CHAPTER 13

Configuring Private VLANs

This chapter describes how to configure private VLANs on the Cisco ME 3400E Ethernet Access switch.

Note For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

The chapter consists of these sections:

Understanding Private VLANs

The private-VLAN feature addresses two problems that service providers face when using VLANs:

- Scalability: The switch supports up to 1005 active VLANs. If a service provider assigns one VLAN per customer, this limits the numbers of customers that the service provider can support.
- To enable IP routing, each VLAN is assigned a subnet address space or a block of addresses, which can waste the unused IP addresses and cause IP address management problems.

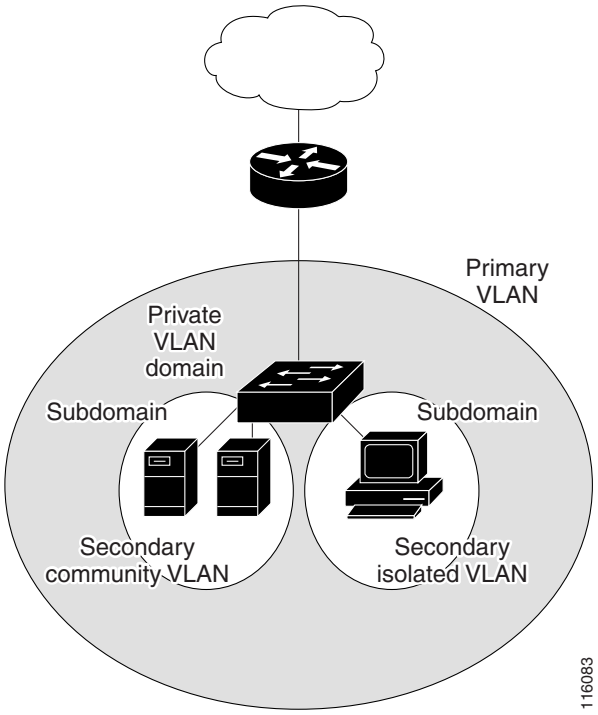
Using private VLANs addresses the scalability problem and provides IP address management benefits for service providers and Layer 2 security for customers.

These sections describe how private VLANs work:

Types of Private VLANs and Private-VLAN Ports

Private VLANs partition a regular VLAN domain into subdomains. A subdomain is represented by a pair of VLANs: a *primary* VLAN and a *secondary* VLAN. A private VLAN can have multiple VLAN pairs, one pair for each subdomain. All VLAN pairs in a private VLAN share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. See Figure 13-1.

Figure 13-1 Private-VLAN Domain



There are two types of secondary VLANs:

- 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 communities at the Layer 2 level. A community VLAN can include a combination of no more than eight user network interfaces (UNIs) and enhanced network interfaces (ENIs).

Private VLANs provide Layer 2 isolation between ports within the same private VLAN. Private-VLAN ports are access ports that are one of these types:

- Promiscuous—A promiscuous port belongs to the primary VLAN and can communicate with all interfaces, including the community and isolated host ports that belong to the secondary VLANs associated with the primary VLAN.

Note Promiscuous ports must be network node interfaces (NNIs). UNIs or ENIs cannot be configured as promiscuous ports.

- Isolated—An isolated port is a host port that belongs to an isolated secondary VLAN. It has complete Layer 2 separation from other ports within the same private VLAN, except for the 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.
- Community—A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities and from isolated ports within their private VLAN. No more than eight UNIs and ENIs can be community ports in the same community VLAN.

Note Trunk ports carry traffic from regular VLANs and also from primary, isolated, and community VLANs.

Primary and secondary VLANs have these characteristics:

- Primary VLAN—A private VLAN has only one primary VLAN. Every port in a private VLAN is a member of the primary VLAN. The primary VLAN carries unidirectional traffic downstream from the promiscuous ports to the (isolated and community) host ports and to other promiscuous ports.
- Isolated VLAN —A private VLAN has only one isolated VLAN. An isolated VLAN is a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports and the gateway.
- 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. Each community VLAN can include a combination of no more than eight UNIs and ENIs.

