



## CHAPTER 4

# Private VLAN Configuration

---

Use this chapter to configure a private VLAN (PVLAN) that divides a normal VLAN into isolated Layer 2 partitions.

The chapter contains the following topics:

- [Information About Private VLANs, page 4-1](#)
- [Configuring a Private VLAN, page 4-5](#)
- [Verifying Private VLAN Configuration, page 4-21](#)
- [Private VLAN Example Configuration, page 4-21](#)
- [Private VLAN Using Port Profiles Example Configuration, page 4-21](#)
- [Default Settings, page 4-25](#)
- [Additional References, page 4-25](#)
- [Feature History for Private VLANs, page 4-26](#)

## Information About Private VLANs

PVLANS achieve device isolation through the use of three separate port designations, each having its own unique set of rules regulating each connected endpoint's ability to communicate with other connected endpoints within the same private VLAN domain.

This section includes the following topics:

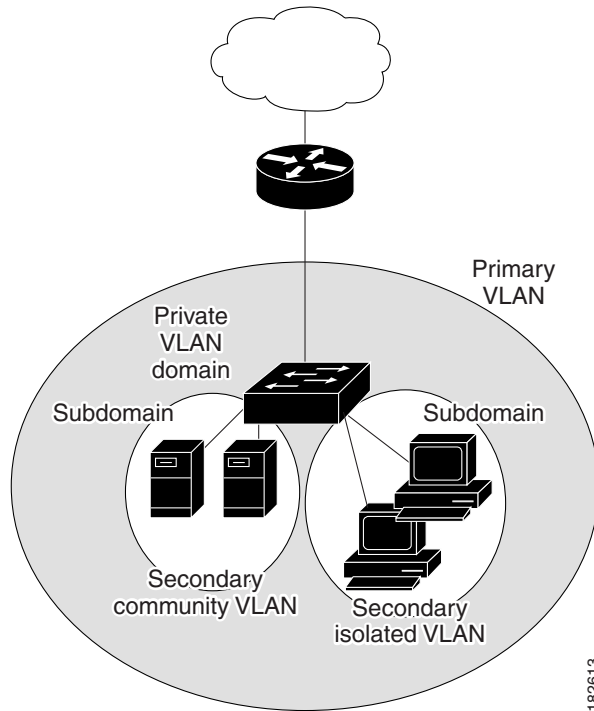
- [Private VLAN Domains, page 4-1](#)
- [Spanning Multiple Switches, page 4-2](#)
- [Private VLAN Ports, page 4-2](#)

## Private VLAN Domains

A private VLAN domain consists of one or more pairs of VLANs. The primary VLAN makes up the domain; and each VLAN pair makes up a subdomain. The VLANs in a pair are called the primary VLAN and the secondary VLAN. All VLAN pairs within a private VLAN have the same primary VLAN. The secondary VLAN ID is what differentiates one subdomain from another (see [Figure 4-1](#)).

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

**Figure 4-1 Private VLAN Domain**



## Spanning Multiple Switches

Private VLANs can span multiple switches, just like regular VLANs. Inter-switch link ports need not be aware of the special VLAN type and carry frames tagged with these VLANs just like they do any other frames. Private VLANs ensure that traffic from an isolated port in one switch does not reach another isolated or community port in a different switch even after traversing an inter-switch link. By embedding the isolation information at the VLAN level and by transporting it along with the packet, it is possible to maintain consistent behavior throughout the network. Therefore, the mechanism which restricts Layer 2 communication between two isolated ports in the same switch, also restricts Layer 2 communication between two isolated ports in two different switches.

## Private VLAN Ports

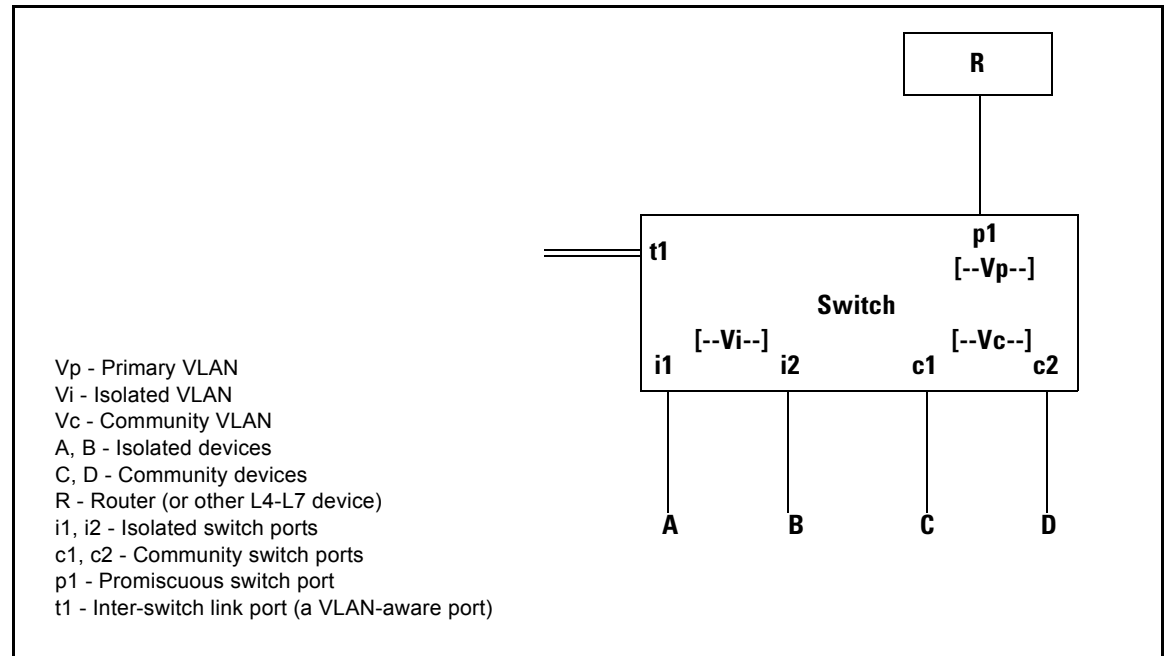
Within a private VLAN domain, there are three separate port designations. Each port designation has its own unique set of rules which regulate the ability of one endpoint to communicate with other connected endpoints within the same private VLAN domain. The following are the three port designations:

