



---

Junos<sup>®</sup> OS

# Layer 2 Port Mirroring Analyzers Feature Guide for MX Series Routers

Release  
15.1



---

Modified: 2015-05-21

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://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<sup>®</sup> OS Layer 2 Port Mirroring Analyzers Feature Guide for MX Series Routers*

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
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Port Mirroring Analyzers Overview . . . . .</b>	<b>3</b>
	Understanding Port Mirroring Analyzers . . . . .	4
	Analyzer Overview . . . . .	5
	Statistical Analyzer Overview . . . . .	5
	Default Analyzer Overview . . . . .	5
	Port Mirroring at a Group of Ports Bound to Multiple Statistical Analyzers . . . . .	5
	Port Mirroring Analyzer Terminology . . . . .	5
	Configuration Guidelines for Port Mirroring Analyzers . . . . .	7
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 2</b>	<b>Configuration Examples . . . . .</b>	<b>13</b>
	Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use . . . . .	13
	Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use . . . . .	16
<b>Chapter 3</b>	<b>Configuration Statements: Port Mirroring . . . . .</b>	<b>27</b>
	[edit forwarding-options analyzer] Configuration Statement Hierarchy . . . . .	27
	analyzer (Port Mirroring) . . . . .	29
	bridge-domain (Analyzer) . . . . .	30
	egress (Analyzer) . . . . .	31
	ingress (Analyzer) . . . . .	32
	input (Analyzer) . . . . .	33
	interface (Analyzer) . . . . .	34
	next-hop-group (Analyzer) . . . . .	35
	output (Mirroring) . . . . .	36

	maximum-packet-length . . . . .	37
	rate (Forwarding Options) . . . . .	38
	routing-instance . . . . .	39
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 4</b>	<b>Operational Commands: Analyzers . . . . .</b>	<b>43</b>
	show forwarding-options analyzer . . . . .	44
<b>Part 4</b>	<b>Index</b>	
	Index . . . . .	49

# List of Figures

Part 2	Configuration	
Chapter 2	Configuration Examples . . . . .	13
	Figure 1: Network Topology for Local Port Mirroring Example . . . . .	14
	Figure 2: Network Topology for Remote Port Mirroring and Analysis . . . . .	18



# List of Tables

	<b>About the Documentation . . . . .</b>	<b>ix</b>
	Table 1: Notice Icons . . . . .	xi
	Table 2: Text and Syntax Conventions . . . . .	xi
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Port Mirroring Analyzers Overview . . . . .</b>	<b>3</b>
	Table 3: Analyzer Terminology . . . . .	5
	Table 4: Configuration Guidelines for Port Mirroring Analyzers . . . . .	7
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 4</b>	<b>Operational Commands: Analyzers . . . . .</b>	<b>43</b>
	Table 5: show forwarding-options analyzer Output Fields . . . . .	44





# 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
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>

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

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

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 <b>Protocols&gt;Ospf</b> .

## 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](mailto: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

- [Port Mirroring Analyzers Overview on page 3](#)





## CHAPTER 1

# Port Mirroring Analyzers Overview

- [Understanding Port Mirroring Analyzers on page 4](#)

## Understanding Port Mirroring Analyzers

---

Port mirroring can be used for traffic analysis on routers and switches that, unlike hubs, do not broadcast packets to every port on the destination device. Port mirroring sends copies of all packets or policy-based sample packets to local or remote analyzers where you can monitor and analyze the data.

In the context of port mirroring analyzers, we use the term *switching device*. The term indicates that the device (including routers) is performing a switching function.

You can use analyzers on a packet level to help you:

- Monitor network traffic
- Enforce network usage policies
- Enforce file sharing policies
- Identify causes of problems
- Identify stations or applications with heavy or abnormal bandwidth usage

You can configure an analyzer to mirror:

- Bridged packets (Layer 2 packets)
- Routed packets (Layer 3 packets)

Mirrored packets can be copied to either a local interface for local monitoring or a VLAN or bridge domain for remote monitoring.

The following packets can be copied:

- **Packets entering or exiting a port**—You can mirror packets entering or exiting ports, in any combination, for up to 256 ports. For example, you can send copies of the packets entering some ports and the packets exiting other ports to the same local analyzer port or analyzer VLAN.
- **Packets entering or exiting a VLAN or bridge domain**—You can mirror the packets entering or exiting a VLAN or bridge domain to either a local analyzer port or to an analyzer VLAN or bridge domain. You can configure multiple VLANs (up to 256 VLANs) or bridge domains as ingress inputs to an analyzer, including a VLAN range and private VLANs (PVLANS).
- **Policy-based sample packets**—You can mirror a policy-based sample of packets that are entering a port, VLAN, or bridge domain. You configure a firewall filter with a policy to select the packets to be mirrored. You can send the sample to a port-mirroring instance or to an analyzer VLAN or bridge domain.

This topic describes:

- [Analyzer Overview on page 5](#)
- [Statistical Analyzer Overview on page 5](#)

- [Default Analyzer Overview on page 5](#)
- [Port Mirroring at a Group of Ports Bound to Multiple Statistical Analyzers on page 5](#)
- [Port Mirroring Analyzer Terminology on page 5](#)
- [Configuration Guidelines for Port Mirroring Analyzers on page 7](#)

## Analyzer Overview

You can configure an analyzer to define both the input traffic and the output traffic in the same analyzer configuration. The input traffic to be analyzed can be either traffic that enters or traffic that exits an interface or VLAN. The analyzer configuration enables you to send this traffic to an output interface, instance, next-hop group, VLAN, or bridge domain. You can configure an analyzer at the **[edit forwarding-options analyzer]** hierarchy level.

## Statistical Analyzer Overview

You can define a set of mirroring properties, such as mirroring rate and maximum packet length for traffic, that you can explicitly bind to physical ports on the router or switch. This set of mirroring properties constitutes a statistical analyzer (also called a nondefault analyzer). At this level, you can bind a named instance to the physical ports associated with a specific FPC.

## Default Analyzer Overview

You can configure an analyzer without configuring any mirroring properties (such as mirroring rate or maximum packet length). By default, the mirroring rate is set to 1 and the maximum packet length is set to the complete length of the packet. These properties are applied at the global level and need not be bound to a specific FPC.

