System Services Feature Guide

Modified: 2018-07-09

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

System Services Feature Guide

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 https://www.juniper.net/support/eula/. 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 https://www.juniper.net/documentation/.

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 https://www.juniper.net/books.

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 CLI Explorer.

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 of the Juniper Networks TechLibrary site at https://www.juniper.net/documentation/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/documentation/feedback/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://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: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/

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

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

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 https://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 https://www.juniper.net/support/requesting-support.html.

PART 1

Port Mirroring

CHAPTER 1

Configuring Port Mirroring

Understanding Port Mirroring

Port Mirroring Overview

Port mirroring copies packets entering or exiting a port or entering a VLAN and sends the copies to a local interface for local monitoring or to a VLAN for remote monitoring. Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on.

Port mirroring is needed for traffic analysis on a switch because a switch normally sends packets only to the port to which the destination device is connected. You configure port mirroring on the switch to send copies of unicast traffic to a local interface or a VLAN and run an analyzer application on a device connected to the interface or VLAN. You configure port mirroring by using the **analyzer** statement.

Keep performance in mind when configuring port mirroring. For example, If you mirror traffic from multiple ports, the mirrored traffic may exceed the capacity of the output interface. We recommend that you limit the amount of copied traffic by selecting specific interfaces instead of using the **all** keyword. You can also limit the amount of mirrored traffic by using a firewall filter to send specific traffic to a port mirroring instance. Mirroring only the necessary packets reduces the possibility of a performance impact.

You can use port mirroring to copy any of the following:

- All packets entering or exiting an interface (in any combination)—For example, you can send copies of the packets entering some interfaces and the packets exiting other interfaces to the same local interface or VLAN. If you configure port mirroring to copy packets exiting an interface, traffic that originates on that switch or Node device (in a QFabric system) is not copied when it egresses. Only switched traffic is copied on egress. (See the limitation on egress mirroring below.)
- All packets entering a VLAN—You cannot use port mirroring to copy packets exiting a VLAN.
- Firewall-filtered sample—Sample of packets entering a port or VLAN. Configure a firewall filter to select certain packets for mirroring.

NOTE: **Firewall filters are not supported on egress ports; therefore, you cannot specify policy-based sampling of packets exiting an interface.**

Port Mirroring Instance Types

To configure port mirroring, you configure an instance of one of the following types:

- Analyzer instance: You must specify the input and output for the instance. This instance type is useful for ensuring that all traffic transiting an interface or VLAN is mirrored and sent to the analyzer device.
- Port-mirroring instance: You do not specify an input for this instance type. Instead, you, create a firewall filter that specifies the required traffic and directs it to the mirror. This instance type is useful for controlling which types of traffic should be mirrored. When you use a port-mirroring instance, you can direct traffic to it in the following ways:
  - Specify the name of the port-mirroring instance in the firewall filter using the **port-mirror-instance *instance-name*** action. You should use this approach if there are multiple port-mirroring instances defined.
  - Configure the filter to send the mirrored packets to the output interface defined in the instance using the **port-mirror** action. You can use this approach if there is only one port-mirroring instance defined.

Port-Mirroring Terminology

Table 3 on page 4 lists the terms used in the documentation about port mirroring and provides definitions.

Table 3: Port Mirroring Terms and Definitions

Term	Description
Analyzer instance	Port-mirroring configuration that includes a name, source interfaces or source VLAN, and a destination for mirrored packets (either a local access interface or a VLAN).

Table 3: Port Mirroring Terms and Definitions (continued)

Port mirroring instance NOTE: Port mirroring instance feature is not supported on NFX150 devices.	A port-mirroring configuration that does not specify an input.. A firewall filter must be used to send traffic to the port mirror. Use the action **port-mirror-instance** ***instance-name*** in the firewall filter configuration to send packets to the port mirror.
Output interface (also known as monitor interface)	Access interface to which packet copies are sent and to which a device running an analyzer application is connected. The following limitations apply to an output interface: • Cannot also be a source port. • Cannot be used for switching. • Cannot be an aggregated Ethernet interface (LAG). • Does not participate in Layer 2 protocols, such as Spanning Tree Protocol (STP). • Loses any existing VLAN associations when you configure it as an analyzer output interface. If the capacity of the output interface is insufficient to handle the traffic from the source ports, overflow packets are dropped.
Output IP address	IP address of the device running an analyzer application. The device can be on a remote network. When you use this feature, the mirrored packets are GRE-encapsulated. The analyzer device must be able to de-encapsulate GRE-encapsulated packets, or the GRE-encapsulated packets must be de-encapsulated before reaching the analyzer device. (You can use a network sniffer to de-encapsulate the packets.) • An output IP address cannot be in the same subnetwork as any of the switch's management interfaces. • If you create virtual routing instances and also create an analyzer configuration that includes an output IP address, the output address belongs to the default virtual routing instance (inet.0 routing table).
Output VLAN (also known as monitor or analyzer VLAN)	VLAN to which copies are sent and to which a device running an analyzer application is connected. The analyzer VLAN can span multiple switches. The following limitations apply to an output VLAN: • Cannot be a private VLAN or VLAN range. • Cannot be shared by multiple **analyzer** statements. • An output VLAN interface cannot be a member of any other VLAN. • An output VLAN interface cannot be an aggregated Ethernet interface (LAG). • On some switches, only one interface can be a member of the analyzer VLAN. This limitation does not apply on the QFX10000 switch if traffic is mirrored on ingress. In this case, multiple QFX10000 interfaces can belong to the output VLAN, and traffic is mirrored to all of those interfaces. If traffic is mirrored on egress on a QFX10000 switch, only one interface can be a member of the analyzer VLAN.
Input interface (also known as mirrored or monitored interface)	Interface that provides traffic to be mirrored. This traffic can be entering or exiting the interface. (Ingress or egress traffic can be mirrored.) An input interface cannot also be an output interface for an analyzer.
Monitoring station	Computer running an analyzer application.

Table 3: Port Mirroring Terms and Definitions (continued)

Local port mirroring	Port-mirroring configuration in which the mirrored packets are sent to an interface on the same switch.
Remote port mirroring	Flooding mirrored packets to an output (analyzer) VLAN that you create to receive mirror traffic or sending the mirrored packets to a remote IP address. (You cannot send mirrored packets to a remote IP address on a QFabric system.)
Policy-based mirroring	Mirroring of packets that match the match a firewall filter term. The action **analyzer *analyzer-name*** is used in the firewall filter to send the packets to the analyzer.

Port Mirroring and STP

The behavior of STP in a port-mirroring configuration depends on the version of Junos OS you are using:

- Junos OS 13.2X50, Junos OS 13.2X51-D25 or earlier, Junos OS 13.2X52: If you enable STP, port mirroring might not work because STP might block the mirrored packets.
- Junos OS 13.2X51-D30, Junos OS 14.1X53: STP is disabled for mirrored traffic. You must ensure that your topology prevents loops for this traffic.

Port Mirroring Constraints and Limitations

Local and Remote Port Mirroring

The following constraints and limitations apply to local and remote port mirroring:

- You can create a total of four port-mirroring configurations.
- You can create a total of four port-mirroring configurations on each Node group in a QFabric system, subject to the following constraints:
  - As many as four of the configurations can be for local port mirroring.
  - As many as three of the configurations can be for remote port mirroring.
- Regardless of whether you are configuring a standalone switch or a Node group, the following limits apply:
  - There can be no more than two configurations that mirror ingress traffic. (If you configure a firewall filter to send traffic to a port mirror—that is, you use the **analyzer** action modifier in a filter term—this counts as an ingress mirroring configuration for switch or Node group on which the filter is applied.)
  - There can be no more than two configurations that mirror egress traffic.

