



Understanding and Configuring Private VLANs

This chapter describes private VLANs on the Catalyst 4000 family switches. It also provides guidelines, procedures, and configuration examples.

This chapter consists of the following sections:

- [Private VLANs Overview, page 8-1](#)
- [Private VLAN Configuration Guidelines, page 8-2](#)
- [Configuring Private VLANs, page 8-4](#)



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference for the Catalyst 4006 Switch with Supervisor Engine III* and the publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

Private VLANs Overview



Note

To configure private VLANs, the switch must be in VTP transparent mode.

Private VLANs provide Layer 2 isolation between ports within the same private VLAN. There are three types of private VLAN ports:

- **Promiscuous**—A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN.
- **Isolated**—An isolated port has complete Layer 2 separation from other ports within the same private VLAN except for the promiscuous port. 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.
- **Community**—Community ports communicate among themselves and with their promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities or isolated ports within their private VLAN.



Note

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.

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

- Primary VLAN—Carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same primary VLAN.
- Isolated VLAN—Carries traffic from isolated ports to a promiscuous port.
- Community VLAN—Carries traffic between community ports and to promiscuous ports. You can configure multiple community VLANs in a private VLAN.

**Note**

Isolated and community VLANs are called secondary VLANs.

You can extend private VLANs across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support private VLANs.

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 only need to communicate with a default gateway to gain access outside the private VLAN. With end stations in a private VLAN, you can do the following:

- Designate selected ports connected to end stations (for example, interfaces connected to servers) as isolated to prevent any communication at Layer 2. (For example, 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 private VLAN. 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 private VLAN servers from an administration workstation.

Private VLAN Configuration Guidelines

**Note**

This release does not support the community VLANs.

Follow these guidelines to configure private VLANs:

- Set VTP to transparent mode. After you configure a private VLAN, you cannot change the VTP mode to client or server.
- You cannot include VLAN 1 or VLANs 1002–1005 in the private VLAN configuration.
- Use only the private VLAN configuration commands to assign ports to primary, isolated, or community VLANs.



Note Layer 2 interfaces assigned to the VLANs that you configure as primary, isolated, or community VLANs are inactive while the VLAN is part of the private VLAN configuration. Layer 2 trunk interfaces remain in the STP forwarding state.

- Configure Layer 3 VLAN interfaces only for primary VLANs.



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

- Do not configure private VLAN ports as EtherChannels.



Note While a port is part of the private VLAN configuration, any EtherChannel configuration for it is inactive.

- Do not configure a destination SPAN port as a private VLAN port.



Note While a port is part of the private VLAN configuration, any destination SPAN configuration for it is inactive.

- 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 separately monitor egress or ingress traffic.
- A primary VLAN can have one isolated VLAN and multiple community VLANs associated with it.
- An isolated or community VLAN can have only one primary VLAN associated with it.
- Enable PortFast and BPDU guard on isolated and community ports to prevent spanning tree loops due to misconfigurations.



Note When enabled, STP applies the BPDU guard feature to all PortFast-configured Layer 2 LAN ports.

- If you delete a VLAN used in the private VLAN configuration, the private VLAN ports associated with the VLAN become inactive.
- Private VLAN 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.
- VTP does not support private VLANs. You must configure private VLANs on each device where you want private VLAN ports.
- To maintain the security of your private VLAN configuration and avoid other use of the VLANs configured as private VLANs, configure private VLANs on all intermediate devices, even if devices that have no private VLAN ports.
- We recommend that you prune the private VLANs from the trunks on devices that carry no traffic in the private VLANs.
- You can apply different quality of service (QoS) configuration to primary, isolated, and community VLANs.

- To apply Cisco IOS output ACLs to all outgoing private VLAN traffic, configure them on the Layer 3 VLAN interface of the primary VLAN.
- Cisco IOS ACLs applied to the Layer 3 VLAN interface of a primary VLAN automatically apply to the associated isolated and community VLANs.
- Do not apply Cisco IOS ACLs to isolated or community VLANs.



Note Cisco IOS ACL configuration applied to isolated and community VLANs is inactive while the VLANs are part of the private VLAN configuration.

- Do not apply dynamic access control entries (ACEs) to primary VLANs.



Note Cisco IOS dynamic ACL configuration applied to a primary VLAN is inactive while the VLAN are part of the private VLAN configuration.

- You can stop Layer 3 switching on an isolated VLAN by deleting the mapping of that VLAN with its primary VLAN.

Configuring Private VLANs

To configure a private VLAN, follow the following procedure:

-
- Step 1** Set VTP mode to transparent. See [Disabling VTP \(VTP Transparent Mode\)](#), page 9-9.
- Step 2** Create the secondary VLANs (isolated or community VLANs). See [Configuring a VLAN as a Private VLAN](#), page 8-5.
-
- **Note** Isolated and community VLANs are called *secondary* VLANs.

