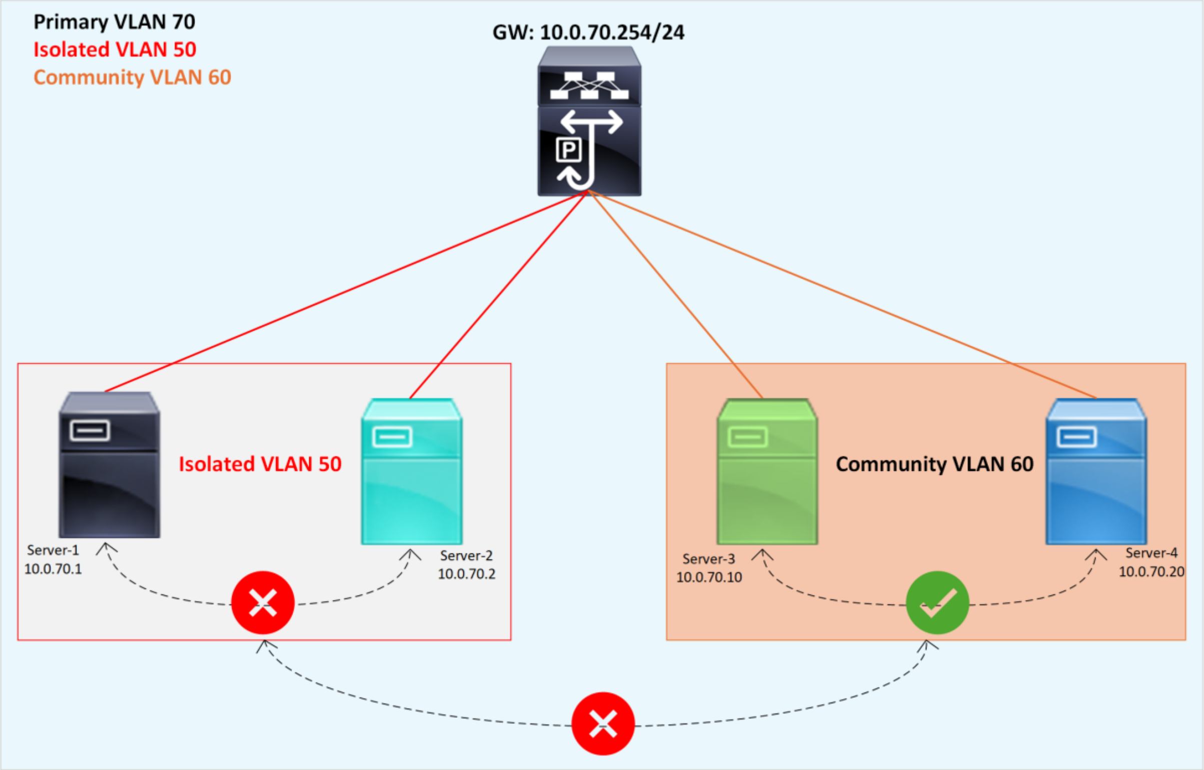
Private VLANs on Cisco Nexus 9000



Lab By: Titus Majeza

Overview

Private VLANs (PVLANs) allow for the segmentation of a broadcast domain (VLAN) into multiple subdomains. The partitioning of a single broadcast domain into multiple broadcast subdomains enhances security and isolation at a Layer 2 level. A Private VLAN domain contains 2 types of VLANs i.e. primary and secondary. The secondary VLAN is nested in the primary VLAN and it has 2 types of subdomains; **Isolated** and **Community**.

An important element that belongs in the primary VLAN is the *“promiscuous port”.* The promiscuous port is able to communicate with all hosts, regardless of the VLAN that they reside in. The promiscuous port allows endpoints across all subdomains to communicate with the default gateway, shared services (DHCP server, NTP server etc).

1. **Primary VLAN:** this is where the broadcast domain and the promiscuous port are defined. The secondary VLANs are associated to this primary VLAN.

2. **Secondary VLAN:** the secondary VLANs defines the subdomains which are associated with the primary VLAN.

