Configuring Private VLANs Using NX-OS

Information About Private VLANs

Note You must enable the private VLAN feature before you can configure this feature.

Note A Layer 2 port can function as either a trunk port, an access port, or a private VLAN port.

In certain instances where similar systems do not need to interact directly, private VLANs provide additional protection at the Layer 2 level. Private VLANs are an association of primary and secondary VLANs.

A primary VLAN defines the broadcast domain with which the secondary VLANs are associated. The secondary VLANs may either be isolated VLANs or community VLANs. Hosts on isolated VLANs communicate only with associated promiscuous ports in primary VLANs, and hosts on community VLANs communicate only among themselves and with associated promiscuous ports but not with isolated ports or ports in other community VLANs.

In configurations that use integrated switching and routing functions, you can assign a single Layer 3 VLAN network interface to each private VLAN to provide routing. The VLAN network interface is created for the primary VLAN. In such configurations, all secondary VLANs communicate at Layer 3 only through a mapping with the VLAN network interface on the primary VLAN. Any VLAN network interfaces previously created on the secondary VLANs are put out-of-service.

Private VLAN Overview

You must enable private VLANs before the device can apply the private VLAN functionality.

You cannot disable private VLANs if the device has any operational ports in a private VLAN mode.

Note You must have already created the VLAN before you can convert the specified VLAN to a private VLAN, either primary or secondary.

Primary and Secondary VLANs in Private VLANs

The private VLAN feature addresses two problems that users encounter when using VLANs:

- Each VDC supports up to 4096 VLANs. If a user assigns one VLAN per customer, the number of customers that the service provider can support is limited.
- To enable IP routing, each VLAN is assigned with a subnet address space or a block of addresses, which can result in wasting the unused IP addresses and creating IP address management problems.

Using private VLANs solves the scalability problem and provides IP address management benefits and Layer 2 security for customers.

The private VLAN feature allows you to partition the Layer 2 broadcast domain of a VLAN into subdomains. A subdomain is represented by a pair of private VLANs: a primary VLAN and a secondary VLAN. A private VLAN domain can have multiple private VLAN pairs, one pair for each subdomain. All VLAN pairs in a private VLAN domain share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another.

Note A private VLAN domain has only one primary VLAN.

Secondary VLANs provide Layer 2 isolation between ports within the same private VLAN. The following two types are secondary VLANs within a primary VLAN:

- 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 community VLANs or in any isolated VLANs at the Layer 2 level.

Private VLAN Ports

Note Both community and isolated private VLAN ports are labeled as PVLAN host ports. A PVLAN host port is either a community PVLAN port or an isolated PVLAN port depending on the type of secondary VLAN with which it is associated.

The types of private VLAN ports are as follows:

- Promiscuous port—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 association for load balancing or redundancy purposes. You can also have secondary VLANs that are not associated to any promiscuous port, but these secondary VLANs cannot communicate to the Layer 3 interface.

Note As a best practice, you should map all the secondary ports on the primary to minimize any loss of traffic.

- Promiscuous trunk—You can configure a promiscuous trunk port to carry traffic for multiple primary VLANs. You map the private VLAN primary VLAN and either all or selected associated VLANs to the promiscuous trunk port. Each primary VLAN and one associated secondary VLAN is a private VLAN pair, For maximum PVLAN mappings, see *Verified Scalability Guide*.

Note Private VLAN promiscuous trunk ports carry traffic for normal VLANs as well as for primary private VLANs.

- Isolated port—An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete Layer 2 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, and each port is completely isolated from all other ports in the isolated VLAN.
- Isolated or secondary trunk—You can configure an isolated trunk port to carry traffic for multiple isolated VLANs. Each secondary VLAN on an isolated trunk port must be associated with a different primary VLAN. You cannot put two secondary VLANs that are associated with the same primary VLAN on an isolated trunk port. Each primary VLAN and one associated secondary VLAN is a private VLAN pair. For maximum PVLAN associations, see *Verified Scalability Guide*.

Note Private VLAN isolated trunk ports carry traffic for normal VLANs as well as for secondary private VLANs.

- 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 associated promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities and from all isolated ports within the private VLAN domain.

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

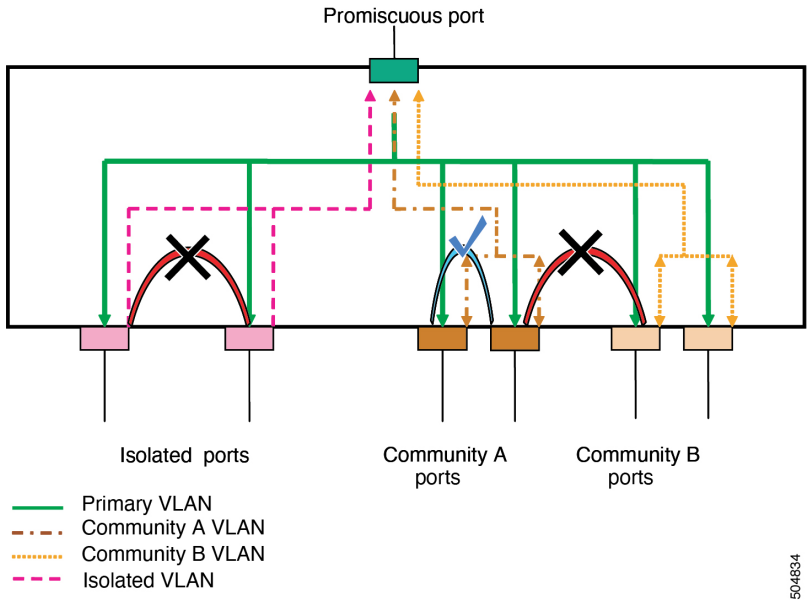
Primary, Isolated, and Community Private VLANs

