Configuring Private VLAN

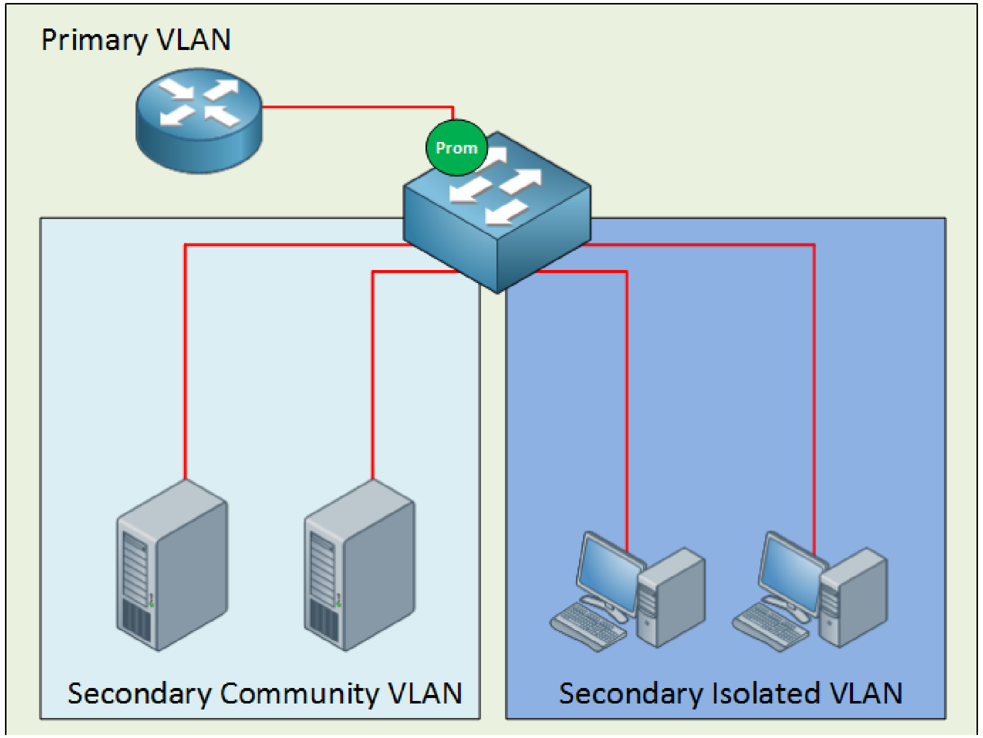
By : Haydar Fadel

Configuring PVLAN

Understanding and Configuring Private VLAN

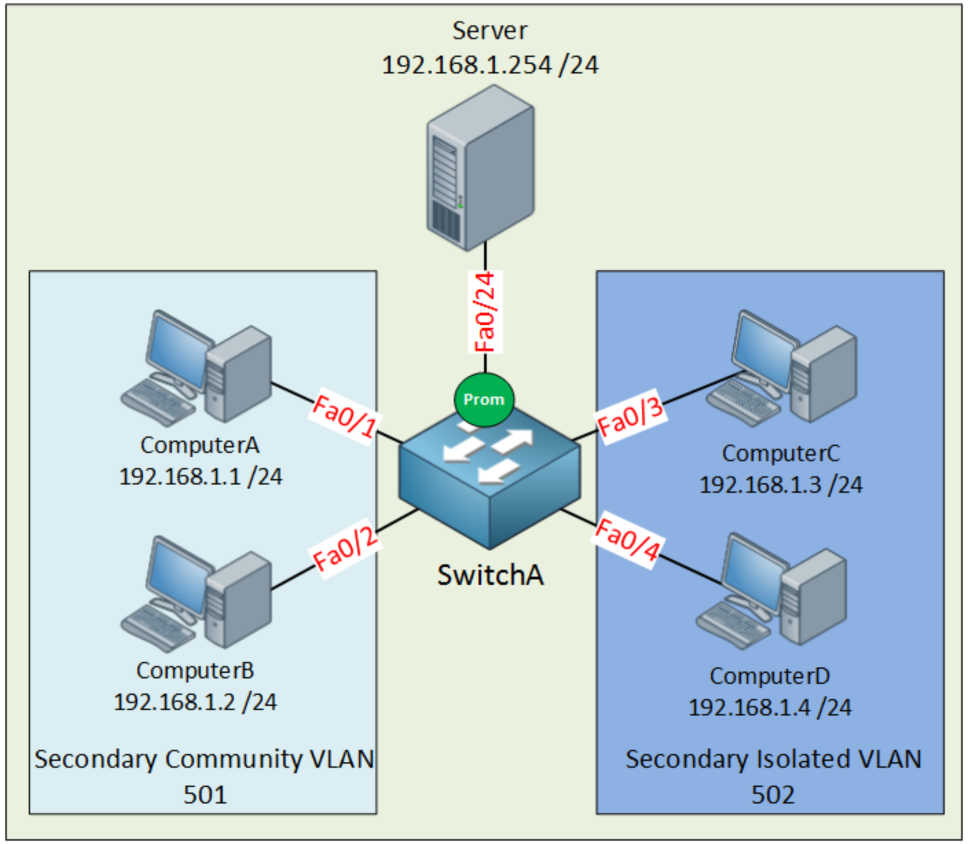
Private VLAN (PVLAN)

