port mirroring instances on MX80 routers. You can only configure port mirroring at the global level on MX80 routers.

6. (Optional) Specify that any packets selected for mirroring are to be mirrored only once to any mirroring destination:

```
[edit forwarding-options port-mirroring instance pm-instance-name family family  
output]  
user@host# up 3  
[edit forwarding-options port-mirroring]  
user@host# set mirror-once
```



TIP: Enable the global mirror-once option when an MX Series router is configured to perform Layer 2 port mirroring at both ingress and egress interfaces, which could result in sending duplicate packets to the same destination (which in turn would complicate the analysis of the mirrored traffic).

7. To configure a mirroring destination for a different packet family type, repeat steps 4 through 6.

8. Verify the minimum configuration of the named instances of Layer 2 port mirroring:

```
[edit forwarding-options ... ]
user@host# top
[edit]
user@host# show forwarding-options

forwarding-options {
  port-mirroring {
    ... optional-global-port-mirroring-configuration ...
    instance {
      pm-instance-name ( # A named instance of port mirroring
        input { # Packet-selection properties
          maximum-packet-length number; # Default is 0.
          rate number;
          run-length number;
        }
        family (ccc | vpls) { # Address- type 'bridge' displays as 'vpls'.
          output { # Mirror destination properties
            interface interface-name;
            no-filter-check; # Optional. Allow filters on interface.
          }
        }
      }
    }
    mirror-once; # Optional. Mirror destinations do not receive duplicate packets.
  }
}
```

**Related
Documentation**

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Named Instances on page 6](#)
- [Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level on page 32](#)
- [Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level on page 34](#)
- [Examples: Layer 2 Port-Mirroring at Multiple Levels of the Chassis on page 36](#)
- [Example: Layer 2 Port Mirroring with Multiple Instances on page 38](#)

Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level

On an MX Series router and on an EX Series switch, you can bind a named instance of Layer 2 port mirroring to a specific DPC or to a specific FPC in the router (or switch) chassis. This is known as binding a named instance of Layer 2 port mirroring *at the FPC level* of the router (or switch) chassis. The port mirroring properties specified in the named instance are applied to all physical ports associated with all Packet Forwarding Engines on the specified DPC or FPC.



NOTE: You can also bind a named instance of Layer 2 port mirroring to a specific Packet Forwarding Engine on a DPC or FPC in the router (or switch) chassis.

For any packet-type family supported by Layer 2 port mirroring

- Port mirroring properties bound to a specific DPC or FPC override any port-mirroring properties configured at the global level.
- Port mirroring properties bound to a specific Packet Forwarding Engine override any port-mirroring properties configured at the DPC or FPC level.

You can apply up to two named instances of Layer 2 port mirroring to the same group of ports within the router (or switch) chassis. By applying two different port-mirroring instances to the same DPC or FPC, you can bind two distinct Layer 2 port mirroring specifications to a single group of ports.

Before you begin, complete the following tasks:

- Define a named instance of Layer 2 port mirroring. See [“Defining a Named Instance of Layer 2 Port Mirroring” on page 28](#).
- Display information about the number and types of DPCs or FPCs in the MX Series router and in the EX Series switch, the number of Packet Forwarding Engines on each, and the number and types of ports per Packet Forwarding Engine. See [“Displaying Information About DPCs or FPCs in an MX Series Router” on page 81](#).

To bind a named instance of Layer 2 port-mirroring to a DPC or FPC and its Packet Forwarding Engines:

1. Enable configuration of the router (or switch) chassis properties:

```
[edit]
user@host# edit chassis
```

2. Enable configuration of a DPC (and its corresponding Packet Forwarding Engines) or an FPC (and its installed PICs):

```
[edit chassis]
user@host# edit fpc slot-number
```

3. Bind a named instance of Layer 2 port mirroring (*pm-instance-name*) to the DPC or FPC:

```
[edit chassis fpc slot-number]
user@host# set port-mirror-instance pm-instance-name
```

4. (Optional) To bind a second named instance of Layer 2 port mirroring to the same DPC or FPC, repeat step 3 and specify a different named instance of Layer 2 port mirroring.
5. Verify the minimum configuration of the binding:

```
[edit chassis fpc slot-number port-mirror-instance pm-instance-name]
user@host# top
[edit]
user@host# show chassis

chassis {
  fpc slot-number { # Bind two port mirroring named instances at the FPC level.
    port-mirror-instance pm-instance-name-1;
    port-mirror-instance pm-instance-name-2;
  }
}
```

**Related
Documentation**

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Named Instances on page 6](#)
- [Defining a Named Instance of Layer 2 Port Mirroring on page 28](#)
- [Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level on page 34](#)
- [Examples: Layer 2 Port-Mirroring at Multiple Levels of the Chassis on page 36](#)
- [Example: Layer 2 Port Mirroring with Multiple Instances on page 38](#)

Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level

On an MX Series router and on an EX Series switch, you can bind a named instance of Layer 2 port mirroring to the ports associated with a specific Packet Forwarding Engine (on a DPC) or to the ports associated with a specific PIC (installed in an FPC). This is known as binding a named instance of Layer 2 port mirroring *at the PIC level* of the router (or switch) chassis. The port-mirroring properties specified in the named instance are applied to all physical ports associated with the specified Packet Forwarding Engine.



NOTE: You can also bind a named instance of Layer 2 port mirroring to a specific DPC or FPC in the router (or switch) chassis.

For any packet-type family supported by Layer 2 port mirroring:

- Port mirroring properties bound to a specific Packet Forwarding Engine override any port-mirroring properties configured at the DPC or FPC level.
- Port mirroring properties bound to a specific DPC or FPC override any port-mirroring properties configured at the global level.

You can apply up to two named instances of Layer 2 port mirroring to the same group of ports within the router (or switch) chassis. By applying two different port-mirroring instances to the same Packet Forwarding Engine or PIC, you can bind two distinct Layer 2 port mirroring specifications to a single group of ports.

For MX960 routers, there is a one-to-one mapping of Packet Forwarding Engines to Ethernet ports. Therefore, on MX960 routers only, you can bind a named instance of Layer 2 port mirroring to a *specific port* by binding the instance to the Packet Forwarding Engine associated with the port.

Before you begin, complete the following tasks:

- Define a named instance of Layer 2 port mirroring. See [“Defining a Named Instance of Layer 2 Port Mirroring” on page 28](#).
- Display information about the number and types of DPCs in the MX Series router or in the EX Series switch, the number of Packet Forwarding Engines on each DPC, and the number and types of ports per Packet Forwarding Engine. See [“Displaying Information About DPCs or FPCs in an MX Series Router” on page 81](#).

To bind a named instance of Layer 2 port-mirroring to a Packet Forwarding Engine:

1. Enable configuration of the router (or switch) chassis properties:

```
[edit]
user@host# edit chassis
```

2. Enable configuration of a Packet Forwarding Engine or PIC:

```
[edit chassis]
user@host# edit fpc slot-number
```

```
user@host# edit pic slot-number
```

3. Bind a named instance of Layer 2 port mirroring (*pm-instance-name*) to the Packet Forwarding Engine or PIC:

```
[edit chassis fpc slot-number pic slot-number]
user@host# set port-mirror-instance pm-instance-name
```

4. (Optional) To bind a second named instance of Layer 2 port mirroring to the same Packet Forwarding Engine or PIC, repeat step 3 and specify a different named instance of Layer 2 port mirroring.
5. Verify the minimum configuration of the binding:

```
[edit forwarding-options ... ]
user@host# top
[edit]
user@host# show chassis
chassis {
  fpc slot-number {
    ... optional-binding-of-a-port-mirroring-instance-at-the-dpc-level ...
    pic slot-number { # Bind two port-mirroring named instances at the PIC level.
      port-mirror-instance pm-instance-name-1;
      port-mirror-instance pm-instance-name-2;
    }
  }
}
```

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Named Instances on page 6](#)
- [Defining a Named Instance of Layer 2 Port Mirroring on page 28](#)
- [Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level on page 32](#)
- [Examples: Layer 2 Port-Mirroring at Multiple Levels of the Chassis on page 36](#)
- [Example: Layer 2 Port Mirroring with Multiple Instances on page 38](#)

Disabling Layer 2 Port Mirroring Instances

You can disable the global instance of Layer 2 port mirroring, a particular named instance, or all instances of port mirroring:

- To disable the global instance of Layer 2 port mirroring, include the **disable** statement at the **[edit forwarding-options port-mirroring]** hierarchy level:

```
[edit]
forwarding-options {
  port-mirroring {
    disable; Disables the global instance of Layer 2 port mirroring.
    ..global-instance-of-layer-2-port-mirroring-configuration...
  }
}
```

- To disable the definition of a particular named instance of Layer 2 port mirroring, include the **disable** statement at the **[edit forwarding-options port-mirroring instance instance-name]** hierarchy level:

```
[edit]
forwarding-options {
  port-mirroring {
    ...optional-configuration-of-the-global-instance-of-layer-2-port-mirroring...
    instance {
      port-mirroring-instance-name {
        disable; Disables this named instance of Layer 2 port mirroring.
        ...definition-of-a-named-instance-of-layer-2-port-mirroring...
      }
    }
  }
}
```

- To disable the global instance and all named instances of Layer 2 port mirroring, include the **disable-all-instances** statement at the **[edit forwarding-options port-mirroring]** hierarchy level:

```
[edit]
forwarding-options {
  port-mirroring {
    disable-all-instances; Disables all instances of Layer 2 port mirroring.
    ...optional-configuration-of-the-global-instance-of-layer-2-port-mirroring...
    instance {
      port-mirroring-instance-name {
        ...definition-of-a-named-instance-of-layer-2-port-mirroring...
      }
    }
  }
}
```

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Global Instance on page 5](#)
- [Layer 2 Port Mirroring Named Instances on page 6](#)
- [Displaying Layer 2 Port-Mirroring Instance Settings and Status on page 81](#)

Examples: Layer 2 Port-Mirroring at Multiple Levels of the Chassis

On an MX Series router or on an EX Series switch, you can apply named instances of Layer 2 port mirroring at the FPC or DPC level of the chassis or at the PIC level of the chassis. However, you can configure (and implicitly apply) only one global instance of Layer 2 port mirroring to the entire chassis.