Because the primary VLAN has the Layer 3 gateway, you associate secondary VLANs with the primary VLAN in order to communicate outside the private VLAN. Primary VLANs and the two types of secondary VLANs, isolated VLANs and community VLANs, have these characteristics:

- Primary VLAN— The primary VLAN carries traffic from the promiscuous ports to the (isolated and community) host ports 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 and the Layer 3 gateway. You can configure one isolated VLAN in a primary VLAN. In addition, 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 gateways 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: Private VLAN Layer 2 Traffic Flows

This figure shows the Layer 2 traffic flows within a primary, or private VLAN, along with the types of VLANs and types of ports.



Note The private VLAN traffic flows are unidirectional from the host ports to the promiscuous ports. Traffic that egresses the promiscuous port acts like the traffic in a normal VLAN, and there is no traffic separation among the associated secondary VLAN.

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

Note You can configure private VLAN promiscuous and isolated trunk ports. These promiscuous and isolated trunk ports carry traffic for multiple primary and secondary VLANs as well as normal VLAN.

Although you can have several promiscuous ports in a primary VLAN, you can have only one Layer 3 gateway per primary VLAN.

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.

Note You must enable the VLAN interface feature before you can configure the Layer 3 gateway. See the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide* for complete information on VLAN network interfaces and IP addressing.

Associating Primary and Secondary VLANs

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

Note See the **show** command display to verify that the association is operational. The device does not issue an error message when the association is nonoperational.

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive. When you reconvert the specified VLAN to private VLAN mode, the original associations are reinstated.

If the association is not operational on private VLAN trunk ports, only that VLAN goes down, not the entire port.

When you enter the **no private-vlan** command, the VLAN returns to the normal VLAN mode. All associations on that VLAN are suspended, but the interfaces remain in private VLAN mode.

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 secondary VLAN.

Note This behavior is different from how Catalyst devices work.

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.

Broadcast Traffic in Private VLANs

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

- The broadcast traffic flows from all promiscuous ports to all ports in the primary VLAN. 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 all isolated ports 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.

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 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 (for example, backup servers) as promiscuous ports to allow all end stations access to a default gateway.

Private VLANs and VLAN Interfaces

A VLAN interface to a Layer 2 VLAN is also called a switched virtual interface (SVI). Layer 3 devices communicate with a private VLAN only through the primary VLAN and not through secondary VLANs.

Configure VLAN network interfaces only for primary VLANs. Do not configure VLAN interfaces for secondary VLANs. VLAN network interfaces for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN. You will see the following actions if you misconfigure the VLAN interfaces:

- If you try to configure a VLAN with an active VLAN network interface as a secondary VLAN, the configuration is not allowed until you disable the VLAN interface.
- If you try to create and enable a VLAN network interface on a VLAN that is configured as a secondary VLAN, that VLAN interface remains disabled and the system returns an error.

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

Note You must enable the VLAN interface feature before you configure VLAN interfaces. See the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*, for information on VLAN interfaces and IP addressing.

Private VLANs Across Multiple Devices

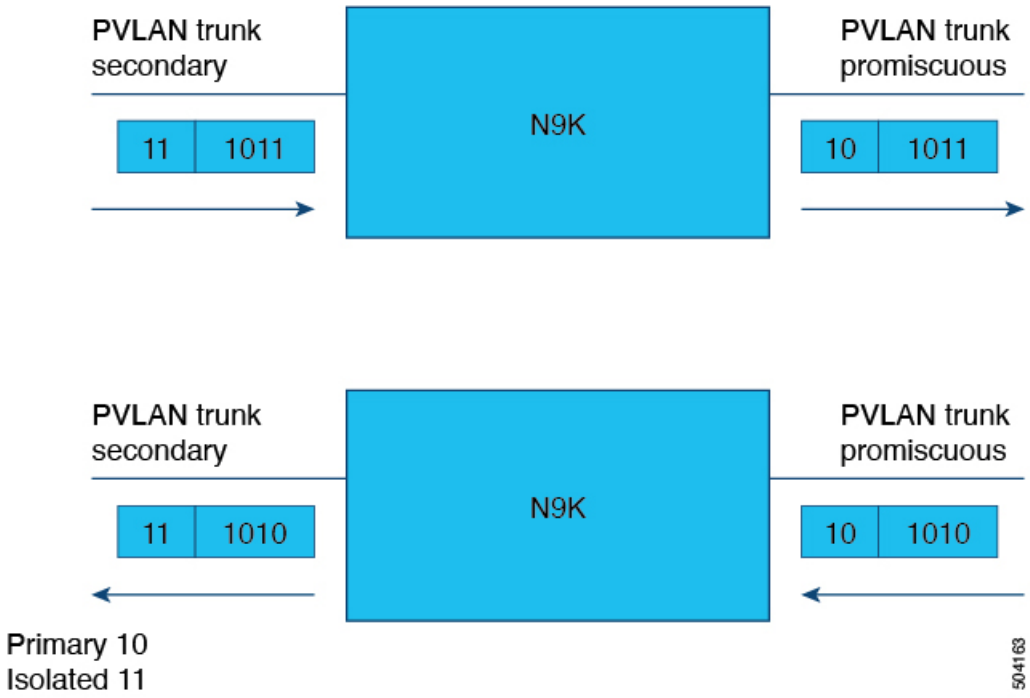
You can extend private VLANs across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support private VLANs. To maintain the security of your private VLAN configuration and to avoid other uses of the VLANs configured to be private VLANs, configure private VLANs on all intermediate devices, including devices that have no private VLAN ports.

