Port Mirroring and Analyzers | Junos OS

Archived: 2026-04-05 19:26:57 UTC

This section describes how port mirroring sends network traffic to analyzer applications.

Understanding Port Mirroring and Analyzers

Port mirroring and analyzers send network traffic to devices running analyzer applications. A port mirror copies Layer 3 IP traffic to an interface. An analyzer copies bridged (Layer 2) packets to an interface. Mirrored traffic can be sourced from single or multiple interfaces. You can use a device attached to a mirror output interface running an analyzer application to perform tasks such as monitoring compliance, enforcing policies, detecting intrusions, monitoring network performance, correlating events, and other problems on the network.

On routers containing an Internet Processor II application-specific integrated circuit (ASIC) or T Series Internet Processor, port mirroring copies Unicast packets entering or exiting a port or entering a VLAN and sends those copies to a local interface for local monitoring or to a VLAN for remote monitoring. The mirrored traffic is received by applications that help you analyze that traffic.

Port mirroring is different from traffic sampling. In traffic sampling, a sampling key based on the IPv4 header is sent to the Routing Engine, where a key is placed in a file or cflowd. Packets based on that key are sent to a cflowd server. In port mirroring, the entire packet is copied and sent out through the specified interface where it can be captured and analyzed in detail.

Use port mirroring to send traffic to devices 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 when you want to perform traffic analysis because a switch normally sends packets only to the port to which the destination device is connected. You probably do not want to send the original packets for analysis before they are forwarded because of the delay that this would cause, so the common alternative is to configure port mirroring to send copies of unicast traffic to another interface and run an analyzer application on a device connected to that interface. .

To configure port mirroring, configure a port-mirroring instance. but don't specify an input for it. Instead, create a firewall filter that specifies the required traffic, and directs it to the instance. Use the `port-mirror` action in a `then` term of the filter for this. The firewall filter must be configured as `family inet`.

Keep performance in mind when configuring port mirroring. Configuring the firewall filter to mirror only the necessary packets reduces the possibility of a performance impact.

You can configure an analyzer statement to define both the input traffic and output traffic in the same analyzer configuration. The traffic to be analyzed can be traffic that enters or exits an interface, or traffic that enters a VLAN. The analyzer configuration enables you to send this traffic to an output interface, instance, or VLAN. You can configure an analyzer at the `[edit forwarding-options analyzer]` hierarchy.

Note:

On EX Series switches, when you disable any interface in a remote port mirroring VLAN, you will need to re-enable the disabled interface and reconfigure the analyzer session to resume port mirroring.

You can use port mirroring to copy:

- All of the packets entering or exiting an interface in any combination. Copies of packets entering some interfaces and packets exiting other interfaces can be sent 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.)
- Any or all packets entering a VLAN. You cannot use port mirroring to copy packets exiting a VLAN.
- A firewall-filtered sample of packets entering a port or VLAN.
- Firewall filters are not supported on egress ports; that is, you cannot specify policy-based sampling of packets exiting an interface
- In VXLAN environments, firewall-filter based port-mirroring is not supported on core- or spine-facing interfaces.

You can configure both traffic sampling and port mirroring, setting an independent sampling rate and run-length for port-mirrored packets. However, if a packet is selected for both traffic sampling and port mirroring, only port mirroring is executed, as it takes precedence. In other words, if you configure an interface to traffic sample every packet input to the interface and port mirroring also selects that packet to be copied and sent to the destination port, only the port mirroring process is executed. Traffic sampled packets that are not selected for port mirroring continue to be sampled and forwarded to the cflowd server.

Port Mirroring and Analyzer Terms and Definitions

The following tables provide terms and definitions for the port mirroring and analyzer documentation.

Table 1: Terminology

Term	Definition

Analyzer	For EX2300, EX3400, or EX4300 switches, in a mirroring configuration (analyzer) on an the analyzer includes: • The name of the analyzer • Source (input) ports or VLAN (optional)
Analyzer instance	Port-mirroring configuration that includes a name, source interfaces or source VLAN, and a destination for mirrored packets (either a local interface or a VLAN).
Analyzer output interface (also known as monitor port)	Interface to which mirrored traffic is sent and to which a protocol analyzer application is connected. For EX2300, EX3400, and EX4300 Switches, Interfaces used as output for an analyzer must be configured as family ethernet-switching. In addition, the following limitations for analyzer output interfaces apply: • Cannot also be a source port. • Cannot be used for switching. • Do not participate in Layer 2 protocols, such as Spanning Tree Protocol (STP), when part of a port mirroring configuration. • If the bandwidth of the analyzer output interface is not sufficient to handle the traffic from the source ports, overflow packets are dropped.
Analyzer VLAN (also known as monitor VLAN)	VLAN to which mirrored traffic is sent. The mirrored traffic can be used by a protocol analyzer application. The member interfaces in the monitor VLAN are spread across the switches in your network.
Bridge-domain-based analyzer	An analyzer session configured to use bridge domains for input, output or both.
Default analyzer	An analyzer with default mirroring parameters. By default, the mirroring rate is 1 and the maximum packet length is the length of the complete packet.
Global port mirror	A port mirroring configuration that does not have an instance name. The firewall filter action port-mirror will be the action for the firewall filter configuration.
Input interface (also known as mirrored or	An interface that copies traffic to the mirror interface. This traffic can be entering or exiting (ingress or egress) the interface. A mirrored input interface cannot be used as an output interface to the analyzer device.