Note The switch also supports UNI-ENI isolated VLANs and UNI-ENI community VLANs. When a VLAN is created, it is by default a UNI-ENI isolated VLAN. Traffic is not switched among UNIs and ENIs on a switch that belong to a UNI-ENI isolated VLAN. For more information on UNI-ENI VLANs, see Chapter 12, “Configuring VLANs.”

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs. Layer 3 gateways are typically connected to the switch 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.

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.

You can use private VLANs to control access to end stations in these ways:

- 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 NNIs 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.

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 use of the VLANs configured as private VLANs, configure private VLANs on all intermediate devices, including devices that have no private-VLAN ports.

IP Addressing Scheme with Private VLANs

Assigning a separate VLAN to each customer creates an inefficient IP addressing scheme:

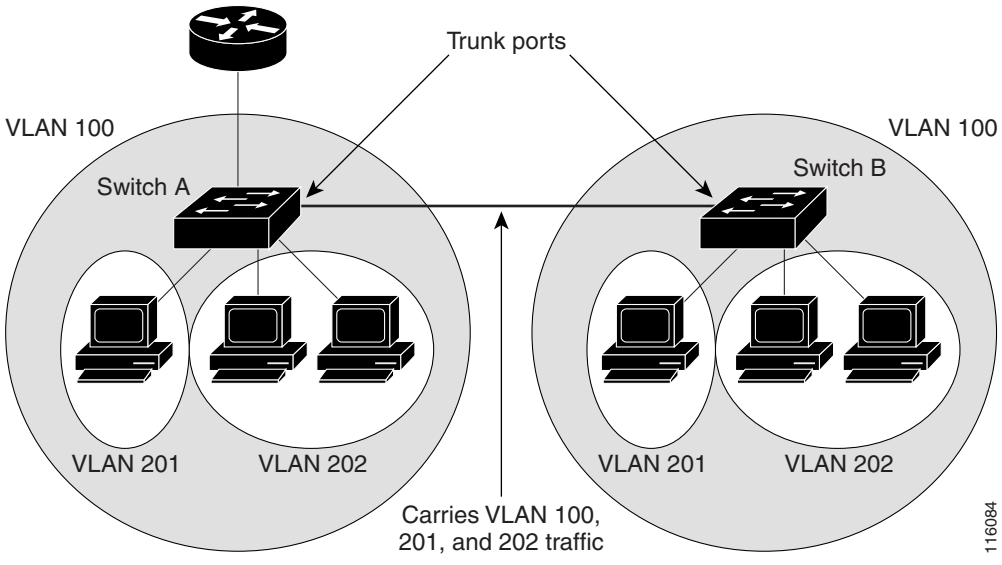
- Assigning a block of addresses to a customer VLAN can result in unused IP addresses.
- If the number of devices in the VLAN increases, the number of assigned address might not be large enough to accommodate them.

These problems are reduced by using private VLANs, where all members in the private VLAN share a common address space, which is allocated to the primary VLAN. Hosts are connected to secondary VLANs, and the DHCP server assigns them IP addresses from the block of addresses allocated to the primary VLAN. Subsequent IP addresses can be assigned to customer devices in different secondary VLANs, but in the same primary VLAN. When new devices are added, the DHCP server assigns them the next available address from a large pool of subnet addresses.

Private VLANs across Multiple Switches

As with regular VLANs, private VLANs can span multiple switches. A trunk port carries the primary VLAN and secondary VLANs to a neighboring switch. The trunk port treats the private VLAN as any other VLAN. A feature of private VLANs across multiple switches is that traffic from an isolated port in switch A does not reach an isolated port on Switch B. See Figure 13-2.

Figure 13-2 Private VLANs across Switches



VLAN 100 = Primary VLAN
VLAN 201 = Secondary isolated VLAN
VLAN 202 = Secondary community VLAN

You must manually configure private VLANs on all switches in the Layer 2 network. If you do not configure the primary and secondary VLAN associations in some switches in the network, the Layer 2 databases in these switches are not merged. This can result in unnecessary flooding of private-VLAN traffic on those switches.