Private VLAN with Inner VLAN Tag Preservation

Beginning with Cisco NX-OS Release 10.2(3)F, if you have configured the global **system dot1q-tunnel transit** <*vlan*> command on a supported Cisco Nexus switch that acts as a transit box, then the packets coming in on private vlan trunk ports with 2 or more tags are preserved and sent out without stripping any of the inner tags. For more information about the command, refer to *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide* of the relevant release on cisco.com.

Note Inner tag preservation does not work when PVLAN and QinQ are configured on the same port.

The following figure illustrates the inner tag preservation on the supported Cisco Nexus switch when the packet moves from PVLAN secondary trunk to PVLAN promiscuous trunk and back.



A sample configuration is as follows:

```
vlan 10
private-vlan primary
private-vlan association 11-12
vlan 11
private-vlan isolated
vlan 12
private-vlan community

interface Ethernet1/1
switchport
switchport mode private-vlan trunk secondary
switchport private-vlan association trunk 10 11
no shutdown

interface Ethernet1/2
switchport
switchport mode private-vlan trunk promiscuous
switchport private-vlan mapping trunk 10 11-12
no shutdown

(config)# system dot1q-tunnel transit vlan 10,11
```

High Availability for Private VLANs

The software supports high availability for both stateful and stateless restarts, as during a cold reboot, for private VLANs. For the stateful restarts, the software supports a maximum of three retries. If you try more than 3 times within 10 seconds of a restart, the software reloads the supervisor module.

Note See the *Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*, for complete information on high-availability features.

Prerequisites for Private VLANs

Private VLANs have the following prerequisites:

- You must be logged onto the device.
- You must enable the private VLAN feature.

Guidelines and Limitations for Configuring Private VLANs

Private VLANs (PVLANs) have the following configuration guidelines and limitations:

- When changing the PVLAN mapping on the vPC Port-channel in the promiscuous mode, the vPC PO member on vPC secondary flaps.
- **show** commands with the **internal** keyword are not supported.
- You must enable PVLANs before the device can apply the PVLAN functionality.
- PVLAN and Port-VLAN mapping can coexist on the same switch but not on the same port. These features operate independently on separate ports. You can configure and use the same VLAN for both functionalities. This is applicable on these releases.
  - Cisco NX-OS Release 10.2(9)M
  - Cisco NX-OS Release10.3(7)M
  - Cisco NX-OS Release 10.4(5)M
- PVLANs are supported over vPCs and port channels for these switches:
  - Cisco Nexus 9200 Setries
  - Cisco Nexus 9300, 9300-EX, 9300-FX, 9300-FX2 and 9300-FX3 Series switches
  - Cisco Nexus 9500 Series switches (with all line cards except the N9K-X9432C-S)

  PVLANs are not supported over vPCs and port channels for these switches:
  - Cisco Nexus 3232C and 3264Q
- You must enable the VLAN interface feature before the device can apply this functionality.
- Shut down the VLAN network interface for all VLANs that you plan to configure as secondary VLANs before you configure these VLANs.

- When a static MAC is created on a regular VLAN and then that VLAN is converted to a secondary VLAN, the Cisco NX-OS maintains the MAC that was configured on the secondary VLAN as the static MAC.
- PVLANs support PVLAN port modes as follows:
  - Promiscuous.
  - Promiscuous trunk.
  - Isolated host.
  - Isolated host trunk.
  - Community host.
- Beginning with Cisco NX-OS Release 9.2(1), PVLANs support VXLANs.
- Private VLANs provide port mode support for port channels.
- Private VLANs provide port mode support for virtual port channels (vPCs) interfaces.
- When you configure PVLAN promiscuous trunks or PVLAN isolated trunks, we recommend that you allow non-PVLANs in the list specified by the **switchport private-vlan trunk allowed** *id* command. PVLANs are mapped or associated depending on the PVLAN trunk mode.

Note You cannot connect a second switch to a promiscuous or isolated PVLAN trunk. The PVLAN promiscuous trunk or PVLAN isolated trunk is supported only on host-switch.

