Example: Configuring Port Mirroring for Remote 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 in an EX3200 or EX4200 switch or exiting a VLAN in an EX8200 switch, to an analyzer interface or a VLAN. You can analyze the mirrored traffic using a protocol analyzer application running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.

This topic includes two related examples that describe how to mirror traffic entering ports on the switch to the remote-analyzer VLAN so that you can perform analysis from a remote monitoring station. 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.

This example describes how to configure remote port mirroring:

Requirements

This example uses the following hardware and software components:

- JUNOS Release 9.5 or later for EX Series switches
- One EX3200 or EX4200 switch connected to another EX3200 or EX4200 switch

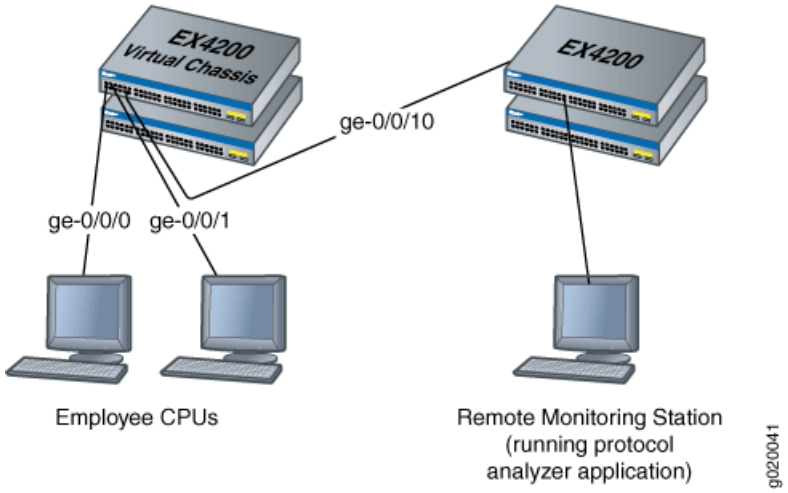
Before you configure port mirroring, be sure you have an understanding of port mirroring concepts.

Input interfaces that are referred by the analyzer must be configured.

Overview and Topology

This topic includes two related examples that describe how to configure port mirroring to the remote-analyzer VLAN so that analysis can be performed from a remote monitoring station. The first example shows how to configure an EX Series switch to mirror all traffic from employee computers. The second example shows the same scenario, but the setup includes a filter to mirror only the employee traffic going to the Web.

Figure 1: Remote Port Mirroring Example Network Topology



In this example:

- Interface ge-0/0/0 is a Layer 2 interface and interface ge-0/0/1 is a Layer 3 interface that serve as connections for employee computers.
- Interface ge-0/0/10 is a Layer 2 interface that connects to another switch.
- VLAN remote-analyzer is configured on all switches in the topology to carry the mirrored traffic.

NOTE: The interface connected to the remote monitoring station must be a member of VLAN remote-analyzer, and this VLAN must be configured on all switches between the monitored switch and the monitoring station.

Mirroring All Employee Traffic for Remote Analysis

To configure port mirroring for remote traffic analysis for all incoming and outgoing employee traffic, perform these tasks:

CLI Quick Configuration

To quickly configure port mirroring for remote traffic analysis for incoming and outgoing employee traffic, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set ethernet-switching-options analyzer employee-monitor input ingress interface
ge-0/0/0.0
set ethernet-switching-options analyzer employee-monitor input ingress interface
ge-0/0/1.0
set ethernet-switching-options analyzer employee-monitor input egress interface
ge-0/0/0.0
set ethernet-switching-options analyzer employee-monitor input egress interface
ge-0/0/1.0
```

```
set ethernet-switching-options analyzer employee-monitor loss-priority high output
vlan remote-analyzer
```

Step-by-Step Procedure To configure basic remote port mirroring:

1. Configure the VLAN tag ID for the remote-analyzer VLAN:

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

2. Configure the interface on the network port connected to another switch for trunk mode and associate it with the remote-analyzer VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching port-mode
trunk
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members
999
```

3. Configure the employee-monitor analyzer:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor loss-priority high
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
user@switch# set analyzer employee-monitor output vlan remote-analyzer
set analyzer employee-monitor input egress interface ge-0/0/0.0
set analyzer employee-monitor input egress interface ge-0/0/1.0
```

Results Check the results of the configuration:

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

}

Mirroring Employee-to-Web Traffic for Remote Analysis

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

CLI Quick Configuration

To quickly configure port mirroring to mirror employee traffic to the external Web, copy the following commands and paste them into the terminal window:

```
[edit]
set ethernet-switching-options analyzer employee-web-monitor loss-priority high
output vlan 999
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching port mode trunk
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
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-web
then analyzer employee-web-monitor
set 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 port mirroring of all traffic from the two ports connected to employee computers to the remote-analyzer VLAN for use from a remote monitoring station:

1. Configure the employee-web-monitor analyzer:

```
[edit ethernet-switching-options]
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching
port mode trunk
user@switch# set analyzer employee-web-monitor loss-priority high output
vlan 999
```

2. Configure the VLAN tag ID for the remote-analyzer VLAN:

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

3. Configure the interface to associate it with the remote-analyzer VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members
999
```

4. Configure the firewall filter called watch-employee:

```
[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
```

5. Apply the firewall filter to the employee interfaces:

```
[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
```

Results Check the results of the configuration:

```
[edit]
user@switch# show
interfaces {
    ...
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members remote-analyzer;
                }
            }
        }
    }
    ge-0/0/0 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
```

```
}
...
firewall {
    family ethernet-switching {
        ...
        filter watch-employee {
            term employee-to-corp {
                from {
                    source-address {
                        192.0.2.16/28;
                    }
                    destination-address {
                        192.0.2.16/28;
                    }
                }
                then accept;
            }
            term employee-to-web {
                from {
                    destination-port 80;
                }
                then analyzer employee-web-monitor;
            }
        }
    }
}
ethernet-switching-options {
    analyzer employee-web-monitor {
        loss-priority high;
        output {
            vlan {
                999;
            }
        }
    }
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That the Analyzer Has Been Correctly Created on page 6

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. To view previously created analyzers that are disabled, go to the J-Web interface.

```
user@switch> show analyzer
 Analyzer name                 : employee-monitor
 Output VLAN                   : remote-analyzer
 Mirror ratio                  : 1
 Loss priority                 : High
 Ingress monitored interfaces : ge-0/0/0.0
 Ingress monitored interfaces : ge-0/0/1.0
```

Meaning This output shows that the employee-monitor analyzer has a ratio of 1 (mirroring every packet, the default), a loss priority of high (set this option to high whenever the analyzer output is to a VLAN), is mirroring the traffic entering ge-0/0/0 and ge-0/0/1, and sending the mirrored traffic to the analyzer called remote-analyzer.

Related Topics

- Example: Configuring Port Mirroring for Local 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)
- Understanding Port Mirroring on EX Series Switches

Published: 2009-09-23