Configuring Private VLANs

This chapter contains the following sections:

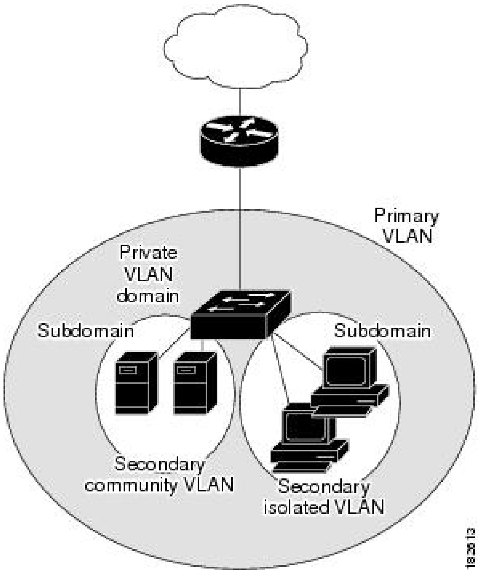
Information About Private VLANs

PVLANs achieve Layer 2 isolation through the use of three separate port designations, each having its own unique set of rules that regulate each connected endpoint's ability to communicate with other connected endpoints within the same private VLAN domain.

Private VLAN Domains

A PVLAN domain consists of one or more pairs of VLANs. The primary VLAN makes up the domain; and each VLAN pair makes up a subdomain. The VLANs in a pair are called the primary VLAN and the secondary VLAN. All VLAN pairs within a private VLAN have the same primary VLAN. The secondary VLAN ID is what differentiates one subdomain from another. See the following figure.

Figure 1: Private VLAN Domain



Spanning Multiple Switches

PVLANs can span multiple switches, just like regular VLANs. Inter-switch link ports do not need to be aware of the special VLAN type and carry frames tagged with these VLANs just like they do any other frames. PVLANs ensure that traffic from an isolated port in one switch does not reach another isolated or community port in a different switch even after traversing an inter-switch link. By embedding the isolation information at the VLAN level and by transporting it with the packet, it is possible to maintain consistent behavior throughout the network. The mechanism that restricts Layer 2 communication between two isolated ports in the same switch also restricts Layer 2 communication between two isolated ports in two different switches.

Private VLAN Ports

Within a PVLAN domain, there are three separate port designations. Each port designation has its own unique set of rules that regulate the ability of one endpoint to communicate with other connected endpoints within the same private VLAN domain. The three port designations are as follows:

- promiscuous
- isolated
- community

Primary VLANs and Promiscuous Ports

The primary VLAN encompasses the entire PVLAN domain. It is a part of each subdomain and provides the Layer 3 gateway out of the VLAN. A PVLAN domain has only one primary VLAN. Every port in a PVLAN domain is a member of the primary VLAN.

A promiscuous port can talk to all other types of ports; it can talk to isolated ports as well as community ports and vice versa. Layer 3 gateways, DHCP servers, and other trusted devices that need to communicate with the customer endpoints are typically connected with a promiscuous port. A promiscuous port can be either an access port or a hybrid/trunk port according to the terminology presented in Annex D of the IEEE 802.1Q specification.

Secondary VLANs and Host Ports

Secondary VLANs provide Layer 2 isolation between ports in a PVLAN domain. A PVLAN domain can have one or more subdomains. A subdomain is made up of a VLAN pair that consists of the primary VLAN and a secondary VLAN. Because the primary VLAN is a part of every subdomain, secondary VLANs differentiate the VLAN subdomains.

To communicate to the Layer 3 interface, you must associate a secondary VLAN with at least one of the promiscuous ports in the primary VLAN. You can associate a secondary VLAN to more than one promiscuous port within the same PVLAN domain, for example, if needed for load balancing or redundancy. A secondary VLAN that is not associated with any promiscuous port cannot communicate with the Layer 3 interface.

A secondary VLAN can be one of the following types:

- Isolated VLANs—Isolated VLANs use isolated host ports. An isolated port cannot talk to any other port in that private VLAN domain except for promiscuous ports. If a device needs to have access only to a gateway router, it should be attached to an isolated port. An isolated port is typically an access port, but in certain applications, it can also be a hybrid or trunk port.

