# Services on the QFX Series

Release
13.2X52

Published: 2014-07-15

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



*Services on the QFX Series*
13.2X52


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:

- QFabric System

## 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 xiii 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 xiii 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:<br><br>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**<br>`No alarms currently active` |
| *Italic text like this* | • Introduces or emphasizes important new terms.<br>• Identifies guide names.<br>• Identifies RFC and Internet draft titles. | • A policy *term* is a named structure that defines match conditions and actions.<br>• *Junos OS CLI User Guide*<br>• 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:<br>[edit]<br>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.<br>• 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**<br>**(*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]<br>routing-options {<br>  static {<br>  route default {<br>  nexthop *address*;<br>  retain;<br>  }<br>  }<br>} |
| ; (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**.<br>• 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

# 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. 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 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 | Port-mirroring configuration. The analyzer includes a name, source interfaces or source VLAN, and a destination for mirrored packets (either a local access interface or a VLAN). |
| 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.<br><br>The following limitations apply to an output interface:<br><br>• Cannot also be a source port.<br>• Cannot be used for switching.<br>• Cannot be an aggregated Ethernet interface (LAG).<br>• Does not participate in Layer 2 protocols, such as Spanning Tree Protocol (STP).<br>• Loses any existing VLAN associations when you configure it as an analyzer output interface.<br><br>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.)<br><br>• An output IP address cannot be in the same subnetwork as any of the switch's management interfaces.<br>• 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). |

Table 3: Port Mirroring Terms and Definitions *(continued)*

| | |
|---|---|
| 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.<br><br>The following limitations apply to an output VLAN:<br><br>• Cannot be a private VLAN or VLAN range.<br>• Cannot be shared by multiple **analyzer** statements.<br>• An output VLAN interface cannot be a member of any other VLAN.<br>• An output VLAN interface cannot be an aggregated Ethernet interface (LAG).<br>• On the source (monitored) 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. |
| 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 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 Constraints and Limitations



### Local and Remote Port Mirroring

The following constraints and limitations apply to local and remote port mirroring with the QFX Series:

- You can create a total of four port-mirroring configurations on a QFX Series standalone switch.
- 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 QFX3500 device 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.
- 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.
- (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 with the QFX Series:

- 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.
- On the source (monitored) switch, only one interface can be a member of the analyzer VLAN.

**Related Documentation**

- Configuring Port Mirroring on page 23
- Example: Configuring Port Mirroring for Local Analysis on page 13
- Example: Configuring Port Mirroring for Remote Analysis on page 18
- *Example: Configuring Port Mirroring for Local Analysis*
- *Example: Configuring Port Mirroring for Remote Analysis*
- Troubleshooting Port Mirroring on page 77

## Understanding Layer 3 Logical Interfaces

A Layer 3 logical interface is a logical division of a physical interface that operates at the network level and therefore can receive and forward 802.1Q VLAN tags. You can use Layer 3 logical interfaces to route traffic among multiple VLANs along a single trunk line that connects a Juniper Networks QFX3500 Switch to a Layer 2 switch. Only one physical connection is required between the switches. You can also use Layer 3 logical interfaces to provide alternative gateway addresses for smart DHCP relay.

To create Layer 3 logical interfaces on a switch, enable VLAN tagging, partition the physical interface into logical partitions, and bind the VLAN ID to the logical interface.

We recommend that you use the VLAN ID as the logical interface number when you configure the logical interface. QFX Series systems support a maximum of 4089 VLANs, which includes the default VLAN. You can, however, assign a VLAN ID in the range of 1 to 4094, but five of these VLAN IDs are reserved for internal use.

VLAN tagging places the VLAN ID in the frame header, allowing each physical interface to handle multiple VLANs. When you configure multiple VLANs on an interface, you must also enable tagging on that interface. Junos OS on switches supports a subset of the 802.1Q standard for receiving and forwarding routed or bridged Ethernet frames with single VLAN tags and running Virtual Router Redundancy Protocol (VRRP) over 802.1Q-tagged interfaces.

**Related Documentation**

- *Interfaces Overview*
- *Configuring a Layer 3 Logical Interface*
- Configuring DHCP and BOOTP Relay on page 26
- *Junos OS Network Interfaces Library for Routing Devices*

CHAPTER 2

# DHCP Relay



## DHCP and BOOTP Relay Overview

You can configure a Juniper Networks switch to act as a Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP) relay agent. This means that if the switch receives a broadcast DHCP or BOOTP request from a locally attached host (client), it relays the message to a specified DHCP or BOOTP server. You should configure the switch to be a DHCP/BOOTP relay agent if you have locally attached hosts and a distant DHCP or BOOTP server.

If you configure a switch to be a DHCP relay agent, you can also enable smart DHCP relay, which enables you to configure alternative gateway addresses for a DHCP server so that if the server fails to reply to the requests sent to the primary gateway address, the switch can resend the requests to the alternative gateway addresses. To use this feature, you must configure a routed VLAN interface or Layer 3 subinterface with multiple IP addresses and configure that interface to be a relay agent.

