Network Configuration Example

Configuring Multiple Port Mirroring Sessions on EX4200 Switches

Published: 2014-04-09

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

Network Configuration Example Configuring Multiple Port Mirroring Sessions on EX4200 Switches
NCE0116

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

Introduction

Port mirroring is a traffic monitoring tool that is available in Juniper Networks® EX Series Ethernet Switches. Port mirroring sends copies of IPv4 or IPv6 packets from configured input sources to monitoring stations. An analyzer application installed in these monitoring stations can further analyze the traffic and identify problems, if any, in the network by locating abnormal or heavy bandwidth usage from particular stations or applications. To obtain maximum benefit from port mirroring, you must adhere to certain guidelines when you configure port mirroring on a switch. For instance, a configuration guideline for Juniper Networks EX2200, EX3200, EX3300, and EX4200 switches says that you can configure multiple analyzers on a switch, but you can enable only one analyzer session at any point in time.

This document provides a workaround to this guideline so that you can configure multiple active analyzer sessions at any point in time on an EX4200 switch. You can use the same workaround for EX2200, EX3200, and EX3300 switches. This document provides a step-by-step procedure that explains the implementation details.

Port Mirroring Overview

Port mirroring enables you to analyze traffic on your Juniper Networks EX Series switch on a packet level. You might use port mirroring when monitoring switch traffic for such purposes as enforcing policies concerning network usage and file sharing. You might also use port mirroring to identify sources of problems on your network by locating abnormal or heavy bandwidth usage by particular stations or applications.

EX Series switches enable you to configure port mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can analyze the mirrored traffic using a protocol analyzer application running on the remote monitoring station if you are sending mirrored traffic to an analyzer VLAN. Port mirroring supports the copying of the following packets:

- Packets entering or exiting a port
- Packets entering a VLAN on EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, or EX6200 switches
- Packets exiting a VLAN on EX8200 switches

Port mirroring might be needed for traffic analysis on a switch because a switch, unlike a hub, does not broadcast packets to every port on the destination device. The switch sends packets only to the port to which the destination device is connected. You can configure an analyzer to mirror bridged packets (Layer 2 packets). To mirror routed packets (Layer 3 packets), you must configure a firewall filter in which the **family** statement is set to **inet** or **inet6**.

You can configure port mirroring to define the input traffic and the destination to which this input traffic must be mirrored to, in the same port mirroring configuration. The input traffic to be analyzed can be either traffic that enters or traffic that exits an interface or VLAN. The port mirroring configuration enables you to send this traffic to an output

interface, instance, next-hop group, or VLAN. You can define the port mirroring configuration at the **[edit ethernet-switching-options analyzer]** hierarchy level.

Related Documentation

- Configuration Guidelines for Port Mirroring on EX Series Switches on page 2
- Example: Configuring Multiple Port Mirroring Sessions on an EX4200 Switch on page 5

Configuration Guidelines for Port Mirroring on EX Series Switches

When you configure port mirroring on EX Series switches, we recommend that you follow certain guidelines to ensure that you obtain optimum benefit from port mirroring.

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

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

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

This document provides a workaround to the port mirroring configuration guideline that limits the number of port mirroring sessions that can be configured on an EX2200, EX3200, EX3300, or EX4200 switch to one session. While you can configure more than the specified number of analyzers on these switches, you can enable only one analyzer for a session. Table 1 on page 2 summarizes further configuration guidelines for port mirroring on the switches.

Table 1: Configuration Guidelines for Port Mirroring

Guideline	Description	Comment
NOTE: "All other switches" or "All switches" in the **Description** column applies to switch platforms that support port mirroring. For details on platform support, see *EX Series Switch Software Features Overview*.		
Number of VLANs that you can use as ingress input to an analyzer	• 1—EX2200 switches • 256—EX3200, EX4200, EX4500, EX4550, and EX6200 switches • Does not apply—EX8200 switches	–

