

HPE Synergy and Cisco Nexus Private VLAN Technical Review

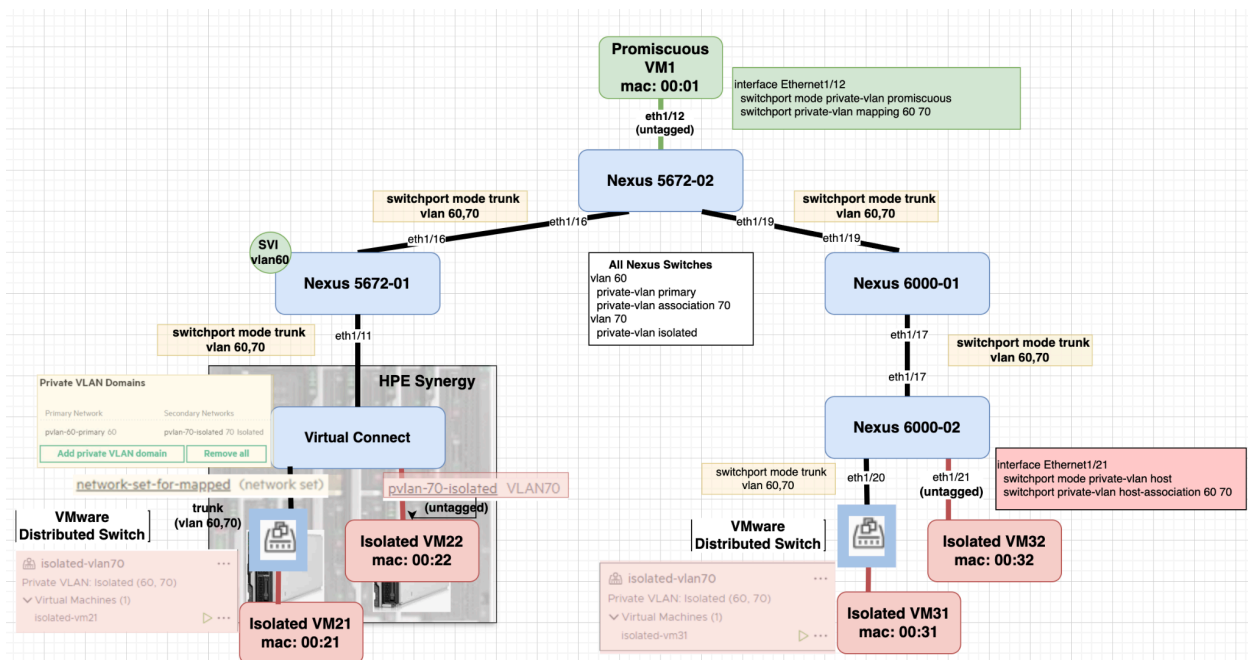
This technical document is designed to provide users with a clear understanding of how to configure Private VLANs (PVLAN) between Cisco Nexus switches and HPE Synergy. Additionally, it illustrates the traffic flow between Promiscuous and Isolated VMs.

The key takeaway from this document is the following:

When configuring Cisco Nexus PVLAN, any switch ports connecting to HPE Synergy or rack servers running VMware DVS PVLAN must be configured as standard trunk ports, not as private-vlan promiscuous or isolated trunks.

This document serves as an addition to the original technical document, "Private VLAN in OneView 4.20," which remains accurate and valid. The latest tests were conducted in 2025 on HPE Synergy OneView 9.20 and 9.30. These features have been available for some time, and the fundamental concepts outlined in the previous white paper remain unchanged. On the Cisco side, although the lab tests utilized the classic Nexus 5500 and 6000 Series switches, the concepts are applicable to the latest Nexus 9000 series switches.

The diagram below illustrates the device connections. A Promiscuous VM is connected at the top to a Nexus switch. On the left side of the switch branch, Synergy VMs are connected, while on the right side, VMs on the rack server are connected. This setup helps users understand how PVLAN can be configured on Cisco switches without involving Synergy.



The image contains two network diagrams illustrating traffic forwarding between VMs across multiple switches and VLANs.