- [Layer 2 Port Mirroring at the FPC Level on page 37](#)
- [Layer 2 Port Mirroring at the PIC Level on page 37](#)
- [Layer 2 Port Mirroring at the FPC and PIC Levels on page 37](#)

Layer 2 Port Mirroring at the FPC Level

In this example configuration of an MX Series router or of an EX Series switch chassis, a named instance of Layer 2 port mirroring (**pm1**) is bound to physical ports grouped at the FPC level:

```
[edit]
chassis {
  fpc 2 {
    port-mirror-instance pm1;
  }
}
```

This is not a complete configuration. The physical interfaces associated with the FPC or DPC in slot 2 must be configured at the **[edit interfaces]** hierarchy level. The Layer 2 port mirroring named instance **pm1** must be configured at the **[edit forwarding-options port-mirroring instance]** hierarchy level.

Layer 2 Port Mirroring at the PIC Level

In this example configuration of an MX Series router or of an EX Series switch chassis, a named instance of Layer 2 port mirroring (**pm2**) is bound to the physical ports grouped at the PIC level:

```
[edit]
chassis {
  fpc 2 {
    pic 0 {
      port-mirror-instance pm2;
    }
  }
}
```

This is not a complete configuration. The physical interfaces associated with the FPC or DPC in slot 2 must be configured at the **[edit interfaces]** hierarchy level. The Layer 2 port mirroring named instance **pm2** must be configured at the **[edit forwarding-options port-mirroring instance]** hierarchy level.

Layer 2 Port Mirroring at the FPC and PIC Levels

In this example configuration of an MX Series router chassis or an EX Series switch, one named instance of Layer 2 port mirroring (**pm1**) is applied at the FPC level of the router (or switch) chassis. A second named instance (**pm2**) is applied at the PIC level:

```
[edit]
chassis {
  fpc 2 {
    port-mirror-instance pm1;
    pic 0 {
      port-mirror-instance pm2;
    }
  }
}
```

This is not a complete configuration. Physical interfaces associated with the FPC or DPC in slot 2, including physical interfaces associated with **pic 0**, must be configured at the

[[edit interfaces](#)] hierarchy level. The Layer 2 port mirroring named instances **pm1** and **pm2** must be configured at the [[edit forwarding-options port-mirroring instance](#)] hierarchy level.

**Related
Documentation**

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Global Instance on page 5](#)
- [Layer 2 Port Mirroring Named Instances on page 6](#)
- [Configuring the Global Instance of Layer 2 Port Mirroring on page 25](#)
- [Defining a Named Instance of Layer 2 Port Mirroring on page 28](#)

Example: Layer 2 Port Mirroring with Multiple Instances

Because you can configure more than one port-mirroring instance, care is required when specifying which instance is meant. This topic contains the following information:

- [Example: Configuring Multiple Instances of Layer 2 Port Mirroring on page 38](#)
- [Explicit Reference of a Port Mirroring Instance on page 41](#)
- [Implicit Reference of Port Mirroring on the Underlying Physical Interface on page 41](#)

Example: Configuring Multiple Instances of Layer 2 Port Mirroring

This configuration example illustrates the configuration of Layer 2 port mirroring at the physical interfaces associated with FPC 2, PIC 0 and at two logical interfaces on one of those ports.

At the physical interface levels of the router chassis, two named instances of port mirroring are configured and then bound to the group of physical ports associated with FPC 2, PIC 0.

At two of the logical interfaces on physical interface **ge-2/0/1**, two Layer 2 port-mirroring firewall filters are applied to the input traffic. One filter *explicitly* references the port mirroring properties specified in one of the named instances of port mirroring. The other filter *implicitly* references the port mirroring properties in effect on the underlying physical interface **ge-2/0/1**.

The resulting configuration is an example of the relationships that can exist between multiple instances of Layer 2 port mirroring applied to an MX Series router.

1. Configure two named instances of Layer 2 port mirroring (**pm_instance_1** and **pm_instance_2**), and include mirror destination properties for bridge domain traffic (**family bridge**):

```
[edit]
forwarding-options {
  port-mirroring {
    instance {
      pm_instance_1 {
        input {
          ... packet-selection-properties-configuration ...
        }
      }
    }
  }
}
```

```

    }
    family bridge {
        ... mirror-destination-properties-configuration ...
    }
}
pm_instance_2 {
    input {
        ... packet-selection-properties-configuration ...
    }
    family bridge {
        ... mirror-destination-properties-configuration ...
    }
}
}
}
}
}

```



NOTE: In this example, no global port-mirroring properties are configured on the router.

2. Apply the Layer 2 port mirroring instances to the same group of ports in the router chassis. In this example, the named instances of Layer 2 port mirroring are applied to the same group of physical interfaces specified at the PIC level of the chassis:

```

[edit]
chassis {
    fpc 2 {
        pic 0 {
            port-mirror-instance pm_instance_1;
            port-mirror-instance pm_instance_2;
        }
    }
}

```

Note that, in this example, two named instances of Layer 2 port mirroring are bound to the PIC level of the chassis at the same group of ports.

3. Configure two Layer 2 port-mirroring firewall filters, both for bridge-domain traffic and with one of the filters explicitly referencing one of the named instances of Layer 2 port mirroring:

- Configure the filter **pm_filter_1** to use the Layer 2 port-mirroring properties configured in the named port-mirroring instance **pm_instance_1**. To refer to the Layer 2 port mirroring properties configured in a particular named instance of port mirroring, use the **port-mirror-instance *port-mirroring-instance-name*** statement.
- Configure the filter **pm_filter_2** to use the Layer 2 port mirroring properties in effect on the underlying physical interface of the logical interface to which the filter is applied. To refer to the Layer 2 port mirroring properties in effect on the underlying physical interface, use the **port-mirror** statement. If two instances of port mirroring are bound to that port, then the firewall filter uses the first instance bound within the **[edit chassis fpc slot-number]** or **[edit chassis fpc slot-number pic slot-number]** hierarchy level.

```

[edit]
firewall {

```

```

family bridge {
  filter pm_filter_1 {
    term pm {
      then port-mirror-instance pm_instance_1;
    }
  }
  filter pm_filter_2 {
    term pm {
      then port-mirror;
    }
  }
}

```



NOTE: Because the `port-mirror` filter action modifier relies on the port-mirroring properties defined at the `[edit forwarding-options port-mirroring]` hierarchy level, the `port-mirror` filter action is not supported for logical systems.

4. Apply the two Layer 2 port-mirroring firewall filters to logical interfaces on interface `ge-2/0/1`:

```

[edit]
interfaces {
  ge-2/0/1 {
    flexible-vlan-tagging;
    encapsulation ethernet-bridge;
    unit 0 {
      vlan-id 201;
      family bridge {
        filter { # Explicitly references a named instance of port mirroring.
          input pm_filter_1;
        }
      }
    }
    unit 1 {
      vlan-id 202;
      family bridge {
        filter { # Implicitly references the underlying port mirroring.
          input pm_filter_2;
        }
      }
    }
  }
}

```

Explicit Reference of a Port Mirroring Instance

On logical interface **ge-2/0/1.0**, the **port-mirror-instance** statement explicitly references the Layer 2 port mirroring properties in the named instance **pm_instance_1**. In this example, the port mirroring properties specified in **pm_instance_1** remain in effect at logical interface **ge-2/0/1.0** under the following conditions:

- The firewall filter **pm_filter_1** remains configured (as shown in step 3).
- The named instance **pm_instance_1** remains configured (as shown in step 1).

Even if the named instance **pm_instance_1** is no longer configured or no longer bound to the router chassis at FPC 2, PIC 0, the port mirroring properties specified in **pm_instance_1** remain in effect at logical interface **fe-2/0/1.0** through firewall filter **pm_filter_1**.

Implicit Reference of Port Mirroring on the Underlying Physical Interface

On logical interface **ge-2/0/1.1**, the **port-mirror** statement implicitly references the Layer 2 port mirroring properties in effect at the underlying physical interface **ge-2/0/1**. In this example, the port mirroring properties specified in **pm_instance_2** remain in effect at the ports associated with FPC 2, PIC 0 under the following conditions:

- The firewall filter **pm_filter_2** remains configured (as shown in step 3).
- The named instance **pm_instance_2** remains configured (as shown in step 1).
- The named instance **pm_instance_2** remains bound to the router chassis at FPC 2, PIC 0 (as shown in step 2).

If you disable the named instance **pm_instance_2** or delete its binding to the physical ports associated with FPC 2, PIC 0, then—if global Layer 2 port mirroring properties had been configured—the global port mirroring properties would be used at logical interface **ge-2/0/1.1** through firewall filter **pm_filter_2**.



NOTE: There is a limitation to a Layer 2 port mirroring firewall filter in which you implicitly reference Layer 2 port mirroring properties by including the **port-mirror** statement. If multiple named instances of Layer 2 port mirroring are bound to the underlying physical interface, then only the first binding in the stanza (or the only binding) is used at the logical interface. This is done mainly for backward compatibility.

