

Private VLAN in OneView 4.20

Thursday, April 4, 2019

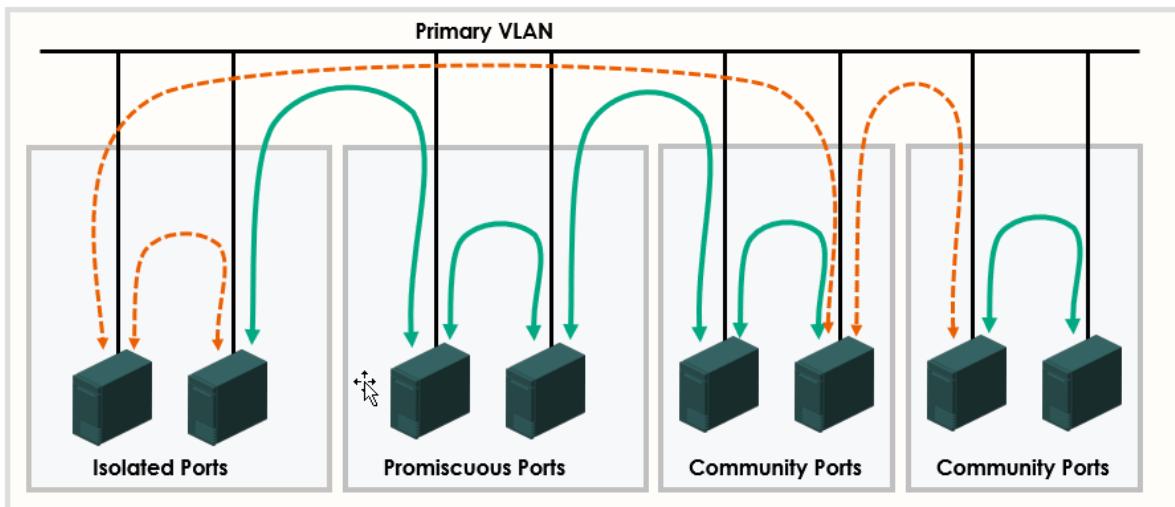
5:43 PM

Private VLAN (PVLAN) provides Ethernet traffic isolation between all the members of the same VLAN. It diverts all the traffic between individual compute modules to flow through the upstream switch infrastructure unless explicitly permitted by a predefined policy.

- Private VLANs can help you restrict how hosts communicate with each other within the primary VLAN
- Private VLANs are helpful for isolating systems within the same subnet, without the lost addresses due to splitting the address range into multiple subnets
- This capability enables interoperability with HPE Synergy and Cisco ACI Intra-EPG (end-point groups) isolation and micro-segmentation features.

There are 3 types of Private VLAN ports in the Cisco world:

- **Promiscuous** ports: communicate with all other private VLAN ports, is the port that you typically use to communicate with external routers
- **Community** ports: communicate among themselves and with their promiscuous ports
- **Isolated** ports: can only communicate with promiscuous ports, have complete Layer 2 isolation from other ports within the same private VLAN (e.g. Ethernet ports in hotel rooms)



With OneView 4.20, we can support **Isolated** ports on the compute module network connections.

This means that all Compute modules connected to the same Private VLAN cannot communicate, they are isolated from each other's. They can only communicate with a Promiscuous port located upstream on a Nexus switch usually connected to a router.

OneView 4.20 supports three types of **Isolated** downlink ports:

1. **ISOLATED TRUNK**: only recommended for PVLAN-unaware operating systems like bare metal server (Linux/Windows) - the traffic is tagged and requires a network set. A NIC teaming with VLAN 70 must be defined in the OS - The primary VLAN ID tags is translated to the isolated VLAN ID tags for traffic egressing to the downlink ports.
2. **PRIVATE VLAN MEMBER**: only recommended for PVLAN-aware operating systems like hypervisors: ESXi/Hyper-V. It requires a network set and a hypervisor virtual switch configured with Private VLAN. Upstream switch sends packets on the Primary VLAN but OS responds on the secondary (isolated) VLAN.
3. **ISOLATED ACCESS**: only recommended for PVLAN-unaware operating systems like bare metal server (Linux/Windows) and for untagged traffic only.

