

Port Mirroring Analyzers for EX9200 Switches

Release
15.1



Modified: 2015-06-03

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.

Port Mirroring Analyzers for EX9200 Switches

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	Understanding Port Mirroring Analyzers	3
	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
Part 2	Configuring Analyzers	
Chapter 2	Copy Packets to a Local Interface for Local Monitoring	13
	Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure)	13
	Configuring an Analyzer for Local Traffic Analysis	14
	Configuring an Analyzer for Remote Traffic Analysis	14
	Configuring a Statistical Analyzer for Local Traffic Analysis	15
	Configuring a Statistical Analyzer for Remote Traffic Analysis	16
	Binding Statistical Analyzers to Ports Grouped at the FPC Level	17
	Configuring an Analyzer with Multiple Destinations by Using Next-Hop Groups	18
	Defining a Next-Hop Group for Layer 2 Mirroring	18
	Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use	19

Chapter 3	Copy Packets to a VLAN or Bridge Domain for Remote Monitoring	25
	Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure)	25
	Configuring an Analyzer for Local Traffic Analysis	26
	Configuring an Analyzer for Remote Traffic Analysis	27
	Configuring a Statistical Analyzer for Local Traffic Analysis	27
	Configuring a Statistical Analyzer for Remote Traffic Analysis	28
	Binding Statistical Analyzers to Ports Grouped at the FPC Level	29
	Configuring an Analyzer with Multiple Destinations by Using Next-Hop Groups	30
	Defining a Next-Hop Group for Layer 2 Mirroring	31
	Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use	31
	Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches	41
	Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches	50
Part 3	Configuration Statements and Operational Commands	
Chapter 4	Configuration Statements	59
	[edit forwarding-options analyzer] Configuration Statement Hierarchy	59
	egress	60
	egress (Analyzer)	61
	ingress (vlans)	61
	ingress (Analyzer)	62
	input (Analyzer)	63
	interface (Analyzer)	64
	no-tag	65
	output (Mirroring)	66
	vlan (Mirroring)	67
Chapter 5	Operational Commands	69
	show forwarding-options analyzer	70

List of Figures

Part 2	Configuring Analyzers	
Chapter 2	Copy Packets to a Local Interface for Local Monitoring	13
	Figure 1: Network Topology for Local Port Mirroring Example	21
Chapter 3	Copy Packets to a VLAN or Bridge Domain for Remote Monitoring	25
	Figure 2: Network Topology for Remote Port Mirroring and Analysis	33
	Figure 3: Remote Mirroring Example Network Topology Using Multiple VLAN Member Interfaces in the Next-Hop Group	43
	Figure 4: Network Monitoring for Remote Mirroring Through a Transit Switch	51

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	xi
	Table 2: Text and Syntax Conventions	xi
Part 1	Overview	
Chapter 1	Understanding Port Mirroring Analyzers	3
	Table 3: Analyzer Terminology	5
	Table 4: Configuration Guidelines for Port Mirroring Analyzers	7
Part 3	Configuration Statements and Operational Commands	
Chapter 5	Operational Commands	69
	Table 5: show forwarding-options analyzer Output Fields	70

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:

- EX 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.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none">Introduces or emphasizes important new terms.Identifies guide names.Identifies RFC and Internet draft titles.	<ul style="list-style-type: none">A policy <i>term</i> is a named structure that defines match conditions and actions.<i>Junos OS CLI User Guide</i>RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast <i>(string1 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 [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
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 Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>

- Download the latest versions of software and review release notes:
<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications:
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

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

CHAPTER 1

Understanding Port Mirroring Analyzers

- [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"> • The name of the analyzer • Source (input) ports, VLANs, or bridge domains

Table 3: Analyzer Terminology (*continued*)

Term	Description
	<ul style="list-style-type: none"> A destination for mirrored packets (either a monitor port, VLAN, or bridge domain)
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>NOTE: Interfaces used as output for an analyzer must be configured under the forwarding-options hierarchy level.</p> <p>Analyzer output interfaces have the following limitations:</p> <ul style="list-style-type: none"> They cannot also be a source port. They do not participate in Layer 2 protocols, such as the Spanning Tree Protocol (STP), when part of a port-mirroring configuration. If the bandwidth of the analyzer output interface is not sufficient to handle the traffic from the source ports, overflow packets are dropped.
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"> • Statistical analyzers must be bound to an FPC for mirroring traffic on ports belonging to that FPC. <p>NOTE: 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"> Virtual Chassis ports (VCPs) Management Ethernet ports (me0 or vme0) Integrated routing and bridging (IRB) interfaces VLAN-tagged Layer 3 interfaces 	
Protocol families that you can include in an analyzer.	ethernet-switching for EX Series switches and bridge for MX Series routers.	Analyzer mirrors only bridged traffic. For mirroring routed traffic, use the port mirroring configuration with family as inet or inet6 .
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"> The trunk interface has to be a member of all VLANs or bridge domains that are related to the input configuration of analyzer. You must use the mirror-once option if the input has been configured as VLAN or bridge domain and the output is a trunk interface. <p>NOTE: 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 input 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 19](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 31](#)
- [Configuring Mirroring on EX9200 Switches to Analyze Traffic \(CLI Procedure\) on page 13](#)

PART 2

Configuring Analyzers

- [Copy Packets to a Local Interface for Local Monitoring on page 13](#)
- [Copy Packets to a VLAN or Bridge Domain for Remote Monitoring on page 25](#)

CHAPTER 2

Copy Packets to a Local Interface for Local Monitoring

- [Configuring Mirroring on EX9200 Switches to Analyze Traffic \(CLI Procedure\) on page 13](#)
- [Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use on page 19](#)

Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure)

EX9200 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy the following packets:

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



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

- Disable the analyzers that you have configured 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.



NOTE: If you want to create additional analyzers without deleting the existing analyzers, then disable the existing analyzers by using the `disable analyzer analyzer-name` statement from the command-line-interface (CLI) or from the J-Web configuration page for mirroring.



NOTE: Interfaces used as output for an analyzer must be configured under the `ethernet-switching` family.