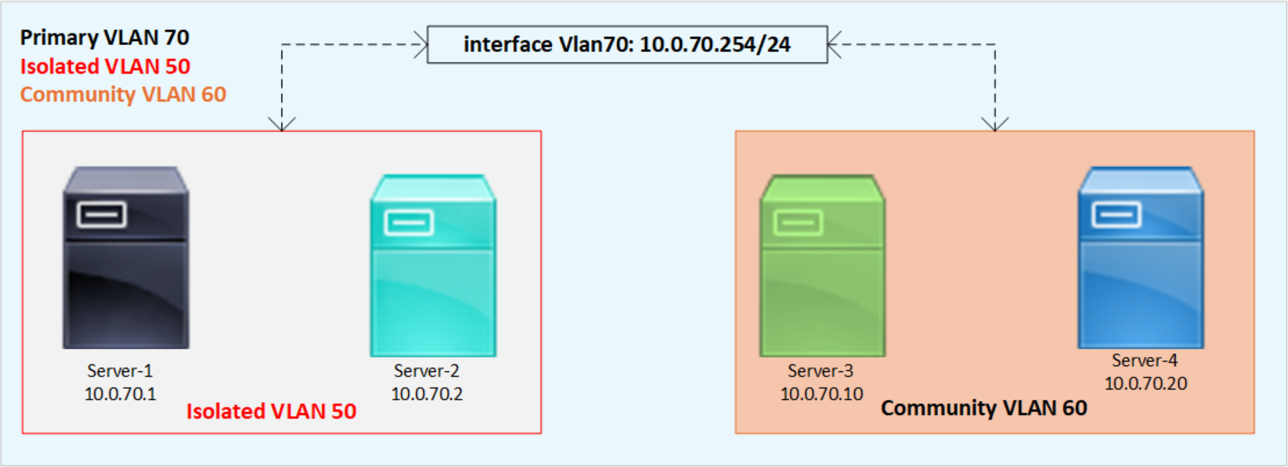
    a. *Isolated VLAN* – A host/endpoint that belongs to an isolated VLAN will only be able to communicate with a promiscuous port. It cannot be able to communicate with any host defined in the same isolated VLAN and other hosts that belon in other secondary VLANs (isolated and community).

    b. *Community VLAN* – A host/endpoint that belongs to a community VLAN is able to communicate with other hosts within the same community VLAN and with the promiscuous port in the primary VLAN. The host however is not able to communicate with other hosts from other secondary VLANs (isolated and community).

This lab dives into the configuration and verification of a Private VLAN domain. Furthermore, the lab will demonstrate the communication restrictions within each configured VLAN.

Lab-Setup

This lab consists of one primary VLAN (VLAN70), one isolated VLAN (VLAN50) and one community VLAN (VLAN60). The primary SVI where the default gateway IP address is defined will be configured as the promiscuous port. Two endpoints belong to the isolated VLAN and another set of two endpoints belongs to the community VLAN.



Note
This lab was conducted in a controlled environment. Any configurations in a production network should be implemented during a designated maintenance window. Additionally, always refer to official Cisco documentation relevant to your specific hardware and software.

Private VLANs Configurations and Verifications

The configuration of a Private VLAN domain in this lab consists of the following steps:

1. Enable the *private-vlan* feature.
2. Define the required primary and secondary VLANs, along with their private-vlan type (primary, isolated, community)
3. Associate the secondary VLANs to the primary VLAN.
4. Define the Layer 3 SVI of the Primary VLAN and associate it with the secondary VLANs.
5. Configure the access ports where the hosts will be connected to.

1. Enable the *private-vlan* feature

```
ACC-DIST# conf t
Enter configuration commands, one per line. End with CNTL/Z.
ACC-DIST(config)# feature private-vlan
ACC-DIST(config)# exit
ACC-DIST#
ACC-DIST# show feature | in private-vlan
private-vlan           1          enabled
```

2. Define the required primary and secondary VLANs, along with their private-vlan type (primary, isolated, community)

```
ACC-DIST# show run vlan

!Command: show running-config vlan
vlan 1,50,60,70
vlan 50
  private-vlan isolated
vlan 60
  private-vlan community
vlan 70
  private-vlan primary
```

Verify that the required VLANs have been configured and the private-vlan type is correct.

```
ACC-DIST# show vlan private-vlan type
Vlan Type
---- -----------------
50   isolated
60   community
70   primary
```

3. Associate the secondary VLANs to the primary VLAN.

```
ACC-DIST# show run vlan 70

!Command: show running-config vlan 70

vlan 70
  private-vlan primary
  private-vlan association 50,60
```

4. Define the Layer 3 SVI of the Primary VLAN and associate it with the secondary VLANs.

```
ACC-DIST# show run interface Vlan70

!Command: show running-config interface Vlan70

interface Vlan70
  no shutdown
  private-vlan mapping 50,60
  ip address 10.0.70.254/24
```

> **Note**
>
> Do not configure VLAN interfaces for secondary VLANs.
>
> - If you try to configure a VLAN with an active VLAN network interface as a secondary VLAN, the configuration is not allowed until you disable the VLAN interface.
> - If you try to create and enable a VLAN network interface on a VLAN that is configured as a secondary VLAN, that VLAN interface remains disabled, and the system returns an error.
>
> When the primary VLAN is associated with and mapped to the secondary VLAN, any configuration on the primary VLAN is propagated to the secondary VLANs.