Private VLAN

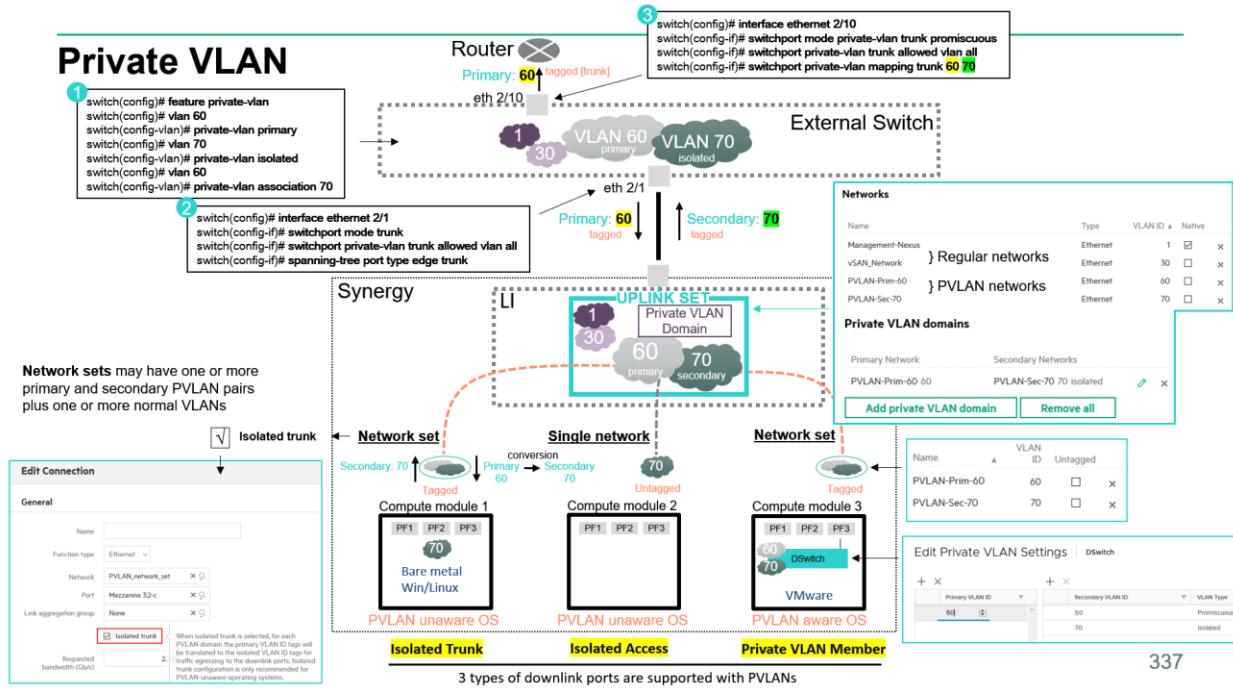
Downlink Port types

Can I create a **Promiscuous Access** ?

A primary network, cannot be used to create connections.

Profile 4	Management VLAN: VLAN60	Type: Ethernet	Mezzanine 32-c	Not bootable	<input checked="" type="checkbox"/>	<input type="button" value="OK"/>	<input type="button" value="Cancel"/>
Profile 5	Management VLAN: VLAN60	Type: Ethernet	Mezzanine 31-d	Not bootable	<input checked="" type="checkbox"/>	<input type="button" value="OK"/>	<input type="button" value="Cancel"/>

Setup:



1. Create one network for the primary Private VLAN

Name: PVLAN-Prim-60	A unique, descriptive name for the network
Type: Ethernet	
VLAN: 60	
Associate with subnet ID: none	
Purpose: General	
Preferred bandwidth: 2.5 Gb/s	
Maximum bandwidth: 20 Gb/s	
<input checked="" type="checkbox"/> Smart link	
<input type="checkbox"/> Private network	

2. Create one network for the secondary isolated Private VLAN

Name A unique, descriptive name for the network

Type

VLAN

Associate with subnet ID

Purpose

Preferred bandwidth Gb/s

Maximum bandwidth Gb/s

Smart link

Private network

3. Go to the **LIG** and add the two networks to the uplink set:

Networks

Name	Type	VLAN ID	Native
Management-Nexus	Ethernet	1	<input checked="" type="checkbox"/>
PVLAN-Prim-60	Ethernet	60	<input type="checkbox"/>
PVLAN-Sec-70	Ethernet	70	<input type="checkbox"/>