monitored interface)	
LAG-based analyzer	An analyzer that has a link aggregation group (LAG) specified as the input (ingress) interface in the analyzer configuration.
Local port mirroring	A port-mirroring configuration where the mirrored packets are copied to an interface on the same switch.
Monitoring station	A computer running a protocol analyzer application.
Next-hop based analyzer	An analyzer configuration that uses the next-hop group as the output to an analyzer.
Native analyzer session	An analyzer session that has both input and output definitions in its analyzer configuration.
Policy-based mirroring	Mirroring of packets that match a firewall filter term. The action `analyzer analyzer-name` is used in the firewall filter to send specified packets to the analyzer.
Port-based analyzer	An analyzer session whose configuration defines interfaces for both input and output.
Port mirroring instance	A port-mirroring configuration that does not specify an input source; it specifies only an output destination. A firewall filter configuration must be defined for the input source. A firewall filter configuration must be defined to mirror packets that match the match conditions defined in the firewall filter term. The action item port-mirror-instance instance-name in the firewall filter configuration is used to send packets to the analyzer and these packets form the input source. Use the `port-mirror-instance instance-name` action in the firewall filter configuration to send packets to the port mirror. Note: Port mirroring instance is not supported on NFX150 devices.
Protocol analyzer application	An application used to examine packets transmitted across a network segment. Also commonly called network analyzer, packet sniffer, or probe.
Output interface (also known as the monitor interface)	The interface to where the copies of packets are sent and to which a device running an analyzer is connected. The following limitations apply to an output interface (the target mirror interface):

	• Cannot also be a source port. • Cannot be used for switching. • Cannot be an aggregated Ethernet interface (LAG). • Cannot participate in Layer 2 protocols, such as Spanning Tree Protocol (STP). • Existing VLAN associations are lost when port mirroring is applied to the interface. • Packets are dropped if the capacity of the output interface is insufficient to handle the traffic from the mirrored source ports.
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: • Mirrored packets are GRE-encapsulated. The analyzer application must be able to de-encapsulate GRE-encapsulated packets or the GRE-encapsulated packets must be de-encapsulated before reaching the analyzer application. (You can use a network sniffer to de-encapsulate the packets.) • The output IP address cannot be in the same subnetwork as any of the switch management interfaces. • If you create virtual routing instances and an analyzer configuration that includes an output IP address, the output IP address belongs to the default virtual routing instance (inet.0 routing table).
Output VLAN (also known as monitor or analyzer VLAN)	VLAN to where copies of the packets are sent and to where a device running an analyzer is connected. The analyzer VLAN can span multiple switches. The following limitations apply to an output VLAN: • Cannot be a private VLAN or VLAN range. • Cannot be shared by multiple `analyzer` statements. • Cannot be a member of any other VLAN. • Cannot be an aggregated Ethernet interface (LAG). • On some switches, only one interface can be a member of the analyzer VLAN. This limitation does not apply on the QFX10000 switch. When *ingress* traffic is

	mirrored, multiple QFX10000 interfaces can belong to the output VLAN and traffic is mirrored from all of those interfaces. If *egress* traffic is mirrored on a QFX10000 switch, only one interface can be a member of the analyzer VLAN.
Remote port mirroring	Functions the same as local port mirroring, except that the mirrored traffic is not copied to a local analyzer port but is flooded to an analyzer VLAN that you create specifically for the purpose of receiving mirrored traffic. You cannot send mirrored packets to a remote IP address on a QFabric system.
VLAN-based analyzer	An analyzer session whose configuration uses VLANs for both input and output or for either input or output.

Instance Types

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

- Analyzer instance—Specify the input and output for the instance. This instance type is useful for ensuring that all traffic transiting an interface or entering a VLAN is mirrored and sent to the analyzer.
- Port-mirroring instance—You create a firewall filter that identifies the desired traffic and copies it to the mirror port. You do not specify an input for this instance type. This instance type is useful for controlling the types of traffic that are mirrored. You can direct traffic to it in the following ways:
  - Specify the name of the port-mirroring instance in the firewall filter by using the `port-mirror-instance *instance-name*` action when there are multiple port-mirroring instances defined.
  - Send the mirrored packets to the output interface defined in the instance by using the `port-mirror` action when there is only one port-mirroring instance defined.

For QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, EX4600 and EX4650 switches, the following port mirroring guidelines apply:

- A maximum of four port mirroring instances, or four analyzer sessions, can be configured at the same time. In other words, you cannot configure four port mirroring instances *and* four analyzer sessions together.
- If there are no port mirroring instances, (that is, only analyzer sessions are configured), then you can enable up to three analyzer sessions for ingress and egress mirroring. The remaining analyzer session must be used for ingress mirroring only.
- If you have only one port mirroring instance configured, then of the remaining instances, you can configure up to three analyzers for ingress mirroring, and two analyzers for egress mirroring.
- If you have two port mirroring instance configured, then of the remaining instances, you can configure up to two analyzers for ingress mirroring, and one analyzer for egress mirroring.
- If you have three port mirroring instance configured, then the remaining instance can only be configured as an analyzer (for either ingress or egress mirroring),

Port Mirroring and STP

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

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

Constraints and Limitations

The following constraints and limitations apply to port mirroring:

Mirroring only the packets required for analysis reduces the possibility of reducing overall performance. If you mirror traffic from multiple ports, the mirrored traffic might exceed the capacity of the output interface. The overflow packets are dropped. We recommend that you limit the amount of mirrored traffic by selecting specific interfaces and avoid using the `all` keyword. You can also limit the amount of mirrored traffic by using a *firewall filter* to send specific traffic to the port mirroring instance.

