CHAPTER 38

# Configuring Private VLANs

This chapter describes private VLANs (PVLANs) on Catalyst 4500 series switches. It also provides restrictions, procedures, and configuration examples.

This chapter includes the following major sections:


- Command List, page 38-1
- Overview of PVLANs, page 38-2
- Configuring PVLANs, page 38-9
- Troubleshooting PVLANs, page 38-21


**Note** For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at this location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cr/index.htm.

## Command List

This table lists the commands most commonly used with PVLANs.

| Command | Purpose | Location |
|---|---|---|
| **private-vlan** {**community** \| **isolated** \| **primary**} | Configures a VLAN as a PVLAN. | Configuring a VLAN as a PVLAN, page 38-12 |
| **private-vlan association** {*secondary_vlan_list* \| **add** *secondary_vlan_list* \| **remove** *secondary_vlan_list*} | Associates the secondary VLAN with the primary VLAN. The list can contain only one VLAN. | Associating a Secondary VLAN with a Primary VLAN, page 38-13 |
| **show vlan private-vlan** [**type**] | Verifies the configuration. | Configuring a VLAN as a PVLAN, page 38-12<br>Associating a Secondary VLAN with a Primary VLAN, page 38-13 |
| **show interface private-vlan mapping** | Verifies the configuration. | Permitting Routing of Secondary VLAN Ingress Traffic, page 38-20 |

| Command | Purpose | Location |
|---|---|---|
| **switchport mode private-vlan** {**host** \| **promiscuous** \| **trunk promiscuous** \| **trunk** [**secondary**]} | Configures a Layer 2 interface as a PVLAN port. | Configuring PVLANs, page 38-9 |
| **switchport private-vlan mapping** [**trunk**] *primary_vlan_ID* {*secondary_vlan_list* \| **add** *secondary_vlan_list* \| **remove** *secondary_vlan_list*} | Maps the PVLAN promiscuous port to a primary VLAN and to selected secondary VLANs. | Configuring a Layer 2 Interface as a PVLAN Promiscuous Port, page 38-14<br>Configuring a Layer 2 Interface as a Promiscuous Trunk Port, page 38-18 |
| Switch(config-if)# **switchport private-vlan host-association** *primary_vlan_ID secondary_vlan_ID* | Associates the Layer 2 interface with a PVLAN. | Configuring a Layer 2 Interface as a PVLAN Host Port, page 38-16 |
| **switchport private-vlan association trunk** *primary_vlan_ID secondary_vlan_ID* | Configures association between primary VLANs and secondary VLANs the PVLAN trunk port with a PVLAN. | Configuring a Layer 2 Interface as a PVLAN Trunk Port, page 38-17 |
| **switchport private-vlan trunk allowed vlan** *vlan_list* **all** \| **none** \| [**add** \| **remove** \| **except**] *vlan_atom*[,*vlan_atom*...] | Configures a list of allowed normal VLANs on a PVLAN trunk port. | Configuring a Layer 2 Interface as a PVLAN Trunk Port, page 38-17 |
| **switchport private-vlan trunk native vlan** *vlan_id* | Configures a VLAN to which untagged packets (as in IEEE 802.1Q tagging) are assigned on a PVLAN trunk port. | Configuring a Layer 2 Interface as a PVLAN Trunk Port, page 38-17 |

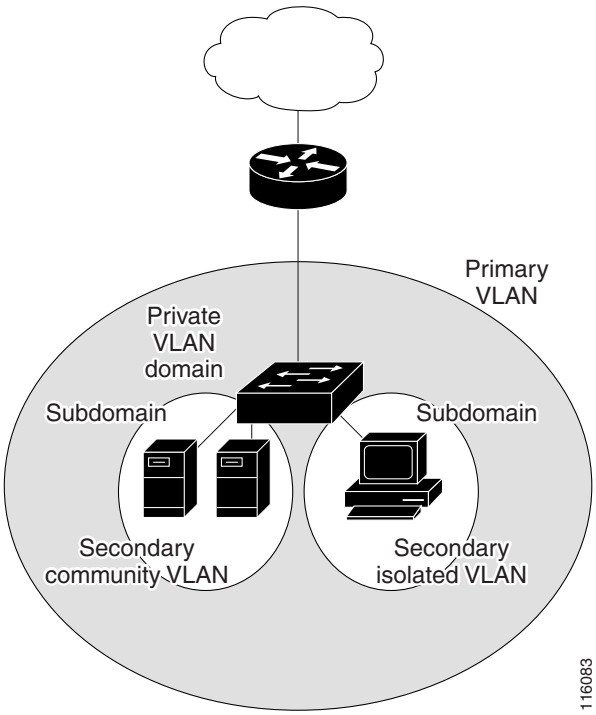
# Overview of PVLANs

The private VLAN feature addresses two problems that service providers face when using VLANs:

- The switch supports up to 1005 active VLANs. If a service provider assigns one VLAN per customer, this limits the numbers of customers the service provider can support.
- To enable IP routing, each VLAN is assigned a subnet address space or a block of addresses, which can result in wasting the unused IP addresses, and cause IP address management problems.

Using private VLANs provides scalability and IP address management benefits for service providers and Layer 2 security for customers. Private VLANs partition a regular VLAN domain into subdomains. A subdomain is represented by a pair of VLANs: a *primary* VLAN and a *secondary* VLAN. A private VLAN can have multiple VLAN pairs, one pair for each subdomain. All VLAN pairs in a private VLAN share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. See Figure 38-1.

*Figure 38-1 Private-VLAN Domain*




There are two types of secondary VLANs:

- Isolated VLANs—Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level.
- Community VLANs—Ports within a community VLAN can communicate with each other but cannot communicate with ports in other communities at the Layer 2 level.

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs. Layer 3 gateways are typically connected to the switch through a promiscuous port.