NOTE: On QFabric systems, there is no system-wide limit on the total number of mirror sessions.

- You can configure no more than one type of output in one port-mirroring configuration. That is, you can use no more than one of the following to complete a **set analyzer *name* output** statement:
  - **interface**
  - **ip-address**
  - **vlan**
- If you configure Junos OS to mirror egress packets, do not configure more than 2000 VLANs on a standalone switch or QFabric system. If you do so, some VLAN packets might contain incorrect VLAN IDs. This applies to any VLAN packets—not only the mirrored copies.
- The **ratio** and **loss-priority** options are not supported.
- Packets with physical layer errors are filtered out and are not sent to the output port or VLAN.
- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit from the output interface.
- You cannot mirror packets exiting or entering the following ports:
  - Dedicated Virtual Chassis interfaces
  - Management interfaces (me0 or vme0)
  - Fibre Channel interfaces
  - Routed VLAN interfaces
- An aggregated Ethernet interface cannot be an output interface if the input is a VLAN or if traffic is sent to the analyzer by a firewall filter.
- When packet copies are sent out the output interface, they are not modified for any changes that are normally applied on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.
- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.
- VLAN-based mirroring is not supported for STP traffic.
- (QFabric systems only) If you configure a QFabric analyzer to mirror egress traffic and the input and output interfaces are on different Node devices, the mirrored copies have incorrect VLAN IDs. This limitation does not apply if you configure a QFabric analyzer to mirror egress traffic and the input and output interfaces are on the *same* Node device. In this case the mirrored copies have the correct VLAN IDs (as long as you do not configure more than 2000 VLANs on the QFabric system).

Remote Port Mirroring Only

The following constraints and limitations apply to remote port mirroring:

- If you configure an output IP address, the address cannot be in the same subnetwork as any of the switch's management interfaces.
- If you create virtual routing instances and also create an analyzer configuration that includes an output IP address, the output address belongs to the default virtual routing instance (inet.0 routing table).
- An output VLAN cannot be a private VLAN or VLAN range.
- An output VLAN cannot be shared by multiple **analyzer** statements.
- An output VLAN interface cannot be a member of any other VLAN.
- An output VLAN interface cannot be an aggregated Ethernet interface.

Port Mirroring Constraints on OCX Series Switches

The following constraints and limitations apply to port mirroring on OCX Series switches:

- You can create a total of four port-mirroring configurations. The following constraints also apply:
  - There can be no more than two configurations that mirror ingress traffic.
  - There can be no more than two configurations that mirror egress traffic.
- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit from the output interface.
- You can create only one port-mirroring session.
- You cannot mirror packets exiting or entering the following ports:
  - Dedicated Virtual Chassis interfaces
  - Management interfaces (me0 or vme0)
  - Fibre Channel interfaces
  - Routed VLAN interfaces or IRB interfaces
- An aggregated Ethernet interface cannot be an output interface.
- Do not include an 802.1Q subinterface that has a unit number other than 0 in a port mirroring configuration. Port mirroring does not work with subinterfaces if their unit number is not 0. (You configure 802.1Q subinterfaces using the **vlan-tagging** statement.)
- When packet copies are sent out the output interface, they are not modified for any changes that are normally applied on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.

- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.
- VLAN-based mirroring is not supported for STP traffic.

See Also

- *Understanding Port Mirroring*
- *Example: Mirroring Employee Web Traffic with a Firewall Filter*
- *Configuring Port Mirroring*

Related Documentation

- Configuring Port Mirroring on page 9
- Examples: Configuring Port Mirroring for Local Analysis on page 12
- Examples: Configuring Port Mirroring for Local Analysis on page 12
- Example: Configuring Port Mirroring for Remote Analysis on page 18
- Troubleshooting Port Mirroring on page 26

Configuring Port Mirroring

You use port mirroring to copy packets and send the copies to a device running an application such as a network analyzer or intrusion detection application so that you can analyze traffic without delaying it. You can mirror traffic entering or exiting a port or entering a VLAN, and you can send the copies to a local access interface or to a VLAN through a trunk interface.

We recommend that you disable port mirroring when you are not using it. To avoid creating a performance issue If you do enable port mirroring, we recommend that you select specific input interfaces instead of using the **all** keyword. You can also limit the amount of mirrored traffic by using a firewall filter.

NOTE: This task uses the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Configuring Port Mirroring*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

NOTE: If you want to create additional analyzers without deleting an existing analyzer, first disable the existing analyzer using the **disable analyzer *analyzer-name*** command.

NOTE: You must configure port mirroring output interfaces as family ethernet-switching.

- Configuring Port Mirroring for Local Analysis on page 10
- Configuring Port Mirroring for Remote Analysis on page 11
- Filtering the Traffic Entering an Analyzer on page 11

Configuring Port Mirroring for Local Analysis

To mirror interface traffic to a local interface on the switch:

1. If you want to mirror traffic that is ingressing or egressing specific interfaces, choose a name for the port-mirroring configuration and configure what traffic should be mirrored by specifying the interfaces and direction of traffic:

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

   NOTE: If you configure Junos OS to mirror egress packets, do not configure more than 2000 VLANs. If you do so, some VLAN packets might contain incorrect VLAN IDs.

   NOTE: If you configure mirroring for packets that egress an access interface, the original packets lose any VLAN tags when they exit the access interface, but the mirrored (copied) packets retain the VLAN tags when they are sent to the analyzer system.

2. If you want to specify that all traffic entering a VLAN should be mirrored, choose a name for the port-mirroring configuration and specify the VLAN:

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

   NOTE: You cannot configure port mirroring to copy traffic that egresses a VLAN.

3. Configure the destination interface for the mirrored packets:

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

Configuring Port Mirroring for Remote Analysis

To mirror traffic to a VLAN for analysis at a remote location:

1. Configure a VLAN to carry the mirrored traffic:

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

2. Configure the interface that connects to another switch (the uplink interface) to trunk mode and associate it with the appropriate VLAN:

   ```
   [edit]
   user@switch# set interfaces interface-name unit 0 family ethernet-switching port-mode
   trunk vlan members (vlan-name | vlan-id)
   ```

3. Configure the analyzer:

   a. Choose a name for the analyzer:

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

   b. Specify the interface to be mirrored and whether the traffic should be mirrored on ingress or egress:

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

   c. Specify the appropriate IP address or VLAN as the output (a VLAN is specified in this example:

      ```
      [edit forwarding-options]
      user@switch# set analyzer analyzer-name output vlan (vlan-name | vlan-id)
      ```

      If you specify an IP address as the output, note the following constraints:

      - The address cannot be in the same subnetwork as any of the switch's management interfaces.
      - If you create virtual routing instances and also create an analyzer configuration that includes an output IP address, the output address belongs to the default virtual routing instance (**inet.0** routing table).
      - The analyzer device must be able to de-encapsulate GRE-encapsulated packets, or the GRE-encapsulated packets must be de-encapsulated before reaching the analyzer device. (You can use a network sniffer to de-encapsulate the packets.)

Filtering the Traffic Entering an Analyzer

NOTE: This functionality is not supported on NFX150 devices.

In addition to specifying which traffic to mirror by configuring an analyzer, you can also use a firewall filter to exercise more control over which packets are copied. For example, you might use a filter to specify that only traffic from certain applications be mirrored. The filter can use any of the available match conditions and must have an action of modifier of **port-mirror-instance *instance-name*.** If you use the same analyzer in multiple filters or terms, the output packets are copied only once.