Table 1: Configuration Guidelines for Port Mirroring *(continued)*

Guideline	Description	Comment
Number of analyzers that you can enable concurrently	• 1—EX2200, EX3200, EX4200, EX3300, and EX6200 switches • 7 port-based or 1 global—EX4500 and EX4550 switches • 7 total, with one based on a VLAN, firewall filter, or LAG and with the remaining 6 based on firewall filters—EX8200 switches NOTE: An analyzer configured using a firewall filter does not support mirroring of packets that are egressing ports.	• You can *configure* more than the specified number of analyzers on the switch, but you can *enable* only the specified number for a session. Use **disable ethernet-switching-options analyzer name** to disable an analyzer. • See the next row entry in this table for the exception to the number of firewall filter-based analyzers allowed on EX4500 and EX4550 switches. • On an EX4550 Virtual Chassis, you can configure only one analyzer if ports in the input and output definitions are on different switches in a Virtual Chassis. To configure multiple analyzers, an entire analyzer session must be configured on the same switch of a Virtual Chassis.
Number of firewall filter-based analyzers that you can configure on EX4500 and EX4550 switches	• 1—EX4500 and EX4550 switches	If you configure multiple analyzers, you cannot attach any of them to a firewall filter.
Types of ports on which you cannot mirror traffic	• Virtual Chassis ports (VCPs) • Management Ethernet ports (**me0** or **vme0**) • Routed VLAN interfaces (RVIs) • VLAN-tagged Layer 3 interfaces	–
If port mirroring is configured to mirror packets exiting or entering 10-Gigabit Ethernet ports, packets are dropped in both network and mirrored traffic when the mirrored packets exceed 60 percent of the 10-Gigabit Ethernet port traffic for egress traffic, and when the mirrored packets exceed 70 percent of the 10-Gigabit Ethernet port traffic for ingress traffic.	• EX8200 switches	–
Traffic directions for which you can specify a ratio	• Ingress only—EX8200 switches • Ingress and egress—All other switches	–
Protocol families that you can include in a firewall filter-based remote analyzer	• Any except **inet** and **inet6**—EX8200 switches • Any—All other switches	You can use **inet** and **inet6** on EX8200 switches in a local analyzer.
Traffic directions that you can configure for mirroring on ports in firewall filter-based configurations	• Ingress only—All switches	–

Table 1: Configuration Guidelines for Port Mirroring *(continued)*

Guideline	Description	Comment
Mirrored packets on tagged interfaces might contain an incorrect VLAN ID or Ethertype.	• Both VLAN ID and Ethertype—EX2200 switches • VLAN ID only—EX3200 and EX4200 switches • Ethertype only—EX4500 and EX4550 switches • Does not apply—EX8200 switches	–
Mirrored packets exiting an interface do not reflect rewritten class-of-service (CoS) DSCP or 802.1p bits.	• All switches	–
The analyzer appends an incorrect 802.1Q (**dot1q**) header to the mirrored packets on the routed traffic or does not mirror any packets on the routed traffic when an egress VLAN that belongs to a routed VLAN interface (RVI) is configured as the input for that analyzer.	• EX8200 switches • Does not apply—All other switches	As a workaround, configure an analyzer that uses each port (member interface) of the VLAN as egress input.
Packets with physical layer errors are not sent to the local or remote analyzer.	• All switches	Packets with these errors are filtered out and thus are not sent to the analyzer.
Port mirroring configuration on a Layer 3 interface with the output configured to a VLAN is not available on EX8200 switches.	• EX8200 switches • Does not apply—All other switches	–
Port mirroring does not support line-rate traffic.	• All switches	Port mirroring for line-rate traffic is done on a best-effort basis.
In an EX8200 Virtual Chassis, if you need to mirror traffic across the virtual chassis, then the output port must be a LAG.	• EX8200 Virtual Chassis • Does not apply—All other switches	In an EX8200 Virtual Chassis: • You can configure a LAG as a monitor port only for native analyzers. • You cannot configure a LAG as a monitor port for analyzers based on firewall filters. • If an analyzer configuration contains a LAG as a monitor port, then you cannot configure VLAN in the input definition of an analyzer.
In standalone EX8200 switches, you can configure LAG in the output definition.	• EX8200 standalone switches • Does not apply—All other switches	In EX8200 standalone switches: • You can configure a LAG as a monitor port on both native and firewall-based analyzers. • If a configuration contains a LAG as a monitor port, then you cannot configure VLAN in the input definition of an analyzer.

Related Documentation

- Example: Configuring Multiple Port Mirroring Sessions on an EX4200 Switch on page 5
- Port Mirroring Overview on page 1

Example: Configuring Multiple Port Mirroring Sessions on an EX4200 Switch

You can configure port mirroring to mirror packets from a single port or from multiple ports to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use port mirroring to copy packets entering or exiting a port, or packets entering or exiting a VLAN.

When you configure port mirroring on an EX Series switch, you must follow certain guidelines discussed in Table 1 on page 2 to obtain maximum benefit from port mirroring. A guideline in this table mentions that you can define multiple port mirroring configurations for an EX2200, EX3200, EX3300, or EX4200 switch, but you can enable only one port mirroring configuration or session at any point in time. If you want to enable multiple port mirroring sessions, follow the workaround provided in this example.

This example describes how to configure multiple port mirroring sessions on an EX4200 switch for local monitoring.

Requirements

This example uses the following hardware and software components:

- One Juniper Networks EX4200 switch
- Junos® operating system (Junos OS) Release 12.1 or later for EX Series switches

Before you configure port mirroring, be sure that you have an understanding of port mirroring concepts. See Understanding Port Mirroring on EX Series Switches for an overview on port mirroring.

Overview

Configuring port mirroring is a way to monitor network traffic by sending a copy of packets entering or exiting a port (or VLAN) on a switch to a local or remote destination for monitoring. Port mirroring enables a network administrator to monitor the performance of the network and to take corrective actions when appropriate. You can configure port mirroring for ingress or egress traffic on a single interface (or multiple interfaces) or on a VLAN (or multiple VLANs).