NOTE: Because DHCP and BOOTP messages are broadcast and are not directed to a specific server, switch, or router, Juniper switches cannot function as both a DHCP server and a DHCP/BOOTP relay agent at the same time. The Junos operating system (Junos OS) generates a commit error if both options are configured at the same time, and the commit operation does not succeed until one of the options is removed.

**Related Documentation**

- Configuring DHCP and BOOTP Relay on page 26
- bootp on page 63

PART 2

# Configuration

CHAPTER 3

# Configuration Examples



## Example: 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 a release of Junos OS that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see *Example: Configuring Port Mirroring for Local Analysis*. 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 11.1
- A switch

## Overview and Topology

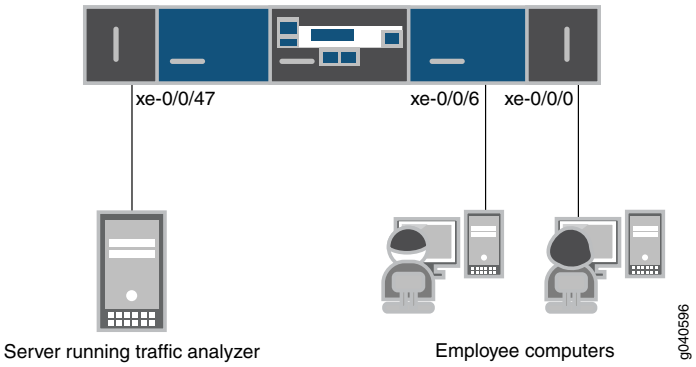
This topic includes two related examples that describe how to mirror traffic entering interfaces on the switch to an access interface on the same switch. The first example shows how to mirror all traffic sent by employee computers to the switch. The second example includes a filter to mirror only the 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 14 shows the network topology for this example.

**Figure 1: Network Topology for Local Port Mirroring 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 ethernet-switching-options analyzer employee-monitor input ingress interface xe-0/0/0.0
set ethernet-switching-options analyzer employee-monitor input ingress interface xe-0/0/6.0
set ethernet-switching-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 ethernet-switching-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 ethernet-switching-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 ethernet-switching-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;
      }
    }
  }
}
```

## Mirroring Employee-to-Web Traffic for Local Analysis

To mirror only traffic sent by employees to the Web for local analysis, perform the tasks explained in this section.

**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 ethernet-switching-options analyzer 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 analyzer
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** analyzer output. (Configure only the output—the input comes from the filter.)

```
[edit ethernet-switching-options]
user@switch# set analyzer 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 analyzer **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 analyzer:

```
[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 analyzer
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 ethernet-switching-options
  analyzer 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 analyzer 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 analyzer
  Analyzer name                 : employee-monitor
  Output interface              : xe-0/0/47.0
  Mirror ratio                  : 1
  Loss priority                 : Low
  Ingress monitored interfaces : xe-0/0/0.0
  Ingress monitored interfaces : xe-0/0/6.0
  Egress monitored interfaces  : None
```

**Meaning** This output shows that the **employee-monitor** analyzer:

- Has a ratio of 1 (mirroring every packet, the default setting)
- Has a loss priority of low (set this option to high only when the analyzer output is to a VLAN)
- Is mirroring the traffic entering the **xe-0/0/0** and **xe-0/0/6** interfaces
- Is sending the mirrored traffic to the **xe-0/0/47** interface

**Related Documentation**

- Understanding Port Mirroring on page 3
- Configuring Port Mirroring on page 23
- 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.

NOTE: This example uses a release of Junos OS that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see *Example: Configuring Port Mirroring for Remote Analysis*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.



## Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.1 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-0/0/10** 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 ethernet-switching-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set ethernet-switching-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set ethernet-switching-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 ethernet-switching-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
ethernet-switching-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 port mode trunk
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999set
ethernet-switching-options analyzer 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 analyzer
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 port 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 ethernet-switching-options]
   user@switch# set ethernet-switching-optionsanalyzer 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 analyzer
   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 {
        port-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 analyzer employee-web-monitor;
      }
    }
  }
}
ethernet-switching-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 23
- Example: Configuring Port Mirroring for Local Analysis on page 13
- *Overview of Firewall Filters*

CHAPTER 4

# Configuration Tasks



## 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 a release of Junos OS that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports 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

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 ethernet-switching-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 ethernet-switching-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 ethernet-switching-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 ethernet-switching-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 ethernet-switching-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 ethernet-switching-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

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 **analyzer *analyzer-name*.** If you use the same analyzer in multiple filters or terms, the output packets are copied only once.

NOTE: You can include the action analyzer in ingress firewall filters only. You can apply ingress filters with this action to ports (Layer 2 interfaces), Layer 3 interfaces, and VLANs.

When you use a firewall filter as the input to an analyzer, you output 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 an analyzer for local or remote analysis. Configure only the output. For example, for local analysis enter:

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

NOTE: Do not configure input to this analyzer.