- promiscuous
- isolated
- community

Figure 4-2 shows the private VLAN ports

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

**Figure 4-2 Private VLAN Ports**



## Primary VLANs and Promiscuous Ports

The primary VLAN encompasses the entire private VLAN domain. It is a part of each subdomain and provides the Layer 3 gateway out of the VLAN. A private VLAN domain has only one primary VLAN. Every port in a private VLAN domain is a member of the primary VLAN. In other words, the primary VLAN is the entire private VLAN domain.

As the name suggests, a promiscuous port (p1 in Figure 4-2) can talk to all other types of ports. A promiscuous port can talk to isolated ports as well as community ports and vice versa. Layer 3 gateways, DHCP servers and other trusted devices that need to communicate with the customer endpoints are typically connected with a promiscuous port. A promiscuous port can be either an access port or a hybrid/trunk port according to the terminology presented in Annex D of the IEEE 802.1Q specification.

## Secondary VLANs and Host Ports

Secondary VLANs provide Layer 2 isolation between ports in a private VLAN domain. A private VLAN domain can have one or more subdomains. A subdomain is made up of a VLAN pair consisting of the primary VLAN and a secondary VLAN. Since the primary VLAN is a part of every subdomain, secondary VLANs differentiate the VLAN subdomains.

In order to communicate to the Layer 3 interface, a secondary VLAN must be associated with at least one of the promiscuous ports in the primary VLAN. You can associate a secondary VLAN to more than one promiscuous port within the same private VLAN domain, for example, if needed for load-balancing or redundancy. A secondary VLAN that is not associated with any promiscuous port cannot communicate with the Layer 3 interface.

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

A secondary VLAN can be one of the following types:

- **Isolated VLANs**— Isolated VLANs use isolated host ports. An isolated port (i1 or i2 in [Figure 4-2](#)) cannot talk to any other port in that private VLAN domain except for promiscuous ports. If a device needs to have access only to a gateway router, then it should be attached to an isolated port. An isolated port is typically an access port, but in certain applications it can also be a hybrid or trunk port.

The distinct characteristic of an isolated VLAN is that it allows all its ports to have the same degree of segregation that could be obtained from using one separate dedicated VLAN per port. Only two VLAN identifiers are consumed in providing this port isolation.



**Note** While there can be multiple community VLANs in a private VLAN domain, one isolated VLAN is sufficient to serve multiple customers. All endpoints connected to its ports are isolated at Layer 2. Service providers can assign multiple customers to the same isolated VLAN, and be assured that their Layer 2 traffic cannot be sniffed by other customers sharing the same isolated VLAN.

- **Community VLANs**—Community VLANs use community host ports. A community port (c1 or c2 in [Figure 4-2](#)) is part of a group of ports. The ports within a community can have Layer 2 communications with one another and can also talk to any promiscuous port. If an ISP customer has, for example, 4 devices and wants them isolated from those of other customers but still be able to communicate among themselves, then community ports should be used.



**Note**

Because trunks can support a VLAN carrying traffic between its ports, it is possible for VLAN traffic to enter or leave the device through a trunk interface.

## Communication Between Private VLAN Ports

The following table shows how access is permitted or denied between private VLAN port types.

**Table 4-1** Communication Between Private VLAN Ports

	Isolated	Promiscuous	Community 1	Community 2	Interswitch Link Port <sup>1</sup>
Isolated	Deny	Permit	Deny	Deny	Permit
Promiscuous	Permit	Permit	Permit	Permit	Permit
Community 1	Deny	Permit	Permit	Deny	Permit
Community 2	Deny	Permit	Deny	Permit	Permit
Interswitch Link Port	Deny <sup>2</sup>	Permit	Permit	Permit	Permit

1. An interswitch link port is a regular port that connects two switches and that happens to carry two or more VLANs.
2. This behavior applies to traffic traversing inter-switch link ports over an isolated VLAN only. Traffic from an inter-switch link port to an isolated port will be denied if it is in the isolated VLAN. Traffic from an inter-switch link port to an isolated port will be permitted if it is in the primary VLAN.

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

## Configuring a Private VLAN

Use the following procedures in this section to configure a private VLAN.

- [Creating a Private VLAN, page 4-5](#)
- [Configuring a VLAN as a Primary VLAN, page 4-6](#)
- [Configuring a VLAN as a Secondary VLAN, page 4-7](#)
- [Associating the VLANs in a PVLAN, page 4-9](#)
- [Configuring a Private VLAN Host Port, page 4-11](#)
- [Associating a Host Port with a Private VLAN, page 4-12](#)
- [Configuring a Layer 2 Interface as a Promiscuous Trunk Port, page 4-14](#)
- [Configuring a Private VLAN Promiscuous Access Port, page 4-16](#)
- [Associating a Promiscuous Access Port with a Private VLAN, page 4-18](#)
- [Removing a Private VLAN Configuration, page 4-19](#)

## Creating a Private VLAN

Use this procedure to create a private VLAN (PVLAN).

### BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.
- You have identified the VLAN IDs to include in this PVLAN; and they already exist on the switch.



