Port Mirroring on EX-series Switches Overview

Use port mirroring to facilitate analyzing traffic on your switch on a packet level. Use port mirroring as part of monitoring switch traffic for such purposes as enforcing policies concerning network usage and file sharing, and identifying sources of problems on your network by locating abnormal or heavy bandwidth usage from particular stations or applications.

Port mirroring copies packets entering or exiting an interface, or entering a VLAN in an EX 3200 or EX 4200 switch or exiting a VLAN in an EX 8200 series switch, to either a local interface for local monitoring or to a VLAN for remote monitoring.

Port Mirroring Overview

Port mirroring is needed for traffic analysis on a switch because a switch, unlike a hub, does not broadcast packets to every port on the 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 interface or an analyzer VLAN. Then you can analyze the mirrored traffic 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.

We recommend that you disable port mirroring when you are not using it, and select specific interfaces as input to the port mirror analyzer in preference to using the all keyword. 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. You should consider whether the traffic being mirrored exceeds the capacity of the analyzer output interface.

You can use port mirroring on an EX-series switch to mirror any of the following:

- **Packets entering or exiting a port**—In any combination. For example, you can send copies of the packets entering some ports and the packets exiting other ports to the same local analyzer port or analyzer VLAN.
- **Packets entering or exiting a Layer 3 port**—In any combination. For example, you can send copies of the packets entering some ports and the packets exiting other ports to the same local analyzer port or analyzer VLAN.
- **Packets entering a VLAN in an EX 3200 or EX 4200 switch**—You can mirror the packets entering a VLAN in an EX 3200 or EX 4200 switch to either a local analyzer port or to an analyzer VLAN. You can configure multiple VLANs (up to 256), including range VLAN and PVLANs, as ingress input to an analyzer.

- **Packets exiting a VLAN in an EX 8200 series switch**—You can mirror the packets exiting a VLAN in an EX 8200 series switch to either a local analyzer port or to an analyzer VLAN. You can configure multiple (up to 256) VLANs, including range VLAN and PVLANs, as egress input to an analyzer.
- **Statistical sample**—Sample of the packets entering or exiting a port or entering a VLAN in an EX 3200 or EX 4200 switch or exiting a VLAN in an EX 8200 series switch. Specify the sample number of packets by setting the ratio. You can send the sample of packets to either a local analyzer port or to an analyzer VLAN.
- **Policy-based sample**—Sample of packets entering a port or entering a VLAN in an EX 3200 or EX 4200 switch or exiting a VLAN in an EX 8200 series switch. You can configure a firewall filter to establish a policy to select certain packets. You can send the sampled packets to a local analyzer interface or to an analyzer VLAN.

NOTE: JUNOS software for EX-series switches implements port mirroring differently than other JUNOS software packages. JUNOS software for EX-series switches does not include the port-mirroring statement found in the edit forwarding-options level of the hierarchy of other JUNOS software packages, nor the port-mirror action in firewall filter terms.

Limitations of Port Mirroring

Port mirroring on EX-series switches has the following limitations:

- Seven analyzers (port mirroring configurations) can be configured on an EX 8208 or EX 8216 switch.
- Packets with physical layer errors are filtered out and thus are not sent to the analyzer port or VLAN.
- The following interfaces cannot be configured as input to an analyzer:
  - Dedicated Virtual Chassis ports (VCPs)
  - Management port (me0 or vme0)
  - Routed VLAN interfaces (RVIs)

Port Mirroring Terminology

Table 1: Port Mirroring Terminology

Term	Description
Analyzer	A port-mirroring configuration on an EX-series switch. The analyzer includes: ■ The name of the analyzer ■ Source (input) ports or VLAN (optional) ■ A destination for mirrored packets (either a monitor port or an analyzer VLAN) ■ Ratio field for specifying statistical sampling of packets (optional) ■ Loss-priority setting

Table 1: Port Mirroring Terminology *(continued)*

Term	Description
Analyzer output interface Also known as monitor interface	Interface to which mirrored traffic is sent and to which a protocol analyzer application is connected. **NOTE:** Interfaces used as output for a port mirror analyzer must be configured as family ethernet-switching. The following limitations apply to analyzer output interfaces: ■ Cannot also be a source port. ■ Cannot be used for switching. ■ Does not participate in Layer 2 protocols, such as Spanning Tree Protocol (STP), when it is part of a port mirroring configuration. ■ When configured as an analyzer output interface, it loses any existing VLAN associations. 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 analyzer VLAN is spread across the switches in your network.
Firewall-based Analyzer	An analyzer session that has only an “output” stanza. Firewall based Analyzer has to be used along with firewall to achieve the functionality of an analyzer.
Input interface Also known as mirrored ports or monitored interfaces	An interface on the switch that is being mirrored, either on traffic entering or exiting the interface. An input interface cannot also be an output interface for an analyzer.
Mirror ratio	See statistical sampling.
Monitoring station	A computer running a protocol analyzer application.
Native analyzer session	An analyzer session that has both “input” and “output” stanzas.
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 instead flooded into an analyzer VLAN that you create specifically for the purpose of receiving mirrored traffic.
Policy-based mirroring	Mirroring of packets that match the match items in the defined firewall filter term. The action item analyzer *analyzer-name* is used in the firewall filter to send the packets to the port mirror analyzer.
Protocol analyzer application	An application used to examine packets transmitted across a network segment. Also commonly called network analyzer, packet sniffer, or probe.
Statistical sampling	You can configure the system to mirror a sampling of the packets, by setting a ratio of 1:*x*, where *x* is a value from 1 through 2047. For example, when the ratio is set to 1, all packets are copied to the analyzer. When the ratio is set to 200, 1 of every 200 packets is copied.

Related Topics

- Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX-series Switches
- Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX-series Switches
- Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) or Configuring Port Mirroring to Analyze Traffic (CLI Procedure)
- Firewall Filter Match Conditions and Actions for EX-series Switches

---

Published: 2009-06-17