[Add networks](#)

[Remove networks](#)

[Remove all](#)

[Add networks from network set](#)

Uplink Ports

Interconnect Module	Enclosure	Bay	Port	Capability	Speed
Virtual Connect SE 40Gb F8 Module for Synergy	1	3	Q5	Ethernet + FCoE	<input type="button" value="Auto"/>
Virtual Connect SE 40Gb F8 Module for Synergy	2	6	Q5	Ethernet + FCoE	<input type="button" value="Auto"/>

[Add uplink ports](#)

[Remove uplink ports](#)

[Remove all](#)

4. Scroll down to the **Private VLAN domains** section and create a PVLAN domain using the two networks:

Private VLAN domains

Primary Network	Secondary Networks	
PVLAN-Prim-60 60	PVLAN-Sec-70 70 isolated	
Add private VLAN domain	Remove all	

Note: Private VLAN networks can be added or removed only in pairs. Both primary and secondary networks need to be added or removed together.

4. Go to the **LI** and **update from group** to set the PVLAN configuration to the VC modules
5. Enable the Nexus Private VLAN feature

```
switch# configure terminal
switch(config)# feature private-vlan
```

6. Configure VLAN 60 as a primary Private VLAN

```
switch(config)# vlan 60
switch(config-vlan)# private-vlan primary
```

7. Configure VLAN 70 as a secondary isolated Private VLAN

```
switch(config)# vlan 70
switch(config-vlan)# private-vlan isolated
```

8. Associate secondary VLAN 70 with Primary Private VLAN 60

```
switch(config)# vlan 60
switch(config-vlan)# private-vlan association 70
```

9. Configure the Nexus interface connected to the Synergy VC uplink set (with PVLAN domain) as a standard trunk port, allowing all networks in use (regular and Private VLANs):

```
switch(config)# interface port-channel20
switch(config-if)# description vpc Synergy
switch(config-if)# switchport mode trunk
switch(config-if)# switchport private-vlan trunk allowed vlan all
switch(config-if)# spanning-tree port type edge trunk
switch(config-if)# vpc 20
```

10. Configure Nexus interface connected to Layer3/Router as promiscuous port:

Note: **Private-vlan Trunk** is required if regular VLANs or multiple primary/secondary PVLANS is also required

```
switch(config)# interface port-channel30
switch(config-if)# description vpc router
switch(config-if)# switchport mode private-vlan trunk promiscuous
switch(config-if)# spanning-tree port type edge trunk
switch(config-if)# switchport private-vlan trunk allowed vlan all
switch(config-if)# switchport private-vlan mapping trunk 60 70
switch(config-if)# vpc 30
```

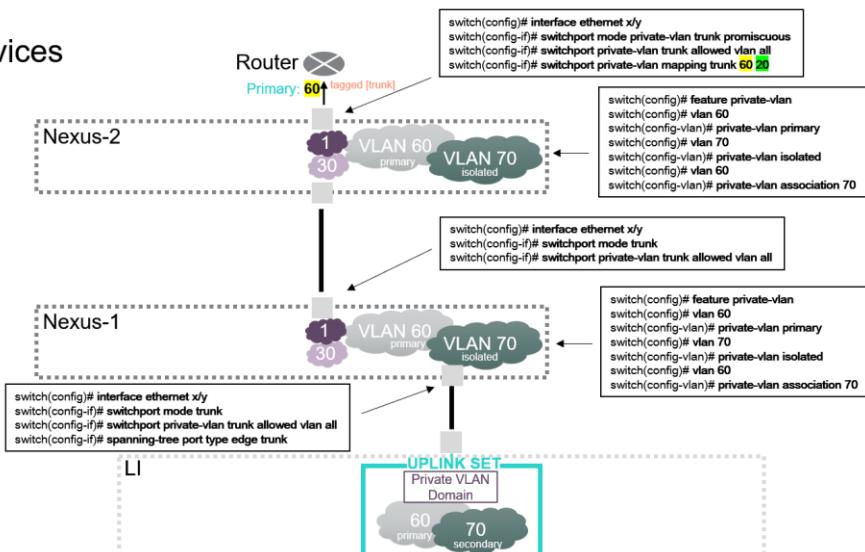
Note: *switchport private-vlan mapping trunk {primary-vlan-id} {secondary-vlan-id}*

Note: According to Cisco documentation, if your Private VLAN networks need to cross over multiple devices to reach the Promiscuous port where you typically connect your external router, you can extend the private VLAN networks by simply trunking the primary, isolated, and community VLANs to other devices as long as those devices support private VLANs.