- [Configuring an Analyzer for Local Traffic Analysis on page 14](#)
- [Configuring an Analyzer for Remote Traffic Analysis on page 14](#)
- [Configuring a Statistical Analyzer for Local Traffic Analysis on page 15](#)
- [Configuring a Statistical Analyzer for Remote Traffic Analysis on page 16](#)
- [Binding Statistical Analyzers to Ports Grouped at the FPC Level on page 17](#)
- [Configuring an Analyzer with Multiple Destinations by Using Next-Hop Groups on page 18](#)
- [Defining a Next-Hop Group for Layer 2 Mirroring on page 18](#)

Configuring an Analyzer for Local Traffic Analysis

To mirror interface traffic or VLAN traffic on the switch to an interface on the switch by using analyzers:

1. Choose a name for the analyzer and specify the input:

```
[edit forwarding-options]
user@switch# set analyzer (Port Mirroring) analyzer-name input ingress interface
interface-name
```

For example, create an analyzer called **employee-monitor** for which the input traffic comprises packets entering interfaces `ge-0/0/0.0` and `ge-0/0/1.0`:

```
[edit forwarding-options]
user@switch# set analyzer (Port Mirroring) employee-monitor input ingress interface
ge-0/0/0.0
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Configure the destination interface for the mirrored packets:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output interface interface-name
```

For example, configure `ge-0/0/10.0` as the destination interface for the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

Configuring an Analyzer for Remote Traffic Analysis

To mirror traffic that is traversing interfaces or a VLAN on the switch to a VLAN for analysis from a remote location (by using analyzers):

1. Configure a VLAN to carry the mirrored traffic:

```
[edit]
user@switch# set vlans analyzer-name vlan-id vlan-ID
```

For example, define an analyzer VLAN called **remote-analyzer** and assign it the VLAN ID **999**:

```
[edit]
```

```
user@switch# set vlans remote-analyzer vlan-id 999
```

2. Set the uplink module interface that is connected to the distribution switch to access mode and associate it with the analyzer VLAN:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching interface-mode
access vlan members vlan-ID
```

For example, set the interface ge-0/1/1 to access mode and associate it with the analyzer VLAN ID 999:

```
[edit]
user@switch# set interfaces ge-0/1/1 unit 0 family ethernet-switching interface-mode access
vlan members 999
```

3. Configure the analyzer:

- a. Define an analyzer and specify the traffic to be mirrored:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input ingress interface interface-name
```

For example, define the **employee-monitor** analyzer for which traffic to be mirrored comprises packets entering interfaces ge-0/0/0.0 and ge-0/0/1.0:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

- b. Specify the analyzer VLAN as the output for the analyzer:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output vlan vlan-ID
```

For example, specify the **remote-analyzer** VLAN as the output analyzer for the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output vlan 999
```

Configuring a Statistical Analyzer for Local Traffic Analysis

To mirror interface traffic or VLAN traffic on the switch to an interface on the switch by using a statistical analyzer:

1. Choose a name for the analyzer and specify the input interfaces:

```
[edit forwarding-options]
user@switch# set analyzer (Port Mirroring) analyzer-name input ingress interface
interface-name
```

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

For example, specify an analyzer called **employee-monitor** and specify the input interfaces ge-0/0/0 and ge-0/0/1:

```
[edit forwarding-options]
user@switch# set analyzer (Port Mirroring) employee-monitor input ingress interface
ge-0/0/0.0
```

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Configure the destination interface for the mirrored packets:

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

```
user@switch# set analyzer employee-monitor output interface interface-name
```

For example, configure ge-0/0/10.0 as the destination interface for the mirrored packets:

```
[edit forwarding-options]  
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

3. Specify mirroring properties.

- a. Specify the mirroring rate—that is, the number of packets to be mirrored per second:

```
[edit forwarding-options]  
user@switch# set analyzer employee-monitor input rate number
```

The valid range is 1 through 65,535.

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

```
[edit forwarding-options]  
user@switch# set analyzer employee-monitor input maximum-packet-length number
```

The valid range is 0 through 9216. The default value is 0, which indicates that mirrored packets are not truncated.

Configuring a Statistical Analyzer for Remote Traffic Analysis

To mirror traffic that is traversing interfaces or a VLAN on the switch to a VLAN for analysis from a remote location by using a statistical analyzer:

1. Configure a VLAN to carry the mirrored traffic:

```
[edit]  
user@switch# set vlans vlan-name vlan-id vlan-ID
```

For example, configure a VLAN called **remote-analyzer** with VLAN ID **999**:

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

2. Set the uplink module interface that is connected to the distribution switch to access mode and associate it with the VLAN:

```
[edit]  
user@switch# set interfaces interface-name unit 0 family ethernet-switching interface-mode  
access vlan members vlan-ID
```

For example, set the uplink module interface ge-0/1/1.0 that is connected to the distribution switch to access mode and associate it with the **remote-analyzer** VLAN:

```
[edit]  
user@switch# set interfaces ge-0/1/1.0 unit 0 family ethernet-switching interface-mode  
access vlan members 999
```

3. Configure the statistical analyzer:

- a. Specify the traffic to be mirrored:

```
[edit forwarding-options]  
user@switch# set analyzer analyzer-name input ingress interface interface-name
```

For example, specify the packets entering ports ge-0/0/0.0 and ge-0/0/1.0 to be mirrored:

```
[edit forwarding-options]  
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0  
[edit forwarding-options]  
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

- b. Specify an output for the analyzer:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output vlan vlan-ID
```

For example, specify the **remote-analyzer** VLAN as the output for the analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output vlan 999
```

4. Specify mirroring properties.

- a. Specify the mirroring rate—that is, the number of packets to be mirrored per second:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input rate number
```

The valid range is 1 through 65,535.

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

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input maximum-packet-length number
```

The valid range is 0 through 9216. The default value is 0, which means the mirrored packets are not truncated.

Binding Statistical Analyzers to Ports Grouped at the FPC Level

You can bind a statistical analyzer to a specific FPC in the switch, that is, you can bind the statistical analyzer instance at the FPC level of the switch. The mirroring properties specified in the statistical analyzer are applied to all physical ports associated with all Packet Forwarding Engines on the specified FPC.

To bind a named instance of Layer 2 analyzer to an FPC:

1. Enable configuration of switch chassis properties:

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

2. Enable configuration of an FPC (and its installed PICs):

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

3. Bind a statistical analyzer instance to the FPC:

```
[edit chassis fpc slot-number]
user@switch# set port-mirror-instance stats_analyzer-1
```

4. (Optional) To bind a second statistical analyzer instance of Layer 2 mirroring to the same FPC, repeat Step 3 and specify a different statistical analyzer name:

```
[edit chassis fpc slot-number]
user@switch# set port-mirror-instance stats_analyzer-2
```

5. Verify the minimum configuration of the binding:

```
[edit chassis fpc slot-number port-mirror-instance analyzer_name]
user@switch# top
[edit]
user@switch# show chassis
chassis {
  fpc slot-number { # Bind two statistical analyzers or port mirroring
                    named instances at the FPC level.

```

```
port-mirror-instance stats_analyzer-1;
port-mirror-instance stats_analyzer-2;
    }
}
```



NOTE: On binding a second instance (`stats_analyzer-2` in this example), the mirroring properties of this session, if configured, overrides any default analyzer.