When you configure port mirroring on EX Series Ethernet Switches, we recommend that you follow certain guidelines to achieve optimum benefit from port mirroring. As per the configuration guidelines mentioned in "Configuration Guidelines for Port Mirroring on EX Series Switches" on page 2, you can enable only one port mirroring configuration at any

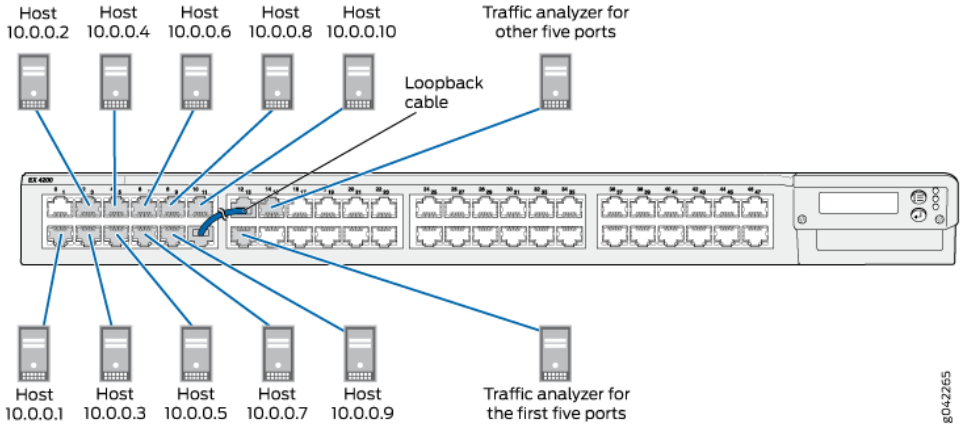
point in time on an EX2200, EX3200, EX3300, or EX4200 switch. You can configure more than the specified number of port mirroring configurations on these switches, but you can enable only one port mirroring session. A workaround to this configuration guideline is to configure many-to-many port mirroring sessions so that multiple port mirroring sessions can be enabled at the same time. This example discusses how to configure and enable two port mirroring sessions on an EX4200 switch. You can use the same workaround for EX2200, EX3200, and EX3300 switches.

Topology

In the topology discussed in this document, 10 hosts are connected to an EX4200 switch, and the IP addresses of those 10 hosts are configured to be within range 10.0.0.1 – 10.0.0.10. The purpose is to configure two port mirroring sessions, which will mirror all IP traffic from 10.0.0.1 – 10.0.0.5 hosts to a monitoring station and from the 10.0.0.6 – 10.0.0.10 hosts to another monitoring station. You can achieve this configuration by connecting a physical-loopback cable and by configuring a firewall filter, which can be used to segregate traffic between the monitoring stations.

Figure 1 on page 6 shows a topology to configure and enable two port mirroring sessions on an EX4200 switch.

Figure 1: Network Topology for Configuring and Enabling Two Port Mirroring Sessions on an EX4200 Switch



This topology shows the following connections and configurations:

- Ports 1–10 are connected to 10 different hosts.
- All hosts are configured to be part of the **vl1** VLAN.
- The ge-0/0/11.0 port is connected to the ge-0/0/12.0 port with an Ethernet cable to form a physical loop.
- An analyzer is configured to accept mirrored IP traffic from the ingressing and egressing interfaces from ge-0/0/1.0 to ge-0/0/10.0. The output port for the analyzer is ge-0/0/12.0.
- Rapid Spanning-Tree Protocol (RSTP) is disabled on ge-0/0/12.0, ge-0/0/13.0, and ge-0/0/14.0.

- The ge-0/0/12.0, ge-0/0/13.0, and ge-0/0/14.0 ports are configured to be a part of a VLAN, and MAC learning is disabled on this VLAN.
- Monitoring stations are connected on the ge-0/0/13.0 and ge-0/0/14.0 ports.
- A firewall filter is applied in the output direction on the ge-0/0/13.0 and ge-0/0/14.0 ports to allow specific mirrored traffic, which is based on the source and destination IP addresses.

Configuration

CLI Quick Configuration

To quickly configure this 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.

