Example: Configuring a Private VLAN on an EX-series Switch

For security reasons, it is often useful to restrict the flow of broadcast and unknown unicast traffic and to even limit the communication between known hosts. The private VLAN (PVLAN) feature on EX-series switches allow an administrator to split a broadcast domain into multiple isolated broadcast subdomains, essentially putting a VLAN inside a VLAN.

This example describes how to create a private VLAN primary VLAN and secondary VLANs:

Requirements

This example requires one EX-series switch with JUNOS Release 9.3 or later for EX-series switches.

Before you begin configuring a private VLAN, make sure you have created and configured the necessary VLAN. See Configuring VLANs for EX-series Switches (CLI Procedure) or Configuring VLANs for EX-series Switches (J-Web Procedure).

Overview and Topology

In a large office with multiple buildings and VLANs, you might need to isolate some workgroups or other endpoints for security reasons or to partition the broadcast domain. This configuration example shows a simple topology to illustrate how to create a private VLAN with one primary VLAN and two community VLANs, one for HR and one for finance, as well as two isolated ports for the mail server and the backup server.

Table 1 lists the settings for the example topology.

Table 1: Components of the Topology for Configuring a Private VLAN

Interface	Description
ge-0/0/0.0	Primary VLAN (pvlan) trunk port
ge-0/0/11.0	User 1, HR Community (hr-comm)
ge-0/0/12.0	User 2, HR Community (hr-comm)
ge-0/0/13.0	User 3, Finance Community (finance-comm)
ge-0/0/14.0	User 4, Finance Community (finance-comm)
ge-0/0/15.0	Mail server, Isolated (isolated)

Table 1: Components of the Topology for Configuring a Private VLAN *(continued)*

ge-0/0/16.0	Backup server, Isolated (isolated)
ge-1/0/0.0	Primary VLAN (pvlan) trunk port

Configuration

CLI Quick Configuration

To quickly create and configure a private VLAN, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans pvlan vlan-id 1000
set interfaces ge-0/0/0 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members pvlan
set interfaces ge-1/0/0 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-1/0/0 unit 0 family ethernet-switching vlan members pvlan
set interfaces ge-0/0/11 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/12 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/13 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/14 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/15 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/16 unit 0 family ethernet-switching port-mode access
set vlans pvlan no-local-switching
set vlans pvlan interface ge-0/0/0.0
set vlans pvlan interface ge-1/0/0.0
set vlans hr-comm interface ge-0/0/11.0
set vlans hr-comm interface ge-0/0/12.0
set vlans finance-comm interface ge-0/0/13.0
set vlans finance-comm interface ge-0/0/14.0
set vlans hr-comm primary-vlan pvlan
set vlans finance-comm primary-vlan pvlan
```

Step-by-Step Procedure

To configure the private VLAN:

1. Set the VLAN ID for the primary VLAN:

```
[edit vlans]
user@switch# set pvlan vlan-id 1000
```

2. Set the interfaces and port modes:

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

user@switch# set ge-0/0/0 unit 0 family ethernet-switching vlan members
pvlan

user@switch# set ge-1/0/0 unit 0 family ethernet-switching port-mode trunk

user@switch# set ge-1/0/0 unit 0 family ethernet-switching vlan members
pvlan
```

```
user@switch# set ge-0/0/11 unit 0 family ethernet-switching port-mode
access

user@switch# set ge-0/0/12 unit 0 family ethernet-switching port-mode
access

user@switch# set ge-0/0/13 unit 0 family ethernet-switching port-mode
access

user@switch# set ge-0/0/14 unit 0 family ethernet-switching port-mode
access

user@switch# set ge-0/0/15 unit 0 family ethernet-switching port-mode
access

user@switch# set ge-0/0/16 unit 0 family ethernet-switching port-mode
access
```

3. Set the primary VLAN to have no local switching:

NOTE: The primary VLAN must be a tagged VLAN.

```
[edit vlans]
user@switch# set pvlan no-local-switching
```

4. Add the trunk interfaces to the primary VLAN:

```
[edit vlans]
user@switch# set pvlan interface ge-0/0/0.0

user@switch# set pvlan interface ge-1/0/0.0
```

5. For each secondary VLAN, configure access interfaces:

NOTE: The secondary VLANs must be untagged VLANs.

```
[edit vlans]
user@switch# set hr-comm interface ge-0/0/11.0


user@switch# set hr-comm interface ge-0/0/12.0

user@switch# set finance-comm interface ge-0/0/13.0

user@switch# set finance-comm interface ge-0/0/14.0
```

6. For each community VLAN, set the primary VLAN:

```
[edit vlans]
user@switch# set hr-comm primary-vlan pvlan

user@switch# set finance-comm primary-vlan pvlan
```