  An isolated VLAN allows all its ports to have the same degree of segregation that could be obtained from using one separate dedicated VLAN per port. Only two VLAN identifiers are used to provide this port isolation.

  Note While multiple community VLANs can be in a private VLAN domain, one isolated VLAN can serve multiple customers. All endpoints that are connected to its ports are isolated at Layer 2. Service providers can assign multiple customers to the same isolated VLAN and be assured that their Layer 2 traffic cannot be sniffed by other customers that share the same isolated VLAN.

- Community VLANs—Community VLANs use community host ports. A community port is part of a group of ports. The ports within a community can communicate at Layer 2 with one another and can also talk to any promiscuous port. For example, if an ISP customer has four devices and wants them isolated from those devices of other customers but still be able to communicate among themselves, community ports should be used.

  Note Because trunks can support a VLAN that carries traffic between its ports, VLAN traffic can enter or leave the device through a trunk interface.

Communication Between Private VLAN Ports

The following table shows how access is permitted or denied between PVLAN port types.

Table 1: Communication Between PVLAN Ports

	Isolated	Promiscuous	Community 1	Community 2	Interswitch Link Port[1]
Isolated	Deny	Permit	Deny	Deny	Permit
Promiscuous	Permit	Permit	Permit	Permit	Permit
Community 1	Deny	Permit	Permit	Deny	Permit
Community 2	Deny	Permit	Deny	Permit	Permit
Interswitch Link Port	Deny[2]	Permit	Permit	Permit	Permit

[1] An interswitch link port is a regular port that connects two switches and that happens to carry two or more VLANs.

[2] This behavior applies to traffic that traverses inter-switch link ports over an isolated VLAN only. Traffic from an inter-switch link port to an isolated port will be denied if it is in the isolated VLAN. Traffic from an inter-switch link port to an isolated port will be permitted if it is in the primary VLAN.

Guidelines and Limitations

PVLANs have the following configuration guidelines and limitations:

Control VLANs, packet VLANs, and management VLANs must be configured as regular VLANs and not as private VLANs.

The following are configuration limits:

- Private VLANs per DVS: 512 maximum
- Primary VLANs per promiscuous trunk port: 64 maximum
- Private VLAN associations: 511 maximum
- Private VLAN ports per DVS : 4096 maximum

Default Settings

Table 2: Default PVLAN Settings

Parameters	Default
PVLANs	Disabled

Configuring a Private VLAN

The following section guides you through the private VLAN configuration process. After completing each procedure, return to this section to make sure that you have completed all required procedures in the correct sequence.

Procedure

Step 1 Enable or disable the PVLAN feature globally.

Step 2 Configure a VLAN as a primary VLAN.

Step 3 Configure a VLAN as a secondary VLAN.

Step 4 Associate the VLANs in a PVLAN.

Step 5 Configure a PVLAN host port.

Step 6 Associate a host port with a PVLAN.

Step 7 Verify a PVLAN configuration.

Enabling or Disabling the Private VLAN Feature Globally

You can globally enable or disable the PVLAN feature.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **feature private-vlan**	Globally enables or disables the PVLAN feature.
Step 3	(Optional) switch(config-vlan)# **show feature**	Displays features available and whether they are enabled globally.
Step 4	(Optional) switch(config-vlan)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

This example shows how to enable or disable the PVLAN feature globally:

```
switch# configure terminal
switch(config)# feature private-vlan
switch(config-vlan)# show feature
Feature Name          Instance  State
--------------------  --------  --------
dhcp-snooping         1         enabled
```

```
http-server          1         enabled
ippool               1         enabled
lacp                 1         enabled
lisp                 1         enabled
lisphelper           1         enabled
netflow              1         disabled
port-profile-roles   1         enabled
private-vlan         1         enabled
sshServer            1         enabled
tacacs               1         enabled
telnetServer         1         enabled
switch(config-vlan)#
```

Configuring a VLAN as a Primary VLAN

You can configure a VLAN to function as the primary VLAN in a PVLAN.

Before you begin

- Log in to the CLI in EXEC mode.
- You have already enabled the private VLAN feature using the Enabling or Disabling the Private VLAN Feature Globally, on page 5.
- Know that the VLAN that you are configuring as a primary VLAN already exists in the system as a normal VLAN, and you know the VLAN ID.