Verify the mapping of the SVI for the primary VLAN and associated secondary VLANs.

```
ACC-DIST# show interface vlan 70 private-vlan mapping
Interface Secondary VLAN
--------- ----------------------------------------------------------------
vlan70    50   60
ACC-DIST#
ACC-DIST# show interface private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan70    50             isolated
vlan70    60             community
```

5. Configure the access ports where the hosts will be connected to.

```
ACC-DIST# show run int eth1/1
!Command: show running-config interface Ethernet1/1
interface Ethernet1/1
  description Server-1(isolated)
  switchport
  switchport mode private-vlan host
  switchport private-vlan host-association 70 50
  spanning-tree port type edge
  no shutdown
```

```
ACC-DIST# show run int eth1/3
!Command: show running-config interface Ethernet1/3
interface Ethernet1/3
  description Server-2(isolated)
  switchport
  switchport mode private-vlan host
  switchport private-vlan host-association 70 50
  spanning-tree port type edge
  no shutdown
!
ACC-DIST# show run int eth1/4

!Command: show running-config interface Ethernet1/4
interface Ethernet1/4
  description Server-3(community)
  switchport
  switchport mode private-vlan host
  switchport private-vlan host-association 70 60
  spanning-tree port type edge
  no shutdown
!
ACC-DIST# show run int eth1/15

!Command: show running-config interface Ethernet1/15
interface Ethernet1/15
  description Server-4(community)
  switchport
  switchport mode private-vlan host
  switchport private-vlan host-association 70 60
  spanning-tree port type edge
  no shutdown
```

Verify that the ports are successfully configured as private-vlan host ports.

```
ACC-DIST# show interface Eth1/1 | grep Port
  Port mode is Private-vlan host
ACC-DIST#
ACC-DIST# show interface Eth1/2 | grep Port
ACC-DIST#
ACC-DIST# show interface Eth1/4 | grep Port
  Port mode is Private-vlan host
ACC-DIST#
ACC-DIST# show interface Eth1/15 | grep Port
  Port mode is Private-vlan host
```

Verify the mapping of the primary VLANs, the associated secondary VLANs, and the host ports.

```
ACC-DIST# show vlan private-vlan
Primary  Secondary  Type             Ports
-------  ---------  ---------------  -------------------------------------------
70       50         isolated         Eth1/1, Eth1/3
70       60         community        Eth1/4, Eth1/15
```

Note

An isolated or community VLAN can be associated with only one primary VLAN.

Servers MAC and IP addresses information:

```
root@server-1#ifconfig Eth1-1
Eth1-1    Link encap:Ethernet  HWaddr b4:de:31:99:30:ff
          inet addr:10.0.70.1  Bcast:10.0.70.255  Mask:255.255.255.0
!
root@server-2#ifconfig Eth1-3
Eth1-3    Link encap:Ethernet  HWaddr 38:0e:4d:8f:7a:61
          inet addr:10.0.70.2  Bcast:10.0.70.255  Mask:255.255.255.0
!
root@server-3#ifconfig Eth1-3
Eth1-3    Link encap:Ethernet  HWaddr 00:f6:63:11:0b:f1
          inet addr:10.0.70.10  Bcast:10.0.70.255  Mask:255.255.255.0
!
root@server-4#ifconfig Eth1-25
Eth1-25   Link encap:Ethernet  HWaddr f8:0f:6f:15:01:07
          inet addr:10.0.70.20  Bcast:10.0.70.255  Mask:255.255.255.0
```

Access/Distribution Switch MAC address table:

```
ACC-DIST# show mac address-table dynamic
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
*   70     00f6.6311.0bf1   dynamic  0         F      F    Eth1/4
*   70     380e.4d8f.7a61   dynamic  0         F      F    Eth1/3
*   70     b4de.3199.30ff   dynamic  0         F      F    Eth1/1
*   70     f80f.6f15.0107   dynamic  0         F      F    Eth1/15
```

All hosts MAC addresses are shown to be a part of the Primary VLAN 70, despite being in their respective subdomains (VLAN 50 and VLAN 60).

