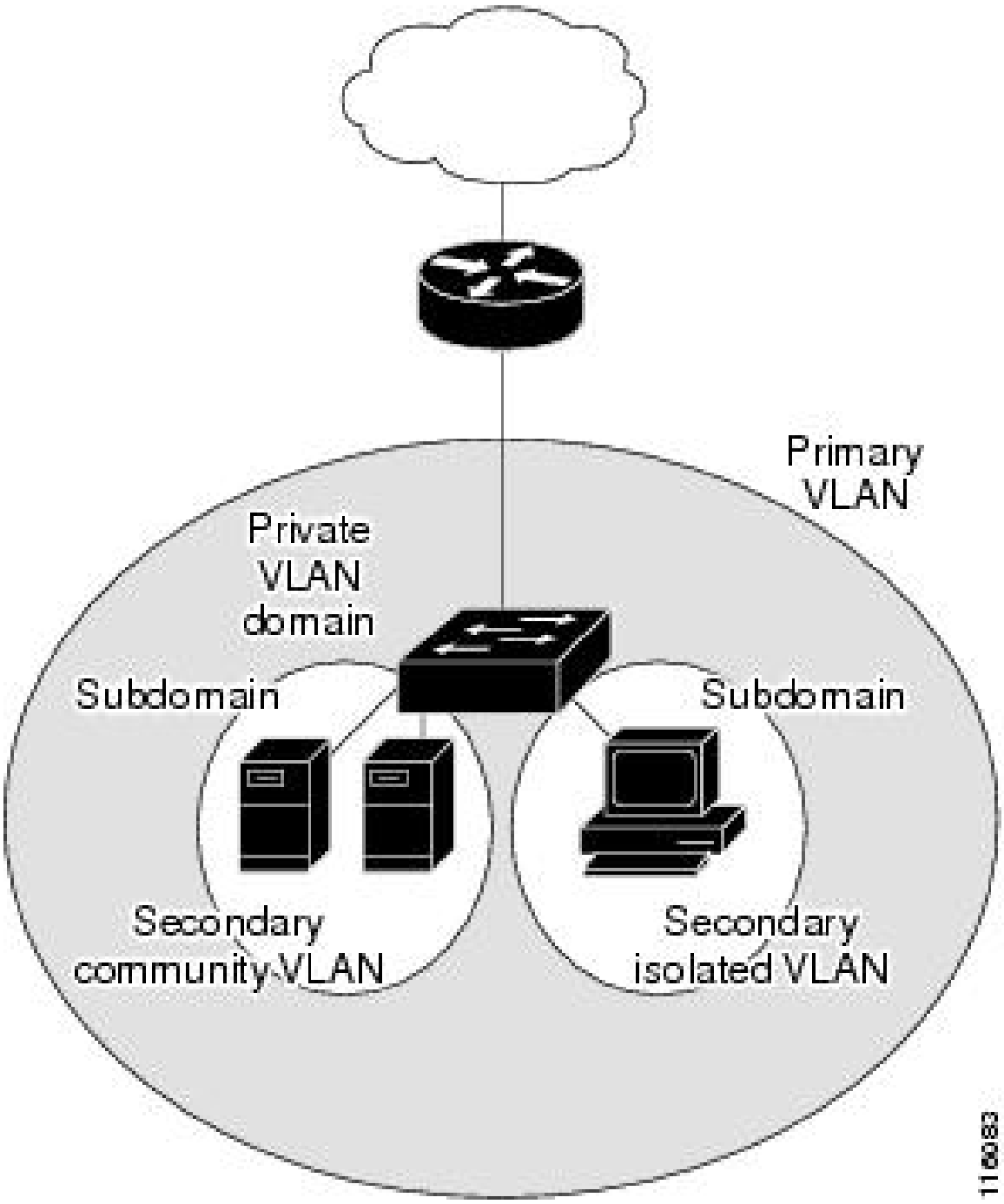
Configuring Private VLANs

Information About Private VLANs

A private VLAN (PVLAN) partitions the Ethernet 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 the following figure). All VLANs in a PVLAN domain share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. The secondary VLANs can either be isolated VLANs or community VLANs. A host on an isolated VLAN can communicate only 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.