In a switched environment, you can assign an individual private VLAN and associated IP subnet to each individual or common group of end stations. The end stations need to communicate only with a default gateway to communicate outside the private VLAN.

You can use private VLANs to control access to end stations in these ways:

- Configure selected interfaces connected to end stations as isolated ports to prevent any communication at Layer 2. For example, if the end stations are servers, this configuration prevents Layer 2 communication between the servers.
- Configure interfaces connected to default gateways and selected end stations (such as, backup servers) as promiscuous ports to allow all end stations access to a default gateway.
- Reduce VLAN and IP subnet consumption; you can prevent traffic between end stations even though they are in the same VLAN and IP subnet.

  With a promiscuous port, you can connect a wide range of devices as access points to a PVLAN. For example, you can connect a promiscuous port to the server port of a LocalDirector to connect an isolated VLAN or a number of community VLANs to the server. LocalDirector can load balance the servers present in the isolated or community VLANs, or you can use a promiscuous port to monitor or back up all the PVLAN servers from an administration workstation.

This section includes the following topics:


- Definition Table, page 38-4
- Standard Trunk Ports, page 38-5
- Private VLANs across Multiple Switches, page 38-5
- Private-VLAN Interaction with Other Features, page 38-8


# Definition Table

| Term | Definition |
|---|---|
| Private VLANs | Private VLANs are sets of VLAN pairs that share a common primary identifier and provide a mechanism for achieving layer-2 separation between ports while sharing a single layer-3 router port and IP subnet. |
| Secondary VLAN | A type of VLAN used to implement private VLANs. Secondary VLANs are associated with a primary VLAN, and are used to carry traffic from hosts to other allowed hosts or to routers. |
| Community Port | A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities and from isolated ports within their private VLAN. |
| Community VLAN | Community VLAN—A community VLAN is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port gateways and to other host ports in the same community. You can configure multiple community VLANs in a private VLAN. |
| Isolated Port | An isolated port is a host port that belongs to an isolated secondary VLAN. It has complete Layer 2 separation from other ports within the same private VLAN, except for the promiscuous ports. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports. |
| Isolated VLAN | Isolated VLAN —A private VLAN has only one isolated VLAN. An isolated VLAN is a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports and the gateway. |
| Primary VLAN | Primary VLAN—A private VLAN has only one primary VLAN. Every port in a private VLAN is a member of the primary VLAN. The primary VLAN carries unidirectional traffic downstream from the promiscuous ports to the (isolated and community) host ports and to other promiscuous ports. |

| Term | Definition |
|---|---|
| Private VLAN Trunk Port | A PVLAN trunk port can carry multiple secondary (isolated only) and non-PVLANs. Packets are received and transmitted with secondary or regular VLAN tags on the PVLAN trunk ports.<br>**Note** Only IEEE 802.1q encapsulation is supported. |
| Promiscuous Port | A promiscuous port belongs to the primary VLAN and can communicate with all interfaces, including the community and isolated host ports and private VLAN trunk ports that belong to the secondary VLANs associated with the primary VLAN. |
| Promiscuous Trunk Port | A promiscuous trunk port can carry multiple primary and normal VLANs. Packets are received and transmitted with primary or regular VLAN tags. Other than that, the port behaves just like a promiscuous access port.<br>**Note** Only IEEE 802.1q encapsulation is supported. |

# Private VLANs across Multiple Switches

This section discusses the following topics:


- Standard Trunk Ports, page 38-5
- Private VLAN Trunks, page 38-6


## Standard Trunk Ports

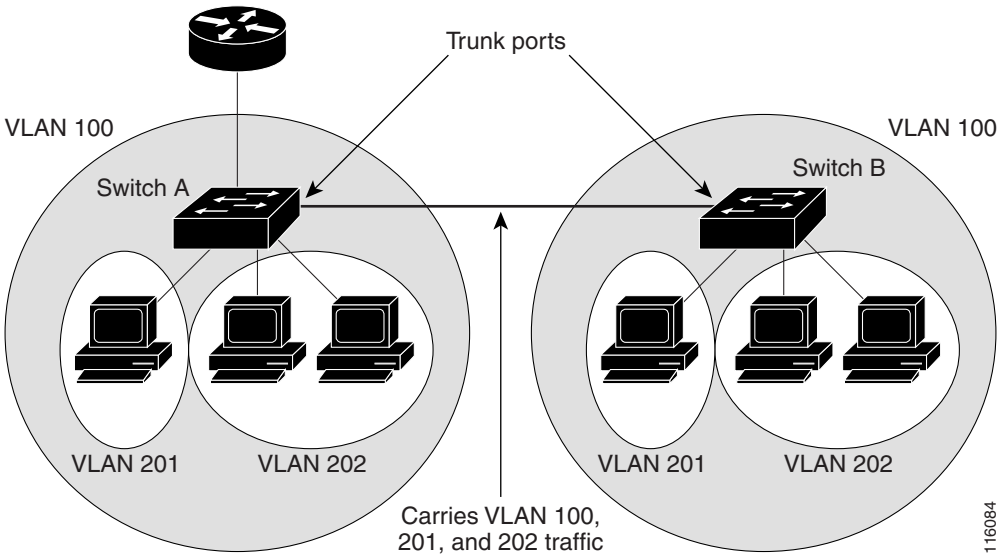
As with regular VLANs, private VLANs can span multiple switches. A trunk port carries the primary VLAN and secondary VLANs to a neighboring switch. The trunk port treats the private VLAN as any other VLAN. A feature of private VLANs across multiple switches is that traffic from an isolated port in switch A does not reach an isolated port on Switch B. See Figure 38-2.

To maintain the security of your private-VLAN configuration and to avoid other use of the VLANs configured as private VLANs, configure private VLANs on all intermediate devices, including devices that have no private-VLAN ports.

