Configuring Private VLANs

This chapter contains the following sections:

Information About Private VLANs

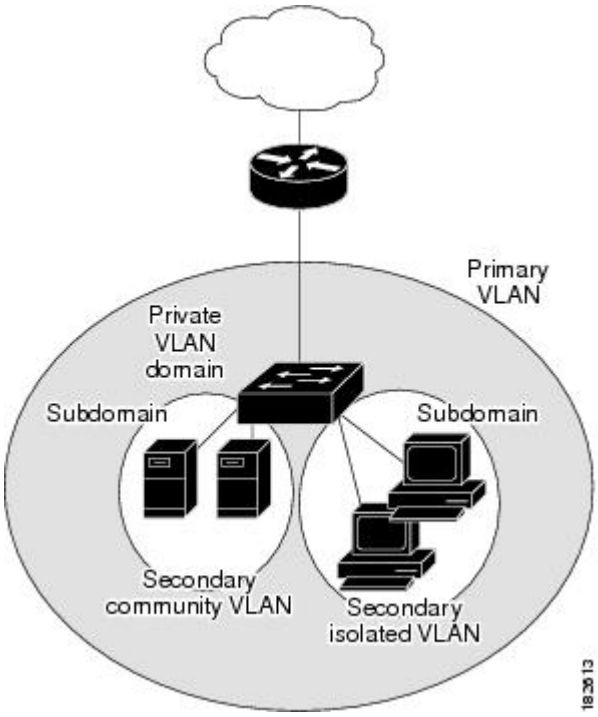
PVLANs achieve Layer 2 isolation through the use of three separate port designations, each having its own unique set of rules that regulate each connected endpoint's ability to communicate with other connected endpoints within the same private VLAN domain.

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 (c1 or c2 in the above figure) 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

Private VLANs have the following configuration guidelines and limitations:

- Control VLANs, packet VLANs, and management VLANs must be configured as regular VLANs and not as PVLANs.
- You should create port profiles with PVLAN configuration and associate them to uplink ports as part of OpenStack deployment.
- For configuring PVLANs on vETH interfaces, publish the port profiles with PVLAN configuration to OpenStack and associate them as policy profiles as part of creating a VM interface.

Default Settings

Table 2: Default VLAN Settings

Parameters	Default
Private VLANs	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. See Enabling or Disabling the Private VLAN Feature Globally, on page 5.

Step 2 Configure one or more VLANs as primary VLAN(s) on the VSM. See Configuring a VLAN as a Primary VLAN, on page 6.

Step 3 Configure a VLAN as a secondary VLAN on the VSM. See Configuring a VLAN as a Secondary VLAN, on page 7.

Step 4 Associate secondary VLANs to a PVLAN. See Associating the VLANs in a PVLAN, on page 8.

Step 5 Configure PVLAN port profiles for host uplink and OpenStack VMs. For more information, see the *Cisco Nexus 1000V for KVM Port Profile Configuration Guide* .

Step 6 Create a network segment in OpenStack for each PVLAN. For more information, see the *Cisco Nexus 1000V for KVM Virtual Network Configuration Guide*.

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	switch(config-vlan)# **show feature**	(Optional) Displays features available and whether they are enabled globally.
Step 4	switch(config-vlan)# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

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. For information about creating a VLAN, see Creating a 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.

	Command or Action	Purpose
Step 5	switch(config)# **show vlan private-vlan**	(Optional) Displays the PVLAN configuration.
Step 6	switch(config)# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

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
n1000v(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 secondary 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 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. For information about creating a VLAN, see Creating a 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.

	Command or Action	Purpose
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.
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 the VLAN configuration mode for the configurations to take affect.
Step 5	switch(config)# **show vlan private-vlan**	(Optional) Displays the PVLAN configuration.
Step 6	switch(config)# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

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
-------  ---------  ----------------  ------------------------------------------
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 secondary VLAN IDs to be associated for each primary VLAN ID.

