



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:

- [Overview of PVLANS, page 10-1](#)
- [PVLAN Configuration Restrictions, page 10-3](#)
- [How to Configure PVLANS, page 10-3](#)



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

Overview of PVLANS

PVLANS provide Layer 2 isolation between ports within the same PVLAN. There are three types of PVLAN ports:

- **Promiscuous**—A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.
- **Isolated**—An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. PVLANS block all traffic to isolated ports except traffic from promiscuous ports. Traffic from isolated port is forwarded only to promiscuous ports.
- **Community**—Community ports communicate among themselves and with their promiscuous ports. These interfaces are separated at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN.

Because trunks can support the VLANs carrying traffic between isolated, community, and promiscuous ports, isolated and community port traffic might enter or leave the switch through a trunk interface.

PVLAN ports are associated with a set of supporting VLANs that are used to create the PVLAN structure. A PVLAN uses VLANs three ways:

- **As a primary VLAN**—Carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same primary VLAN.

- As an isolated VLAN—Carries traffic from isolated ports to a promiscuous port.
- As a community VLAN—Carries traffic between community ports and to promiscuous ports. You can configure multiple community VLANs in a PVLAN.

Isolated and community VLANs are called secondary VLANs. You can extend PVLANS across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support PVLANS.

In a switched environment, you can assign an individual PVLAN and associated IP subnet to each individual or common group of end stations. The end stations need to communicate with a default gateway only to gain access outside the PVLAN. With end stations in a PVLAN, you can do the following:

- Designate which ports will be connected to end stations. For example, interfaces connected to servers as isolated ports prevent any communication at Layer 2. Or, if the end stations are servers, this configuration prevents Layer 2 communication between the servers.
- Designate the interfaces to which the default gateway(s) and selected end stations (for example, backup servers or LocalDirector) are attached as promiscuous ports to allow all end stations access.
- Reduce VLAN and IP subnet consumption, because you can prevent traffic between end stations even though they are in the same VLAN and IP subnet.

**Note**

A promiscuous port can service only one primary VLAN. A promiscuous port can service one isolated or many community VLANs.

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.

PVLAN Trunks

A PVLAN trunkport can carry multiple secondary and non-PVLANS. Packets are received and transmitted with secondary or regular VLAN tags on the PVLAN trunk ports.

PVLAN trunk port behavior is the same as PVLAN isolated or community port behavior, except that PVLANS can tag packets and carry multiple secondary and regular VLANs.

**Note**

Only IEEE 802.1q encapsulation is supported.

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 the packet is untagged and the port's native VLAN is a secondary VLAN.

A packet received on a PVLAN host or trunk port and assigned to 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 applies to the packet.

PVLAN Configuration Restrictions

Keep the following restrictions in mind when configuring PVLANS correctly:

- PVLAN trunk ports support only IEEE 802.1q encapsulation.
- Community VLANs are not supported in this release.
- You cannot change the VTP mode to client or server for PVLANS.
- An isolated or community VLAN can have only one primary VLAN associated with it.
- VTP does not support PVLANS. You must configure PVLANS on each device where you want PVLAN ports.

How to Configure PVLANS

To configure a PVLAN, follow this procedure:

-
- Step 1** Set VTP mode to transparent. See the [“Disabling VTP \(VTP Transparent Mode\)”](#) section on page 11-9.
 - Step 2** Create the secondary VLANs. See the [“Configuring a VLAN as a PVLAN”](#) section on page 10-5.
 - Step 3** Create the primary VLAN. See the [“Configuring a VLAN as a PVLAN”](#) section on page 10-5.
 - Step 4** Associate the secondary VLAN to the primary VLAN. See the [“Associating a Secondary VLAN with a Primary VLAN”](#) section on page 10-6.