Configuring an Analyzer with Multiple Destinations by Using Next-Hop Groups

On EX9200 switches, you can mirror traffic to multiple destinations by configuring next-hop groups as analyzer output. The mirroring of packets to multiple destinations is also known as multipacket port mirroring.

To mirror interface traffic or VLAN traffic on the switch to an interface on the switch (by using analyzers):

1. Choose a name for the analyzer and specify the input:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input ingress interface interface-name
```

For example, create an analyzer called **employee-monitor** for which the input traffic comprises packets entering interfaces `ge-0/0/0.0` and `ge-0/0/1.0`:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Configure the destination interface for the mirrored packets:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output next-hop-group next-hop-group-name
```

For example, configure the next-hop group **nhg** as the destination for the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output next-hop-group nhg
```

Defining a Next-Hop Group for Layer 2 Mirroring

On EX9200 switches, the next-hop group configuration at the **[edit forwarding-options]** configuration level enables you to define a next-hop group name, the type of addresses to be used in the next-hop group, and the logical interfaces that form the multiple destinations to which traffic can be mirrored. By default, the next-hop group is specified using Layer 3 addresses using the **[edit forwarding-options next-hop-group next-hop-group-name group-type inet]** statement. To specify a next-hop group using Layer 2 addresses instead, include the **[edit forwarding-options next-hop-group next-hop-group-name group-type layer-2]** statement.

To define a next-hop group for Layer 2 mirroring:

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


```
[edit forwarding-options ]
user@switch# set next-hop-group next-hop-group-name
```

For example, configure **next-hop-group** with name **nhg**:

```
[edit forwarding-options]
user@switch# set next-hop-group nhg
```

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

```
[edit forwarding-options next-hop-group next-hop-group-name]
user@switch# set group-type layer-2
```

For example, configure **next-hop-group type** as **layer-2** because the analyzer output must be **layer-2** only:

```
[edit forwarding-options]
user@switch# set next-hop-group nhg group-type layer-2
```

- Specify the logical interfaces of the next-hop group:

```
[edit forwarding-options next-hop-group next-hop-group-name]
user@switch# set interface logical-interface-name-1
user@switch# set interface logical-interface-name-2
```

For example, to specify ge-0/0/10.0 and ge-0/0/11.0 as the logical interfaces of the next-hop group **nhg**:

```
[edit forwarding-options]
user@switch# set next-hop-group nhg interface ge-0/0/10.0
user@switch# set next-hop-group nhg interface ge-0/0/11.0
```

Related Documentation

- [Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use on page 19](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 31](#)
- [Understanding Port Mirroring Analyzers on page 4](#)

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 20](#)
- [Overview and Topology on page 20](#)
- [Mirroring All Employee Traffic for Local Analysis on page 21](#)
- [Verification on page 22](#)

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.

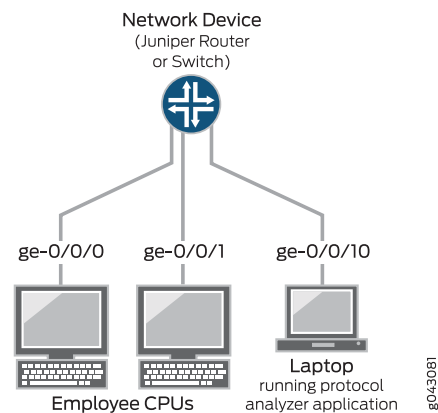
Connect a PC running a protocol analyzer application to the analyzer output interface to analyze the mirrored traffic.



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

[Figure 1 on page 21](#) 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 31](#)
 - [Configuring Mirroring on EX9200 Switches to Analyze Traffic \(CLI Procedure\) on page 13](#)
 - [Understanding Port Mirroring Analyzers on page 4](#)

CHAPTER 3

Copy Packets to a VLAN or Bridge Domain for Remote Monitoring

- [Configuring Mirroring on EX9200 Switches to Analyze Traffic \(CLI Procedure\) on page 25](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 31](#)
- [Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches on page 41](#)
- [Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches on page 50](#)

Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure)

EX9200 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy the following packets:

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



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

- Disable the analyzers that you have configured 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.
-



NOTE: If you want to create additional analyzers without deleting the existing analyzers, then disable the existing analyzers by using the `disable analyzer analyzer-name` statement from the command-line-interface (CLI) or from the J-Web configuration page for mirroring.



NOTE: Interfaces used as output for an analyzer must be configured under the `ethernet-switching` family.

- [Configuring an Analyzer for Local Traffic Analysis on page 26](#)
- [Configuring an Analyzer for Remote Traffic Analysis on page 27](#)
- [Configuring a Statistical Analyzer for Local Traffic Analysis on page 27](#)
- [Configuring a Statistical Analyzer for Remote Traffic Analysis on page 28](#)
- [Binding Statistical Analyzers to Ports Grouped at the FPC Level on page 29](#)
- [Configuring an Analyzer with Multiple Destinations by Using Next-Hop Groups on page 30](#)
- [Defining a Next-Hop Group for Layer 2 Mirroring on page 31](#)

Configuring an Analyzer for Local Traffic Analysis

To mirror interface traffic or VLAN traffic on the switch to an interface on the switch by using analyzers:

1. Choose a name for the analyzer and specify the input:

```
[edit forwarding-options]
user@switch# set analyzer (Port Mirroring) analyzer-name input ingress interface
interface-name
```

For example, create an analyzer called **employee-monitor** for which the input traffic comprises packets entering interfaces `ge-0/0/0.0` and `ge-0/0/1.0`:

```
[edit forwarding-options]
user@switch# set analyzer (Port Mirroring) employee-monitor input ingress interface
ge-0/0/0.0
```

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Configure the destination interface for the mirrored packets:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output interface interface-name
```

For example, configure `ge-0/0/10.0` as the destination interface for the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```


Configuring an Analyzer for Remote Traffic Analysis

To mirror traffic that is traversing interfaces or a VLAN on the switch to a VLAN for analysis from a remote location (by using analyzers):

1. Configure a VLAN to carry the mirrored traffic:

```
[edit]
user@switch# set vlans analyzer-name vlan-id vlan-ID
```

For example, define an analyzer VLAN called **remote-analyzer** and assign it the VLAN ID **999**:

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

2. Set the uplink module interface that is connected to the distribution switch to access mode and associate it with the analyzer VLAN:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching interface-mode access vlan members vlan-ID
```

For example, set the interface **ge-0/1/1** to access mode and associate it with the analyzer VLAN ID **999**:

```
[edit]
user@switch# set interfaces ge-0/1/1 unit 0 family ethernet-switching interface-mode access vlan members 999
```

3. Configure the analyzer:

- a. Define an analyzer and specify the traffic to be mirrored:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input ingress interface interface-name
```

For example, define the **employee-monitor** analyzer for which traffic to be mirrored comprises packets entering interfaces **ge-0/0/0.0** and **ge-0/0/1.0**:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

- b. Specify the analyzer VLAN as the output for the analyzer:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output vlan vlan-ID
```

For example, specify the **remote-analyzer** VLAN as the output analyzer for the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output vlan 999
```

Configuring a Statistical Analyzer for Local Traffic Analysis

To mirror interface traffic or VLAN traffic on the switch to an interface on the switch by using a statistical analyzer:

1. Choose a name for the analyzer and specify the input interfaces:

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

```
user@switch# set analyzer (Port Mirroring) analyzer-name input ingress interface interface-name
```

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

```
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

For example, specify an analyzer called **employee-monitor** and specify the input interfaces ge-0/0/0 and ge-0/0/1:

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

```
user@switch# set analyzer (Port Mirroring) employee-monitor input ingress interface ge-0/0/0.0
```

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

```
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Configure the destination interface for the mirrored packets:

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

```
user@switch# set analyzer employee-monitor output interface interface-name
```

For example, configure ge-0/0/10.0 as the destination interface for the mirrored packets:

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

```
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

3. Specify mirroring properties.

- a. Specify the mirroring rate—that is, the number of packets to be mirrored per second:

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

```
user@switch# set analyzer employee-monitor input rate number
```

The valid range is 1 through 65,535.

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

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

```
user@switch# set analyzer employee-monitor input maximum-packet-length number
```

The valid range is 0 through 9216. The default value is 0, which indicates that mirrored packets are not truncated.

Configuring a Statistical Analyzer for Remote Traffic Analysis

To mirror traffic that is traversing interfaces or a VLAN on the switch to a VLAN for analysis from a remote location by using a statistical analyzer:

1. Configure a VLAN to carry the mirrored traffic:

```
[edit]
```

```
user@switch# set vlans vlan-name vlan-id vlan-ID
```

For example, configure a VLAN called **remote-analyzer** with VLAN ID 999:

```
[edit]
```

```
user@switch# set vlans remote-analyzer vlan-id 999
```

2. Set the uplink module interface that is connected to the distribution switch to access mode and associate it with the VLAN:

```
[edit]
```

```
user@switch# set interfaces interface-name unit 0 family ethernet-switching interface-mode access vlan members vlan-ID
```

For example, set the uplink module interface ge-0/1/1.0 that is connected to the distribution switch to access mode and associate it with the **remote-analyzer** VLAN:

```
[edit]
user@switch# set interfaces ge-0/1/1.0 unit 0 family ethernet-switching interface-mode
access vlan members 999
```

3. Configure the statistical analyzer:

a. Specify the traffic to be mirrored:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input ingress interface interface-name
```

For example, specify the packets entering ports ge-0/0/0.0 and ge-0/0/1.0 to be mirrored:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

b. Specify an output for the analyzer:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output vlan vlan-ID
```

For example, specify the **remote-analyzer** VLAN as the output for the analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output vlan 999
```

4. Specify mirroring properties.

a. Specify the mirroring rate—that is, the number of packets to be mirrored per second:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input rate number
```

The valid range is 1 through 65,535.

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

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input maximum-packet-length number
```

The valid range is 0 through 9216. The default value is 0, which means the mirrored packets are not truncated.

Binding Statistical Analyzers to Ports Grouped at the FPC Level

You can bind a statistical analyzer to a specific FPC in the switch, that is, you can bind the statistical analyzer instance at the FPC level of the switch. The mirroring properties specified in the statistical analyzer are applied to all physical ports associated with all Packet Forwarding Engines on the specified FPC.

To bind a named instance of Layer 2 analyzer to an FPC:

1. Enable configuration of switch chassis properties:

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

2. Enable configuration of an FPC (and its installed PICs):

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

3. Bind a statistical analyzer instance to the FPC:

```
[edit chassis fpc slot-number]
user@switch# set port-mirror-instance stats_analyzer-1
```

4. (Optional) To bind a second statistical analyzer instance of Layer 2 mirroring to the same FPC, repeat Step 3 and specify a different statistical analyzer name:

```
[edit chassis fpc slot-number]
user@switch# set port-mirror-instance stats_analyzer-2
```

5. Verify the minimum configuration of the binding:

```
[edit chassis fpc slot-number port-mirror-instance analyzer_name]
user@switch# top
[edit]
user@switch# show chassis
chassis {
  fpc slot-number { # Bind two statistical analyzers or port mirroring
                    named instances at the FPC level.
    port-mirror-instance stats_analyzer-1;
    port-mirror-instance stats_analyzer-2;
  }
}
```



NOTE: On binding a second instance (stats_analyzer-2 in this example), the mirroring properties of this session, if configured, overrides any default analyzer.

Configuring an Analyzer with Multiple Destinations by Using Next-Hop Groups

On EX9200 switches, you can mirror traffic to multiple destinations by configuring next-hop groups as analyzer output. The mirroring of packets to multiple destinations is also known as multipacket port mirroring.

To mirror interface traffic or VLAN traffic on the switch to an interface on the switch (by using analyzers):

1. Choose a name for the analyzer and specify the input:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input ingress interface interface-name
```

For example, create an analyzer called **employee-monitor** for which the input traffic comprises packets entering interfaces ge-0/0/0.0 and ge-0/0/1.0:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Configure the destination interface for the mirrored packets:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output next-hop-group next-hop-group-name
```

For example, configure the next-hop group **nhg** as the destination for the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output next-hop-group nhg
```

Defining a Next-Hop Group for Layer 2 Mirroring

On EX9200 switches, the next-hop group configuration at the **[edit forwarding-options]** configuration level enables you to define a next-hop group name, the type of addresses to be used in the next-hop group, and the logical interfaces that form the multiple destinations to which traffic can be mirrored. By default, the next-hop group is specified using Layer 3 addresses using the **[edit forwarding-options next-hop-group next-hop-group-name group-type inet]** statement. To specify a next-hop group using Layer 2 addresses instead, include the **[edit forwarding-options next-hop-group next-hop-group-name group-type layer-2]** statement.

To define a next-hop group for Layer 2 mirroring:

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

```
[edit forwarding-options ]
user@switch# set next-hop-group next-hop-group-name
```

For example, configure **next-hop-group** with name **nhg**:

```
[edit forwarding-options]
user@switch# set next-hop-group nhg
```

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

