Configuring Port Mirroring to Analyze Traffic (CLI Procedure)

EX Series switches allow 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 use port mirroring to copy these packets:

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

We recommend that you disable port mirroring when you are not using it and select specific input interfaces in preference to using the all keyword. You can also limit the amount of mirrored traffic by using a firewall filter or the ratio keyword to mirror only a selection of packets.

NOTE: If you want to create additional analyzers without deleting the existing analyzer, first disable the existing analyzer using the disable analyzer *analyzer-name* command or the J-Web configuration page for port mirroring.

NOTE: Interfaces used as output for a port mirror analyzer must be configured as family ethernet-switching.

Configuring Port Mirroring for Local Traffic Analysis

To mirror interface traffic or VLAN traffic on the switch to an interface on the switch:

1. Choose a name for the port mirroring configuration—in this case, employee-monitor—and specify the input—in this case, packets entering ge-0/0/0 and ge-0/0/1:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface
ge-0/0/0.0

[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface
ge-0/0/1.0
```

2. Optionally, you can specify a statistical sampling of the packets by setting a ratio:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor ratio 200
```

When the ratio is set to 200, 1 of every 200 packets is mirrored to the analyzer. You can use statistical sampling to reduce the volume of mirrored traffic, as a high volume of mirrored traffic can be performance intensive for the switch. On EX8200 switches, you can set a ratio only for ingress packets.

3. Configure the destination interface for the mirrored packets:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

Configuring Port Mirroring for Remote Traffic Analysis

To mirror traffic that is traversing interfaces or a VLAN on the switch to a VLAN for analysis from a remote location:

1. Configure a VLAN to carry the mirrored traffic. This VLAN is called remote-analyzer and given the ID of 999 by convention in this documentation:

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

2. Set the uplink module interface that is connected to the distribution switch to trunk mode and associate it with the remote-analyzer VLAN:

```
[edit]
user@switch# set interfaces ge-0/1/1 unit 0 family ethernet-switching
port-mode trunk vlan members 999
```

3. Configure the analyzer:

   a. Choose a name and set the loss priority to high. Loss priority should always be set to high when configuring for remote port mirroring:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor loss-priority high
```

   b. Specify the traffic to be mirrored—in this example the packets entering ports ge-0/0/0 and ge-0/0/1:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface
ge-0/0/0.0
```

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface
ge-0/0/1.0
```

   c. Specify the remote-analyzer VLAN as the output for the analyzer:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor output vlan 999
```

4. Optionally, you can specify a statistical sampling of the packets by setting a ratio:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor ratio 200
```

When the ratio is set to 200, 1 out of every 200 packets is mirrored to the analyzer. You can use this to reduce the volume of mirrored traffic as a very high volume of mirrored traffic can be performance intensive for the switch.

Filtering the Traffic Entering an Analyzer

To filter which packets are mirrored to an analyzer, create the analyzer and then use it as the action in the firewall filter. You can use firewall filters in both local and remote port mirroring configurations.

If the same analyzer is used in multiple filters or terms, the packets are copied to the analyzer output port or analyzer VLAN only once.

To filter mirrored traffic, create an analyzer and then create a firewall filter. The filter can use any of the available match conditions and must have an action of analyzer *analyzer-name*. The action of the firewall filter provides the input to the analyzer.

To configure port mirroring with filters:

1. Configure the analyzer name (here, employee-monitor) and the output:

   a. For local analysis, set the output to the local interface to which you will connect the computer running the protocol analyzer application:

   ```
   [edit ethernet-switching-options]
   user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
   ```

   b. For remote analysis, set the loss priority to high and set the output to the remote-analyzer VLAN:

   ```
   [edit ethernet-switching-options]
   user@switch# set analyzer employee-monitor loss-priority high output vlan
   999
   ```

2. Create a firewall filter using any of the available match conditions and specify the action as analyzer employee-monitor:

   This step shows a firewall filter called example-filter, with two terms:

   a. Create the first term to define the traffic that should not pass through to the analyzer:

   ```
   [edit firewall family ethernet-switching]
   user@switch# set filter example-filter term no-analyzer from source-address
   ip-address
   ```

   ```
   [edit firewall family ethernet-switching]
   user@switch# set filter example-filter term no-analyzer from
   destination-address ip-address
   ```

   ```
   [edit firewall family ethernet-switching]
   user@switch# set filter example-filter term no-analyzer then accept
   ```

   b. Create the second term to define the traffic that should pass through to the analyzer:

   ```
   [edit firewall family ethernet-switching]
   ```

```
user@switch# set filter example-filter term to-analyzer from
destination-port 80

[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer then analyzer
employee-monitor
```

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

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

[edit]
user@switch# set vlan rspan filter input example-filter
```

Related Topics

- Configuring Port Mirroring to Analyze Traffic (J-Web Procedure)
- 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
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches
- Understanding Port Mirroring on EX Series Switches
- Firewall Filters for EX Series Switches Overview

Published: 2010-04-26