Junos® OS for EX Series Ethernet Switches

Analyzers for EX9200 Switches

Release
13.3

Published: 2014-07-15

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS for EX Series Ethernet Switches Analyzers for EX9200 Switches
Release 13.3

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

List of Figures

List of Tables

About the Documentation

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.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	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** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** ***metric*****>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  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.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.

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

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Analyzers

Understanding Analyzers on EX9200 Switches

Mirroring might be needed for traffic analysis on a switch because a switch, unlike a hub, does not broadcast packets to every port on the destination device. The switch sends packets only to the port to which the destination device is connected. You can use analyzers to facilitate analyzing traffic on your Juniper Networks EX9200 Ethernet Switch on a packet level. You can configure an analyzer to mirror bridged packets (Layer 2 packets). To mirror routed packets (Layer 3 packets), you can use a port-mirroring configuration in which the **family** statement is set to **inet** or **inet6**. You might use analyzers as part of monitoring switch traffic for such purposes as enforcing policies concerning network usage and file sharing and for identifying sources of problems on your network by locating abnormal or heavy bandwidth usage by particular stations or applications.

Mirrored packets can be copied to either a local interface for local monitoring or a VLAN 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**—You can mirror the packets entering or exiting a VLAN to either a local analyzer port or to an analyzer VLAN. You can configure multiple VLANs (up to 256 VLANs), including a VLAN range and private VLANs (PVLANs), as ingress input to an analyzer.
- **Policy-based sample packets**—You can mirror a policy-based sample of packets that are entering a port or a VLAN. You configure a firewall filter to establish a policy to select the packets to be mirrored. You can send the sample to a port-mirroring instance or to an analyzer VLAN.

This topic describes:

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, or VLAN. You can configure an analyzer at the **[edit forwarding-options analyzer]** hierarchy level.

Statistical Analyzer Overview

On an EX9200 switch, 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 constitute 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 Flexible Port Concentrator (FPC).

Default Analyzer Overview

On an EX9200 switch, 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.

Mirroring at a Group of Ports Bound to Multiple Statistical Analyzers

On an EX9200 switch, you can apply up to two statistical analyzers to the same port groups on the switch. 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 switch. Default-analyzer properties are overridden on binding a second instance on the same port group.

Analyzer Terminology for EX9200 Switches

Table 3 on page 4 lists some analyzer terms and their descriptions with regard to EX9200 switches.

Table 3: Analyzer Terminology

Term	Description
Analyzer	In a mirroring configuration on an EX9200 switch, the analyzer includes: • The name of the analyzer • Source (input) ports or VLAN • A destination for mirrored packets (either a monitor port or a monitor VLAN)

Table 3: Analyzer Terminology *(continued)*

Term	Description
Analyzer output interface (Also known as monitor port)	Interface to which mirrored traffic is sent and to which a protocol analyzer application is connected. NOTE: Interfaces used as output for an analyzer must be configured under the **ethernet-switching** hierarchy level. Analyzer output interfaces have the following limitations: • Cannot also be a source port. • Do not participate in Layer 2 protocols, such as 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 (Also known as monitor VLAN)	VLAN to which mirrored traffic is sent. The mirrored traffic can be used by a protocol analyzer application. The member interfaces in the monitor VLAN are spread across the switches in your network.
Default analyzer	An analyzer with default mirroring parameters. In this configuration, 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 switch 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 whose configuration uses the next-hop group as the analyzer output.
Port-based analyzer	An analyzer session whose configuration defines interfaces for both input and output.
Protocol analyzer application	An application used to examine packets transmitted across a network segment. Also commonly called 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 that you create specifically for the purpose of receiving mirrored traffic. Mirrored packets will have an additional outer VLAN tag of the analyzer VLAN.
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 Analyzers on EX9200 Switches

When you configure analyzers on EX9200 switches, we recommend that you follow certain guidelines to ensure that you obtain optimum benefit from mirroring. Additionally, we recommend that you disable mirroring when you are not using it and that you select specific interfaces for which packets must be mirrored (that is, select specific interfaces as input to the analyzer) in preference to using the **all** keyword option, which enables mirroring on all interfaces. You can also limit the amount of mirrored traffic by using statistical sampling, setting a ratio to select a statistical sample, or using a firewall filter. Mirroring only the necessary packets reduces any potential performance impact.

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. Thus, while configuring an analyzer, you must consider whether the traffic being mirrored exceeds the capacity of the analyzer output interface.