- You can create a total of four port-mirroring configurations.
- On EX9200 switches, port mirroring is **not** supported on EX9200-15C line cards.
- Each Node group in a QFabric system is subject to the following constraints:
    - Up to four of the configurations can be used for local port mirroring.
    - Up to three of the configurations can be used for remote port mirroring.
- Regardless of whether you are configuring a standalone switch or a Node group:
    - There can be no more than two configurations that mirror ingress traffic. If you configure a firewall filter to send mirrored traffic to a port, this counts as an ingress mirroring configuration for the switch or Node group to which the filter is applied.
    - There can be no more than two configurations that mirror egress traffic.
    - On QFabric systems, there is no system-wide limit on the total number of mirror sessions.
- You can configure only one type of output in one port-mirroring configuration to complete a `set analyzer` *`name`* `output` statement:
    - `interface`
    - `ip-address`
    - `vlan`

- Configure mirroring in an analyzer (with `set forwarding-options analyzer`) on only one logical interface for the same physical interface. If you try to configure mirroring on multiple logical interfaces configured on a physical interface, only the first logical interface is successfully configured; the remaining logical interfaces return configuration errors.
- If you mirror egress packets, do not configure more than 2000 VLANs on a standalone switch or QFabric system. If you do, some VLAN packets might contain incorrect VLAN IDs. This applies to any VLAN packets, not just the mirrored copies.
- The `ratio` and `loss-priority` options are not supported.
- Packets with physical layer errors 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 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
  - Integrated routing and bridging (IRB) interfaces (also known as routed VLAN interfaces or RVIs)
- In a port-mirroring instance, you cannot configure an `inet` or `inet6` interface as the output interface. The following switches do not support the `set forwarding-options port-mirroring instance <*instance-name*> family inet output interface <*interface-name*>` configuration:

Table 2: Switches Not Supporting `family inet/inet6` as Output Interface

EX Switches	**QFX Switches**
EX2300	QFX3500
EX3400	QFX5100
EX4100	QFX5110
EX4300	QFX5120
EX4400	QFX5130

EX Switches	QFX Switches
EX4600	QFX5200
EX4650	QFX5210
	QFX5220
	QFX5700

- An aggregated Ethernet interface cannot be an output interface if the input is a VLAN or if traffic is sent to the analyzer by using a firewall filter.
- When mirrored packets are sent out of an output interface, they are not modified for any changes that might be applied to the original packets 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 will 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 will have the correct VLAN IDs (as long as you do not configure more than 2000 VLANs on the QFabric system).
- True egress mirroring is defined as mirroring the exact number of copies and the exact packet modifications that went out the egress port. Because the processors on QFX5100 and EX4600 switches implement egress mirroring in the ingress pipeline, those switches do not provide accurate egress packet modifications, so egress mirrored traffic can carry incorrect VLAN tags that differ from the tags in the original traffic.
- If you configure a port-mirroring instance to mirror traffic exiting an interface that performs VLAN encapsulation, the source and destination MAC addresses of the mirrored packets are not the same as those of the original packets.
- Mirroring on member interfaces of a LAG is not supported.

- Egress VLAN mirroring is not supported.

The following constraints and limitations apply to remote port mirroring:

- If you configure an output IP address, that address cannot be in the same subnetwork as any of the switch management interfaces.
- If you create virtual routing instances and you create an analyzer configuration that includes an output IP address, the output IP 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 sessions or port-mirror instances.
- An output VLAN interface cannot be a member of any other VLAN.
- An output VLAN interface cannot be an aggregated Ethernet interface.
- If the output VLAN has more than one member interface, then traffic is mirrored only to the first member of the VLAN, and other members of the same VLAN do not carry any mirrored traffic.
- For remote port mirroring to an IP address (GRE encapsulation), if you configure more than one analyzer session or port-mirror instance, and the IP addresses of the analyzers or port-mirror instance are reachable through the same interface, then only one analyzer session or port-mirror instance will be configured.
- The number of possible output interfaces in remote port mirroring varies among the switches in the QFX5K line:
    - QFX5110, QFX5120, QFX5210—Support a maximum of 4 output interfaces
    - QFX5100 and QFX5200—Support a maximum of 3 output interfaces.
- Whenever any member in a remote port mirroring VLAN is removed from that VLAN, reconfigure the analyzer session for that VLAN.

Constraints and Limitations for QFX5100 and QFX5200 Switches

The following considerations apply to port mirroring on QFX5100 and QFX5200 switches:

- When configuring mirroring with output to IP address, the destination IP address should be reachable, and ARP must be resolved.
- ECMP (Equal Cost Multiple Path) load balancing is not supported for mirrored destinations.
- The number of output interfaces in remote port mirroring (RSPAN) varies. For QFX5110, QFX5120, and QFX5210, switches the maximum is four output interfaces. For QFX5100 and QFX5200 switches, the maximum is three.