Note If the VLAN does not already exist, you are prompted to create it when you create the primary VLAN.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **vlan** *primary-vlan-id*	Enters VLAN configuration mode for the specified VLAN and configures the primary VLAN ID in the running configuration.
Step 3	switch(config-vlan)# **private-vlan primary**	Designates the primary VLAN as a private VLAN in the running configuration.
Step 4	switch(config-vlan)# **exit**	Exits VLAN configuration mode. **Note** You must exit VLAN configuration mode for the configurations to take effect.
Step 5	(Optional) switch(config)# **show vlan private-vlan**	Displays the PVLAN configuration.

	Command or Action	Purpose
Step 6	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

This example shows how to configure a VLAN as a primary VLAN:

```
switch# configure terminal
switch(config)# vlan 202
switch(config-vlan)# private-vlan primary
switch(config-vlan)# exit
switch(config)# show vlan private-vlan
Primary  Secondary  Type             Ports
-------  ---------  ---------------  -------------------------------------------
202                 primary

switch(config)#
```

Configuring a VLAN as a Secondary VLAN

You can configure a VLAN to function as the primary VLAN in a PVLAN.

Before you begin

- Log in to the CLI in EXEC mode.
- You have already enabled the private VLAN feature.
- Know that the VLAN that you are configuring as a secondary VLAN already exists in the system as a normal VLAN, and you know the VLAN ID.

  Note If the VLAN does not already exist, you are prompted to create it when you create the secondary VLAN.

- Know whether you want the secondary VLANs to be community VLANs or isolated VLANs, and the VLAN IDs for each.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **vlan** *secondary-vlan-id*	Enters VLAN configuration mode for the specified VLAN and configures the secondary VLAN ID in the running configuration.

	Command or Action	Purpose
Step 3	switch(config-vlan)# **private-vlan** {**community** | **isolated**}	Designates the VLAN as either a community or isolated private VLAN in the running configuration.
Step 4	switch(config-vlan)# **exit**	Exits VLAN configuration mode. **Note** You must exit VLAN configuration mode for the configurations to take effect.
Step 5	(Optional) switch(config)# **show vlan private-vlan**	Displays the PVLAN configuration.
Step 6	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

This example shows how to configure a VLAN as a secondary VLAN:

```
switch# configure terminal
switch(config)# vlan 303
switch(config-vlan)# private-vlan community
switch(config-vlan)# exit
switch(config)# show vlan private-vlan
Primary  Secondary  Type             Ports
-------  ---------  ---------------  -------------------------------------------
202                 primary
         303        community

switch(config)#
```

Associating the VLANs in a PVLAN

You can associate the primary VLANs in a PVLAN with the secondary VLANs.

Before you begin

- Log in to the CLI in EXEC mode.
- Know that the primary VLAN for this PVLAN is already configured as a PVLAN.
- Know that the secondary VLANs for this PVLAN are already configured as PVLANs.
- Know the VLAN IDs for each VLAN that is a part of the PVLAN.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	Required: switch(config)# **vlan** *primary-vlan-id*	Enters VLAN configuration mode and associates the VLANs to function as a PVLAN in the running configuration.
Step 3	switch(config-vlan)# **private-vlan association** {**add** | **remove**} *secondary vlan-id*	Associates a specified secondary VLAN with the primary VLAN to function as a PVLAN in the running configuration. To associate additional secondary VLANs, repeat this step.
Step 4	switch(config-vlan)# **exit**	Exits VLAN configuration mode.
Step 5	(Optional) switch(config)# **show vlan private-vlan**	Displays the PVLAN configuration.
Step 6	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

This example shows how to associate VLANs in a PVLAN:

```
switch# configure terminal
switch(config)# vlan 202
switch(config-vlan)# private-vlan association add 303
switch(config-vlan)# exit
switch(config)# show vlan private-vlan
Primary  Secondary  Type             Ports
-------  ---------  ---------------  -------------------------------------------
202        303         community
switch(config)#
```

Associating a vEthernet Port Profile with a Private VLAN

You can associate the vEthernet port profile with the primary and secondary VLANs in a PVLAN.