Table 4 on page 6 summarizes further configuration guidelines for analyzers on EX9200 switches.

Table 4: Configuration Guidelines for Analyzers on EX9200 Switches

Guideline	Value or Support Information	Comment
Number of analyzers that you can enable concurrently.	64–Default analyzers 2 per FPC–Statistical analyzer	• Statistical analyzers must be bound to an FPC for mirroring traffic on ports belonging to that FPC. NOTE: Default analyzer properties are implicitly bound on the last (or second) 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.
Number of VLANs and interfaces that you can use as ingress input to an analyzer.	256	
Types of ports on which you cannot mirror traffic.	• 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 a analyzer.	**ethernet-switching**	Analyzer mirrors only bridged traffic. For mirroring routed traffic, use the port-mirroring configuration with **family** as **inet** or **inet6**.

Table 4: Configuration Guidelines for Analyzers on EX9200 Switches *(continued)*

Guideline	Value or Support Information	Comment
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	• The trunk interface has to be a member of all VLANs that are related to the input configuration of analyzer. • You must use the **mirror-once** option if the input has been configured as VLAN and the output is a trunk interface. 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.
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.
Egress mirroring of aggregated Ethernet (ae) interfaces and its child logical interfaces configured for different analyzers.	Not supported	

Related Documentation

- Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX9200 Switches on page 11
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX9200 Switches on page 14
- Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure) on page 37

PART 2

Configuration

CHAPTER 2

Configuration Examples

Example: Configuring Mirroring for Local 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

You can analyze the mirrored traffic using a protocol analyzer application installed on a system connected to the local destination interface (or a running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN).

This topic describes how to configure local mirroring on an EX9200 switch. The examples in this topic describe how to configure an EX9200 switch to mirror traffic entering interfaces connected to employee computers to an analyzer output interface on the same switch.

Requirements

The examples use the following hardware and software components:

- One EX9200 switch
- Junos OS Release 13.2.0 or later for EX Series switches

Before you configure mirroring, be sure you have an understanding of mirroring concepts. For information about analyzers, see "Understanding Analyzers on EX9200 Switches" on page 3. For information about port mirroring, see *Layer 2 Port Mirroring Overview*.

Overview and Topology

This topic includes two examples that describe how to mirror traffic entering ports on the switch to a destination interface on the same switch (local mirroring). The first example shows how to mirror all traffic entering the ports connected to employee computers. The second example assumes the same scenario, but includes a filter to mirror only the employee traffic going to the Web.

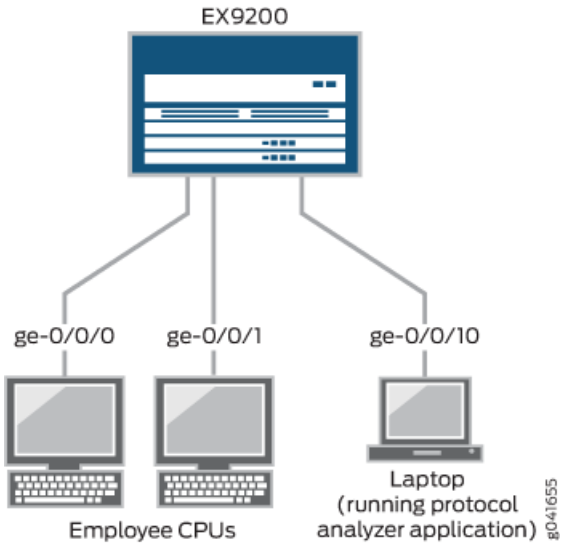
The interfaces ge-0/0/0 and ge-0/0/1 serve as connections for employee computers.

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.

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

Figure 1 on page 12 shows the network topology for this example.

Figure 1: Network Topology for Local Mirroring Example



Mirroring All Employee Traffic for Local Analysis

To configure mirroring for all employee traffic for local analysis, perform these tasks:

CLI Quick Configuration

To quickly configure local mirroring for ingress traffic to the two ports connected to employee computers, copy the following commands and paste them into the switch terminal window:

```
[edit]
set interfaces ge-0/0/0 unit 0 family ethernet-switching
set interfaces ge-0/0/10 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 output interface ge-0/0/10.0
```

Step-by-Step Procedure

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

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

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

2. Configure the output analyzer interface for the **employee-monitor** analyzer. This will be the destination interface for the mirrored packets:

