



Send feedback to nx5000-docfeedback@cisco.com

CHAPTER 1

Configuring Private VLANs

This chapter shows you how to configure private VLANs.



Note

You must enable the private VLAN feature before you can perform any of the configurations in this chapter.

This chapter includes the following sections:

- [About Private VLANs, page 1-1](#)
- [Configuring a Private VLAN, page 1-5](#)
- [Verifying Private VLAN Configuration, page 1-10](#)

About Private VLANs

A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing you to isolate the ports on the switch from each other. A subdomain consists of a primary VLAN and one or more secondary VLANs (see [Figure 1-1](#)). All VLANs in a private VLAN domain share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. The secondary VLANs may either be isolated VLANs or community VLANs. A host on an isolated VLAN can only communicate with the associated promiscuous port in its primary VLAN. Hosts on community VLANs can communicate among themselves and with their associated promiscuous port but not with ports in other community VLANs.

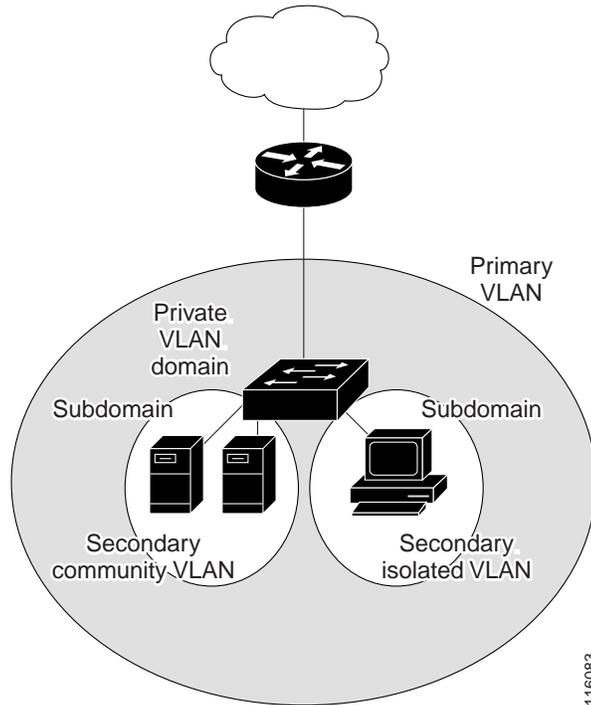


Note

A PVLAN isolated port on a Cisco Nexus 5000 Series switch running the current release of Cisco NX-OS does not support IEEE 802.1q encapsulation and cannot be used as a trunk port.

Send feedback to nx5000-docfeedback@cisco.com

Figure 1-1 Private VLAN Domain



Note

You must first create the VLAN before you can convert it to a private VLAN, either primary or secondary. See [Chapter 1, “Configuring VLANs”](#) for information on creating VLANs.

This section includes the following topics:

- [Primary and Secondary VLANs in Private VLANs, page 1-2](#)
- [Understanding Private VLAN Ports, page 1-3](#)
- [Understanding Broadcast Traffic in Private VLANs, page 1-5](#)
- [Understanding Private VLAN Port Isolation, page 1-5](#)

Primary and Secondary VLANs in Private VLANs

A private VLAN domain has only one primary VLAN. Each port in a private VLAN domain is a member of the primary VLAN; the primary VLAN is the entire private VLAN domain.

Secondary VLANs provide isolation between ports within the same private VLAN domain. The following two types are secondary VLANs within a primary VLAN:

- **Isolated VLANs**—Ports within an isolated VLAN cannot communicate directly 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 community VLANs or in any isolated VLANs at the Layer 2 level.