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vl1
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members vl1
set interfaces ge-0/0/3 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members vl1
set interfaces ge-0/0/4 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members vl1
set interfaces ge-0/0/5 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members vl1
set interfaces ge-0/0/6 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/6 unit 0 family ethernet-switching vlan members vl1
set interfaces ge-0/0/7 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/7 unit 0 family ethernet-switching vlan members vl1
set interfaces ge-0/0/8 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/8 unit 0 family ethernet-switching vlan members vl1
set interfaces ge-0/0/9 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/9 unit 0 family ethernet-switching vlan members vl1
set interfaces ge-0/0/10 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members vl1
set interfaces ge-0/0/11 unit 0 family ethernet-switching
set ethernet-switching-options analyzer multi-session input ingress interface ge-0/0/1.0
set ethernet-switching-options analyzer multi-session input ingress interface ge-0/0/2.0
set ethernet-switching-options analyzer multi-session input ingress interface ge-0/0/3.0
set ethernet-switching-options analyzer multi-session input ingress interface ge-0/0/4.0
set ethernet-switching-options analyzer multi-session input ingress interface ge-0/0/5.0
set ethernet-switching-options analyzer multi-session input ingress interface ge-0/0/6.0
set ethernet-switching-options analyzer multi-session input ingress interface ge-0/0/7.0
set ethernet-switching-options analyzer multi-session input ingress interface ge-0/0/8.0
set ethernet-switching-options analyzer multi-session input ingress interface ge-0/0/9.0
set ethernet-switching-options analyzer multi-session input ingress interface ge-0/0/10.0
set ethernet-switching-options analyzer multi-session input egress interface ge-0/0/1.0
set ethernet-switching-options analyzer multi-session input egress interface ge-0/0/2.0
set ethernet-switching-options analyzer multi-session input egress interface ge-0/0/3.0
set ethernet-switching-options analyzer multi-session input egress interface ge-0/0/4.0
set ethernet-switching-options analyzer multi-session input egress interface ge-0/0/5.0
set ethernet-switching-options analyzer multi-session input egress interface ge-0/0/6.0
set ethernet-switching-options analyzer multi-session input egress interface ge-0/0/7.0
set ethernet-switching-options analyzer multi-session input egress interface ge-0/0/8.0
set ethernet-switching-options analyzer multi-session input egress interface ge-0/0/9.0
set ethernet-switching-options analyzer multi-session input egress interface ge-0/0/10.0
set ethernet-switching-options analyzer multi-session output interface ge-0/0/11.0
```

```
set protocols rstp interface ge-0/0/12.0 disable
set protocols rstp interface ge-0/0/13.0 disable
set protocols rstp interface ge-0/0/14.0 disable
set vlans mirror vlan-id 100
set vlans mirror no-mac-learning
set interfaces ge-0/0/12 unit 0 family ethernet-switching vlan members mirror
set interfaces ge-0/0/13 unit 0 family ethernet-switching vlan members mirror
set interfaces ge-0/0/14 unit 0 family ethernet-switching vlan members mirror
set firewall family ethernet-switching filter first-5-ff term 10 from source-address 10.0.0.1/32
set firewall family ethernet-switching filter first-5-ff term 10 from source-address 10.0.0.2/32
set firewall family ethernet-switching filter first-5-ff term 10 from source-address 10.0.0.3/32
set firewall family ethernet-switching filter first-5-ff term 10 from source-address 10.0.0.4/32
set firewall family ethernet-switching filter first-5-ff term 10 from source-address 10.0.0.5/32
set firewall family ethernet-switching filter first-5-ff term 10 then accept
set firewall family ethernet-switching filter first-5-ff term 20 from destination-address 10.0.0.1/32
set firewall family ethernet-switching filter first-5-ff term 20 from destination-address 10.0.0.2/32
set firewall family ethernet-switching filter first-5-ff term 20 from destination-address 10.0.0.3/32
set firewall family ethernet-switching filter first-5-ff term 20 from destination-address 10.0.0.4/32
set firewall family ethernet-switching filter first-5-ff term 20 from destination-address 10.0.0.5/32
set firewall family ethernet-switching filter first-5-ff term 20 then accept
set firewall family ethernet-switching filter first-5-ff term default then discard
set interfaces ge-0/0/13 unit 0 family ethernet-switching filter output first-5-ff
set firewall family ethernet-switching filter last-5-ff term 10 from source-address 10.0.0.6/32
set firewall family ethernet-switching filter last-5-ff term 10 from source-address 10.0.0.7/32
set firewall family ethernet-switching filter last-5-ff term 10 from source-address 10.0.0.8/32
set firewall family ethernet-switching filter last-5-ff term 10 from source-address 10.0.0.9/32
set firewall family ethernet-switching filter last-5-ff term 10 from source-address 10.0.0.10/32
set firewall family ethernet-switching filter last-5-ff term 10 then accept
set firewall family ethernet-switching filter last-5-ff term 20 from destination-address 10.0.0.6/32
set firewall family ethernet-switching filter last-5-ff term 20 from destination-address 10.0.0.7/32
set firewall family ethernet-switching filter last-5-ff term 20 from destination-address 10.0.0.8/32
set firewall family ethernet-switching filter last-5-ff term 20 from destination-address 10.0.0.9/32
set firewall family ethernet-switching filter last-5-ff term 20 from destination-address 10.0.0.10/32
set firewall family ethernet-switching filter last-5-ff term 20 then accept
set firewall family ethernet-switching filter last-5-ff term default then discard
set interfaces ge-0/0/14 unit 0 family ethernet-switching filter output last-5-ff
```

Configuring Two Port Mirroring Sessions

Step-by-Step Procedure

The following example requires that you navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure and enable two port mirroring sessions on an EX4200 switch:

1. Configure the port mode for the ge-0/0/1.0 through ge-0/0/10 .0 ports as access ports, and configure those ports to be part of the **vl1** VLAN.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family ethernet-switching port-mode access
user@host# set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vl1
user@host# set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
user@host# set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members vl1
user@host# set interfaces ge-0/0/3 unit 0 family ethernet-switching port-mode access
user@host# set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members vl1
user@host# set interfaces ge-0/0/4 unit 0 family ethernet-switching port-mode access
user@host# set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members vl1
user@host# set interfaces ge-0/0/5 unit 0 family ethernet-switching port-mode access
user@host# set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members vl1
user@host# set interfaces ge-0/0/6 unit 0 family ethernet-switching port-mode access
user@host# set interfaces ge-0/0/6 unit 0 family ethernet-switching vlan members vl1
user@host# set interfaces ge-0/0/7 unit 0 family ethernet-switching port-mode access
user@host# set interfaces ge-0/0/7 unit 0 family ethernet-switching vlan members vl1
user@host# set interfaces ge-0/0/8 unit 0 family ethernet-switching port-mode access
user@host# set interfaces ge-0/0/8 unit 0 family ethernet-switching vlan members vl1
user@host# set interfaces ge-0/0/9 unit 0 family ethernet-switching port-mode access
user@host# set interfaces ge-0/0/9 unit 0 family ethernet-switching vlan members vl1
user@host# set interfaces ge-0/0/10 unit 0 family ethernet-switching port-mode access
user@host# set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members vl1
```