A typical device-to-device PVLAN configuration would be as follow:

Private VLAN Across Multiple Devices

- Private VLANs can be extended across multiple devices by simply trunking the primary, isolated, and community VLANs to other devices that support private VLANs.
- To maintain the security of your private VLAN configuration and to avoid other uses of the VLANs configured to be private VLANs:
 - Configure private VLANs on all intermediate devices, including devices that have no private VLAN ports.
 - Avoid a non-PVLAN aware switches between PVLAN switches



11. For the **Isolated Trunk** and **Private VLAN Member** downlink configuration, you must create a **network set** with the pair of PVLAN networks:

Create Network Set | General

General

Name	PVLAN_network_set
Scope	Select zero or more scopes <input type="button" value="Q"/>
Preferred bandwidth	2.5 Gb/s
Maximum bandwidth	20 Gb/s

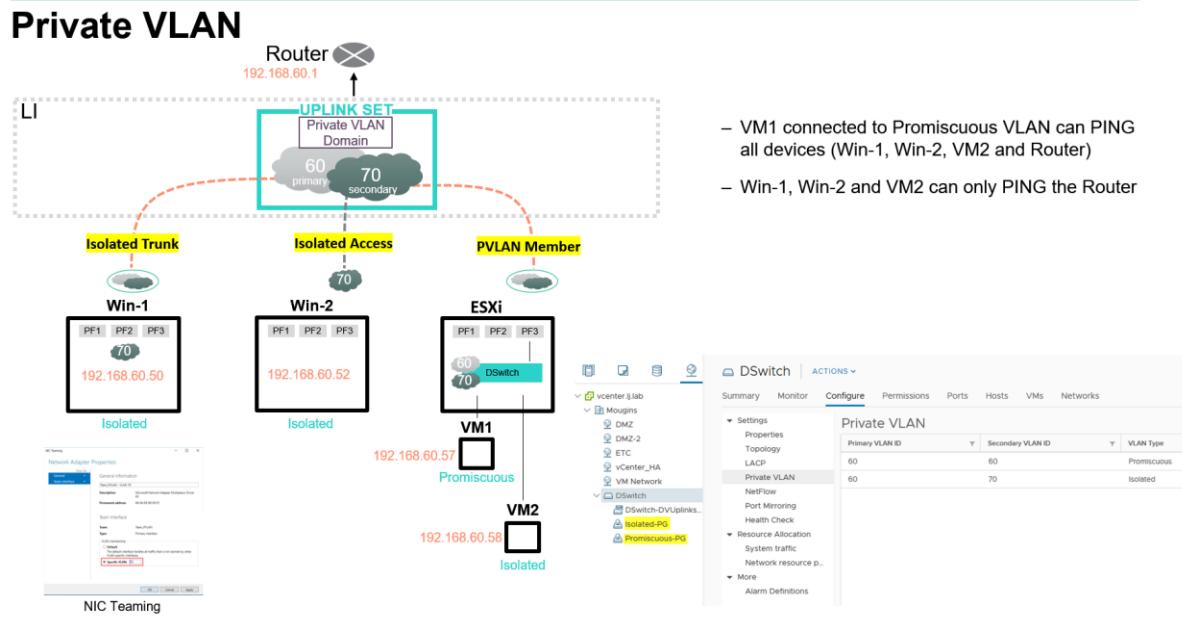
Networks

Name	VLAN	ID	Untagged	X
PVLAN-Prim-60	60	<input type="checkbox"/>	<input type="checkbox"/>	X
PVLAN-Sec-70	70	<input type="checkbox"/>	<input type="checkbox"/>	X