Send feedback to nx5000-docfeedback@cisco.com

Understanding Private VLAN Ports

The types of private VLAN ports are as follows:

- **Promiscuous**—A promiscuous port belongs to the primary VLAN. The promiscuous port can communicate with all interfaces, including the community and isolated host ports, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN. You can have several promiscuous ports in a primary VLAN. Each promiscuous port can have several secondary VLANs, or no secondary VLANs, associated to that port. You can associate a secondary VLAN to more than one promiscuous port, as long as the promiscuous port and secondary VLANs are within the same primary VLAN. You may want to do this for load-balancing or redundancy purposes. You can also have secondary VLANs that are not associated to any promiscuous port.
- **Isolated**—An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated 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. You can have more than one isolated port in a specified isolated VLAN. Each port is completely isolated from all other ports in the isolated VLAN.
- **Community**—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 associated promiscuous ports. These interfaces are isolated from all other interfaces in other communities and from all isolated ports within the private VLAN domain.



Note

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

Understanding Primary, Isolated, and Community Private VLANs

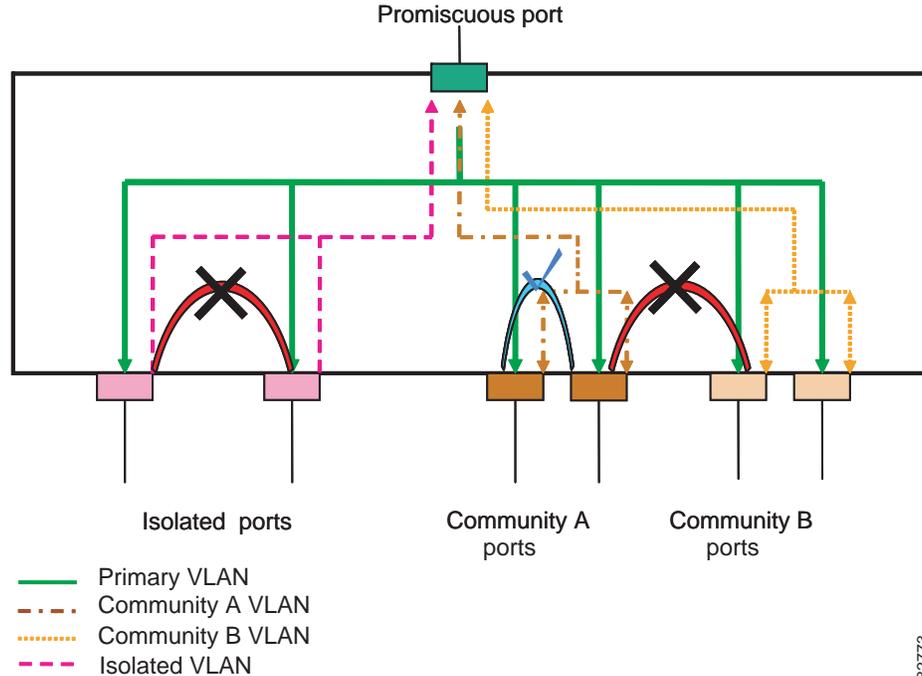
Primary VLANs and the two types of secondary VLANs (isolated and community) have these characteristics:

- **Primary VLAN**— The primary VLAN carries traffic from the promiscuous ports to the host ports, both isolated and community, and to other promiscuous ports.
- **Isolated VLAN** —An isolated VLAN is a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports. You can configure multiple isolated VLANs in a private VLAN domain; all the traffic remains isolated within each one. Each isolated VLAN can have several isolated ports, and the traffic from each isolated port also remains completely separate.
- **Community VLAN**—A community VLAN is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port and to other host ports in the same community. You can configure multiple community VLANs in a private VLAN domain. The ports within one community can communicate, but these ports cannot communicate with ports in any other community or isolated VLAN in the private VLAN.

Figure 1-2 shows the traffic flows within a private VLAN, along with the types of VLANs and types of ports.

Send feedback to nx5000-docfeedback@cisco.com

Figure 1-2 Private VLAN Traffic Flows



182773

**Note**

The private VLAN traffic flows are unidirectional from the host ports to the promiscuous ports. Traffic received on primary VLAN enforces no separation and forwarding is done as in normal VLAN.