- When specifying a link aggregation group (LAG) as the mirroring output interface, a maximum of eight interfaces are mirrored.
- The mirroring input can be a LAG, a physical interface with any unit (such as ae0.101 or xe-0/0/0.100), or a sub-interface. In any case, all the traffic on the LAG or physical interface is mirrored.
- You cannot set up an independent mirroring instance on a member interface of a LAG.
- An output interface that is included in one mirroring instance cannot also be used in another mirroring instance.
- In a port-mirroring instance, dropped packets in the egress pipeline of forwarding-path are never-the-less mirrored to the destination. This is because the mirroring action occurs at the ingress pipeline, before the drop action.
- In a port-mirroring instance, only one mirror output destination can be specified.
- Output mirror destinations that are configured across multiple port-mirroring or analyzer instances must all be unique.
- For ERSPAN IPv6 addresses, egress mirroring is not supported when the output to the analyzer/port-mirroring is a remote IPv6 address. Egress mirror is not supported.
- For local mirroring, the output interface must be `family ethernet-switching`, with or without VLAN (that is, not a Layer 3 interface).
- When configuring a port-mirroring or analyzer instance in a service provider environment, use the VLAN name rather than the VLAN ID.

Port Mirroring on QFX5230-64CD and QFX5240 Switches

This section of the document describes a port-mirroring configuration detail that is specific to QFX5230-64CD and QFX5240 switches. For general information about port mirroring on switches, see earlier sections in this *Port Mirroring and Analyzers* document.

Use the values given in the following list to configure the number of mirroring sessions on the QFX5230-64CD and QFX5240 switches. These are maximum configuration values for three types of mirroring sessions—ingress mirrors, egress mirrors, and port-mirroring instances. The values are tuned to make the best use of the total number of available mirroring sessions:

- On QFX5230-64CD:
    - Total mirror sessions available: 8
    - Max. ingress mirror: 5
    - Max. egress mirror: 3

    - Max. port-mirror: 3

  For example, if you configure 3 port-mirroring instances, you then have a maximum of 5 sessions to split between ingress mirrors and egress mirrors.

- On QFX5240:

    - Total mirror sessions available: 7
    - Max. ingress mirror: 4
    - Max. egress mirror: 3
    - Max. port-mirror: 3

  For example, if you configure 1 port-mirroring instance, you then have a maximum of 6 sessions to split between ingress mirrors and egress mirrors.

Port Mirroring on QFX10000 Series Switches

The following list describes constraints and limitations that apply specifically to QFX10000 Series switches. For general information about port mirroring on switches, see earlier sections in this *Port Mirroring and Analyzers* document that do not specifically call out other platform names in the section title.

- Only ingress global port mirroring is supported. You can configure global port mirroring with input parameters such as `rate` , `run-length` , and `maximum-packet-length` . Egress global port mirroring is not supported.
- Port mirroring instances are supported only for remote port mirroring. Port mirroring **global** instances are supported for local mirroring.
- Local port mirroring is supported on these firewall filter families only: `inet` and `inet6` .
- Local port mirroring is not supported on firewall filter families `any` or `ccc` .

Port Mirroring on QFabric

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

- You can create a total of four port-mirroring configurations.
- Each Node group in a QFabric system is subject to the following constraints:

    - Up to four of the configurations can be used for local port mirroring.
    - Up to three of the configurations can be used for remote port mirroring.

- Regardless of whether you are configuring a standalone switch or a Node group:

    - There can be no more than two configurations that mirror ingress traffic. If you configure a firewall filter to send mirrored traffic to a port—that is, you use the `analyzer` action modifier in a filter term—this counts as an ingress mirroring configuration for the switch or Node group to which the filter is applied.
    - There can be no more than two configurations that mirror egress traffic.
    - On QFabric systems, there is no system-wide limit on the total number of mirror sessions.
- You can configure only one type of output in one port-mirroring configuration to complete a `set analyzer` *`name`* `output` statement:
    - `interface`
    - `ip-address`
    - `vlan`
- Configure mirroring in an analyzer (with `set forwarding-options analyzer`) on only one logical interface for the same physical interface. If you try to configure mirroring on multiple logical interfaces configured on a physical interface, only the first logical interface is successfully configured; the remaining logical interfaces return configuration errors.
- If you mirror egress packets, do not configure more than 2000 VLANs on a QFX Series switch. If you do, some VLAN packets might contain incorrect VLAN IDs. This applies to any VLAN packets, not just the mirrored copies.
- The `ratio` and `loss-priority` options are not supported.
- Packets with physical layer errors 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 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
    - Integrated routing and bridging (IRB) interfaces (also known as routed VLAN interfaces or RVIs)
- An aggregated Ethernet interface cannot be an output interface if the input is a VLAN or if traffic is sent to the analyzer by using a firewall filter.
- When mirrored packets are sent out of an output interface, they are not modified for any changes that might be applied to the original packets 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 will 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 will have the correct VLAN IDs (as long as you do not configure more than 2000 VLANs on the QFabric system).
- True egress mirroring is defined as mirroring the exact number of copies and the exact packet modifications that went out the egress port. Because the processors on QFX5xxx (including QFX5100, QFX5110, QFX5120, QFX5200, and QFX5210) and EX4600 (including EX4600 and EX4650) switches implement egress mirroring in the ingress pipeline, those switches do not provide accurate egress packet modifications, so egress mirrored traffic can carry incorrect VLAN tags that differ from the tags in the original traffic.
- If you configure a port-mirroring instance to mirror traffic exiting an interface that performs VLAN encapsulation, the source and destination MAC addresses of the mirrored packets are not the same as those of the original packets.
- Mirroring on member interfaces of a LAG is not supported.
- Egress VLAN mirroring is not supported.