Add networks **Remove networks** **Remove all**

12. In **Server Profile**, define two connections with the desired downlink PVLAN option:

- A. **ISOLATED TRUNK**: only recommended for PVLAN-unaware operating systems like bare metal server (Linux/Windows) - the traffic is tagged and requires a network set. A NIC teaming with VLAN 70 must be defined in the OS - The primary VLAN ID tags is translated to the isolated VLAN ID tags for traffic egressing to the downlink ports.
- B. **PRIVATE VLAN MEMBER**: only recommended for PVLAN-aware operating systems like hypervisors: ESXi/Hyper-V. It requires a network set and a hypervisor virtual switch configured with Private VLAN. Upstream switch sends packets on the Primary VLAN but OS responds on the secondary (isolated) VLAN.
- C. **ISOLATED ACCESS**: only recommended for PVLAN-unaware operating systems like bare metal server (Linux/Windows) and for untagged traffic only.



A. **ISOLATED TRUNK:**

- Select the PVLAN Network set
- Check the **Isolated trunk** option

General

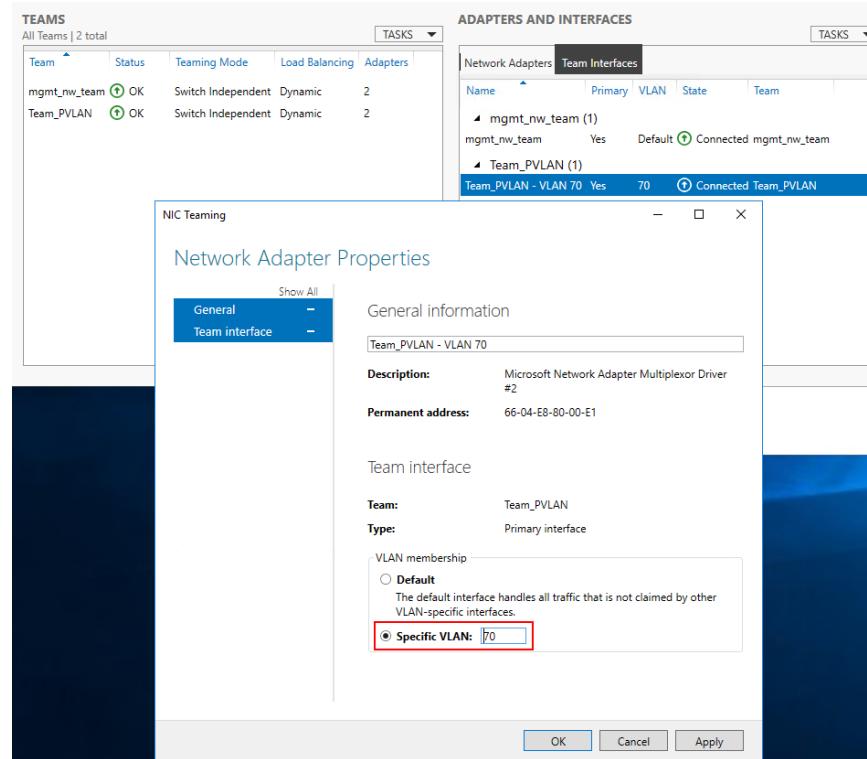
Name	<input type="text"/>
Function type	Ethernet
Network	PVLAN_network_set
Port	Mezzanine 3:1-d
Link aggregation group	None
<input checked="" type="checkbox"/> Isolated trunk	
Requested bandwidth (Gb/s)	2.5
Requested virtual functions	<input checked="" type="radio"/> None <input type="radio"/> Custom <input type="radio"/> Auto
Boot	Not bootable

- The following is displayed in OneView for the Server Profile PVLAN network connection:

Connections

Expand all	Collapse all	ID	Name	Network	Port	Boot
▶	● 1	Deployment Network A	iSCSI-Deployment	VLAN8	Mezzanine 3:1-a	iSCSI primary
▶	● 2	Deployment Network B	iSCSI-Deployment	VLAN8	Mezzanine 3:2-a	iSCSI secondary
▶	● 3		Management	VLAN5	Mezzanine 3:1-c	Not bootable
▶	● 4		Management	VLAN5	Mezzanine 3:2-c	Not bootable
▼	● 5		PVLAN network set	(network set)	Mezzanine 3:1-d	Not bootable
			Interconnect	Frame1, interconnect_3		
			Type	Ethernet		
			MAC address	66:04:E8:80:00:EA (v)		
			Requested virtual functions	None		
			Requested bandwidth	2.5 Gb/s		
			Allocated bandwidth	2.5 Gb/s		
			Max bandwidth	20 Gb/s		
			Link aggregation group	None		
			Private VLAN port type	Isolated trunk		
▶	● 6			PVLAN network set	(network set)	Mezzanine 3:2-d Not bootable