A promiscuous port can serve only one primary VLAN and multiple secondary VLANs (community and isolated VLANs). With a promiscuous port, you can connect a wide range of devices as access points to a private VLAN. For example, you can use a promiscuous port to monitor or back up all the private VLAN servers from an administration workstation.

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.

Associating Primary and Secondary VLANs

For host ports in secondary VLANs to communicate outside the private VLAN, you associate secondary VLANs to the primary VLAN. If the association is not operational, the host ports (community and isolated ports) in the secondary VLAN are brought down.

**Note**

You can associate a secondary VLAN with only one primary VLAN.

For an association to be operational, the following conditions must be met:

- The primary VLAN must exist and be configured as a primary VLAN.
- The secondary VLAN must exist and be configured as either an isolated or community VLAN.

Send feedback to nx5000-docfeedback@cisco.com



Note

Use the **show** command to verify that the association is operational. The switch does not display an error message when the association is nonoperational. (See the “[Verifying Private VLAN Configuration](#)” section on page 1-10 for information on configuration verification.)

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive. Use the **no private-vlan** command to return the VLAN to the normal mode. All primary and secondary associations on that VLAN are suspended, but the interfaces remain in private VLAN mode. When you convert the VLAN back to private VLAN mode, the original associations are reinstated.

If you enter the **no vlan** command for the primary VLAN, all private VLAN associations with that VLAN are lost. However, if you enter the **no vlan** command for a secondary VLAN, the private VLAN associations with that VLAN are suspended and return when you recreate the specified VLAN and configure it as the previous secondary VLAN.

In order to change the association between a secondary and primary VLAN, you must first remove the current association and then add the desired association.

Understanding Broadcast Traffic in Private VLANs

Broadcast traffic from ports in a private VLAN flows in the following ways:

- The broadcast traffic flows from a promiscuous port to all ports in the primary VLAN (which includes all the ports in the community and isolated VLANs). This broadcast traffic is distributed to all ports within the primary VLAN, including those ports that are not configured with private VLAN parameters.
- The broadcast traffic from an isolated port is distributed only to those promiscuous ports in the primary VLAN that are associated to that isolated port.
- The broadcast traffic from community ports is distributed to all ports within the port’s community and to all promiscuous ports that are associated to the community port. The broadcast packets are not distributed to any other communities within the primary VLAN, or to any isolated ports.

Understanding Private VLAN Port Isolation

You can use private VLANs to control access to end stations as follows:

- Configure selected interfaces connected to end stations as isolated ports to prevent any communication. For example, if the end stations are servers, this configuration prevents communication between the servers.
- Configure interfaces connected to default gateways and selected end stations (for example, backup servers) as promiscuous ports to allow all end stations access to a default gateway.

Configuring a Private VLAN



Note

You must have already created the VLAN before you can assign the specified VLAN as a private VLAN,

This section includes the following topics:

Send feedback to nx5000-docfeedback@cisco.com

- Configuration Guidelines for Private VLANs, page 1-6
- Enabling Private VLANs, page 1-6
- Configuring a VLAN as a Private VLAN, page 1-7
- Associating Secondary VLANs with a Primary Private VLAN, page 1-7
- Configuring an Interface as a Private VLAN Host Port, page 1-8
- Configuring an Interface as a Private VLAN Promiscuous Port, page 1-9

Configuration Guidelines for Private VLANs

When configuring private VLANs, follow these guidelines:

- You must enable private VLANs before the switch can apply the private VLAN functionality.
- You cannot disable private VLANs if the switch has any operational ports in a private VLAN mode.
- Enter the **private-vlan synchronize** command to map the secondary VLANs to the same Multiple Spanning Tree (MST) instance as the primary VLAN. See the “[Mapping Secondary VLANs to Same MSTI as Primary VLANs for Private VLANs](#)” section on page 1-16 for more details.