Left Diagram: Traffic From Isolated to Promiscuous

- Top:** Promiscuous VM MAC1 (green box).
- Switches:** Three switches (Switch 1, Switch 2, Switch 3) in the center, each with a "MAC Look up" section.
- Left Side (Promiscuous VLAN - green):** Contains MAC1, MAC2, and MAC3.
- Right Side (Isolated VLAN - red):** Contains MAC4, MAC5, and MAC6.
- Bottom:** Isolated VM MAC4 (red box).
- Flow:** A solid arrow points from the Isolated VM MAC4 up through the switches to the Promiscuous VM MAC1. Dashed arrows indicate MAC lookups at each switch. A curved arrow points from the isolated side towards the promiscuous side.

Traffic From Isolated to Promiscuous

- * Forwarding using secondary VLAN
- * Lookup in primary VLAN

Right Diagram: Traffic From Promiscuous to Isolated

- Top:** Promiscuous VM MAC1 (green box).
- Switches:** Three switches (Switch 1, Switch 2, Switch 3) in the center, each with a "MAC Look up" section.
- Left Side (Promiscuous VLAN - green):** Contains MAC1, MAC2, and MAC3.
- Right Side (Isolated VLAN - red):** Contains MAC4, MAC5, and MAC6.
- Bottom:** Isolated VM MAC4 (red box).
- Flow:** A solid arrow points from the Promiscuous VM MAC1 down through the switches to the Isolated VM MAC4. Dashed arrows indicate MAC lookups at each switch. A curved arrow points from the promiscuous side towards the isolated side.

Traffic From Promiscuous to Isolated

- * Forwarding using primary VLAN
- * Lookup in primary and secondary VLAN

No.	Time	Source	Destination	ERSPAN.vlan	VLAN ID	Protocol	Length	Info
6	19:56:21.263482	192.168.60.32	192.168.60.1		70	ICMP	106	Echo (ping) request
7	19:56:21.263677	192.168.60.1	192.168.60.32		60	ICMP	106	Echo (ping) reply
27	19:56:22.263580	192.168.60.32	192.168.60.1		70	ICMP	106	Echo (ping) request
28	19:56:22.263797	192.168.60.1	192.168.60.32		60	ICMP	106	Echo (ping) reply
64	19:56:23.263586	192.168.60.32	192.168.60.1		70	ICMP	106	Echo (ping) request
65	19:56:23.263750	192.168.60.1	192.168.60.32		60	ICMP	106	Echo (ping) reply

▶ Frame 6: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{09BA9358-74}

▶ Ethernet II, Src: VMware_00:00:32 (00:50:56:00:00:32), Dst: VMware_00:00:01 (00:50:56:00:00:01)

▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 70

▶ Internet Protocol Version 4, Src: 192.168.60.32, Dst: 192.168.60.1

▶ Internet Control Message Protocol

Below is the Cisco SPAN session capturing traffic that shows promiscuous VM ping reply activity to isolated VM within primary VLAN 60.

ip.addr == 192.168.60.32									
No.	Time	Source	Destination	ERSPAN.vlan	VLAN ID	Protocol	Length	Info	
6	19:56:21.263482	192.168.60.32	192.168.60.1	70	ICMP	106	Echo (ping)	request	
7	19:56:21.263677	192.168.60.1	192.168.60.32	60	ICMP	106	Echo (ping)	reply	
27	19:56:22.263580	192.168.60.32	192.168.60.1	70	ICMP	106	Echo (ping)	request	
28	19:56:22.263797	192.168.60.1	192.168.60.32	60	ICMP	106	Echo (ping)	reply	
64	19:56:23.263586	192.168.60.32	192.168.60.1	70	ICMP	106	Echo (ping)	request	
65	19:56:23.263750	192.168.60.1	192.168.60.32	60	ICMP	106	Echo (ping)	reply	

> Frame 7: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{09BA9358-74...}								0000	00 50
> Ethernet II, Src: VMware_00:00:01 (00:50:56:00:00:01), Dst: VMware_00:00:32 (00:50:56:00:00:32)								0010	08 00
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 60								0020	3c 01
> Internet Protocol Version 4, Src: 192.168.60.1, Dst: 192.168.60.32								0030	93 67
> Internet Control Message Protocol								0040	12 13
								0050	22 23
								0060	32 33

Nexus also has two PVLAN trunk configuration options named Promiscuous trunk and Secondary trunk.

```
hst-5672-02(config-if)# switchport mode private-vlan trunk ?
promiscuous  Port mode trunk promiscuous
secondary    Port mode trunk isolated
```

Neither of these two modes supports the transmission of both primary and secondary VLANs over the port, which is necessary for PVLAN-aware devices to forward traffic between each other. As a result, these modes should not be used for connections between PVLAN-aware devices, such as Nexus to Synergy Virtual Connect or Nexus to VMware DVS.