Port Mirroring on OCX Series Switches

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

- You can create a total of four port-mirroring configurations. There can be no more than two configurations that mirror ingress or egress traffic.
- If you use sFlow monitoring to sample traffic, it does not sample the mirror copies when they exit the output interface.
- You can create only one port-mirroring session.
- You cannot mirror packets exiting or entering the following ports:
  - Dedicated Virtual Chassis interfaces
  - Management interfaces (me0 or vme0)
  - Fibre Channel interfaces

    - Routed VLAN interfaces or IRB interfaces

- An aggregated Ethernet interface cannot be an output interface.
- Do not include an 802.1Q subinterface that has a unit number other than 0 in a port mirroring configuration. Port mirroring does not work with subinterfaces if their unit number is not 0. (You configure 802.1Q subinterfaces by 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.

Port Mirroring on EX2300, EX3400, and EX4300 Switches

Mirroring might be needed for traffic analysis on a switch because a switch, unlike a hub, does not broadcast packets to every port on the destination device. The switch sends packets only to the port to which the destination device is connected.

- Overview
- Configuration Guidelines for Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches

Overview

Junos OS running on EX2300, EX3400, and EX4300 Series switches supports the Enhanced Layer 2 Software (ELS) configurations that facilitate analyzing traffic on these switches at the packet level.

You use port mirroring to copy packets to a local interface for local monitoring or to a VLAN for remote monitoring. You can use analyzers to enforce policies concerning network usage and file sharing, and to identify sources of problems on your network by locating abnormal or heavy bandwidth usage by specific stations or applications.

Port mirroring is configured at the `[edit forwarding-options port-mirroring]` hierarchy level. To mirror routed (Layer 3) packets, you can use the port mirroring configuration in which the `family` statement is set to `inet` or `inet6`.

You can use port mirroring to copy these packets:

- `Packets entering or exiting a port`—You can mirror the packets in any combination of packets entering or exiting ports up to 256 ports.

  In other words, you can send copies of the packets entering some ports and the packets exiting other ports to the same local analyzer port or analyzer VLAN.

- `Packets entering a VLAN`—You can mirror the packets entering a VLAN to either a local analyzer port or to an analyzer VLAN. You can configure up to 256 VLANs, including a VLAN range and PVLANs, as ingress input to an analyzer.
- `Policy-based sample packets`—You can mirror a policy-based sample of packets that are entering a port or a VLAN. You configure a *firewall filter* to establish a policy to select the packets to be mirrored and send the sample to a port-mirroring instance or to an analyzer VLAN.

You can configure port mirroring on the switch to send copies of Unicast traffic to an output destination such as an interface, a routing-instance, or a VLAN. Then, you can analyze the mirrored traffic by using a protocol analyzer application. The protocol analyzer application can run either on a computer connected to the analyzer output interface or on a remote monitoring station. For the input traffic, you can configure a firewall filter term to specify whether port mirroring must be applied to all packets at the interface to which the firewall filter is applied. You can apply a firewall filter configured with the action `port-mirror` or `port-mirror-instance name` to the input or output logical interfaces (including aggregated Ethernet logical interfaces), to traffic forwarded or flooded to a VLAN, or traffic forwarded or flooded to a VPLS routing instance. EX2300, EX3400, and EX4300 switches support port mirroring of VPLS (`family ethernet-switching` or `family vpls`) traffic and VPN traffic with `family ccc` in a Layer 2 environment.

Within a firewall filter term, you can specify the port-mirroring properties under the `then` statement in the following ways:

- Implicitly reference the port-mirroring properties in effect on the port.
- Explicitly reference a particular named instance of port mirroring.

Configuration Guidelines for Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches

When you configure port mirroring we recommend that you follow certain guidelines to ensure that you obtain optimum benefit from mirroring. Additionally, we recommend that you disable mirroring when you are not using it and that you select specific interfaces for which packets must be mirrored (that is, select specific interfaces as input to the analyzer) in preference to using the `all` keyword option that enables mirroring on all interfaces and can impact overall performance. Mirroring only the necessary packets reduces any potential performance impact.

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

You can configure an analyzer at the `[edit forwarding-options analyzer]` hierarchy.

Note:

True egress mirroring is defined as mirroring the exact number of copies and the exact packet modifications that went out the egress switched port. Because the processor on EX2300 and EX3400 switches implements egress

mirroring in the ingress pipeline, those switches do not provide accurate egress packet modifications, so egress mirrored traffic can carry VLAN tags that differ from the tags in the original traffic.

Table 3 summarizes additional configuration guidelines for mirroring on EX2300, EX3400, and EX4300 switches.

Table 3: Configuration Guidelines for Port Mirroring and Analyzers on EX2300, EX3400, and EX4300 Switches

Guideline	Value or Support Information	Comment
Number of VLANs that you can use as ingress input to an analyzer.	256	
Number of port-mirroring sessions and analyzers that you can enable concurrently.	4	You can configure a total of four sessions and you can enable only one of the following at any point in time: • A maximum of four port-mirroring sessions (including the global port-mirroring session). • A maximum of four analyzer sessions. • A combination of port-mirroring and analyzer sessions, and the total of this combination must be four. You can configure more than the specified number of port-mirroring instances or analyzers on the switch, but you can enable only the specified number for a session.
Types of ports on which you cannot mirror traffic.	• *Virtual Chassis* ports (VCPs) • Management Ethernet ports (me0 or vme0) • Integrated routing and bridging (IRB)	