---

**Note** If the VLAN does not already exist, you are prompted to create it. To create a VLAN, see the section, [Creating a VLAN, page 3-3](#).

---

- You have identified which VLAN will be the primary VLAN.
- You have identified which VLANs will be the secondary VLANs and whether they will function as community VLANs or isolated VLANs.

### SUMMARY STEPS

1. **config t**
2. **vlan *primary-vlan-id***
3. **private-vlan primary**
4. **vlan *secondary-vlan-id***
5. **private-vlan {community | isolated}**
6. **vlan *primary-vlan-id***
7. **private-vlan association {add | remove} *secondary vlan-id***
8. **interface *interface name***
9. **switchport mode private-vlan host**

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

10. **switchport private-vlan host-association** *primaryvlan-id secondary vlan-id(s)*
11. **interface** *type slot/port*
12. **switchport mode private-vlan trunk promiscuous**
13. **switchport private-vlan trunk allowed vlan all**
14. **switchport private-vlan mapping trunk** *primary\_vlan\_ID {secondary\_vlan\_list | add secondary\_vlan\_list | remove secondary\_vlan\_list}*
15. **exit**
16. **show vlan private-vlan**
17. **copy running-config startup-config**

## Configuring a VLAN as a Primary VLAN

Use this procedure to configure a VLAN to function as the primary VLAN in a PVLAN.

### BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.
- The VLAN you are configuring as a primary VLAN already exists in the system as a normal VLAN, and you know the VLAN ID.




---

**Note** If the VLAN does not already exist, you are prompted to create it when you create the primary VLAN. To create a VLAN, see the [“Creating a VLAN” procedure on page 3-3](#).

---

- For information about private VLANs, see the [“Private VLANs” section on page 1-6](#).

### SUMMARY STEPS

1. **config t**
2. **vlan** *primary-vlan-id*
3. **private-vlan primary**
4. **exit**
5. **show vlan private-vlan**
6. **copy running-config startup-config**

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

## DETAILED STEPS

	Command	Description
Step 1	<b>config t</b>  <b>Example:</b> n1000v# configure t n1000v(config)#	Places you in CLI Global Configuration mode.
Step 2	<b>vlan primary-vlan-id</b>  <b>Example:</b> n1000v(config)# vlan 202 n1000v(config-vlan)#	Places you into VLAN Configuration mode for the specified VLAN and configures the primary VLAN ID in the running configuration.
Step 3	<b>private-vlan primary</b>  <b>Example:</b> n1000v(config-vlan)# private-vlan primary	Designates the primary VLAN as a private VLAN in the running configuration.
Step 4	<b>exit</b>  <b>Example:</b> n1000v(config-vlan)# exit n1000v(config)#	Exits the VLAN Configuration mode.
Step 5	<b>show vlan private-vlan</b>  <b>Example:</b> n1000v(config)# show vlan private-vlan	(Optional) Displays the PVLAN configuration.
Step 6	<b>copy running-config startup-config</b>  <b>Example:</b> n1000v(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```

Example:
n1000v(config)# vlan 202
n1000v(config-vlan)# private-vlan primary
n1000v(config-vlan)# exit
n1000v(config-vlan)# show vlan private-vlan
Primary  Secondary  Type          Ports
-----  -
202                primary
n1000v(config-vlan)#

```

## Configuring a VLAN as a Secondary VLAN

Use this procedure to configure VLANs to function as secondary VLANs in a PVLAN.

### BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.
- The VLANs you are configuring as secondary VLANs already exists in the system as normal VLANs, and you know their VLAN IDs.

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**



**Note** If the VLAN does not already exist, you are prompted to create it when you create the secondary VLAN. To create a VLAN, see the section, [Creating a VLAN, page 3-3](#).

- You know whether you want the secondary VLANs to be community VLANs or isolated VLANs, and the VLAN IDs for each.
- For information about private VLANs, see the section, [Private VLANs, page 1-6](#).

## SUMMARY STEPS

1. **config t**
2. **vlan *secondary-vlan-id***
3. **private-vlan {community | isolated}**
4. **exit**
5. **show vlan private-vlan**
6. **copy running-config startup-config**

## DETAILED STEPS

	Command	Description
Step 1	<b>config t</b>  <b>Example:</b> n1000v# configure t n1000v(config)#	Places you in CLI Global Configuration mode.
Step 2	<b>vlan <i>secondary-vlan-id</i></b>  <b>Example:</b> n1000v(config)# vlan 303 n1000v(config-vlan)#	Places you in VLAN Configuration mode for the specified VLAN; and configures the secondary VLAN ID in the running configuration.
Step 3	<b>private-vlan {community   isolated}</b>  <b>Example:</b> n1000v(config-vlan)# private-vlan community n1000v(config-vlan)#  <b>Example:</b> n1000v(config-vlan)# private-vlan isolated n1000v(config-vlan)#	Designates the VLAN as either a community or isolated private VLAN in the running configuration.
Step 4	Do one of the following: <ul style="list-style-type: none"> <li>• If you are configuring additional secondary VLANs for your PVLAN, repeat <a href="#">Step 2</a> and <a href="#">Step 3</a>.</li> <li>• Otherwise, continue with <a href="#">Step 5</a>.</li> </ul>	
Step 5	<b>exit</b>  <b>Example:</b> n1000v(config-vlan)# exit n1000v(config)#	Exits the VLAN Configuration mode.



**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

	Command	Description
Step 6	<code>show vlan private-vlan</code>  <b>Example:</b> n1000v(config)# show vlan private-vlan	(Optional) Displays the PVLAN configuration.
Step 7	<code>copy running-config startup-config</code>  <b>Example:</b> n1000v(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```

Example:
n1000v(config)# vlan 303
n1000v(config-vlan)# private-vlan community
n1000v(config-vlan)# exit
n1000v(config)# show vlan private-vlan
Primary  Secondary  Type           Ports
-----  -
202                primary
303                community
n1000v(config)#

```

## Associating the VLANs in a PVLAN

Use this procedure to associate the primary VLANs in a PVLAN with the secondary VLANs.

### BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.
- The primary VLAN for this PVLAN is already configured as a PVLAN.
- The secondary VLANs for this PVLAN are already configured as PVLANs.
- You know the VLAN IDs for each VLAN that is a part of the PVLAN.
- For information about private VLANs, see the [“Private VLANs” section on page 1-6](#).

### SUMMARY STEPS

1. `config t`
2. `vlan primary-vlan-id`
3. `private-vlan association {add | remove} secondary vlan-id`
4. `exit`
5. `show vlan private-vlan`
6. `copy running-config startup-config`

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

## DETAILED STEPS

	Command	Description
Step 1	<code>config t</code>  <b>Example:</b> n1000v# configure t n1000v(config)#	Places you in CLI Global Configuration mode.
Step 2	<code>vlan primary-vlan-id</code>  <b>Example:</b> n1000v(config)# vlan 202 n1000v(config-vlan)#	Places you in VLAN Configuration mode and associates the VLANs to function as a PVLAN in the running configuration.
Step 3	<code>private-vlan association {add   remove} secondary vlan-id</code>  <b>Example:</b> n1000v(config-vlan)# private-vlan association add 303 n1000v(config-vlan)#	Associates a specified secondary VLAN with the primary VLAN to function as a PVLAN in the running configuration.
Step 4	Do one of the following: <ul style="list-style-type: none"> <li>• If you are associating additional secondary VLANs, repeat <a href="#">Step 3</a>.</li> <li>• Otherwise, continue with <a href="#">Step 5</a>.</li> </ul>	
Step 5	<code>exit</code>  <b>Example:</b> n1000v(config-vlan)# exit n1000v(config)#	Exits the VLAN Configuration mode and returns you to CLI Global Configuration mode.
Step 6	<code>show vlan private-vlan</code>  <b>Example:</b> n1000v(config)# show vlan private-vlan	(Optional) Displays the PVLAN configuration.
Step 7	<code>copy running-config startup-config</code>  <b>Example:</b> n1000v(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```

Example:
n1000v(config)# vlan 202
n1000v(config-vlan)# private-vlan association add 303
n1000v(config-vlan)# exit
n1000v(config)# show vlan private-vlan
Primary  Secondary  Type           Ports
-----  -
202      303           community     Veth1
n1000v(config)#

```

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

## Configuring a Private VLAN Host Port

Use this procedure to configure an interface as a host port to function with a PVLAN.

### BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.
- The primary VLAN for this PVLAN is already configured as a PVLAN.
- The secondary VLANs for this PVLAN are already configured as PVLANS.
- The secondary VLANs are already associated with the primary VLAN.
- You know the name of the interface to be used with the PVLAN as a host port.
- For information about private VLANs, see the section, [Private VLANs, page 1-6](#).

### SUMMARY STEPS

1. **config t**
2. **interface** *interface name*
3. **switchport mode private-vlan host**
4. **exit**
5. **show interface** *interface name*
6. **copy running-config startup-config**

### DETAILED STEPS

	Command	Description
Step 1	<b>config t</b>  <b>Example:</b> n1000v# configure t n1000v(config)#	Places you in CLI Global Configuration mode.
Step 2	<b>interface</b> <i>interface name</i>  <b>Example:</b> n1000v(config)# interface veth1 n1000v(config-if)#	Places you in Interface Configuration mode and configures a name for the specified interface in the running configuration.
Step 3	Do one of the following: <ul style="list-style-type: none"> <li>• If you are configuring a physical interface, continue with the next step.</li> <li>• Otherwise, go to <a href="#">Step 4</a>.</li> </ul>	
Step 4	<b>switchport mode private-vlan host</b>  <b>Example:</b> n1000v(config-if)# switchport mode private-vlan host n1000v(config-if)#	Designates that the physical interface is to function as a PVLAN host port in the running configuration.
Step 5	<b>exit</b>  <b>Example:</b> n1000v(config-if)# exit n1000v(config)#	Exits the interface configuration submode and returns you to CLI Global Configuration mode.

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

	Command	Description
Step 6	<b>show interface</b> <i>interface name</i>  <b>Example:</b> n1000v(config)# show interface veth1	(Optional) Displays the interface configuration.
Step 7	<b>copy running-config startup-config</b>  <b>Example:</b> n1000v(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```

Example:
n1000v# config t
n1000v(config)# interface veth1
n1000v(config-if)# switchport mode private-vlan host
n1000v(config-if)# exit
n1000v(config)# show interface veth1
Vethernet1 is up
  Hardware is Virtual, address is 0050.56b0.34c8
  Owner is VM "HAM61-RH5-32bit-ENVM-7.60.1.3"
  Active on module 2, host VISOR-HAM61.localdomain 0
  VMware DVS port 16777215
  Port-Profile is vlan631
  Port mode is Private-vlan host
  Rx
  48600 Input Packets 34419 Unicast Packets
  0 Multicast Packets 14181 Broadcast Packets
  4223732 Bytes
  Tx
  34381 Output Packets 34359 Unicast Packets
  22 Multicast Packets 0 Broadcast Packets 0 Flood Packets
  3368196 Bytes
  5 Input Packet Drops 11 Output Packet Drops

n1000v(config)#

```

## Associating a Host Port with a Private VLAN

Use this procedure to associate the host port with the primary and secondary VLANs in a PVLAN.

### BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.
- You know the VLAN IDs of the primary and secondary VLANs in the PVLAN.
- The primary and secondary VLANs are already configured as PVLAN.
- You know the name of the interface functioning in the PVLAN as a host port.
- For information about private VLANs, see the section, [Private VLANs, page 1-6](#).

### SUMMARY STEPS

1. **config t**
2. **interface** *interface name*
3. **switchport private-vlan host-association** *primaryvlan-id secondary vlan-id(s)*
4. **exit**

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

5. `show interface interface name`
6. `copy running-config startup-config`

## DETAILED STEPS

	Command	Description
Step 1	<code>config t</code>  <b>Example:</b> n1000v# <code>configure t</code> n1000v(config)#	Places you in CLI Global Configuration mode.
Step 2	<code>interface interface name</code>  <b>Example:</b> n1000v(config-if)# <code>interface veth1</code> n1000v(config-if)#	Places you in Interface Configuration mode and configures a name for the specified interface in the running configuration.
Step 3	<code>switchport private-vlan host-association primaryvlan-id secondary vlan-id(s)</code>  <b>Example:</b> n1000v(config-if)# <code>switchport private-vlan host-association 202 303</code> n1000v(config-if)#	Associates the host port with the primary and secondary VLAN IDs for the PVLAN in the running configuration.  The interface is associated with the VLANs in the PVLAN.
Step 4	<code>exit</code>  <b>Example:</b> n1000v(config-if)# <code>exit</code> n1000v(config)#	Exits the interface configuration submode and returns you to CLI Global Configuration mode.
Step 5	<code>show interface interface name</code>  <b>Example:</b> n1000v(config)# <code>show interface veth1</code>	(Optional) Displays the interface configuration.
Step 6	<code>copy running-config startup-config</code>  <b>Example:</b> n1000v# <code>copy running-config startup-config</code>	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```

Example:
n1000v# config t
n1000v(config)# interface veth1
n1000v(config-if)# switchport mode private-vlan host
n1000v(config-if)# exit
n1000v(config)# show interface veth1
Vethernet1 is up
  Hardware is Virtual, address is 0050.56b0.34c8
  Owner is VM "HAM61-RH5-32bit-ENVM-7.60.1.3"
  Active on module 2, host VISOR-HAM61.localdomain 0
  VMware DVS port 16777215
  Port-Profile is vlan631
  Port mode is Private-vlan host
  Rx
  48600 Input Packets 34419 Unicast Packets
  0 Multicast Packets 14181 Broadcast Packets
  4223732 Bytes
  Tx
  34381 Output Packets 34359 Unicast Packets
  22 Multicast Packets 0 Broadcast Packets 0 Flood Packets

```

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

```

3368196 Bytes
5 Input Packet Drops 11 Output Packet Drops

n1000v(config)#

```

## Configuring a Layer 2 Interface as a Promiscuous Trunk Port

Use this procedure to configure a Layer 2 interface as a promiscuous trunk port that does the following:

- Combines multiple promiscuous ports into a single trunk port.
- Carries all normal VLANs.
- Carries multiple PVLAN primary VLANs each with selected secondary VLANs.



### Note

A promiscuous port can be either access or trunk. If you have one primary vlan you can use a promiscuous access port. If you have multiple primary vlans you can use a promiscuous trunk port.

### BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.
- The **private-vlan mapping trunk** command does not decide or override the trunk configuration of a port.
- The port is already configured in a regular trunk mode before adding the private-vlan trunk configurations.
- Primary VLANs must be added to the list of allowed VLAN for the promiscuous trunk port.
- Secondary VLANs are not configured in the allowed VLAN list.
- The trunk port can carry normal VLANs in addition to primary VLANs.

### SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **switchport mode private-vlan trunk promiscuous**
4. **switchport private-vlan trunk allowed vlan all**
5. **switchport private-vlan mapping trunk** *primary\_vlan\_ID* {*secondary\_vlan\_list* | **add** *secondary\_vlan\_list* | **remove** *secondary\_vlan\_list*}
6. **exit**
7. **show interfaces** [*type slot/port*] **switchport**
8. **copy running-config startup-config**

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

## DETAILED STEPS

	Command	Description
Step 1	<b>config t</b>  <b>Example:</b> n1000v# configure t n1000v(config)#	Places you in CLI Global Configuration mode.
Step 2	<b>interface type slot/port</b>  <b>Example:</b> n1000v(config)# interface eth2/6 n1000v(config-if)#	Places you in Interface Configuration mode for the specified interface.
Step 3	<b>switchport mode private-vlan trunk promiscuous</b>  <b>Example:</b> n1000v(config-if)# switchport mode private-vlan trunk promiscuous n1000v(config-if)#	In the running configuration, designates the interface as a promiscuous private-vlan trunk port.
Step 4	<b>switchport private-vlan trunk allowed vlan all</b>  <b>Example:</b> n1000v(config-if)# switchport private-vlan trunk allowed vlan all n1000v(config-if)#	In the running configuration, designates that the private-vlan trunk port will carry all normal VLANs.
Step 5	<b>switchport private-vlan mapping trunk primary_vlan_ID {secondary_vlan_list   add secondary_vlan_list   remove secondary_vlan_list}</b>  <b>Example:</b> n1000v(config-if)# switchport private-vlan mapping trunk 202 303, 440 n1000v(config-if)# switchport private-vlan mapping trunk 210 310, 450	Maps the private-vlan trunk port to a primary VLAN and to selected secondary VLANs in the running configuration.  Multiple private-vlan pairs can be specified so that a promiscuous trunk port can carry multiple primary VLANs.
Step 6	<b>exit</b>	Exits Interface Configuration mode and returns you to CLI Global Configuration mode.
Step 7	<b>show interface [type slot/port] switchport</b>  <b>Example:</b> n1000v(config-if)# show int switchport	Displays the configuration for verification.
Step 8	<b>copy running-config startup-config</b>  <b>Example:</b> n1000v# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

**Example:**  
n1000v# **config t**  
n1000v(config)# **int eth2/6**  
n1000v(config-if)# **switchport mode private-vlan trunk promiscuous**  
n1000v(config-if)# **switchport private-vlan trunk allowed vlan all**  
n1000v(config-if)# **switchport private-vlan mapping trunk 202 303, 440**  
n1000v(config-if)# **switchport private-vlan mapping trunk 210 310, 450**  
n1000v(config-if)# **show int switchport**  
Name: Vethernet1

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

