Configuring Private VLANs

This chapter contains the following sections:

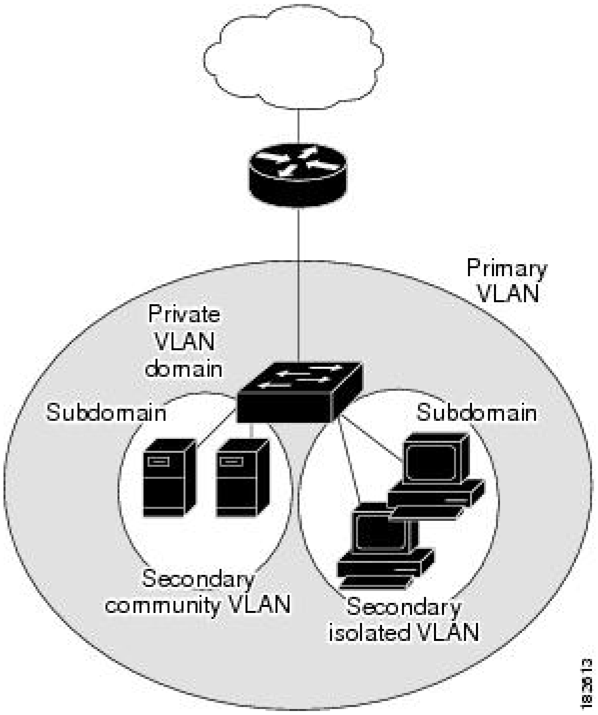
Information About Private VLANs

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

Private VLAN Domains

A private VLAN 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

Private VLANs can span multiple switches, just like regular VLANs. Inter-switch link ports need not be aware of the special VLAN type and carry frames tagged with these VLANs just like they do any other frames. Private VLANs 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 along with the packet, it is possible to maintain consistent behavior throughout the network. Therefore, the mechanism which 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 private VLAN domain, there are three separate port designations. Each port designation has its own unique set of rules which regulate the ability of one endpoint to communicate with other connected endpoints within the same private VLAN domain. The following are the three port designations:

- promiscuous
- isolated
- community

Primary VLANs and Promiscuous Ports

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

As the name suggests, a promiscuous port can talk to all other types of ports. A promiscuous port 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 private VLAN domain. A private VLAN domain can have one or more subdomains. A subdomain is made up of a VLAN pair consisting of the primary VLAN and a secondary VLAN. Since the primary VLAN is a part of every subdomain, secondary VLANs differentiate the VLAN subdomains.

In order to communicate to the Layer 3 interface, a secondary VLAN must be associated 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 private VLAN 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 (i1 or i2 in the above figure) 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, then 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.

  The distinct characteristic of an isolated VLAN is that it 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 consumed in providing this port isolation.

  Note While there can be multiple community VLANs in a private VLAN domain, one isolated VLAN is sufficient to serve multiple customers. All endpoints 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 sharing 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 have Layer 2 communications with one another and can also talk to any promiscuous port. If an ISP customer has, for example, 4 devices and wants them isolated from those of other customers but still be able to communicate among themselves, then community ports should be used.

  Note Because trunks can support a VLAN carrying traffic between its ports, it is possible for VLAN traffic to 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 private VLAN port types.

Table 1: Communication Between Private VLAN 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 traversing 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 VLAN has the following configuration guidelines and limitations:

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

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

Step 2 Configuring a VLAN as a Primary VLAN. SeeConfiguring a VLAN as a Primary VLAN, on page 6.

Step 3 Configuring a VLAN as a Secondary VLAN. See Configuring a VLAN as a Secondary VLAN, on page 7.

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

Step 5 Configuring a Private VLAN Host Port. See Configuring a Private VLAN Host Port, on page 8.

Step 6 Associating a Host Port with a Private VLAN. See Associating a Host Port with a Private VLAN, on page 10.

Step 7 Verifying a Private VLAN Configuration. See Verifying a Private VLAN Configuration, on page 16.

Enabling or Disabling the Private VLAN Feature Globally

Use this procedure to globally enable or disable the private VLAN 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 private VLAN feature.
Step 3	switch(config-vlan)# **show feature**	(Optional) Displays features available, such as PVLAN, 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.

```
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

Use this procedure to configure a VLAN to function as the primary VLAN in a PVLAN.

Before You Begin

- You are logged 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.
- The VLAN 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)# **show vlan private-vlan**	(Optional) Displays the PVLAN configuration.
Step 5	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.

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

switch(config-vlan)#
```

Configuring a VLAN as a Secondary VLAN

Use this procedure to configure a VLAN to function as the primary VLAN in a PVLAN.

