

Configuring Private VLANs on the PowerConnect 3448

Written by: Greg Gibbs
10/11/2005

Introduction:

VLANs (Virtual Local Area Networks) can be used to segment a Layer 2 device to provide basic security. Private VLANs (PVLANS) can be used to further segment the network and provide access to a shared resource without the use of a router or Layer 3 device.

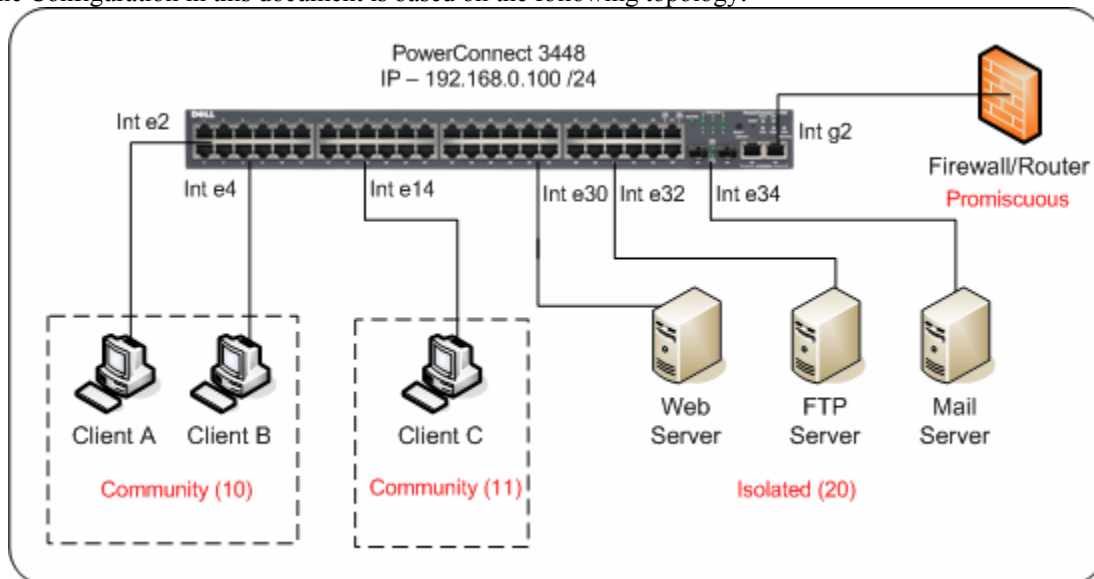
Prior to the implementation of Private VLANs, the only way to accomplish this goal was using a configuration commonly referred to as “port overlapping.” Port overlapping relies on preventing the switch from learning MAC addresses on particular VLANs. Since the switch cannot learn these MAC addresses, communication is established using unknown unicasts. Since bridges (switches) flood unknown unicasts, this generates excess broadcast traffic and presents security concerns. Private VLANs accomplish this goal without the excess traffic and security concerns.

Private VLAN implements three modes:

- ❖ **Isolated** – Ports configured as Isolated can communicate only with a Promiscuous port
- ❖ **Community** – Ports configured as Community can communicate with other ports in the same community and Promiscuous ports
- ❖ **Promiscuous** – Ports configured as Promiscuous can communicate with both the Isolated and Community ports

When Private VLANs are implemented, all ingress and egress (inbound and outbound) traffic is untagged. If a port configured in a Private VLAN mode receives a tagged frame, the frame will be dropped.

The Configuration in this document is based on the following topology:



****Note:** This configuration provides connectivity based strictly on OSI Layer 2. To provide this connectivity, all devices must be configured to use the same IP (Layer 3) subnet.

Basic Configuration:

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address 192.168.0.100 /24
console(config-if)# exit
```

Private VLAN Configuration:

(Configure the Primary VLAN – VLAN ID 1000 is used for this example)

```
console# configure
console(config)# vlan database
console(config-vlan)# vlan 1000
console(config-vlan)# exit
console(config)# interface vlan 1000
console(config-if)# private-vlan primary
```

(Specify the Community VLANs to be associated with the Primary VLAN)

```
console(config-if)# private-vlan community add 10-11
```

(Specify the Isolated VLAN to be associated with the Primary VLAN)

****Note:** Only one Isolated VLAN can be associated with a Primary VLAN

```
console(config-if)# private-vlan isolated 20
```

Interface Configuration:

```
console# configure
console(config)# interface range ethernet e2,e4
console(config-if)# switchport mode private-vlan community
console(config-if)# switchport private-vlan community 10
console(config-if)# exit
console(config)# interface ethernet e14
console(config-if)# switchport mode private-vlan community
console(config-if)# switchport private-vlan community 11
console(config-if)# exit
console(config)# interface range ethernet e30,e32,e34
console(config-if)# switchport mode private-vlan isolated
console(config-if)# switchport private-vlan isolated 1000 (Note the use of the Primary VLAN)
console(config-if)# exit
console(config)# interface ethernet g2
console(config-if)# switchport mode private-vlan promiscuous
console(config-if)# switchport private-vlan promiscuous 1000
```

Verify PVLAN Configuration:

```
console# show vlan private-vlan primary 1000  
Primary VLAN: 1000  
Isolated VLAN: 20  
Community VLANs: 10,11  
Promiscuous ports: g2  
Isolated ports: e30,e32,e34
```

Community	Ports
10	e(2,4)
11	e14

Conclusion:

With this configuration, the following goals are accomplished:

- ✓ Clients A and B can communicate with each other and the firewall/router. They cannot communicate with Client C or the servers
- ✓ Client C can only communicate with the firewall/router. If another client were added to Community 11, it would be able to communicate with Client C.
- ✓ The servers can only communicate with the firewall/router. If security on one of the servers is compromised, this prevents the attacker from using this server to attack other servers/clients.