```
Switchport: Enabled
Operational Mode: trunk
Access Mode VLAN: 156(VLAN0156)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1-3967,4048-4093
Administrative private-vlan host-association: not available
Administrative private-vlan mapping: not available
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: not available

n1000v(config-if)#
```

## Configuring a Private VLAN Promiscuous Access Port

Use this procedure to configure a port to be used as a promiscuous access port in a PVLAN.

### BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.
- You know the name of the interface that will function as a promiscuous access port.
- For information about private VLANs, see the section, [Private VLANs, page 1-6](#).

### SUMMARY STEPS

1. **config t**
2. **interface** *type [slot/port | number]*
3. **switchport mode private-vlan promiscuous**
4. **exit**
5. **show interface** *type [slot/port | number]*
6. **copy running-config startup-config**



***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

## DETAILED STEPS

	Command	Description
Step 1	<b>config t</b>  <b>Example:</b> n1000v# <b>configure t</b> n1000v(config)#	Places you in CLI Global Configuration mode.
Step 2	<b>interface type [slot/port / number]</b>  <b>Example:</b> n1000v(config-if)# <b>interface veth1</b> n1000v(config-if)#  <b>Example:</b> n1000v(config-if)# <b>interface eth3/2</b> n1000v(config-if)#	Places you in Interface Configuration mode for a specified interface.
Step 3	<b>switchport mode private-vlan promiscuous</b>  <b>Example:</b> n1000v(config-if)# <b>switchport mode private-vlan promiscuous</b> n1000v(config-if)#	Designates that the interface is to function as a promiscuous access port for a PVLAN in the running configuration.
Step 4	<b>exit</b>  <b>Example:</b> n1000v(config-if)# <b>exit</b> n1000v(config)#	Returns you to Global Configuration mode.
Step 5	<b>show interface type [slot/port / number]</b>  <b>Example:</b> n1000v(config)# <b>show interface eth3/2</b>	(Optional) Displays the interface configuration.
Step 6	<b>copy running-config startup-config</b>  <b>Example:</b> n1000v# <b>copy running-config startup-config</b>	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```

Example:
n1000v# config t
n1000v(config)# interface eth3/2
n1000v(config-if)# switchport mode private-vlan promiscuous
n1000v(config-if)# exit
n1000v(config)# show int eth3/2
Ethernet3/2 is up
  Hardware is Ethernet, address is 0050.5655.2e85 (bia 0050.5655.2e85)
  MTU 1500 bytes, BW -1942729464 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is promiscuous
  full-duplex, 1000 Mb/s
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Rx
  276842 Input Packets 100419 Unicast Packets
  138567 Multicast Packets 37856 Broadcast Packets
  25812138 Bytes
  Tx

```

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

```
128154 Output Packets 100586 Unicast Packets
1023 Multicast Packets 26545 Broadcast Packets 26582 Flood Packets
11630220 Bytes
173005 Input Packet Drops 37 Output Packet Drops
```

```
n1000v(config)#
```

## Associating a Promiscuous Access Port with a Private VLAN

Use this procedure to associate the promiscuous access port with the primary and secondary VLANs in a PVLAN.

### BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.
- You know the VLAN IDs of the primary and secondary VLANs in the PVLAN.
- The primary and secondary VLANs are already configured as PVLAN.
- You know the name of the interface functioning in the PVLAN as a promiscuous access port.
- For information about private VLANs, see the section, [Private VLANs, page 1-6](#).

### SUMMARY STEPS

1. **config t**
2. **interface** *type* [*slot/port* | *number*]
3. **switchport private-vlan mapping** *primary vlan-id secondary vlan-id(s)*
4. **exit**
5. **show interface** *type* [*slot/port* | *number*]
6. **copy running-config startup-config**

### DETAILED STEPS

	Command	Description
Step 1	<b>config t</b>  <b>Example:</b> n1000v# configure t n1000v(config)#	Places you in CLI Global Configuration mode.
Step 2	<b>interface</b> <i>type</i> [ <i>slot/port</i>   <i>number</i> ]  <b>Example:</b> n1000v(config)# interface eth3/2 n1000v(config-if)#	Places you in Interface Configuration mode for the specified interface in the running configuration.