Figure 1: Private VLAN Domain



Note You must first create the VLAN before you can convert it to a PVLAN, either primary or secondary.

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.

Private VLAN Ports

The three types of PVLAN 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 that are 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.

  A promiscuous port can be configured as an access port.

- Isolated port—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 PVLAN domain, except that it can communicate with associated promiscuous ports. PVLANs 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.

  An isolated port can be configured an access port.

- 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 from all other interfaces in other communities and from all isolated ports within the PVLAN domain.

  A community port must be configured as an access port.

Primary, Isolated, and Community Private VLANs

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

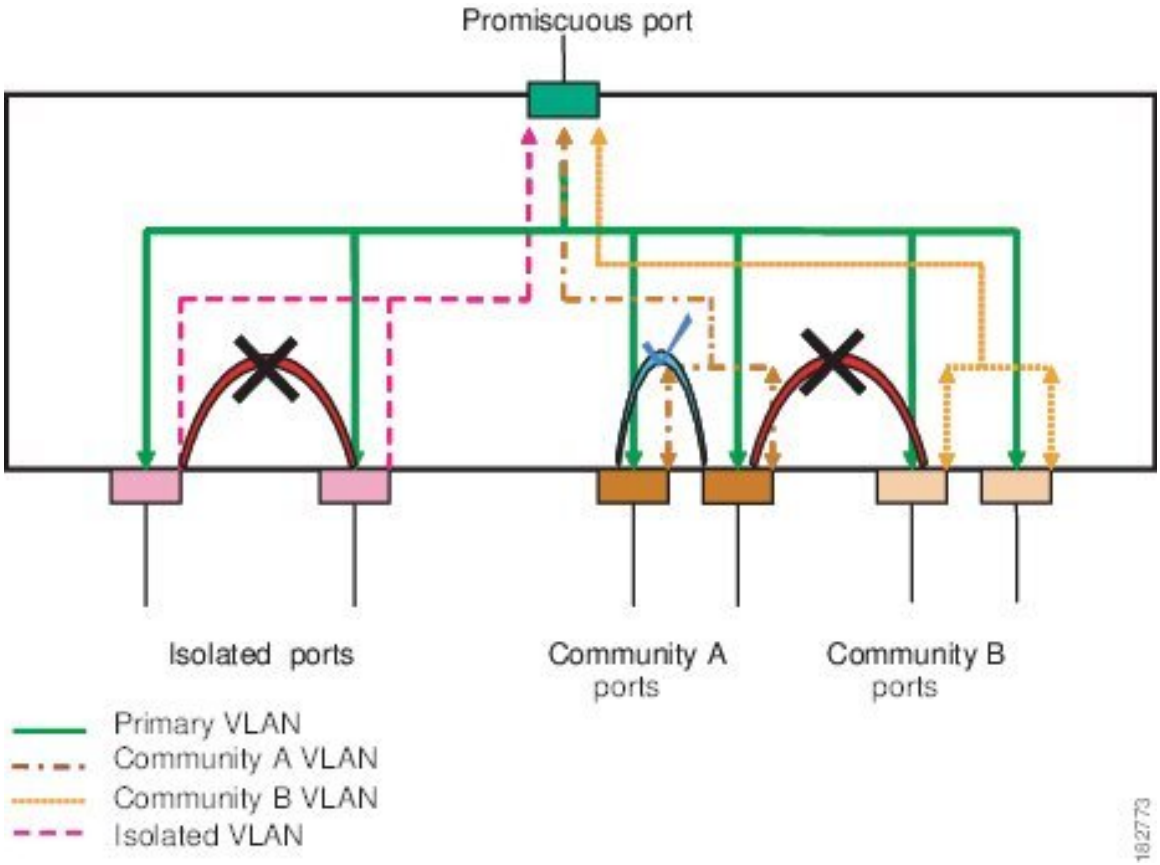
- Primary VLAN— The primary VLAN carries traffic from the promiscuous ports to the host ports, both isolated and community, and to other promiscuous ports.
- Isolated VLAN —An isolated VLAN is a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports. You can configure only one isolated VLAN in a PVLAN