Before you begin

- Log in to the CLI in EXEC mode.
- Know the VLAN IDs of the primary and secondary VLANs in the PVLAN.
- Know that the primary VLAN for this PVLAN is already configured as a PVLAN.
- Know that the secondary VLANs for this PVLAN are already configured as PVLANs.
- Know the name of the interface functioning in the PVLAN as a host port.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile type vethernet** *name*	Enters port profile configuration mode for the specified port profile.
Step 3	switch(config-port-profile)# **switchport mode private-vlan host**	Associates the vEthernet port with the PVLAN configuration. The port profile is associated with the VLANs in the PVLAN.
Step 4	switch(config-port-profile)# **switchport private-vlan host-association** *vlan_ids*	Assigns the primary and secondary VLAN IDs to the port profile and saves this association in the running configuration.
Step 5	switch(config-port-profile)# **no shut**	Enables the port profile.
Step 6	switch(config-port-profile)# **vmware port-group**	Designates the port profile as a VMware port group. The port profile is mapped to a VMware port group of the same name unless you specify a name here. When you connect the VSM to vCenter Server, the port group is distributed to the virtual switch on vCenter Server.
Step 7	switch(config-port-profile)# **state enabled**	Enables the port profile and applies its configuration to the assigned ports.
Step 8	(Optional) switch(config-if)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to associate a vEthernet port with a PVLAN:

```
switch # configure terminal
switch(config)# port-profile type vethernet pvlan_community_303
switch(config-port-prof)# switchport mode private-vlan host
switch(config-port-prof)# switchport private-vlan host-association 202 303
switch(config-port-prof)# no shut
switch(config-port-prof)# vmware port-group
switch(config-port-prof)# state enabled
```

Configuring a vEthernet Port Using PVLAN Port-Profile

You can associate a vEthernet port-profile with PVLAN configuration to a virtual machine adapter in the vCenter server.

Before you begin

- You should know the VMware vCenter login credentials.
- You should be logged into vCenter Server.
- You have information about the virtual machine adapeter to which por-profile will be attached.

Procedure

Step 1 Navigate to VMware vCenter Server.

Step 2 On the **Navigator** pane, choose the virtual machine to which you want to bind the port-profile

Step 3 Right click a virtual machine, and from the pop-up menu, select **Edit Settings**.

Step 4 In the **Edit Settings** dialog box, select a port-profile from the drop-down list for a network adapter.

Step 5 Click **Ok**

A vEthernet port with the selected port-profile configuration is brought up on Nexus 1000VE.

Step 6 (Optional) Use the **show interface brief** command to check whether the new interface is configured properly or not.

```
N1KV_140_NG# show interface brief

--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0    --           up     10.197.128.234                          1000     1500

--------------------------------------------------------------------------------
Ethernet     VLAN    Type Mode    Status  Reason                   Speed    Port
Interface                                                                   Ch #
--------------------------------------------------------------------------------
Eth3/1       1       eth  trunk   up      none                     10G
Eth4/1       1       eth  trunk   up      none                     10G

--------------------------------------------------------------------------------
Vethernet    VLAN/    Type Mode    Status  Reason                   MTU  Module
             Segment
--------------------------------------------------------------------------------
Veth1        1500     virt access  up      none                     1500 3
```

Step 7 (Optional) Use the **show running-config interface vethernet** command to view the summary of the interface configuration.

```
N1KV_140_NG# show run interface vethernet 1

!Command: show running-config interface Vethernet1
!Time: Thu Jul  5 15:18:19 2018

version 5.2(1)SV5(1.1)

interface Vethernet1
  inherit port-profile pvlan_community_303
  description HPING_229_210, Net Adapter 1
```

```
vmware dvport 0 dvswitch uuid "50 37 b6 e5 fd 04 3f 61-9f f5 b0 e1 5b 00 db f3"
vmware vm mac 0050.56B7.C299
```

Configuring a Layer 2 Port Profile as a Promiscuous Trunk Port

You can configure a Layer 2 interface as a promiscuous trunk port that does the following:

- Combines multiple promiscuous ports into a single trunk port.
- Carries all normal VLANs.
- Carries multiple PVLAN primary VLANs each with selected secondary VLANs.

Note A promiscuous port can be either access or trunk. If you have one primary VLAN, you can use a promiscuous access port. If you have multiple primary VLANs, you can use a promiscuous trunk port.

