CHAPTER 10

Configuring Private VLANs

This chapter describes how to configure private VLANs on the Catalyst 6500 series switches. Release 12.1 E supports private VLANs with Release 12.1(11b)E and later.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

Understanding How Private VLANs Work

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.
- Isolated VLAN—Carries traffic from isolated ports to promiscuous ports.
- 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 both 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 were servers, this configuration would prevent 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 to allow all end stations access.
- Reduce VLAN and IP subnet consumption by preventing traffic between end stations even though they are in the same VLAN and IP subnet.

A promiscuous port can serve only one primary VLAN.

A promiscuous port can serve as many isolated or community VLANs as desired.

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 LocalDirector to connect an isolated VLAN or a number of community VLANs to the server so that 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 Restrictions and Guidelines

Follow these restrictions and 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. See Chapter 8, “Configuring VTP.”
- You cannot include VLAN 1 or VLANs 1002 to 1005 in the private VLAN configuration.
- Use only the private VLAN configuration commands to assign ports to primary, isolated, or community VLANs. Layer 2 access ports 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. 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. While a port is part of the private VLAN configuration, any EtherChannel configuration for it is inactive.
- Destination SPAN configuration supersedes private VLAN configuration. While a port is a destination SPAN port, any private VLAN configuration for it is inactive.
- 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 separately monitor egress or ingress traffic.

  For more information about SPAN, see Chapter 34, "Configuring Local SPAN and RSPAN."
- 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 STP loops due to misconfigurations and to speed up STP convergence (see Chapter 16, "Configuring Optional STP Features"). 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.
- **12-Port Restriction:**
  - In all releases, the "12-port restriction" applies to these 10 Mb, 10/100 Mb, and 100 Mb Ethernet switching modules: WS-X6324-100FX, WS-X6348-RJ-45, WS-X6348-RJ-45V, WS-X6348-RJ-21V, WS-X6248-RJ-45, WS-X6248A-TEL, WS-X6248-TEL, WS-X6148-RJ-45, WS-X6148-RJ-45V, WS-X6148-45AF, WS-X6148-RJ-21, WS-X6148-RJ-21V, WS-X6148-21AF, WS-X6024-10FL-MT.
  - In releases earlier than Release 12.1(19)E, the "12-port restriction" applies to these Ethernet switching modules: WS-X6548-RJ-45, WS-X6548-RJ-21, WS-X6524-100FX-MM.
  - In Release 12.1(19)E and later releases, the "12-port restriction" does not apply to these Ethernet switching modules: WS-X6548-RJ-45, WS-X6548-RJ-21, WS-X6524-100FX-MM (CSCea67876).

  Within groups of 12 ports (1–12, 13–24, 25–36, and 37–48), do not configure ports as isolated or community VLAN ports when one port within the 12 ports is a trunk or a SPAN destination or a promiscuous private VLAN port. While one port within the 12 ports is a trunk or a SPAN destination or a promiscuous private VLAN port, any isolated or community VLAN configuration for other ports within the 12 ports is inactive. To reactivate the ports, remove the isolated or community VLAN port configuration and enter **shutdown** and **no shutdown** commands.
- **24-Port Restriction:**
- In all releases, this "24-port restriction" applies to the WS-X6548-GE-TX and WS-X6148-GE-TX 10/100/1000 Mb Ethernet switching modules: within groups of 24 ports (1–24, 25–48), do not configure ports as isolated or community VLAN ports when one port within the 24 ports is a trunk or a SPAN destination or a promiscuous private VLAN port. While one port within the 24 ports is a trunk or a SPAN destination or a promiscuous private VLAN port, any isolated or community VLAN configuration for other ports within the 24 ports is inactive. To reactivate the ports, remove the isolated or community VLAN port configuration and enter **shutdown** and **no shutdown** commands.
- Private VLAN ports can be on different network devices 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, including 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.
- In networks with some devices using MAC address reduction, and others not using MAC address reduction, STP parameters do not necessarily propagate to ensure that the spanning tree topologies match. You should manually check the STP configuration to ensure that the primary, isolated, and community VLANs' spanning tree topologies match.
- If you enable MAC address reduction on the switch, we recommend that you enable MAC address reduction on all the devices in your network to ensure that the STP topologies of the private VLANs match.
- In a network where private VLANs are configured, if you enable MAC address reduction on some devices and disable it on others (mixed environment), use the default bridge priorities to make sure that the root bridge is common to the primary VLAN and to all its associated isolated and community VLANs. Be consistent with the ranges employed by the MAC address reduction feature regardless of whether it is enabled on the system. MAC address reduction allows only discrete levels and uses all intermediate values internally as a range. You should disable a root bridge with private VLANs and MAC address reduction, and configure the root bridge with any priority higher than the highest priority range used by any nonroot bridge.
- You can apply different quality of service (QoS) configuration to primary, isolated, and community VLANs (see Chapter 31, "Configuring PFC QoS").
- You cannot apply VACLs to secondary VLANs (see the "Configuring VLAN ACLs" section on page 23-8).
- To apply Cisco IOS output ACLs to all outgoing private VLAN traffic, configure them on the Layer 3 VLAN interface of the primary VLAN (see Chapter 23, "Configuring Network Security").
- 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. 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. Cisco IOS dynamic ACL configuration applied to a primary VLAN is inactive while the VLAN are part of the private VLAN configuration.
- ARP entries learned on Layer 3 private VLAN interfaces are sticky ARP entries (we recommend that you display and verify private VLAN interface ARP entries).
- For security reasons, private VLAN port sticky ARP entries do not age out. Connecting a device with a different MAC address but with the same IP address generates a message and the ARP entry is not created.