Enabling Private VLANs

You must enable private VLANs on the switch to use the private VLAN functionality.



Note

The private VLAN commands do not appear until you enable the private VLAN feature.

To enable private VLAN functionality on the switch, perform this task:

	Command	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# feature private-vlan	Enables the private VLAN feature on the switch.

This example shows how to enable the private VLAN feature on the switch:

```
switch# configure terminal
switch(config)# feature private-vlan
```

To disable private VLAN functionality, perform this task:

	Command	Purpose
	switch(config)# no feature private-vlan	Disables the private VLAN feature on the switch.
		Note You cannot disable private VLANs if there are operational ports on the switch that are in private VLAN mode.

Send feedback to nx5000-docfeedback@cisco.com

Configuring a VLAN as a Private VLAN

To create a private VLAN, you first create a VLAN, and then configure that VLAN to be a private VLAN. Ensure that the private VLAN feature is enabled.

To create a private VLAN, perform this task:

	Command	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# vlan {vlan-id vlan-range}	Places you into the VLAN configuration submode.
Step 3	switch(config-vlan)# private-vlan {community isolated primary}	Configures the VLAN as either a community, isolated, or primary private VLAN. In a private VLAN, you must have one primary VLAN. You can have multiple community and isolated VLANs.

This example shows how to assign VLAN 5 to a private VLAN as the primary VLAN:

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# private-vlan primary
```

This example shows how to assign VLAN 100 to a private VLAN as a community VLAN:

```
switch(config-vlan)# exit
switch(config)# vlan 100
switch(config-vlan)# private-vlan community
```

This example shows how to assign VLAN 109 to a private VLAN as an isolated VLAN:

```
switch(config-vlan)# exit
switch(config)# vlan 109
switch(config-vlan)# private-vlan isolated
```

To disable a private VLAN, perform this task:

Command	Purpose
switch(config-vlan)# no private-vlan {community isolated primary}	Removes the private VLAN configuration from the specified VLAN(s) and returns it to normal VLAN mode. If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive.

Associating Secondary VLANs with a Primary Private VLAN

When you associate secondary VLANs with a primary VLAN, follow these guidelines:

- The *secondary-vlan-list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single secondary VLAN ID or a hyphenated range of secondary VLAN IDs.
- The *secondary-vlan-list* parameter can contain multiple community and isolated VLAN IDs.

Send feedback to nx5000-docfeedback@cisco.com

- 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.
- You change the association between a secondary and primary VLAN by removing the existing association and then adding the desired association.

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive. When you enter the **no private-vlan** command, the VLAN returns to the normal VLAN mode. All primary and secondary associations on that VLAN are suspended, but the interfaces remain in private VLAN mode. If you again convert the specified VLAN to private VLAN mode, the original associations are reinstated.

If you enter the **no vlan** command for the primary VLAN, all private VLAN associations with that VLAN are lost. However, if you enter the **no vlan** command for a secondary VLAN, the private VLAN associations with that VLAN are suspended and return when you recreate the specified VLAN and configure it as the previous secondary VLAN.

Ensure that the private VLAN feature is enabled.

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

	Command	Purpose
Step 1	<code>switch# configure terminal</code>	Enters configuration mode.
Step 2	<code>switch(config)# vlan primary-vlan-id</code>	Enter the number of the primary VLAN that you are working in for the private VLAN configuration.
Step 3	<code>switch(config-vlan)# private-vlan association {[add] secondary-vlan-list remove secondary-vlan-list}</code>	Associates the secondary VLANs with the primary VLAN.

This example shows how to associate community VLANs 100 through 103 and isolated VLAN 109 with primary VLAN 5:

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# private-vlan association 100-103, 109
```

To remove all associations from the private VLAN, perform this task:

	Command	Purpose
	<code>switch(config-vlan)# no private-vlan association</code>	Removes all associations from the primary VLAN and returns it to normal VLAN mode.