Before you begin

- Log in to the CLI in EXEC mode.
- Know that the **private-vlan mapping trunk** command does not decide or override the trunk configuration of a port.
- Know that the port is already configured in a regular trunk mode before adding the PVLAN trunk configurations.
- Know that primary VLANs must be added to the list of allowed VLAN for the promiscuous trunk port.
- Know that secondary VLANs are not configured in the allowed VLAN list.
- Know that the trunk port can carry normal VLANs in addition to primary VLANs.
- Know that you can map up to 64 primary VLANs to their secondary VLANs in one promiscuous trunk port.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile type ethernet** *name*	Places you in port-profile mode.
Step 3	switch(config-port-prof)# **switchport mode trunk**	Designates that the interfaces are to be used as trunking ports.
Step 4	switch(config-port-prof)# **switchport mode private-vlan trunk promiscuous**	In the running configuration, designates the interface as a promiscuous PVLAN trunk port.

	Command or Action	Purpose
Step 5	switch(config-port-prof)# **switchport private-vlan trunk allowed vlan** *vlan_range*	Sets the allowed VLANs and VLAN IDs when the interface is in PVLAN trunking mode.
Step 6	switch(config-port-prof)# **switchport private-vlan mapping trunk** *primary_vlan_ID* {*secondary_vlan_list* | **add** *secondary_vlan_list* | **remove** *secondary_vlan_list*}	Maps the PVLAN trunk port to a primary VLAN and to selected secondary VLANs in the running configuration. Multiple PVLAN pairs can be specified so that a promiscuous trunk port can carry multiple primary VLANs.
Step 7	switch(config-port-prof)# **no shut**	Enables the port profile.
Step 8	switch(config-port-profile)# **vmware port-group**	Designates the port profile as a VMware port group. The port profile is mapped to a VMware port group of the same name unless you specify a name here. When you connect the VSM to vCenter Server, the port group is distributed to the virtual switch on the vCenter Server.
Step 9	switch(config-port-profile)# **state enabled**	Enables the port profile and applies its configuration to the assigned ports.
Step 10	(Optional) switch(config-if)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure a Layer 2 port profile as a promiscuous trunk port:

```
switch # configure terminal
switch(config)# port-profile type eth allaccess1
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport mode private-vlan trunk promiscuous
 switch(config-port-prof)# switchport private-vlan trunk allowed vlan 2,126-128,150-155
switch(config-port-prof)# switchport private-vlan mapping trunk 126 127,128
switch(config-port-prof)# no shut
switch(config-port-prof)# vmware port-group
switch(config-port-prof)# state enabled
```

Configuring a Layer 2 Port Profile as a Promiscuous Access Port

You can configure a Layer 2 interface as a promiscuous access port.

Note A promiscuous port can be either access or trunk. If you have one primary VLAN, you can use a promiscuous access port. If you have multiple primary VLANs, you can use a promiscuous trunk port.

Before you begin

- Log in to the CLI in EXEC mode.
- Know that the **private-vlan mapping** command does not decide or override the access configuration of a port.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile type vethernet** *name*	Places you in port-profile mode.
Step 3	switch(config-port-prof)# **switchport mode private-vlan promiscuous**	In the running configuration, designates the interface as a promiscuous PVLAN port.
Step 4	switch(config-port-prof)# **switchport private-vlan mapping** *primary_vlan_ID* {*secondary_vlan_list* | **add** *secondary_vlan_list* | **remove** *secondary_vlan_list*}	Maps the PVLAN access port to a primary VLAN and to the selected secondary VLANs in the running configuration.
Step 5	switch(config-port-prof)# **no shut**	Enables the port profile.
Step 6	switch(config-port-profile)# **vmware port-group**	Designates the port profile as a VMware port group. The port profile is mapped to a VMware port group of the same name unless you specify a name here. When you connect the VSM to vCenter Server, the port group is distributed to the virtual switch on the vCenter Server.
Step 7	switch(config-port-profile)# **state enabled**	Enables the port-profile and applies its configuration to the assigned ports.
Step 8	(Optional) switch(config-if)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure a Layer 2 port profile as a promiscuous trunk port:

```
switch # configure terminal
switch(config)# port-profile type vethernet pvlan-prom-pp
switch(config-port-prof)# switchport mode private-vlan promiscuous
switch(config-port-prof)# switchport private-vlan mapping 202 303
switch(config-port-prof)# no shut
switch(config-port-prof)# vmware port-group
switch(config-port-prof)# state enabled
```

Removing a Private VLAN Configuration

You can remove a PVLAN configuration and return the VLAN to normal VLAN mode.