- A NIC teaming with VLAN 70 network adapter must be defined under the OS:



B. **PRIVATE VLAN MEMBER:** for hypervisor PVLAN aware OS's like ESXi/Hyper-v:

- Select the PVLAN Network set
- Unckeck the **Isolated trunk** option

General

Name	<input type="text"/>
Function type	Ethernet
Network	PVLAN_network_set
Port	Mezzanine 3:1-d
Link aggregation group	None
Requested bandwidth (Gb/s)	<input type="checkbox"/> Isolated trunk
Requested virtual functions	<input checked="" type="radio"/> None <input type="radio"/> Custom <input type="radio"/> Auto
Boot	Not bootable

When isolated trunk is selected, for each PVLAN domain the primary VLAN ID tags will be translated to the isolated VLAN ID tags for traffic egressing to the downlink ports. Isolated trunk configuration is only recommended for PVLAN-unaware operating systems.

- The following is displayed in OneView for the Server Profile PVLAN network connection:

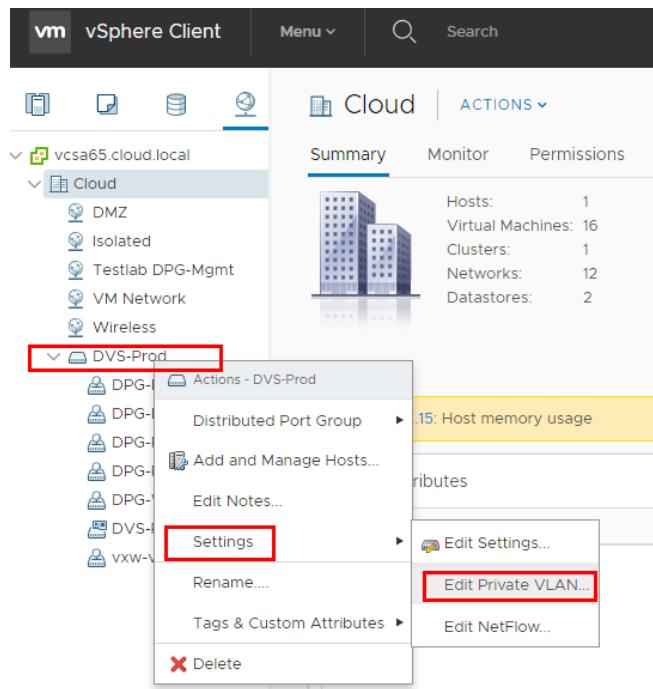
Connections

Expand all		Collapse all		
ID	Name	Network	Port	Boot
1	Deployment Network A	iSCSI-Deployment VLAN8	Mezzanine 3:1-a	iSCSI primary
2	Deployment Network B	iSCSI-Deployment VLAN8	Mezzanine 3:2-a	iSCSI secondary
3		Management VLAN5	Mezzanine 3:1-c	Not bootable
4		Management VLAN5	Mezzanine 3:2-c	Not bootable
5		FCA Fabric attach	Mezzanine 3:1-b	Not bootable
6		FCB Fabric attach	Mezzanine 3:2-b	Not bootable
7		PVLAN_network_set (network set)	Mezzanine 3:1-d	Not bootable
Interconnect Type: Ethernet MAC address: 66:04:E8:80:00:F8 (v) Requested virtual functions: None Requested bandwidth: 2.5 Gb/s Allocated bandwidth: 2.5 Gb/s Max bandwidth: 20 Gb/s Link aggregation group: None Private VLAN port type: Private VLAN member				
8		PVLAN_network_set (network set)	Mezzanine 3:2-d	Not bootable