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 to an isolated or community port. See the [“Configuring a Layer 2 Interface as a PVLAN Host Port”](#) section on page 10-8.
 - 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 10-6.
 - Step 7** Configure an interface as a promiscuous port. See the [“Configuring a Layer 2 Interface as a PVLAN Promiscuous Port”](#) section on page 10-7.
 - 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 10-7.
-

These sections describe how to configure PVLANS:

- “PVLAN Configuration Guidelines” section on page 10-4
- “Configuring a VLAN as a PVLAN” section on page 10-5
- “Associating a Secondary VLAN with a Primary VLAN” section on page 10-6
- “Configuring a Layer 2 Interface as a PVLAN Promiscuous Port” section on page 10-7
- “Configuring a Layer 2 Interface as a PVLAN Host Port” section on page 10-8
- “Permitting Routing of Secondary VLAN Ingress Traffic” section on page 10-10

PVLAN Configuration Guidelines

Follow these guidelines when configuring PVLANS:

- To configure a PVLAN correctly, enable VTP in transparent mode.
- Do not include VLAN 1 or VLANs 1002–1005 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 PVLAN ports as EtherChannel.
EtherChannel ports in PVLANS are inactive.
- Do not configure a destination SPAN port in a PVLAN.
Destination SPAN ports are inactive in PVLANS.
- If you delete a VLAN in a PVLAN, the PVLAN ports in the VLAN become inactive.
- Do not apply Cisco IOS ACLs to isolated or community VLANs.
Cisco IOS ACL configuration applied to isolated and community VLANs is inactive while the VLANs are part of the PVLAN configuration.
- 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.
- Do not apply Cisco IOS ACLs to isolated or community VLANs.
Cisco IOS ACL configuration applied to isolated and community VLANs is inactive while the VLANs are part of the PVLAN configuration.
- Do not apply dynamic access control entries (ACEs) to primary VLANs.
Dynamic ACLs applied to a primary VLAN are inactive in PVLANS.
- Enable PortFast on the PVLAN trunk ports with the **spanning-tree portfast trunk** command.
- Any VLAN ACL configured on an isolated VLAN is effective in the input direction, and any VLAN ACL configured on the primary VLAN associated with the isolated VLAN is effective in the output direction.

- You can stop Layer 3 switching on an isolated VLAN by deleting the mapping of that VLAN with its primary VLAN.
- PVLAN ports do not have to be on the same network device as long as the devices are trunk connected and the primary and secondary VLANs have not been removed from the trunk.
- You can use VLAN-based SPAN (VSPAN) on primary, isolated, and community VLANs, or use SPAN on only one VLAN to separately monitor egress or ingress traffic.
- Enable PortFast and bridge packet data unit (BPDU) guard on isolated and community ports to prevent spanning tree loops due to misconfigurations.
When PortFast and BPDU guard enabled, STP applies the BPDU guard to all PortFast-configured Layer 2 LAN ports.
- To maintain the security of your PVLAN configuration and avoid other use of the VLANs configured as PVLANS, configure PVLANS on all intermediate devices, even if devices have no PVLAN ports.
- Prune the PVLANS from the trunks on devices that carry no traffic in the PVLANS.
- To apply Cisco IOS output ACLs to all outgoing PVLAN traffic, configure them on the Layer 3 VLAN interface of the primary VLAN.
- You can apply different quality of service (QoS) configuration to primary, 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.
- Cisco IOS ACLs applied to the Layer 3 VLAN interface of a primary VLAN automatically apply to the associated isolated and community VLANs.

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 <i>vlan_ID</i> Switch(config-vlan)# private-vlan { isolated primary }	Configures a VLAN as a PVLAN. <ul style="list-style-type: none"> • The command does not take effect until you exit VLAN configuration submode. • You can use the no keyword to clear PVLAN status.
Step 3	Switch(config-vlan)# end	Exits VLAN configuration mode.
Step 4	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 type
```

```
Vlan Type
-----
202 primary
440 isolated
```

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 type
```

```
Vlan Type
-----
202 primary
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 <i>primary_vlan_ID</i>	Enters VLAN configuration mode for the primary VLAN.
Step 3	Switch(config-vlan)# [no] private-vlan association { <i>secondary_vlan_list</i> add <i>secondary_vlan_list</i> remove <i>secondary_vlan_list</i> }	Associates the secondary VLAN with the primary VLAN. The list can contain only one VLAN. You can use the no keyword to delete all associations from the primary VLAN.
Step 4	Switch(config-vlan)# end	Exits VLAN configuration mode.
Step 5	Switch# show vlan private-vlan [<i>type</i>]	Verifies the configuration.

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

- The *secondary_vlan_list* parameter contains only one isolated VLAN ID.
- Use the **remove** keyword with the *secondary_vlan_list* variable to clear the association between the secondary VLAN and the primary VLAN. The list can contain only one VLAN.
- The command does not take effect until you exit VLAN configuration submode.

This example shows how to associate isolated VLAN 440 with primary VLAN 202 and verify the configuration:

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