**Note** Trunk ports carry traffic from regular VLANs and also from primary, isolated, and community VLANs.

**Note** You should use standard trunk ports if both switches undergoing trunking support PVLANs.

*Figure 38-2 Private VLANs across Switches*




VLAN 100 = Primary VLAN
VLAN 201 = Secondary isolated VLAN
VLAN 202 = Secondary community VLAN

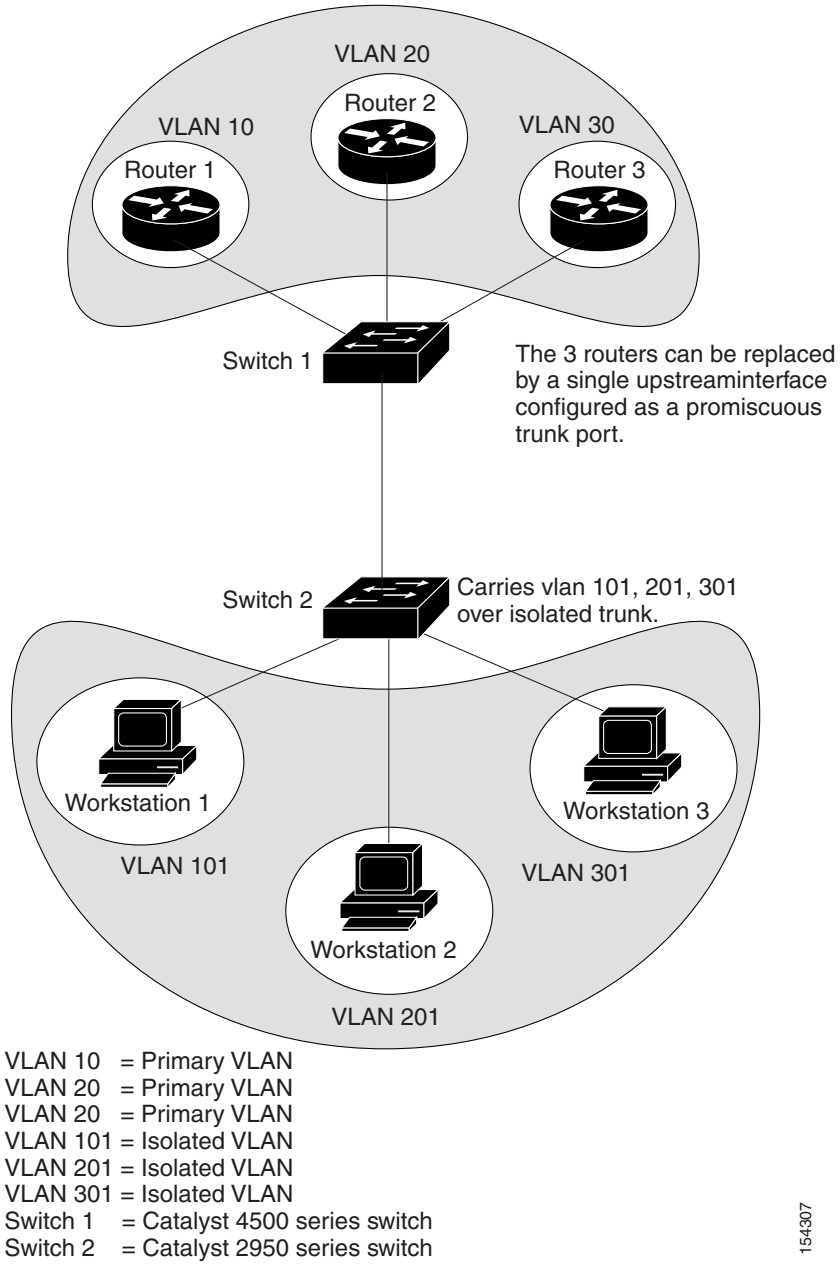
Because VTP does not support private VLANs, you must manually configure private VLANs on all switches in the Layer 2 network. If you do not configure the primary and secondary VLAN association in some switches in the network, the Layer 2 databases in these switches are not merged. This can result in unnecessary flooding of private-VLAN traffic on those switches.

## Private VLAN Trunks

A private VLAN isolated trunk is used when you want a private VLAN port to carry multiple secondary VLANs.

Figure 38-3 provides a typical topology.

*Figure 38-3 Private VLAN Trunk Topology*




In this topology, switch 1 trunks traffic for all isolated VLANs over a private VLAN trunk to Switch 2 that does not understand private VLANs. It also communicates with different routers connected to different promiscuous ports. Switch 2 is connected to multiple hosts that belong to different secondary VLANs.

Isolated trunk ports allow you to combine traffic for all secondary ports over a trunk.

Promiscuous trunk ports allow you to combine the multiple promiscuous ports required in this topology in a single trunk port that carries multiple primary VLANs.

# Private-VLAN Interaction with Other Features

Private VLANs have specific interaction with some other features, described in these sections:


- PVLANs and VLAN ACL/QoS, page 38-8
- Private VLANs and Unicast, Broadcast, and Multicast Traffic, page 38-8
- Private VLANs and SVIs, page 38-9


You should also see the "PVLAN Configuration Guidelines and Restrictions" section on page 38-10 for details.

## PVLANs and VLAN ACL/QoS

PVLAN ports use primary and secondary VLANs, as follows:

- A packet received on a PVLAN host port belongs to the secondary VLAN.
- A packet received on a PVLAN trunk port belongs to the secondary VLAN if the packet is tagged with a secondary VLAN or if the packet is untagged and the native VLAN on the port is a secondary VLAN.

A packet received on a PVLAN host or trunk port and assigned to a secondary VLAN is bridged on the secondary VLAN. Because of this bridging, the secondary VLAN ACL as well as the secondary VLAN QoS (on input direction) apply.

When a packet is transmitted out of a PVLAN host or trunk port, the packet logically belongs to the primary VLAN. This relationship applies even though the packet may be transmitted with the secondary VLAN tagging for PVLAN trunk ports. In this situation, the primary VLAN ACL and the primary VLAN QoS on output apply to the packet.