Before You Begin

- You are logged 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.
- The VLAN 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.

- You 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.
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)# **show vlan private-vlan**	(Optional) Displays the PVLAN configuration.
Step 5	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.

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

switch(config-vlan)#
```

Associating the VLANs in a PVLAN

Use this procedure to associate the primary VLANs in a PVLAN with the secondary VLANs.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- The primary VLAN for this PVLAN is already configured as a PVLAN.
- The secondary VLANs for this PVLAN are already configured as PVLANs.
- You 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.
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)# **show vlan private-vlan**	(Optional) Displays the PVLAN configuration.
Step 5	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.

```
switch# configure terminal
switch(config)# vlan 202
switch(config-vlan)# private-vlan association add 303
switch(config-vlan)# show vlan private-vlan
Primary  Secondary  Type             Ports
-------  ---------  ---------------  -------------------------------------------
202      303        community        Veth1
n1000v(config-vlan)#
```

Configuring a Private VLAN Host Port

Use this procedure to configure an interface as a host port to function with a PVLAN.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- The primary VLAN for this PVLAN is already configured as a PVLAN.
- The secondary VLANs for this PVLAN are already configured as PVLANs.
- The secondary VLANs are already associated with the primary VLAN.
- You know the name of the interface to be used with the PVLAN as a host port.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface type** *if_id*	Enters interface configuration mode and creates a the named interface if it does not exist.
Step 3	switch(config-if)# **switchport mode private-vlan host**	Designates that the physical interface is to function as a PVLAN host port in the running configuration.
Step 4	switch(config-if)# **show interface type** *if_id*	(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.

```
switch# configure terminal
switch(config)# interface veth1
switch(config-if)# switchport mode private-vlan host
switch(config-if)# show interface veth1
Vethernet1 is up
    Hardware is Virtual, address is 0050.56b0.34c8
    Owner is VM "HAM61-RH5-32bit-ENVM-7.60.1.3"
    Active on module 2, host VISOR-HAM61.localdomain 0
    VMware DVS port 16777215
    Port-Profile is vlan631
    Port mode is Private-vlan host
    Rx
    48600 Input Packets 34419 Unicast Packets
    0 Multicast Packets 14181 Broadcast Packets
    4223732 Bytes
    Tx
    34381 Output Packets 34359 Unicast Packets
    22 Multicast Packets 0 Broadcast Packets 0 Flood Packets
    3368196 Bytes
    5 Input Packet Drops 11 Output Packet Drops

switch(config-if)#
```

Associating a Host Port with a Private VLAN

Use this procedure to associate the host port with the primary and secondary VLANs in a PVLAN.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You know the VLAN IDs of the primary and secondary VLANs in the PVLAN.
- The primary VLAN for this PVLAN is already configured as a PVLAN.
- The secondary VLANs for this PVLAN are already configured as PVLANs.
- You 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)# **interface type** *if_id*	Enters interface configuration mode and configures a name for the specified interface in the running configuration.
Step 3	switch(config-if)# **switchport private-vlan host-association** *primaryvlan-id secondary vlan-id*	Associates the host port with the primary and secondary VLAN IDs for the PVLAN in the running configuration. The interface is associated with the VLANs in the PVLAN.
Step 4	switch(config-if)# **show interface type***if_id*	(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.

```
switch# configure terminal
switch(config)# interface veth1
switch(config-if)# switchport private-vlan host-association 202 303
switch(config-if)# show interface veth1
Name: Vethernet1
Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: access
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: 202
  Administrative private-vlan secondary host-association: 203
  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:
  Operational private-vlan: 202, 203