2. Configure an analyzer named **multi-session**, and assign the ge-0/0/11.0 port to be the output port for **multi-session** to mirror traffic for all the ports.

```
[edit]
user@host# set interfaces ge-0/0/11 unit 0 family ethernet-switching
user@host# set ethernet-switching-options analyzer multi-session input ingress interface
ge-0/0/1.0
user@host# set ethernet-switching-options analyzer multi-session input ingress interface
ge-0/0/2.0
user@host# set ethernet-switching-options analyzer multi-session input ingress interface
ge-0/0/3.0
user@host# set ethernet-switching-options analyzer multi-session input ingress interface
ge-0/0/4.0
user@host# set ethernet-switching-options analyzer multi-session input ingress interface
ge-0/0/5.0
user@host# set ethernet-switching-options analyzer multi-session input ingress interface
ge-0/0/6.0
user@host# set ethernet-switching-options analyzer multi-session input ingress interface
ge-0/0/7.0
user@host# set ethernet-switching-options analyzer multi-session input ingress interface
ge-0/0/8.0
user@host# set ethernet-switching-options analyzer multi-session input ingress interface
ge-0/0/9.0
user@host# set ethernet-switching-options analyzer multi-session input ingress interface
ge-0/0/10.0
```

```
user@host# set ethernet-switching-options analyzer multi-session input egress interface
ge-0/0/1.0
user@host# set ethernet-switching-options analyzer multi-session input egress interface
ge-0/0/2.0
user@host# set ethernet-switching-options analyzer multi-session input egress interface
ge-0/0/3.0
user@host# set ethernet-switching-options analyzer multi-session input egress interface
ge-0/0/4.0
user@host# set ethernet-switching-options analyzer multi-session input egress interface
ge-0/0/5.0
user@host# set ethernet-switching-options analyzer multi-session input egress interface
ge-0/0/6.0
user@host# set ethernet-switching-options analyzer multi-session input egress interface
ge-0/0/7.0
user@host# set ethernet-switching-options analyzer multi-session input egress interface
ge-0/0/8.0
user@host# set ethernet-switching-options analyzer multi-session input egress interface
ge-0/0/9.0
user@host# set ethernet-switching-options analyzer multi-session input egress interface
ge-0/0/10.0
user@host# set ethernet-switching-options analyzer multi-session output interface
ge-0/0/11.0
```

3. Define a VLAN named **mirror** and tag it as **100**.

```
[edit]
user@host# set vlans mirror vlan-id 100
```

4. Configure the ge-0/0/12.0, ge-0/0/13.0, and ge-0/0/14.0 ports to be part of the **mirror** VLAN.

```
[edit]
user@host# set vlans mirror vlan-id 100
user@host# set interfaces ge-0/0/12 unit 0 family ethernet-switching vlan members mirror
user@host# set interfaces ge-0/0/13 unit 0 family ethernet-switching vlan members mirror
user@host# set interfaces ge-0/0/14 unit 0 family ethernet-switching vlan members mirror
```

5. Disable MAC learning on the **mirror** VLAN so that the switch acts like a hub and floods all the received mirrored traffic to the ge-0/0/13.0 and ge-0/0/14.0 ports.

```
[edit]
user@host# set vlans mirror no-mac-learning
```