2. Create a firewall filter using any of the available match conditions and specify the action as **analyzer *analyzer-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
- Example: Configuring Port Mirroring for Local Analysis on page 13
- Example: Configuring Port Mirroring for Remote Analysis on page 18
- *Overview of Firewall Filters*

## Configuring DHCP and BOOTP Relay

You can configure the QFX Series to act as a Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) relay agent. This means that if a locally attached host can issue a DHCP or BOOTP request as a broadcast message and the switch relays the message to a specified DHCP or BOOTP server. You should configure a switch to be a DHCP and BOOTP relay agent if you have locally attached hosts and a remote DHCP or BOOTP server.

NOTE: This task uses a release of Junos OS that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see *Configuring DHCP and BOOTP*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

If you configure a switch to be a DHCP relay agent, you can also enable smart DHCP relay, which allows you to configure alternative gateway addresses for a DHCP server so that if the server fails to reply to the requests sent using the primary gateway address, the switch can resend the requests via the alternative gateway addresses. To use this feature, you must configure a routed VLAN interface or Layer 3 logical interface with multiple IP addresses and configure that interface to be a relay agent.

- Configuring a DHCP and BOOTP Relay Agent on page 26
- Configuring DHCP Smart Relay on page 28

### Configuring a DHCP and BOOTP Relay Agent

To configure a switch to act as a DHCP and BOOTP relay agent, include the **bootp** statement at the **[edit forwarding-options helpers]** hierarchy level:

```
[edit forwarding-options helpers]
bootp {
  apply-secondary-as-giaddr text-description;
```

```
    client-response-ttl number;
    description text-description;
    interface (interface-name | interface-group) {
      client-response-ttl number;
      description text-description;
      maximum-hop-count number;
      minimum-wait-time seconds;
      no-listen;
      server address
      apply-secondary-as-giaddr
    }
    maximum-hop-count number;
    minimum-wait-time seconds;
    relay-agent-option;
    server server-identifier
  }
```

To include a description of the BOOTP service, DHCP service, or interface, use the **description** statement.

To configure a logical interface or a group of logical interfaces with a specific DHCP relay or BOOTP configuration, include the **interface** statement.

To stop packets from being forwarded, include the **no-listen** statement.

To set the maximum allowed number in the hops field of the BOOTP message, include the **maximum-hop-count** statement. BOOTP messages that have a larger number in the hops field than the maximum allowed are not forwarded. If you omit the **maximum-hop-count** statement, the default maximum number of hops is four.

To set the minimum allowed number of seconds in the **secs** field of the BOOTP message, include the **minimum-wait-time** statement. This setting configures a minimum number of seconds since the client sent its first BOOTP request. BOOTP messages that have a smaller number in the **secs** field than the allowed minimum are not forwarded. The default value for the minimum wait time is zero (0).

To set the IP address that specify the DHCP or BOOTP server for the router, switch, or interface, include the **server** statement. You can include multiple **server** statements.

To set an IP time-to-live (TTL) value for DHCP response packets sent to a DHCP client, include the **client-response-ttl** statement.

The following example demonstrates a BOOTP relay agent configuration.

```
user@host# show forwarding-options
helpers {
  bootp {
    description "dhcp relay agent global parameters";
    server 192.168.55.44;
    server 172.16.0.3 routing-instance c3;
    maximum-hop-count 10;
    minimum-wait-time 8;
    interface {
      xe-0/0/1 {
        description "use this info for this interface";
```

```
            server 10.10.10.10;
            server 192.168.14.14;
            maximum-hop-count 11;
            minimum-wait-time 3;
          }
          xe-0/0/2 {
            no-listen; ###ignore DHCPDISCOVER messages on this interface
          }
          all {
            description "globals apply to all other interfaces";
          }
        }
      }
    }
```

## Configuring DHCP Smart Relay

You can use DHCP smart relay to provide redundancy and resiliency to your DHCP relay configuration. Smart relay provides additional relay functionality and requires all of the configuration settings required by DHCP relay. To use DHCP smart relay, you also need an interface with multiple IP addresses assigned to it. You can achieve this by doing either of the following tasks:

- Create a routed VLAN interface and assign at least two IP addresses to it. See *Configuring Routed VLAN Interfaces* and *Example: Configuring Routing Between VLANs on One Switch* for information about this approach.
- Create a Layer 3 logical interface (by using VLAN tagging) and assign at least two IP addresses to it. See "Understanding Layer 3 Logical Interfaces" on page 7 and *Configuring a Layer 3 Logical Interface* for information about this approach.

Once you have created an interface with multiple IP addresses, complete the smart relay configuration by entering one of the following statements:

- **set forwarding-options helpers bootp smart-relay-global**: Use this statement to enable smart relay on all the interfaces that are configured as relay agents.
- **set forwarding-options helpers bootp interface *interface-name* smart-relay-agent**: Use this statement to enable smart relay on a specific interface.

When smart relay is configured for an interface, the switch initially sends DHCP request (discover) messages out of that interface using the primary address of the interface as the gateway IP address (in the giaddr field) for the DHCP message. If no DHCP offer message is received from a server in reply, the switch allows the client to send as many as three more discover messages using the same gateway IP address. If no DHCP offer message is received after three retries, the switch resends the discover message using the alternate IP address as the gateway IP address. If you configure more than two IP addresses on the relay agent interface, the switch repeats this process until a DHCP offer message is received or all of the IP addresses have been used without success.