7. Add each isolated interface to the primary VLAN:

```
[edit vlans]
user@switch# set pvlan interface ge-0/0/15.0

user@switch# set pvlan interface ge-0/0/16.0
```

Results Check the results of the configuration:

```
user@switch> show configuration vlans
finance-comm {
    interface {
        ge-0/0/13.0;
        ge-0/0/14.0;
    }
    primary-vlan pvlan;
}
    hr-comm {
        interface {
            ge-0/0/11.0;
            ge-0/0/12.0;
        }
        primary-vlan pvlan;
    }
    pvlan {
        vlan-id 1000;
        interface {
            ge-0/0/15.0;
            ge-0/0/16.0;
            ge-0/0/0.0;
            ge-1/0/0.0;
        }
        no-local-switching;
    }
```

Verification

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

- Verifying the Private VLAN and Secondary VLANs Were Created on page 4

Verifying the Private VLAN and Secondary VLANs Were Created

Purpose Verify that the primary VLAN and secondary VLANs were properly created on the switch.

Action Use the show vlans command:

```
user@switch> show vlans pvlan extensive
VLAN: pvlan, Created at: Tue Sep 16 17:59:47 2008
802.1Q Tag: 1000, Internal index: 18, Admin State: Enabled, Origin: Static
Private VLAN Mode: Primary
Protocol: Port Mode
Number of interfaces: Tagged 2 (Active = 0), Untagged  6 (Active = 0)
      ge-0/0/0.0, tagged, trunk
      ge-0/0/11.0, untagged, access
      ge-0/0/12.0, untagged, access
      ge-0/0/13.0, untagged, access
      ge-0/0/14.0, untagged, access
      ge-0/0/15.0, untagged, access
      ge-0/0/16.0, untagged, access
      ge-1/0/0.0, tagged, trunk
Secondary VLANs: Isolated 2, Community  2
  Isolated VLANs :
      __pvlan_pvlan_ge-0/0/15.0__
      __pvlan_pvlan_ge-0/0/16.0__
  Community VLANs :
      finance-comm
      hr-comm
user@switch> show vlans hr-comm extensive
VLAN: hr-comm, Created at: Tue Sep 16 17:59:47 2008
Internal index: 22, Admin State: Enabled, Origin: Static
Private VLAN Mode: Community, Primary VLAN: pvlan
Protocol: Port Mode
Number of interfaces: Tagged 2 (Active = 0), Untagged  2 (Active = 0)
      ge-0/0/0.0, tagged, trunk
      ge-0/0/11.0, untagged, access
      ge-0/0/12.0, untagged, access
      ge-1/0/0.0, tagged, trunk
user@switch> show vlans finance-comm extensive
VLAN: finance-comm, Created at: Tue Sep 16 17:59:47 2008
Internal index: 21, Admin State: Enabled, Origin: Static
Private VLAN Mode: Community, Primary VLAN: pvlan
Protocol: Port Mode
Number of interfaces: Tagged 2 (Active = 0), Untagged  2 (Active = 0)
      ge-0/0/0.0, tagged, trunk
      ge-0/0/13.0, untagged, access
      ge-0/0/14.0, untagged, access
      ge-1/0/0.0, tagged, trunk
user@switch> show vlans __pvlan_pvlan_ge-0/0/15.0__ extensive
VLAN: __pvlan_pvlan_ge-0/0/15.0__, Created at: Tue Sep 16 17:59:47 2008
Internal index: 19, Admin State: Enabled, Origin: Static
Private VLAN Mode: Isolated, Primary VLAN: pvlan
Protocol: Port Mode
Number of interfaces: Tagged 2 (Active = 0), Untagged  1 (Active = 0)
      ge-0/0/0.0, tagged, trunk
      ge-0/0/15.0, untagged, access
      ge-1/0/0.0, tagged, trunk
user@switch> show vlans __pvlan_pvlan_ge-0/0/16.0__ extensive
VLAN: __pvlan_pvlan_ge-0/0/16.0__, Created at: Tue Sep 16 17:59:47 2008
Internal index: 20, Admin State: Enabled, Origin: Static
Private VLAN Mode: Isolated, Primary VLAN: pvlan
Protocol: Port Mode
Number of interfaces: Tagged 2 (Active = 0), Untagged  1 (Active = 0)
      ge-0/0/0.0, tagged, trunk
```

```
ge-0/0/16.0, untagged, access
ge-1/0/0.0, tagged, trunk
```

Meaning The output shows that the primary VLAN was created and identifies the interfaces and secondary VLANs associated with it.

Related Topics

- Creating a Private VLAN (CLI Procedure)