When you use a firewall filter as the input to a port-mirroring instance, you send the copied traffic to a local interface or a VLAN just as you do when a firewall is not involved.

To configure port mirroring with filters:

1. Configure a port-mirroring instance for local or remote analysis. Configure only the output. For example, for local analysis enter:

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

   NOTE: You cannot configure input to this instance.

2. Create a firewall filter using any of the available match conditions. In a **then** term, specify include the action modifier **port-mirror-instance *instance-name***.

3. Apply the firewall filter to the interfaces or VLAN that should provide the input to the analyzer:

   ```
   [edit]
   user@switch# set interfaces interface-name unit 0 family ethernet-switching filter input
   filter-name
   [edit]
   user@switch# set vlan (vlan-name | vlan-id) filter input filter-name
   ```

Related Documentation

- Understanding Port Mirroring on page 3
- Examples: Configuring Port Mirroring for Local Analysis on page 12
- Example: Configuring Port Mirroring for Remote Analysis on page 18
- *Overview of Firewall Filters*

Examples: Configuring Port Mirroring for Local Analysis

Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on. Port mirroring copies packets entering or exiting an interface or entering a VLAN and sends the copies to a local interface for local monitoring.

NOTE: This example uses the Enhanced Layer 2 Software (ELS) configuration style. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

This example describes how to configure port mirroring to copy traffic sent by employee computers to a switch to an access interface on the same switch.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 13.2
- A switch

Overview and Topology

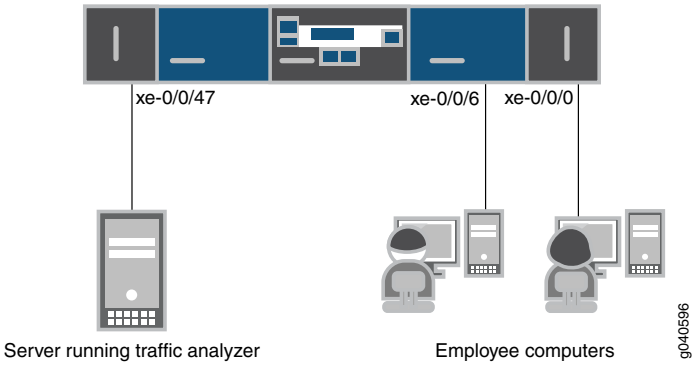
This topic includes two related examples that describe how to mirror traffic entering interfaces on the switch to an access interface on the same switch. The first example shows how to mirror all traffic sent by employee computers to the switch. The second example includes a filter to mirror only the employee traffic going to the Web.

In this example, **xe-0/0/0** and **xe-0/0/6** serve as connections for employee computers. Interface **xe-0/0/47** is connected to a device running an analyzer application.

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

Figure 1 on page 13 shows the network topology for this example.

Figure 1: Network Topology for Local Port Mirroring Example



Example: Mirroring All Employee Traffic for Local Analysis

To configure port mirroring for all traffic sent by employee computers for local analysis, perform the tasks explained in this section.

CLI Quick Configuration

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

```
[edit]
set interfaces xe-0/0/0 unit 0 family ethernet-switching
set interfaces xe-0/0/6 unit 0 family ethernet-switching
set interfaces xe-0/0/47 unit 0 family ethernet-switching
set forwarding-options analyzer employee-monitor input ingress interface xe-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface xe-0/0/6.0
set forwarding-options analyzer employee-monitor output interface xe-0/0/47.0
```

Step-by-Step Procedure

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

1. Configure the interfaces connected to employee computers as input interfaces for the port-mirror analyzer **employee-monitor**:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input ingress interface xe–0/0/0.0
   user@switch# set analyzer employee-monitor input ingress interface xe–0/0/6.0
   ```

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 xe-0/0/47.0
   ```

Results

Check the results of the configuration:

```
[edit]
user@switch# show forwarding-options analyzer
  employee-monitor {
    input {
      ingress {
        interface xe-0/0/0.0;
        interface xe-0/0/6.0;
      }
    }
    output {
      interface {
        xe-0/0/47.0;
      }
    }
  }
}
```

Example: Mirroring Employee Web Traffic with a Firewall Filter

Requirements

This example uses the following hardware and software components:

- One switch
- Junos 13.2X51

Overview

Rather than mirror all traffic, it is usually desirable to mirror only certain traffic. This is a more-efficient use of your bandwidth and hardware and might be necessary because constraints on these assets. To select specific traffic for mirroring, you use a firewall filter to match the desired traffic and direct it to a port-mirroring instance. The port-mirroring instance then copies the packets and sends them to the output VLAN, interface, or IP address.

Configuring

To specify that the only traffic that will be mirrored is traffic sent by employees to the Web, perform the tasks explained in this section. To select this traffic for mirroring, you use a firewall filter to specify this traffic and direct it to a port-mirroring instance.

CLI Quick Configuration

To quickly configure local port mirroring of traffic from employee computers that is destined for the Web, copy the following commands and paste them into a switch terminal window:

```
[edit]
set forwarding-options port-mirroring instance employee–web–monitor output interface
xe-0/0/47.0
set firewall family ethernet-switching filter watch-employee term employee-to-corp from
destination-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp from
source-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp then accept
set firewall family ethernet-switching filter watch-employee term employee-to-web from
destination-port 80
set firewall family ethernet-switching filter watch-employee term employee-to-web then
port-mirror-instance employee-web-monitor
set interfaces xe-0/0/0 unit 0 family ethernet-switching filter input watch-employee
set interfaces xe-0/0/6 unit 0 family ethernet-switching filter input watch-employee
```

Step-by-Step Procedure

To configure local port mirroring of employee-to-web traffic from the two ports connected to employee computers:

1. Configure the output interface:

```
[edit interfaces]
user@switch# set xe-0/0/47 unit 0 family ethernet-switching
```

2. Configure the **employee-web-monitor** output interface. (Configure only the output—the input comes from the filter.)

```
[edit forwarding-options]
user@switch# set port-mirroring instance family ethernet-switching
employee–web–monitor output interface xe-0/0/47.0
```

3. Configure a firewall filter called **watch-employee** that includes a term to match traffic sent to the Web and send it to the port-mirroring instance **employee-web-monitor**. Traffic to and from the corporate subnet (destination or source address of **192.0.2.16/28**) does not need to be copied, so create another term to accept that traffic before it reaches the term that sends Web traffic to the instance:

```
[edit firewall family ethernet-switching]
user@switch# set filter watch-employee term employee-to-corp from destination-address
192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp from source-address
192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirror-instance
employee-web-monitor
```

4. Apply the firewall filter to the appropriate interfaces as an ingress filter (egress filters do not allow analyzers):

```
[edit interfaces]
user@switch# set xe-0/0/0 unit 0 family ethernet-switching filter input watch-employee
user@switch# set xe-0/0/6 unit 0 family ethernet-switching filter input watch-employee
```

Results

Check the results of the configuration:

```
[edit]
user@switch# show
forwarding-options {
  port-mirroring {
    instance {
      employee-web-monitor {
        output {
          interface xe-0/0/47.0;
          }
        }
      }
    }
  }
```

```
}
...
firewall family ethernet-switching {
    filter watch-employee {
        term employee-to-web {
            from {
                destination-port 80;
            }
            then port-mirror-instance employee-web-monitor;
        }
    }
}
...
interfaces {
    xe-0/0/0 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
    xe-0/0/6 {
        family ethernet-switching {
            filter {
                input watch-employee;
            }
        }
    }
}
```

Verification

Verifying That the Analyzer Has Been Correctly Created

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

Action You can verify that the port mirror analyzer has been configured as expected using the **show analyzer** command.

```
user@switch> show forwarding-options port-mirroring
  Port mirror name                : employee-monitor
Mirror rate                      : 1
  Maximum packet length             : 0
  State                             : up
  Ingress monitored interfaces : xe-0/0/0.0
  Ingress monitored interfaces : xe-0/0/6.0
   Output interface                  : xe-0/0/47.0
```

Meaning This output shows that the port-mirroring instance **employee-monitor** has a ratio of 1 (mirroring every packet, the default setting), the maximum size of the original packet that was mirrored (**0** indicates the entire packet), the state of the configuration (is up indicates that the instance is mirroring the traffic entering the xe-0/0/0, and xe-0/0/6 interfaces, and sending the mirrored traffic to the xe-0/0/47 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 instance will not be programmed for mirroring.