- Similarly, a packet received on a PVLAN promiscuous access port belongs to primary VLAN.
- A packet received on a PVLAN promiscuous trunk port could belong to the primary VLAN or normal VLAN depending on incoming VLAN.

For traffic flowing in normal VLAN on promiscuous trunk ports, normal VLAN ACL and QoS policies apply. For traffic flowing in a private VLAN domain, a packet received on a promiscuous port is bridged in primary VLAN. Therefore, the primary VLAN ACL and QoS policies apply on input.

When a packet is transmitted out of a promiscuous trunk port, the packet could logically belong to secondary VLAN if received from a secondary port, or in primary VLAN if bridged from another promiscuous port. Because we cannot differentiate between both packets, all VLAN QoS policies are ignored on packets egressing promiscuous trunk ports.

## Private VLANs and Unicast, Broadcast, and Multicast Traffic

In regular VLANs, devices in the same VLAN can communicate with each other at the Layer 2 level, but devices connected to interfaces in different VLANs must communicate at the Layer 3 level. In private VLANs, the promiscuous ports are members of the primary VLAN, while the host ports belong to secondary VLANs. Because the secondary VLAN is associated to the primary VLAN, members of the these VLANs can communicate with each other at the Layer 2 level.

In a regular VLAN, broadcasts are forwarded to all ports in that VLAN. Private VLAN broadcast forwarding depends on the port sending the broadcast:

- An isolated port sends a broadcast only to the promiscuous ports or trunk ports.
- A community port sends a broadcast to all promiscuous ports, trunk ports, and ports in the same community VLAN.
- A promiscuous port sends a broadcast to all ports in the private VLAN (other promiscuous ports, trunk ports, isolated ports, and community ports).

Multicast traffic is routed or bridged across private-VLAN boundaries and within a single community VLAN. Multicast traffic is not forwarded between ports in the same isolated VLAN or between ports in different secondary VLANs.

### Private VLANs and SVIs

In a Layer 3 switch, a switch virtual interface (SVI) represents the Layer 3 interface of a VLAN. Layer 3 devices communicate with a private VLAN only through the primary VLAN and not through secondary VLANs. Configure Layer 3 VLAN interfaces (SVIs) only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

- If you try to configure a VLAN with an active SVI as a secondary VLAN, the configuration is not allowed until you disable the SVI.
- If you try to create an SVI on a VLAN that is configured as a secondary VLAN and the secondary VLAN is already mapped at Layer 3, the SVI is not created, and an error is returned. If the SVI is not mapped at Layer 3, the SVI is created, but it is automatically shut down.

When the primary VLAN is associated with and mapped to the secondary VLAN, any configuration on the primary VLAN is propagated to the secondary VLAN SVIs. For example, if you assign an IP subnet to the primary VLAN SVI, this subnet is the IP subnet address of the entire private VLAN.

## Configuring PVLANs

These sections describe how to configure PVLANs:

- Tasks for Configuring Private VLANs, page 38-10
- Default Private-VLAN Configuration, page 38-10
- PVLAN Configuration Guidelines and Restrictions, page 38-10
- Configuring a VLAN as a PVLAN, page 38-12
- Associating a Secondary VLAN with a Primary VLAN, page 38-13
- Configuring a Layer 2 Interface as a PVLAN Promiscuous Port, page 38-14
- Configuring a Layer 2 Interface as a PVLAN Host Port, page 38-16
- Configuring a Layer 2 Interface as a PVLAN Trunk Port, page 38-17
- Configuring a Layer 2 Interface as a Promiscuous Trunk Port, page 38-18
- Permitting Routing of Secondary VLAN Ingress Traffic, page 38-20

# Tasks for Configuring Private VLANs

To configure a PVLAN, follow these steps:

**Step 1** Set VTP mode to transparent. See the "Disabling VTP (VTP Transparent Mode)" section on page 13-16.

**Step 2** Create the secondary VLANs. See the "Configuring a VLAN as a PVLAN" section on page 38-12.

**Step 3** Create the primary VLAN. See the "Configuring a VLAN as a PVLAN" section on page 38-12.

**Step 4** Associate the secondary VLAN to the primary VLAN. See the "Associating a Secondary VLAN with a Primary VLAN" section on page 38-13.

**Note** Only one isolated VLAN can be mapped to a primary VLAN, but more than one community VLAN can be mapped to a primary VLAN.

**Step 5** Configure an interface as an isolated or community host or trunk port. See the "Configuring a Layer 2 Interface as a PVLAN Host Port" section on page 38-16 and "Configuring a Layer 2 Interface as a PVLAN Trunk Port" section on page 38-17.

**Step 6** Associate the isolated port or community port to the primary-secondary VLAN pair. See the "Associating a Secondary VLAN with a Primary VLAN" section on page 38-13.

**Step 7** Configure an interface as a promiscuous port. See the "Configuring a Layer 2 Interface as a PVLAN Promiscuous Port" section on page 38-14.

**Step 8** Map the promiscuous port to the primary-secondary VLAN pair. See the "Configuring a Layer 2 Interface as a PVLAN Promiscuous Port" section on page 38-14.

**Step 9** If you plan to use inter-VLAN routing, configure the primary SVI, and map secondary VLANs to the primary. See the "Permitting Routing of Secondary VLAN Ingress Traffic" section on page 38-20.

**Step 10** Verify private-VLAN configuration. See the "Troubleshooting PVLANs" section on page 38-21.

# Default Private-VLAN Configuration

No private VLANs are configured.

# PVLAN Configuration Guidelines and Restrictions

Follow these guidelines when configuring PVLANs:

- To configure a PVLAN correctly, enable VTP in transparent mode.