## Port Mirroring at a Group of Ports Bound to Multiple Statistical Analyzers

You can apply up to two statistical analyzers to the same port groups on the switching device. By applying two different statistical analyzer instances to the same FPC or Packet Forwarding Engine, you can bind two distinct Layer 2 mirroring specifications to a single port group. Mirroring properties that are bound to an FPC override any analyzer (default analyzer) properties bound at the global level on the switching device. Default analyzer properties are overridden by binding a second analyzer instance on the same port group.

## Port Mirroring Analyzer Terminology

[Table 3 on page 5](#) lists some port mirroring analyzer terms and their descriptions.

**Table 3: Analyzer Terminology**

Term	Description
Analyzer	<p>In a mirroring configuration, the analyzer includes:</p> <ul style="list-style-type: none"> <li>• The name of the analyzer</li> <li>• Source (input) ports, VLANs, or bridge domains</li> </ul>

Table 3: Analyzer Terminology (*continued*)

Term	Description
	<ul style="list-style-type: none"> <li>A destination for mirrored packets (either a monitor port, VLAN, or bridge domain)</li> </ul>
Analyzer output interface (Also known as a monitor port)	<p>Interface to which mirrored traffic is sent and to which a protocol analyzer application is connected.</p> <p><b>NOTE:</b> Interfaces used as output for an analyzer must be configured under the <b>forwarding-options</b> hierarchy level.</p> <p>Analyzer output interfaces have the following limitations:</p> <ul style="list-style-type: none"> <li>They cannot also be a source port.</li> <li>They do not participate in Layer 2 protocols, such as the Spanning Tree Protocol (STP), when part of a port-mirroring configuration.</li> <li>If the bandwidth of the analyzer output interface is not sufficient to handle the traffic from the source ports, overflow packets are dropped.</li> </ul>
Analyzer VLAN or bridge domain (Also known as a monitor VLAN or bridge domain)	VLAN or bridge domain to which mirrored traffic is sent. The mirrored traffic can be used by a protocol analyzer application. The member interfaces in the monitor VLAN or bridge domain are spread across the switching devices in your network.
Bridge-domain-based analyzer	An analyzer session whose configuration uses bridge domains for both input and output or for either input or output.
Default analyzer	An analyzer with default mirroring parameters. By default, the mirroring rate is 1 and the maximum packet length is the length of the complete packet.
Input interface (Also known as mirrored ports or monitored interfaces)	An interface on the switching device that is being mirrored. Traffic that is either entering or exiting this interface is mirrored.
LAG-based analyzer	An analyzer that has a link aggregation group (LAG) specified as the input (ingress) interface in the analyzer configuration.
Local mirroring	An analyzer configuration in which packets are mirrored to a local analyzer port.
Monitoring station	A computer running a protocol analyzer application.
Analyzer based on next-hop group	An analyzer session configuration that uses the next-hop group as the analyzer output.
Port-based analyzer	An analyzer session configuration that defines interfaces for both input and output.
Protocol analyzer application	An application used to examine packets transmitted across a network segment. Also commonly called a network analyzer, packet sniffer, or probe.
Remote mirroring	Functions the same way as local mirroring, except that the mirrored traffic is not copied to a local analyzer port but is flooded to an analyzer VLAN or bridge domain that you create specifically for the purpose of receiving mirrored traffic. Mirrored packets have an additional outer tag of the analyzer VLAN or bridge domain.

Table 3: Analyzer Terminology (*continued*)

Term	Description
Statistical analyzer (Also known as a nondefault analyzer)	You can define a set of mirroring properties that you can explicitly bind to physical ports on the switch. This set of analyzer properties is known as a statistical analyzer.
VLAN-based analyzer	An analyzer session whose configuration uses VLANs for both input and output or for either input or output.

### Configuration Guidelines for Port Mirroring Analyzers

When you configure port mirroring analyzers, we recommend that you follow these guidelines to ensure optimum benefit. We recommend that you disable mirroring when you are not using it, and that you select specific interfaces as input to the analyzer rather than using the **all** keyword option, which enables mirroring on all interfaces. Mirroring only necessary packets reduces any potential performance impact.

You can also limit the amount of mirrored traffic by:

- Using statistical sampling
- Using a firewall filter
- Setting a ratio to select a statistical sample

With local mirroring, traffic from multiple ports is replicated to the analyzer output interface. If the output interface for an analyzer reaches capacity, packets are dropped. You must consider whether the traffic being mirrored exceeds the capacity of the analyzer output interface.

[Table 4 on page 7](#) summarizes further configuration guidelines for analyzers.

Table 4: Configuration Guidelines for Port Mirroring Analyzers

Guideline	Value or Support Information	Comment
Number of analyzers that you can enable concurrently.	64—Default analyzers  2 per FPC—Statistical analyzer	<ul style="list-style-type: none"> <li>• Statistical analyzers must be bound to an FPC for mirroring traffic on ports belonging to that FPC.</li> </ul> <p><b>NOTE:</b> Default analyzer properties are implicitly bound on the last (or second to last) instance on all FPCs in the system. Therefore, when you explicitly bind a second statistical analyzer on the FPC, the default analyzer properties are overridden.</p>
Number of interfaces, VLANs, or bridge domains that you can use as ingress input to an analyzer.	256	—

Table 4: Configuration Guidelines for Port Mirroring Analyzers (*continued*)

Guideline	Value or Support Information	Comment
Types of ports on which you cannot mirror traffic.	<ul style="list-style-type: none"> <li>Virtual Chassis ports (VCPs)</li> <li>Management Ethernet ports (me0 or vme0)</li> <li>Integrated routing and bridging (IRB) interfaces</li> <li>VLAN-tagged Layer 3 interfaces</li> </ul>	
Protocol families that you can include in an analyzer.	<b>ethernet-switching</b> for EX Series switches and <b>bridge</b> for MX Series routers.	Analyzer mirrors only bridged traffic. For mirroring routed traffic, use the port mirroring configuration with <b>family</b> as <b>inet</b> or <b>inet6</b> .
Packets with physical layer errors are not sent to the local or remote analyzer.	Applicable	Packets with these errors are filtered out and thus are not sent to the analyzer.
Analyzer does not support line-rate traffic.	Applicable	Mirroring for line-rate traffic is done on a best-effort basis.
Analyzer output on a LAG interface.	Supported	
Analyzer output interface mode as trunk mode.	Supported	<ul style="list-style-type: none"> <li>The trunk interface has to be a member of all VLANs or bridge domains that are related to the input configuration of analyzer.</li> <li>You must use the <b>mirror-once</b> option if the input has been configured as VLAN or bridge domain and the output is a trunk interface.</li> </ul> <p><b>NOTE:</b> With the mirror-once option, if the input is for both ingress and egress mirroring, only ingress traffic is mirrored. If both ingress and egress mirroring are required, the output interface cannot be a trunk. In such cases, configure the interface as an access interface.</p>
Egress mirroring of host-generated control packets.	Not supported	
Configuring Layer 3 logical interfaces in the <b>input</b> stanza of an analyzer.	Not supported	
The analyzer input and output stanzas containing members of the same VLAN or the VLAN itself must be avoided.	Applicable	
Support for VLAN and its member interfaces in different analyzer sessions	Not supported	If mirroring is configured, either of the analyzers is active.