Related Documentation

- Understanding Port Mirroring on page 3

Related Documentation

- Understanding Port Mirroring on page 3
- Configuring Port Mirroring on page 9
- Example: Configuring Port Mirroring for Remote Analysis on page 18

Example: Configuring Port Mirroring for Remote Analysis

Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on. Port mirroring copies packets entering or exiting an interface or entering a VLAN and sends the copies either to a local interface for local monitoring or to a VLAN for remote monitoring. This example describes how to configure port mirroring for remote analysis.

- Requirements on page 19
- Overview and Topology on page 19
- Mirroring All Employee Traffic for Remote Analysis on page 19
- Mirroring Employee-to-Web Traffic for Remote Analysis on page 20
- Verification on page 23

Requirements

This example uses the following hardware and software components:

- Junos OS Release 13.2 for the QFX Series
- A switch

Overview and Topology

This topic includes two related examples that describe how to mirror traffic entering ports on the switch to an analyzer VLAN so that you can perform analysis using a remote device. The first example shows how to mirror all traffic sent by employee computers to the switch. The second example includes a filter to mirror only the employee traffic going to the Web.

In this example:

- Interfaces **ge-0/0/0** and **ge-0/0/1** are Layer 2 interfaces that connect to employee computers.
- Interface **ge-0/0/2** is a Layer 2 interface that connects to another switch.
- VLAN **remote-analyzer** is configured on all switches in the topology to carry the mirrored traffic.

NOTE: In addition to performing the configuration steps described here, you must also configure the analyzer VLAN (remote-analyzer in this example) on the other switches that are used to connect the source switch (the one in this configuration) to the one that the monitoring station is connected to.

Mirroring All Employee Traffic for Remote Analysis

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **edit** hierarchy level:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching port-mode trunk
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 output vlan remote-analyzer
```

Step-by-Step Procedure

To configure basic remote port mirroring:

1. Configure the analyzer VLAN (called **remote-analyzer** in this example):

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

2. Configure the interface connected to another switch for trunk mode and associate it with the **remote-analyzer** VLAN:

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

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

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

4. Configure the **remote-analyzer** VLAN on the switches that connect this switch to the monitoring workstation.

Results

Check the results of the configuration:

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

Mirroring Employee-to-Web Traffic for Remote Analysis

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **edit** hierarchy level:

```
[edit]
```

```
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999set
forwarding-options port-mirroring instance employee-web-monitor loss-priority high output vlan
999
set firewall family ethernet-switching filter watch-employee term employee-to-web from
destination-port 80
set firewall family ethernet-switching filter watch-employee term employee-to-web then
port-mirror-instance employee-web-monitor employee-web-monitor
set ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

Step-by-Step Procedure

1. Configure the analyzer VLAN (called **remote-analyzer** in this example):

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

2. Configure an interface to associate it with the **remote-analyzer** VLAN:

   ```
   [edit interfaces]
   user@switch# set interfaces 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
   ```

3. Configure the **employee-web-monitor** analyzer. (Configure only the output—the input comes from the filter.)

   ```
   [edit forwarding-options]
   user@switch# set forwarding-options port-mirroring instance employee-web-monitor
   output vlan 999
   ```

4. Configure a firewall filter called **watch-employee** to match traffic sent to the Web and send it to the analyzer **employee-web-monitor**:

   ```
   [edit firewall family ethernet-switching]
   user@switch# set filter watch-employee term employee-to-web from destination-port 80
   user@switch# set filter watch-employee term employee-to-web then port-mirror-instance
   employee-web-monitor
   ```

5. Apply the firewall filter to the appropriate interfaces as an ingress filter:

   ```
   [edit interfaces]
   user@switch# set ge-0/0/0 unit 0 family ethernet-switching filterinput watch-employee
   user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
   ```

6. Configure the **remote-analyzer** VLAN on the switches that connect this switch to the monitoring workstation.

Results Check the results of the configuration:

```
[edit]
user@switch# show
interfaces {
   ...
```

```
    ge-0/0/10 {
      unit 0 {
        family ethernet-switching {
          interface-mode trunk;
          vlan {
            members remote-analyzer;
          }
        }
      }
    }
    ge-0/0/0 {
      unit 0 {
        family ethernet-switching {
          filter {
            input watch-employee;
          }
        }
      }
    }
    ge-0/0/1 {
      unit 0 {
        family ethernet-switching {
          filter {
            input watch-employee;
          }
        }
      }
    }
  }
  ...
  firewall {
    family ethernet-switching {
      ...
      filter watch-employee {
        term employee-to-web {
          from {
            destination-port 80;
          }
          then port-mirror-instance employee-web-monitor;
        }
      }
    }
  }
  forwarding-options analyzer {
    employee-web-monitor {
      output {
        vlan {
          999;
        }
      }
    }
  vlans {
    remote-analyzer {
      vlan-id 999;
    }
  }
```

Verification

Verifying That the Analyzer Has Been Correctly Created

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

Action You can verify the port mirror analyzer is configured as expected using the **show analyzer** command.

```
user@switch> show analyzer
 Analyzer name                 : employee-monitor
 Output VLAN                   : remote-analyzer
 Ingress monitored interfaces : ge-0/0/0.0
 Ingress monitored interfaces : ge-0/0/1.0
```

Meaning This output shows that the **employee-monitor** analyzer is mirroring the traffic entering **ge-0/0/0** and **ge-0/0/1** and is sending the mirror traffic to the analyzer **remote-analyzer**.

Related Documentation

- Understanding Port Mirroring on page 3
- Configuring Port Mirroring on page 9
- Examples: Configuring Port Mirroring for Local Analysis on page 12
- *Overview of Firewall Filters*

Example: Mirroring Employee Web Traffic with a Firewall Filter

Requirements

This example uses the following hardware and software components:

- One switch
- Junos 13.2X51

Overview

Rather than mirror all traffic, it is usually desirable to mirror only certain traffic. This is a more-efficient use of your bandwidth and hardware and might be necessary because constraints on these assets. To select specific traffic for mirroring, you use a firewall filter

to match the desired traffic and direct it to a port-mirroring instance. The port-mirroring instance then copies the packets and sends them to the output VLAN, interface, or IP address.

Configuring

To specify that the only traffic that will be mirrored is traffic sent by employees to the Web, perform the tasks explained in this section. To select this traffic for mirroring, you use a firewall filter to specify this traffic and direct it to a port-mirroring instance.