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

Results

Check the results of the configuration:

```
[edit]
user@switch> show
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
            interface ge-0/0/0.0;
        }
        output {
            interface {
                ge-0/0/10.0;
            }
        }
    }
}
```

Verification

To confirm that the configuration is correct, perform these tasks:

- Verifying That the Analyzer Has Been Correctly Created on page 13

Verifying That the Analyzer Has Been Correctly Created

Purpose

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

Action To verify, by using the **show forwarding-options analyzer** command, whether an analyzer is configured as expected.

```
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
  Output interface                   : ge-0/0/10.0
```

Meaning The output shows that the **employee-monitor** analyzer has a ratio of 1 (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 Mirroring for Remote Monitoring of Employee Resource Use on EX9200 Switches on page 14
- Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure) on page 37
- Understanding Analyzers on EX9200 Switches on page 3

Example: Configuring Mirroring 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

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 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 mirroring:

Requirements

The examples use the following hardware and software components:

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

Before you configure remote mirroring, be sure that:

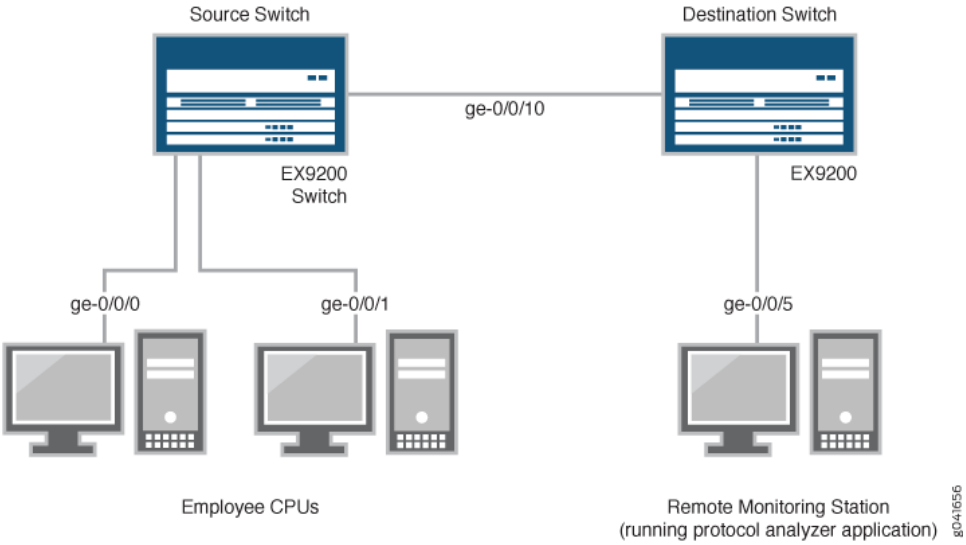
- You have an understanding of mirroring concepts. For information about analyzers, see "Understanding Analyzers on EX9200 Switches" on page 3. For information about port mirroring, see *Layer 2 Port Mirroring Overview*.
- The interfaces that the analyzer will use as input interfaces have been configured on the switch.

Overview and Topology

This topic includes two related examples that describe how to configure mirroring to a remote analyzer VLAN so that analysis can be performed from a remote monitoring station. The first example shows how to configure a switch to mirror all traffic from employee computers. The second example assumes the same scenario, but the setup includes a filter to mirror only the employee traffic going to the Web.

Figure 2 on page 16 shows the network topology for both these example scenarios.

Figure 2: Network Topology for Remote Mirroring



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 the source switch to the destination switch.
- Interface ge-0/0/5 is a Layer 2 interface that connects the destination switch to the remote monitoring station.
- The analyzer VLAN, **remote-analyzer**, is configured on all switches in the topology to carry the mirrored traffic.

Mirroring Employee Traffic for Remote Analysis by Using a Statistical Analyzer

To configure a statistical analyzer for remote traffic analysis for all incoming and outgoing employee traffic, perform these tasks:

CLI Quick Configuration

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

- Copy and paste the following commands in the source 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
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 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 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 switch:

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

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

   - Configure the interface on the network port connected to the destination 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 statistical analyzer **employee-monitor**:

     ```
     [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 instance 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
     user@switch# set forwarding-options analyzer employee-monitor input rate 2
     user@switch# set forwarding-options analyzer employee-monitor input
     maximum-packet-length 128
     ```

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

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

2. 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 interface on the destination 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 interface connected to the destination switch for access mode:

     ```
     [edit interfaces]
     user@switch# set ge-0/0/5 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-0/0/5.0
```

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

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

- Bind the employee-monitor to the FPC containing the input ports:

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

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

```
[edit]
user@switch> show
forwarding-options {
  analyzer employee-monitor {
    input {
      maximum-packet-length 128;
      rate 2;
      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;
      }
    }
  }
}
interfaces {
  ge-0/0/10 {
    unit 0 {
      family ethernet-switching {
        interface-mode access;
        vlan {
          members 999;
        }
      }
    }
  }
}
vlans {
  remote-analyzer {
    vlan-id 999;
    interface {
```

```
        ge-0/0/10.0
        }
      }
    }
}
```

Check the results of the configuration on the destination switch:

```
[edit]
user@switch# 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;
        }
      }
    }
  }
}
vlans {
  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;
      }
    }
  }
}
```

Verification

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

- Verifying That the Analyzer Has Been Correctly Created on page 20

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 configuration example:

```
user@switch> 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 (mirroring every packet, the default), 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 Mirroring for Local Monitoring of Employee Resource Use on EX9200 Switches on page 11
- Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches on page 21
- Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure) on page 37
- Understanding Analyzers on EX9200 Switches on page 3

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

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 Analyzers on EX9200 Switches" on page 3. 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.

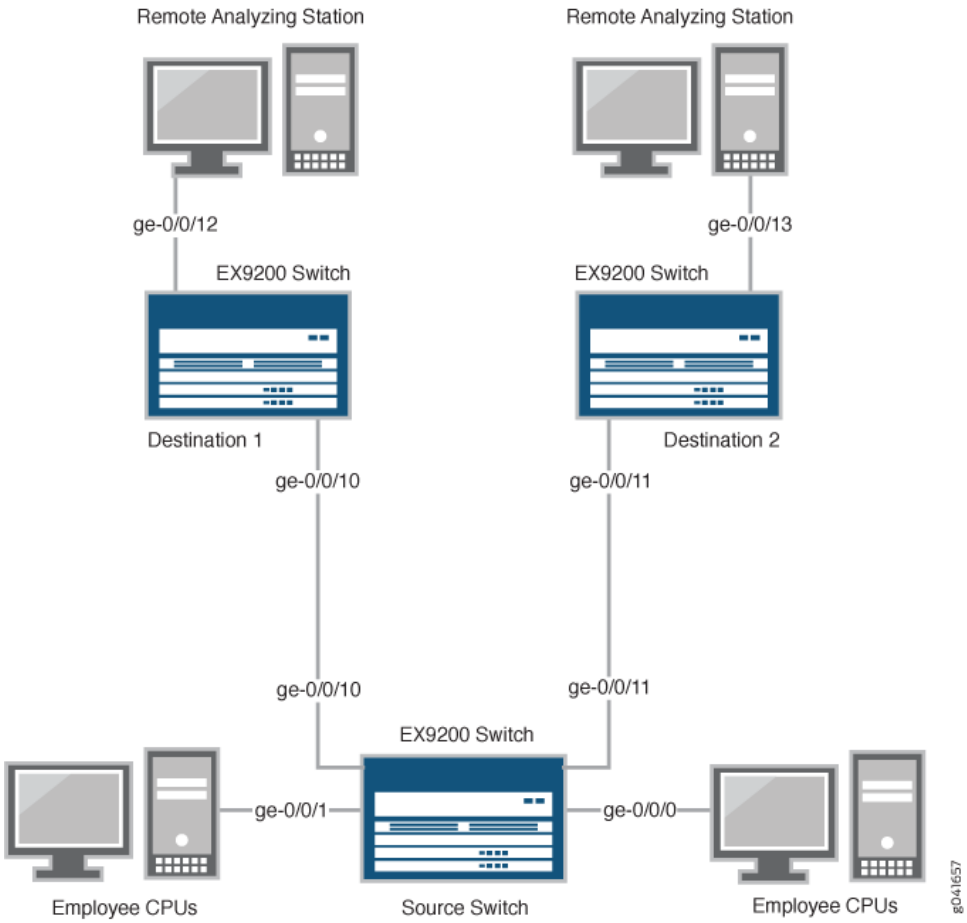
Overview and Topology

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 23 shows the network topology for this example.

