

Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX-series Switches

EX-series switches allow you to configure port mirroring to send copies of packets entering or exiting an interface, or entering a VLAN, to an analyzer interface or VLAN. You can analyze the mirrored traffic using a protocol analyzer application installed on a system connected to the local destination interface (or a running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN).

This example describes how to configure an EX-series switch to mirror traffic entering interfaces connected to employee computers to an analyzer output interface on the same switch.

This example describes how to configure local port mirroring:

- Requirements on page 1
- Overview and Topology on page 1
- Mirroring All Employee Traffic for Local Analysis on page 2
- Mirroring Employee-to-Web Traffic for Local Analysis on page 3
- Verification on page 5

Requirements

This example uses the following hardware and software components:

- JUNOS Release 9.0 or later for EX-series switches
- One EX 3200 or EX 4200 switch

Before you configure port mirroring, be sure you have an understanding of port mirroring concepts.

Overview and Topology

This topic includes two related examples that describe how to mirror traffic entering ports on the switch to a destination interface on the same switch. The first example shows how to mirror all traffic entering the ports connected to employee computers. The second example shows the same scenario, but includes a filter to mirror only the employee traffic going to the Web.

Network Topology

In this example, `ge-0/0/0` and `ge-0/0/1` serve as connections for employee computers.

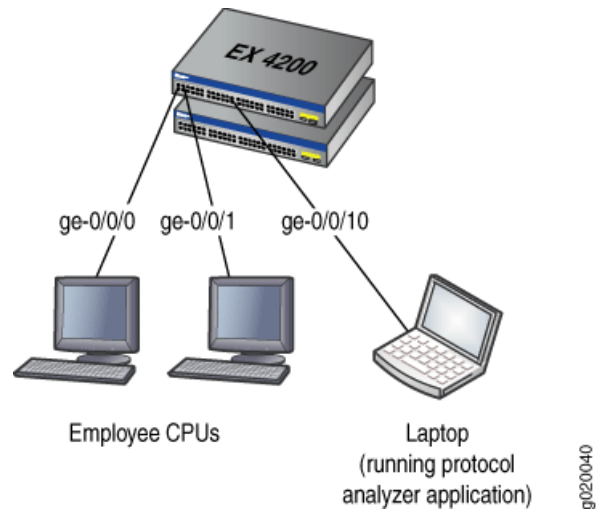
In this example, one interface, `ge-0/0/10`, is reserved for analysis of mirrored traffic. Connect a PC running a protocol analyzer application to the analyzer output interface to analyze the mirrored traffic.



NOTE: Multiple ports mirrored to one interface can cause buffer overflow and dropped packets.

Figure 1 on page 2 shows the network topology for this example.

Figure 1: Network Topology for Local Port Mirroring Example



Mirroring All Employee Traffic for Local Analysis

To configure port mirroring for all employee traffic for local analysis, perform these tasks:

CLI Quick Configuration To quickly configure local port mirroring for ingress traffic to the two ports connected to employee computers, copy the following commands and paste them into the switch terminal window:

```
[edit ethernet-switching-options]
set analyzer employee-monitor input ingress interface ge-0/0/0.0
set analyzer employee-monitor input ingress interface ge-0/0/1.0
set analyzer employee-monitor output interface ge-0/0/10.0
```

Step-by-Step Procedure To configure an analyzer called `employee-monitor` and specify the input (source) interfaces and the analyzer output interface.

1. Configure each interface connected to employee computers as an input interface for the port-mirror analyzer that we are calling `employee-monitor`:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface
ge-0/0/0.0
user@switch# set analyzer employee-monitor input ingress interface
ge-0/0/1.0
```

2. Configure the output analyzer interface for the `employee-monitor` analyzer. This will be the destination interface for the mirrored packets:

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

3. `commit`

Results Check the results of the configuration:

```
[edit]
user@switch# show
ethernet-switching-options {
  analyzer employee-monitor {
    input {
      ingress {
        interface ge-0/0/0.0;
        interface ge-0/0/1.0;
      }
    }
    output {
      interface {
        ge-0/0/10.0;
      }
    }
  }
}
```

Mirroring Employee-to-Web Traffic for Local Analysis

To configure port mirroring for employee to web traffic, perform these tasks:

CLI Quick Configuration To quickly configure local port mirroring of traffic from the two ports connected to employee computers, filtering so that only traffic to the external Web is mirrored, copy the following commands and paste them into the switch terminal window:

```
[edit]
set ethernet-switching-options analyzer employee-web-monitor output interface
ge-0/0/10.0
set firewall family ethernet-switching filter watch-employee term employee-to-corp
from destination-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp
from source-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp
then accept
set firewall family ethernet-switching filter watch-employee term employee-to-web
from destination-port 80
set firewall family ethernet-switching filter watch-employee term
employee_to_internet then analyzer employee-web-monitor
set firewall family ethernet-switching filter watch-employee
set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input
watch-employee
```

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input
watch-employee
```

Step-by-Step Procedure

To configure local port mirroring of employee-to-Web traffic from the two ports connected to employee computers:

1. Configure the local analyzer interface:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching
```

2. Configure the `employee-web-monitor` analyzer output (the input to the analyzer comes from the action of the filter):

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

3. Configure a firewall filter called `watch-employee` to send mirrored copies of employee requests to the Web to the `employee-web-monitor` analyzer. Accept all traffic to and from the corporate subnet (destination or source address of `192.0.2.16/28`). Send mirrored copies of all packets destined for the Internet (destination port 80) to the `employee-web-monitor` analyzer.

```
[edit firewall family ethernet-switching]
user@switch# set filter watch-employee term employee-to-corp from
destination-address 192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp from
source-address 192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from
destination-port 80
user@switch# set filter watch-employee term employee-to-web then analyzer
employee-web-monitor
```

4. Apply the `watch-employee` filter to the appropriate ports:

```
[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching filter input
watch-employee
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input
watch-employee
```

5. `commit`

Results Check the results of the configuration:

```
[edit]
user@switch# show
ethernet-switching-options {
  analyzer employee-web-monitor {
    output {
      interface ge-0/0/10.0;
    }
  }
}
```

```

    }
}
...
firewall family ethernet-switching {
  filter watch-employee {
    term employee-to-corp {
      from {
        destination-address 192.0.2.16/28;
        source-address 192.0.2.16/28;
      }
      then
        accept;
    }
    term employee-to-web;
    from {
      destination-port 80;
    }
    then
      analyzer employee-web-monitor;
  }
}
...
interfaces
ge-0/0/0 {
  unit 0
  family ethernet-switching {
    port-mode trunk;
    vlan members [employee-vlan, voice-vlan];
    filter {
      input watch-employee;
    }
  }
}
ge-0/0/1 {
  family ethernet-switching {
    port-mode trunk;
    vlan members [employee-vlan, voice-vlan];
    filter {
      input watch-employee;
    }
  }
}
}

```

Verification

To confirm that the configuration is correct, perform these tasks:

- Verifying That the Analyzer Has Been Correctly Created on page 5

Verifying That the Analyzer Has Been Correctly Created

Purpose Verify that the analyzer named `employee-monitor` or `employee-web-monitor` has been created on the switch with the appropriate input interfaces, and appropriate output interface.

Action You can verify the port mirror analyzer is configured as expected using the `show analyzer` command.

```
user@switch> show analyzer
Analyzer name           : employee-monitor
Output interface        : ge-0/0/10.0
Mirror ratio            : 1
Loss priority           : Low
Ingress monitored interfaces : ge-0/0/0.0
Ingress monitored interfaces : ge-0/0/1.0
Egress monitored interfaces  : None
```

Meaning This output shows that the employee-monitor analyzer has a ratio of 1 (mirroring every packet, the default setting), a loss priority of low (set this option to high only when the analyzer output is to a VLAN), is mirroring the traffic entering the `ge-0/0/0` and `ge-0/0/1` interfaces, and sending the mirrored traffic to the `ge-0/0/10` interface.

- Related Topics**
- Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX-series Switches
 - Configuring Port Mirroring to Analyze Traffic (CLI Procedure)
 - Configuring Port Mirroring to Analyze Traffic (J-Web Procedure)
 - Port Mirroring on EX-series Switches Overview