Table 4: Configuration Guidelines for Port Mirroring Analyzers (*continued*)

Guideline	Value or Support Information	Comment
Egress mirroring of aggregated Ethernet (ae) interfaces and its child logical interfaces configured for different analyzers.	Not supported	

**Related Documentation**

- [Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use on page 13](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 16](#)
- [Configuring Mirroring on EX9200 Switches to Analyze Traffic \(CLI Procedure\)](#)





## PART 2

# Configuration

- [Configuration Examples on page 13](#)
- [Configuration Statements: Port Mirroring on page 27](#)



## CHAPTER 2

# Configuration Examples

- [Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use on page 13](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 16](#)

### Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use

---

Juniper Networks devices allow you to configure port mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN or bridge domain for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering or exiting a VLAN or bridge domain

You can then analyze the mirrored traffic locally or remotely using a protocol analyzer application. You can install analyzers on a system connected to the local destination interface, or running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN or bridge domain.

This topic describes how to configure local mirroring on a switching device. The examples in this topic describe how to configure a switching device to mirror traffic entering interfaces connected to employee computers to an analyzer output interface on that same device.

- [Requirements on page 13](#)
- [Overview and Topology on page 14](#)
- [Mirroring All Employee Traffic for Local Analysis on page 14](#)
- [Verification on page 16](#)

### Requirements

Use either one of the following hardware and software components:

- One EX9200 switch with Junos OS Release 13.2 or later
- One MX Series router with Junos OS Release 14.1 or later

Before you configure port mirroring, be sure you have an understanding of mirroring concepts. For information about analyzers, see [“Understanding Port Mirroring Analyzers” on page 4](#). For information about port mirroring, see [Layer 2 Port Mirroring Overview](#).

## Overview and Topology

This topic describes how to mirror all traffic entering ports on the switching device to a destination interface on the same device (local mirroring). In this case, the traffic is entering ports connected to employee computers.



**NOTE:** Mirroring all traffic requires significant bandwidth and should only be done during an active investigation.

The interfaces ge-0/0/0 and ge-0/0/1 serve as connections for employee computers.

The interface ge-0/0/10 is reserved for analysis of mirrored traffic. Connect a PC running a protocol analyzer application to the analyzer output interface to analyze the mirrored traffic.

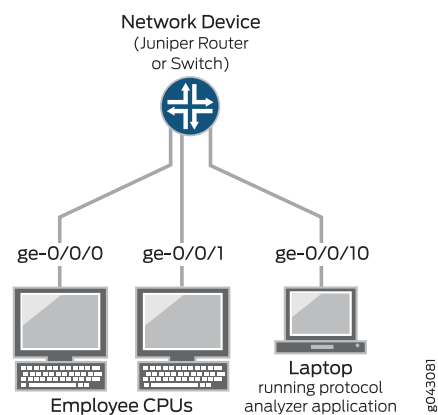
Connect a PC running a protocol analyzer application to the analyzer output interface to analyze the mirrored traffic.



**NOTE:** Multiple ports mirrored to one interface can cause buffer overflow and dropped packets.

[Figure 1 on page 14](#) shows the network topology for this example.

**Figure 1: Network Topology for Local Port Mirroring Example**



## Mirroring All Employee Traffic for Local Analysis

### CLI Quick Configuration

To quickly configure local mirroring for ingress traffic sent to the two ports connected to employee computers, copy either the following commands for EX Series switches or for MX Series routers and paste them into the switching device's terminal window:

**EX Series**      [edit]  
 set interfaces ge-0/0/0 unit 0 family ethernet-switching  
 set interfaces ge-0/0/1 unit 0 family ethernet-switching  
 set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0  
 set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0  
 set forwarding-options analyzer employee-monitor output interface ge-0/0/10.0

**MX Series**      [edit]  
 set interfaces ge-0/0/0 unit 0 family bridge interface-mode access vlan-id 99  
 set interfaces ge-0/0/1 unit 0 family bridge interface-mode access vlan-id 98  
 set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0  
 set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0  
 set forwarding-options analyzer employee-monitor output interface ge-0/0/10.0

**Step-by-Step Procedure**      To configure an analyzer called **employee-monitor** and specify both the input (source) interfaces and the analyzer output interface:

1. Configure each interface you are to use in the analyzer configuration. Use the family protocol that is correct for your platform.

#### EX Series

[edit]  
 set interfaces ge-0/0/0 unit 0 family ethernet-switching  
 set interfaces ge-0/0/1 unit 0 family ethernet-switching

#### MX Series

To configure **family bridge** on an interface, you need to configure **interface-mode access** or **interface-mode trunk** as well. You also must configure **vlan-id**.

[edit]  
 set interfaces ge-0/0/0 unit 0 family bridge interface-mode access vlan-id 99  
 set interfaces ge-0/0/1 unit 0 family bridge interface-mode access vlan-id 98

2. Configure each interface connected to employee computers as an input interface for the analyzer **employee-monitor**.

[edit forwarding-options]  
 set analyzer employee-monitor input ingress interface ge-0/0/0.0  
 set analyzer employee-monitor input ingress interface ge-0/0/1.0

3. Configure the output analyzer interface for the **employee-monitor** analyzer.

This will be the destination interface for the mirrored packets.

[edit forwarding-options]  
 set analyzer employee-monitor output interface ge-0/0/10.0

**Results**      Check the results of the configuration.

[edit]  
 user@device# show forwarding-options  
 analyzer {  
 employee-monitor {  
 input {  
 ingress {

```
        interface ge-0/0/0.0;
        interface ge-0/0/1.0;
    }
}
output {
    interface ge-0/0/10.0;
}
}
```

## Verification

### Verifying That the Analyzer Has Been Correctly Created

---

**Purpose** Verify that the analyzer **employee-monitor** has been created on the switching device with the appropriate input interfaces and the appropriate output interface.