In the example above, filter **pmff_bd_filter_2** uses the **port-mirror** statement, and so the filter action uses the mirroring properties of the first port mirroring instance applied to the router chassis at the **[edit chassis fpc 2 pic 0]** hierarchy level, which is the instance **pm_instance_1**.

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Named Instances on page 6](#)
- [Layer 2 Port Mirroring Firewall Filters on page 8](#)

- [Defining a Named Instance of Layer 2 Port Mirroring on page 28](#)
- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)

CHAPTER 5

Layer 2 Port Mirroring Configuration for Logical Interfaces

- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)
- [Applying Layer 2 Port Mirroring to a Logical Interface on page 47](#)
- [Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain on page 50](#)
- [Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance on page 52](#)
- [Configuring Protocol-Independent Firewall Filter for Port Mirroring on page 54](#)
- [Example: Layer 2 Port Mirroring at a Logical Interface on page 55](#)
- [Example: Layer 2 Port Mirroring for a Layer 2 VPN on page 58](#)
- [Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links on page 60](#)

Defining a Layer 2 Port-Mirroring Firewall Filter

For virtual private LAN service (VPLS) traffic (**family bridge** or **family vpls**) and for Layer 2 VPNs with family **cccon** MX Series routers and on EX Series switches only, you can define a firewall filter that specifies Layer 2 port mirroring as the action to be performed if a packet matches the conditions configured in the firewall filter term

You can use a Layer 2 port-mirroring firewall filter in the following ways:

- To mirror packets received or sent on a logical interface.
- To mirror packets forwarded or flooded to a bridge domain.
- To mirror packets forwarded or flooded to a VPLS routing instance.
- To mirror tunnel interface input packets only to multiple destinations.

For a summary of the three types of Layer 2 port-mirroring you can configure on an MX Series router, see [“Application of Layer 2 Port Mirroring Types” on page 20](#).

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

To define a firewall filter with a Layer 2 port-mirroring action:

1. Enable configuration of firewall filters for Layer 2 packets that are part of a bridge domain, a Layer 2 switching cross-connect, or a virtual private LAN service (VPLS):

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

The value of the **family** option can be **bridge**, **ccc**, or **vpls**.

2. Enable configuration of a firewall filter **pm-filter-name**:

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

3. Enable configuration of a firewall filter term **pm-filter-term-name**:

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

For more information about firewall filter terms in general (including in a Layer 3 environment), see *Guidelines for Configuring Firewall Filters* in the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.

4. (Optional) Specify the firewall filter match conditions based on the route source address *only if* you want to mirror a subset of the sampled packets.

For information about configuring firewall filter match conditions in general (including in a Layer 3 environment), 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*.

- For detailed information about Layer 2 bridging firewall filter match conditions (which are supported on MX Series routers only), see *Firewall Filter Match Conditions for Layer 2 Bridging Traffic*.
- For detailed information about VPLS firewall filter match conditions, see *Firewall Filter Match Conditions for VPLS Traffic*.
- For detailed information about Layer 2 circuit cross-connect (CCC) firewall filter match conditions, see *Firewall Filter Match Conditions for Layer 2 CCC Traffic*.



NOTE: If you want all sampled packets to be considered to match (and be subjected to the actions specified in the **then** statement), then omit the **from** statement altogether.

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

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

6. Specify the actions to be taken on matching packets:

```
[edit firewall family family filter pm-filter-name term pm-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.

7. Specify Layer 2 port mirroring or a next-hop group as the **action-modifier**:

- To reference the Layer 2 port mirroring properties currently in effect for the Packet Forwarding Engine or PIC associated with the underlying physical interface, use the **port-mirror** statement:

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

- To reference the Layer 2 port mirroring properties configured in a specific named instance, use the **port-mirror-instance** *pm-instance-name* action modifier:

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

If the underlying physical interface is not bound to a named instance of Layer 2 port mirroring but instead is implicitly bound to the global instance of Layer 2 port mirroring, then traffic at the logical interface is mirrored according to the properties

specified in the named instance referenced by the **port-mirror-instance** action modifier.

- 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** *pm-next-hop-group-name* action modifier:

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

For configuration information about next-hop groups, see [“Defining a Next-Hop Group for Layer 2 Port Mirroring” on page 63](#). If you specify a next-hop group for Layer 2 port mirroring, the firewall filter term applies to the tunnel interface input only.

8. Verify the minimum configuration of the Layer 2 port-mirroring firewall filter:

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

family (bridge | ccc | mpls | vpls) { # Type of packets to mirror
  filter pm-filter-name { # Firewall filter name
    term pm-filter-term-name {
      from { # Do not specify match conditions based on route source address
      }
      then {
        action; # Recommended action is 'accept'
        action-modifier; # Three options for Layer 2 port mirroring
      }
    }
  }
}
```

In the firewall filter term **then** statement, the *action-modifier* can be **port-mirror**, **port-mirror-instance** *pm-instance-name*, or **next-hop-group** *pm-next-hop-group-name*.

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Firewall Filters on page 8](#)
- [Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups on page 10](#)
- [Example: Layer 2 Port Mirroring at a Logical Interface on page 55](#)
- [Example: Layer 2 Port Mirroring for a Layer 2 VPN on page 58](#)
- [Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links on page 60](#)
- [Example: Layer 2 Port Mirroring to Multiple Destinations on page 64](#)

Applying Layer 2 Port Mirroring to a Logical Interface

You can apply a Layer 2 port-mirroring firewall filter to the input or to the output of a logical interface, including an aggregated Ethernet logical interface. Only packets of the address-type family specified by the filter action are mirrored.

Before you begin, complete the following task:

- Define a Layer 2 port-mirroring firewall filter to be applied to the input to a logical interface or output to a logical interface. For details, see [“Defining a Layer 2 Port-Mirroring Firewall Filter”](#) on page 44.



NOTE: This configuration task shows two Layer 2 port-mirroring firewall filters: one filter applied to the logical interface ingress traffic, and one filter applied to the logical interface egress traffic.

To apply a Layer 2 port-mirroring firewall filter to an input or output logical interface:

1. Configure the underlying physical interface for the logical interface.
 - a. Enable configuration of the underlying physical interface:

```
[edit]
user@host# edit interfaces interface-name
```



NOTE: A port-mirroring firewall filter can also be applied to an aggregated-Ethernet logical interface.

- b. For Fast Ethernet and Gigabit Ethernet interfaces and aggregated Ethernet interfaces configured for VPLS, enable the reception and transmission of 802.1Q VLAN-tagged frames on the interface:

```
[edit interfaces interface-name]
user@host# set vlan-tagging
```

- c. For Ethernet interfaces that have IEEE 802.1Q VLAN tagging and bridging enabled and that must accept packets carrying TPID 0x8100 or a user-defined TPID, set the logical link-layer encapsulation type:

```
[edit interfaces interface-name]
user@host# set encapsulation extended-vlan-bridge
```

2. Configure the logical interface to which you want to apply a Layer 2 port-mirroring firewall filter.
 - a. Specify the logical unit number:

```
[edit interfaces interface-name]
user@host# edit unit logical-unit-number
```

- b. For a Fast Ethernet, Gigabit Ethernet, or Aggregated Ethernet interface, bind an 802.1Q VLAN tag ID to the logical interface:

```
[edit interfaces interface-name unit logical-unit-number]
user@host# set vlan-id number
```

3. Enable specification of an input or output filter to be applied to Layer 2 packets that are part of bridging domain, Layer 2 switching cross-connects, or virtual private LAN service (VPLS).

- If the filter is to be evaluated when packets are received on the interface:

```
[edit interfaces interface-name unit logical-unit-number]
user@host# set family family filter input pm-filter-name-a
```

- If the filter is to be evaluated when packets are sent on the interface:

```
[edit interfaces interface-name unit logical-unit-number]
user@host# set family family filter output pm-filter-name-b
```

The value of the *family* option can be **bridge**, **ccc**, or **vpls**.



NOTE: If port-mirroring firewall filters are applied at both the input and output of a logical interface, two copies of each packet are mirrored. To prevent the router from forwarding duplicate packets to the same destination, include the optional **mirror-once** statement at the [edit forwarding-options] hierarchy level.

4. Verify the minimum configuration for applying a named Layer 2 port mirroring firewall filter to a logical interface:

```
[edit interfaces interface-name unit logical-unit-number family family filter ... ]
user@host# top
[edit]
user@host# show interfaces
```

```
interfaces {
  interface-name {
    vlan-tagging;
    encapsulation extended-vlan-bridge;
    unit number { # Apply a filter to the input of this interface
      vlan-id number;
      family (bridge | ccc | vpls) {
        filter {
          input pm-filter-for-logical-interface-input;
        }
      }
    }
    unit number { # Apply a filter to the output of this interface
      vlan-id number;
      family (bridge | ccc | vpls) {
        filter {
          output pm-filter-for-logical-interface-output;
        }
      }
    }
  }
}
```

```
    }  
  }  
}
```

**Related
Documentation**

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Firewall Filters on page 8](#)
- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)
- [Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain on page 50](#)
- [Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance on page 52](#)
- [Example: Layer 2 Port Mirroring at a Logical Interface on page 55](#)
- [Example: Layer 2 Port Mirroring for a Layer 2 VPN on page 58](#)
- [Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links on page 60](#)

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain

You can apply a Layer 2 port-mirroring firewall filter to traffic being forwarded or flooded to a bridge domain. Only packets of the specified family type and forwarded or flooded to that bridge domain are mirrored.

Before you begin, complete the following task:

- Define a Layer 2 port-mirroring firewall filter to be applied to the traffic being forwarded to a bridge domain or flooded to a bridge domain. For details, see “[Defining a Layer 2 Port-Mirroring Firewall Filter](#)” on page 44.