6. Disable RSTP on the ge-0/0/12.0, ge-0/0/13.0, and ge-0/0/14.0 ports because RSTP is enabled by default on all ports in a switch.

```
[edit]
user@host# set protocols rstp interface ge-0/0/12.0 disable
user@host# set protocols rstp interface ge-0/0/13.0 disable
user@host# set protocols rstp interface ge-0/0/14.0 disable
```

7. Create and apply an outgoing firewall filter on the ge-0/0/13.0 port. This port is connected to the first monitoring station that listens to the mirrored traffic for the first five hosts 10.0.0.1 through 10.0.0.5.

```
[edit]
user@host# set firewall family ethernet-switching filter first-5-ff term 10 from
source-address 10.0.0.1/32
user@host# set firewall family ethernet-switching filter first-5-ff term 10 from
source-address 10.0.0.2/32
```



```
user@host# set firewall family ethernet-switching filter first-5-ff term 10 from
source-address 10.0.0.3/32
user@host# set firewall family ethernet-switching filter first-5-ff term 10 from
source-address 10.0.0.4/32
user@host# set firewall family ethernet-switching filter first-5-ff term 10 from
source-address 10.0.0.5/32
user@host# set firewall family ethernet-switching filter first-5-ff term 10 then accept
user@host# set firewall family ethernet-switching filter first-5-ff term 20 from
destination-address 10.0.0.1/32
user@host# set firewall family ethernet-switching filter first-5-ff term 20 from
destination-address 10.0.0.2/32
user@host# set firewall family ethernet-switching filter first-5-ff term 20 from
destination-address 10.0.0.3/32
user@host# set firewall family ethernet-switching filter first-5-ff term 20 from
destination-address 10.0.0.4/32
user@host# set firewall family ethernet-switching filter first-5-ff term 20 from
destination-address 10.0.0.5/32
user@host# set firewall family ethernet-switching filter first-5-ff term 20 then accept
user@host# set firewall family ethernet-switching filter first-5-ff term default then discard
user@host# set interfaces ge-0/0/13 unit 0 family ethernet-switching filter output first-5-ff
```

8. Create and apply an outgoing firewall filter on the ge-0/0/14.0 port. This port is connected to the second monitoring station, which listens to the mirrored traffic for the last five hosts 10.0.0.6 through 10.0.0.10.

```
[edit]
user@host# set firewall family ethernet-switching filter last-5-ff term 10 from
source-address 10.0.0.6/32
user@host# set firewall family ethernet-switching filter last-5-ff term 10 from
source-address 10.0.0.7/32
user@host# set firewall family ethernet-switching filter last-5-ff term 10 from
source-address 10.0.0.8/32
user@host# set firewall family ethernet-switching filter last-5-ff term 10 from
source-address 10.0.0.9/32
user@host# set firewall family ethernet-switching filter last-5-ff term 10 from
source-address 10.0.0.10/32
user@host# set firewall family ethernet-switching filter last-5-ff term 10 then accept
user@host# set firewall family ethernet-switching filter last-5-ff term 20 from
destination-address 10.0.0.6/32
user@host# set firewall family ethernet-switching filter last-5-ff term 20 from
destination-address 10.0.0.7/32
user@host# set firewall family ethernet-switching filter last-5-ff term 20 from
destination-address 10.0.0.8/32
user@host# set firewall family ethernet-switching filter last-5-ff term 20 from
destination-address 10.0.0.9/32
user@host# set firewall family ethernet-switching filter last-5-ff term 20 from
destination-address 10.0.0.10/32
user@host# set firewall family ethernet-switching filter last-5-ff term 20 then accept
user@host# set firewall family ethernet-switching filter last-5-ff term default then discard
user@host# set interfaces ge-0/0/14 unit 0 family ethernet-switching filter output last-5-ff
```

Results

From configuration mode, confirm your configuration by entering the **show firewall**, **show interfaces**, **show ethernet-switching-options**, **show protocols**, and **show vlans** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# show firewall
family ethernet-switching {
    filter first-5-ff {
        term 10 {
            from {
                source-address {
                    10.0.0.1/32;
                    10.0.0.2/32;
                    10.0.0.3/32;
                    10.0.0.4/32;
                    10.0.0.5/32;
                }
                then accept;
            }
        }
        term 20 {
            from {
                destination-address {
                    10.0.0.1/32;
                    10.0.0.2/32;
                    10.0.0.3/32;
                    10.0.0.4/32;
                    10.0.0.5/32;
                }
                then accept;
            }
        }
        term default {
            then discard;
        }
    }
    filter last-5-ff {
        term 10 {
            from {
                source-address {
                    10.0.0.6/32;
                    10.0.0.7/32;
                    10.0.0.8/32;
                    10.0.0.9/32;
                    10.0.0.10/32;
                }
                then accept;
            }
        }
        term 20 {
            from {
                destination-address {
                    10.0.0.6/32;
                    10.0.0.7/32;
                    10.0.0.8/32;
                    10.0.0.9/32;
                    10.0.0.10/32;
                }
                then accept;
            }
```