Guideline	Value or Support Information	Comment
	interfaces; also known as routed VLAN interfaces (RVIs). • VLAN-tagged Layer 3 interfaces	
Protocol families that you can include in a port-mirroring configuration for remote traffic.	`any`	
Traffic directions that you can configure for mirroring on ports in firewall-filter–based configurations.	Ingress and egress	
Mirrored packets exiting an interface that reflect rewritten class-of-service (CoS) DSCP or 802.1p bits.	Applicable	
Packets with physical layer errors.	Applicable	Packets with these errors are filtered out and thus are not sent to the analyzer.
Port mirroring does not support line-rate traffic.	Applicable	Port mirroring for line-rate traffic is done on a best-effort basis.
Mirroring of packets egressing a VLAN.	Not supported	
Port-mirroring or analyzer output on a LAG interface.	Supported	

Guideline	Value or Support Information	Comment
Maximum number of child members on a port-mirroring or analyzer output LAG interface.	8	
Maximum number of interfaces in a remote port-mirroring or analyzer VLAN.	1	
Egress mirroring of host-generated control packets.	Not Supported	
Configuring Layer 3 logical interfaces in the `input` stanza of an analyzer.	Not supported	This functionality can be achieved by configuring port mirroring.
The analyzer input and output stanzas containing members of the same VLAN or the VLAN itself must be avoided.	Applicable	

Port Mirroring on ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200, and EX8200 Series Switches

Juniper Networks Junos operating system (Junos OS) running on ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200 or EX8200 Series switches does not support Enhanced Layer 2 Software (ELS) configurations. As such, Junos OS does not include the `port-mirroring` statement found at the `edit forwarding-options` level of the hierarchy of other Junos OS packages, or the `port-mirror` action in firewall filter terms.

You can use *port mirroring* to facilitate analyzing traffic on your Juniper Networks EX Series Ethernet Switch on a packet level. You might use port mirroring as part of monitoring switch traffic for such purposes as enforcing policies concerning network usage and file sharing and for identifying sources of problems on your network by locating abnormal or heavy bandwidth usage by particular stations or applications.

You can use port mirroring to copy these packets to a local interface or to a VLAN:

- Packets entering or exiting a port
- You can send copies of the packets entering some ports and the packets exiting other ports to the same local analyzer port or analyzer VLAN.
- Packets entering a VLAN on ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, or EX6200 switches
- Packets exiting a VLAN on EX8200 switches

Overview

Port mirroring is used 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 configure port mirroring on the switch to send copies of Unicast traffic to either a local analyzer port or an analyzer VLAN. Then you can analyze the mirrored traffic by using a protocol analyzer. The protocol analyzer can run either on a computer connected to the analyzer output interface or on a remote monitoring station.

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

- `Packets entering or exiting a port`—You can mirror the packets in any combination of packets entering or exiting ports up to 256 ports.

  In other words, you can send copies of the packets entering some ports and the packets exiting other ports to the same local analyzer port or analyzer VLAN.

- `Packets entering a VLAN on an ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, or EX6200 switch`—You can mirror the packets entering a VLAN on an analyzer VLAN. On EX3200, EX4200, EX4500, and EX4550 switches, you can configure multiple VLANs (up to 256 VLANs), including a VLAN range and PVLANs, as ingress input to an analyzer.

- `Packets exiting a VLAN on an EX8200 switch`—You can mirror the packets exiting a VLAN on an EX8200 switch to either a local analyzer port or to an analyzer VLAN. You can configure multiple VLANs (up to 256 VLANs), including a VLAN range and PVLANs, as egress input to an analyzer.

- `Statistical samples`—You can mirror a statistical sample of packets that are:

  - Entering or exiting a port

    - Entering a VLAN on an ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, or EX6200 switch
    - Exiting a VLAN on an EX8200 switch

  You specify the sample number of packets by setting the ratio. You can send the sample to either a local analyzer port or to an analyzer VLAN.

- `Policy-based sample`—You can mirror a policy-based sample of packets that are entering a port or a VLAN. You configure a *firewall filter* to establish a policy to select the packets to be mirrored. You can send the sample to a local analyzer port or to an analyzer VLAN.

Configuration Guidelines for ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200, and EX8200 Series Switches

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

With local port 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.

Note:

On ACX5448 routers, under the [`edit forwarding-options analyzer an input egress`] hierarchy level, analyser input must be configured only on .0 logical interfaces for ingress and egress interfaces. If you configure logical interfaces other than .0, then an error is shown during commit. The following is a sample commit error shown when the analyzer input is configured .100 logical interface:

content_copy zoom_out_map

```
[edit forwarding-options analyzer an input egress]
  'interface ge-0/0/12.100'
    Analyzer input can only be on .0 interfaces
error: configuration check-out failed
```

Note: “All other switches” or “All switches” in the description apply to all switch platforms that support port mirroring. For details on platform support, see Feature Explorer.

Table 4: Configuration Guidelines

Guideline	Description	Comment
Number of VLANs that you can use as ingress input to an analyzer	• 16 Ingress or 8 Ingress and 8 Egress—ACX7024 devices 1—EX2200 switches • 256—EX3200, EX4200, EX4500, EX4550, and EX6200 switches • Does not apply—EX8200 switches	
Number of analyzers that you can enable concurrently (applies to both standalone switches and to Virtual Chassis)	• 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.

Guideline	Description	Comment
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 10-Gigabit Ethernet ports on EX8200 switches, packets are dropped in both network and mirrored traffic when the mirrored packets exceed 60 percent of the 10-Gigabit Ethernet port 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	You can use `inet` and `inet6` on EX8200 switches in a local analyzer.