switch(config-if)#
```

Configuring a Layer 2 Interface as a Promiscuous Trunk Port

Use this procedure to 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

- You are logged in to the CLI in EXEC mode.
- The **private-vlan mapping trunk** command does not decide or override the trunk configuration of a port.
- The port is already configured in a regular trunk mode before adding the private-vlan trunk configurations.
- Primary VLANs must be added to the list of allowed VLAN for the promiscuous trunk port.
- Secondary VLANs are not configured in the allowed VLAN list.
- The trunk port can carry normal VLANs in addition to primary VLANs.
- 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)# **interface** *type slot/port*	Enters interface configuration mode for the specified interface.
Step 3	switch(config-if)# **switchport mode private-vlan trunk promiscuous**	In the running configuration, designates the interface as a promiscuous private-vlan trunk port.
Step 4	switch(config-if)# **switchport private-vlan trunk allowed vlan all**	In the running configuration, designates that the private-vlan trunk port will carry all normal VLANs.

	Command or Action	Purpose
Step 5	switch(config-if)# **switchport private-vlan mapping trunk** *primary_vlan_ID* { *secondary_vlan_list* | **add** *secondary_vlan_list* | **remove** *secondary_vlan_list* }	Maps the private-vlan trunk port to a primary VLAN and to selected secondary VLANs in the running configuration. Multiple private-vlan pairs can be specified so that a promiscuous trunk port can carry multiple primary VLANs.
Step 6	switch(config-if)# **switchport private-vlan trunk native vlan** *vlan_ID*	Sets the private vlan trunking native configuration. *vlan_id*: The VLAN (1-3967, 4048-4093) to be used as a native VLAN for the private VLAN trunk port.
Step 7	switch(config-if)# **show interfaces** [*type slot/port*] **switchport**	(Optional) Displays the configuration for verification.
Step 8	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.

```
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)# switchport private-vlan mapping trunk 210 add 451,460
switch(config-if)# switchport private-vlan mapping trunk 210 remove 310
switch(config-if)# switchport private-vlan trunk native vlan 100
switch(config-if)#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: 25-27
  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: 100
  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) (210,450) (210,451)
 (210,460)
  Operational private-vlan: 202,210,303,440,450-451,460

switch(config-if)#
```

Configuring a Private VLAN Promiscuous Access Port

Use this procedure to configure a port to be used as a promiscuous access port in a PVLAN.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You 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.

```
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)#
switch# configure terminal
switch(config)# interface vethernet1
n1000v(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# show interface vethernet 1
Vethernet1 is up
  Port description is VM-1, Network Adapter 7
  Hardware: Virtual, address: 0050.569e.009f (bia 0050.569e.009f)
  Owner is VM "VM-1", adapter is Network Adapter 7
  Active on module 5
  VMware DVS port 5404
  Port-Profile is pri_25
  Port mode is Private-vlan promiscuous
  5 minute input rate 0 bits/second, 0 packets/second
  5 minute output rate 7048 bits/second, 2 packets/second
  Rx
    20276 Input Packets 379239 Unicast Packets
    24 Multicast Packets 1395 Broadcast Packets
    1428168 Bytes
  Tx
    256229 Output Packets 74946 Unicast Packets
    16247 Multicast Packets 2028117 Broadcast Packets 190123 Flood Packets
    44432239 Bytes
    162 Input Packet Drops 159 Output Packet Drops

switch(config-if)#
```

Associating a Promiscuous Access Port with a Private VLAN

Use this procedure to associate the promiscuous access port with the primary and secondary VLANs in a PVLAN.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You know the VLAN IDs of the primary and secondary VLANs in the PVLAN.
- The primary and secondary VLANs are already configured as PVLAN.
- You 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.
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.

```
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, Veth1

switch(config-if)#
```

Removing a Private VLAN Configuration

Use this procedure to remove a private VLAN configuration and return the VLAN to normal VLAN mode.

Before You Begin

- You are logged 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)# **show vlan private-vlan**	(Optional) Displays the PVLAN configuration.
Step 5	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.

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

switch(config-vlan)#
```

Verifying a Private VLAN Configuration

Use the following commands to verify a private VLAN configuration:

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

Configuration Example for Private VLAN

Example: PVLAN Trunk Port

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

- private VLAN trunk port
- mapped to primary private VLAN 202 which is associated with secondary VLANs 303 and 440
- mapped to primary private VLAN 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 440,450
switch(config-vlan)# private-vlan isolated

switch(config)# vlan 202
switch(config-vlan)# private-vlan primary
switch(config-vlan)# private-vlan association 303,440

switch(config)# vlan 210
switch(config-vlan)# private-vlan primary
switch(config-vlan)# private-vlan association 310,450

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

The following 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 primary VLAN 156 as a result of the command, **switchport private-vlan mapping trunk 156 153-155**.

```
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 VLAN

Feature Name	Feature Name	Releases
feature private-vlan command	4.2(1)SV1(4)	The ability to globally enable the private VLAN feature.
Private VLAN	4.0(4)SV1(1)	This feature was introduced.