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



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 acess
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;
      }
    }
  }
}
vlans {
  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
vlans {
  remote-analyzer {
    vlan-id 999;
```



```
    }
  }
  interfaces {
    ge-0/0/10 {
      unit 0 {
        ethernet-switching {
          interface-mode acess;
        }
      }
    }
    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
  vlans {
    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 28

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 Mirroring for Local Monitoring of Employee Resource Use on EX9200 Switches on page 11
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX9200 Switches on page 14
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX9200 Switches on page 30
- Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure) on page 37
- Understanding Analyzers on EX9200 Switches on page 3

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

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 Analyzers on EX9200 Switches" on page 3. 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.

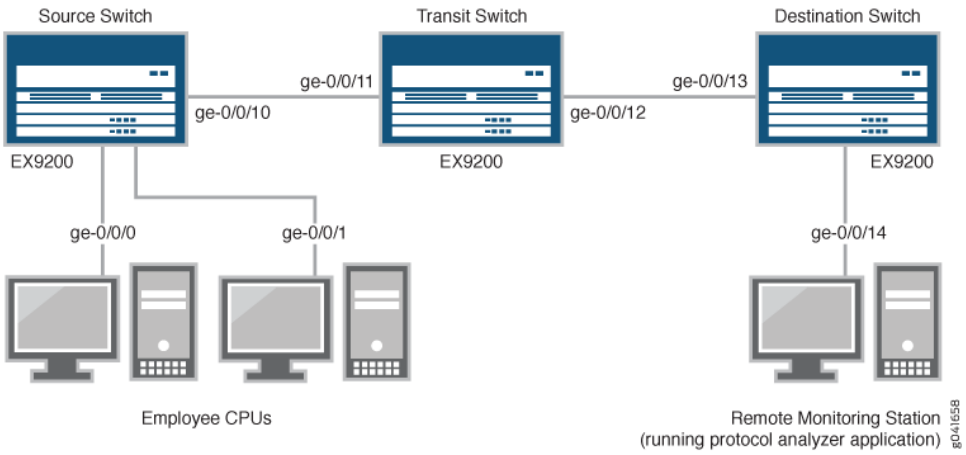
Overview and Topology

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 31 shows the network topology for this example.

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



In this example:

a. 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.

b. Interface ge-0/0/10 is a Layer 2 interface that connects to the transit switch.

c. Interface ge-0/0/11 is a Layer 2 interface on the transit switch.

d. Interface ge-0/0/12 is a Layer 2 interface on the transit switch and connects to the destination switch.

e. 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 switch terminal 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;
          }
        }
      }
    }
    vlans {
      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
vlans {
  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 36

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 Mirroring for Remote Monitoring of Employee Resource Use on EX9200 Switches on page 14
- Example: Configuring Mirroring to Multiple Interfaces for Remote Monitoring of Employee Resource Use on EX9200 Switches on page 21
- Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX9200 Switches on page 11
- Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure) on page 37
- Understanding Analyzers on EX9200 Switches on page 3

CHAPTER 3

Configuration Tasks

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

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 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 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 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 Mirroring for Local Monitoring of Employee Resource Use on EX9200 Switches on page 11
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX9200 Switches on page 14
- Understanding Analyzers on EX9200 Switches on page 3

CHAPTER 4

Configuration Statements: Port Mirroring

[edit forwarding-options analyzer] Configuration Statement Hierarchy for EX Series Switches

```
forwarding-options {
  analyzer analyzer-name {
    input {
      egress {
        interface (all | interface-name);
      }
      ingress {
        interface (all | interface-name);
        routing-instance routing-instance-name {
          vlan (vlan-name | vlan-id | vlan-list);
        }
        vlan (vlan-name | vlan-id | vlan-list);
      }
    }
    output {
      interface interface-name;
      routing-instance routing-instance-name {
        vlan (vlan-name |vlan-id);
          no-tag;
      }
      vlan (vlan-name | vlan-id) {
```

```
            no-tag;
        }
    }
}
}
```

Related Documentation
- *Notational Conventions Used in Junos OS Configuration Hierarchies*
- *[edit forwarding-options] Configuration Statement Hierarchy on EX Series Switches*

egress

Syntax egress;

Hierarchy Level [edit vlans *vlan-name* vlan-id *number* interface *interface-name*]

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
- *Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches*

egress (Analyzer)

Syntax
```
egress {
    interface (all | interface-name);
}
```

Hierarchy Level [edit forwarding-options [edit forwarding-options analyzer] Configuration Statement Hierarchy on page 45 *name* input]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10 (ELS).