- Many network students believe private VLANs are very complex when they see this for the first time. The private VLAN always has **one primary VLAN**. Within the primary VLAN you will find the promiscuous port.
- In my picture below you can see that there's a router connected to a promiscuous port. **All other ports are able to communicate with the promiscuous port**.
- Within the primary VLAN you will encounter one or more secondary VLANs, there are two types:
  - ➢ **Community VLAN**: All ports within the community VLAN are **able** to communicate with each other and the promiscuous port.
  - ➢ **Isolated VLAN**: All ports within the isolated VLAN are **unable** to communicate with each other but they can communicate with the promiscuous port.



Configuration

- First let me show you the topology that I will use for this demonstration:



Let me sum up what we have here:

- The primary VLAN has number 500.
- The secondary community VLAN has number 501.
- The secondary isolated VLAN has number 502.
- I just made up these VLAN numbers; you can use whatever you like.
- ComputerA and ComputerB in the community VLAN should be able to reach each other and also the server connected to the promiscuous port.
- ComputerC and ComputerD in the isolated VLAN can only communicate with the server on the promiscuous port.
- The server should be able to reach all ports.

Configuration

- Configuring private VLANs requires us to change the VTP mode to Transparent.

```
SwitchA(confg)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
```

- Let’s start with the configuration of the community VLAN.
- First I create VLAN 501 and tell the switch that this is a community VLAN by typing the private-vlan community command.
- Secondly I am creating VLAN 500 and configuring it as the primary VLAN with the private-vlan primary command. Last but not least I need to tell the switch that VLAN 501 is a secondary VLAN by using the private-vlan association command.

```
SwitchA(confg)#vlan 501
SwitchA(confg-vlan)#private-vlan community
SwitchA(confg-vlan)#vlan 500
SwitchA(confg-vlan)#private-vlan primary
SwitchA(confg-vlan)#private-vlan association add 501
```

Configuration

- Interface fa0/1 and fa0/2 are connected to ComputerA and ComputerB and belong to the community VLAN 501.
- On the interface level I need to tell the switch that these are host ports by issuing the switchport mode private-vlan host command.
- I also have to use the switchport private vlan host-association command to tell the switch that VLAN 500 is the primary VLAN and 501 is the secondary VLAN.

```
SwitchA(confg)#interface range fa0/1 - 2
SwitchA(confg-if-range)#switchport mode private-vlan host
SwitchA(confg-if-range)#switchport private-vlan host-association 500 501
```

Configuration

- This is how I configure the promiscuous port.
- First I have to tell the switch that fa0/24 is a promiscuous port by typing the switchport mode private-vlan promiscuous command.
- I also have to map the VLANs by using the switchport private-vlan mapping command.

```
SwitchA(confg)#interface fa0/24
SwitchA(confg-if)#switchport mode private-vlan promiscuous
SwitchA(confg-if)#switchport private-vlan mapping 500 501
```

Configuration

- Here is the output for FastEthernet 0/1:

```
SwitchA#show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 500
(VLAN0500) 501 (VLAN0501)
Administrative private-vlan mapping: none
```

Configuration

- Let’s continue with the configuration of the isolated VLAN.
- The configuration is the same as the community VLAN but this time I’m using the **private vlan isolated** command.
- Don’t forget to add the association between the primary and secondary VLAN using the private-vlan association add command.
- The private-vlan primary command is obsolete because I already did this before, I’m just showing it to keep the configuration complete.

```
SwitchA(confg)#vlan 502
SwitchA(confg-vlan)#private-vlan isolated
SwitchA(confg-vlan)#vlan 500
SwitchA(confg-vlan)#private-vlan primary
SwitchA(confg-vlan)#private-vlan association add 502
```

Configuration

- This part is exactly the same as the configuration for the community VLAN but I'm configuring interface fa0/3 and fa0/4 which are connected to ComputerC and ComputerD.

```
SwitchA(config)#interface range fa0/3 - 4
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 500 502
```

```
SwitchA(config)#interface fa0/24
SwitchA(config-if)#switchport mode private-vlan promiscuous
SwitchA(config-if)#switchport private-vlan mapping 500 501 502
```