NOTE: This configuration task shows two Layer_2 port-mirroring firewall filters: one filter applied to the bridge domain forwarding table ingress traffic, and one filter applied to the bridge domain flood table ingress traffic.

To apply a Layer 2 port-mirroring firewall filter to the forwarding table or flood table of a bridge domain:

1. Enable configuration of the bridge domain **bridge-domain-name** to which you want to apply a Layer 2 port-mirroring firewall filter for forwarded or flooded traffic:

- For a bridge domain:

```
[edit]
user@host# edit bridge-domains bridge-domain-name
```

- For a bridge domain under a routing instance:

```
[edit]
user@host# edit routing-instances routing-instance-name bridge-domains
bridge-domain-name
user@host# set instance-type virtual-switch
```

For more detailed configuration information, see *Configuring a VPLS Routing Instance*.

2. Configure the bridge domain:

```
[edit]
user@host# set domain-type bridge
user@host# set interface interface-name
user@host# set routing-interface routing-interface-name
```

For more detailed configuration information, see *Configuring a Bridge Domain* and *Configuring VLAN Identifiers for Bridge Domains and VPLS Routing Instances*.

3. Enable configuration of traffic forwarding on the bridge domain:

```
[edit ... bridge-domains bridge-domain-name]
user@host# edit forwarding-options
```

4. Apply a Layer 2 port-mirroring firewall filter to the bridge domain forwarding table or flood table.

- To mirror packets being forwarded to the bridge domain:

```
[edit ... bridge-domains bridge-domain-name forwarding-options]
user@host# set filter input pm-filter-for-bd-ingress-forwarded
```

- To mirror packets being flooded to the bridge domain:

```
[edit ... bridge-domains bridge-domain-name forwarding-options]
user@host# set flood input pm-filter-for-bd-ingress-flooded
```

5. Verify the minimum configuration for applying a Layer 2 port-mirroring firewall filter to the forwarding table or flood table of the bridge domain.

- a. Navigate to the hierarchy level at which the bridge domain is configured:

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

- b. Display the bridge domain configurations:

```
user@host# show bridge domains
```

```
bridge-domains {
  bridge-domain-name {
    instance-type virtual-switch; # For a bridge domain under a routing instance.
    domain-type bridge;
    interface interface-name;
    forwarding-options {
      filter { # Mirror ingress forwarded traffic
        input pm-filter-for-bd-ingress-forwarded;
      }
      flood { # Mirror ingress flooded traffic
        input pm-filter-for-bd-ingress-flooded;
      }
    }
  }
}
```

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Firewall Filters on page 8](#)
- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)
- [Applying Layer 2 Port Mirroring to a Logical Interface on page 47](#)
- [Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance on page 52](#)
- [Example: Layer 2 Port Mirroring at a Logical Interface on page 55](#)
- [Example: Layer 2 Port Mirroring for a Layer 2 VPN on page 58](#)
- [Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links on page 60](#)

Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance

You can apply a Layer 2 port-mirroring firewall filter to traffic being forwarded or flooded to a VPLS routing instance. Only packets of the specified family type and forwarded or flooded to that VPLS routing instance are mirrored.

Before you begin, complete the following task:

- Define a Layer 2 port-mirroring firewall filter to be applied to the traffic being forwarded to a VPLS routing instance or flooded to a bridge domain. For details, see [“Defining a Layer 2 Port-Mirroring Firewall Filter” on page 44](#).



NOTE: This configuration task shows two Layer_2 port-mirroring firewall filters: one filter applied to the VPLS routing instance forwarding table ingress traffic, and one filter applied to the VPLS routing instance flood table ingress traffic.

To apply a Layer 2 port-mirroring firewall filter to the forwarding table or flood table of a VPLS routing instance:

1. Enable configuration of the VPLS routing instance to which you want to apply a Layer 2 port-mirroring firewall filter for forwarded or flooded traffic:

```
[edit]
user@host# edit routing-instances routing-instance-name
user@host# set instance-type vpls
user@host# set interface interface-name
user@host# set route-distinguisher (as-number:number | ip-address:number)
user@host# set vrf-import [policy-names]
user@host# set vrf-export [policy-names]
user@host# edit protocols vpls
user@host@ ... vpls-configuration ...
```

For more detailed configuration information, see *Configuring a VPLS Routing Instance*.

2. Enable configuration of traffic forwarding on the VPLS routing instance:

```
[edit routing-instances routing-instance-name protocols vpls]
user@host# up 2
[edit routing-instances routing-instance-name]
user@host# edit forwarding-options
```

3. Apply a Layer 2 port-mirroring firewall filter to the VPLS routing instance forwarding table or flood table.

- To mirror packets being forwarded to the VPLS routing instance:

```
[edit routing-instances routing-instance-name forwarding-options]
user@host# set filter input pm-filter-for-vpls-ri-forwarded
```

- To mirror packets being flooded to the VPLS routing instance:

```
[edit routing-instances routing-instance-name forwarding-options]
user@host# set flood input pm-filter-for-vpls-ri-flooded
```

4. Verify the minimum configuration for applying a Layer 2 port-mirroring firewall filter to the forwarding table or flood table of the VPLS routing instance:

```
[edit routing-instances routing-instance-name forwarding-options]
user@host# top
[edit]
user@host# show routing-instances
```

```
routing-instances {
  routing-instance-name {
    instance-type vpls;
    interface interface-name;
    route-distinguisher (as-number:number | ip-address:number);
    vrf-import [policy-names];
    vrf-export [policy-names];
    protocols {
      vpls {
        ...vpls-configuration...
      }
    }
    forwarding-options {
      family vpls {
        filter { # Mirror ingress forwarded traffic
          input pm-filter-for-vpls-ri-forwarded;
        }
        flood { # Mirror ingress flooded traffic
          input pm-filter-for-vpls-ri-flooded;
        }
      }
    }
  }
}
```

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Firewall Filters on page 8](#)
- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)
- [Applying Layer 2 Port Mirroring to a Logical Interface on page 47](#)
- [Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a Bridge Domain on page 50](#)
- [Example: Layer 2 Port Mirroring at a Logical Interface on page 55](#)
- [Example: Layer 2 Port Mirroring for a Layer 2 VPN on page 58](#)
- [Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links on page 60](#)

Configuring Protocol-Independent Firewall Filter for Port Mirroring

On MX Series routers with MPCs, you can configure a firewall filter to mirror Layer 2 and Layer 3 packets at a global level and at an instance level. When port mirror is configured at ingress or egress, the packet entering or exiting an interface is copied and the copies are sent to the local interface for local monitoring.

Typically, the firewall filter is configured such that it mirrors either Layer 2 or Layer 3 packets based on the family configured at the interface. However, in case of an integrated routing and bridging (IRB) interface, Layer 2 packets are not completely mirrored because IRB interfaces are configured to mirror only Layer 3 packets. On such an interface, you can configure a firewall filter and port mirroring parameters in the family **any** to ensure that a packet is completely mirrored irrespective of whether it is a Layer 2 or a Layer 3 packet.



NOTE:

- For port mirroring at an instance, you can configure one or more families such as **inet**, **inet6**, **ccc**, and **vpls** simultaneously for the same instance.
- In case of Layer 2 port mirroring, VLAN tags, MPLS headers are retained and can be seen in the mirrored copy at egress.
- For VLAN normalization, the information before normalization is seen for a mirrored packet at ingress. Similarly, at egress, the information after normalization is seen for the mirrored packet.

Before you begin configuring port mirroring, you must configure valid physical interfaces.

To configure a protocol-independent firewall filter for port mirroring:

1. Configure a global firewall filter for port-mirroring egress or ingress traffic.

```
[edit firewall family any]
user@host# set filter filter-name {
  term term-name {
    then {
      port-mirror;
      accept;
    }
  }
}
```

2. Configure a firewall filter to port-mirror traffic for an instance.

```
[edit firewall family any]
user@host# set filter filter-name {
  term term-name {
    then {
      port-mirror-instance instance-name;
      accept;
    }
  }
}
```

```
}
```

3. Configure port mirroring parameters for egress and ingress traffic.

```
[edit forwarding-options port-mirroring]
user@host# input {
  maximum-packet-length bytes
  rate rate;
}
family any {
  output {
    (next-hop-group group-name | interface interface-name);
  }
}
```

4. Configure port mirroring parameters for an instance. In this configuration, you can specify the output or destination for the Layer 2 packets to be either a valid next-hop group or a Layer 2 interface.

```
[edit forwarding-options port-mirroring]
user@host# instance instance-name {
  family any {
    output {
      (next-hop-group group-name | interface interface-name);
    }
  }
}
```

5. Configure the firewall filter at the ingress or egress interface on which the packets are transmitted.

```
[edit interface interface-name unit]
user@host# filter {
  output filter-name;
  input filter-name;
}
```

- Related Documentation**
- [Configuring Ethernet Physical Interface Properties](#)
 - [Configuring Port Mirroring](#)

Example: Layer 2 Port Mirroring at a Logical Interface

The following steps describe an example in which the global port-mirroring instance and a port-mirroring firewall filter are used to configure Layer 2 port mirroring for the input to a logical interface.

1. Configure the bridge domain **example-bd-with-analyzer**, which contains the external packet analyzer, and the bridge domain **example-bd-with-traffic**, which contains the source and destination of the Layer 2 traffic being mirrored:

```
[edit]
bridge-domains {
  example-bd-with-analyzer { # Contains an external traffic analyzer
    vlan-id 1000;
    interface ge-2/0/0.0; # External analyzer
  }
}
```

```
}
example-bd-with-traffic { # Contains traffic input and output interfaces
    vlan-id 1000;
    interface ge-2/0/6.0; # Traffic input port
    interface ge-3/0/1.2; # Traffic output port
}
}
```

Assume that logical interface **ge-2/0/0.0** is associated with an external traffic analyzer that is to receive port-mirrored packets. Assume that logical interfaces **ge-2/0/6.0** and **ge-3/0/1.2** will be traffic input and output ports, respectively.