**Action** Use the **show forwarding-options analyzer** operational command to verify whether an analyzer is configured as expected.

```
user@device> show forwarding-options analyzer
Analyzer name           : employee-monitor
Mirror rate             : 1
Maximum packet length   : 0
State                   : up
Ingress monitored interfaces : ge-0/0/0.0
Output interface        : ge-0/0/10.0
```

**Meaning** The output shows that the **employee-monitor** analyzer has a ratio of 1 (that is, mirroring every packet, the default setting), the maximum size of the original packet mirrored is 0 (which indicates that the entire packet is mirrored), the state of the configuration is **up**, and the analyzer is mirroring the traffic entering the ge-0/0/0 interface, and sending the mirrored traffic to the ge-0/0/10 interface.

If the state of the output interface is **down** or if the output interface is not configured, the value of **State** will be **down** and the analyzer will not be programmed for mirroring.

- Related Documentation**
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 16](#)
  - [Configuring Mirroring on EX9200 Switches to Analyze Traffic \(CLI Procedure\)](#)
  - [Understanding Port Mirroring Analyzers on page 4](#)

## Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use

---

Juniper Networks devices allow you to configure port mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN or bridge domain for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port

- Packets entering or exiting a VLAN
- Packets entering or exiting a bridge domain

If you are sending mirrored traffic to an analyzer VLAN or bridge domain, you can analyze the mirrored traffic using a protocol analyzer application running on a remote monitoring station.



**BEST PRACTICE:** Mirror only necessary packets to reduce potential performance impact. We recommend that you do the following:

- Disable your configured mirroring sessions when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by:
  - Using statistical sampling.
  - Setting ratios to select statistical samples.
  - Using firewall filters.

The examples in this topic describe how to configure remote port mirroring to analyze employee resource usage.

- [Requirements on page 17](#)
- [Overview and Topology on page 18](#)
- [Mirroring Employee Traffic for Remote Analysis Using a Statistical Analyzer on page 18](#)
- [Verification on page 26](#)

## Requirements

This example uses one of the following pairs of hardware and software components:

- One EX9200 switch connected to another EX9200 switch, both running Junos OS Release 13.2 or later
- One MX Series router connected to another MX Series router, both running Junos OS Release 14.1 or later

Before you configure remote mirroring, be sure that:

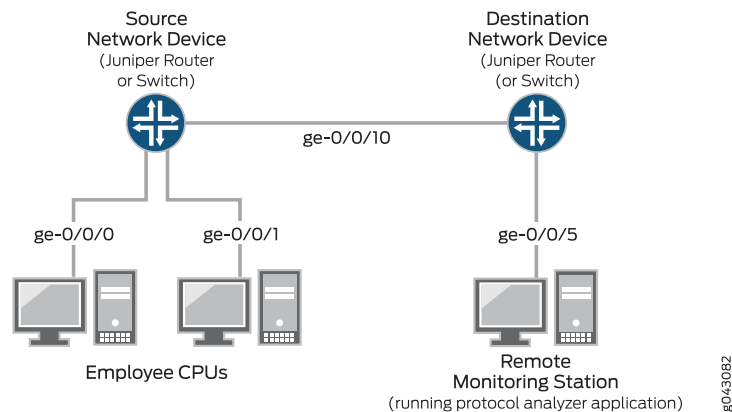
- You have an understanding of mirroring concepts. For information about analyzers, see [“Understanding Port Mirroring Analyzers” on page 4](#). For information about port mirroring, see [Layer 2 Port Mirroring Overview](#).
- The interfaces that the analyzer will use as input interfaces have already been configured on the switching device.

## Overview and Topology

This topic describes how to configure port mirroring to a remote analyzer VLAN or bridge domain so that analysis can be done from a remote monitoring station.

Figure 2 on page 18 shows the network topology for both the EX Series example and the MX Series example scenarios.

**Figure 2: Network Topology for Remote Port Mirroring and Analysis**



In this example:

- Interface ge-0/0/0 is a Layer 2 interface, and interface ge-0/0/1 is a Layer 3 interface (both interfaces on the source device) that serve as connections for employee computers.
- Interface ge-0/0/10 is a Layer 2 interface that connects the source switching device to the destination switching device.
- Interface ge-0/0/5 is a Layer 2 interface that connects the destination switching device to the remote monitoring station.
- The analyzer **remote-analyzer** is configured on all switching devices in the topology to carry the mirrored traffic. The topology can use either a VLAN or a bridge domain.

## Mirroring Employee Traffic for Remote Analysis Using a Statistical Analyzer

To configure a statistical analyzer for remote traffic analysis for all incoming and outgoing employee traffic, select one of the following examples:

- [Mirroring Employee Traffic for Remote Analysis for EX Series Switches on page 18](#)
- [Mirroring Employee Traffic for Remote Analysis for MX Series Routers on page 22](#)

### Mirroring Employee Traffic for Remote Analysis for EX Series Switches

#### CLI Quick Configuration

To quickly configure a statistical analyzer for remote traffic analysis of incoming and outgoing employee traffic, copy the following commands for EX Series switches and paste them into the correct switching device's terminal window.



- Copy and paste the following commands in the *source* switching device's terminal window:

#### EX Series

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output vlan remote-analyzer
set forwarding-options analyzer employee-monitor input rate 2
set forwarding-options analyzer employee-monitor input maximum-packet-length 128
set chassis fpc 0 port-mirror-instance employee-monitor
```

- Copy and paste the following commands in the *destination* switching device's terminal window:

#### EX Series

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set interfaces ge-0/0/5 unit 0 family ethernet-switching interface-mode access
set forwarding-options analyzer employee-monitor input ingress vlan remote-analyzer
set forwarding-options analyzer employee-monitor output interface ge-0/0/5.0
```

#### Step-by-Step Procedure

To configure basic remote mirroring:

1. On the source switching device, do the following:

- Configure the VLAN ID for the **remote-analyzer** VLAN.

```
[edit]
user@device# set vlans remote-analyzer vlan-id 999
```

- Configure the interface on the network port connected to the destination switching device for access mode and associate it with the **remote-analyzer** VLAN.

```
[edit]
user@device# set interfaces ge-0/0/10 unit 0 family ethernet-switching
interface-mode access
user@device# set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan
members 999
```