  You cannot change the VTP mode to client or server for PVLANs.
- Do not include VLAN 1 or VLANs 1002 through 1005 in PVLANs.
- Use only PVLAN commands to assign ports to primary, isolated, or community VLANs.

  Layer 2 interfaces on primary, isolated, or community VLANs are inactive in PVLANs. Layer 2 trunk interfaces remain in the STP forwarding state.
- You cannot configure Layer 3 VLAN interfaces for secondary VLANs.

Layer 3 VLAN interfaces for isolated and community (secondary) VLANs are inactive while the VLAN is configured as an isolated or community VLAN.

- Do not configure private VLAN ports as EtherChannels. While a port is part of the private VLAN configuration, its associated EtherChannel configuration is inactive.
- Do not apply dynamic access control entries (ACEs) to primary VLANs.

  Cisco IOS dynamic ACL configuration applied to a primary VLAN is inactive while the VLAN is part of the PVLAN configuration.
- To prevent spanning tree loops due to misconfigurations, enable PortFast on the PVLAN trunk ports with the **spanning-tree portfast trunk** command.
- Any VLAN ACL configured on a secondary VLAN is effective in the input direction, and any VLAN ACL configured on the primary VLAN associated with the secondary VLAN is effective in the output direction.
- You can stop Layer 3 switching on an isolated or community VLAN by deleting the mapping of that VLAN with its primary VLAN.
- PVLAN ports can be on different network devices as long as the devices are trunk-connected and the primary and secondary VLANs remain associated with the trunk
- Isolated ports on two different devices cannot communicate with each other, but community VLAN ports can.
- Private VLANs support the following SPAN features:
  - You can configure a private VLAN port as a SPAN source port.
  - You can use VLAN-based SPAN (VSPAN) on primary, isolated, and community VLANs or use SPAN on only one VLAN to monitor egress or ingress traffic separately.

  For more information about SPAN, see Chapter 41, “Configuring SPAN and RSPAN.”
- A primary VLAN can be associated with multiple community VLANs, but only one isolated VLAN.
- An isolated or community VLAN can be associated with only one primary VLAN.
- If you delete a VLAN used in a private VLAN configuration, the private VLAN ports associated with the VLAN become inactive.
- VTP does not support private VLANs. You must configure private VLANs on each device in which you plan to use private VLAN ports.
- To maintain the security of your PVLAN configuration and avoid other use of VLANs configured as PVLANs, configure PVLANs on all intermediate devices, even if the devices have no PVLAN ports.
- Prune the PVLANs from trunks on devices that carry no traffic in the PVLANs.
- With port ACLS functionality available, you can apply Cisco IOS ACLS to secondary VLAN ports and Cisco IOS ACLS to PVLANS (VACLs). For more information on VACLs, see Chapter 37, “Configuring Network Security with ACLs.”
- You can apply different quality of service (QoS) configurations to primary, isolated, and community VLANs. (See Chapter 30, “Configuring Quality of Service.”) Cisco IOS ACLs applied to the Layer 3 VLAN interface of a primary VLAN automatically apply to the associated isolated and community VLANs.
- On a PVLAN trunk port a secondary VLAN ACL is applied on ingress traffic and a primary VLAN ACL is applied on egress traffic.
- On a promiscuous port the primary VLAN ACL is applied on ingress traffic.

- Both PVLAN secondary and promiscuous trunk ports support only IEEE 802.1q encapsulation.
- Community VLANs cannot be propagated or carried over private VLAN trunks.
- ARP entries learned on Layer 3 PVLAN interfaces are termed “sticky” ARP entries (we recommend that you display and verify PVLAN interface ARP entries).
- For security reasons, PVLAN port sticky ARP entries do not age out. Connecting a device with a different MAC address but with the same IP address generates an error message and the ARP entry is not created.
- Because PVLAN port sticky ARP entries do not age out, you must manually remove the entries if you change the MAC address. To overwrite a sticky ARP entry, first delete the entry with the **no arp** command, then overwrite the entry with the **arp** command.
- In a DHCP environment, if you shut down your PC, it is not possible to give your IP address to someone else. To solve this problem, the Catalyst 4500 series switch supports the **no ip sticky-arp** command. This command promotes IP address overwriting and reuse in a DHCP environment.
- Normal VLANs can be carried on a promiscuous trunk port.
- The default native VLAN for promiscuous trunk port is VLAN 1, the management VLAN. All untagged packets are forwarded in the native VLAN. Either the primary VLANs or a regular VLAN can be configured as native VLAN.
- Promiscuous trunks cannot be configured to carry secondary VLANs. If a secondary VLAN is specified in the allowed VLAN list, the configuration is accepted but the port is not operational/forwarding in the secondary VLAN. This includes even those VLANs that are of scondary but not associated with any primary VLAN on given port.
- On a promiscuous trunk port, the primary VLAN ACL and QoS are applied on ingress traffic coming in primary VLANs.
- On a promiscuous trunk port, no VLAN ACL or QoS is applied to the egress traffic. This is because for upstream direction, traffic in private VLAN logically flows in the secondary VLAN. Due to VLAN translation in hardware, information about received secondary VLANs has been lost. Hence, no policies are applied. This restriction also applies to traffic bridged from other ports in the same primary VLANs.
- Do not configure port security on PVLAN promiscuous trunk port and vice versa.

  If port security is enabled on a promiscuous trunk port, that port may behave in an unpredictable manner because this functionality is not supported.
- Do not configure IEEE 802.1X on a PVLAN promiscuous trunk port.