Description Specify ports for which traffic exiting the interface is mirrored in a mirroring configuration.

The remaining statements are explained separately.

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

Related Documentation
- *Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches*

ingress (vlans)

Syntax ingress;

Hierarchy Level [edit vlans *vlan-name* vlan-id *number* interface *interface-name*]

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
- *Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches*

ingress (Analyzer)

Syntax
```
ingress {
  interface (all | interface-name);
  routing-instance routing-instance-name {
    vlan (vlan-name | vlan-id | vlan-list);
  }
  vlan (vlan-id | vlan-name);
}
```

Hierarchy Level [edit forwarding-options [edit forwarding-options analyzer] Configuration Statement Hierarchy on page 45 *name* input]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10 (ELS).

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

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-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 EX4300 Switches*

input (Analyzer)

Syntax

```
input {
  ingress {
    interface (all | interface-name);
    routing-instance routing-instance-name {
      vlan (vlan-name | vlan-id | vlan-list);
    }
    vlan (vlan-id | vlan-name);
  }
  egress {
    interface (all | interface-name);
  }
}
```

Hierarchy Level

[edit forwarding-options [edit forwarding-options analyzer] Configuration Statement Hierarchy on page 45 *name*]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10 (ELS).

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 a VLAN

The remaining statements are explained separately.

Default

No default.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches*
- *Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches*
- *Understanding Port Mirroring and Analyzers on EX4300 Switches*

interface

Syntax interface (all | *interface-name*);

Hierarchy Level [edit forwarding-options [edit forwarding-options analyzer] Configuration Statement Hierarchy on page 45 *name* input egress],
[edit forwarding-options [edit forwarding-options analyzer] Configuration Statement Hierarchy on page 45 *name* input ingress],
[edit forwarding-options [edit forwarding-options analyzer] Configuration Statement Hierarchy on page 45 *name* output]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10 (ELS).

Description Configure the interfaces for which traffic is mirrored.

Options all—Apply mirroring to all interfaces on the switch. Mirroring a high volume of traffic can be performance intensive for the switch. 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.

interface-name—Apply mirroring to the specified interface only.

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

Related Documentation

- *Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches*
- *Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches*
- *Understanding Port Mirroring and Analyzers on EX4300 Switches*

no-tag

Syntax no-tag;

Hierarchy Level [edit forwarding-options [edit forwarding-options analyzer] Configuration Statement Hierarchy on page 45 *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

- *Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches*
- *Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches*

output (Mirroring)

Syntax

```
output {
  interface interface-name;
  vlan (vlan-id | vlan-name) {
    no-tag;
  }
}
```

Hierarchy Level

[edit forwarding-options [edit forwarding-options analyzer] Configuration Statement Hierarchy on page 45 *name*]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10 (ELS).

Description

Configure the destination for mirrored traffic, either an interface on the switch, for local monitoring, or a VLAN, for remote monitoring. You can optionally configure the **no-tag** statement so that remote port mirroring packets are not tagged.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches*
- *Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches*

vlan (Mirroring)

Syntax

```
vlan (vlan-id | vlan-name) {
  no-tag;
}
```

Hierarchy Level

[edit forwarding-options [edit forwarding-options analyzer] Configuration Statement Hierarchy on page 45 *name* output]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2X50-D10 (ELS).

Description

Configure mirrored traffic to be sent to a VLAN for remote monitoring. On a destination (**output**) VLAN, you can also configure the **no-tag** statement.

Options

vlan-id—Numeric VLAN identifier.

vlan-name—Name of the VLAN.

The remaining statement is explained separately.

Required Privilege Level

system—To view this statement in the configuration.
routing-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 EX4300 Switches*
- *Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches*

PART 3

Administration

CHAPTER 5

Operational Commands: Port Mirroring

- show forwarding-options analyzer

show forwarding-options analyzer

Syntax **show forwarding-options analyzer *analyzer-name***

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level **[edit forwarding-options]** introduced in Junos OS Release 13.2.

Description Display information about analyzers configured for mirroring.

Options ***analyzer-name***—(Optional) Displays the status of a specific analyzer on the switch.

Required Privilege Level view

Related Documentation
- Understanding Analyzers on EX9200 Switches on page 3

List of Sample Output show forwarding-options analyzer on page 56

Output Fields Table 5 on page 56 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@host> 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
```