- Configure the statistical analyzer **employee-monitor**.

```
[edit forwarding-options]
user@device# set analyzer employee-monitor input ingress interface ge-0/0/0.0
user@device# set analyzer employee-monitor input ingress interface ge-0/0/1.0
user@device# set analyzer employee-monitor input egress interface ge-0/0/0.0
user@device# set analyzer employee-monitor input egress interface ge-0/0/1.0
user@device# set analyzer employee-monitor output vlan remote-analyzer
user@device# set analyzer employee-monitor input rate 2
```

```
user@device# set analyzer employee-monitor input maximum-packet-length 128
```

- Bind the statistical analyzer to the FPC that contains the input interface.

```
[edit]
user@device# set chassis fpc 0 port-mirror-instance employee-monitor
```

2. On the destination network device, do the following:

- Configure the VLAN ID for the **remote-analyzer** VLAN.

```
[edit]
user@device# set vlans remote-analyzer vlan-id 999
```

- Configure the interface on the destination switching device for access mode and associate it with the **remote-analyzer** VLAN.

```
[edit interfaces]
user@device# set ge-0/0/10 unit 0 family ethernet-switching interface-mode
access
user@device# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure the interface connected to the destination switching device for access mode.

```
[edit interfaces]
user@device# set ge-0/0/5 unit 0 family ethernet-switching interface-mode
access
```

- Configure the **employee-monitor** analyzer.

```
[edit forwarding-options]
user@device# set analyzer employee-monitor input ingress vlan remote-analyzer
user@device# set analyzer employee-monitor output interface ge-0/0/5.0
```

- Specify mirroring parameters such as rate and the maximum packet length for the **employee-monitor** analyzer.

```
[edit]
user@device# set forwarding-options analyzer employee-monitor input rate 2
user@device# set forwarding-options analyzer employee-monitor input
maximum-packet-length 128
```

- Bind the **employee-monitor** analyzer to the FPC containing the input ports.

```
[edit]
user@device# set chassis fpc 0 port-mirror-instance employee-monitor
```

**Results** Check the results of the configuration on the source switching device:

```
[edit]
user@device# show
forwarding-options {
  analyzer employee-monitor {
    input {
      ingress {
        interface ge-0/0/0.0;
        interface ge-0/0/1.0;
      }
      egress {
```

```

        interface ge-0/0/0.0;
        interface ge-0/0/1.0;
    }
    maximum-packet-length 128;
    rate 2;
}
output {
    vlan {
        remote-analyzer;
    }
}
}
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members 999;
                }
            }
        }
    }
}
vlangs {
    remote-analyzer {
        vlan-id 999;
    }
}
}

```

Check the results of the configuration on the destination switching device.

```

[edit]
user@device# show
interfaces {
    ge0/0/5 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members 999;
                }
            }
        }
    }
}
vlangs {
    remote-analyzer {

```

```
vlan-id 999;
interface {
    ge-0/0/10.0;
}
}
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                vlan remote-analyzer;
            }
        }
        output {
            interface {
                ge-0/0/5.0;
            }
        }
    }
}
```

---

### Mirroring Employee Traffic for Remote Analysis for MX Series Routers

#### CLI Quick Configuration

To quickly configure a statistical analyzer for remote traffic analysis of incoming and outgoing employee traffic, copy the following commands for MX Series routers and paste them into the correct switching device's terminal window.

- Copy and paste the following commands in the *source* switching device's terminal window:

#### MX Series

```
[edit]
set bridge-domains remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family bridge interface-mode access
set interfaces ge-0/0/10 unit 0 family bridge vlan-id 999
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output bridge-domain
    remote-analyzer
set forwarding-options analyzer employee-monitor input rate 2
set forwarding-options analyzer employee-monitor input maximum-packet-length 128
set chassis fpc 0 port-mirror-instance employee-monitor
```

- Copy and paste the following commands in the *destination* switching device's terminal window:

#### MX Series

```
[edit]
set bridge-domains remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family bridge interface-mode access
set interfaces ge-0/0/10 unit 0 family bridge vlan-id 999
set interfaces ge-0/0/5 unit 0 family bridge interface-mode access
```

```

set forwarding-options analyzer employee-monitor input ingress bridge-domain
remote-analyzer
set forwarding-options analyzer employee-monitor output interface ge-0/0/5.0

```

### Step-by-Step Procedure

To configure basic remote mirroring using MX Series routers:

1. On the source switching device, do the following:

- Configure the VLAN ID for the **remote-analyzer** bridge domain.

```

[edit]
user@device# set bridge-domains remote-analyzer vlan-id 999

```

- Configure the interface on the network port connected to the destination switching device for access mode and associate it with the **remote-analyzer** bridge domain.

```

[edit]
user@device# set interfaces ge-0/0/10 unit 0 family bridge interface-mode access
user@device# set interfaces ge-0/0/10 unit 0 family bridge vlan members 999

```

- Configure the statistical analyzer **employee-monitor**.

```

[edit forwarding-options]
user@device# set analyzer employee-monitor input ingress interface ge-0/0/0.0
user@device# set analyzer employee-monitor input ingress interface ge-0/0/1.0
user@device# set analyzer employee-monitor input egress interface ge-0/0/0.0
user@device# set analyzer employee-monitor input egress interface ge-0/0/1.0
user@device# set analyzer employee-monitor output bridge-domain
remote-analyzer
user@device# set analyzer employee-monitor input rate 2
user@device# set analyzer employee-monitor input maximum-packet-length 128

```

- Bind the statistical analyzer to the FPC that contains the input interface.

```

[edit]
user@device# set chassis fpc 0 port-mirror-instance employee-monitor

```

2. On the destination switching device, do the following:

- Configure the VLAN ID for the **remote-analyzer** bridge domain.

```

[edit bridge-domains]
user@device# set remote-analyzer vlan-id 999

```

- Configure the interface on the destination switching device for access mode and associate it with the **remote-analyzer** bridge domain.

```

[edit interfaces]
user@device# set ge-0/0/10 unit 0 family bridge interface-mode access
user@device# set ge-0/0/10 unit 0 family bridge vlan members 999

```

- Configure the interface connected to the destination switching device for access mode.

```

[edit interfaces]
user@device# set ge-0/0/5 unit 0 family bridge interface-mode access

```

- Configure the **employee-monitor** analyzer.