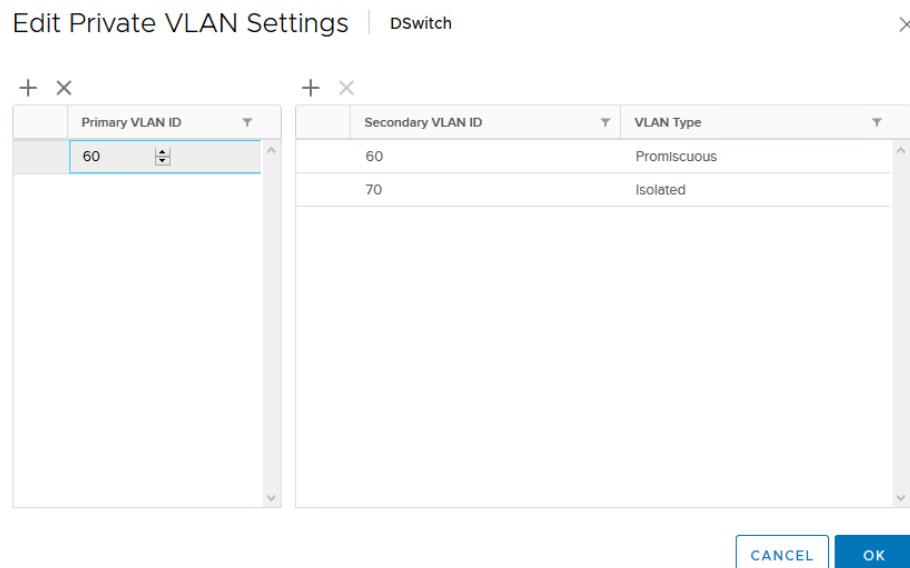
- **PVLAN with VMWare ESXi:**

PVLANs in ESXi must be configured on virtual distributed switches.

To set PVLAN, right-click on the distributed switch and select **Settings** then **Edit Private VLAN**.



Click the “+” signs to add the Primary VLAN ID **60** with VLAN Type **Promiscuous**, then add the Secondary VLAN **70** as **Isolated**.



Next is to create a first distributed port group which will be connected to newly created primary PVLAN, select **Private VLAN** as VLAN Type and select **Promiscuous (60, 60)** as Private VLAN ID:

Promiscuous-PG - Edit Settings

General

Advanced

VLAN

Security

Teaming and failover

Traffic shaping

Monitoring

Miscellaneous

VLAN type	Private VLAN
Private VLAN ID	Promiscuous (60, 60)

Next is to create a second distributed port group which will be connected to newly created isolated PVLAN, select **Private VLAN** as VLAN Type and select **Isolated (60, 70)** as Private VLAN ID:

New Distributed Port Group

✓ 1 Select name and location
2 Configure settings
3 Ready to complete

Configure settings
Set general properties of the new port group.

Port binding	Static binding
Port allocation	Elastic
Number of ports	8
Network resource pool	(default)

VLAN

VLAN type	Private VLAN
Private VLAN ID	Isolated (60, 70)

Advanced

Customize default policies configuration

Primary VLAN ID	Secondary VLAN ID	VLAN Type
60	60	Promiscuous
60	70	Isolated

- Then VMs must be attached to the respective Port Groups for either isolation or promiscuous modes...

Note: In Promiscuous mode, the VM can PING all VMs (in either isolated or promiscuous mode) and all Computers (in OneView isolated access or isolated trunk mode)

- C. **ISOLATED ACCESS:** This option is for PVLAN unaware OS - traffic is **untagged** and does not need any specific OS requirements.

- For this single network option, do not select the network set but the Secondary Isolated VLAN 70: **PVLAN-Sec-70**.

General

Name	<input type="text"/>
Function type	Ethernet <input type="button" value="▼"/>
Network	PVLAN-Sec-70 <input type="button" value="X"/> <input type="button" value="Q"/>
Port	Mezzanine 3:1-d <input type="button" value="X"/> <input type="button" value="Q"/>
Link aggregation group	None <input type="button" value="X"/> <input type="button" value="Q"/>
Requested bandwidth (Gb/s)	2.5 <input type="button" value="▲"/> <input type="button" value="▼"/>
Requested virtual functions	<input checked="" type="radio"/> None <input type="radio"/> Custom <input type="radio"/> Auto
Boot	Not bootable <input type="button" value="▼"/>

- The following is displayed in OneView for the Server Profile PVLAN network connection:

Connections

[Expand all](#) [Collapse all](#)

ID	Name	Network	Port	Boot
▶ ● 1	Deployment Network A	iSCSI-Deployment VLAN8	Mezzanine 3:1-a	iSCSI primary
▶ ● 2	Deployment Network B	iSCSI-Deployment VLAN8	Mezzanine 3:2-a	iSCSI secondary
▶ ● 3		Management VLAN5	Mezzanine 3:1-c	Not bootable
▶ ● 4		Management VLAN5	Mezzanine 3:2-c	Not bootable
▼ ● 5		PVLAN-Sec-70 VLAN70	Mezzanine 3:1-d	Not bootable
Interconnect				
Type		Frame1_interconnect_3		
MAC address		Ethernet		
Requested virtual functions		66:04:E8:80:00:F0 (v)		
Requested bandwidth		None		
Allocated bandwidth		2.5 Gb/s		
Max bandwidth		2.5 Gb/s		
Link aggregation group		20 Gb/s		
Private VLAN port type		<i>None</i>		
		Isolated access		
▶ ● 6		PVLAN-Sec-70 VLAN70	Mezzanine 3:2-d	Not bootable

Troubleshooting

```
nexus5624-TOP# sh vlan private-vlan
```

Primary	Secondary	Type	Ports
60	70	isolated	Po30

```
nexus5624-TOP# sh vlan private-vlan type
```

Vlan	Type
60	primary
70	isolated

```
# Interface of the Router
```

```
nexus5624-TOP# sh int po 30 switchport
```

Name: port-channel30
Switchport: Enabled
Switchport Monitor: Not enabled
Operational Mode: **Private-vlan trunk promiscuous**
Access Mode VLAN: 60 (VLAN0060)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Allowed: 1-4094
Voice VLAN: none
Extended Trust State : not trusted [COS = 0]
Administrative private-vlan primary host-association: none
Administrative private-vlan secondary host-association: none
Administrative private-vlan primary mapping: none
Administrative private-vlan secondary mapping: none
Administrative private-vlan trunk native VLAN: 1
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 1-59,61-69,71-3967,4048-4093
Administrative private-vlan trunk private VLANs: (60 70)
Operational private-vlan: (60 70)
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

```
# Interface of the Synergy uplink set
```

```
nexus5624-TOP# sh int po 20 switchport
```

interface port-channel40
description vpc SY-5900AF-BOTTOM
nexus5624-TOP# sh int po 20 switchport
Name: port-channel20
Switchport: Enabled
Switchport Monitor: Not enabled
Operational Mode: **trunk**
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)

Trunking VLANs Allowed: **1-4094**
Voice VLAN: none
Extended Trust State : not trusted [COS = 0]
Administrative private-vlan primary host-association: none
Administrative private-vlan secondary host-association: none
Administrative private-vlan primary mapping: none
Administrative private-vlan secondary mapping: none
Administrative private-vlan trunk native VLAN: 1
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Interface of the Router
nexus5624-TOP# **sh int po30 br**

Port-channel	VLAN	Type	Mode	Status	Reason	Speed	Protocol
Interface							
Po30	1	eth	pvlan	up	none	a-10G(D)	lacp

Interface of the Synergy uplink set
nexus5624-TOP# **sh int po20 br**

Port-channel	VLAN	Type	Mode	Status	Reason	Speed	Protocol
Interface							
Po20	1	eth	trunk	up	none	a-40G(D)	lacp

Interface of the Router
nexus5624-TOP# **sh vpc 30**
vPC status

id	Port	Status	Consistency	Reason	Active vlans
30	Po30	up	success	success	1,6,10,20,30,60

Interface of the Synergy uplink set
nexus5624-TOP# **sh vpc 20**
vPC status

id	Port	Status	Consistency	Reason	Active vlans

```
20 Po20    up  success  success      1,6,10,20,30,60,70
```

```
# Interface of the Synergy uplink set  
nexus5624-TOP# sh int po 20 status err-vlans
```

Port	Name	Err-Vlans	Status
Po20	vpc Synergy	none	none

```
# Interface of the Router  
nexus5624-TOP# sh int po 30 status err-vlans
```

Port	Name	Err-Vlans	Status
Po30	vpc Router	none	none