# Configuring a VLAN as a PVLAN

To configure a VLAN as a PVLAN, perform this task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# configure terminal` | Enters configuration mode. |
| **Step 2** | `Switch(config)# vlan vlan_ID` | Enters VLAN configuration mode. |

| | Command | Purpose |
|---|---|---|
| **Step 3** | `Switch(config-vlan)# private-vlan {community \| isolated \| primary}` | Configures a VLAN as a PVLAN.<br>• This command does not take effect until you exit VLAN configuration submode.<br>You can use the **no** keyword to clear PVLAN status. |
| **Step 4** | `Switch(config-vlan)# end` | Exits VLAN configuration mode. |
| **Step 5** | `Switch# show vlan private-vlan [type]` | Verifies the configuration. |

This example shows how to configure VLAN 202 as a primary VLAN and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# end
Switch# show vlan private-vlan
Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
```

This example shows how to configure VLAN 303 as a community VLAN and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 303
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
        303       community
```

This example shows how to configure VLAN 440 as an isolated VLAN and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 440
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
        303       community
        440       isolated
```

# Associating a Secondary VLAN with a Primary VLAN

To associate secondary VLANs with a primary VLAN, perform this task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# configure terminal` | Enters configuration mode. |
| **Step 2** | `Switch(config)# vlan primary_vlan_ID` | Enters VLAN configuration mode for the primary VLAN. |

| | Command | Purpose |
|---|---|---|
| **Step 3** | `Switch(config-vlan)# private-vlan association {secondary_vlan_list \| add secondary_vlan_list \| remove secondary_vlan_list}` | Associates the secondary VLAN with the primary VLAN. The list can contain only one VLAN.<br>You can use the **no** keyword to clear all secondary associations. |
| **Step 4** | `Switch(config-vlan)# end` | Exits VLAN configuration mode. |
| **Step 5** | `Switch# show vlan private-vlan [type]` | Verifies the configuration. |

When you associate secondary VLANs with a primary VLAN, note the following:

- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private VLAN ID or a hyphenated range of private VLAN IDs.
- The *secondary_vlan_list* parameter can contain multiple community VLAN IDs.
- The *secondary_vlan_list* parameter can contain only one isolated VLAN ID.
- Enter a *secondary_vlan_list* or use the **add** keyword with a *secondary_vlan_list* to associate secondary VLANs with a primary VLAN.
- Use the **remove** keyword with a *secondary_vlan_list* to clear the association between secondary VLANs and a primary VLAN.
- The command does not take effect until you exit VLAN configuration submode.

This example shows how to associate community VLANs 303 through 307 and 309 and isolated VLAN 440 with primary VLAN 202 and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan association 303-307,309,440
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202     303       community
202     304       community
202     305       community
202     306       community
202     307       community
202     309       community
202     440       isolated
        308       community
```

**Note** The secondary VLAN 308 has no associated primary VLAN.

# Configuring a Layer 2 Interface as a PVLAN Promiscuous Port

To configure a Layer 2 interface as a PVLAN promiscuous port, perform this task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | `Switch(config)# interface {fastethernet \| gigabitethernet \| tengigabitethernet} slot/port` | Specifies the LAN interface to configure. |

| | Command | Purpose |
|---|---|---|
| **Step 3** | `Switch(config-if)# switchport mode private-vlan {host \| promiscuous \| trunk promiscuous \| trunk [secondary]}` | Configures a Layer 2 interface as a PVLAN promiscuous port. |
| **Step 4** | `Switch(config-if)# [no] switchport private-vlan mapping [trunk] primary_vlan_ID {secondary_vlan_list \| add secondary_vlan_list \| remove secondary_vlan_list}` | Maps the PVLAN promiscuous port to a primary VLAN and to selected secondary VLANs. |
| **Step 5** | `Switch(config-if)# end` | Exits configuration mode. |
| **Step 6** | `Switch# show interfaces {fastethernet \| gigabitethernet \| tengigabitethernet} slot/port switchport` | Verifies the configuration. |

**Note** The maximum number of unique private VLAN pairs supported by the **switchport private-vlan mapping trunk** command above is 500. For example, one thousand secondary VLANs could map to one primary VLAN, or one thousand secondary VLANs could map one to one to one thousand primary VLANs.

When you configure a Layer 2 interface as a PVLAN promiscuous port, note the following:

- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single PVLAN ID or a hyphenated range of PVLAN IDs.
- Enter a *secondary_vlan_list* or use the **add** keyword with a *secondary_vlan_list* to map the secondary VLANs to the PVLAN promiscuous port.
- Use the **remove** keyword with a *secondary_vlan_list* to clear the mapping between secondary VLANs and the PVLAN promiscuous port.

This example shows how to configure interface FastEthernet 5/2 as a PVLAN promiscuous port, map it to a PVLAN, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 200 2
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name:Fa5/2
Switchport:Enabled
Administrative Mode:private-vlan promiscuous
Operational Mode:private-vlan promiscuous
Administrative Trunking Encapsulation:negotiate
Operational Trunking Encapsulation:native
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Voice VLAN:none
Administrative Private VLAN Host Association:none
Administrative Private VLAN Promiscuous Mapping:200 (VLAN0200) 2 (VLAN0002)
Private VLAN Trunk Native VLAN:none
Administrative Private VLAN Trunk Encapsulation:dot1q
Administrative Private VLAN Trunk Normal VLANs:none
Administrative Private VLAN Trunk Private VLANs:none
Operational Private VLANs:
  200 (VLAN0200) 2 (VLAN0002)
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
```

