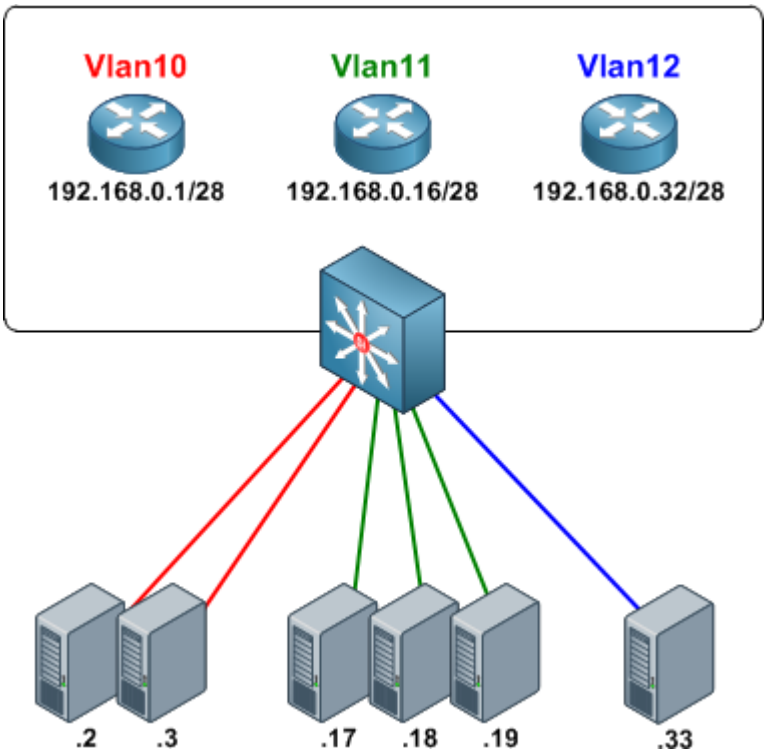
Basic Private VLAN Configuration

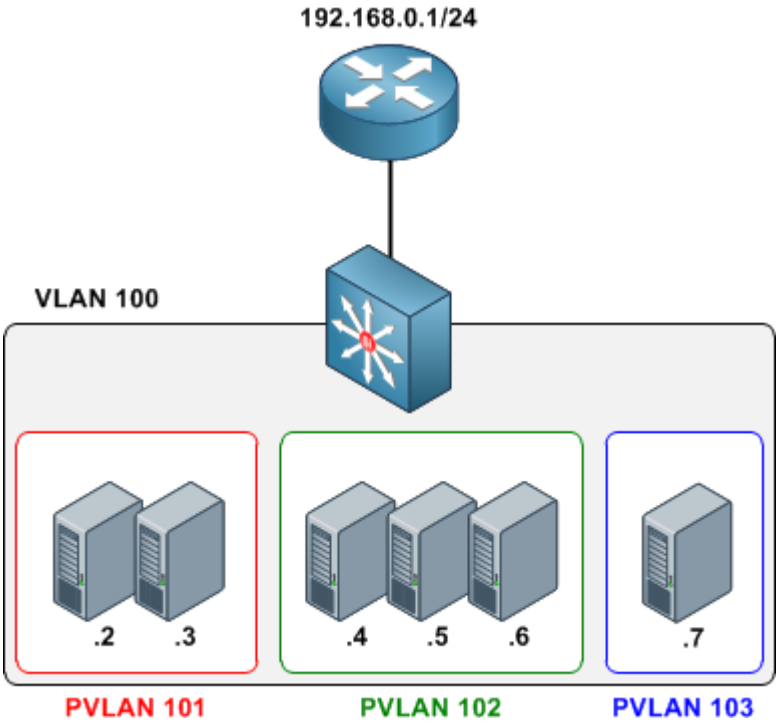
By stretch | Monday, August 30, 2010 at 12:53 a.m. UTC

Now that the community lab has been equipped with a Catalyst 3560, I have finally been able to write about private VLANs (which are supported only on Catalyst 3560 and higher switches). This article discusses the concept of private VLANs and includes a basic configuration example, with more complex configurations deferred for future articles.

Private VLANs were developed to provide the ability to isolate end hosts at layer two. To understand the motivation behind this feature, consider a colocation environment in which the network operator must connect servers belonging to different customers to the Internet. These servers must all be able to reach their first-hop router, but for security reasons, servers belonging to one customer must not be able to communicate with servers belonging to another. An obvious design solution for these requirements is to place each customer's servers in a separate VLAN, which also requires the assignment of a separate IP subnet per customer (even if they have only one server).



This approach wastes both VLAN IDs and IP address space. Private VLANs were introduced as a more elegant alternative, allowing multiple devices to reside in the same IP subnet, yet remain isolated from one another at layer two.