CLI Quick Configuration

To quickly configure local port mirroring of traffic from employee computers that is destined for the Web, copy the following commands and paste them into a switch terminal window:

```
[edit]
set forwarding-options port-mirroring instance employee–web–monitor output interface
xe-0/0/47.0
set firewall family ethernet-switching filter watch-employee term employee-to-corp from
destination-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp from
source-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp then accept
set firewall family ethernet-switching filter watch-employee term employee-to-web from
destination-port 80
set firewall family ethernet-switching filter watch-employee term employee-to-web then
port-mirror-instance employee-web-monitor
set interfaces xe-0/0/0 unit 0 family ethernet-switching filter input watch-employee
set interfaces xe-0/0/6 unit 0 family ethernet-switching filter input watch-employee
```

Step-by-Step Procedure

To configure local port mirroring of employee-to-web traffic from the two ports connected to employee computers:

1. Configure the output interface:

   ```
   [edit interfaces]
   user@switch# set xe-0/0/47 unit 0 family ethernet-switching
   ```

2. Configure the **employee-web-monitor** output interface. (Configure only the output—the input comes from the filter.)

   ```
   [edit forwarding-options]
   user@switch# set port-mirroring instance family ethernet-switching
   employee–web–monitor output interface xe-0/0/47.0
   ```

3. Configure a firewall filter called **watch-employee** that includes a term to match traffic sent to the Web and send it to the port-mirroring instance **employee-web-monitor**. Traffic to and from the corporate subnet (destination or source address of **192.0.2.16/28**) does not need to be copied, so create another term to accept that traffic before it reaches the term that sends Web traffic to the instance:

   ```
   [edit firewall family ethernet-switching]
   user@switch# set filter watch-employee term employee-to-corp from destination-address
   192.0.2.16/28
   ```

```
user@switch#  set filter watch-employee term employee-to-corp from source-address
192.0.2.16/28
user@switch#  set filter watch-employee term employee-to-corp then accept
user@switch#  set filter watch-employee term employee-to-web from destination-port 80
user@switch#  set filter watch-employee term employee-to-web then port-mirror-instance
employee-web-monitor
```

4. Apply the firewall filter to the appropriate interfaces as an ingress filter (egress filters do not allow analyzers):

```
[edit interfaces]
user@switch#  set xe-0/0/0 unit 0 family ethernet-switching filter input watch-employee
user@switch#  set xe-0/0/6 unit 0 family ethernet-switching filter input watch-employee
```

Results Check the results of the configuration:

```
[edit]
user@switch# show
forwarding-options {
  port-mirroring {
    instance {
      employee-web-monitor {
        output {
          interface xe-0/0/47.0;
          }
        }
      }
    }
  }
}
...
firewall family ethernet-switching {
  filter watch-employee {
    term employee-to-web {
      from {
        destination-port 80;
      }
      then port-mirror-instance employee-web-monitor;
    }
  }
}
...
interfaces {
  xe-0/0/0 {
    unit 0 {
      family ethernet-switching {
        filter {
          input watch-employee;
        }
      }
    }
  }
  xe-0/0/6 {
    family ethernet-switching {
      filter {
```

```
            input watch-employee;
        }
    }
  }
}
```

Verification

Verifying That the Analyzer Has Been Correctly Created

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

Action You can verify that the port mirror analyzer has been configured as expected using the **show analyzer** command.

```
user@switch> show forwarding-options port-mirroring
  Port mirror name                : employee-monitor
Mirror rate                      : 1
  Maximum packet length             : 0
  State                             : up
  Ingress monitored interfaces : xe-0/0/0.0
  Ingress monitored interfaces : xe-0/0/6.0
   Output interface                  : xe-0/0/47.0
```

Meaning This output shows that the port-mirroring instance **employee-monitor** has a ratio of 1 (mirroring every packet, the default setting), the maximum size of the original packet that was mirrored (**0** indicates the entire packet), the state of the configuration (is up indicates that the instance is mirroring the traffic entering the xe-0/0/0, and xe-0/0/6 interfaces, and sending the mirrored traffic to the xe-0/0/47 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 instance will not be programmed for mirroring.

Related Documentation

- Understanding Port Mirroring on page 3

Troubleshooting Port Mirroring

- Port Mirroring Constraints and Limitations on page 27
- Egress Port Mirroring with VLAN Translation on page 29
- Egress Port Mirroring with Private VLANs on page 30

Port Mirroring Constraints and Limitations

Local and Remote Port Mirroring

The following constraints and limitations apply to local and remote port mirroring:

- You can create a total of four port-mirroring configurations.
- You can create a total of four port-mirroring configurations on each Node group in a QFabric system, subject to the following constraints:
  - As many as four of the configurations can be for local port mirroring.
  - As many as three of the configurations can be for remote port mirroring.
- Regardless of whether you are configuring a standalone switch or a Node group, the following limits apply:
  - There can be no more than two configurations that mirror ingress traffic. (If you configure a firewall filter to send traffic to a port mirror—that is, you use the **analyzer** action modifier in a filter term—this counts as an ingress mirroring configuration for switch or Node group on which the filter is applied.)
  - There can be no more than two configurations that mirror egress traffic.

NOTE: **On QFabric systems, there is no system-wide limit on the total number of mirror sessions.**

- You can configure no more than one type of output in one port-mirroring configuration. That is, you can use no more than one of the following to complete a **set analyzer *name* output** statement:
  - **interface**
  - **ip-address**
  - **vlan**
- If you configure Junos OS to mirror egress packets, do not configure more than 2000 VLANs on a standalone switch or QFabric system. If you do so, some VLAN packets might contain incorrect VLAN IDs. This applies to any VLAN packets—not only the mirrored copies.
- The **ratio** and **loss-priority** options are not supported.
- Packets with physical layer errors are filtered out and are not sent to the output port or VLAN.

- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit from the output interface.
- You cannot mirror packets exiting or entering the following ports:
  - Dedicated Virtual Chassis interfaces
  - Management interfaces (me0 or vme0)
  - Fibre Channel interfaces
  - Routed VLAN interfaces
- An aggregated Ethernet interface cannot be an output interface if the input is a VLAN or if traffic is sent to the analyzer by a firewall filter.
- When packet copies are sent out the output interface, they are not modified for any changes that are normally applied on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.
- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.
- VLAN-based mirroring is not supported for STP traffic.
- (QFabric systems only) If you configure a QFabric analyzer to mirror egress traffic and the input and output interfaces are on different Node devices, the mirrored copies have incorrect VLAN IDs. This limitation does not apply if you configure a QFabric analyzer to mirror egress traffic and the input and output interfaces are on the *same* Node device. In this case the mirrored copies have the correct VLAN IDs (as long as you do not configure more than 2000 VLANs on the QFabric system).

Remote Port Mirroring Only

The following constraints and limitations apply to remote port mirroring:

- If you configure an output IP address, the address cannot be in the same subnetwork as any of the switch's management interfaces.
- If you create virtual routing instances and also create an analyzer configuration that includes an output IP address, the output address belongs to the default virtual routing instance (inet.0 routing table).
- An output VLAN cannot be a private VLAN or VLAN range.
- An output VLAN cannot be shared by multiple **analyzer** statements.
- An output VLAN interface cannot be a member of any other VLAN.
- An output VLAN interface cannot be an aggregated Ethernet interface.