```
        }
        term default {
          then discard;
        }
      }
    }
}
user@host# show interfaces
ge-0/0/1 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
                members vl1;
            }
        }
    }
}
ge-0/0/2 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
                members vl1;
            }
        }
    }
}
ge-0/0/3 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
                members vl1;
            }
        }
    }
}
ge-0/0/4 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
                members vl1;
            }
        }
    }
}
ge-0/0/5 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
                members vl1;
            }
        }
    }
```

```
}
ge-0/0/6 {
  unit 0 {
    family ethernet-switching {
      port-mode access;
      vlan {
        members vl1;
      }
    }
  }
}
ge-0/0/7 {
  unit 0 {
    family ethernet-switching {
      port-mode access;
      vlan {
        members vl1;
      }
    }
  }
}
ge-0/0/8 {
  unit 0 {
    family ethernet-switching {
      port-mode access;
      vlan {
        members vl1;
      }
    }
  }
}
ge-0/0/9 {
  unit 0 {
    family ethernet-switching {
      port-mode access;
      vlan {
        members vl1;
      }
    }
  }
}
ge-0/0/10 {
  unit 0 {
    family ethernet-switching {
      port-mode access;
      vlan {
        members vl1;
      }
    }
  }
}
ge-0/0/11 {
  unit 0 {
    family ethernet-switching {
    }
  }
```

```
}
ge-0/0/12 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members mirror;
      }
    }
  }
}
ge-0/0/13 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members mirror;
      }
      filter {
        output first-5-ff;
      }
    }
  }
}
ge-0/0/14 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members mirror;
      }
      filter {
        output last-5-ff;
      }
    }
  }
}
user@host# show ethernet-switching-options
analyzer multi-session {
  input {
    ingress {
      interface ge-0/0/1.0;
      interface ge-0/0/2.0;
      interface ge-0/0/3.0;
      interface ge-0/0/4.0;
      interface ge-0/0/5.0;
      interface ge-0/0/6.0;
      interface ge-0/0/7.0;
      interface ge-0/0/8.0;
      interface ge-0/0/9.0;
      interface ge-0/0/10.0;
    }
    egress {
      interface ge-0/0/1.0;
      interface ge-0/0/2.0;
      interface ge-0/0/3.0;
      interface ge-0/0/4.0;
      interface ge-0/0/5.0;
      interface ge-0/0/6.0;
```

```
            interface ge-0/0/7.0;
            interface ge-0/0/8.0;
            interface ge-0/0/9.0;
            interface ge-0/0/10.0;
        }
    }
    output {
        interface {
            ge-0/0/11.0;
        }
    }
}
user@host# show protocols
rstp {
    interface ge-0/0/12.0 {
        disable;
    }
    interface ge-0/0/13.0 {
        disable;
    }
    interface ge-0/0/14.0 {
        disable;
    }
}
user@host# show vlans
mirror {
    vlan-id 100;
    no-mac-learning;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying That the Analyzer Has Been Created Properly on page 16
- Verifying That the Firewall Filter Is Configured Properly to Obtain Traffic from the First Five Hosts on page 17
- Verifying That the First Monitoring Interface Is Configured Properly on page 18
- Verifying That the Firewall Filter Is Configured Properly to Obtain Traffic from the Last Five Hosts on page 19
- Verifying That the Second Monitoring Interface Is Configured Properly on page 20

Verifying That the Analyzer Has Been Created Properly

Purpose Verify that the analyzer has been created on the switch with the appropriate input and output interfaces.

Action Issue the following command:

```
user@host> show analyzer
Analyzer name : multi-session
```

```
Output interface : ge-0/0/11.0
Mirror ratio : 1
Loss priority : Low
Ingress monitored interfaces : ge-0/0/1.0
Ingress monitored interfaces : ge-0/0/2.0
Ingress monitored interfaces : ge-0/0/3.0
Ingress monitored interfaces : ge-0/0/4.0
Ingress monitored interfaces : ge-0/0/5.0
Ingress monitored interfaces : ge-0/0/6.0
Ingress monitored interfaces : ge-0/0/7.0
Ingress monitored interfaces : ge-0/0/8.0
Ingress monitored interfaces : ge-0/0/9.0
Ingress monitored interfaces : ge-0/0/10.0
Egress monitored interfaces : ge-0/0/1.0
Egress monitored interfaces : ge-0/0/2.0
Egress monitored interfaces : ge-0/0/3.0
Egress monitored interfaces : ge-0/0/4.0
Egress monitored interfaces : ge-0/0/5.0
Egress monitored interfaces : ge-0/0/6.0
Egress monitored interfaces : ge-0/0/7.0
Egress monitored interfaces : ge-0/0/8.0
Egress monitored interfaces : ge-0/0/9.0
Egress monitored interfaces : ge-0/0/10.0
```

Meaning The output shows the **multi-session** analyzer has the following configuration:

- Has a mirroring 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).
- Mirrors traffic entering the ge-0/0/1.0 through ge-0/0/10.0 interfaces and traffic exiting the ge-0/0/1.0 through ge-0/0/10.0 interfaces.
- Sends the mirrored traffic to the ge-0/0/10.0 interface.