A private VLAN is defined as a pairing of a *primary VLAN* with a *secondary VLAN*. Primary VLANs are the normal VLANs we all know and love. Secondary VLANs use the same VLAN ID range and are defined in the same manner as primary VLANs, but are specially designated to operate as secondary VLANs in one of two modes:

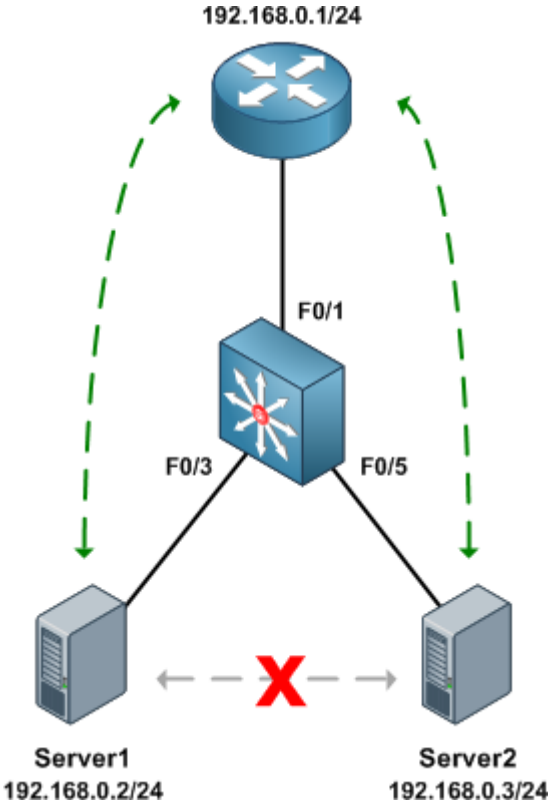
- **Isolated** - The end points of all ports assigned to an isolated private VLAN cannot communicate with one another, nor with host ports in any other private VLANs.
- **Community** - End points attached to community ports can communicate with one another, but not with ports in other private VLANs.

An access port assigned to a private VLAN operates in one of two modes:

- **Host** - The port inherits its behavior from the type of private VLAN it is assigned to.
- **Promiscuous** - The port can communicate with any other private VLAN port in the same primary VLAN.

Configuring Private VLANs

We'll configure an isolated private VLAN to allow two servers owned by different customers in the same IP subnet to communicate with their first-hop router, but not with one another.



Before getting started with private VLAN configuration, ensure that VTP has been set to transparent mode. There are numerous reasons for running VTP in transparent mode beyond the scope of this article, and to enable private VLANs it's explicitly required.

```
Switch(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
```

As with normal VLANs, private VLANs must be created before they can be used. Upon creation, we must also define a type (isolated, community, or primary) for each. We'll create our secondary VLANs first, then our primary VLAN. The secondary private VLAN is mapped under the configuration of the primary private VLAN.

```
Switch(config)# vlan 101
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# vlan 100
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 101
```

Our completed VLAN configuration looks like this:

```
vlan 100
 private-vlan primary
 private-vlan association 101
!
vlan 101
 private-vlan isolated
```

Next, we designate our private VLAN interfaces. Our uplink port to the router will be set to promiscuous mode, with the primary VLAN mapped to the secondary VLAN.

```
Switch(config)# interface f0/1
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 100 101
```

Our two server ports will be configured in host mode:

```
Switch(config)# interface f0/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 101
Switch(config-if)# interface f0/5
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 101
```

At this point our private VLAN configuration is complete. We can verify private VLAN interface assignments with the command `show vlan private-vlan`:

```
Switch# show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
100     101       isolated          Fa0/1, Fa0/3, Fa0/5
Switch# show interface status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    100        a-full  a-100 10/100BaseTX
Fa0/2                        notconnect   1            auto   auto 10/100BaseTX
Fa0/3                        connected    100,101    a-full  a-100 10/100BaseTX
Fa0/4                        notconnect   1            auto   auto 10/100BaseTX
Fa0/5                        connected    100,101    a-full  a-100 10/100BaseTX
Fa0/6                        notconnect   1            auto   auto 10/100BaseTX
Fa0/7                        notconnect   1            auto   auto 10/100BaseTX
...
```

The command `show interface switchport` is also useful for examining private VLAN details per interface.

Finally, we can verify that the router can communicate with both servers, but the servers cannot communicate directly with one another.

```
Router# ping 192.168.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Router# ping 192.168.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Server1# ping 192.168.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Further Reading

- Configuring Private VLANs - Catalyst 3560 configuration guide
- RFC 5517 - Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment

Posted in Switching