```
[edit forwarding-options next-hop-group next-hop-group-name]
user@switch# set group-type layer-2
```

For example, configure **next-hop-group type** as **layer-2** because the analyzer output must be **layer-2** only:

```
[edit forwarding-options]
user@switch# set next-hop-group nhg group-type layer-2
```

3. Specify the logical interfaces of the next-hop group:

```
[edit forwarding-options next-hop-group next-hop-group-name]
user@switch# set interface logical-interface-name-1
user@switch# set interface logical-interface-name-2
```

For example, to specify ge-0/0/10.0 and ge-0/0/11.0 as the logical interfaces of the next-hop group **nhg**:

```
[edit forwarding-options]
user@switch# set next-hop-group nhg interface ge-0/0/10.0
user@switch# set next-hop-group nhg interface ge-0/0/11.0
```

Related Documentation

- [Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use on page 19](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 31](#)
- [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 32](#)
- [Overview and Topology on page 33](#)
- [Mirroring Employee Traffic for Remote Analysis Using a Statistical Analyzer on page 33](#)
- [Verification on page 41](#)

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:

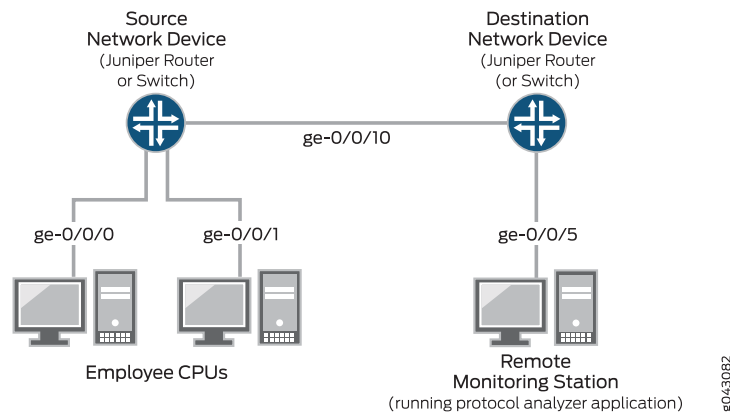
- You have an understanding of mirroring concepts. For information about analyzers, see [“Understanding Port Mirroring Analyzers” on page 4](#). For information about port mirroring, see *Layer 2 Port Mirroring Overview*.
- The interfaces that the analyzer will use as input interfaces have already been 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 33 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 33](#)
- [Mirroring Employee Traffic for Remote Analysis for MX Series Routers on page 37](#)

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 19](#)
 - [Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches on page 41](#)
 - [Configuring Mirroring on EX9200 Switches to Analyze Traffic \(CLI Procedure\) on page 13](#)
 - [Understanding Port Mirroring Analyzers on page 4](#)

Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches

EX9200 switches allow you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port

- Packets entering or exiting a VLAN on

You can analyze the mirrored traffic using a protocol analyzer application running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.



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

- Disable your configured mirroring analyzers 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.

This example describes how to configure remote mirroring to multiple interfaces on an analyzer VLAN:

- [Requirements on page 42](#)
- [Overview and Topology on page 42](#)
- [Mirroring All Employee Traffic to Multiple VLAN Member Interfaces for Remote Analysis on page 44](#)
- [Verification on page 48](#)

Requirements

This example uses the following hardware and software components:

- Three EX9200 switches
- Junos OS Release 13.2 or later for EX Series switches

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 been configured on the switch.

Overview and Topology

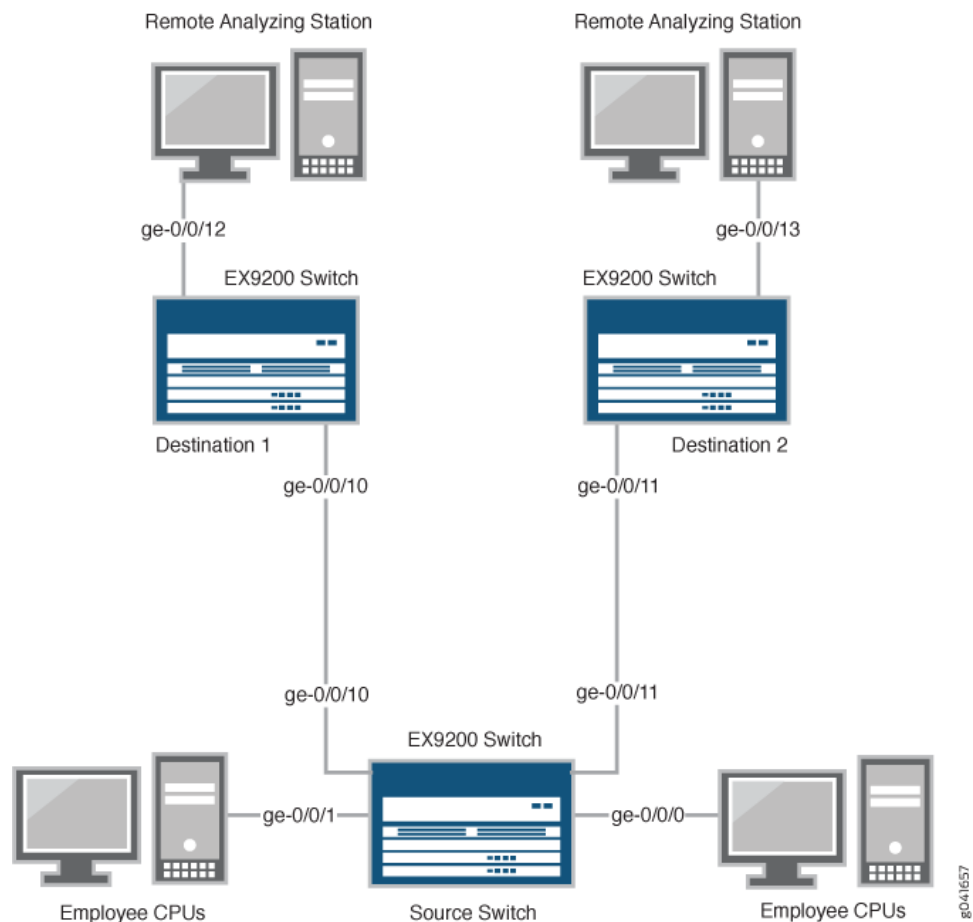
This example describes how to mirror traffic entering ports on the switch to the remote analyzer VLAN so that you can perform analysis from a remote monitoring station. The remote-analyzer VLAN in this example contains multiple member interfaces. Therefore,

the same traffic is mirrored to all member interfaces of the remote-analyzer VLAN so that mirrored packets can be sent to different remote monitoring stations. You can install applications, such as sniffers and intrusion detection systems, on remote monitoring stations to analyze these mirrored packets and to obtain useful statistical data. For instance, if there are two remote monitoring stations, you can install a sniffer on one remote monitoring station and an intrusion detection system on the other station. You can use a firewall filter analyzer configuration to forward a specific type of traffic to a remote monitoring station.

This example describes how to configure an analyzer to mirror traffic to multiple interfaces in the next-hop group so that traffic is sent to different monitoring stations for analysis.

Figure 3 on page 43 shows the network topology for this example.

Figure 3: Remote Mirroring Example Network Topology Using Multiple VLAN Member Interfaces in the Next-Hop Group



g041657

In this example:

- Interfaces ge-0/0/0 and ge-0/0/1 are Layer 2 interfaces (both interfaces on the source switch) that serve as connections for employee computers.
- Interfaces ge-0/0/10 and ge-0/0/11 are Layer 2 interfaces that are connected to different destination switches.
- Interface ge-0/0/12 is a Layer 2 interface that connects the Destination 1 switch to the remote monitoring station.
- Interface ge-0/0/13 is a Layer 2 interface that connects the Destination 2 switch to the remote monitoring station.
- VLAN **remote-analyzer** is configured on all switches in the topology to carry the mirrored traffic.

Mirroring All Employee Traffic to Multiple VLAN Member Interfaces for Remote Analysis

To configure mirroring to multiple VLAN member interfaces for remote traffic analysis for all incoming and outgoing employee traffic, perform these tasks:

CLI Quick Configuration

To quickly configure mirroring for remote traffic analysis for incoming and outgoing employee traffic, copy the following commands and paste them into the switch terminal window:

- In the source switch terminal window, copy and paste the following commands:

```
[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-0/0/11 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/11 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 next-hop-group remote-analyzer-nhg
set forwarding-options next-hop-group remote-analyzer-nhg interface ge-0/0/10.0
set forwarding-options next-hop-group remote-analyzer-nhg interface ge-0/0/11.0
set forwarding-options next-hop-group remote-analyzer-nhg group-type layer-2
```

- In the Destination 1 switch terminal window, copy and paste the following commands:

```
[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-0/0/12 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 loss-priority high output interface
ge-0/0/12.0
```

- In the Destination 2 switch terminal window, copy and paste the following commands:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/11 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/13 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 loss-priority high output interface
ge-0/0/13.0
```

Step-by-Step Procedure

To configure basic remote mirroring to two VLAN member interfaces:

1. On the source switch:

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

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

- Configure the interfaces on the network port connected to destination switches for access mode and associate it with the **remote-analyzer** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
user@switch# set ge-0/0/11 unit 0 family ethernet-switching interface-mode trunk
user@switch# set ge-0/0/11 unit 0 family ethernet-switching vlan members 999
```

- Configure the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
user@switch# set analyzer employee-monitor input egress interface ge-0/0/0.0
user@switch# set analyzer employee-monitor input egress interface ge-0/0/1.0
user@switch# set analyzer employee-monitor output next-hop-group
remote-analyzer-nhg
```

In this analyzer configuration, traffic that enters and exits interfaces ge-0/0/0.0 and ge-0/0/1.0 are sent to the output destination defined by the next-hop group named **remote-analyzer-nhg**.

- Configure the **remote-analyzer-nhb** next-hop group:

```
[edit forwarding-options]
user@switch# set next-hop-group remote-analyzer-nhg interface ge-0/0/10.0
user@switch# set next-hop-group remote-analyzer-nhg interface ge-0/0/11.0
user@switch# set next-hop-group remote-analyzer-nhg group-type layer-2
```

2. On the Destination 1 switch:

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

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

- Configure the ge-0/0/10 interface on the Destination 1 switch for access mode:

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

- Configure the interface connected to the remote monitoring station for access mode:

```
[edit interfaces]
user@switch# set ge-0/0/12 unit 0 family ethernet-switching interface-mode access
```

- Configure the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor loss-priority high output interface
ge-0/0/12.0
```

3. On the Destination 2 switch:

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

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

- Configure the ge-0/0/11 interface on the Destination 2 switch for access mode:

```
[edit interfaces]
user@switch# set ge-0/0/11 unit 0 family ethernet-switching interface-mode access
```

- Configure the interface connected to the remote monitoring station for access mode:

```
[edit interfaces]
user@switch# set ge-0/0/13 unit 0 family ethernet-switching interface-mode access
```

- Configure the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor loss-priority high output interface
ge-0/0/13.0
```

Results Check the results of the configuration on the source switch:

```
[edit]
user@switch# 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;
      }
    }
    output {
      next-hop-group {
        remote-analyzer-nhg;
      }
    }
  }
}
vllans {
  remote-analyzer {
    vlan-id 999;
    interface {
      ge-0/0/10.0
      ge-0/0/11.0
    }
  }
}
interfaces {
  ge-0/0/10 {
    unit 0 {
```

```

        family ethernet-switching {
            interface-mode access;
        }
    }
}
ge-0/0/11 {
    unit 0 {
        family ethernet-switching {
            interface-mode access;
        }
    }
}
}
}

```

Check the results of the configuration on the Destination 1 switch:

```

[edit]
user@switch# show
vpls {
    remote-analyzer {
        vlan-id 999;
    }
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            ethernet-switching {
                interface-mode access;
            }
        }
    }
    ge-0/0/12 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
}
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                vlan remote-analyzer;
            }
        }
        loss-priority high;
        output {
            interface {
                ge-0/0/12.0;
            }
        }
    }
}
}

```

Check the results of the configuration on the Destination 2 switch:

```
[edit]
user@switch# show
vpls {
  remote-analyzer {
    vlan-id 999;
    interface {
      ge-0/0/11.0
    }
  }
}
interfaces {
  ge-0/0/11 {
    unit 0 {
      family ethernet-switching {
        interface-mode access;
      }
    }
  }
  ge-0/0/13 {
    unit 0 {
      family ethernet-switching {
        interface-mode access;
      }
    }
  }
}
forwarding-options {
  employee-monitor {
    input {
      ingress {
        vlan remote-analyzer;
      }
    }
    loss-priority high;
    output {
      interface {
        ge-0/0/13.0;
      }
    }
  }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying That the Analyzer Has Been Correctly Created on page 48](#)

Verifying That the Analyzer Has Been Correctly Created

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

Action You can verify the analyzer is configured as expected by using the **show forwarding-options analyzer** command.

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