Guideline	Description	Comment
	• Any—All other switches	
Traffic directions that you can configure for mirroring on ports in firewall-filter–based configurations	• Ingress only—All switches	
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	

Guideline	Description	Comment
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, to mirror traffic across the Virtual Chassis, the output port must be a LAG.	• EX8200 Virtual Chassis • Does not apply—All other switches	In an EX8200 Virtual Chassis: • You can configure LAG as a monitor port only for native analyzers. • You cannot configure LAG as a monitor port for analyzers based on firewall filters. • If an analyzer configuration contains LAG as a monitor port, then you cannot configure

Guideline	Description	Comment
		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 LAG as a monitor port, then you cannot configure VLAN in the input definition of an analyzer.

Port Mirroring on SRX Series Firewalls

Port mirroring copies packets entering or exiting a port and sends the copies to a local interface for monitoring. Port mirroring is used 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. </para><para>Port mirroring is used to send a copy of all the packets or only the sampled packets seen on a port to a network monitoring connection. You can mirror the packets either on the incoming port (ingress port mirroring) or the outgoing port (egress port mirroring).

Port mirroring is supported only on the SRX Series Firewalls with the following I/O cards:

- SRX1K-SYSIO-GE
- SRX1K-SYSIO-XGE
- SRX3K-SFB-12GE
- SRX3K-2XGE-XFP
- SRX5K-FPC-IOC Flex I/O

On SRX Series Firewalls, all packets passing through the `mirrored` port are copied and sent to the specified `mirror-to` port. These ports must be on the same Broadcom chipset in the I/O cards.

On SRX Series Firewalls, port mirroring works on physical interfaces only.

Understanding Layer 2 Port Mirroring

On routing platforms and switches that contain an Internet Processor II ASIC, you can send a copy of any incoming packet from the routing platform or switch to an external host address or a packet analyzer for analysis. This is known as *port mirroring*.

In Junos OS Release 9.3 and later, Juniper Networks MX Series 5G Universal Routing Platforms in a Layer 2 environment support *port mirroring* for Layer 2 bridging traffic and virtual private LAN service (VPLS) traffic.

In Junos OS Release 9.4 and later, MX Series routers in a Layer 2 environment support port mirroring for Layer 2 VPN traffic over a circuit cross-connect (CCC) that transparently connects logical interfaces of the same type.

In Junos OS Release 12.3R2, Juniper Networks EX Series switches support port mirroring for Layer 2 bridging traffic.

Layer port mirroring enables you to specify the manner in which incoming and outgoing packets at specified ports are monitored and the manner in which copies of selected packets are forwarded to another destination, where the packets can be analyzed.

MX Series routers and EX Series switches support Layer 2 port mirroring by performing flow monitoring functions by using a class-of-service (CoS) architecture that is in concept similar to, but in particular different from, other routing platforms and switches.

Like the M120 Multiservice Edge Router and M320 Multiservice Edge Router, MX Series routers and EX Series switches support the mirroring of IPv4, IPv6, and VPLS packets simultaneously.

In a Layer 3 environment, MX Series routers and EX Series switches support the mirroring of IPv4 (`family inet`) and IPv6 (`family inet6`) traffic. For information about Layer 3 port mirroring, see the Routing Policies, Firewall Filters, and Traffic Policers User Guide.

Layer 2 Port Mirroring Properties

Port mirroring specifies the following types of properties:

- Packet-Selection
- Packet Address Family
- Mirror Destination Properties
- Mirror-Once Option

Packet-Selection

The packet-selection properties of Layer 2 port-mirroring specify how the sampled packets are to be selected for mirroring:

- The number of packets in each sample.
- The number of packets to mirror from each sample.
- The length to which mirrored packets are to be truncated.

Packet Address Family

The packet address family type specifies the type of traffic to be mirrored. In a Layer 2 environment, MX Series routers and EX Series switches support port mirroring for the following packet address families:

- Family type `ethernet-switching` —For mirroring VPLS traffic when the physical interface is configured with encapsulation type `ethernet-bridge` .
- Family type `ccc` —For mirroring Layer 2 VPN traffic.
- Family type `vpls` —For mirroring VPLS traffic.

Note:

In typical applications, you send mirrored packets directly to an analyzer, not to another router or switch. If you must send mirrored packets over a network, you should use tunnels. For Layer 2 VPN implementations, you can use the Layer 2 VPN routing instance type `l2vpn` to tunnel the packets to a remote destination.

For information about configuring a routing instance for Layer 2 VPN, see the Junos OS VPNs Library for Routing Devices. For a detailed Layer 2 VPN example configuration, see Junos OS. For information about tunnel interfaces, see the Junos OS Network Interfaces Library for Routing Devices.

Mirror Destination Properties

For a given packet address family, the mirror destination properties of a Layer 2 port-mirroring instance specify how the selected packets are to be sent on a particular physical interface:

- The physical interface on which to send the selected packets.
- Whether filter checking is to be disabled for the mirror destination interface. By default, filter checking is enabled on all interfaces.

  Note:

  If you apply a filter to an interface that is also a Layer 2 port-mirroring destination, a commit failure occurs unless you have disabled filter checking for that mirror destination interface .

Mirror-Once Option

If port mirroring is enabled at both ingress and egress interfaces, you can prevent the MX Series router and an EX Series switch from sending duplicate packets to the same destination (which would complicate the analysis of the mirrored traffic).

Note:

The mirror-once port-mirroring option is a global setting. The option is independent of the packet selection properties and the packet family type-specific mirror destination properties.

Application of Layer 2 Port Mirroring Types

You can apply different sets of Layer 2 port-mirroring properties to the VPLS packets at different ingress or egress points of an MX Series or of an EX Series route.