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 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	switch(config)# **show vlan private-vlan**	(Optional) Displays the PVLAN configuration.
Step 6	switch(config)# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

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)#
```

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.
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)# **publish port-profile**	Pushes the port profile to the VEMs and to the OpenStack controller.
Step 9	switch(config-port-profile)# **state enabled**	Enables the port profile and applies its configuration to the assigned ports.

	Command or Action	Purpose
Step 10	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

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 2,202,150-155
switch(config-port-prof)# switchport private-vlan mapping trunk 202 303
switch(config-port-prof)# no shut
switch(config-port-prof)# publish port-profile
switch(config-port-prof)# state enabled
```

Configuring a Private VLAN Promiscuous Access Port

You can configure a port to be used as a promiscuous access port in a PVLAN.

Before You Begin

- Log in to the CLI in EXEC mode.
- Know the name of the interface that will function as a promiscuous access port.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type* [*slot/port* | *number*]	Enters interface configuration mode for the specified interface.
Step 3	switch(config-if)# **switchport mode private-vlan promiscuous**	Designates that the interface is to function as a promiscuous access port for a PVLAN in the running configuration.
Step 4	switch(config-if)# **show interface** *type* [*slot/port* | *number*]	(Optional) Displays the interface configuration.
Step 5	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to configure a PVLAN promiscuous access port:

```
switch# configure terminal
switch(config)# interface eth3/2
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# show interface eth3/2
Ethernet3/2 is up
    Hardware is Ethernet, address is 0050.5655.2e85 (bia 0050.5655.2e85)
    MTU 1500 bytes, BW -1942729464 Kbit, DLY 10 usec,
       reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA
    Port mode is promiscuous
    full-duplex, 1000 Mb/s
    Beacon is turned off
    Auto-Negotiation is turned on
    Input flow-control is off, output flow-control is off
    Rx
    276842 Input Packets 100419 Unicast Packets
    138567 Multicast Packets 37856 Broadcast Packets
    25812138 Bytes
    Tx
    128154 Output Packets 100586 Unicast Packets
    1023 Multicast Packets 26545 Broadcast Packets 26582 Flood Packets
    11630220 Bytes
    173005 Input Packet Drops 37 Output Packet Drops

switch(config-if)#
```

Associating a Promiscuous Access Port with a Private VLAN

You can associate the promiscuous access port 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 the primary and secondary VLANs that are already configured as PVLAN.
- Know the name of the interface functioning in the PVLAN as a promiscuous access port.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type* [*slot/port* | *number*]	Enters interface configuration mode for the specified interface.
Step 3	switch(config-if)# **switchport private-vlan mapping** *primary_vlan_ID* {*secondary_vlan_list* | **add** *secondary_vlan_list* | **remove** *secondary_vlan_list*}	Associates the promiscuous access port with the VLAN IDs in the PVLAN in the running configuration.
Step 4	switch(config-if)# **show interface** *type* [*slot/port* | *number*]	(Optional) Displays the interface configuration.

	Command or Action	Purpose
Step 5	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to associate a promiscuous access port with a PVLAN:

```
switch# configure terminal
switch(config)# interface eth3/2
switch(config-if)# switchport private-vlan mapping 202 303
switch(config-if)# show vlan private-vlan
Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------
202      303        community        Eth3/2

switch(config-if)#
```

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	switch(config)# **show vlan private-vlan**	(Optional) Displays the PVLAN configuration.

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

This example shows how to remove a PVLAN configuration:

```
switch# configure terminal
switch(config)# vlan 202
switch(config-vlan)# no private-vlan association secondary vlan-ids
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

switch# configure terminal
switch(config)# int eth2/6
switch(config-if)# switchport mode private-vlan trunk promiscuous
switch(config-if)# switchport private-vlan trunk allowed vlan all
switch(config-if)# switchport private-vlan mapping trunk 202 303, 440
switch(config-if)# switchport private-vlan mapping trunk 210 310, 450
switch(config-if)# show interface switchport
Name: Ethernet2/6
  Switchport: 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: 1-3967, 4048-4093
  Administrative private-vlan trunk private VLANs: (202,303) (202,440) (210,310) (210,450)
  Operational private-vlan: 202,210,303,310,440,450
switch(config-if)#
```

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 4.0(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#
```

Feature History for Private VLANs

Feature Name	Feature Name	Releases
Private VLAN	5.2(1)SK3(2.1)	This feature was introduced.