```
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
Egress monitored interfaces : ge-0/0/0.0
Egress monitored interfaces : ge-0/0/1.0
Output nhg              : remote-analyzer-nhg

user@switch> show forwarding-options next-hop-group
Next-hop-group: remote-analyzer-nhg
Type: layer-2
State: up
Members Interfaces:
  ge-0/0/10.0
  ge-0/0/11.0
```

Meaning This output shows that the **employee-monitor** analyzer has a ratio of 1 (mirroring every packet, which is the default behavior), the state of the configuration is **up**, which indicates proper state and that the analyzer is programmed, mirrors traffic entering or exiting interfaces ge-0/0/0 and ge-0/0/1, and sends mirrored traffic to multiple interfaces ge-0/0/10.0 and ge-0/0/11.0 through the next-hop-group **remote-analyzer-nhg**. 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 19](#)
 - [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 31](#)
 - [Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches on page 50](#)
 - [Configuring Mirroring on EX9200 Switches to Analyze Traffic \(CLI Procedure\) on page 13](#)
 - [Understanding Port Mirroring Analyzers on page 4](#)

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches

EX9200 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy these packets:

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

You can analyze the mirrored traffic using a protocol analyzer application running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.

This topic includes an example that describes how to mirror traffic entering ports on the switch to the remote-analyzer VLAN through a transit switch, so that you can perform analysis from a remote monitoring station.



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

- 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.

This example describes how to configure remote mirroring through a transit switch:

- [Requirements on page 50](#)
- [Overview and Topology on page 51](#)
- [Mirroring All Employee Traffic for Remote Analysis Through a Transit Switch on page 52](#)
- [Verification on page 56](#)

Requirements

This example uses the following hardware and software components:

- An EX9200 switch connected to another EX9200 switch through a third EX9200 switch
- Junos OS Release 13.2 or later for EX Series switches

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 been configured on the switch.

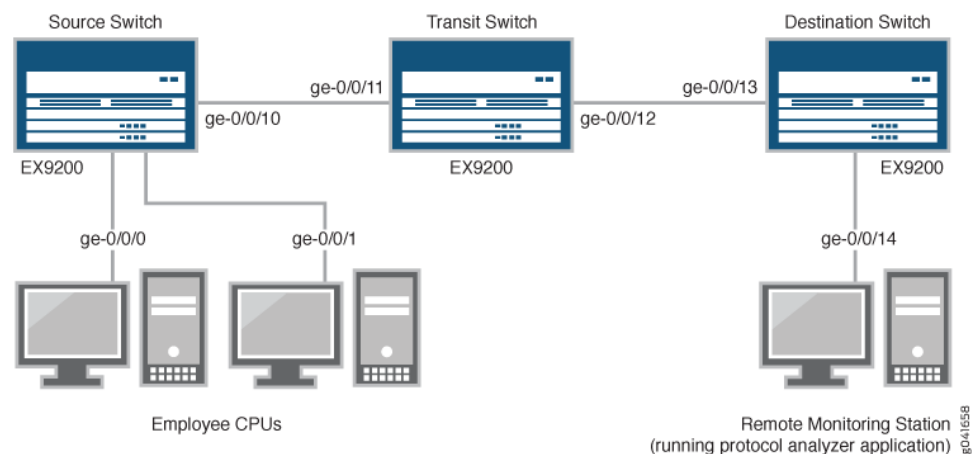
Overview and Topology

This example describes how to mirror traffic entering ports on the switch to the **remote-analyzer** VLAN through a transit switch so that you can perform analysis from a remote monitoring station. The example shows how to configure a switch to mirror all traffic from employee computers to a remote analyzer.

In this configuration, an analyzer session is required on the destination switch to mirror incoming traffic from the analyzer VLAN to the egress interface to which the remote monitoring station is connected.

[Figure 4 on page 51](#) shows the network topology for this example.

Figure 4: Network Monitoring for Remote Mirroring Through a Transit Switch



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 switch) that serve as connections for employee computers.
- Interface ge-0/0/10 is a Layer 2 interface that connects to the transit switch.
- Interface ge-0/0/11 is a Layer 2 interface on the transit switch.
- Interface ge-0/0/12 is a Layer 2 interface on the transit switch and connects to the destination switch.
- Interface ge-0/0/13 is a Layer 2 interface on the destination switch.

- f. Interface ge-0/0/14 is a Layer 2 interface on the destination switch and connects to the remote monitoring station.
- g. VLAN **remote-analyzer** is configured on all switches in the topology to carry the mirrored traffic.

Mirroring All Employee Traffic for Remote Analysis Through a Transit Switch

To configure mirroring for remote traffic analysis through a transit switch, for all incoming and outgoing employee traffic, perform these tasks:

CLI Quick Configuration To quickly configure mirroring for remote traffic analysis through a transit switch, for incoming and outgoing employee traffic, copy the following commands and paste them into the switchterminal window:

- Copy and paste the following commands in the source switch (monitored switch) terminal window:

```
[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
```

- Copy and paste the following commands in the transit switch window:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/11 unit 0 family ethernet-switching interface-mode access
set vlans remote-analyzer interface ge-0/0/11
set interfaces ge-0/0/12 unit 0 family ethernet-switching interface-mode access
set vlans remote-analyzer interface ge-0/0/12
```

- Copy and paste the following commands in the destination switch window:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/13 unit 0 family ethernet-switching interface-mode access
set vlans remote-analyzer interface ge-0/0/13 ingress
set interfaces ge-0/0/14 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-0/0/14.0
```

Step-by-Step Procedure To configure remote mirroring through a transit switch:

1. On the source switch:

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

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

- Configure the interfaces on the network port connected to transit switch for access mode and associate it with the **remote-analyzer** VLAN:

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

```
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure the **employee-monitor** analyzer:

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

2. On the transit switch:

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

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

- Configure the ge-0/0/11 interface for access mode, associate it with the **remote-analyzer** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/11 unit 0 family ethernet-switching interface-mode access
```

- Configure the ge-0/0/12 interface for access mode, associate it with the **remote-analyzer** VLAN, and set the interface for egress traffic only:

```
[edit interfaces]
user@switch# set ge-0/0/12 unit 0 family ethernet-switching interface-mode access
user@switch# set vlans remote-analyzer interface ge-0/0/12
```

3. On the destination switch:

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

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

- Configure the ge-0/0/13 interface for access mode, associate it with the **remote-analyzer** VLAN, and set the interface for ingress traffic only:

```
[edit interfaces]
user@switch# set ge-0/0/13 unit 0 family ethernet-switching interface-mode access
user@switch# set vlans remote-analyzer interface ge-0/0/13 ingress
```

- Configure the interface connected to the remote monitoring station for access mode:

```
[edit interfaces]
user@switch# set ge-0/0/14 unit 0 family ethernet-switching interface-mode access
```

- Configure the **employee-monitor** analyzer:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor output interface ge-0/0/14.0
```