Table 5 describes the three types of Layer 2 *port mirroring* that you can configure on an MX Series routers and EX Series switches, the: global instance, named instances, and firewall filters.

Table 5: Application of Layer 2 Port Mirroring Types

Type of Layer 2 Port Mirroring Definition	**Point of Application**	**Scope of Mirroring**	**Description**	**Configuration Details**
Global Instance of Layer 2 Port Mirroring	All ports in the MX Series router (or switch) chassis.	VPLS packets received on all ports in the MX Series router (or switch) chassis.	If configured, the global port-mirroring properties implicitly apply to all the VPLS packets received on all ports in the router (or switch) chassis.	See Configuring the Global Instance of Layer 2 Port Mirroring
Named Instance of Layer 2 Port Mirroring	Ports grouped at the FPC level See Binding Layer 2 Port Mirroring to Ports Grouped at the FPC Level.	VPLS packets received on ports associated with a specific DPC or FPC and its Packet Forwarding Engines.	Overrides any port-mirroring properties configured by the global port-mirroring instance.	See Defining a Named Instance of Layer 2 Port Mirroring. The number of port-mirroring destinations supported for an MX Series router and for an EX Series switch are limited to the number of Packet Forwarding Engines contained on the DPCs or FPCs installed in the

Type of Layer 2 Port Mirroring Definition	**Point of Application**	**Scope of Mirroring**	**Description**	**Configuration Details**
	Ports grouped at the PIC level See Binding Layer 2 Port Mirroring to Ports Grouped at the PIC Level.	VPLS packets received on ports associated with a specific Packet Forwarding Engine.	Overrides any port-mirroring properties configured at the FPC level or in the global port-mirroring instance.	router or switch chassis.
Layer 2 Port-Mirroring Firewall Filter	*Logical interface* (including an aggregated Ethernet interface) See Applying Layer 2 Port Mirroring to a Logical Interface.	VPLS packets received or sent on a logical interface.	In the *firewall filter* configuration, include *action* and *action-modifier* terms to apply to the packets selected for mirroring: • The `accept` action is recommended. • The `port-mirror` modifier implicitly references the port-mirroring properties currently bound to the underlying physical interfaces. • The `port-mirror-instance` *`pm-instance-`*	See Defining a Layer 2 Port-Mirroring Firewall Filter. Note: Layer 2 port-mirroring firewall filters are not supported for logical systems. For mirroring tunnel interface input packets to multiple destinations, also see Defining a Next-Hop Group for Layer 2 Port Mirroring.
	VLAN forwarding table or flood table See Applying Layer 2 Port Mirroring to Traffic	Layer 2 traffic forwarded or flooded to a VLAN		

Type of Layer 2 Port Mirroring Definition	Point of Application	Scope of Mirroring	Description	Configuration Details
	Forwarded or Flooded to a Bridge Domain.		`name` modifier explicitly references a named instance of port mirroring. • (Optional) For tunnel interface input packets only, to mirror the packets to additional destinations, include the `next-hop-group next-hop-group-name` modifier. This modifier references a next-hop-group that specifies the next-hop addresses (for sending additional copies of packets to an analyzer).	
	VPLS routing instance forwarding table or flood table See Applying Layer 2 Port Mirroring to Traffic Forwarded or Flooded to a VPLS Routing Instance.	Layer 2 traffic forwarded or flooded to a VPLS routing instance		

Restrictions on Layer 2 Port Mirroring

The following restrictions apply to Layer 2 *port mirroring*:

- Only Layer 2 transit data (packets that contain chunks of data transiting the routing platform or switch as they are forwarded from a source to a destination) can be mirrored. Layer 2 local data (packets that contain chunks of data that are destined for or sent by the Routing Engine, such as Layer 2 control packets) are not mirrored.
- If you apply a port-mirroring filter to the output of a *logical interface*, only Unicast packets are mirrored. To mirror Broadcast packets, Multicast packets, Unicast packets with an unknown destination media access control (MAC) address, or packets with a MAC entry in the destination MAC (DMAC) routing table, apply a filter to the input to the flood table of a VLAN or virtual private LAN service (VPLS) routing instance.

- The mirror destination device should be on a dedicated VLAN and should not participate in any bridging activity; the mirror destination device should not have a bridge to the ultimate traffic destination, and the mirror destination device should not send the mirrored packets back to the source address.
- For either the global port-mirroring instance or a named port-mirroring instance, you can configure only one mirror output interface per port-mirroring instance and packet address family. If you include more than one `interface` statement under the `family (ethernet-switching | ccc | vpls) output` statement, the previous `interface` statement is overridden.
- Layer 2 port-mirroring firewall filtering is not supported for logical systems.

  In a Layer 2 port-mirroring *firewall filter* definition, the *`action-modifier`* filter (`port-mirror` or `port-mirror-instance` *`pm-instance-name`*) relies on port-mirroring properties defined in the global instance or named instances of Layer 2 port mirroring, which are configured under the `[edit forwarding-options port-mirroring]` hierarchy. Therefore, the *`term`* filter cannot support Layer 2 port mirroring for logical systems.
- For a Layer 2 port mirroring firewall filter in which you implicitly reference Layer 2 port mirroring properties by including the `port-mirror` statement, if multiple named instances of Layer 2 port mirroring are bound to the underlying physical interface, then only the first binding in the stanza (or the only binding) is used at the logical interface. This is done for backward compatibility.
- Layer 2 port-mirroring firewall filters do not support the use of next-hop subgroups for load-balancing mirrored traffic.