domain. An isolated VLAN can have several isolated ports. 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 PVLAN 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.

The following figure shows the traffic flows within a PVLAN, along with the types of VLANs and types of ports.

Figure 2: Private VLAN Traffic Flows



Note The PVLAN 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 a normal VLAN.

A promiscuous access 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 PVLAN. For example, you can use a promiscuous port to monitor or back up all the PVLAN servers from an administration workstation.

In a switched environment, you can assign an individual PVLAN and associated IP subnet to each individual or common group of end stations. The end stations need to communicate only with a default gateway to communicate outside the private VLAN.

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 VLAN IDs and 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.
- 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 VLAN becomes inactive on the port where the association is configured. 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 PVLAN mode. If you again convert the specified VLAN to PVLAN mode, the original associations are reinstated.

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

Before you begin

Ensure that the PVLAN feature is enabled.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan** *primary-vlan-id*
3. switch(config-vlan)# **private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}
4. (Optional) switch(config-vlan)# **no private-vlan association**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **vlan** *primary-vlan-id*	Enters the number of the primary VLAN that you are working in for the PVLAN configuration.

	Command or Action	Purpose
Step 3	switch(config-vlan)# **private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}	Associates the secondary VLANs with the primary VLAN. Use the **remove** keyword with a *secondary-vlan-list* to clear the association between secondary VLANs and a primary VLAN.
Step 4	(Optional) switch(config-vlan)# **no private-vlan association**	Removes all associations from the primary VLAN and returns it to normal VLAN mode.

Example

This example shows how to associate community VLANs 100 through 110 and isolated VLAN 200 with primary VLAN 5:

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# private-vlan association 100-110, 200
```

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.

Private VLAN Port Isolation

You can use PVLANs 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.

Guidelines and Limitations for Private VLANs

When configuring PVLANs, follow these guidelines:

- You must have already created the VLAN before you can assign the specified VLAN as a private VLAN.
- You must enable PVLANs before the switch can apply the PVLAN functionality.
- IGMP runs only on the primary VLAN and uses the configuration of the primary VLAN for all secondary VLANs.
- Any IGMP join request in the secondary VLAN is treated as if it is received in the primary VLAN.
- You cannot disable PVLANs if the switch has any operational ports in a PVLAN mode.
- Enter the **private-vlan synchronize** command from within the Multiple Spanning Tree (MST) region definition to map the secondary VLANs to the same MST instance as the primary VLAN.
- You cannot connect a second switch to a promiscuous or isolated PVLAN trunk. The promiscuous or isolated PVLAN trunk is supported only on host-switch.

Configuring a Private VLAN

Enabling Private VLANs

You must enable PVLANs on the switch to use the PVLAN functionality.

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

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature private-vlan**
3. (Optional) switch(config)# **no feature private-vlan**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature private-vlan**	Enables the PVLAN feature on the switch.
Step 3	(Optional) switch(config)# **no feature private-vlan**	Disables the PVLAN feature on the switch. **Note** You cannot disable PVLANs if there are operational ports on the switch that are in PVLAN mode.

Example

This example shows how to enable the PVLAN feature on the switch:

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

Enabling IGMP Snooping on Private VLANs

Beginning with Cisco NX-OS Release 10.2(2), you can enable IGMP Snooping on Private VLANs.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **feature private-vlan**	Enables the PVLAN feature on the switch.
Step 2	(Optional) switch(config)# **no system multicast pvlan route-replication**	Enables the IGMP Snooping feature on PVLAN. The no option disables the IGMP Snooping feature.

Example

This example shows how to enable the IGMP Snooping feature on PVLAN:

```
switch# configure terminal
switch(config)# feature private-vlan
switch(config)# system multicast pvlan route-replication
```

Configuring a VLAN as a Private VLAN

To create a PVLAN, you first create a VLAN, and then configure that VLAN to be a PVLAN.

Before you begin

Ensure that the PVLAN feature is enabled.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan** {*vlan-id* | *vlan-range*}
3. switch(config-vlan)# **private-vlan** {**community** | **isolated** | **primary**}
4. (Optional) switch(config-vlan)# **no private-vlan** {**community** | **isolated** | **primary**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global 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 PVLAN. In a PVLAN, you must have one primary

	Command or Action	Purpose
		VLAN. You can have multiple community and isolated VLANs.
Step 4	(Optional) switch(config-vlan)# **no private-vlan** {**community** | **isolated** | **primary**}	Removes the PVLAN 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.

Example

This example shows how to assign VLAN 5 to a PVLAN 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 PVLAN as a community VLAN:

```
switch# configure terminal
switch(config)# vlan 100
switch(config-vlan)# private-vlan community
```

This example shows how to assign VLAN 200 to a PVLAN as an isolated VLAN:

```
switch# configure terminal
switch(config)# vlan 200
switch(config-vlan)# private-vlan isolated
```

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 VLAN IDs and 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.
- 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 VLAN becomes inactive on the port where the association is configured. 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 PVLAN mode. If you again convert the specified VLAN to PVLAN mode, the original associations are reinstated.

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

Before you begin

Ensure that the PVLAN feature is enabled.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan** *primary-vlan-id*
3. switch(config-vlan)# **private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}
4. (Optional) switch(config-vlan)# **no private-vlan association**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **vlan** *primary-vlan-id*	Enters the number of the primary VLAN that you are working in for the PVLAN configuration.
Step 3	switch(config-vlan)# **private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}	Associates the secondary VLANs with the primary VLAN. Use the **remove** keyword with a *secondary-vlan-list* to clear the association between secondary VLANs and a primary VLAN.
Step 4	(Optional) switch(config-vlan)# **no private-vlan association**	Removes all associations from the primary VLAN and returns it to normal VLAN mode.

Example

This example shows how to associate community VLANs 100 through 110 and isolated VLAN 200 with primary VLAN 5:

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# private-vlan association 100-110, 200
```

Configuring an Interface as a Private VLAN Host Port

In PVLANs, host ports are part of the secondary VLANs, which are either community VLANs or isolated VLANs. Configuring a PVLAN host port involves two steps. First, you define the port as a PVLAN host port and then you configure a host association between the primary and secondary VLANs.

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

Before you begin

Ensure that the PVLAN feature is enabled.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type* [*chassis*/]*slot*/*port*
3. switch(config-if)# **switchport mode private-vlan host**
4. switch(config-if)# **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*}
5. (Optional) switch(config-if)# **no switchport private-vlan host-association**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type* [*chassis*/]*slot*/*port*	Selects the port to configure as a PVLAN host port. This port can be on a FEX (identified by the chassis option).
Step 3	switch(config-if)# **switchport mode private-vlan host**	Configures the port as a host port for a PVLAN.
Step 4	switch(config-if)# **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*}	Associates the port with the primary and secondary VLANs of a PVLAN. The secondary VLAN can be either an isolated or community VLAN.
Step 5	(Optional) switch(config-if)# **no switchport private-vlan host-association**	Removes the PVLAN association from the port.