Port Mirroring Constraints on OCX Series Switches

The following constraints and limitations apply to port mirroring on OCX Series switches:

- You can create a total of four port-mirroring configurations. The following constraints also apply:
  - There can be no more than two configurations that mirror ingress traffic.
  - There can be no more than two configurations that mirror egress traffic.
- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit from the output interface.
- You can create only one port-mirroring session.
- You cannot mirror packets exiting or entering the following ports:
  - Dedicated Virtual Chassis interfaces
  - Management interfaces (me0 or vme0)
  - Fibre Channel interfaces
  - Routed VLAN interfaces or IRB interfaces
- An aggregated Ethernet interface cannot be an output interface.
- Do not include an 802.1Q subinterface that has a unit number other than 0 in a port mirroring configuration. Port mirroring does not work with subinterfaces if their unit number is not 0. (You configure 802.1Q subinterfaces using the **vlan-tagging** statement.)
- When packet copies are sent out the output interface, they are not modified for any changes that are normally applied on egress, such as CoS rewriting.
- An interface can be the input interface for only one mirroring configuration. Do not use the same interface as the input interface for multiple mirroring configurations.
- CPU-generated packets (such as ARP, ICMP, BPDU, and LACP packets) cannot be mirrored on egress.
- VLAN-based mirroring is not supported for STP traffic.

Related Documentation

- *Understanding Port Mirroring*
- *Example: Mirroring Employee Web Traffic with a Firewall Filter*
- *Configuring Port Mirroring*

Egress Port Mirroring with VLAN Translation

Problem

Description: If you create a port-mirroring configuration that mirrors customer VLAN (CVLAN) traffic on egress and the traffic undergoes VLAN translation before being mirrored, the VLAN translation does not apply to the mirrored packets. That is, the mirrored packets retain the service VLAN (SVLAN) tag that should be replaced by the CVLAN tag

on egress. The original packets are unaffected—on these packets VLAN translation works properly, and the SVLAN tag is replaced with the CVLAN tag on egress.

Solution This is expected behavior.

See Also
- *Understanding Q-in-Q Tunneling on EX Series Switches*

Egress Port Mirroring with Private VLANs

Problem **Description:** If you create a port-mirroring configuration that mirrors private VLAN (PVLAN) traffic on egress, the mirrored traffic (the traffic that is sent to the analyzer system) has the VLAN tag of the ingress VLAN instead of the egress VLAN. For example, assume the following PVLAN configuration:

- Promiscuous trunk port that carries primary VLANs pvlan100 and pvlan400.
- Isolated access port that carries secondary VLAN isolated200. This VLAN is a member of primary VLAN pvlan100.
- Community port that carries secondary VLAN comm300. This VLAN is also a member of primary VLAN pvlan100.
- Output interface (monitor interface) that connects to the analyzer system. This interface forwards the mirrored traffic to the analyzer.

If a packet for pvlan100 enters on the promiscuous trunk port and exits on the isolated access port, the original packet is untagged on egress because it is exiting on an access port. However, the mirror copy retains the tag for pvlan100 when it is sent to the analyzer.

Here is another example: If a packet for comm300 ingresses on the community port and egresses on the promiscuous trunk port, the original packet carries the tag for pvlan100 on egress, as expected. However, the mirrored copy retains the tag for comm300 when it is sent to the analyzer.

Solution This is expected behavior.

Related Documentation
- Understanding Port Mirroring on page 3
- Examples: Configuring Port Mirroring for Local Analysis on page 12
- Example: Configuring Port Mirroring for Remote Analysis on page 18
- Example: Mirroring Employee Web Traffic with a Firewall Filter on page 15

PART 2

Configuration Statements and Operational Commands

CHAPTER 2

Configuration Statements (Port Mirroring)

analyzer

Syntax

```
analyzer {
  name {
    input {
      egress {
        interface (all | interface-name);
        vlan (vlan-id | vlan-name);
      }
      ingress {
        interface (all | interface-name);
        vlan (vlan-id | vlan-name);
      }
    output {
      interface interface-name;
      ip-address ip-address;
      routing-instance
      vlan (vlan-id | vlan-name);
    }
  }
}
```

Hierarchy Level

For platforms without ELS:

[edit ethernet-switching-options]

For platforms with ELS:

[edit forwarding-options]

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Option **output vlan** added in Junos OS Release 12.1 for the QFX Series.
Option **output ip-address** added in Junos OS Release 12.3 for the QFX Series for non-ELS platforms and added in 14.1X53-D10 for ELS platforms.

Description

Configure port mirroring. You can create a total of four port-mirroring configurations on the QFX Series, subject to the following limits:

- There can be no more than two configurations that mirror ingress traffic.
- There can be no more than two configurations that mirror egress traffic.

Default

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

Options

all—Mirror all the access interfaces. Using this option does not cause the QSFP+ or management interfaces to be mirrored.

CAUTION: Configuring the all option in a QFabric system causes all the access interfaces on all the nodes to be mirrored. Be cautious about using this option on a QFabric system.

name—Name of the analyzer. The name can include as many as 125 characters; must begin with a letter; and can include uppercase letters, lowercase letters, numbers, dashes, and underscores. No other special characters are allowed.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Understanding Port Mirroring on page 3
- Configuring Port Mirroring on page 9
- Examples: Configuring Port Mirroring for Local Analysis on page 12

egress

Syntax

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

Hierarchy Level

For platforms without ELS:

[edit ethernet-switching-options analyzer *name* input]

For platforms with ELS:

[edit forwarding-options analyzer *name* input]

Release Information

Statement introduced in Junos OS Release 11.2 for the QFX Series.

Description

Specify interface or VLAN for which egressing traffic is mirrored. (The **vlan** statement is not supported on all switches.)

The remaining statement is explained separately. See CLI Explorer.

NOTE: If you configure Junos OS to mirror egress packets, do not configure more than 2000 VLANs. If you do so, some of the mirrored packets might contain incorrect VLAN IDs.

Required Privilege Level

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

Related Documentation

- Understanding Port Mirroring on page 3
- Configuring Port Mirroring on page 9
- Examples: Configuring Port Mirroring for Local Analysis on page 12

ethernet-switching (Port Mirroring)

Syntax

```
ethernet-switching;
output {
  interface interface-name {
  }
  no-filter-check;
  }
  vlan vlan-name {
    no-tag;
  }
}
```

Hierarchy Level [edit forwarding-options port-mirroring [instance *name*] family]

Release Information Statement introduced in Junos OS Release 13.2 for the QFX Series.

Description Specify that the output interface for the port mirror will be configured as an **ethernet-switching** interface.

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

Related Documentation

- Understanding Port Mirroring on page 3
- Configuring Port Mirroring on page 9
- Examples: Configuring Port Mirroring for Local Analysis on page 12

family (Port Mirroring)

List of Syntax

MX, M, T Series Routers, EX Series Switches and SRX Series Firewalls on page 38
Syntax: QFX Series Switches, EX4600 and NFX Series Devices on page 38

MX, M, T Series Routers, EX Series Switches and SRX Series Firewalls

```
family (inet | inet6) {
  output {
    interface interface-name {
      next-hop address;
    }
    no-filter-check;
  }
}
```

Syntax: QFX Series Switches, EX4600 and NFX Series Devices

```
family
  ethernet-switching {
    output {
      interface interface-name {
      }
      no-filter-check;
      }
      vlan vlan-name {
        no-tag;
      }
    }
  inet
    output {
      ip-address address {
      }
      routing-instance instance-name {
        ip-address address {
      }
    }
```

Hierarchy Level

[edit forwarding-options port-mirroring]

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T Series routers, EX Series switches and SRX Series firewalls.
Statement introduced in Junos OS Release 13.2 for the QFX Series and EX4600.