```
[edit forwarding-options]
user@device# set analyzer employee-monitor input ingress bridge-domain
remote-analyzer
user@device# set analyzer employee-monitor output interface ge-0/0/5.0
```

- Specify mirroring parameters such as rate and the maximum packet length for the **employee-monitor** analyzer.

```
[edit]
user@device# set forwarding-options analyzer employee-monitor input rate 2
user@device# set forwarding-options analyzer employee-monitor input
maximum-packet-length 128
```

- Bind the **employee-monitor** analyzer to the FPC containing the input ports.

```
[edit]
user@device# set chassis fpc 0 port-mirror-instance employee-monitor
```

**Results** Check the results of the configuration on the source switching device:

```
[edit]
user@device# show
bridge-domains {
  remote-analyzer {
    vlan-id 999;
  }
}
forwarding-options {
  analyzer {
    employee-monitor {
      input {
        ingress {
          interface ge-0/0/0.0;
          interface ge-0/0/1.0;
        }
        egress {
          interface ge-0/0/0.0;
          interface ge-0/0/1.0;
        }
        maximum-packet-length 128;
        rate 2;
      }
      output {
        bridge-domain {
          remote-analyzer;
        }
      }
    }
  }
}
interfaces {
  ge-0/0/0 {
    unit 0 {
      family bridge {
        interface-mode access;
        vlan-id 99;
      }
    }
  }
}
```

```

    }
  }
  ge-0/0/1 {
    unit 0 {
      family bridge {
        interface-mode access;
        vlan-id 98;
      }
    }
  }
  ge-0/0/10 {
    unit 0 {
      family bridge {
        interface-mode access;
        vlan-id 999;
      }
    }
  }
}

```

Check the results of the configuration on the destination switching device.

```

[edit]
user@device# show
bridge-domains {
  remote-analyzer {
    vlan-id 999;
  }
}
forwarding-options {
  analyzer {
    employee-monitor {
      input {
        ingress {
          interface ge-0/0/0.0;
          interface ge-0/0/1.0;
          bridge-domain remote-analyzer;
        }
      }
      output {
        interface ge-0/0/5.0;
      }
    }
  }
}
interfaces {
  ge-0/0/5 {
    unit 0 {
      family bridge {
        interface-mode access;
      }
    }
  }
}

```

## Verification

### Verifying That the Analyzer Has Been Correctly Created

---

**Purpose** Verify that the analyzer named **employee-monitor** has been created on the device with the appropriate input interfaces and appropriate output interface.

**Action** To verify that the analyzer is configured as expected while monitoring all employee traffic on the source switching device, run the **show forwarding-options analyzer** command on the source switching device. The following output is displayed for this configuration example.

```
user@device> show forwarding-options analyzer
```

```
Analyzer name           : employee-monitor
Mirror rate             : 2
Maximum packet length   : 128
State                   : up
Ingress monitored interfaces : ge-0/0/0.0
Ingress monitored interfaces : ge-0/0/1.0
Egress monitored interfaces : ge-0/0/0.0
Egress monitored interfaces : ge-0/0/1.0
Output VLAN             : default-switch/remote-analyzer
```

**Meaning** This output shows that the **employee-monitor** instance has a ratio of 2, the maximum size of the original packet that were mirrored is 128, the state of the configuration is **up**, which indicates proper state and that the analyzer is programmed, and the analyzer is mirroring the traffic entering ge-0/0/0.0 and ge-0/0/1.0, and is sending the mirrored traffic to the VLAN called remote-analyzer.

If the state of the output interface is **down** or if the output interface is not configured, the value of **State** will be down and the analyzer will not be able to mirror traffic.

- Related Documentation**
- [Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use on page 13](#)
  - [Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches](#)
  - [Configuring Mirroring on EX9200 Switches to Analyze Traffic \(CLI Procedure\)](#)
  - [Understanding Port Mirroring Analyzers on page 4](#)



## CHAPTER 3

# Configuration Statements: Port Mirroring

- [\[edit forwarding-options analyzer\] Configuration Statement Hierarchy on page 27](#)
- [analyzer \(Port Mirroring\) on page 29](#)
- [bridge-domain \(Analyzer\) on page 30](#)
- [egress \(Analyzer\) on page 31](#)
- [ingress \(Analyzer\) on page 32](#)
- [input \(Analyzer\) on page 33](#)
- [interface \(Analyzer\) on page 34](#)
- [next-hop-group \(Analyzer\) on page 35](#)
- [output \(Mirroring\) on page 36](#)
- [maximum-packet-length on page 37](#)
- [rate \(Forwarding Options\) on page 38](#)
- [routing-instance on page 39](#)

### [\[edit forwarding-options analyzer\] Configuration Statement Hierarchy](#)

---

```
forwarding-options {
  analyzer (Port Mirroring) {
    analyzer-name {
      input {
        egress {
          bridge-domain bridge-domain-name;
          interface (all | interface-name);
          routing-instance {
            instance-name {
              bridge-domain bridge-domain-name;
            }
          }
        }
      }
    }
    ingress {
      bridge-domain bridge-domain-name;
      interface (all | interface-name);
      routing-instance {
        instance-name {
          bridge-domain bridge-domain-name;
        }
      }
      vlan (vlan-id | vlan-name);
    }
  }
}
```

```
    }
    vlan (vlan-id | vlan-name);
  }
  maximum-packet-length bytes;
  rate number;
}
output {
  bridge-domain bridge-domain-name;
  interface interface-name;
  next-hop-group next-hop-group-name;
  routing-instance {
    instance-name {
      bridge-domain {
        bridge-domain-name;
      }
    }
  }
  vlan (vlan-id | vlan-name);
}
vlan (vlan-id | vlan-name);
}
}
```

- Related Documentation**
- [Understanding Port Mirroring Analyzers on page 4](#)
  - *Notational Conventions Used in Junos OS Configuration Hierarchies*

## analyzer (Port Mirroring)