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

	Command	Description
Step 3	<pre>switchport private-vlan mapping primary vlan-id secondary vlan-id(s)  Example: n1000v(config-if)# switchport private-vlan mapping 202 303 n1000v(config-if)#</pre>	Associates the promiscuous access port with the VLAN IDs in the PVLAN in the running configuration.
Step 4	<pre>exit  Example: n1000v(config-if)# exit n1000v(config)#</pre>	Returns you to EXEC mode.
Step 5	<pre>show interface type [slot/port   number]  Example: n1000v(config)# show vlan private-vlan</pre>	(Optional) Displays the interface configuration.
Step 6	<pre>copy running-config startup-config  Example: n1000v# copy running-config startup-config</pre>	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```
Example:
n1000v(config)# int eth3/2
n1000v(config-if)# switchport private-vlan mapping 202 303
n1000v(config-if)# exit

n1000v(config)# show vlan private-vlan
Primary Secondary Type Ports
-----
202 303 community Eth3/2, Veth1
n1000v(config)#
```

## Removing a Private VLAN Configuration

Use this procedure to remove a private VLAN configuration and return the VLAN to normal VLAN mode.

### BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.
- The VLAN is configured as a private VLAN, and you know the VLAN ID.
- When you remove a PVLAN configuration, the ports associated with it become inactive.
- For information about private VLANs, see the section, [Private VLANs, page 1-6](#).

### SUMMARY STEPS

1. `config t`
2. `vlan private vlan-id`
3. `no private-vlan {community | isolated | primary}`
4. `exit`

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

5. `show vlan private-vlan`
6. `copy running-config startup-config`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code>  <b>Example:</b> n1000v# <code>configure t</code> n1000v(config)#	Places you in CLI Global Configuration mode.
Step 2	<code>vlan private vlan-id</code>  <b>Example:</b> n1000v(config)# <code>vlan 5</code> n1000v(config-vlan)#	Places you in the VLAN configuration mode for the specified VLAN.
Step 3	<code>no private-vlan {community   isolated   primary}</code>  <b>Example:</b> n1000v(config-vlan)# <code>no private-vlan primary</code> n1000v(config-vlan)#	Removes the specified VLAN from a PVLAN in the running configuration.  The private VLAN configuration is removed from the specified VLAN(s). The VLAN is returned to normal VLAN mode. The ports associated with the VLAN are inactive.
Step 4	<code>exit</code>  <b>Example:</b> n1000v(config-vlan)# <code>exit</code> n1000v(config)#	Exits the VLAN configuration submode.
Step 5	<code>show vlan private-vlan</code>	(Optional) Displays the PVLAN configuration.
Step 6	<code>copy running-config startup-config</code>  <b>Example:</b> n1000v# <code>copy running-config startup-config</code>	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```

Example:
n1000v# configure t
n1000v(config)# vlan 5
n1000v(config-vlan)# no private-vlan primary
n1000v(config-vlan)# exit
n1000v(config)# show vlan private-vlan
Primary  Secondary  Type                Ports
-----  -
n1000v(config)#

```

*Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).*

## Verifying Private VLAN Configuration

Use the following commands to display configuration information about private VLANs.

Command	Purpose
<code>show running-config vlan &lt;vlan-id&gt;</code>	Displays VLAN information.
<code>show vlan private-vlan [type]</code>	Displays information about private VLANs
<code>show interface private-vlan mapping</code>	Displays interface private VLAN information.
<code>show interface switchport</code>	Displays information about all interfaces configured as switchports.

## Private VLAN Example Configuration

The following example shows how to configure interface Ethernet 2/6 as the following:

- private VLAN trunk port
- mapped to primary private VLAN 202 which is associated with secondary VLANs 303 and 440
- mapped to primary private VLAN 210 which is associated with secondary VLANs 310 and 450

**Example:**

```
n1000v# config t
n1000v(config)# int eth2/6
n1000v(config-if)# switchport mode private-vlan trunk promiscuous
n1000v(config-if)# switchport private-vlan trunk allowed vlan all
n1000v(config-if)# switchport private-vlan mapping trunk 202 303, 440
n1000v(config-if)# switchport private-vlan mapping trunk 210 310, 450
n1000v(config-if)# show int switchport
Name: Vethernet1
  Switchport: Enabled
  Operational Mode: trunk
  Access Mode VLAN: 156(VLAN0156)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan host-association: not available
  Administrative private-vlan mapping: not available
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: not available

n1000v(config-if)#
```

## Private VLAN Using Port Profiles Example Configuration

The following is a sample configuration showing interface eth2/6 using port-profile, uppvlanpromtrunk156.

In this configuration, packets from secondary interfaces 153, 154, and 155 are translated into the primary VLAN 156 as a result of the command, `switchport private-vlan mapping trunk 156 153-155`.

**Example:**

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

```

vlan 153-154
  private-vlan community
vlan 155
  private-vlan isolated
vlan 156
  private-vlan association 153-155,157-158
  private-vlan primary
vlan 157
  private-vlan community
vlan 158
  private-vlan isolated

n1000v# show run int eth2/6
version 4.0(1)

interface Ethernet2/6
  switchport
  inherit port-profile uppvlanpromtrunk156

n1000v# show port-profile name uppvlanpromtrunk156
port-profile uppvlanpromtrunk156
description:
status: enabled
capability privileged: no
capability uplink: yes
port-group: uppvlanpromtrunk156
config attributes:
  switchport mode private-vlan trunk promiscuous
  switchport private-vlan trunk allowed vlan all
  switchport private-vlan mapping trunk 156 153-155
  no shutdown
evaluated config attributes:
  switchport mode trunk
  switchport trunk allowed vlan all
  switchport private-vlan mapping trunk 156 153-155
  no shutdown
assigned interfaces:
  Ethernet2/6
  Ethernet3/3

n1000v# show int
mgmt0 is up
  Hardware is GigabitEthernet, address is 0000.0000.0000 (bia 0050.56b8.6790)
  Internet Address is 172.28.15.94/24
  MTU 1500 bytes, BW 0 Kbit, DLY 0 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  full-duplex, 1000 Mb/s
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  61570 packets input, 15391960 bytes
  0 multicast frames, 0 compressed
  0 input errors, 0 frame, 0 overrun, 0 fifo
  4062 packets output, 967297 bytes
  0 underrun, 0 output errors, 0 collisions
  0 fifo, 0 carrier errors

Ethernet2/2 is up
  Hardware is Ethernet, address is 0050.565e.4c39 (bia 0050.565e.4c39)
  MTU 1500 bytes, BW 1826767368 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA

```

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

```
Port mode is trunk
full-duplex, 1000 Mb/s
Beacon is turned off
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
Rx
681251 Input Packets 161488 Unicast Packets
365259 Multicast Packets 154504 Broadcast Packets
54980953 Bytes
Tx
176537 Output Packets 172242 Unicast Packets
4100 Multicast Packets 195 Broadcast Packets 5 Flood Packets
19753822 Bytes
98004 Input Packet Drops 9 Output Packet Drops

Ethernet2/6 is up
Hardware is Ethernet, address is 0050.565b.b9db (bia 0050.565b.b9db)
MTU 1500 bytes, BW 1689405960 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
Port mode is trunk
full-duplex, 1000 Mb/s
Beacon is turned off
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
Rx
702 Input Packets 0 Unicast Packets
702 Multicast Packets 0 Broadcast Packets
46133 Bytes
Tx
95 Output Packets 0 Unicast Packets
95 Multicast Packets 0 Broadcast Packets 0 Flood Packets
6487 Bytes
44 Input Packet Drops 10 Output Packet Drops

Ethernet3/2 is up
Hardware is Ethernet, address is 0050.5653.98ac (bia 0050.5653.98ac)
MTU 1500 bytes, BW 348735240 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
Port mode is access
full-duplex, 1000 Mb/s
Beacon is turned off
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
Rx
579977 Input Packets 138070 Unicast Packets
308931 Multicast Packets 132976 Broadcast Packets
45973630 Bytes
Tx
165416 Output Packets 163449 Unicast Packets
1830 Multicast Packets 137 Broadcast Packets 3 Flood Packets
22602711 Bytes
1975345 Input Packet Drops 0 Output Packet Drops

n1000v# show port-profile name upvlanpromtrunk156
port-profile upvlanpromtrunk156
description:
status: enabled
capability privileged: no
capability uplink: yes
port-group: upvlanpromtrunk156
config attributes:
    switchport mode private-vlan trunk promiscuous
```

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

```

switchport private-vlan trunk allowed vlan all
switchport private-vlan mapping trunk 156 153-155
no shutdown
evaluated config attributes:
switchport mode trunk
switchport trunk allowed vlan all
switchport private-vlan mapping trunk 156 153-155
no shutdown
assigned interfaces:
Ethernet2/6
Ethernet3/3

n1000v# show port-profile expand-interface

port-profile uplinkportprofile1
Ethernet2/2
switchport mode private-vlan trunk promiscuous
switchport private-vlan trunk allowed vlan all
switchport trunk allowed vlan 150-152
no shutdown

port-profile upaccess152

port-profile upvlanpromaccess156
Ethernet3/2
switchport mode private-vlan promiscuous
switchport private-vlan mapping 156 153-155
no shutdown

port-profile pvlancomm154
Vethernet49
switchport mode private-vlan host
switchport private-vlan host-association 156 154
no shutdown
Vethernet81
switchport mode private-vlan host
switchport private-vlan host-association 156 154
no shutdown

port-profile pvlaniso155

port-profile pvlancomm157
n1000v# show port-profile expand-interface ?
<CR>
> Redirect it to a file
name Select a port profile by name
| Pipe command output to filter

n1000v# show port-profile expand-interface name upvlanpromtrunk156

port-profile upvlanpromtrunk156
Ethernet2/6
switchport mode trunk
switchport trunk allowed vlan 1-3967,4048-4093
switchport private-vlan mapping trunk 156 153-155
no shutdown
Ethernet3/3
switchport trunk allowed vlan 1-3967,4048-4093
n1000v# show int eth2/6
Ethernet2/6 is up
Hardware is Ethernet, address is 0050.565b.b9db (bia 0050.565b.b9db)
MTU 1500 bytes, BW 1689405960 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA

```



**[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)**

```

Port mode is trunk
full-duplex, 1000 Mb/s
Beacon is turned off
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
Rx
953 Input Packets 0 Unicast Packets
953 Multicast Packets 0 Broadcast Packets
62600 Bytes
Tx
96 Output Packets 0 Unicast Packets
96 Multicast Packets 0 Broadcast Packets 0 Flood Packets
6683 Bytes
44 Input Packet Drops 10 Output Packet Drops

```

## Default Settings

Table 4-2 lists the default setting for private VLANs.

**Table 4-2** Default Private VLAN Setting

Parameters	Default
Private VLANs	Disabled

## Additional References

For additional information related to implementing private VLANs, see the following sections:

- [Related Documents, page 4-25](#)
- [Standards, page 4-26](#)

## Related Documents

Related Topic	Document or Chapter Title
VLANs	<a href="#">Chapter 3, “VLAN Configuration”</a>
Layer 2 MAC addresses	<a href="#">Chapter 2, “MAC Address Table”</a>
Port Profiles	<i>Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(1)</i>
VLAN interfaces, IP addressing	<i>Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(1)</i>
Static MAC addresses, security	<i>Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(1)</i>
CLI configuration basics	<i>Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(1)</i>
System management	<i>Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(1)</i>

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

Related Topic	Document or Chapter Title
Release notes	<i>Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(1)</i>
Layer 2 commands	<i>Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(1)</i>

## 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.	—

## Feature History for Private VLANs

This section provides the private VLAN release history.

Feature Name	Releases	Feature Information
Private VLANs	4.0(4)SV1(1)	This feature was introduced.