Access/Distribution Switch ARP table:

```
ACC-DIST# show ip arp
Total number of entries: 4
Address         Age       MAC Address     Interface       Flags
10.0.70.1       00:03:26  b4de.3199.30ff  Vlan70
10.0.70.2       00:03:09  380e.4d8f.7a61  Vlan70
10.0.70.10      00:03:09  00f6.6311.0bf1  Vlan70
10.0.70.20      00:00:54  f80f.6f15.0107  Vlan70
```

Server-1 communication tests:

```
Server-1 (isolated) can communicate only with the default gateway:
root@server-1#ping -I 10.0.70.1 10.0.70.254
PING 10.0.70.254 (10.0.70.254) from 10.0.70.1 : 56(84) bytes of data.
64 bytes from 10.0.70.254: icmp_seq=1 ttl=255 time=0.648 ms
64 bytes from 10.0.70.254: icmp_seq=2 ttl=255 time=0.636 ms
64 bytes from 10.0.70.254: icmp_seq=3 ttl=255 time=0.660 ms
64 bytes from 10.0.70.254: icmp_seq=4 ttl=255 time=0.560 ms
^C
--- 10.0.70.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 36ms
rtt min/avg/max/mdev = 0.560/0.626/0.660/0.039 ms
```

```
root@server-1#
Server-1 (isolated) cannot communicate with Server-2 that is in the same isolated VLAN:
root@server-1#ping -I 10.0.70.1 10.0.70.2
PING 10.0.70.2 (10.0.70.2) from 10.0.70.1 : 56(84) bytes of data.
From 10.0.70.1 icmp_seq=1 Destination Host Unreachable
From 10.0.70.1 icmp_seq=2 Destination Host Unreachable
From 10.0.70.1 icmp_seq=3 Destination Host Unreachable
^C
--- 10.0.70.2 ping statistics ---
6 packets transmitted, 0 received, +3 errors, 100% packet loss, time 65ms
pipe 4
root@server-1#
Server-1 (isolated) cannot communicate with any Server in the community VLAN.
root@server-1#ping -I 10.0.70.1 10.0.70.10
PING 10.0.70.10 (10.0.70.10) from 10.0.70.1 : 56(84) bytes of data.
From 10.0.70.1 icmp_seq=1 Destination Host Unreachable
From 10.0.70.1 icmp_seq=2 Destination Host Unreachable
From 10.0.70.1 icmp_seq=3 Destination Host Unreachable
^C
--- 10.0.70.10 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 52ms
pipe 4
```

Server-2 communication tests:

```
Server-2 (isolated) can communicate only with the default gateway:
root@server-2#ping -I 10.0.70.2 10.0.70.254
PING 10.0.70.254 (10.0.70.254) from 10.0.70.2 : 56(84) bytes of data.
64 bytes from 10.0.70.254: icmp_seq=1 ttl=255 time=0.616 ms
64 bytes from 10.0.70.254: icmp_seq=2 ttl=255 time=0.643 ms
64 bytes from 10.0.70.254: icmp_seq=3 ttl=255 time=0.588 ms
64 bytes from 10.0.70.254: icmp_seq=4 ttl=255 time=0.670 ms
^C
--- 10.0.70.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.588/0.629/0.670/0.035 ms
root@server-2#

Server-2 (isolated) cannot communicate with Server-1 that is in the same isolated VLAN:
root@server-2#ping -I 10.0.70.2 10.0.70.1
PING 10.0.70.1 (10.0.70.1) from 10.0.70.2 : 56(84) bytes of data.
From 10.0.70.2 icmp_seq=1 Destination Host Unreachable
From 10.0.70.2 icmp_seq=2 Destination Host Unreachable
From 10.0.70.2 icmp_seq=3 Destination Host Unreachable
^C
--- 10.0.70.1 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 4007ms
pipe 4
root@server-2#
```