Example

This example shows how to configure Ethernet port 1/12 as a host port for a PVLAN 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
```

Configuring an Interface as a Private VLAN Promiscuous Port

In a PVLAN domain, promiscuous ports are part of the primary VLAN. Configuring a promiscuous port involves two steps. First, you define the port as a promiscuous port and then you configure the mapping between a secondary VLAN and the primary VLAN.

Before you begin

Ensure that the PVLAN feature is enabled.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **switchport mode private-vlan promiscuous**
4. switch(config-if)# **switchport private-vlan mapping** {*primary-vlan-id*} {*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*}
5. (Optional) switch(config-if)# **no switchport private-vlan mapping**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type slot*/*port*	Selects the port to configure as a PVLAN promiscuous port. A physical interface is required. This port cannot be on a FEX.
Step 3	switch(config-if)# **switchport mode private-vlan promiscuous**	Configures the port as a promiscuous port for a PVLAN. You can only enable a physical Ethernet port as the promiscuous port.
Step 4	switch(config-if)# **switchport private-vlan mapping** {*primary-vlan-id*} {*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*}	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.
Step 5	(Optional) switch(config-if)# **no switchport private-vlan mapping**	Clears the mapping from the PVLAN.

Example

This example shows how to configure Ethernet interface 1/4 as a promiscuous port associated with primary VLAN 5 and secondary isolated VLAN 200:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# switchport private-vlan mapping 5 200
```

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

	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 2/11`
	`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:**	Configures the Layer 2 port as an isolated trunk port to carry traffic for multiple isolated VLANs.

	Command or Action	Purpose
	`switch(config-if)# switchport mode private-vlan trunk secondary` `switch(config-if)#`	**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:
	`switch(config-if)# switchport private-vlan association trunk 10 101`
	`switch(config-if)#`
		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 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.

	Command or Action	Purpose

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 secondary
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 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

	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:**	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

	Command or Action	Purpose
	`switch(config-if)# switchport private-vlan trunk allowed vlan add 1` `switch(config-if)#`	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 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 add 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 2 add 3
switch(config-if)# switchport private-vlan mapping trunk 4 add 5
switch(config-if)# switchport private-vlan mapping trunk 1 add 20
switch(config-if)# exit
switch(config)#
```

Mapping Secondary VLANs to the VLAN Interface of a Primary VLAN

Note See the *Cisco Nexus 7000 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 in the correct VDC (or enter the **switchto vdc** command). You can repeat VLAN names and IDs in different VDCs, so you must confirm that you are working in the correct VDC.
- 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. Enter one of the following commands:
4. **exit**
5. (Optional) **show interface vlan** *primary-vlan-id* **private-vlan mapping**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

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

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

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 and places you into the interface configuration mode for the primary VLAN.

Step 3	Enter one of the following commands: **private-vlan mapping** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*} — Maps 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. **no private-vlan mapping** — Clears the mapping to the Layer 3 interface between the secondary VLANs and the primary VLANs. **Example:** `switch(config-if)# private-vlan mapping 100-105, 109`	

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits 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)#
```

Verifying the Private VLAN Configuration

Use the following commands to display PVLAN configuration information.

Command	Purpose
switch# **show feature**	Displays the features enabled on the switch.
switch# **show interface switchport**	Displays information on all interfaces configured as switch ports.
switch# **show vlan private-vlan** [**type**]	Displays the status of the PVLAN.

This example shows how to display the PVLAN configuration:

```
switch# show vlan private-vlan
Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------
5        100        community
5        101        community        Eth1/12, Eth100/1/1
5        102        community
5        110        community
5        200        isolated         Eth1/2
switch# show vlan private-vlan type
Vlan Type
---- -----------------
5    primary
100  community
101  community
102  community
110  community
200  isolated
```

This example shows how to display enabled features (some of the output has been removed for brevity):

```
switch# show feature
Feature Name          Instance  State
--------------------  --------  --------
fcsp                  1         enabled
...
interface-vlan        1         enabled
private-vlan          1         enabled
udld                  1         disabled
```

. . .