CHAPTER 5

# Configuration Statements for Port Mirroring

## analyzer

**Syntax**

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

**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.

**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 23
- Example: Configuring Port Mirroring for Local Analysis on page 13

## egress

**Syntax**

```
egress {
  interface (all | interface-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 interfaces for which egressing traffic is mirrored.

The statement is explained separately.

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 23
- Example: Configuring Port Mirroring for Local Analysis on page 13

## ethernet-switching-options

**Syntax**

```
ethernet-switching-options {
  analyzer {
    name {
      input {
        egress {
          interface (all | interface-name);
        }
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
      output {
        interface interface-name;
        ip-address ip-address;
        vlan (vlan-id | vlan-name);
      }
    }
  }
  bpdu-block {
    interface (all | [interface-name]);
    disable-timeout timeout;
  }
  dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100)
  }
  interfaces interface-name {
    no-mac-learning;
  }
  mac-table-aging-time seconds {
  }
  port-error-disable {
    disable-timeout timeout;
  }
  secure-access-port {
    dhcp-snooping-file {
      location local_pathname | remote_URL;
      timeout seconds;
      write-interval seconds;
    }
    interface (all | interface-name) {
      allowed-mac {
        mac-address-list;
      }
      (dhcp-trusted | no-dhcp-trusted);
      fcoe-trusted;
      mac-limit limit action action;
      no-allowed-mac-log;
    }
    vlan (all | vlan-name) {
      (arp-inspection | no-arp-inspection) [
        forwarding-class (for DHCP Snooping or DAI Packets) class-name;
      }
```

```
        dhcp-option82 {
          circuit-id {
            prefix (Circuit ID for Option 82) hostname;
            use-interface-description;
            use-vlan-id;
          }
          remote-id {
            prefix (Remote ID for Option 82) hostname | mac | none;
            use-interface-description;
            use-string string;
          }
          vendor-id <string>;
        }
        (examine-dhcp | no-examine-dhcp) {
          forwarding-class (for DHCP Snooping or DAI Packets) class-name;
        }
        examine-fip {
          examine-vn2vn {
            beacon-period milliseconds;
          }
          fc-map fc-map-value;
          no-fip-snooping-scaling;
        }
        mac-move-limit limit <fabric-limit limit action action;
      }
    }
    static {
      vlan vlan-id {
        mac mac-address next-hop interface-name;
      }
    }
    storm-control {
      interface (all | interface-name) {
        bandwidth bandwidth;
        no-broadcast;
        no-multicast;
        no-unknown-unicast;
      }
    }
    traceoptions {
      file filename <files number> <no-stamp> <replace> <size size> <world-readable |
        no-world-readable>;
      flag flag <disable>;
    }
}
```

**Hierarchy Level** [edit]

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

**Description** Configure Ethernet switching options.

The remaining statements are explained separately.

**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
- *Overview of Access Port Protection*
- *Understanding Storm Control*

## ingress (ethernet-switching-options)

**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 statements are explained separately.

**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 23
- Example: Configuring Port Mirroring for Local Analysis on page 13

## 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 statements are explained separately.

**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 23
- Example: Configuring Port Mirroring for Local Analysis on page 13

## 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]

**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 23
- Example: Configuring Port Mirroring for Local Analysis on page 13

## ip-address (Port Mirroring)

**Syntax** ip-address *ip-address*;

**Hierarchy Level** [edit ethernet-switching-options analyzer *name* output]

**Release Information** Statement introduced in Junos OS Release 12.3 for the QFX 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.

**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 23
- Example: Configuring Port Mirroring for Local Analysis on page 13

## output

**Syntax**

```
output {
  interface interface-name;
  ip-address ip-address;
  vlan (vlan-id | vlan-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.
Option **output vlan** added in Junos OS Release 12.1 for the QFX Series.

**Description**

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

The statements are explained separately.

**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 23
- Example: Configuring Port Mirroring for Local Analysis on page 13

## vlan (Port Mirroring)

**Syntax** vlan (*vlan-id* | *vlan-name*);

**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]

**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.

**Description** Specify that traffic entering into a VLAN should be mirrored. Configure mirrored traffic to be sent to a VLAN for remote monitoring (output).

**Options** *vlan-id*—Numeric VLAN identifer.

*vlan-name*—Name of the 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 23
- Example: Configuring Port Mirroring for Local Analysis on page 13

CHAPTER 6

# Configuration Statements for Encryption

## authentication-key-chains

**Syntax**

```
authentication-key-chains {
  key-chain key-chain-name {
    description text-string;
    key key {
      algorithm (md5 | hmac-sha-1);
      options (basic | isis-enhanced);
      secret secret-data;
      start-time yyyy-mm-dd.hh:mm:ss;
    }
    tolerance seconds;
  }
}
```

**Hierarchy Level** [edit security]

**Release Information**

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure authentication key updates for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol. When the **authentication-key-chains** statement is configured at the **[edit security]** hierarchy level, and is associated with the BGP, LDP, or IS-IS protocols at the **[edit protocols]** hierarchy level or with the BFD protocol using the **bfd-liveness-detection** statement, authentication key updates can occur without interrupting routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).