Description

Specify the type of interface that will be used to forward port mirrored packet to an analyzer device. Configure the protocol family to be sampled. Only IPv4 (**inet**) and IPv6 (**inet6**) are supported.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring Port Mirroring on M, T MX, and PTX Series Routers*
- Understanding Port Mirroring on page 3
- Configuring Port Mirroring on page 9
- Examples: Configuring Port Mirroring for Local Analysis on page 12

inet (Port Mirroring)

Syntax

```
inet {
output {
  ip-addressaddress {
  }
  routing-instance instance-name {
    ip-address address {
  }
}
```

Hierarchy Level [edit forwarding-options port-mirroring [instance *name*] family]

Release Information Statement introduced in Junos OS Release 14.1X53 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify that the output interface will be of type **inet**. Use this statement so that you can send the mirrored packets to the IP address of the device running an analyzer application. The device can be on a remote network. When you use this feature, the mirrored packets are GRE-encapsulated. The analyzer device must be able to de-encapsulate GRE-encapsulated packets, or the GRE-encapsulated packets must be de-encapsulated before reaching the analyzer device. (You can use a network sniffer to de-encapsulate the packets.)

NOTE: An output IP address cannot be in the same subnetwork as any of the switch's management interfaces.

NOTE: If you create virtual routing instances and also create an analyzer configuration that includes an output IP address, the output address belongs to the default virtual routing instance (inet.0 routing table).

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

ingress (Port Mirroring)

Syntax

```
ingress {
  interface (all | interface-name);
  vlan (vlan-id | vlan-name);
}
```

Hierarchy Level

For platforms without ELS:

[edit ethernet-switching-options analyzer *name* input]

For platforms with ELS:

[edit forwarding-options analyzer *name* input]

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Specify the interfaces or VLANs for which incoming traffic is mirrored as part of a port mirroring configuration.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Understanding Port Mirroring on page 3
- Configuring Port Mirroring on page 9
- Examples: Configuring Port Mirroring for Local Analysis on page 12

input

Syntax

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

Hierarchy Level

For platforms without ELS:

[edit ethernet-switching-options analyzer *name*]

For platforms with ELS:

[edit forwarding-options analyzer *name*]

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Define the traffic to be mirrored. The definition can be a combination of traffic entering or exiting specific ports or VLANs.

The remaining statements are explained separately. See CLI Explorer.

Default

No default.

Required Privilege Level

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

Related Documentation

- Understanding Port Mirroring on page 3
- Configuring Port Mirroring on page 9
- Examples: Configuring Port Mirroring for Local Analysis on page 12

instance (Port Mirroring)

List of Syntax

Syntax: MX, M and T Series Routers and SRX Series Firewalls on page 42
Syntax: QFX Series Switches, EX4600 and NFX Series Devices on page 42

Syntax: MX, M and T Series Routers and SRX Series Firewalls

```
instance instance-name {
  disable;
  input {
    rate number;
    maximum-packet-length bytes
  }
  family (any | inet | inet6 | vpls) {
    output {
      (next-hop-group group-name | interface interface-name);
    }
  }
}
```

Syntax: QFX Series Switches, EX4600 and NFX Series Devices

```
instance instance-name{
  family
    ethernet-switching {
      output {
        interface interface-name {
        }
        no-filter-check;
        }
        vlan vlan-name {
          no-tag;
        }
      }
    inet
      output {
        ip-address address {
        }
        routing-instance instance-name {
          ip-address address {
        }
      }
    }
  }
```

Hierarchy Level

[edit forwarding-options port-mirroring]

Release Information

Statement introduced in Junos OS Release 9.6 for MX, M and T Series routers and SRX Series firewalls.
Statement introduced in Junos OS Release 13.2 for the QFX Series.

Description

Specify a port-mirroring configuration (instance). You do not specify an input for this instance. Instead, you, create a firewall filter that specifies the required traffic and directs it to the mirror. This is useful for controlling which types of traffic should be mirrored.

The remaining statements are explained separately. See CLI Explorer.

Usage Guidelines

See *Configuring Sampling Instance on MX, M and T Series Routers or QFX Series Switches*.

Required Privilege Level

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

Related Documentation

- Understanding Port Mirroring on page 3
- Configuring Port Mirroring on page 9
- Examples: Configuring Port Mirroring for Local Analysis on page 12
- Example: Mirroring Employee Web Traffic with a Firewall Filter on page 15

interface (Port Mirroring)

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

Hierarchy Level For platforms without ELS:

[edit ethernet-switching-options analyzer *name* input (egress | ingress)],
[edit ethernet-switching-options analyzer *name* output]

For platforms with ELS:

[edit forwarding-options analyzer *name* input (egress | ingress)]
[edit forwarding-options analyzer *name* output]
[edit forwarding-options port-mirroring [instance *name*] family ethernet-switching output]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Specify the interfaces for which ingressing traffic is mirrored. Specify the interface that mirrored traffic should be copied to (the output interface).

Options all—Apply port mirroring to all interfaces on the switch (except the output interface). Mirroring a high volume of traffic can cause performance issues, so you should generally select specific input interfaces.

CAUTION: **Configuring all in a QFabric system causes all the access interfaces on all the nodes to be mirrored. Be cautious about using this option on a QFabric system.**

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

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

Related Documentation

- Understanding Port Mirroring on page 3
- Configuring Port Mirroring on page 9
- Examples: Configuring Port Mirroring for Local Analysis on page 12

ip-address (Port Mirroring)

Syntax ip-address *ip-address*;

Hierarchy Level [edit forwarding-options] analyzer *name* output]
[edit forwarding-options port-mirroring [instance *name*] family ethernet-switching output interface *name*]

Release Information Statement introduced in Junos OS Release 14.1X53 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify the IP address to which traffic should be mirrored (the IP address of the analyzer system). The device can be on a remote network. The analyzer device must be able to de-encapsulate GRE-encapsulated packets, or the GRE-encapsulated packets must be de-encapsulated before reaching the analyzer device. (You can use a network sniffer to de-encapsulate the packets.) This statement is not supported on QFabric systems.

NOTE: An output IP address cannot be in the same subnetwork as any of the switch's management interfaces.

NOTE: If you create virtual routing instances and also create an analyzer configuration that includes an output IP address, the output address belongs to the default virtual routing instance (inet.0 routing table).

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

no-tag

Syntax no-tag;

Hierarchy Level [edit forwarding-options analyzer *name* output vlan]
[edit forwarding-options port-mirroring [instance *name*] family ethernet-switching output vlan]

Release Information Statement introduced in Junos OS Release 15.1X53-D10 for QFX10000 switches.

Description Specify that remote mirrored packets are not tagged with the tag of the output (analyzer) VLAN.

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 Analysis on page 18

output

Syntax

```
output {
  interface interface-name;
  ip-address ip-address;
  vlan (vlan-id | vlan-name);
  routing-instance instance-name {
    ip-address address {
}
```

Hierarchy Level

For platforms without ELS:

[edit ethernet-switching-options analyzer *name*]

For platforms with ELS:

[edit forwarding-options analyzer *name*]
[edit forwarding-options port-mirroring [instance *name*] family ethernet-switching]

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Option **output vlan** added in Junos OS Release 12.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the destination for mirrored traffic, either an interface on the switch (for local monitoring) or a VLAN (for remote monitoring).