Private VLANs and Unicast, Broadcast, and Multicast Traffic

In regular VLANs, devices in the same VLAN can communicate with each other at the Layer 2 level, but devices connected to interfaces in different VLANs must communicate at the Layer 3 level. In private VLANs, the promiscuous ports are members of the primary VLAN, while the host ports belong to secondary VLANs. Because the secondary VLAN is associated to the primary VLAN, members of the these VLANs can communicate with each other at the Layer 2 level.

In a regular VLAN, broadcasts are forwarded to all ports in that VLAN. Private-VLAN broadcast forwarding depends on the port sending the broadcast:

- An isolated port sends a broadcast only to the promiscuous ports or trunk ports.
- A community port sends a broadcast to all promiscuous ports, trunk ports, and ports in the same community VLAN.
- A promiscuous port (only NNI) sends a broadcast to all ports in the private VLAN (other promiscuous ports, trunk ports, isolated ports, and community ports).

Multicast traffic is routed or bridged across private-VLAN boundaries and within a single community VLAN. Multicast traffic is not forwarded between ports in the same isolated VLAN or between ports in different secondary VLANs.

Private VLANs and SVIs

In a Layer 3 switch (a switch running the metro IP access image), a switch virtual interface (SVI) represents the Layer 3 interface of a VLAN. Layer 3 devices communicate with a private VLAN only through the primary VLAN and not through secondary VLANs. Configure Layer 3 VLAN interfaces only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

- If you try to configure a VLAN with an active SVI as a secondary VLAN, the configuration is not allowed until you disable the SVI.
- If you try to create an SVI on a VLAN that is configured as a secondary VLAN and the secondary VLAN is already mapped at Layer 3, the SVI is not created, and an error is returned. If the SVI is not mapped at Layer 3, the SVI is created, but it is automatically shut down.

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

Configuring Private VLANs

Tasks for Configuring Private VLANs

To configure a private VLAN, follow these steps:

Step 1 Create the primary and secondary VLANs and associate them. See the "Configuring and Associating VLANs in a Private VLAN" section on page 13-10.

Note If the VLAN is not created already, the private-VLAN configuration process creates it.

Step 2 Configure interfaces to be isolated or community host ports, and assign VLAN membership to the host port. See the "Configuring a Layer 2 Interface as a Private-VLAN Host Port" section on page 13-11.

Step 3 Configure NNIs as promiscuous ports, and map the promiscuous ports to the primary-secondary VLAN pair. See the "Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port" section on page 13-13.

Step 4 If inter-VLAN routing will be used, configure the primary SVI, and map secondary VLANs to the primary. See the "Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface" section on page 13-14.

Step 5 Verify private-VLAN configuration.

Default Private-VLAN Configuration

No private VLANs are configured. Newly created VLANs are UNI-ENI isolated VLANs.

Private-VLAN Configuration Guidelines

Guidelines for configuring private VLANs fall into these categories:

Secondary and Primary VLAN Configuration

Follow these guidelines when configuring private VLANs:

- You use VLAN configuration mode to configure private VLANs. For more information about VLAN configuration, see the "Creating and Modifying VLANs" section on page 12-7.
- You must configure private VLANs on each device where you want private-VLAN ports.
- A private VLAN cannot be a UNI-ENI VLAN.
  - To change a UNI-ENI isolated VLAN (the default) to a private VLAN, enter the **private-vlan** VLAN configuration command; this overwrites the default isolated VLAN configuration.
  - To change a UNI-ENI community VLAN to a private VLAN, you must first enter the **no uni-vlan** VLAN configuration command to return to the default UNI isolated VLAN configuration.
- You cannot configure VLAN 1 or VLANs 1002 to 1005 as primary or secondary VLANs. Extended VLANs (VLAN IDs 1006 to 4094) can belong to private VLANs
- A primary VLAN can have one isolated VLAN and multiple community VLANs associated with it. An isolated or community VLAN can have only one primary VLAN associated with it.
- Although a private VLAN contains more than one VLAN, only one Spanning Tree Protocol (STP) instance runs for the entire private VLAN. When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN are propagated to the secondary VLAN.
- You can enable DHCP snooping on private VLANs. When you enable DHCP snooping on the primary VLAN, it is propagated to the secondary VLANs. If you configure DHCP on a secondary VLAN, the configuration does not take effect if the primary VLAN is already configured.
- If you enable IP source guard on private-VLAN ports, you must enable DHCP snooping on the primary VLAN.
- You can apply different quality of service (QoS) configurations to primary, isolated, and community VLANs.
- When the switch is running the metro IP access image and you configure private VLANs, sticky Address Resolution Protocol (ARP) is enabled by default, and ARP entries learned on Layer 3 private VLAN interfaces are sticky ARP entries. For security reasons, private VLAN port sticky ARP entries do not age out.