Some Cisco PVLAN documentation like the following

[VLAN Configuration Guide, Cisco IOS XE Amsterdam 17.3.x \(Catalyst 9400 Switches\) - Configuring Private VLANs \[Support\]](#)

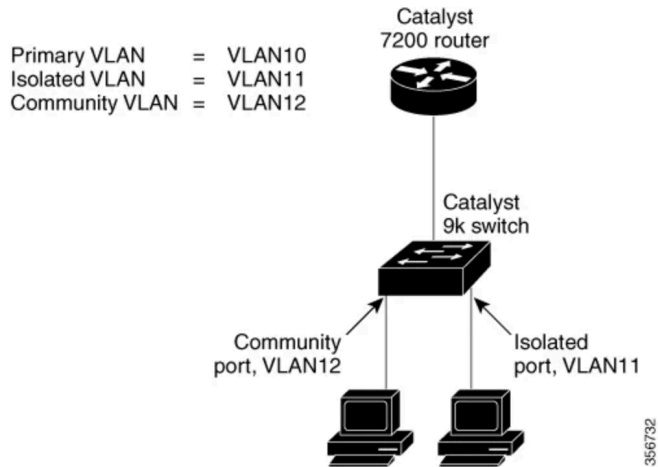
has good diagrams explaining the use cases for promiscuous and secondary private-vlan trunk.

In a promiscuous private-vlan trunk, only primary VLANs and regular VLANs are allowed over the port.

Promiscuous Private VLAN Trunk Ports

Promiscuous private VLAN trunk ports are used in situations where a PVLAN promiscuous host port is normally used, but where it is necessary to carry multiple VLANs, either normal VLANs or multiple PVLAN domains. You can connect to an upstream router that does not support PVLANS, such as a Cisco 7200 router.

Figure 4. Promiscuous PVLAN Trunk Ports

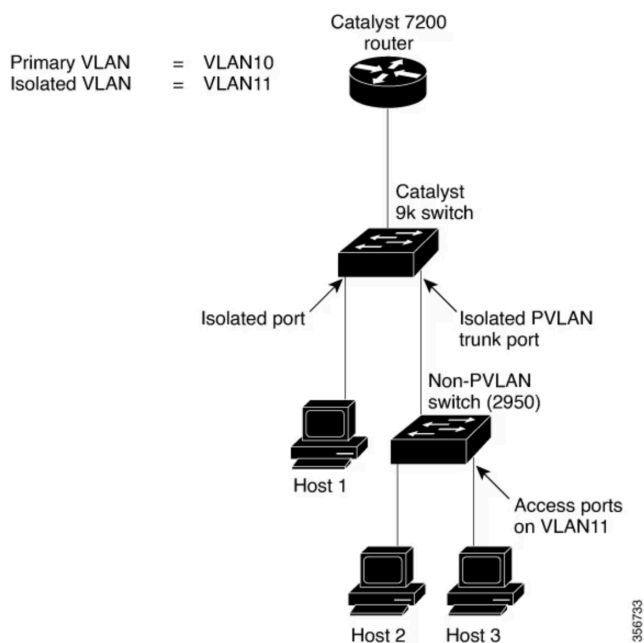


In an isolated private-vlan trunk, only isolated VLANs and regular VLANs are allowed over the port.

Isolated Private VLAN Trunk Ports

You use isolated PVLAN trunk ports if you anticipate using PVLAN isolated host ports to carry multiple VLANs, either normal VLANs or multiple PVLAN domains. You can connect a downstream switch that does not support PVLANS, such as a Catalyst 2950.