Configuring an Interface as a Private VLAN Host Port

You can configure an interface as a private VLAN host port. In private VLANs, host ports are part of the secondary VLANs, which are either community VLANs or isolated VLANs. You then associate the host port with both the primary and secondary VLANs.

Send feedback to nx5000-docfeedback@cisco.com



Note

We recommend that you enable BPDU Guard on all interfaces configured as a host ports. See [Chapter 1, “Configuring STP Extensions”](#) for information on configuring BPDU Guard.

Ensure that the private VLAN feature is enabled.

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

	Command	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# interface <i>type slot/port</i>	Selects the port to configure as a private VLAN host port. The interface can be either a physical Ethernet port.
Step 3	switch(config-if)# switchport mode private-vlan host	Configures the port as a host port for a private VLAN.
Step 4	switch(config-if)# switchport private-vlan host-association { <i>primary-vlan-id</i> } { <i>secondary-vlan-id</i> }	Associates the port with the primary and secondary VLANs of a private VLAN. The secondary VLAN can be either an isolated or community VLAN.

This example shows how to configure the Ethernet port 1/12 as a host port for a private VLAN and associate it to primary VLAN 5 and secondary VLAN 101:

```
switch# configure terminal
switch(config)# interface ethernet 1/12
switch(config-if)# switchport mode private-vlan host
switch(config-if)# switchport private-vlan host-association 5 101
```

To remove the private VLAN association from an interface, perform this task:

	Command	Purpose
	switch(config-if)# no switchport private-vlan host-association	Removes the private VLAN association from the port.

Configuring an Interface as a Private VLAN Promiscuous Port

You can configure an interface as a private VLAN promiscuous port, and then you can associate that promiscuous port with the primary and secondary VLANs.

Ensure that the private VLAN feature is enabled.

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

	Command	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# interface <i>type slot/port</i>	Selects the port to configure as a private VLAN promiscuous port. A physical interface is required.

Send feedback to nx5000-docfeedback@cisco.com

	Command	Purpose
Step 3	<code>switch(config-if)# switchport mode private-vlan promiscuous</code>	Configures the port as a promiscuous port for a private VLAN. You can only enable a physical Ethernet port as the promiscuous port.
Step 4	<code>switch(config-if)# switchport private-vlan mapping {primary-vlan-id} {secondary-vlan-list add secondary-vlan-list remove secondary-vlan-list}</code>	Configures the port as a promiscuous port and associates the specified port with a primary VLAN and a selected list of secondary VLANs. The secondary VLAN can be either an isolated or community VLAN.

This example shows how to configure port 1/2 as a promiscuous port associated with the primary VLAN 5 and the secondary isolated VLAN 109:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# switchport private-vlan mapping 5 109
```

You can only apply this command to a physical interface.

To clear the private VLAN mapping, perform this task:

Command	Purpose
<code>switch(config-if)# no switchport private-vlan mapping</code>	Clears the mapping from the private VLAN.

Verifying Private VLAN Configuration

To display private VLAN configuration information, use the following commands:

Command	Purpose
<code>switch# show system internal clis feature</code>	Displays the features enabled on the switch.
<code>switch# show vlan private-vlan [type]</code>	Displays the status of the private VLAN.
<code>switch# show interface switchport</code>	Displays information on all interfaces configured as switchports.

The following example shows how to display the private VLAN configuration:

```
switch# show vlan private-vlan
Primary Secondary Type Ports
-----
5 100 community
5 101 community Eth1/12, veth1/1
5 102 community
5 103 community
5 109 isolated Eth1/2
switch# show vlan private-vlan type
Vlan Type
-----
5 primary
```

Send feedback to nx5000-docfeedback@cisco.com

```
100 community
101 community
102 community
103 community
109 isolated
```

The following example shows how to display enabled features:

```
switch# show system internal clis feature
7 pvlan enabled
```

Send feedback to nx5000-docfeedback@cisco.com