- Step 3** Create the primary VLAN. See [Configuring a VLAN as a Private VLAN](#), page 8-5.
- Step 4** Associate the secondary VLAN to the primary VLAN. See [Associating Secondary VLANs with a Primary VLAN](#), page 8-6.
-
- **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 [Configuring a Layer 2 Interface as a Private VLAN Host Port](#), page 8-7.
- Step 6** Associate the isolated port or community port to the primary-secondary VLAN pair. See [Associating Secondary VLANs with a Primary VLAN](#), page 8-6.
- Step 7** Configure an interface as a promiscuous port. See [Configuring a Layer 2 Interface as a Private VLAN Promiscuous Port](#), page 8-6.
- Step 8** Map the promiscuous port to the primary-secondary VLAN pair. See [Configuring a Layer 2 Interface as a Private VLAN Promiscuous Port](#), page 8-6.
-

These sections describe how to configure private VLANs:

- [Configuring a VLAN as a Private VLAN, page 8-5](#)
- [Associating Secondary VLANs with a Primary VLAN, page 8-6](#)
- [Configuring a Layer 2 Interface as a Private VLAN Promiscuous Port, page 8-6](#)
- [Configuring a Layer 2 Interface as a Private VLAN Host Port, page 8-7](#)
- [Permitting Routing of Secondary VLAN Ingress Traffic, page 8-8](#)

Configuring a VLAN as a Private VLAN

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

	Task	Command
Step 1	Enter configuration mode.	Switch# configure terminal
Step 2	Configure a VLAN as a private VLAN. <ul style="list-style-type: none"> • Use the no keyword to clear private VLAN status. • The command does not take effect until you exit VLAN configuration submenu. 	Switch(config)# vlan <i>vlan_ID</i> Switch(config-vlan)# [no] private-vlan { isolated primary }
Step 3	Exit configuration mode.	Switch(config-vlan)# end
Step 4	Verify the configuration.	Switch# show vlan private-vlan [type]

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
```

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

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
```

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

Associating Secondary VLANs with a Primary VLAN

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

	Task	Command
Step 1	Enter configuration mode.	Switch# configure terminal
Step 2	Enter VLAN configuration mode for the primary VLAN.	Switch(config)# vlan primary_vlan_ID
Step 3	Associate the secondary VLAN with the primary VLAN. The list can only contain one VLAN. Use the no keyword to delete all associations from the primary VLAN.	Switch(config-vlan)# [no] private-vlan association { <i>secondary_vlan_list</i> add <i>secondary_vlan_list</i> remove <i>secondary_vlan_list</i> }
Step 4	Exit VLAN configuration mode.	Switch(config-vlan)# end
Step 5	Verify the configuration.	Switch# show vlan private-vlan [type]

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 only contain one VLAN.
- Use the **no** keyword to clear all associations from the primary 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 Private VLAN Promiscuous Port

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

	Task	Command
Step 1	Enter configuration mode.	Switch# configure terminal
Step 2	Select the LAN interface to configure.	Switch(config)# interface { <i>fastethernet</i> <i>gigabitethernet</i> } <i>slot/port</i>
Step 3	Configure a Layer 2 interface as a private VLAN promiscuous port.	Switch(config-if)# switchport mode private-vlan { <i>host</i> <i>promiscuous</i> }

Task	Command
Step 4 Map the private VLAN promiscuous port to a primary VLAN and to selected secondary VLANs. Use the no keyword to delete all associations from the primary VLAN.	<pre>Switch(config-if)# [no] switchport private-vlan mapping primary_vlan_ID {secondary_vlan_list add secondary_vlan_list remove secondary_vlan_list}</pre>
Step 5 Exit configuration mode.	<pre>Switch(config-if)# end</pre>
Step 6 Verify the configuration.	<pre>Switch# show interfaces {fastethernet gigabitethernet} slot/port switchport</pre>

When you configure a Layer 2 interface as a private VLAN 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 private VLAN ID or a hyphenated range of private VLAN IDs.
- Enter a *secondary_vlan_list* or use the **add** keyword with a *secondary_vlan_list* to map the secondary VLANs to the private VLAN promiscuous port.
- Use the **remove** keyword with a *secondary_vlan_list* to clear the mapping between secondary VLANs and the private VLAN promiscuous port.
- Use the **no** keyword to clear all mapping from the private VLAN promiscuous port.

This example shows how to configure interface FastEthernet 5/2 as a private VLAN promiscuous port, map it to a private VLAN, 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: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none ((Inactive))
→ Administrative private-vlan mapping: 202 (VLAN0202) 440 (VLAN0440)
→ Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

Configuring a Layer 2 Interface as a Private VLAN Host Port

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

Task	Command
Step 1 Enter configuration mode.	<pre>Switch# configure terminal</pre>
Step 2 Select the LAN port to configure.	<pre>Switch(config)# interface {fastethernet gigabitethernet} slot/port</pre>

Task	Command
Step 3 Configure a Layer 2 interface as a private VLAN host port.	Switch(config-if)# switchport mode private-vlan { host promiscuous }
Step 4 Associate the Layer 2 interface with a private VLAN. Use the no keyword to delete all associations from the primary VLAN.	Switch(config-if)# [no] switchport private-vlan host-association <i>primary_vlan_ID</i> <i>secondary_vlan_ID</i>
Step 5 Exit configuration mode.	Switch(config-if)# end
Step 6 Verify the configuration.	Switch# show interfaces { fastethernet gigabitethernet } <i>slot/port</i> switchport

This example shows how to configure interface FastEthernet 5/1 as a private VLAN 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: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
→ Administrative private-vlan host-association: 202 (VLAN0202)
Administrative private-vlan mapping: none
→ Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

Permitting Routing of Secondary VLAN Ingress Traffic

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

Task	Command
Step 1 Enter configuration mode.	Switch# configure terminal
Step 2 Enter interface configuration mode for the primary VLAN.	Switch(config)# interface vlan <i>primary_vlan_ID</i>
Step 3 To permit routing on the secondary VLAN ingress traffic, map the secondary VLAN to the primary VLAN. Use the no keyword to delete all associations from the primary VLAN.	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> }
Step 4 Exit configuration mode.	Switch(config-if)# end
Step 5 Verify the configuration.	Switch# show interface private-vlan mapping

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.
- Use the **no** keyword to clear all mapping from the primary VLAN.

This example shows how to permit routing of secondary VLAN ingress traffic from private VLAN440 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#
```