- The **system private-vlan fex trunk** command is not supported on Cisco Nexus 9300 -FX, -FX2, -FX3 platform switches. The following PVLAN modes are supported on FEX ports and port-channels only in single-homed FEX configurations (no support in AA or ST vPC modes).
  - Isolated host
  - Community host
  - Isolated trunk

  These modes are supported only on FEX ports and port-channels in single-homed FEX configurations (with no support in AA or ST vPC modes).
- PVLANs support PACLs and RACLs.
- PVLANs support SVIs as follows:
  - SVIs on the primary VLANs.
  - Primary and secondary IP addresses on the SVI.
  - HSRP on the primary SVI.
- PVLANs support Layer 2 forwarding.
- PVLANs support STP as follows:

  - RSTPs
  - MSTs
- PVLANs are supported across switches through a regular trunk port.
- PVLANs are supported on the 10G ports of the Cisco Nexus 9396PQ and 93128TX switches.
- PVLAN configurations are not supported on the ALE ports of Cisco Nexus 9300 Series switches.
- PVLAN port mode is not supported on the Cisco Nexus 3164Q switch.
- On Network Forwarding Engines (NFE), PVLANs do not provide support on breakout.
- PVLANs are not supported on vPC or port channel FEX ports.
- PVLANs do not provide support for IP multicast or IGMP snooping.
- Beginning with Cisco NX-OS Release 9.3(3), the following features are supported on Cisco Nexus C9316D-GX, C93600CD-GX, and 9364C-GX switches.
  - vPC
  - 200k Mac scale
  - Dot1x
  - Port-security
  - Selective QinQ
  - Selective QinQ with multiple provider VLAN
- Beginning with Cisco NX-OS Release 9.3(5), PVLANs support DHCP snooping.
- Beginning with Cisco NX-OS Release 9.3(5), PVLAN is supported on N9K-C93180YC-FX3S platform switches.
- Beginning with Cisco NX-OS Release 9.3(9), PVLAN configuration is not allowed on vPC Peer-link interfaces.
- PVLANs do not provide support for PVLAN QoS.
- PVLANs do not provide support for VACLs.
- PVLANs do not provide support for VTP.
- PVLANs do not provide support for tunnels.
- PVLANs do not provide support for SPAN when the source is a PVLAN VLAN.
- You cannot configure a shared interface to be part of a PVLAN. For more details, see the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*.
- Although the Cisco NX-OS CLI allows the configuration of multiple isolated VLAN configurations per PVLAN group, such a configuration is not supported. A PVLAN group can have at most one isolated VLAN.
- PVLAN association on a VLAN is not supported.

- MAC address learning for PVLAN host ports and normal trunks happens on the Primary VLAN. For normal trunks, packets are exchanged using secondary VLAN, but MAC learning is still enforced in Primary VLAN.
- PVLANs are not supported on Cisco Nexus 9500 Series switches with N9K-X9636C-R, N9K-X9636Q-R, N9K-X9636C-RX line cards.
- Beginning with Cisco NX-OS Release 10.1(2), the combination of PVLAN and portSec feature on a vPC orphan port has limitations on dynamic Mac syncing across peers and triggers.
- Beginning with Cisco NX-OS Release 10.2(2)F, the following features are supported on Cisco N9K-9332D-GX2B platform switches.
  - PVLAN and Flex Links
  - VPC
  - Selective QinQ
  - Selective QinQ with multiple provider Vlan
- Beginning with Cisco NX-OS Release 10.2(3)F, if the global command, **system dot1q-tunnel transit**, is configured on the Nexus switch that acts as a transit box, then when a packet comes in with two or more tags, the Private VLAN with Inner VLAN Tag Preservation feature allows for preservation of the inner tag for PVLAN. This feature is supported only on EX, FX, FX2, FX3, GX, and GX2B based Cisco Nexus 9000 Series TOR switches.
- Inner tag preservation does not work when PVLAN and Q-in-Q are configured on the same port.
- Beginning with Cisco NX-OS Release 10.3(3)F, IPv6 underlay is supported on PVLAN for VXLAN EVPN on Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2 switches and Cisco Nexus 9500 switches with 9700-EX/FX/GX line cards.
- Beginning with Cisco NX-OS Release 10.4(2)F, PVLAN is supported on C93108TC-FX3 switch.

Default Settings for Private VLANs

This table lists the default setting for private VLANs.

Table 1: Default Private VLAN Setting

Parameters	Default
Private VLANs	Disabled

Configuring a Private VLAN

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

See the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*, for information on assigning IP addresses to VLAN interfaces.

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Enabling Private VLANs - CLI Version

You must enable private VLANs on the device to have the private VLAN functionality.

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

SUMMARY STEPS

1. **config t**
2. **feature private-vlan**
3. **exit**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**feature private-vlan**
	Example:
	`switch(config)# feature private-vlan`
	`switch(config)#`
		Enables private VLAN functionality on the device.
		Note
		You must completely remove any PVLAN configuration before disabling the private VLAN feature using the **no feature private-vlan** command. For earlier software releases, you must bring any PVLAN ports to the operationally down state before applying the **no feature private-vlan** command.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits the configuration mode.