Results Check the results of the configuration on the source switch:

```
[edit]
user@switch> 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;
    }
}
output {
    vlan {
        remote-analyzer;
    }
}
}
vlangs {
    remote-analyzer {
        vlan-id 999;
    }
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    member 999;
                }
            }
        }
    }
}
}
```

Check the results of the configuration on the transit switch:

```
[edit]
user@switch> show
vlangs {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/11.0 {
            }
            ge-0/0/12.0 {
            }
        }
    }
}
interfaces {
    ge-0/0/11 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
    ge-0/0/12 {
```

```
    unit 0 {  
        family ethernet-switching {  
            interface-mode access;  
        }  
    }  
}  
}
```

Check the results of the configuration on the destination switch:

```
[edit]  
user@switch> show  
vlans {  
    remote-analyzer {  
        vlan-id 999;  
        interface {  
            ge-0/0/13.0 {  
                ingress;  
            }  
        }  
    }  
}  
interfaces {  
    ge-0/0/13 {  
        unit 0 {  
            family ethernet-switching {  
                interface-mode access;  
            }  
        }  
    }  
    ge-0/0/14 {  
        unit 0 {  
            family ethernet-switching {  
                interface-mode access;  
            }  
        }  
    }  
}  
forwarding-options {  
    analyzer employee-monitor {  
        input {  
            ingress {  
                vlan remote-analyzer;  
            }  
        }  
        output {  
            interface {  
                ge-0/0/14.0;  
            }  
        }  
    }  
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying That the Analyzer Has Been Correctly Created on page 56](#)

Verifying That the Analyzer Has Been Correctly Created

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

Action You can verify the analyzer is configured as expected by using the **show forwarding-options analyzer** command.

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

```
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
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** analyzer has a mirroring ratio of 1 (mirroring every packet, the default), the state of the configuration is **up**, which indicates proper state and that the analyzer is programmed, is mirroring the traffic entering ge-0/0/0 and ge-0/0/1, and is sending the mirrored traffic to the analyzer 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 for Remote Monitoring of Employee Resource Use on page 31](#)
 - [Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches on page 41](#)
 - [Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use on page 19](#)
 - [Configuring Mirroring on EX9200 Switches to Analyze Traffic \(CLI Procedure\) on page 13](#)
 - [Understanding Port Mirroring Analyzers on page 4](#)

PART 3

Configuration Statements and Operational Commands

- Configuration Statements on page 59
- Operational Commands on page 69

CHAPTER 4

Configuration Statements

- [\[edit forwarding-options analyzer\] Configuration Statement Hierarchy on page 59](#)
- [egress on page 60](#)
- [egress \(Analyzer\) on page 61](#)
- [ingress \(vlangs\) on page 61](#)
- [ingress \(Analyzer\) on page 62](#)
- [input \(Analyzer\) on page 63](#)
- [interface \(Analyzer\) on page 64](#)
- [no-tag on page 65](#)
- [output \(Mirroring\) on page 66](#)
- [vlan \(Mirroring\) on page 67](#)

[\[edit forwarding-options analyzer\] 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*

egress

Syntax	egress;
Hierarchy Level	[edit vlans <i>vlan-name</i> <i>vlan-id</i> <i>number</i> interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 10.0 for EX Series switches.
Description	Specify that the member interface of the VLAN allows only egress traffic.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches</i>

egress (Analyzer)

Syntax	<pre>egress { bridge-domain <i>bridge-domain-name</i>; interface (all <i>interface-name</i>); routing-instance { <i>instance-name</i> { bridge-domain <i>bridge-domain-name</i>; } } }</pre>
Hierarchy Level	[edit forwarding-options analyzer <i>analyzer-name</i> input]
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	Specify ports where traffic exiting the interface is to be mirrored in a mirroring configuration. 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"> • Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches on page 50

ingress (vlands)

Syntax	ingress;
Hierarchy Level	[edit vlands <i>vlan-name</i> vlan-id <i>number</i> interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 10.0 for EX Series switches.
Description	Specify that the member interface of the VLAN allows only ingress traffic.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches

ingress (Analyzer)

Syntax 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*);
 }

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

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 ports, routing instances, VLANs, or bridge domains for which the entering traffic is mirrored as part of a mirroring configuration.

 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 Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches on page 50](#)

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 19](#)
 - [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 31](#)
 - [Understanding Port Mirroring Analyzers on page 4](#)

interface (Analyzer)

Syntax	<code>interface (all <i>interface-name</i>);</code>
Hierarchy Level	[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]
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 interfaces for which traffic is mirrored.
Options	<p>all—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 all keyword, or use the all keyword in combination with setting a ratio for statistical sampling. The all keyword is not available for the [edit forwarding-options analyzer <i>analyzer-name</i> output] hierarchy level.</p> <p><i>interface-name</i>—Apply mirroring to the specified interface only.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Port Mirroring Analyzers for Local Monitoring of Employee Resource Use on page 19• Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 31• Understanding Port Mirroring Analyzers on page 4

no-tag

Syntax	no-tag;
Hierarchy Level	[edit [edit forwarding-options analyzer] Configuration Statement Hierarchy on page 59 analyzer-name output vlan (vlan-id vlan-name)]
Release Information	Statement introduced in Junos OS Release 11.3 for EX Series switches. Hierarchy level [edit forwarding-options] introduced in Junos OS Release 13.2X50-D10 (ELS).
Description	Specify that remote mirroring packets are not tagged.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches</i> • <i>Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches</i>

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 19](#)
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 31](#)

vlan (Mirroring)

Syntax	<code>vlan (<i>vlan-id</i> <i>vlan-name</i>);</code>
Hierarchy Level	<p>[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>]</p>
Release Information	Statement introduced in Junos OS Release 13.2X50-D10 (ELS).
Description	Configure mirrored traffic to be sent to a VLAN for remote monitoring.
Options	<p><i>vlan-id</i>—Numeric VLAN identifier.</p> <p><i>vlan-name</i>—Name of the VLAN.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches on page 50 • Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on page 31

CHAPTER 5

Operational Commands

- `show forwarding-options analyzer`

show forwarding-options analyzer

Syntax	show forwarding-options analyzer <i>analyzer-name</i>
Release Information	Hierarchy level [edit forwarding-options] introduced in Junos OS Release 13.2X50-D10 (ELS).
Description	Display information about analyzers configured for mirroring.
Options	<i>analyzer-name</i> —(Optional) Displays the status of a specific analyzer on the switch.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> <i>Understanding Port Mirroring and Analyzers on EX4300 Switches</i>
List of Sample Output	show forwarding-options analyzer on page 70
Output Fields	Table 5 on page 70 lists the output fields for the show forwarding-options analyzer 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