2. Configure Layer 2 port-mirroring for the global instance, with the port-mirroring destination being the bridge domain interface associated with the external analyzer (logical interface **ge-2/0/0.0** on bridge domain **example-bd-with-analyzer**). Be sure to enable the option that allows filters to be applied to this port-mirroring destination:

```
[edit]
forwarding-options {
    port-mirroring {
        input {
            rate 10;
            run-length 5;
        }
        family bridge {
            output {
                interface ge-2/0/0.0; # Mirror packets to the external analyzer
                no-filter-check; # Allow filters on the mirror destination interface
            }
        }
    }
}
```

The **input** statement at the **[edit forwarding-options port-mirroring]** hierarchy level specifies that sampling begins every tenth packet and that each of the first five packets selected are to be mirrored.

The **output** statement at the **[edit forwarding-options port-mirroring family bridge]** hierarchy level specifies the output mirror interface for Layer 2 packets in a bridging environment:

- Logical interface **ge-2/0/0.0**, which is associated with the external packet analyzer, is configured as the port-mirroring destination.
- The optional **no-filter-check** statement allows filters to be configured on this destination interface.

3. Configure the Layer 2 port-mirroring firewall filter **example-bridge-pm-filter**:

```
[edit]
firewall {
    family bridge {
        filter example-bridge-pm-filter {
            term example-filter-terms {
                then {
                    accept;
                    port-mirror;
                }
            }
        }
    }
}
```

```

    }
  }
}

```

When this firewall filter is applied to the input or output of a logical interface for traffic in a bridging environment, Layer 2 port mirroring is performed according to the input packet-sampling properties and mirror destination properties configured for the Layer 2 port mirroring global instance. Because this firewall filter is configured with the single, default filter action **accept**, all packets selected by the **input** properties (**rate = 10** and **run-length = 5**) match this filter.

4. Configure the logical interfaces:

```

[edit]
interfaces {
  ge-2/0/0 { # Define the interface to the external analyzer
    encapsulation ethernet-bridge;
    unit 0 {
      family bridge;
    }
  }
  ge-2/0/6 { # Define the traffic input port
    flexible-vlan-tagging;
    encapsulation extended-vlan-bridge;
    unit 0 {
      vlan-id 100;
      family bridge {
        filter {
          input example-bridge-pm-filter; # Apply the port-mirroring firewall filter
        }
      }
    }
  }
  ge-3/0/1 { # Define the traffic output port
    flexible-vlan-tagging;
    encapsulation extended-vlan-bridge;
    unit 2 {
      vlan-tags outer 10 inner 20;
      family bridge;
    }
  }
}

```

Packets received at logical interface **ge-2/0/6.0** on bridge domain **example-bd-with-traffic** are evaluated by the port-mirroring firewall filter **example-bridge-pm-filter**. The firewall filter acts on the input traffic according to the filter actions configured in the firewall filter itself plus the input packet-sampling properties and mirror destination properties configured in the global port-mirroring instance:

- All packets received at **ge-2/0/6.0** are forwarded to their (assumed) normal destination at logical interface **ge-3/0/1.2**.

- For every ten input packets, copies of the first five packets in that selection are forwarded to the external analyzer at logical interface **ge-0/0/0.0** in the other bridge domain, **example-bd-with-analyzer**.

If you configure the port-mirroring firewall filter **example-bridge-pm-filter** to take the **discard** action instead of the **accept** action, all original packets are discarded while copies of the packets selected using the global port-mirroring **input** properties are sent to the external analyzer.

**Related
Documentation**

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Firewall Filters on page 8](#)
- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)

Example: Layer 2 Port Mirroring for a Layer 2 VPN

The following example is not a complete configuration, but shows all the steps needed to configure port mirroring on an L2VPN using **family ccc**.

1. Configure the bridge domain **port-mirror-bd**, which contains the external packet analyzer:

```
[edit]
bridge-domains {
  port-mirror-bd { # Contains an external traffic analyzer
    interface ge-2/2/9.0; # External analyzer
  }
}
```

2. Configure the Layer 2 VPN CCC to connect logical interface **ge-2/0/1.0** and logical interface **ge-2/0/1.1**:

```
[edit]
protocols {
  mpls {
    interface all;
  }
  connections {
    interface-switch if_switch {
      interface ge-2/0/1.0;
      interface ge-2/0/1.1;
    }
  }
}
```

3. Configure Layer 2 port mirroring for the global instance, with the port-mirroring destination being the bridge domain interface associated with the external analyzer (logical interface **ge-2/2/9.0** on bridge domain **example-bd-with-analyzer**):

```
[edit]
forwarding-options {
  port-mirroring {
    input {
      rate 1;
    }
  }
}
```

```

        maximum-packet-length 200;
    }
    family ccc {
        output {
            interface ge-2/2/9.0; # Mirror packets to the external analyzer
        }
    }
    instance {
        inst1 {
            input {
                rate 1;
                maximum-packet-length 300;
            }
            family ccc {
                output {
                    interface ge-2/2/9.0;
                }
            }
        }
    }
}

```

4. Define the Layer 2 port-mirroring firewall filter **pm_filter_ccc** for **family ccc**:

```

[edit]
firewall {
    family ccc {
        filter pm_filter_ccc {
            term pm {
                then port-mirror;
            }
        }
    }
}

```

5. Apply the port mirror instance to the chassis:

```

[edit]
chassis {
    fpc 2 {
        port-mirror-instance inst1;
    }
}

```

6. Configure interface **ge-2/2/9** for the VLANs, and configure interface **ge-2/0/1** for port mirroring with the **pm_filter_ccc** firewall filter:

```

[edit]
interfaces {
    ge-2/2/9 {
        encapsulation ethernet-bridge;
        unit 0 {
            family bridge;
        }
    }
    ge-2/0/1 {

```

```
vlan-tagging;
encapsulation extended-vlan-ccc;
unit 0 {
    vlan-id 10;
    family ccc {
        filter {
            input pm_filter_ccc;
        }
    }
}
unit 1 {
    vlan-id 20;
    family ccc {
        filter {
            output pm_filter_ccc;
        }
    }
}
}
```

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Firewall Filters on page 8](#)
- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)

Example: Layer 2 Port Mirroring for a Layer 2 VPN with LAG Links

The following example is not a complete configuration, but shows all the steps needed to configure port mirroring on an L2VPN using **family ccc** and aggregated Ethernet links.

1. Configure the bridge domain **port_mirror_bd**, which contains the external packet analyzer:

```
[edit]
bridge-domains {
    port_mirror_bd { # Contains an external traffic analyzer
        interface ge-2/2/8.0; # External analyzer
    }
}
```

2. Configure the Layer 2 VPN CCC to connect interface **ae0.0** and interface **ae0.1**:

```
[edit]
protocols {
    mpls {
        interface all;
    }
    connections {
        interface-switch if_switch {
            interface ae0.0;
            interface ae0.1;
        }
    }
}
```

```
}
```

3. Configure Layer 2 port mirroring for the global instance, with the port-mirroring destination being the bridge domain interface associated with the external analyzer (logical interface **ge-2/2/9.0** on bridge domain **example_bd_with_analyzer**):

```
[edit]
forwarding-options {
  port-mirroring {
    input {
      rate 1;
      maximum-packet-length 200;
    }
    family ccc {
      output {
        interface ge-2/2/8.0; # Mirror packets to the external analyzer
      }
    }
  }
  instance {
    pm_instance_1 {
      input {
        rate 1;
        maximum-packet-length 300;
      }
      family ccc {
        output {
          interface ge-2/2/8.0;
        }
      }
    }
  }
}
```

4. Configure the firewall filter **pm_ccc** for **family ccc**:

```
[edit]
firewall {
  family ccc {
    filter pm_ccc {
      term pm {
        then port-mirror;
      }
    }
  }
}
```

5. Apply the aggregated Ethernet interfaces and port mirror instance to the chassis:

```
[edit]
chassis {
  aggregated-devices {
    ethernet {
      device-count 10;
    }
  }
  fpc 2 {
```

```
        port-mirror-instance pm_instance_1;
    }
}
```

6. Configure interfaces **ae0** and **ge-2/0/2** (for aggregated Ethernet) and **ge-2/2/8** (for port mirroring) with the **pm_ccc** filter:

```
[edit]
interfaces {
  ae0 {
    vlan-tagging;
    encapsulation extended-vlan-ccc;
    unit 0 {
      vlan-id 10;
      family ccc {
        filter {
          input pm_ccc;
        }
      }
    }
    unit 1 {
      vlan-id 20;
      family ccc {
        filter {
          output pm_ccc;
        }
      }
    }
  }
  ge-2/0/2 {
    gigether-options {
      802.3ad ae0;
    }
  }
  ge-2/2/8 {
    encapsulation ethernet-bridge;
    unit 0 {
      family bridge;
    }
  }
}
```

**Related
Documentation**

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Firewall Filters on page 8](#)
- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)

CHAPTER 6

Layer 2 Port Mirroring Configuration for Multiple Destinations

- [Defining a Next-Hop Group for Layer 2 Port Mirroring on page 63](#)
- [Example: Layer 2 Port Mirroring to Multiple Destinations on page 64](#)

Defining a Next-Hop Group for Layer 2 Port Mirroring

On MX Series routers and EX Series switches, 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 and on an EX Series switch.