```
Capture Mode Disabled
Capture VLANs Allowed:ALL
```

# Configuring a Layer 2 Interface as a PVLAN Host Port

To configure a Layer 2 interface as a PVLAN host port, perform this task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# configure terminal` | Enters configuration mode. |
| **Step 2** | `Switch(config)# interface {fastethernet \| gigabitethernet \| tengigabitethernet} slot/port` | Specifies the LAN port to configure. |
| **Step 3** | `Switch(config-if)# switchport mode private-vlan {host \| promiscuous \| trunk promiscuous \| trunk [secondary]}` | Configures a Layer 2 interface as a PVLAN host port. |
| **Step 4** | `Switch(config-if)# [no] switchport private-vlan host-association primary_vlan_ID secondary_vlan_ID` | Associates the Layer 2 interface with a PVLAN.<br>You can use the **no** keyword to delete all associations from the primary VLAN. |
| **Step 5** | `Switch(config-if)# end` | Exits configuration mode. |
| **Step 6** | `Switch# show interfaces {fastethernet \| gigabitethernet \| tengigabitethernet} slot/port switchport` | Verifies the configuration. |

This example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end
```

```
Switch# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Appliance trust: none
Administrative Private Vlan
  Host Association: 202 (VLAN0202) 440 (VLAN0440)
  Promiscuous Mapping: none
  Trunk encapsulation : dot1q
  Trunk vlans:
Operational private-vlan(s):
  202 (VLAN0202) 440 (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

# Configuring a Layer 2 Interface as a PVLAN Trunk Port

To configure a Layer 2 interface as a PVLAN trunk port, perform this task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | `Switch(config)# interface {fastethernet \| gigabitethernet \| tengigabitethernet} slot/port` | Specifies the LAN port to configure. |
| **Step 3** | `Switch(config-if)# switchport mode private-vlan {host \| promiscuous \| trunk promiscuous \| trunk [secondary]}` | Configures a Layer 2 interface as a PVLAN trunk port. |
| **Step 4** | `Switch(config-if)# [no] switchport private-vlan association trunk primary_vlan_ID secondary_vlan_ID` | Configures association between primary VLANs and secondary VLANs the PVLAN trunk port with a PVLAN.<br>**Note** Multiple PVLAN pairs can be specified using this command so that a PVLAN trunk port can carry multiple secondary VLANs. If an association is specified for the existing primary VLAN, the existing association is replaced. If there is no trunk association, any packets received on secondary VLANs are dropped.<br>You can use the **no** keyword to delete all associations from the primary VLAN. |
| **Step 5** | `Switch(config-if)# [no] switchport private-vlan trunk allowed vlan vlan_list all \| none \| [add \| remove \| except] vlan_atom[,vlan_atom...]` | Configures a list of allowed normal VLANs on a PVLAN trunk port.<br>You can use the **no** keyword to remove all allowed normal VLANs on a PVLAN trunk port. |
| **Step 6** | `Switch(config-if)# switchport private-vlan trunk native vlan vlan_id` | Configures a VLAN to which untagged packets (as in IEEE 802.1Q tagging) are assigned on a PVLAN trunk port.<br>If there is no native VLAN configured, all untagged packets are dropped.<br>If the native VLAN is a secondary VLAN and the port does not have the association for the secondary VLAN, the untagged packets are dropped.<br>You can use the **no** keyword to remove all native VLANs on a PVLAN trunk port. |
| **Step 7** | `Switch(config-if)# end` | Exits configuration mode. |
| **Step 8** | `Switch# show interfaces {fastethernet \| gigabitethernet \| tengigabitethernet} slot/port switchport` | Verifies the configuration. |

This example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10. 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
    Switchport: Enabled
    Administrative Mode: private-vlan trunk secondary
    Operational Mode: private-vlan trunk secondary
    Administrative Trunking Encapsulation: negotiate
    Operational Trunking Encapsulation: dot1q
    Negotiation of Trunking: On
    Access Mode VLAN: 1 (default)
    Trunking Native Mode VLAN: 1 (default)
    Administrative Native VLAN tagging: enabled
    Voice VLAN: none
    Administrative private-vlan host-association: none A
    dministrative private-vlan mapping: none
    Administrative private-vlan trunk native VLAN: 10
    Administrative private-vlan trunk Native VLAN tagging: enabled
    Administrative private-vlan trunk encapsulation: dot1q
    Administrative private-vlan trunk normal VLANs: none
    Administrative private-vlan trunk associations:
        3 (VLAN0003) 301 (VLAN0301)
    Administrative private-vlan trunk mappings: none
    Operational private-vlan: none
    Operational Normal VLANs: none
    Trunking VLANs Enabled: ALL
    Pruning VLANs Enabled: 2-1001
    Capture Mode Disabled Capture VLANs Allowed: ALL

    Unknown unicast blocked: disabled
    Unknown multicast blocked: disabled
    Appliance trust: none
```

# Configuring a Layer 2 Interface as a Promiscuous Trunk Port

To configure a Layer 2 interface as a PVLAN promiscuous trunk port, perform this task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | `Switch(config)# interface {fastethernet \| gigabitethernet \| tengigabitethernet} slot/port` | Specifies the LAN interface to configure. |
| **Step 3** | `Switch(config-if)# switchport mode private-vlan {host \| promiscuous \| trunk promiscuous \| trunk [secondary]}` | Configures a Layer 2 interface as a PVLAN promiscuous trunk port. |
| **Step 4** | `Switch(config-if)# [no] switchport private-vlan mapping [trunk] primary_vlan_ID {secondary_vlan_list \| add secondary_vlan_list \| remove secondary_vlan_list}` | Maps the PVLAN promiscuous port to a primary VLAN and to selected secondary VLANs.<br>This command offers 3 levels of removal. See the examples that follow this table. |

| | Command | Purpose |
|---|---|---|
| **Step 5** | `Switch(config-if)# end` | Exits configuration mode. |
| **Step 6** | `Switch# show interfaces {fastethernet \| gigabitethernet \| tengigabitethernet} slot/port switchport` | Verifies the configuration. |

**Note** The maximum number of unique private VLAN pairs supported by the **switchport private-vlan mapping trunk** command above is 500. For example, one thousand secondary VLANs could map to one primary VLAN, or one thousand secondary VLANs could map one to one to one thousand primary VLANs.