Verifying That the Firewall Filter Is Configured Properly to Obtain Traffic from the First Five Hosts

Purpose Verify that traffic from the first five hosts is mirrored to the first monitoring interface. You can verify this by checking whether the firewall filter is configured to obtain traffic from the first five hosts and by checking whether this traffic is directed to the first monitoring interface.

Action Verify that the firewall filter configured to obtain traffic from the first five ports (10.0.0.1 through 10.0.0.5) connected to the first five hosts.

```
user@host# show firewall family ethernet-switching filter first-5-ff
term 10 {
    from {
        source-address {
            10.0.0.1/32;
            10.0.0.2/32;
            10.0.0.3/32;
            10.0.0.4/32;
            10.0.0.5/32;
        }
    }
    then accept;
}
term 20 {
    from {
        destination-address {
            10.0.0.1/32;
            10.0.0.2/32;
            10.0.0.3/32;
            10.0.0.4/32;
            10.0.0.5/32;
        }
    }
    then accept;
}
term default {
    then discard;
}
```

Meaning This configuration shows that the **first-5-ff** filter allows traffic originating from and destined to addresses 10.0.0.1 through 10.0.0.5 that are connected to the first five hosts, and that traffic from any other source or destination address is discarded. When this firewall filter is applied to the ge-0/0/13.0 interface, this interface obtains traffic only from those five addresses, even though traffic from other sources or destinations is passing through the interface.

Verifying That the First Monitoring Interface Is Configured Properly

Purpose Verify the configuration for the ge-0/0/13 interface, which is connected to the first monitoring station (that listens to the mirrored traffic for the first five hosts).

Action Verify that the ge-0/0/13.0 interface is configured as expected by using the **show interfaces ge-0/0/13.0** command.

```
user@host# show interfaces ge-0/0/13.0
family ethernet-switching {
    filter {
        output first-5-ff;
    }
}
```

Meaning This output indicates that the **first-5-ff** firewall filter is configured as an egress filter to the ge-0/0/13.0 interface. This means that the ge-0/0/13.0 interface allows traffic from

the first five hosts connected to the switch, as per the configuration in the **first-5-ff** firewall filter configuration. The monitoring station connected to this interface can now monitor traffic from these five hosts.

Verifying That the Firewall Filter Is Configured Properly to Obtain Traffic from the Last Five Hosts

Purpose Verify that traffic from the last five hosts is mirrored to the second monitoring interface by checking whether the firewall filter is configured properly to obtain traffic from the last five hosts connected to the switch and by checking whether this traffic is directed to the second monitoring interface.

Action Verify that the firewall filter is configured to obtain traffic from the last five ports from 10.0.0.6 through 10.0.0.10 that are connected to the last five hosts.

```
user@host# show firewall family ethernet-switching filter last-5-ff
term 10 {
    from {
        source-address {
            10.0.0.6/32;
            10.0.0.7/32;
            10.0.0.8/32;
            10.0.0.9/32;
            10.0.0.10/32;
        }
    }
    then accept;
}
term 20 {
    from {
        destination-address {
            10.0.0.6/32;
            10.0.0.7/32;
            10.0.0.8/32;
            10.0.0.9/32;
            10.0.0.10/32;
        }
    }
    then accept;
}
term default {
    then discard;
}
```

Meaning This configuration shows that the **last-5-ff** filter allows traffic originating from and destined to addresses 10.0.0.6.0 through 10.0.0.10.0 that are connected to the last five hosts, and that traffic from any other source or destination address is discarded. When this firewall filter is applied to the ge-0/0/14.0 interface, this interface receives traffic only from those five addresses even though traffic from other sources or destinations are passing through that interface.

Verifying That the Second Monitoring Interface Is Configured Properly

Purpose Verify the configuration for the ge-0/0/14.0 interface, which is connected to the second monitoring station (that listens to the mirrored traffic for the last five hosts).

Action Verify that the ge-0/0/14.0 interface is configured as expected by using the **show interfaces ge-0/0/14.0** command.

```
user@host# show interfaces ge-0/0/14.0
family ethernet-switching {
    filter {
        output last-5-ff;
    }
}
```

Meaning This output indicates that the **last-5-ff** firewall filter is configured as an egress filter to the ge-0/0/14.0 interface. This means that the ge-0/0/14.0 interface allows traffic from the last five hosts connected to the switch, as per the configuration in the **last-5-ff** firewall filter configuration. The monitoring station connected to this interface can now monitor traffic from these five hosts.

Related Documentation

- Port Mirroring Overview on page 1
- Configuration Guidelines for Port Mirroring on EX Series Switches on page 2