NOTE: This topic describes how to define a next-hop group for Layer 2 port mirroring to multiple destinations. For detailed information about defining a firewall filter for Layer 2 port mirroring to multiple destinations, see [“Defining a Layer 2 Port-Mirroring Firewall Filter” on page 44](#).

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

1. Enable configuration of Layer 2 forwarding options.
 - To enable Layer 2 forwarding options at the top level:

```
[edit]  
user@host edit forwarding-options port-mirroring family (ccc | vpls) output
```
 - To enable Layer 2 forwarding options for a routing instance:

```
[edit]  
user@host edit forwarding-options port-mirroring instance instance-name  
family (ccc | vpls) output
```
2. Enable configuration of a next-hop-group for Layer 2 port mirroring:

```
[edit forwarding-options port-mirroring ... family (ccc | vpls) output]  
user@host# edit next-hop-group pm-next-hop-group-name
```

3. Specify the type of addresses to be used in the next-hop group configuration. By default, the next-hop group is specified using Layer 3 addresses (**group-type inet**). To specify the next-hop group using Layer 2 addresses instead, you must include the **group-type layer-2** statement:

```
[edit forwarding-options port-mirroring ... family (ccc | vpls) output next-hop-group
  pm-next-hop-group-name]
user@host# set group-type layer-2
```

4. Specify the logical interfaces of the next-hop route (or switch) r:

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

The MX Series router and the EX Series switch 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.

5. Verify the configuration of the next-hop group:

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

```
...
next-hop-group pm-next-hop-group-name { # Next-hop group on a bridge domain.
  group-type layer-2;
  interface logical-interface-name-1;
  interface logical-interface-name-2;
}
...
```

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups on page 10](#)
- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)
- [Displaying Next-Hop Group Settings and Status on page 82](#)
- [Example: Layer 2 Port Mirroring to Multiple Destinations on page 64](#)

Example: Layer 2 Port Mirroring to Multiple Destinations

On MX Series routers, you can mirror traffic to multiple destinations by configuring next-hop groups in Layer 2 port-mirroring firewall filters applied to tunnel interfaces.

1. Configure the chassis to support tunnel services at PIC 0 on FPC 2. This configuration includes two logical tunnel interfaces on FPC 2, PIC 0, port 10.

```
[edit]
chassis {
  fpc 2 {
```

```

pic 0 {
    tunnel-services {
        bandwidth 1g;
    }
}
}
}

```

2. Configure the physical and logical interfaces for three bridge domains and one Layer 2 VPN CCC:

- Bridge domain **bd** will span logical interfaces **ge-2/0/1.0** and **ge-2/0/1.1**.
- Bridge domain **bd_next_hop_group** will span logical interfaces **ge-2/2/9.0** and **ge-2/0/2.0**.
- Bridge domain **bd_port_mirror** will use the logical tunnel interface **lt-2/0/10.2**.
- Layer 2 VPN CCC **if_switch** will connect logical interfaces **ge-2/0/1.2** and **lt-2/0/10.1**.

```

[edit]
interfaces {
    ge-2/0/1 {
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 0 { # An interface on bridge domain 'bd'.
            encapsulation vlan-bridge;
            vlan-id 200;
            family bridge {
                filter {
                    input pm_bridge;
                }
            }
        }
        unit 1 { # An interface on bridge domain 'bd'.
            encapsulation vlan-bridge;
            vlan-id 201;
            family bridge {
                filter {
                    input pm_bridge;
                }
            }
        }
        unit 2 {
            encapsulation vlan-ccc;
            vlan-id 1000;
        }
    }
    ge-2/0/2 { # For 'bd_next_hop_group'
        encapsulation ethernet-bridge;
        unit 0 {
            family bridge;
        }
    }
    lt-2/0/10 {
        unit 1 {
            encapsulation ethernet-ccc;
            peer-unit 2;
        }
    }
}

```

```

    }
    unit 2 {
        encapsulation ethernet-bridge;
        peer-unit 1;
        family bridge {
            filter {
                output redirect_to_nhg;
            }
        }
    }
}
ge-2/2/9 {
    encapsulation ethernet-bridge;
    unit 0 { # For 'bd_next_hop_group'
        family bridge;
    }
}
}

```

3. Configure the three bridge domains and the Layer 2 VPN switching CCC:

- Bridge domain **bd** spans logical interfaces **ge-2/0/1.0** and **ge-2/0/1.1**.
- Bridge domain **bd_next_hop_group** spans logical interfaces **ge-2/2/9.0** and **ge-2/0/2.0**.
- Bridge domain **bd_port_mirror** uses the logical tunnel interface **lt-2/0/10.2**.
- Layer 2 VPN CCC **if_switch** connects interfaces **ge-2/0/1.2** and **lt-2/0/10.1**.

```

[edit]
bridge-domains {
    bd {
        interface ge-2/0/1.0;
        interface ge-2/0/1.1;
    }
    bd_next_hop_group {
        interface ge-2/2/9.0;
        interface ge-2/0/2.0;
    }
    bd_port_mirror {
        interface lt-2/0/10.2;
    }
}
protocols {
    mpls {
        interface all;
    }
    connections {
        interface-switch if_switch {
            interface ge-2/0/1.2;
            interface lt-2/0/10.1;
        }
    }
}
}

```

For detailed information about configuring the CCC connection for Layer 2 switching cross-connects, see the *Junos OS MPLS Applications Library for Routing Devices*.

4. Configure forwarding options:

- Configure global port mirroring properties to mirror **family vpls** traffic to an interface on the bridge domain **bd_port_mirror**.
- Configure the next-hop group **nhg_mirror_to_bd** to forward Layer 2 traffic to the bridge domain **bd_next_hop_group**.

Both of these forwarding options will be referenced by the port-mirroring firewall filter:

```
[edit]
forwarding-options {
  port-mirroring { # Global port mirroring properties.
    input {
      rate 1;
    }
    family vpls {
      output {
        interface lt-2/0/10.2; # Interface on 'bd_port_mirror' bridge domain.
        no-filter-check;
      }
    }
  }
  next-hop-group nhg_mirror_to_bd { # Configure a next-hop group.
    group-type layer-2; # Specify 'layer-2' for Layer 2; default 'inet' is for Layer 3.
    interface ge-2/0/2.0; # Interface on 'bd_next_hop_group' bridge domain.
    interface ge-2/2/9.0; # Interface on 'bd_next_hop_group' bridge domain.
  }
}
```

5. Configure two Layer 2 port-mirroring firewall filters for **family bridge** traffic:

- **filter_pm_bridge**—Sends all **family bridge** traffic to the global port mirroring destination.
- **filter_redirect_to_nhg**—Sends all **family bridge** traffic to the final next-hop group **nhg_mirror_to_bd**.

Layer 2 port-mirroring firewall filters for **family bridge** traffic applies to traffic on a physical interface configured with encapsulation **ethernet-bridge**.

```
[edit]
firewall {
  family bridge {
    filter filter_pm_bridge {
      term term_port_mirror {
        then port-mirror;
      }
    }
    filter filter_redirect_to_nhg {
      term term_nhg {
        then next-hop-group nhg_mirror_to_bd;
      }
    }
  }
}
```

**Related
Documentation**

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups on page 10](#)
- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)
- [Defining a Next-Hop Group for Layer 2 Port Mirroring on page 63](#)
- [Displaying Next-Hop Group Settings and Status on page 82](#)

CHAPTER 7

Layer 2 Port Mirroring Configuration Statements

- family (Port Mirroring) on page 70
- interface (Port Mirroring) on page 71
- input (Port Mirroring) on page 71
- maximum-packet-length on page 72
- no-filter-check on page 73
- output (Port Mirroring) on page 74
- port-mirroring on page 75
- rate (Forwarding Options) on page 77
- run-length on page 78

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 <i>instance-name</i>]
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

- *Configuring Active Flow Monitoring on PTX Series Packet Transport Routers*

interface (Port Mirroring)

Syntax	<code>interface <i>interface-name</i> { next-hop <i>address</i>; }</code>
Hierarchy Level	[edit forwarding-options port-mirroring output], [edit forwarding-options port-mirroring family (inet inet6) output]
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	<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"> • <i>Configuring Port Mirroring</i>

input (Port Mirroring)

Syntax	<code>input { maximum-packet-length <i>bytes</i>; rate <i>number</i>; run-length <i>number</i>; }</code>
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"> • <i>Configuring Port Mirroring</i>

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 <i>instance-name</i> input], [edit forwarding-options sampling input], [edit forwarding-options sampling instance <i>instance-name</i> 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.



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*
- *Configuring Traffic Sampling*

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

- *Configuring Port Mirroring*

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	[edit forwarding-options port-mirroring family (ccc inet inet6 mpls vpls)], [edit forwarding-options port-mirroring instance <i>instance-name</i> family (ccc inet inet6 mpls vpls)]
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">• <i>Configuring Port Mirroring</i>• <i>Configuring Active Flow Monitoring on PTX Series Packet Transport Routers</i>

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	<p>Specify the address family, rate, run length, interface, and next-hop address for sending copies of packets to an analyzer.</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>Configuring Port Mirroring</i>• <i>Configuring Active Flow Monitoring on PTX Series Packet Transport Routers</i>

rate (Forwarding Options)

Syntax	<code>rate <i>number</i>;</code>
Hierarchy Level	<p>[edit forwarding-options analyzer <i>analyzer-name</i> input] [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],</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. 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.</p>
Description	<p>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.</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. Range: 1 through 65,535</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"> • <i>Configuring Port Mirroring</i> • <i>Configuring Traffic Sampling</i>

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">• <i>Applying Forwarding Table Filters</i>• <i>Configuring Port Mirroring</i>• <i>Configuring Traffic Sampling</i>

PART 3

Administration

- [Displaying Information on page 81](#)
- [Operational Mode Commands for Packet Forwarding Engine Components on page 83](#)
- [Operational Mode Commands for Layer 2 Port-Mirroring Instances on page 353](#)
- [Operational Mode Commands for Firewall Filter Statistics and Logs on page 357](#)
- [Operational Mode Commands for Next-Hop Groups for Layer 2 Port Mirroring on page 371](#)

CHAPTER 8

Displaying Information

- [Displaying Information About DPCs or FPCs in an MX Series Router on page 81](#)
- [Displaying Layer 2 Port-Mirroring Instance Settings and Status on page 81](#)
- [Displaying Next-Hop Group Settings and Status on page 82](#)

Displaying Information About DPCs or FPCs in an MX Series Router

To display information about the number and types of DPCs or FPCs in an MX Series router, the number of Packet Forwarding Engines on each, and the number and types of ports per Packet Forwarding Engine, you can use the following chassis operational mode commands:

- [show chassis hardware](#)
- [show chassis fabric fpcs](#)

For more information about chassis operational mode commands, see the [CLI Explorer](#).