- Because the private VLAN port sticky ARP entries do not age out, you must manually remove private VLAN port ARP entries if a MAC address changes. You can add or remove private VLAN ARP entries manually as follows:

```
Router(config)# no arp 11.1.3.30
IP ARP:Deleting Sticky ARP entry 11.1.3.30

Router(config)# arp 11.1.3.30 0000.5403.2356 arpa
IP ARP:Overwriting Sticky ARP entry 11.1.3.30, hw:00d0.bb09.266e by hw:0000.5403.2356
```

Configuring Private VLANs

These sections describe how to configure private VLANs:

Note If the VLAN is not defined already, the private VLAN configuration process defines it.

Note With Release 12.1(11b)E and later, when you are in configuration mode you can enter EXEC mode-level commands by entering the **do** keyword before the EXEC mode-level command.

Configuring a VLAN as a Private VLAN

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

	Command	Purpose
Step 1	`Router(config)# vlan vlan_ID`	Enters VLAN configuration submode.
Step 2	`Router(config-vlan)# private-vlan {community | isolated | primary}`	Configures a VLAN as a private VLAN.
	`Router(config-vlan)# no private-vlan {community | isolated | primary}`	Clears the private VLAN configuration. **Note** These commands do not take effect until you exit VLAN configuration submode.
Step 3	`Router(config-vlan)# end`	Exits configuration mode.
Step 4	`Router# show vlan private-vlan [type]`	Verifies the configuration.

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

```
Router# configure terminal
Router(config)# vlan 202
Router(config-vlan)# private-vlan primary
Router(config-vlan)# end
Router# 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:

```
Router# configure terminal
Router(config)# vlan 303
Router(config-vlan)# private-vlan community
Router(config-vlan)# end
Router# 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:

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

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

Associating Secondary VLANs with a Primary VLAN

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

	Command	Purpose
Step 1	`Router(config)# vlan` *primary_vlan_ID*	Enters VLAN configuration submode for the primary VLAN.
Step 2	`Router(config-vlan)# private-vlan association` {*secondary_vlan_list* | **add** *secondary_vlan_list* | **remove** *secondary_vlan_list*}	Associates the secondary VLANs with the primary VLAN.
	`Router(config-vlan)# no private-vlan association`	Clears all secondary VLAN associations.
Step 3	`Router(config-vlan)# end`	Exits VLAN configuration mode.
Step 4	`Router# show vlan private-vlan` [**type**]	Verifies the configuration.

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

- 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:

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

Mapping Secondary VLANs to the Layer 3 VLAN Interface of a Primary VLAN

Note Isolated and community VLANs are both called secondary VLANs.