```
Primary Secondary Type          Interfaces
-----
202      440      isolated
```

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} slot/port	Specifies the LAN interface to configure.
Step 3	Switch(config-if)# switchport mode private-vlan {host promiscuous trunk}	Configures a Layer 2 interface as a PVLAN promiscuous port.
Step 4	Switch(config-if)# [no] switchport private-vlan mapping 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. 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} slot/port switchport	Verifies the configuration.

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 202 440
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 } <i>slot/port</i>	Specifies the LAN port to configure.
Step 3	Switch(config-if)# switchport mode private-vlan { host promiscuous } trunk	Configures a Layer 2 interface as a PVLAN host port.
Step 4	Switch(config-if)# [no] switchport private-vlan host-association <i>primary_vlan_ID secondary_vlan_ID</i>	Associates the Layer 2 interface with a PVLAN. 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 } <i>slot/port switchport</i>	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):
  2 (VLAN0202) 3 (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> enable	Enters privileged EXEC mode.
Step 2	Switch# configure terminal	Enters global configuration mode.
Step 3	Switch(config)# interface {fastethernet gigabitethernet} slot/port	Specifies the LAN port to configure.
Step 4	Switch(config-if)# switchport mode private-vlan {host promiscuous trunk}	Configures a Layer 2 interface as a PVLAN trunk port for multiple secondary VLANs.
Step 5	Switch(config-if)# [no] switchport private-vlan association trunk primary_vlan_ID secondary_vlan_ID	<p>Configures association between primary VLANs and secondary VLANs the PVLAN trunk port with a PVLAN.</p> <p>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.</p> <p>You can use the no keyword to delete all associations from the primary VLAN.</p>
Step 6	Switch(config-if)# [no] switchport private-vlan trunk allowed vlan vlan_list all none [add remove except] vlan_atom[,vlan_atom...]	<p>Configures a list of allowed normal VLANs on a PVLAN trunk port.</p> <p>You can use the no keyword to remove all allowed normal VLANs on a PVLAN trunk port.</p>
Step 7	Switch(config-if)# [no] switchport private-vlan trunk native vlan vlan_id	<p>Configures a VLAN to which untagged packets (as in IEEE 802.1Q tagging) are assigned on a PVLAN trunk port.</p> <p>If there is no native VLAN configured, all untagged packets are dropped.</p> <p>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.</p> <p>You can use the no keyword to remove all native VLANs on a PVLAN trunk port.</p>
Step 8	Switch(config-if)# end	Exits configuration mode.
Step 9	Switch# show interfaces {fastethernet gigabitethernet} slot/port switchport	Verifies the configuration.

This example shows how to configure interface FastEthernet 5/1 as a PVLAN trunk port, maps VLAN0202 to VLAN0440, and configures the PVLAN trunk:

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

Switch#show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan trunk
Operational Mode: private-vlan trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
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:
    202 (VLAN0202) 440 (VLAN0440)
Operational private-vlan(s):
  202 (VLAN0202) 440 (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Permitting Routing of Secondary VLAN Ingress Traffic

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 <i>primary_vlan_ID</i>	Enters interface configuration mode for the primary VLAN.
Step 3	Switch(config-if)# [no] private-vlan mapping <i>primary_vlan_ID</i> { <i>secondary_vlan_list</i> add <i>secondary_vlan_list</i> remove <i>secondary_vlan_list</i> }	To permit routing on the secondary VLAN ingress traffic, map the secondary VLAN to the primary VLAN. 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:

- Enter a value for the *secondary_vlan_list* variable or use the **add** keyword with the *secondary_vlan_list* variable to map the secondary VLANs to the primary VLAN.
- Use the **remove** keyword with the *secondary_vlan_list* variable to clear the mapping between secondary VLANs and the primary VLAN.

This example shows how to permit routing of secondary VLAN ingress traffic from PVLAN 440 and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface vlan 202
Switch(config-if)# private-vlan mapping add 440
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan202    440          isolated

Switch#
```