Server-3 communication tests:

```
Server-3 (community) can communicate with the default gateway:
root@server-3#ping -I 10.0.70.10 10.0.70.254
PING 10.0.70.254 (10.0.70.254) from 10.0.70.10 : 56(84) bytes of data.
64 bytes from 10.0.70.254: icmp_seq=1 ttl=255 time=0.733 ms
64 bytes from 10.0.70.254: icmp_seq=2 ttl=255 time=0.681 ms
64 bytes from 10.0.70.254: icmp_seq=3 ttl=255 time=0.747 ms
64 bytes from 10.0.70.254: icmp_seq=4 ttl=255 time=0.713 ms
^C
--- 10.0.70.254 ping statistics ---
```

```
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.681/0.718/0.747/0.036 ms
root@server-3#
Server-3 (community) can communicate with Server-4 in the same Community VLAN.
root@server-3#ping -I 10.0.70.10 10.0.70.20
PING 10.0.70.20 (10.0.70.20) from 10.0.70.10 : 56(84) bytes of data.
64 bytes from 10.0.70.20: icmp_seq=1 ttl=255 time=0.509 ms
64 bytes from 10.0.70.20: icmp_seq=2 ttl=255 time=0.563 ms
64 bytes from 10.0.70.20: icmp_seq=3 ttl=255 time=0.521 ms
64 bytes from 10.0.70.20: icmp_seq=4 ttl=255 time=0.551 ms
64 bytes from 10.0.70.20: icmp_seq=5 ttl=255 time=0.532 ms
^C
--- 10.0.70.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.509/0.535/0.563/0.024 ms
root@server-3#
Server-3 (community) cannot communicate with any Server in the Isolated VLAN.
root@server-3#ping -I 10.0.70.10 10.0.70.2
PING 10.0.70.2 (10.0.70.2) from 10.0.70.10 : 56(84) bytes of data.
From 10.0.70.10 icmp_seq=1 Destination Host Unreachable
From 10.0.70.10 icmp_seq=2 Destination Host Unreachable
From 10.0.70.10 icmp_seq=3 Destination Host Unreachable
^C
--- 10.0.70.2 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 4007ms
pipe 4
root@server-3#
```

Server-4 communication tests:

```
Server-4 (community) can communicate with the default gateway:
root@server-4#ping -I 10.0.70.20 10.0.70.254
PING 10.0.70.254 (10.0.70.254) from 10.0.70.20 : 56(84) bytes of data.
64 bytes from 10.0.70.254: icmp_seq=1 ttl=255 time=0.519 ms
64 bytes from 10.0.70.254: icmp_seq=2 ttl=255 time=0.598 ms
64 bytes from 10.0.70.254: icmp_seq=3 ttl=255 time=0.579 ms
64 bytes from 10.0.70.254: icmp_seq=4 ttl=255 time=0.592 ms
^C
--- 10.0.70.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 42ms
rtt min/avg/max/mdev = 0.519/0.572/0.598/0.031 ms
root@server-4#
Server-4 (community) can communicate with Server-3 in the same Community VLAN.
root@server-4#ping -I 10.0.70.20 10.0.70.10
PING 10.0.70.10 (10.0.70.10) from 10.0.70.20 : 56(84) bytes of data.
64 bytes from 10.0.70.10: icmp_seq=1 ttl=255 time=1.50 ms
64 bytes from 10.0.70.10: icmp_seq=2 ttl=255 time=1.05 ms
64 bytes from 10.0.70.10: icmp_seq=3 ttl=255 time=1.07 ms
64 bytes from 10.0.70.10: icmp_seq=4 ttl=255 time=1.18 ms
^C
--- 10.0.70.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 1.053/1.202/1.502/0.179 ms
root@server-4#
Server-4 (community) cannot communicate with any Server in the Isolated VLAN.
root@server-4#ping -I 10.0.70.20 10.0.70.1
PING 10.0.70.1 (10.0.70.1) from 10.0.70.20 : 56(84) bytes of data.
From 10.0.70.20 icmp_seq=1 Destination Host Unreachable
From 10.0.70.20 icmp_seq=2 Destination Host Unreachable
From 10.0.70.20 icmp_seq=3 Destination Host Unreachable
^C
```

```
--- 10.0.70.1 ping statistics ---
4 packets transmitted, 0 received, +3 errors, 100% packet loss, time 51ms
pipe 4
root@server-4#
```

Communication Matrix:

	Default Gateway	**Server-1**	**Server-2**	**Server-3**	**Server-4**
Default Gateway	⊗	✅	✅	✅	✅
Server-1	✅	⊗	❌	❌	❌
Server-2	✅	❌	⊗	❌	❌
Server-3	✅	❌	❌	⊗	✅
Server-4	✅	❌	❌	✅	⊗

This lab effectively demonstrated the implementation and verifications of Private VLANs on a Cisco Nexus 9000 switch. The lab highlighted:

1. Essential configurations for setting up PVLANs.
2. Verification commands to ensure proper PVLAN functionality.
3. Communication tests between hosts in isolated and community VLANs.

The results conclusively showed that PVLANs successfully achieve Layer 2 network segmentation, providing enhanced security and traffic isolation within a shared network environment.

References

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/92x/Layer-2_switching/configuration/guide/b-cisco-nexus-9000-nx-os-layer-2-switching-configuration-guide-92x/b-cisco-nexus-9000-nx-os-layer-2-switching-configuration-guide-92x_chapter_0111.html