The remaining statements are explained separately.

**Required Privilege Level**

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

**Related Documentation**

- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

## cache-size

**Syntax** cache-size *bytes*;

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the cache size for digital certificates.

**Options** ***bytes***—Cache size for digital certificates.

**Range:** 64 through 4,294,967,295

**Default:** 2 megabytes (MB)

NOTE: We recommend that you limit your cache size to 4 MB.

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

**Related Documentation**

- *Configuring Digital Certificates for an ES PIC*

## cache-timeout-negative

**Syntax** cache-timeout-negative *seconds*;

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** (Encryption interface on M Series and T Series routers and EX Series switches only) Configure a negative cache for digital certificates.

**Options** ***seconds***—Negative time to cache digital certificates, in seconds.

**Range:** 10 through 4,294,967,295

**Default:** 20

CAUTION: Configuring a large negative cache value can lead to a denial-of-service attack.

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

**Related Documentation**

- *Configuring Digital Certificates for an ES PIC*

## ca-name

**Syntax** ca-name *ca-identity*;

**Hierarchy Level** [edit security certificates certification-authority]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** (Encryption interface on M Series and T Series routers and EX Series switches only) Specify the certificate authority (CA) identity to use in the certificate request.

**Options** ***ca-identity***—CA identity to use in the certificate request.

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

**Related Documentation**

- *Configuring Digital Certificates for an ES PIC*

## certificates

**Syntax**

```
certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority ca-profile-name {
    ca-name ca-identity;
    crl file-name;
    encoding (binary | pem);
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
  }
  enrollment-retry attempts;
  local certificate-name {
    certificate-key-string;
    load-key-file URL filename;
  }
  maximum-certificates number;
  path-length certificate-path-length;
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the digital certificates for IPsec.

The remaining statements are explained separately.

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

**Related Documentation**

- *Configuring Digital Certificates for an ES PIC*

## certification-authority

**Syntax**

```
certification-authority ca-profile-name {
  ca-name ca-identity;
  crl file-name;
  encoding (binary | pem);
  enrollment-url url-name;
  file certificate-filename;
  ldap-url url-name;
}
```

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** (Encryption interface on M Series and T Series routers and EX Series switches only) Configure a certificate authority profile name.

The remaining statements are explained separately.

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

**Related Documentation**

- *Configuring Digital Certificates for an ES PIC*

## crl (Encryption Interface)

**Syntax** crl *file-name*;

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.

**Options** ***file-name***—Specify the file from which to read the CRL.

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

**Related Documentation**

- *Configuring Digital Certificates for an ES PIC*

## encoding

**Syntax** encoding (binary | pem);

**Hierarchy Level** [edit security ike policy *ike-peer-address*],
[edit security certificates certification-authority *ca-profile-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** (Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file format used for the **local-certificate** and **local-key-pair** statements.

**Options** **binary**—Binary file format.

**pem**—Privacy-enhanced mail (PEM), an ASCII base 64 encoded format.

**Default:** binary

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

**Related Documentation**
- *Configuring Digital Certificates for an ES PIC*
- *Configuring an IKE Policy for Digital Certificates for an ES PIC*

## enrollment-retry

**Syntax** enrollment-retry *attempts*;

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** (Encryption interface on M Series and T Series routers and EX Series switches only) Specify how many times a router or switch can resend a digital certificate request.

**Options** ***attempts***—Number of enrollment retries.

**Range:** 0 through 100

**Default:** 0

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

**Related Documentation**
- *Configuring Digital Certificates for an ES PIC*

## enrollment-url

**Syntax** enrollment-url *url-name*;

**Hierarchy Level** [edit security certificates certification-authority *ca-profile-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** (Encryption interface on M Series and T Series routers and EX Series switches only) Specify where your router or switch sends Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests (certificate authority URL).

**Options** *url-name*—Certificate authority URL.

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

**Related Documentation**
- *Configuring Digital Certificates for an ES PIC*

## file

**Syntax** file *certificate-filename*;

**Hierarchy Level** [edit security certificates certification-authority *ca-profile-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** (Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file from which to read the digital certificate.

**Options** *certificate-filename*—File from which to read the digital certificate.

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

**Related Documentation**
- *Configuring Digital Certificates for an ES PIC*

## key (Authentication Keychain)

**Syntax**

```
key key {
    algorithm (md5 | hmac-sha-1);
    options (basic | isis-enhanced);
    secret secret-data;
    start-time yyyy-mm-dd.hh:mm:ss;
}
```

**Hierarchy Level** [edit security authentication-key-chains key-chain *key-chain-name*]

**Release Information**

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

**Description** Configure the authentication element.

**Options** ***key***—Each key within a keychain is identified by a unique integer value.

**Range:** 0 through 63

The remaining statements are explained separately.

**Required Privilege Level**

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

**Related Documentation**

- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

## key-chain (Security)

**Syntax**