```
Syntax  analyzer {
        analyzer-name {
            input {
                egress {
                    bridge-domain bridge-domain-name;
                    interface (all | interface-name);
                    routing-instance {
                        instance-name {
                            bridge-domain bridge-domain-name;
                        }
                    }
                }
            }
            ingress {
                bridge-domain bridge-domain-name;
                interface (all | interface-name);
                routing-instance {
                    instance-name {
                        bridge-domain bridge-domain-name;
                    }
                }
                vlan (vlan-id | vlan-name);
            }
            maximum-packet-length bytes;
            rate number;
        }
        output {
            bridge-domain bridge-domain-name;
            interface interface-name;
            next-hop-group next-hop-group-name;
            routing-instance {
                instance-name {
                    bridge-domain {
                        bridge-domain-name;
                    }
                }
            }
            vlan (vlan-id | vlan-name);
        }
        vlan (vlan-id | vlan-name);
    }
}
```

**Hierarchy Level** [edit forwarding-options]

**Release Information** Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.  
Statement introduced in Junos OS Release 14.1 for MX Series routers.

**Description** Configure port mirroring.

**Default** Port mirroring is disabled and Junos OS creates no default analyzers.

<b>Options</b>	<b><i>analyzer-name</i></b> —Name that identifies the analyzer. The name can be up to 125 characters long, must begin with a letter, and can include uppercase letters, lowercase letters, numbers, dashes, and underscores. No other special characters are allowed.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Understanding Port Mirroring Analyzers on page 4</a></li><li>• <a href="#">Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use on page 13</a></li><li>• <a href="#">Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 16</a></li></ul>

---

## bridge-domain (Analyzer)

---

<b>Syntax</b>	<code>bridge-domain <i>bridge-domain-name</i>;</code>
<b>Hierarchy Level</b>	[edit forwarding-options analyzer <i>analyzer-name</i> input egress], [edit forwarding-options analyzer <i>analyzer-name</i> input egress routing-instance <i>instance-name</i> ], [edit forwarding-options analyzer <i>analyzer-name</i> input ingress], [edit forwarding-options analyzer <i>analyzer-name</i> input ingress routing-instance <i>instance-name</i> ], [edit forwarding-options analyzer <i>analyzer-name</i> output], [edit forwarding-options analyzer <i>analyzer-name</i> output routing-instance <i>instance-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	Configure the bridge domain to monitor outgoing traffic.
<b>Options</b>	<b><i>bridge-domain-name</i></b> —Name of the bridge domain that monitors outgoing traffic.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 16</a></li><li>• <a href="#">Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches</a></li><li>• <a href="#">[edit forwarding-options analyzer] Configuration Statement Hierarchy on page 27</a></li></ul>

## egress (Analyzer)

<b>Syntax</b>	<pre>egress {   bridge-domain bridge-domain-name;   interface (all   interface-name);   routing-instance {     instance-name {       bridge-domain bridge-domain-name;     }   } }</pre>
<b>Hierarchy Level</b>	[edit forwarding-options analyzer <i>analyzer-name</i> input]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 14.1 for MX Series routers.
<b>Description</b>	<p>Specify ports where traffic exiting the interface is to be mirrored in a mirroring configuration.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches</i></li> </ul>

## ingress (Analyzer)

---

<b>Syntax</b>	<pre>ingress {   bridge-domain bridge-domain-name;   interface (all   interface-name);   routing-instance {     instance-name {       bridge-domain bridge-domain-name;     }     vlan (vlan-id   vlan-name);   }   vlan (vlan-id   vlan-name); }</pre>
<b>Hierarchy Level</b>	[edit forwarding-options analyzer <i>analyzer-name</i> input]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 14.1 for MX Series routers.
<b>Description</b>	<p>Configure ports, routing instances, VLANs, or bridge domains for which the entering traffic is mirrored as part of a mirroring configuration.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches</i></li></ul>

## input (Analyzer)