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

port-mirroring

List of Syntax

Syntax: MX Series and PTX Series Routers, M120 and M320 on page 48
Syntax: QFX Series Switches, EX4600 and NFX Series Devices on page 49
Syntax: OCX1100 on page 50

Syntax: MX Series and PTX Series Routers, M120 and M320

```
port-mirroring {
  input {
    maximum-packet-length bytes;
    rate number;
    run-length number;
  }
  family (ccc | inet | inet6 | vpls) {
    output {
      interface interface-name {
        next-hop address;
      }
      next-hop-group group-name{
        group-type inet6;
        interface interface-name {
          next-hop ipv6-address;
        }
        next-hop-subgroup group-name{
          interface interface-name {
            next-hop ipv6-address;
          }
        }
      }
      no-filter-check;
    }
  }
  instance {
    instance-name {
      input {
        maximum-packet-length bytes;
        rate number;
        run-length number;
      }
      family (ccc | inet | inet6 | vpls) {
        output {
          interface interface-name {
            next-hop address;
          }
          no-filter-check;
          server-profile server-profile-name;
        }
      }
    }
  }
  mirror-once;
  traceoptions {
    file filename <files number> <size bytes> <world-readable | no-world-readable>;
  }
}
```

Syntax: QFX Series Switches, EX4600 and NFX Series Devices

```
port-mirroring {
  family {
    ethernet-switching
      output {
        interface interface-name {
        }
        no-filter-check;
        }
        vlan vlan-name {
          no-tag;
        }
      }
    inet
      output {
        ip-address address {
        }
        routing-instance instance-name {
          ip-address address {
        }
      }
  }
  instance instance-name {
    family
      ethernet-switching {
        output {
          interface interface-name {
          }
          no-filter-check;
          }
          vlan vlan-name {
            no-tag;
          }
        }
      inet
        output {
          ip-address address {
          }
          routing-instance instance-name {
            ip-address address {
          }
        }
      }
    }
  }
}
```

Syntax: OCX1100

```
port-mirroring {
  family {
    inet
      output {
        ip-address address {
        }
        routing-instance instance-name {
          ip-address address {
        }
      }
  }
  instance instance-name {
    family
      inet
        output {
          ip-address address {
          }
          routing-instance instance-name {
            ip-address address {
          }
        }
      }
    }
  }
}
```

Hierarchy Level [edit forwarding-options]

Release Information

Statement introduced before Junos OS Release 7.4 for MX Series and PTX Series routers, M120 and M320.
family vpls statement introduced in Junos OS Release 9.3 (MX Series routers only); support extended to M7i, M10, M120, and M320 routers in Junos OS Release 9.5.
instance ***port-mirroring-instance-name*** statement introduced in Junos OS Release 9.3 (MX Series routers only); support extended to M120 and M320 routers in Junos OS Release 9.5.
mirror-once statement introduced in Junos OS Release 9.3 (MX Series routers only); support extended to M120 routers in Junos OS Release 9.5.
family ccc statement introduced in Junos OS Release 9.6 (M120 and M320 routers only).
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
family inet6 and **next-hop-group** statements introduced in Junos OS Release 14.2 (MX Series routers only).
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Create a port-mirroring configuration. Specify the address family, rate, run length, interface, and next-hop address for sending copies of packets to an analyzer.

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation

- *Configuring Port Mirroring*

  Configuring Port Mirroring on page 9
- *Configuring Port Mirroring*
- *Configuring Active Flow Monitoring on PTX Series Packet Transport Routers*
- Understanding Port Mirroring on page 3
- *Understanding Port Mirroring*
- Examples: Configuring Port Mirroring for Local Analysis on page 12
- Example: Mirroring Employee Web Traffic with a Firewall Filter on page 15
- *Example: Mirroring Employee Web Traffic with a Firewall Filter*

routing-instance (Port Mirroring)

Syntax
routing-instance *instance-name*;

Hierarchy Level
[edit forwarding-options] analyzer *name* output]
[edit forwarding-options port-mirroring [instance *name*] family inet output interface *name*]

Release Information
Statement introduced in Junos OS Release 12.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Configure a port mirroring instance. You do not specify an input for this instance. Instead, you, create a firewall filter that specifies the required traffic and directs it to the mirror. This instance type is useful for controlling which types of traffic should be mirrored.

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

vlan (Port Mirroring)

Syntax

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

Hierarchy Level

For platforms without ELS:

[edit ethernet-switching-options analyzer *name* input ingress],
[edit ethernet-switching-options analyzer *name* output]

For platforms with ELS:

[edit forwarding-options analyzer *name* input (egress | ingress)]
[edit forwarding-options analyzer *name* output]
[edit forwarding-options port-mirroring [instance *name*] family ethernet-switching output]

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Option**output vlan** added in Junos OS Release 12.1 for the QFX Series.
Option**no-tag** added in Junos OS Release 15.1X53-D10 for QFX10000 switches.

Description

When used in an **input** statement, specifies that traffic entering or exiting a VLAN should be mirrored. (You can include this statement in an **ingress** statement or **egress** statement within the **input** statement. It is not supported in an **egress** statement on all switches) When used in an **output** statement, specifies that mirrored traffic to be sent to a VLAN for remote monitoring.

On some switches, only one interface can be a member of the output (analyzer) VLAN. This limitation does not apply on the QFX10000 switch if traffic is mirrored on ingress. In this case, multiple QFX10000 interfaces can belong to the output VLAN, and traffic is mirrored to all of those interfaces. If traffic is mirrored on egress on a QFX10000 switch, only one interface can be a member of the analyzer VLAN.

Options

vlan-id—Numeric VLAN identifer.

vlan-name—Name of the VLAN.

no-tag—Specifies that remote mirrored packets are not tagged with the tag of the output (analyzer) VLAN.

Required Privilege Level

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

Related Documentation

- Understanding Port Mirroring on page 3
- Configuring Port Mirroring on page 9
- Examples: Configuring Port Mirroring for Local Analysis on page 12

CHAPTER 3

Operational Command (Port Mirroring)

- show analyzer

show analyzer

Syntax **show analyzer <*analyzer-name*>**

Release Information Command introduced in Junos OS Release 11.1 for the QFX Series.

Description Display information about port mirroring.

Options ***analyzer-name***—(Optional) Displays the status of a specific analyzer (port-mirroring configuration).

Required Privilege Level view

Related Documentation
- *Understanding Layer 2 Port Mirroring*
- Troubleshooting Port Mirroring on page 26

List of Sample Output show analyzer on page 54

Output Fields Table 4 on page 54 describes the output fields for the **show analyzer** command. Output fields are listed in the approximate order in which they appear.

Table 4: show analyzer Output Fields

Field Name	Field Description
Analyzer name	Name of the analyzer.
Output interface	Local interface to which mirror packets are sent. If you configure an output interface, you cannot also configure an output VLAN.
Output VLAN	VLAN to which mirror packets are sent. If you configure an output VLAN, you cannot also configure an output interface.
Egress monitored interfaces	Interfaces for which egress traffic is mirrored.
Egress monitored VLANs	VLANs for which egress traffic is mirrored.
Ingress monitored interfaces	Interfaces for which ingress traffic is mirrored.
Ingress monitored VLANs	VLANs for which ingress traffic is mirrored.

Sample Output

show analyzer

```
user@switch> show analyzer
```

```
Analyzer name                  : employee-monitor
  Output interface             : ge-0/0/10.0
  Output VLAN                  : remote-analyzer
  Egress monitored interfaces  : ge-0/0/7.0
  Ingress monitored interfaces : ge-0/0/8.0
  Ingress monitored interfaces : ge-0/0/9.0
```