```
keychain key-chain-name {
  description text-string;
  key key {
    algorithm (md5 | hmac-sha-1);
    options (basic | isis-enhanced);
    secret secret-data;
    start-time yyyy-mm-dd.hh:mm:ss;
  }
  tolerance seconds;
}
```

**Hierarchy Level** [edit security authentication-key-chains]

**Release Information**

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description** Create the key-chain configuration for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol.

**Options**

***key-chain-name***—Authentication keychain name. It can be up to 126 characters. Characters can include any ASCII strings. If you include spaces, enclose all characters in quotation marks (“ ”).

**Required Privilege Level**

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

**Related Documentation**

- authentication-key-chains on page 42
- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

## ldap-url

**Syntax** <ldap-url *url-name*>;

**Hierarchy Level** [edit security certificates certification-authority *ca-profile-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** (Encryption interface on M Series and T Series routers and EX Series switches only) (Optional) Specify the Lightweight Directory Access Protocol (LDAP) URL for digital certificates.

**Options** ***url-name***—Name of the LDAP URL.

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

**Related Documentation**
- *Configuring Digital Certificates for an ES PIC*

## local

**Syntax**

```
local certificate-name {
    certificate-key-string;
    load-key-file URL filename;
}
```

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** Import a paired X.509 private key and authentication certificate, to enable Junos XML protocol client applications to establish Secure Sockets Layer (SSL) connections to the router or switch.

**Options**

***certificate-namecertificate-key-string***—String of alphanumeric characters that constitute the private key and certificate.

***certificate-name***—Name that uniquely identifies the certificate.

**load-key-file *URL filename***—File that contains the private key and certificate. It can be one of two types of values:

- Pathname of a file on the local disk (assuming you have already used another method to copy the certificate file to the router's or switch's local disk)
- URL to the certificate file location (for instance, on the computer where the Junos XML protocol client application runs)

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

**Related Documentation**

- *Importing SSL Certificates for Junos XML Protocol Support*

## maximum-certificates

**Syntax** maximum-certificates *number*;

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the maximum number of peer digital certificates to be cached.

**Options** ***number***—Maximum number of peer digital certificates to be cached.
**Range:** 64 through 4,294,967,295 peer certificates
**Default:** 1024 peer certificates

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

**Related Documentation**
- *Configuring Digital Certificates for an ES PIC*

## path-length

**Syntax** path-length *certificate-path-length*;

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the digital certificate path length.

**Options** ***certificate-path-length***—Digital certificate path length.
**Range:** 2 through 15 certificates
**Default:** 15 certificates

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

**Related Documentation**
- *Configuring Digital Certificates for an ES PIC*

## secret

**Syntax** secret *secret-data*;

**Hierarchy Level** [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

**Release Information** Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

**Description** Specify a password in encrypted text or plain text format. The secret password always appears in encrypted format.

**Options** ***secret-data***—Password to use; it can include spaces if the character string is enclosed in quotation marks.

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

**Related Documentation**

- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

## security

**Syntax**

```
security {
  authentication-key-chains {
    key-chain key-chain-name {
      key key {
        secret secret-data;
        start-time yyyy-mm-dd.hh:mm:ss;
      }
    }
  certificates {
    cache-size bytes;
    cache-timeout-negative seconds;
    certification-authority ca-profile-name {
      ca-name ca-identity;
      crl file-name;
      encoding (binary | pem);
      enrollment-url url-name;
      file certificate-filename;
      ldap-url url-name;
    }
    enrollment-retry attempts;
    local certificate-filename {
      certificate-key-string;
      load-key-file key-file-name;
    }
    maximum-certificates number;
    path-length certificate-path-length;
  }
  ssh-known-hosts {
    host {
      fetch-from-server host-name;
      load-key-file file-name;
    }
  }
  traceoptions {
    file filename <files number> <size size>;
    flag flag;
    level level;
    no-remote-trace
  }
}
```

**Hierarchy Level** [edit]

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

**Description** Configure security services. Most of the configuration statements do not have default values. If you do not specify an identifier for a statement that does not have a default value, you cannot commit the configuration.

**Required Privilege Level**

**Related Documentation**

## ssh-known-hosts

**Syntax**