Step 4	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	`switch(config)# copy running-config startup-config`	

Example

This example shows how to enable private VLAN functionality on the device:

```
switch# config t
switch(config)# feature private-vlan
switch(config)#
```

Configuring a VLAN as a Private VLAN - CLI Version

Note Before you configure a VLAN as a secondary VLAN—that is, either a community or isolated VLAN—you must first shut down the VLAN network interface.

You can configure 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.

You create all VLANs that you want to use in the private VLAN as a primary VLAN, a community VLAN, or an isolated VLAN. You will later associate multiple isolated and multiple community VLANs to one primary VLAN. You can have many primary VLANs and associations, which means that you could have many private VLANs.

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive.

On private VLAN trunk ports, if you delete either the secondary or primary VLAN, only that specific VLAN becomes inactive; the trunk ports stay up.

SUMMARY STEPS

1. **config t**
2. **vlan** {*vlan-id* | *vlan-range*}
3. [**no**] **private-vlan** {**community** | **isolated | primary**}
4. **exit**
5. (Optional) **show vlan private-vlan** [*type*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**config t** **Example:**	Enters configuration mode.

	Command or Action	Purpose
	`switch# config t` `switch(config)#`	

Step 2	**vlan** {*vlan-id* | *vlan-range*}
	Example:
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		Places you into the VLAN configuration submode.

Step 3	[**no**] **private-vlan** {**community** | **isolated** | **primary**} **Example:** `switch(config-vlan)# private-vlan 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. or 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.

Step 4	**exit**
	Example:
	`switch(config-vlan)# exit`
	`switch(config)#`
		Exits the VLAN configuration submode.

Step 5	(Optional) **show vlan private-vlan** [*type*] **Example:** `switch# show vlan private-vlan`	Displays the private VLAN configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

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

```
switch# config t
switch(config)# vlan 5
switch(config-vlan)# private-vlan primary
switch(config-vlan)# exit
switch(config)#
```

Associating Secondary VLANs with a Primary Private VLAN - CLI Version

Follow these guidelines when you associate secondary VLANs with a primary VLAN:

- 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.
- Enter a *secondary-vlan-list* or enter the **add** keyword with a *secondary-vlan-list* to associate secondary VLANs with a primary VLAN.
- Enter 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 associations on that VLAN are suspended, but the interfaces remain in private VLAN mode.

When you reconvert 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.

Before you begin

Ensure that the private VLAN feature is enabled.

SUMMARY STEPS

1. **config t**
2. **vlan** *primary-vlan-id*
3. [**no**] **private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}
4. **exit**
5. (Optional) **show vlan private-vlan** [**type**]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**vlan** *primary-vlan-id*
	Example:
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		Enters the number of the primary VLAN that you are working in for the private VLAN configuration.

	Command or Action	Purpose
Step 3	[**no**] **private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*} **Example:** `switch(config-vlan)# private-vlan association 100-105,109`	Use one form of the command to Associate the secondary VLANs with the primary VLAN. or Remove all associations from the primary VLAN and return it to normal VLAN mode.

Step 4	**exit**
	Example:
	`switch(config-vlan)# exit`
	`switch(config)#`
		Exits the VLAN configuration submode.

Step 5	(Optional) **show vlan private-vlan** [**type**] **Example:** `switch# show vlan private-vlan`	Displays the private VLAN configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

This example shows how to associate community VLANs 100 through 105 and isolated VLAN 109 with primary VLAN 5:

```
switch(config)# vlan 5
switch(config-vlan)# private-vlan association 100-105, 109
switch(config-vlan)# exit
switch(config)#
```

Mapping Secondary VLANs to the VLAN Interface of a Primary VLAN - CLI Version

Note See the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*, for information on assigning IP addresses to VLAN interfaces on primary VLANs of private VLANs.

You map secondary VLANs to the VLAN interface of a primary VLAN. Isolated and community VLANs are both called secondary VLANs. To allow Layer 3 processing of private VLAN ingress traffic, you map secondary VLANs to the VLAN network interface of a primary VLAN.

Note You must enable VLAN network interfaces before you configure the VLAN network interface. VLAN network interfaces on community or isolated VLANs that are associated with a primary VLAN will be out of service. Only the VLAN network interface on the primary VLAN is in service.

Before you begin

- Enable the private VLAN feature.
- Enable the VLAN interface feature.
- Ensure that you are working on the correct primary VLAN Layer 3 interface to map the secondary VLANs.

SUMMARY STEPS

1. **config t**
2. **interface vlan** *primary-vlan-ID*
3. [**no**] **private-vlan mapping** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}
4. **exit**
5. (Optional) **show interface vlan** *primary-vlan-id* **private-vlan mapping**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**interface vlan** *primary-vlan-ID*
	Example:
	`switch(config)# interface vlan 5`
	`switch(config-if)#`
		Enters the number of the primary VLAN that you are working in for the private VLAN configuration. Places you into the interface configuration mode for the primary VLAN.