Figure 3. Isolated PVLAN Trunk Ports



The following captures illustrate when PVLAN works correctly, all switches store and display promiscuous and isolated VMs in their own perspective VLANs like regular VLANs. However, the PVLAN traffic forwarding has different MAC lookup mechanisms like explained earlier.

```
hst-n6k-01# show mac address-table vlan 60
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen, + - primary entry using vPC Peer-Link
VLAN    MAC Address      Type      age      Secure NTFY  Ports/SWID.SSID.LID
-----+-----+-----+-----+-----+-----
* 60     002a.6ae0.a601    dynamic   60        F    F  Eth1/19
* 60     0050.5600.0001    dynamic   20        F    F  Eth1/19
hst-n6k-01# show mac address-table vlan 70
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen, + - primary entry using vPC Peer-Link
VLAN    MAC Address      Type      age      Secure NTFY  Ports/SWID.SSID.LID
-----+-----+-----+-----+-----+-----
* 70     0050.5600.0021    dynamic   30        F    F  Eth1/19
* 70     0050.5600.0022    dynamic   60        F    F  Eth1/19
* 70     0050.5600.0031    dynamic   20        F    F  Eth1/17
* 70     0050.5600.0032    dynamic   20        F    F  Eth1/17
hst-n6k-01#
```

```
hst-n6k-02# show mac address-table vlan 60
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen, + - primary entry using vPC Peer-Link
VLAN    MAC Address      Type      age      Secure NTFY  Ports/SWID.SSID.LID
-----+-----+-----+-----+-----+-----
* 60     002a.6ae0.a601    dynamic   10        F    F  Eth1/17
* 60     0050.5600.0001    dynamic   10        F    F  Eth1/17
hst-n6k-02# show mac address-table vlan 70
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen, + - primary entry using vPC Peer-Link
VLAN    MAC Address      Type      age      Secure NTFY  Ports/SWID.SSID.LID
-----+-----+-----+-----+-----+-----
* 70     0050.5600.0021    dynamic   10        F    F  Eth1/17
* 70     0050.5600.0022    dynamic   10        F    F  Eth1/17
* 70     0050.5600.0031    dynamic   10        F    F  Eth1/20
* 70     0050.5600.0032    dynamic   10        F    F  Eth1/21
hst-n6k-02#
```

```
hst-5672-02# show mac address-table vlan 60
```

```
Legend:
```

```
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
```

```
age - seconds since last seen,+ - primary entry using vPC Peer-Link
```

VLAN	MAC Address	Type	age	Secure	NTFY	Ports/SWID.SSID.LID
* 60	002a.6ae0.a601	dynamic	110	F	F	Eth1/16
* 60	0050.5600.0001	dynamic	0	F	F	Eth1/12

```
hst-5672-02# show mac address-table vlan 70
```

```
Legend:
```

```
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
```

```
age - seconds since last seen,+ - primary entry using vPC Peer-Link
```

VLAN	MAC Address	Type	age	Secure	NTFY	Ports/SWID.SSID.LID
* 70	0050.5600.0021	dynamic	0	F	F	Eth1/16
* 70	0050.5600.0022	dynamic	80	F	F	Eth1/16
* 70	0050.5600.0031	dynamic	0	F	F	Eth1/19
* 70	0050.5600.0032	dynamic	0	F	F	Eth1/19

```
hst-5672-02#
```

```
hst-5672-01# show mac address-table vlan 60
```

```
Legend:
```

```
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
```

```
age - seconds since last seen,+ - primary entry using vPC Peer-Link
```

VLAN	MAC Address	Type	age	Secure	NTFY	Ports/SWID.SSID.LID
* 60	0050.5600.0001	dynamic	0	F	F	Eth1/16

```
hst-5672-01# show mac address-table vlan 70
```

```
Legend:
```

```
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
```

```
age - seconds since last seen,+ - primary entry using vPC Peer-Link
```

VLAN	MAC Address	Type	age	Secure	NTFY	Ports/SWID.SSID.LID
* 70	0050.5600.0021	dynamic	10	F	F	Eth1/11
* 70	0050.5600.0022	dynamic	10	F	F	Eth1/11
* 70	0050.5600.0031	dynamic	120	F	F	Eth1/16
* 70	0050.5600.0032	dynamic	300	F	F	Eth1/16

```
hst-5672-01#
```