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Properties on page 4](#)
- [Layer 2 Port Mirroring Named Instances on page 6](#)

Displaying Layer 2 Port-Mirroring Instance Settings and Status

To display the current state of port-mirroring instances, use the [show forwarding-options port-mirroring <terse | detail> <instance-name>](#) operational command.

For more information about displaying port mirroring instance settings and status, see the *Junos OS Administration Library for Routing Devices*.

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring Global Instance on page 5](#)
- [Layer 2 Port Mirroring Named Instances on page 6](#)
- [Configuring the Global Instance of Layer 2 Port Mirroring on page 25](#)
- [Defining a Named Instance of Layer 2 Port Mirroring on page 28](#)

- [Disabling Layer 2 Port Mirroring Instances on page 35](#)
- [Examples: Layer 2 Port-Mirroring at Multiple Levels of the Chassis on page 36](#)
- [Example: Layer 2 Port Mirroring with Multiple Instances on page 38](#)

Displaying Next-Hop Group Settings and Status

To display the current state of next-hop groups, use the [show forwarding-options next-hop-group <terse | brief | detail> <group-name>](#) operational command.

For more information, see the [CLI Explorer](#).

Related Documentation

- [Layer 2 Port Mirroring Overview on page 3](#)
- [Layer 2 Port Mirroring to Multiple Destinations Using Next-Hop Groups on page 10](#)
- [Defining a Layer 2 Port-Mirroring Firewall Filter on page 44](#)
- [Defining a Next-Hop Group for Layer 2 Port Mirroring on page 63](#)
- [Example: Layer 2 Port Mirroring to Multiple Destinations on page 64](#)


```
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
FPC 6
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
FPC 7
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
```



```
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
FPC 1
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
FPC 2
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
```

```

        Plane 6: Plane enabled
        Plane 7: Plane enabled
PFE #1
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
PFE #2
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
PFE #3
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
FPC 3
    PFE #0
        Plane 0: Plane enabled
        Plane 1: Plane enabled
        Plane 2: Plane enabled
        Plane 3: Plane enabled
        Plane 4: Plane enabled
        Plane 5: Plane enabled
        Plane 6: Plane enabled
        Plane 7: Plane enabled
    PFE #1
        Plane 0: Plane enabled
        Plane 1: Plane enabled
        Plane 2: Plane enabled
        Plane 3: Plane enabled
        Plane 4: Plane enabled
        Plane 5: Plane enabled
        Plane 6: Plane enabled
        Plane 7: Plane enabled
    PFE #2
        Plane 0: Plane enabled
        Plane 1: Plane enabled
        Plane 2: Plane enabled
        Plane 3: Plane enabled
        Plane 4: Plane enabled
        Plane 5: Plane enabled
        Plane 6: Plane enabled
        Plane 7: Plane enabled
    PFE #3
        Plane 0: Plane enabled
        Plane 1: Plane enabled
        Plane 2: Plane enabled

```

```

Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
FPC 4
...
```

show chassis fabric fpcs (MX2020 Router with MPC4E)

```

user@host > show chassis fabric fpcs
Fabric management FPC state:
FPC 0
  PFE #0
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
  PFE #1
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
FPC 9
  PFE #0
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
  PFE #1
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
FPC 10
  PFE #0
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
FPC 14
```

```
PFE #0
  Plane 0: Plane enabled
  Plane 1: Plane enabled
  Plane 2: Plane enabled
  Plane 3: Plane enabled
  Plane 4: Plane enabled
  Plane 5: Plane enabled
  Plane 6: Plane enabled
  Plane 7: Plane enabled
PFE #1
  Plane 0: Plane enabled
  Plane 1: Plane enabled
  Plane 2: Plane enabled
  Plane 3: Plane enabled
  Plane 4: Plane enabled
  Plane 5: Plane enabled
  Plane 6: Plane enabled
  Plane 7: Plane enabled
FPC 19
  PFE #0
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
  PFE #1
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
  PFE #2
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
  PFE #3
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
```

show chassis fabric fpcs (T320 Router)

```
user@host> show chassis fabric fpcs
FPC #3
  PFE #1
```

```

SIB #0
    Links ok
SIB #1
    Plane enabled
SIB #2
    Plane enabled
FPC #5
    PFE #1
        SIB #0
            Links ok
        SIB #1
            Plane enabled
        SIB #2
            Plane enabled
FPC #7
    PFE #1
        SIB #0
            Links ok
        SIB #1
            Plane enabled
        SIB #2
            Plane enabled

```

show chassis fabric fpcs (T640 Router)

```

user@host> show chassis fabric fpcs
Fabric management FPC state:

```

```

FPC #2
    PFE #1
        SIB #0
            Links ok
        SIB #1
            Plane enabled
        SIB #2
            Plane enabled
        SIB #3
            Plane enabled
        SIB #4
            Plane enabled
FPC #3
    PFE #1
        SIB #2
            Plane enabled
        SIB #3
            Link error
            Destination error on PFES
            8   9   10   11   12   13   14   15   16   17   18   19   20   21
        SIB #4
            Destination error on PFES
            8   9   10   11   12   13   14   15   16   17   18   19   20   21
...

```

show chassis fabric fpcs (TX Matrix Router)

```

user@host> show chassis fabric fpcs
1cc0-re0:
-----
Fabric management FPC state:
FPC #0
    PFE #1

```

```

SIB #0
    Links ok
SIB #2
    Links ok
SIB #3
    Links ok
SIB #4
    Links ok
FPC #2
    PFE #1
        SIB #0
            Links ok
        SIB #2
            Links ok
        SIB #3
            Links ok
        SIB #4
            Links ok
FPC #3
    PFE #1
        SIB #2
            Plane enabled
        SIB #3
            Link error
            Destination error on PFES
            0 1 2 3 4 5 6 7
            8 9 10 11 12 13 14 15 16 17 18 19 20 21
        SIB #4
            Destination error on PFES
            0 1 2 3 4 5 6 7
            8 9 10 11 12 13 14 15 16 17 18 19 20 21
...
FPC #4
    PFE #0
        SIB #4 Links ok
    PFE #1
        SIB #4 Links ok
FPC #5
    PFE #1
        SIB #4 Links ok
FPC #6
    PFE #1
        SIB #4 Links ok

lcc2-re0:
-----
Fabric management FPC state:
FPC #0
    PFE #1
        SIB #4 Links ok
FPC #1
    PFE #1
        SIB #4 Links ok
FPC #2
    PFE #0
        SIB #4 Links ok
    PFE #1
        SIB #4 Links ok
FPC #4
    PFE #0
        SIB #4 Links ok
    PFE #1
        SIB #4 Links ok
FPC #5

```

```
PFE #1
SIB #4 Links ok
```

show chassis fabric fpcs (TX Matrix Router with 3D SIBs)

```
user@host> show chassis fabric fpcs
1cc0-re0:
```

```
-----
Fabric management FPC state:
```

```
FPC #0
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
  PFE #1
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
FPC #3
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
  PFE #1
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
FPC #4
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok
```

```

SIB #2
    Links ok
SIB #3
    Links ok
SIB #4
    Links ok
PFE #1
    SIB #0
        Links ok
    SIB #1
        Links ok
    SIB #2
        Links ok
    SIB #3
        Links ok
    SIB #4
        Links ok
FPC #5
    PFE #0
        SIB #0
            Links ok
        SIB #1
            Links ok
        SIB #2
            Links ok
        SIB #3
            Links ok
        SIB #4
            Links ok
    PFE #1
        SIB #0
            Links ok
        SIB #1
            Links ok
        SIB #2
            Links ok
        SIB #3
            Links ok
        SIB #4
            Links ok
FPC #6
    PFE #0
        SIB #0
            Links ok
        SIB #1
            Links ok
        SIB #2
            Links ok
        SIB #3
            Links ok
        SIB #4
            Links ok
    PFE #1
        SIB #0
            Links ok
        SIB #1
            Links ok
        SIB #2
            Links ok
        SIB #3
            Links ok