Step 3	[**no**] **private-vlan mapping** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*} **Example:** `switch(config-if)# private-vlan mapping 100-105, 109`	Map the secondary VLANs to the SVI or Layer 3 interface of the primary VLAN. This action allows the Layer 3 switching of private VLAN ingress traffic. or Clear the mapping to the Layer 3 interface between the secondary VLANs and the primary VLANs.

	Command or Action	Purpose

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits the interface configuration mode.

Step 5	(Optional) **show interface vlan** *primary-vlan-id* **private-vlan mapping** **Example:** `switch(config)# show interface vlan 101 private-vlan mapping`	Displays the interface private VLAN information.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

This example shows how to map the secondary VLANs 100 through 105 and 109 on the Layer 3 interface of the primary VLAN 5:

```
switch #config t
switch(config)# interface vlan 5
switch(config-if)# private-vlan mapping 100-105, 109
switch(config-if)# exit
switch(config)#
```

Configuring a Layer 2 Interface as a Private VLAN Host Port

You can configure a Layer 2 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.

Note We recommend that you enable BPDU Guard on all interfaces configured as a host port.

You then associate the host port with both the primary and secondary VLANs.

Before you begin

Ensure that the private VLAN feature is enabled.

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **switchport mode private-vlan host**
4. [**no**] **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*}

5. **exit**
6. (Optional) **show interface switchport**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Selects the Layer 2 port to configure as a private VLAN host port.

Step 3	**switchport mode private-vlan host**
	Example:
	`switch(config-if)# switchport mode private-vlan host`
	`switch(config-if)#`
		Configures the Layer 2 port as a host port for a private VLAN.

Step 4	[**no**] **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*} **Example:** `switch(config-if)# switchport private-vlan host-association 10 50`	Associate the Layer 2 host port with the primary and secondary VLANs of a private VLAN. The secondary VLAN can be either an isolated or community VLAN. or Remove the private VLAN association from the port.

Step 5	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits the interface configuration mode.

Step 6	(Optional) **show interface switchport** **Example:** `switch# show interface switchport`	Displays information on all interfaces configured as switch ports.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

This example shows how to configure the Layer 2 port 2/1 as a host port for a private VLAN and associate it to primary VLAN 10 and secondary VLAN 50:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode private-vlan host
switch(config-if)# switchport private-vlan host-association 10 50
switch(config-if)# exit
switch(config)#
```

Configuring a Layer 2 Interface as a Private VLAN Isolated Trunk Port

You can configure a Layer 2 interface as a private VLAN isolated trunk port. These isolated trunk ports carry traffic for multiple secondary VLANs as well as normal VLANs.

Note You must associate the primary and secondary VLANs before they become operational on the private VLAN isolated trunk port.

Before you begin

Ensure that the private VLAN feature is enabled.

SUMMARY STEPS

1. **config t**
2. **interface** {*type slot/port*}
3. **switchport**
4. **switchport mode private-vlan trunk secondary**
5. (Optional) **switchport private-vlan trunk native vlan** *vlan-id*
6. **switchport private-vlan trunk allowed vlan** {**add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
7. [**no**] **switchport private-vlan association trunk** {*primary-vlan-id* [*secondary-vlan-id*]}
8. **exit**
9. (Optional) **show interface switchport**
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**config t** **Example:**	Enters configuration mode.

	Command or Action	Purpose
	`switch# config t` `switch(config)#`	

Step 2	**interface** {*type slot/port*}
	Example:
	`switch(config)# interface ethernet 2/11`
	`switch(config-if)#`
		Selects the Layer 2 port to configure as a private VLAN isolated trunk port.

Step 3	**switchport**
	Example:
	`switch(config-if)# switchport`
	`switch(config-if)#`
		Configures the Layer 2 port as a switch port.

Step 4	**switchport mode private-vlan trunk secondary**
	Example:
	`switch(config-if)# switchport mode private-vlan trunk secondary`
	`switch(config-if)#`
		Configures the Layer 2 port as an isolated trunk port to carry traffic for multiple isolated VLANs.
		Note
		You cannot put community VLANs into the isolated trunk port.

Step 5	(Optional) **switchport private-vlan trunk native vlan** *vlan-id* **Example:** `switch(config-if)# switchport private-vlan trunk native vlan 5`	Sets the native VLAN for the 802.1Q trunk. Valid values are from 1 to 3968 and 4048 to 4093. The default value is 1. **Note** If you are using a private VLAN as the native VLAN for the isolated trunk port, you must enter a value for a secondary VLAN or a normal VLAN; you cannot configure a primary VLAN as the native VLAN.

Step 6	**switchport private-vlan trunk allowed vlan** {**add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
	Example:
	`switch(config-if)# switchport private-vlan trunk allowed vlan add 1`
	`switch(config-if)#`
		Sets the allowed VLANs for the private VLAN isolated trunk interface. Valid values are from 1 to 3968 and 4048 to 4093.
		When you map the private primary and secondary VLANs to the isolated trunk port, the system automatically puts all the primary VLANs into the allowed VLAN list for this port.
		Note
		Ensure that the native VLAN is part of the allowed VLAN list. The default for this command is to allow no VLANs on this interface, so you must configure the native VLAN as an allowed VLAN, unless it is already added as an associated VLAN, to pass native VLAN traffic.

Step 7	[**no**] **switchport private-vlan association trunk** {*primary-vlan-id* [*secondary-vlan-id*]} **Example:**	Associate the Layer 2 isolated trunk port with the primary and secondary VLANs of private VLANs. The secondary VLAN must be an isolated VLAN. You can associate a maximum of 16 private VLAN primary and secondary

	Command or Action	Purpose
	`switch(config-if)# switchport private-vlan association trunk 10 101` `switch(config-if)#`	pairs on each isolated trunk port. You must reenter the command for each pair of primary and secondary VLANs that you are working with. **Note** Each secondary VLAN on an isolated trunk port must be associated with a different primary VLAN. You cannot put two isolated VLANs that are associated with the same primary VLAN into a private VLAN isolated trunk port. If you do, the last entry overwrites the previous entry. or Remove the private VLAN association from the private VLAN isolated trunk port.

Step 8	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits the interface configuration mode.

Step 9	(Optional) **show interface switchport** **Example:** `switch# show interface switchport`	Displays information on all interfaces configured as switch ports.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

This example shows how to configure the Layer 2 port 2/1 as a private VLAN isolated trunk port associated with three different primary VLANs and an associated secondary VLAN:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode private-vlan trunk
switch(config-if)# switchport private-vlan trunk allowed vlan add 1
switch(config-if)# switchport private-vlan association trunk 10 101
switch(config-if)# switchport private-vlan association trunk 20 201
switch(config-if)# switchport private-vlan association trunk 30 102
switch(config-if)# exit
switch(config)#
```