To map secondary VLANs to the Layer 3 VLAN interface of a primary VLAN to allow Layer 3 switching of private VLAN ingress traffic, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface vlan` *primary_vlan_ID*	Enters interface configuration mode for the primary VLAN.
Step 2	`Router(config-if)# private-vlan mapping` {*secondary_vlan_list* | **add** *secondary_vlan_list* | **remove** *secondary_vlan_list*}	Maps the secondary VLANs to the Layer 3 VLAN interface of a primary VLAN to allow Layer 3 switching of private VLAN ingress traffic.
	`Router(config-if)# [no] private-vlan mapping`	Clears the mapping between the secondary VLANs and the primary VLAN.
Step 3	`Router(config-if)# end`	Exits configuration mode.
Step 4	`Router# show interface private-vlan mapping`	Verifies the configuration.

When you map secondary VLANs to the Layer 3 VLAN interface of a primary VLAN, note the following syntax information:

- 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:

```
Router# configure terminal
Router(config)# interface vlan 202
Router(config-if)# private-vlan mapping add 303-307,309,440
Router(config-if)# end
Router# 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

Router#
```

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:

	Command	Purpose
Step 1	`Router(config)# interface` *type*[1] *slot/port*	Selects the LAN port to configure.
Step 2	`Router(config-if)# switchport`	Configures the LAN port for Layer 2 switching: • You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional **switchport** commands with keywords. • Required only if you have not entered the **switchport** command already for the interface.
Step 3	`Router(config-if)# switchport mode private-vlan {host | promiscuous}`	Configures the Layer 2 port as a private VLAN host port.
	`Router(config-if)# no switchport mode private-vlan`	Clears private VLAN port configuration.
Step 4	`Router(config-if)# switchport private-vlan host-association` *primary_vlan_ID secondary_vlan_ID*	Associates the Layer 2 port with a private VLAN.
	`Router(config-if)# no switchport private-vlan host-association`	Clears the association.
Step 5	`Router(config-if)# end`	Exits configuration mode.
Step 6	`Router# show interfaces [`*type*[1] *slot/port*`] switchport`	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

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

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport mode private-vlan host
Router(config-if)# switchport private-vlan host-association 202 303
Router(config-if)# end
Router# 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) 303 (VLAN0303)
Administrative private-vlan mapping: none
→ 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 Promiscuous Port

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

	Command	Purpose
Step 1	`Router(config)# interface` *type*[1] *slot/port*	Selects the LAN interface to configure.
Step 2	`Router(config-if)# switchport`	Configures the LAN interface for Layer 2 switching: • You must enter the **switchport** command once without any keywords to configure the LAN interface as a Layer 2 interface before you can enter additional **switchport** commands with keywords. • Required only if you have not entered the **switchport** command already for the interface.
Step 3	`Router(config-if)# switchport mode private-vlan {host | promiscuous}` `Router(config-if)# no switchport mode private-vlan`	Configures the Layer 2 port as a private VLAN promiscuous port. Clears the private VLAN port configuration.
Step 4	`Router(config-if)# switchport private-vlan mapping` *primary_vlan_ID* {*secondary_vlan_list* | **add** *secondary_vlan_list* | **remove** *secondary_vlan_list*} `Router(config-if)# no switchport private-vlan mapping`	Maps the private VLAN promiscuous port to a primary VLAN and to selected secondary VLANs. Clears all mapping between the private VLAN promiscuous port and the primary VLAN and any secondary VLANs.
Step 5	`Router(config-if)# end`	Exits configuration mode.
Step 6	`Router# show interfaces` [*type*[1] *slot/port*] `switchport`	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

When you configure a Layer 2 interface as a private VLAN promiscuous port, note the following syntax information:

- 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* value or use the **add** keyword with a *secondary_vlan_list* value to map the secondary VLANs to the private VLAN promiscuous port.
- Use the **remove** keyword with a *secondary_vlan_list* value to clear the mapping between secondary VLANs and the private VLAN promiscuous port.

This example shows how to configure interface FastEthernet 5/2 as a private VLAN promiscuous port and map it to a private VLAN:

```
Router# configure terminal
Router(config)# interface fastethernet 5/2
Router(config-if)# switchport mode private-vlan promiscuous
Router(config-if)# switchport private-vlan mapping 202 303,440
Router(config-if)# end
```

This example shows how to verify the configuration:

```
Router# 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) 303 (VLAN0303) 440 (VLAN0440)
→ Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```