**Note** By default, when you configure the mode to private VLAN trunk promiscuous, the native VLAN is set to 1.

The [**no**] **switchport private-vlan mapping** command provides the following three levels of removal:

- Remove one or more secondary VLANs from the list. For example:

  ```
  Switch(config-if)# switchport private-vlan mapping trunk 2 remove 222
  ```

- Remove the entire mapping of PVLAN promiscuous trunk port to the specified primary VLAN (and all of its selected secondary VLANs). For example:

  ```
  Switch(config-if)# no switchport private-vlan mapping trunk 2
  ```

- Remove the mapping of a PVLAN promiscuous trunk port to all previously configured primary VLANs (and all of their selected secondary VLANs). For example:

  ```
  Switch(config-if)# no switchport private-vlan mapping trunk
  ```

When you configure a Layer 2 interface as a PVLAN promiscuous port, note the following:

- Multiple private VLAN pairs can be specified using the **switchport private-vlan mapping trunk** command so that a promiscuous trunk port can carry multiple primary VLANs.
- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single PVLAN ID or a hyphenated range of PVLAN IDs.
- Enter a *secondary_vlan_list* or use the **add** keyword with a *secondary_vlan_list* to map the secondary VLANs to the PVLAN promiscuous port.
- Use the **remove** keyword with a *secondary_vlan_list* to clear the mapping between secondary VLANs and the PVLAN promiscuous port.

This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan mapping trunk 3 301, 302
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
```

```
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 3-4,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    3 (VLAN0003) 301 (VLAN0301)  302 (VLAN0302)
Operational private-vlan:
  3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

# Permitting Routing of Secondary VLAN Ingress Traffic

**Note** Isolated and community VLANs are both called secondary VLANs.

To permit routing of secondary VLAN ingress traffic, perform this task:

| | Command | Purpose |
|---|---|---|
| **Step 1** | `Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | `Switch(config)# interface vlan` *primary_vlan_ID* | Enters interface configuration mode for the primary VLAN. |
| **Step 3** | `Switch(config-if)# [no] private-vlan mapping` *primary_vlan_ID* {*secondary_vlan_list* \| **add** *secondary_vlan_list* \| **remove** *secondary_vlan_list*} | To permit routing on the secondary VLAN ingress traffic, map the secondary VLAN to the primary VLAN.<br>You can use the **no** keyword to delete all associations from the primary VLAN. |
| **Step 4** | `Switch(config-if)# end` | Exits configuration mode. |
| **Step 5** | `Switch# show interface private-vlan mapping` | Verifies the configuration. |

When you permit routing on the secondary VLAN ingress traffic, note the following:

- The **private-vlan mapping** interface configuration command only affects private VLAN ingress traffic that is Layer 3 switched.
- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private VLAN ID or a hyphenated range of private VLAN IDs.
- Enter a *secondary_vlan_list* parameter or use the **add** keyword with a *secondary_vlan_list* parameter to map the secondary VLANs to the primary VLAN.
- Use the **remove** keyword with a *secondary_vlan_list* parameter to clear the mapping between secondary VLANs and the primary VLAN.

This example shows how to permit routing of secondary VLAN ingress traffic from private VLANs 303 through 307, 309, and 440 and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface vlan 202
Switch(config-if)# private-vlan mapping add 303-307,309,440
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan202   303            community
vlan202   304            community
vlan202   305            community
vlan202   306            community
vlan202   307            community
vlan202   309            community
vlan202   440            isolated

Switch#
```

# Troubleshooting PVLANs

The following topics are discussed:

- Monitoring Private VLANs, page 38-21
- debug Command, page 38-23

## Monitoring Private VLANs

Private VLANs and ports should be configured following the instructions in the "Tasks for Configuring Private VLANs" section on page 38-10. To verify that the configuration is complete, following display commands are useful.

Table 38-1 shows the privileged EXEC commands for monitoring private-VLAN activity.

***Table 38-1 Private VLAN Monitoring Commands***

| Command | Purpose |
|---|---|
| **show interfaces status** | Displays the status of interfaces, including the VLANs to which they belong. |
| **show vlan private-vlan** [**type**] | Display the private-VLAN information for the switch. |

*Table 38-1 Private VLAN Monitoring Commands*

| Command | Purpose |
|---|---|
| **show interface switchport** | Display private-VLAN configuration on interfaces. |
| **show interface private-vlan mapping** | Display information about the private-VLAN mapping for VLAN SVIs. |

The following example shows how to verify that the primary VLAN and secondary VLANs are correctly associated with each other and the same association also exists on the PVLAN port:

```
Switch# show vlan private-vlan

Primary Secondary Type              Ports
------- ---------       -----------------
-----------------------------------------
10         100           community     Fa3/1, Fa3/2
```

Now, let's say that you remove the VLAN association, as follows:

```
Switch(config)# vlan 10
Switch(config-vlan)# private-vlan association remove 100
Switch(config-vlan)# end
Switch# show vlan private
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10                primary
        100       community
```

You can use the following command to verify PVLAN configuration on the interface:

```
Switch# show interface f3/2 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa3/2                        connected    pvlan seco a-full  a-100 10/100BaseTX

Switch# show interface f3/1 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa3/1                        connected    pvlan prom a-full  a-100 10/100BaseTX
Switch#
```

You can use the **show interface switchport** command to display complete administrative and operational information about private VLANs, active and inactive. In the following example, interface fa3/1 is a promiscuous trunk port and private VLAN configuration relevent to this mode has been highlighted.

```
Switch# show interface f3/1 switchport
show interface f3/1 switchport
Name: Fa3/1
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

```
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 1
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 1
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    10 (VLAN0010) 100 (VLAN0100)
Operational private-vlan:
  10 (VLAN0010) 100 (VLAN0100)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

# debug Command

Issuing the **debug pm pvlan** command displays messages associated with the execution of private VLAN configuration on ports. The output is useful for engineers and TAC in debugging port security-related issues.

**Note** The output might not remain the same across releases and is strictly intended for use by the Cisco engineering team.

Here is an example of how to enable debugging:

```
Switch# debug pm pvlan
debug pm pvlan
PM private vlan events debugging is on
```