Configuring a Layer 2 Interface as a Private VLAN Promiscuous Port

You can configure a Layer 2 interface as a private VLAN promiscuous port and then associate that promiscuous port with the primary and secondary VLANs.

Before you begin

Ensure that the private VLAN feature is enabled.

SUMMARY STEPS

1. **config t**
2. **interface** {*type slot/port*}
3. **switchport mode private-vlan promiscuous**
4. [**no**] **switchport private-vlan mapping** {*primary-vlan-id*} {*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*}
5. **exit**
6. (Optional) **show interface switchport**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**interface** {*type slot/port*}
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Selects the Layer 2 port to configure as a private VLAN promiscuous port.

Step 3	**switchport mode private-vlan promiscuous** **Example:** `switch(config-if)# switchport mode private-vlan promiscuous`	Configures the Layer 2 port as a promiscuous port for a private VLAN.
Step 4	[**no**] **switchport private-vlan mapping** {*primary-vlan-id*} {*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*} **Example:** `switch(config-if)# switchport private-vlan mapping 10 50`	Configure the Layer 2 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. or Clear the mapping from the private VLAN.

Step 5	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits the interface configuration mode.

	Command or Action	Purpose
Step 6	(Optional) **show interface switchport** **Example:** `switch# show interface switchport`	Displays information on all interfaces configured as switch ports.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