```
Syntax  input {
        egress {
            bridge-domain bridge-domain-name;
            interface (all | interface-name);
            routing-instance {
                instance-name {
                    bridge-domain bridge-domain-name;
                }
            }
        }
        ingress {
            bridge-domain bridge-domain-name;
            interface (all | interface-name);
            routing-instance {
                instance-name {
                    bridge-domain bridge-domain-name;
                }
            }
            vlan (vlan-id | vlan-name);
        }
        vlan (vlan-id | vlan-name);
    }
    maximum-packet-length bytes;
    rate number;
}
```

**Hierarchy Level** [edit forwarding-options analyzer *analyzer-name*]

**Release Information** Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.  
Statement introduced in Junos OS Release 14.1 for MX Series routers.

**Description** Define the traffic to be mirrored in a mirroring configuration—the definition can be a combination of:

- Packets entering or exiting a port
- Packets entering or exiting a VLAN
- Packets entering or exiting a bridge domain

The remaining statements are explained separately.

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.

**Default** No default.

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

- Related Documentation**
- [Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use on page 13](#)
  - [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 16](#)
  - [Understanding Port Mirroring Analyzers on page 4](#)

---

## interface (Analyzer)

---

<b>Syntax</b>	<code>interface (all   <i>interface-name</i>);</code>
<b>Hierarchy Level</b>	[edit forwarding-options analyzer <i>analyzer-name</i> input egress], [edit forwarding-options analyzer <i>analyzer-name</i> input ingress], [edit forwarding-options analyzer <i>analyzer-name</i> output]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 14.1 for MX Series routers.
<b>Description</b>	Configure the interfaces for which traffic is mirrored.
<b>Options</b>	<p><b>all</b>—Apply mirroring to all interfaces on the network device. Mirroring a high volume of traffic can be performance intensive for the device. Therefore, you should generally select specific input interfaces in preference to using the <b>all</b> keyword, or use the <b>all</b> keyword in combination with setting a ratio for statistical sampling. The <b>all</b> keyword is not available for the [edit forwarding-options analyzer <i>analyzer-name</i> output] hierarchy level.</p> <p><b><i>interface-name</i></b>—Apply mirroring to the specified interface only.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use on page 13</a></li><li>• <a href="#">Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 16</a></li><li>• <a href="#">Understanding Port Mirroring Analyzers on page 4</a></li></ul>



## next-hop-group (Analyzer)

---

<b>Syntax</b>	<code>next-hop-group <i>next-hop-group-name</i>;</code>
<b>Hierarchy Level</b>	[edit forwarding-options analyzer <i>analyzer-name</i> output]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1 for MX Series routers.
<b>Description</b>	Configure next-hop group through which the port-mirrored traffic is sent.
<b>Options</b>	<i>next-hop-group-name</i> —Name of the next-hop group through which the port-mirrored traffic is sent.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches</i></li></ul>

## output (Mirroring)

---

**Syntax**    `output {  
              bridge-domain bridge-domain-name;  
              interface interface-name;  
              next-hop-group next-hop-group-name;  
              routing-instance {  
                  instance-name {  
                      bridge-domain {  
                          bridge-domain-name;  
                      }  
                  }  
              }  
              vlan (vlan-id | vlan-name);  
              }  
              vlan (vlan-id | vlan-name);  
          }`

**Hierarchy Level**    [ edit forwarding-options analyzer *analyzer-name* ]

**Release Information**    Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.  
                              Statement introduced in Junos OS Release 14.1 for MX Series routers.

**Description**    Configure the destination for mirrored traffic, either an interface on the network device for local monitoring, or a VLAN or bridge domain, for remote monitoring.

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**

- [Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use on page 13](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 16](#)

## maximum-packet-length

<b>Syntax</b>	<code>maximum-packet-length bytes;</code>
<b>Hierarchy Level</b>	[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]
<b>Release Information</b>	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.
<b>Description</b>	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`.

<b>Options</b>	<i>bytes</i> —Maximum length (in bytes) of the mirrored packet or the sampled packet. <b>Range:</b> 0 through 9216 <b>Default:</b> 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** interface—To view this statement in the configuration.  
**Level** interface-control—To add this statement to the configuration.

**Related Documentation**

- *Configuring Port Mirroring*
- *Configuring Traffic Sampling*

---

## rate (Forwarding Options)

---

**Syntax** `rate number;`

**Hierarchy Level** [edit forwarding-options analyzer *analyzer-name* input]  
[edit forwarding-options port-mirroring input],  
[edit forwarding-options sampling input],  
[edit forwarding-options sampling instance *instance-name* input],  
[edit forwarding-options port-mirroring family (inet|inet6) input],

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.  
Support at the [edit forwarding-options analyzer *analyzer-name* input] hierarchy level for MX Series routers introduced in Junos OS Release 14.1.

**Description** Set a ratio of the number of packets to be sampled. For example, if you specify a rate of 10, every tenth packet (1 packet out of 10) is sampled.

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** *number*—Denominator of the ratio.  
**Range:** 1 through 65,535

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

**Related Documentation**

- *Configuring Port Mirroring*
- *Configuring Traffic Sampling*

## routing-instance

---

<b>Syntax</b>	<pre> routing-instance {   instance-name {     bridge-domain bridge-domain-name;   }   vlan (vlan-id   vlan-name); } </pre>
<b>Hierarchy Level</b>	[edit forwarding-options analyzer <i>analyzer-name</i> input egress], [edit forwarding-options analyzer <i>analyzer-name</i> input ingress], [edit forwarding-options analyzer <i>analyzer-name</i> output]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	Configure routing instance.
<b>Options</b>	<i>instance-name</i> —Name of the routing instance.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">[edit forwarding-options analyzer] Configuration Statement Hierarchy on page 27</a></li> </ul>



## PART 3

# Administration

- [Operational Commands: Analyzers on page 43](#)





## CHAPTER 4

# Operational Commands: Analyzers

- `show forwarding-options analyzer`

## show forwarding-options analyzer

<b>Syntax</b>	<b>show forwarding-options analyzer <i>analyzer-name</i></b>
<b>Release Information</b>	Hierarchy level <b>[edit forwarding-options]</b> introduced in Junos OS Release 13.2X50-D10 (ELS).
<b>Description</b>	Display information about analyzers configured for mirroring.
<b>Options</b>	<b><i>analyzer-name</i></b> —(Optional) Displays the status of a specific analyzer on the switch.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Understanding Port Mirroring and Analyzers on EX4300 Switches</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show forwarding-options analyzer on page 44</a>
<b>Output Fields</b>	<a href="#">Table 5 on page 44</a> lists the output fields for the <b>show forwarding-options analyzer</b> command. Output fields are listed in the approximate order in which they appear.

**Table 5: show forwarding-options analyzer Output Fields**

Field Name	Field Description
Analyzer name	Displays the name of the analyzer.
Output interface	Specifies a local interface to which mirrored packets are sent. An analyzer can have output to either an interface or a VLAN, not both.
Output VLAN	Specifies a VLAN to which mirrored packets are sent. An analyzer can have output to either an interface or a VLAN, not both.
Mirror ratio	Displays the ratio of packets to be mirrored.
Egress monitored interfaces	Displays interfaces for which traffic exiting the interfaces is mirrored.
Ingress monitored interfaces	Displays interfaces for which traffic entering the interfaces is mirrored.
Ingress monitored VLANs	Displays VLANs for which traffic entering the VLAN is mirrored.

## Sample Output

### show forwarding-options analyzer

```

user@switch> show forwarding-options analyzer
Analyzer name           : employee-monitor
Mirror rate             : 1
Maximum packet length   : 0
State                   : up
Ingress monitored interfaces : ge-0/0/0.0

```

```
Ingress monitored interfaces : ge-0/0/1.0
Output VLAN                 : default-switch/remote-analyzer
```



## PART 4

# Index

- [Index on page 49](#)



# Index

## Symbols

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

## A

analyzer statement.....	29
analyzers.....	4
configuring for local monitoring.....	13
configuring for remote monitoring.....	16

## B

braces, in configuration statements.....	xii
brackets	
angle, in syntax descriptions.....	xii
square, in configuration statements.....	xii
bridge-domain statement.....	30

## C

command-name command.....	44
comments, in configuration statements.....	xii
conventions	
text and syntax.....	xi
curly braces, in configuration statements.....	xii
customer support.....	xiii
contacting JTAC.....	xiii

## D

documentation	
comments on.....	xiii

## E

egress (Analyzer)	
configuration statement.....	31
egress statement	
port mirroring.....	31

## F

font conventions.....	xi
-----------------------	----

## I

ingress statement.....	32
input statement.....	33
interface statement	
port mirroring.....	34

## M

manuals	
comments on.....	xiii
maximum-packet-length statement.....	37

## N

network traffic	
monitoring.....	13, 16
next-hop-group statement.....	35

## O

output statement	
port mirroring.....	36

## P

packet analysis.....	4
parentheses, in syntax descriptions.....	xii
port mirroring	
configuration.....	32, 33
configuring for local monitoring.....	13
configuring for remote monitoring.....	16
port mirroring analyzers.....	4

## R

rate statement.....	38
---------------------	----

## S

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

## T

technical support	
contacting JTAC.....	xiii
topic1	
sub-topic.....	44
topic2	
sub-topic.....	44
traffic monitoring.....	4