```
ssh-known-hosts {
  host host-name {
    fetch-from-server host-name;
    load-key-file file-name;
  }
}
```

**Hierarchy Level** [edit security ssh-known-hosts]

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

**Description** Configure SSH support for known hosts and for administering SSH host key updates.

**Options** **host *host-name***—Hostname of the SSH known host entry. This option has the following suboptions:

- **fetch-from-server *host-name***—Retrieve SSH public host key information from a specified server.
- **load-key-file *filename***—Import SSH host key information from the **/var/tmp/ssh-known-hosts** file.

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

**Related Documentation**

- *Understanding Security Features on the QFabric System*
- *Configuring SSH Host Keys for Secure Copying of Data*

## start-time (Authentication Key Transmission)

**Syntax** start-time (now | *yyyy-mm-dd.hh:mm:ss*);

**Hierarchy Level** [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

**Release Information** Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

**Description** Specify a start time for key transmission. You do not need to specify an end time for the key. If a new key is present with a new start time, the keychain rolls over to the new one. The start time must be unique within the keychain.

**Options** **now**—Start time as the current year, month, day, hour, minute, and second.

***day*days**—Start time as the specified number of days after the current day. For example, if the current day is the 12th and you configure **start-time 2day**, the start time will be on the 14th, exactly two days after the configuration is entered.

***hour*hours**—Start time as the specified number of hours after the current hour. For example, if the current hour is 9:00 and you configure **start-time 3hour**, the start time will be in 12:00, exactly three hours after the configuration is entered.

***minute*minutes**—Start time as the specified number of minutes after the current minute. For example, if the current minute is 27 minutes after the hour and you configure **start-time 5min**, the start time will be in 32 minutes after the hour, exactly five minutes after the configuration is entered.

***month*months**—Start time as the specified number of months after the current month. For example, if the current month is March and you configure **start-time 4month**, the start time will be in July, exactly four months after the configuration is entered.

***second*seconds**—Start time as the specified number of seconds after the current second. For example, if the current second is 10:20:40 and you configure **start-time 10seconds**, the start time will be 10:20:50, exactly 10 seconds after the configuration is entered.

***year*years**—Start time as the specified number of years after the current year. For example, if the current year is 2011 and you configure **start-time 1year**, the start time will be in 2012, exactly one year after the configuration is entered.

***yyyy–mm-dd.hh:mm:ss***—Start time in UTC (Coordinated Universal Time). The start time must be unique within the keychain.

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

**Related Documentation**

- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Static Routes*
- *Example: Configuring BFD Authentication for Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

## traceoptions

**Syntax**

```
traceoptions {
  file filename <files number> <size size>;
  flag all;
  flag certificates;
  flag database;
  flag general;
  flag ike;
  flag parse;
  flag policy-manager;
  flag routing-socket;
  flag timer;
  level
  no-remote-trace
}
```

**Hierarchy Level**

[edit security],
[edit services ipsec-vpn]

Trace options can be configured at either the **[edit security]** or the **[edit services ipsec-vpn]** hierarchy level, but not at both levels.

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Configure security trace options.

To specify more than one trace option, include multiple **flag** statements. Trace option output is recorded in the **/var/log/kmd** file.

NOTE: The **traceoptions**statement is not supported on QFabric systems.

**Options**

**files** ***number***—(Optional) Maximum number of trace files. When a trace file (for example, **kmd**) reaches its maximum size, it is renamed **kmd.0**, then **kmd.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with the **size** option.

**Range:** 2 through 1000 files

**Default:** 0 files

**size** ***size***—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, **kmd**) reaches this size, it is renamed, **kmd.0**, then **kmd.1** and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

**Default:** 1024 KB

**flag *flag***—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace all security events.
- **certificates**—Trace certificate events.
- **database**—Trace database events.
- **general**—Trace general events.
- **ike**—Trace IKE module processing.
- **parse**—Trace configuration processing.
- **policy-manager**—Trace policy manager processing.
- **routing-socket**—Trace routing socket messages.
- **timer**—Trace internal timer events.

**level *level***—(Optional) Set traceoptions level.

- **all**—match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

**no-remote-trace**—(Optional) Disable remote tracing

**Required Privilege Level**

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

**Related Documentation**

- *Configuring Tracing Operations for Security Services*

CHAPTER 7

# Configuration Statements for DHCP Relay

## apply-secondary-as-giaddr

**Syntax** apply-secondary-as-giaddr;

**Hierarchy Level** [edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface]

**Release Information** Statement introduced in Junos OS Release 12.3 for QFX Series switches.

**Description** Configures the interfaces on a switch that are DHCP relay agents to be enabled for smart DHCP relay:

- When you configure this statement directly under the **bootp** statement, it enables smart relay on all the interfaces that are relay agents.
- When you configure this statement under the **interface** statement, it enables smart relay on the specified interface.

Smart relay requires the interfaces to be routed VLAN interfaces or Layer 3 logical interfaces that have multiple IP addresses.

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

**Related Documentation**
- Configuring DHCP and BOOTP Relay on page 26

## bootp

**Syntax**