```

```
SIB #4
Links ok
```

```
lcc2-re0:
```

```
lcc4-re0:
```

```
Fabric management FPC state:
```

```
FPC #2
```

```
PFE #0
```

```
SIB #0
Links ok
SIB #1
Links ok
SIB #2
Links ok
SIB #3
Links ok
SIB #4
Links ok
```

```
PFE #1
```

```
SIB #0
Links ok
SIB #1
Links ok
SIB #2
Links ok
SIB #3
Links ok
SIB #4
Links ok
```

```
FPC #3
```

```
PFE #0
```

```
SIB #0
Links ok
SIB #1
Links ok
SIB #2
Links ok
SIB #3
Links ok
SIB #4
Links ok
```

```
PFE #1
```

```
SIB #0
Links ok
SIB #1
Links ok
SIB #2
Links ok
SIB #3
Links ok
SIB #4
Links ok
```

```
lcc6-re0:
```



```
SIB #1
Plane enabled
SIB #2
Plane enabled
SIB #3
Plane enabled
SIB #4
Plane enabled
PFE #1
SIB #0
Links ok
SIB #1
Plane enabled
SIB #2
Plane enabled
SIB #3
Plane enabled
SIB #4
Plane enabled
FPC #1
PFE #0
SIB #0
Links ok
SIB #1
Plane enabled
SIB #2
Plane enabled
SIB #3
Plane enabled
SIB #4
Plane enabled
PFE #1
SIB #0
Links ok
SIB #1
Plane enabled
SIB #2
Plane enabled
SIB #3
Plane enabled
SIB #4
Plane enabled
FPC #2
PFE #0
SIB #0
Links ok
SIB #1
Plane enabled
SIB #2
Plane enabled
SIB #3
Plane enabled
SIB #4
Plane enabled
FPC #4
PFE #0
SIB #0
Links ok
SIB #1
Plane enabled
SIB #2
```

```

        Plane enabled
    SIB #3      Plane enabled
    SIB #4      Plane enabled
PFE #1
    SIB #0      Links ok
    SIB #1      Plane enabled
    SIB #2      Plane enabled
    SIB #3      Plane enabled
    SIB #4      Plane enabled
FPC #3
    PFE #1
        SIB #2      Plane enabled
        SIB #3      Link error
                        Destination error on PFEs
                        8   9   10  11  12  13  14  15  16  17  18  19  20  21
        SIB #4      Destination error on PFEs
                        8   9   10  11  12  13  14  15  16  17  18  19  20  21

```

show chassis fabric fpcs (T4000 Core Router)

Fabric management FPC state:

```

FPC #2
    PFE #0
        SIB #0      Links ok
        SIB #1      Plane enabled
        SIB #2      Plane enabled
        SIB #3      Plane enabled
        SIB #4      Plane enabled
FPC #3
    PFE #0
        SIB #0      Links ok
        SIB #1      Plane enabled
        SIB #2      Plane enabled
        SIB #3      Plane enabled
        SIB #4      Plane enabled
FPC #5
    PFE #0
        SIB #0      Links ok
        SIB #1      Plane enabled

```

```

SIB #2
    Plane enabled
SIB #3
    Plane enabled
SIB #4
    Plane enabled
PFE #1
SIB #0
    Links ok
SIB #1
    Plane enabled
SIB #2
    Plane enabled
SIB #3
    Plane enabled
SIB #4
    Plane enabled
FPC #6
PFE #0
SIB #0
    Links ok
SIB #1
    Plane enabled
SIB #2
    Plane enabled
SIB #3
    Plane enabled
SIB #4
    Plane enabled
PFE #1
SIB #0
    Links ok
SIB #1
    Plane enabled
SIB #2
    Plane enabled
SIB #3
    Plane enabled
SIB #4
    Plane enabled

```

show chassis fabric fpcs (TX Matrix Plus Router)

```

user@host> show chassis fabric fpcs
lcc0-re0:

```

```

-----
Fabric management FPC state:

```

```

FPC #0
PFE #1
SIB #0
    Unused
SIB #1
    Links ok
SIB #2
    Links ok
SIB #3
    Links ok
SIB #4
    Links ok
FPC #2
PFE #0

```

```

SIB #0
    Unused
SIB #1
    Links ok
SIB #2
    Links ok
SIB #3
    Links ok
SIB #4
    Links ok
PFE #1
    SIB #0
        Unused
    SIB #1
        Links ok
    SIB #2
        Links ok
    SIB #3
        Links ok
    SIB #4
        Links ok
FPC #3
    PFE #1
        SIB #2
            Plane enabled
        SIB #3
            Link error
            Destination error on PFes
            8      9      10      11      12      13      14      15      16      17      18      19      20      21
            0      1      2      3      4      5      6      7
SIB #4
            Destination error on PFes
            8      9      10      11      12      13      14      15      16      17      18      19      20      21
            0      1      2      3      4      5      6      7
FPC #4
    PFE #0
        SIB #0
            Unused
        SIB #1
            Links ok
        SIB #2
            Links ok
        SIB #3
            Links ok
        SIB #4
            Links ok
    PFE #1
        SIB #0
            Unused
        SIB #1
            Links ok
        SIB #2
            Links ok
        SIB #3
            Links ok
        SIB #4
            Links ok
FPC #6
    PFE #0
        SIB #0
            Unused
        SIB #1
            Links ok

```

```
SIB #2
    Links ok
SIB #3
    Links ok
SIB #4
    Links ok
PFE #1
    SIB #0
        Unused
    SIB #1
        Links ok
    SIB #2
        Links ok
    SIB #3
        Links ok
    SIB #4
        Links ok
FPC #7
    PFE #0
        SIB #0
            Unused
        SIB #1
            Links ok
        SIB #2
            Links ok
        SIB #3
            Links ok
        SIB #4
            Links ok
```

lcc1-re0:

Fabric management FPC state:

```
FPC #2
    PFE #0
        SIB #0
            Links ok
        SIB #1
            Links ok
        SIB #2
            Links ok
        SIB #3
            Links ok
        SIB #4
            Links ok
    PFE #1
        SIB #0
            Links ok
        SIB #1
            Links ok
        SIB #2
            Links ok
        SIB #3
            Links ok
        SIB #4
            Links ok
FPC #4
    PFE #0
        SIB #0
            Links ok
        SIB #1
```

```

SIB #2 Links ok
SIB #3 Links ok
SIB #4 Links ok
PFE #1
SIB #0 Links ok
SIB #1 Links ok
SIB #2 Links ok
SIB #3
Destination error on PFES 1 8 9 29 40 65 72 73
93 104
SIB #4 Links ok
FPC #6
PFE #0
SIB #0 Links ok
SIB #1 Links ok
SIB #2 Links ok
SIB #3 Links ok
SIB #4 Links ok
PFE #1
SIB #0 Links ok
SIB #1 Links ok
SIB #2 Links ok
SIB #3 Links ok
SIB #4 Links ok
FPC #7
PFE #0
SIB #0 Links ok
SIB #1 Links ok
SIB #2 Links ok
SIB #3 Links ok
SIB #4 Links ok

lcc2-re0:
-----
Fabric management FPC state:
FPC #0
PFE #0

```

```
SIB #0
Links ok
SIB #1
Links ok
SIB #2
Links ok
SIB #3
Links ok
SIB #4
Links ok
PFE #1
SIB #0
Links ok
SIB #1
Links ok
SIB #2
Links ok
SIB #3
Links ok
SIB #4
Links ok
FPC #2
PFE #0
SIB #0
Links ok
SIB #1
Links ok
SIB #2
Links ok
SIB #3
Links ok
SIB #4
Links ok
PFE #1
SIB #0
Links ok
SIB #1
Links ok
SIB #2
Links ok
SIB #3
Links ok
SIB #4
Links ok
FPC #4
PFE #0
SIB #0
Links ok
SIB #1
Links ok
SIB #2
Links ok
SIB #3
Links ok
SIB #4
Links ok
FPC #5
PFE #0
SIB #0
Links ok
SIB #1
```

```

SIB #2      Links ok
SIB #3      Links ok
SIB #4      Links ok
PFE #1
SIB #0      Links ok
SIB #1      Links ok
SIB #2      Links ok
SIB #3      Links ok
SIB #4      Links ok
FPC #6
PFE #0
SIB #0      Links ok
SIB #1      Links ok
SIB #2      Links ok
SIB #3      Links ok
SIB #4      Links ok
PFE #1
SIB #0      Links ok
SIB #1      Links ok
SIB #2      Links ok
SIB #3      Links ok
SIB #4      Links ok
FPC #7
PFE #0
SIB #0      Links ok
SIB #1      Links ok
SIB #2      Links ok
SIB #3      Links ok
SIB #4      Links ok

```

lcc3-re0:

Fabric management FPC state:

```

FPC #0
PFE #0
SIB #0      Links ok

```

```
SIB #1
    Links ok
SIB #2
    Links ok
SIB #3
    Links ok
SIB #4
    Links ok
PFE #1
    SIB #0
        Links ok
    SIB #1
        Links ok
    SIB #2
        Links ok
    SIB #3
        Links ok
    SIB #4
        Links ok
FPC #2
    PFE #0
        SIB #0
            Links ok
        SIB #1
            Links ok
        SIB #2
            Links ok
        SIB #3
            Links ok
        SIB #4
            Links ok
    PFE #1
        SIB #0
            Links ok
        SIB #1
            Links ok
        SIB #2
            Links ok
        SIB #3
            Links ok
        SIB #4
            Links ok
FPC #4
    PFE #0
        SIB #0
            Links ok
        SIB #1
            Links ok
        SIB #2
            Links ok
        SIB #3
            Links ok
        SIB #4
            Links ok
    PFE #1
        SIB #0
            Links ok
        SIB #1
            Links ok
        SIB #2
            Links ok
```


CHAPTER 12

Operational Mode Commands for Next-Hop Groups for Layer 2 Port Mirroring

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

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 354
List of Sample Output	show forwarding-options next-hop-group terse on page 373 show forwarding-options next-hop-group brief on page 373 show forwarding-options next-hop-group detail on page 373
Output Fields	Table 13 on page 372 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 13: 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 13: 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

```


PART 4

Index

- [Index on page 377](#)