Before you begin

- Log in to the CLI in EXEC mode.
- The VLAN is configured as a private VLAN, and you know the VLAN ID.
- When you remove a PVLAN configuration, the ports associated with it become inactive.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **vlan** *private vlan-id*	Enters the VLAN configuration mode for the specified VLAN.
Step 3	switch(config-vlan)# **no private-vlan** {**community** | **isolated** | **primary**}	Removes the specified VLAN from a PVLAN in the running configuration. The private VLAN configuration is removed from the specified VLAN(s). The VLAN is returned to normal VLAN mode. The ports associated with the VLAN are inactive.
Step 4	switch(config-vlan)# **exit**	Exits VLAN configuration mode.
Step 5	(Optional) switch(config)# **show vlan private-vlan**	Displays the PVLAN configuration.
Step 6	(Optional) switch(config)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

This example shows how to remove a PVLAN configuration:

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# no private-vlan primary
switch(config-vlan)# exit
switch(config)# show vlan private-vlan
Primary  Secondary  Type             Ports
-------  ---------  ---------------  -------------------------------------------

switch(config)#
```

Verifying a Private VLAN Configuration

Use the following commands to verify a private VLAN configuration:

Command	Purpose
show feature	Displays features available and whether they are enabled globally.
show running-config vlan *vlan-id*	Displays VLAN information.
show vlan private-vlan [*type*]	Displays information about PVLANs.
show interface switchport	Displays information about all interfaces configured as switchports.

Configuration Examples for Private VLANs

Example: PVLAN Trunk Port

This example shows how to configure interface Ethernet 2/6 as the following:

- PVLAN trunk port
- Mapped to primary PVLAN 202 which is associated with secondary VLANs 303 and 440
- Mapped to primary PVLAN 210 which is associated with secondary VLANs 310 and 450

```
switch# configure terminal
switch(config)# vlan 303,310
switch(config-vlan)# private-vlan community
switch(config-vlan)# exit
switch(config)# vlan 440,450
switch(config-vlan)# private-vlan isolated
switch(config-vlan)# exit
switch(config)# vlan 202
switch(config-vlan)# private-vlan primary
switch(config-vlan)# private-vlan association 303,440
switch(config-vlan)# exit
switch(config)# vlan 210
switch(config-vlan)# private-vlan primary
switch(config-vlan)# private-vlan association 310,450
switch(config-vlan)# exit
```

Example: PVLAN Using Port Profiles

This example configuration shows how to configure interface eth2/6 using port-profile, uppvlanpromtrunk156.

In this configuration, packets from secondary interfaces 153, 154, and 155 are translated into the PVLAN 156:

```
vlan 153-154
  private-vlan community
vlan 155
```

```
  private-vlan isolated
vlan 156
  private-vlan association 153-155
  private-vlan primary


switch# show run int eth2/6

version 5.2(1)
interface Ethernet2/6
switchport
inherit port-profile uppvlanpromtrunk156

switch# show port-profile name uppvlanpromtrunk156
port-profile uppvlanpromtrunk156
description:
status: enabled
capability privileged: no
capability uplink: yes
port-group: uppvlanpromtrunk156
config attributes:
switchport mode private-vlan trunk promiscuous
switchport private-vlan trunk allowed vlan all
switchport private-vlan mapping trunk 156 153-155
no shutdown
evaluated config attributes:
switchport mode trunk
switchport trunk allowed vlan all
switchport private-vlan mapping trunk 156 153-155
no shutdown
assigned interfaces:
Ethernet2/6

switch# show interface eth 2/6 switchport
Name: Ethernet2/6
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: Private-vlan trunk promiscuous
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  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: 1-155,157-3967,4048-4093
  Administrative private-vlan trunk private VLANs: (156,153) (156,155)
  Operational private-vlan: 156,153,155 inherit port-profile uppvlanpromtrunk156
 switch#
```