```
bootp {
  client-response-ttl number;
  description text-description;
  apply-secondary-as-giaddr
  interface (interface-name | interface-group) {
    broadcast number;
    client-response-ttl number;
    description text-description;
    maximum-hop-count number;
    minimum-wait-time seconds;
    no-listen;
    server address ;
    apply-secondary-as-giaddr
  }
  maximum-hop-count number;
  minimum-wait-time seconds;
  server address {
  }
}
```

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

**Release Information** Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description** Configure a router, switch, or interface to act as a Dynamic Host Configuration Protocol (DHCP) or bootstrap protocol (BOOTP) relay agent.

**Options** The remaining statements are explained separately.

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

**Related Documentation**

- Configuring DHCP and BOOTP Relay on page 26

## broadcast

**Syntax** broadcast *number*;

**Hierarchy Level** [edit forwarding-options helpers bootp interface (*interface-name* | *interface-group*)]

**Release Information** Statement introduced in Junos OS Release 11.3 for QFX Series switches.

**Description** If the specified interface is unavailable, broadcast DHCP and BOOTP packets.

**Options** None

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

**Related Documentation**
- Configuring DHCP and BOOTP Relay on page 26

## client-response-ttl

**Syntax** client-response-ttl *number*;

**Hierarchy Level** [edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface (*interface-name* | *interface-group*)]

**Release Information** Statement introduced in Junos OS Release 8.1.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

**Description** Set the IP time-to-live (TTL) value in DHCP response packets sent to a DHCP client.

**Options** ***number***—Decrement amount.
**Default:** None

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

**Related Documentation**
- *Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents*

## description (Forwarding Options)

**Syntax** description *text-description*;

**Hierarchy Level** [edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootpinterface (*interface-name* | *interface-group*)],
[edit forwarding-options helpers domain],
[edit forwarding-options helpers domain interface *interface-name*],
[edit forwarding-options helpers tftp],
[edit forwarding-options helpers tftpinterface *interface-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

**Description** Describe a BOOTP, DHCP, Domain Name System (DNS), or Trivial File Transfer Protocol (TFTP) service, or an interface that is configured for the service.

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

**Related Documentation**

- *Configuring DNS and TFTP Packet Forwarding*
- *Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents*

## interface (BOOTP)

**Syntax**

```
interface (interface-name | interface-group) {
  broadcast;
  client-response-ttl number;
  description text-description;
  maximum-hop-count number;
  minimum-wait-time seconds;
  no-listen;
  server address {
    logical-system logical-system-name <routing-instance [ <default>
      routing-instance-names ]>;
    routing-instance [ <default> routing-instance-names ];
  }
  apply-secondary-as-giaddr (QFX platforms only)
}
```

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

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

**Description** Specify the interface for a DHCP and BOOTP relay agent.

**Options** *interface-group*—Sets a logical interface or group of logical interfaces with a specific DHCP relay configuration.

The remaining statements are explained separately.

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

**Related Documentation**

- *Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents*
- *Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)*

## maximum-hop-count

**Syntax** maximum-hop-count *number*;

**Hierarchy Level** [edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootpinterface (*interface-name* | *interface-group*)]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

**Description** Specify the maximum number of hops allowed.

**Options** ***number***—Maximum number of hops.
**Default:** 4 hops

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

**Related Documentation**
- *Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents*

## minimum-wait-time

**Syntax** minimum-wait-time *seconds*;

**Hierarchy Level** [edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootpinterface (*interface-name* | *interface-group*)]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

**Description** Specify the minimum time allowed.

**Options** ***seconds***—Minimum time.
**Default:** 0 seconds

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

**Related Documentation**
- *Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents*

## no-listen

**Syntax** no-listen;

**Hierarchy Level** [edit forwarding-options helpers bootp interface (*interface-name* | *interface-group*)],
[edit forwarding-options helpers domain interface *interface-name*],
[edit forwarding-options helpers tftp interface *interface-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

**Description** Disable recognition of DNS requests or stop packets from being forwarded on a logical interface, a group of logical interfaces, a router, or a switch.

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

**Related Documentation**
- *Configuring DNS and TFTP Packet Forwarding*
- *Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents*

## server (DHCP and BOOTP Relay Agent)

**Syntax**
```
server address {
  logical-system logical-system-name <routing-instance [ <default>
    routing-instance-names ]>;
  routing-instance [ <default> routing-instance-names ];
}
```

**Hierarchy Level** [edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface (*interface-name* | *interface-group*)]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

**Description** Configure the router or switch to act as a DHCP and BOOTP relay agent.

**Options**
- ***address***—One or more addresses of the server.
- **logical-system *logical-system-name***—(Optional) Logical system of the server.
- **routing-instance *routing-instance-names***—(Optional) Routing instance name that belong to the DHCP or BOOTP relay agent.

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

**Related Documentation**
- *Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents*

PART 3

# Administration

CHAPTER 8

# Monitoring Commands for 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**

- *Layer 2 Port Mirroring Overview*
- Port Mirroring Constraints and Limitations on page 5
- Example: Configuring Port Mirroring for Local Analysis on page 13
- Example: Configuring Port Mirroring for Remote Analysis on page 18

**List of Sample Output** show analyzer on page 72

**Output Fields** Table 4 on page 72 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. |
| **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
```

PART 4

# Troubleshooting

CHAPTER 9

# Troubleshooting Procedures



## Troubleshooting Port Mirroring



### Port Mirroring Constraints and Limitations



#### Local and Remote Port Mirroring

The following constraints and limitations apply to local and remote port mirroring with the QFX Series:

- You can create a total of four port-mirroring configurations on a QFX Series standalone switch.
- 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 QFX3500 device 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.
- 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.
- (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 with the QFX Series:

- 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.
- On the source (monitored) switch, only one interface can be a member of the analyzer VLAN.

### 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.

### 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
- Example: Configuring Port Mirroring for Local Analysis on page 13
- Example: Configuring Port Mirroring for Remote Analysis on page 18