This example shows how to configure the Layer 2 port 2/1 as a promiscuous port associated with the primary VLAN 10 and the secondary isolated VLAN 50:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# switchport private-vlan mapping 10 50
switch(config-if)# exit
switch(config)#
```

Configuring a Layer 2 Interface as a Private VLAN Promiscuous Trunk Port

You can configure a Layer 2 interface as a private VLAN promiscuous trunk port and then associate that promiscuous trunk port with multiple primary VLANs. These promiscuous trunk ports carry traffic for multiple primary VLANs as well as normal VLANs.

Note You must associate the primary and secondary VLANs before they become operational on the private VLAN promiscuous trunk port.

Before you begin

Ensure that the private VLAN feature is enabled.

SUMMARY STEPS

1. **config t**
2. **interface** {*type slot/port*}
3. **switchport**
4. **switchport mode private-vlan trunk promiscuous**
5. (Optional) **switchport private-vlan trunk native vlan** *vlan-id*
6. **switchport mode private-vlan trunk allowed vlan** {**add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
7. [**no**]**switchport private-vlan mapping trunk** *primary-vlan-id* [*secondary-vlan-id*] {**add** *secondary-vlan-list* | **remove** *secondary-vlan-id*}
8. **exit**

9. (Optional) **show interface switchport**
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**interface** {*type slot/port*}
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Selects the Layer 2 port to configure as a private VLAN promiscuous trunk port.

Step 3	**switchport**
	Example:
	`switch(config-if)# switchport`
	`switch(config-if)#`
		Configures the Layer 2 port as a switch port.

Step 4	**switchport mode private-vlan trunk promiscuous**
	Example:
	`switch(config-if)# switchport mode private-vlan trunk promiscuous`
	`switch(config-if)#`
		Configures the Layer 2 port as a promiscuous trunk port to carry traffic for multiple private VLANs as well as normal VLANs.

Step 5	(Optional) **switchport private-vlan trunk native vlan** *vlan-id* **Example:** `switch(config-if)# switchport private-vlan trunk native vlan 5`	Sets the native VLAN for the 802.1Q trunk. Valid values are from 1 to 3968 and 4048 to 4093. The default value is 1. **Note** If you are using a private VLAN as the native VLAN for the promiscuous trunk port, you must enter a value for a primary VLAN or a normal VLAN; you cannot configure a secondary VLAN as the native VLAN.

Step 6	**switchport mode private-vlan trunk allowed vlan** {**add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
	Example:
	`switch(config-if)# switchport private-vlan trunk allowed vlan add 1`
	`switch(config-if)#`
		Sets the allowed VLANs for the private VLAN promiscuous trunk interface. Valid values are from 1 to 3968 and 4048 to 4093.
		When you map the private primary and secondary VLANs to the promiscuous trunk port, the system automatically puts all the primary VLANs into the allowed VLAN list for this port.
		Note

	Command or Action	Purpose
		Ensure that the native VLAN is part of the allowed VLAN list. The default for this command is to allow no VLANs on this interface, so you must configure the native VLAN as an allowed VLAN, unless it is already added as an associated VLAN, to pass native VLAN traffic.

Step 7	[**no**]**switchport private-vlan mapping trunk** *primary-vlan-id* [*secondary-vlan-id*] {**add** *secondary-vlan-list* | **remove** *secondary-vlan-id*}
	Example:
	`switch(config-if)# switchport private-vlan mapping trunk 4 5`
	`switch(config-if)#`
		Map or remove the mapping for the promiscuous trunk port with the primary VLAN and a selected list of associated secondary VLANs. The secondary VLAN can be either an isolated or community VLAN. The private VLAN association between primary and secondary VLANs must be operational to pass traffic. You can map a maximum of 16 private VLAN primary and secondary pairs on each promiscuous trunk port. You must reenter the command for each primary VLAN that you are working with.
		or
		Remove the private VLAN promiscuous trunk mappings from the interface.

Step 8	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits the interface configuration mode.

Step 9	(Optional) **show interface switchport** **Example:** `switch# show interface switchport`	Displays information on all interfaces configured as switch ports.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

This example shows how to configure the Layer 2 port 2/1 as a promiscuous trunk port associated with two primary VLANs and their associated secondary VLANs:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport
switch(config-if)# switchport mode private-vlan trunk promiscuous
switch(config-if)# switchport private-vlan trunk allowed vlan add 1
switch(config-if)# switchport private-vlan mapping trunk 10 20
switch(config-if)# switchport private-vlan mapping trunk 11 21
switch(config-if)# exit
switch(config)#
```

Verifying the Private VLAN Configuration

To display private VLAN configuration information, perform one of the following tasks:

Command	Purpose
show running-config vlan *vlan-id*	Displays VLAN information.
show vlan private-vlan [*type*]	Displays information on private VLANs.
show interface private-vlan mapping	Displays information on interfaces for private VLAN mapping.
show interface vlan *primary-vlan-id* **private-vlan mapping**	Displays information on interfaces for private VLAN mapping.
show interface switchport	Displays information on all interfaces configured as switch ports.

Displaying and Clearing Private VLAN Statistics

To display private VLAN configuration information, perform one of the following tasks:

Command	Purpose
clear vlan [**id** *vlan-id*] **counters**	Clears counters for all VLANs or for a specified VLAN.
show vlan counters	Displays information on Layer 2 packets in each VLAN.

Configuration Examples for Private VLANs

The following example shows how to create the three types of private VLANs, how to associate the secondary VLANs to the primary VLAN, how to create a private VLAN host and promiscuous port and assign them to the correct VLAN, and how to create a VLAN interface, or SVI, to allow the primary VLAN to communicate with the rest of the network:

```
switch# configure terminal
switch(config)# vlan 2
switch(config-vlan)# private-vlan primary
switch(config-vlan)# exit
switch(config)# vlan 3
switch(config-vlan)# private-vlan community
switch(config-vlan)# exit
switch(config)# vlan 4
switch(config-vlan)# private-vlan isolated
switch(config-vlan)# exit

switch(config)# vlan 2
```

```
switch(config-vlan)# private-vlan association 3,4
switch(config-vlan)# exit

switch(config)# interface ethernet 1/11
switch(config-if)# switchport
switch(config-if)# switchport mode private-vlan host
switch(config-if)# exit
switch(config)# interface ethernet 1/12
switch(config-if)# switchport
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# exit

switch(config)# interface ethernet 1/11
switch(config-if)# switchport private-vlan host-association 2 3
switch(config-if)# exit
switch(config)# interface ethernet 1/12
switch(config-if)# switchport private-vlan mapping 2 3,4
switch(config-if)# exit

switch(config)# interface vlan 2
switch(config-vlan)# private-vlan mapping 3,4
switch(config-vlan)# exit
switch(config)#
```

Additional References for Private VLANs -- CLI Version

Related Documents

Related Topic	Document Title
VLAN interfaces, IP addressing	*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*
Static MAC addresses, security	*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*
Cisco NX-OS fundamentals	*Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*
High availability	*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*
System management	*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*
Licensing	*Cisco NX-OS Licensing Guide*
Release notes	*Cisco Nexus 9000 Series NX-OS Release Notes*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
• CISCO-PRIVATE-VLAN-MIB	For more information, refer to https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html.