  Note We recommend that you display and verify private-VLAN interface ARP entries.

  Connecting a device with a different MAC address but with the same IP address displays a message and the ARP entry is not created. Because the private-VLAN port sticky ARP entries do not age out, you must manually remove private-VLAN port ARP entries if a MAC address changes.
  - You can remove a private-VLAN ARP entry by using the **no arp** *ip-address* global configuration command.
  - You can add a private-VLAN ARP entry by using the **arp** ip-*address hardware-address* **type** global configuration command.
- You can configure VLAN maps on primary and secondary VLANs (see the "Configuring VLAN Maps" section on page 32-29). However, we recommend that you configure the same VLAN maps on private-VLAN primary and secondary VLANs.

- When a frame is forwarded through Layer 2 within a private VLAN, the same VLAN map is applied at the receiving and sending sides. When a frame is routed from inside a private VLAN to an external port, the private-VLAN map is applied at the receiving side.
  - For frames going upstream from a host port to a promiscuous port, the VLAN map configured on the secondary VLAN is applied.
  - For frames going downstream from a promiscuous port to a host port, the VLAN map configured on the primary VLAN is applied.

  To filter out specific IP traffic for a private VLAN, you should apply the VLAN map to both the primary and secondary VLANs.
- If the switch is running the metro IP access image, you can apply router ACLs only on the primary-VLAN SVIs. The ACL is applied to both primary and secondary VLAN Layer 3 traffic.
- Although private VLANs provide host isolation at Layer 2, hosts can communicate with each other at Layer 3.
- Private VLANs support these Switched Port Analyzer (SPAN) features:
  - You can configure a private-VLAN port as a SPAN source port.
  - You can use VLAN-based SPAN (VSPAN) on primary, isolated, and community VLANs or use SPAN on only one VLAN to separately monitor sent or received traffic.

Private-VLAN Port Configuration

Follow these guidelines when configuring private-VLAN ports:

- Promiscuous ports must be NNIs; UNIs and ENIs cannot be configured as promiscuous ports.
- Use only the private-VLAN configuration commands to assign ports to primary, isolated, or community VLANs. Layer 2 access ports assigned to the VLANs that you configure as primary, isolated, or community VLANs are inactive while the VLAN is part of the private-VLAN configuration. Layer 2 trunk interfaces remain in the STP forwarding state.
- Do not configure NNI ports that belong to a Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP) EtherChannel as private-VLAN ports. While a port is part of the private-VLAN configuration, any EtherChannel configuration for it is inactive.
- Enable Port Fast and BPDU guard on NNI isolated and community host ports to prevent STP loops due to misconfigurations and to speed up STP convergence (see Chapter 17, “Configuring Optional Spanning-Tree Features”). When enabled, STP applies the BPDU guard feature to all Port Fast-configured Layer 2 LAN ports. Do not enable Port Fast and BPDU guard on promiscuous ports.
- If you delete a VLAN used in the private-VLAN configuration, the private-VLAN ports associated with the VLAN become inactive.
- Private-VLAN ports can be on different network devices if the devices are trunk-connected and the primary and secondary VLANs have not been removed from the trunk.
- A community private VLAN can include no more than eight UNIs and ENIs. If you try to add more than eight, the configuration is not allowed. If you try to configure a VLAN that includes a combination of more than eight UNIs and ENIs as a community private VLAN, the configuration is not allowed.

Limitations with Other Features

When configuring private VLANs, remember these limitations with other features:

Note In some cases, the configuration is accepted with no error messages, but the commands have no effect.

- When IGMP snooping is enabled on the switch (the default), the switch supports no more than 20 private-VLAN domains.
- A private VLAN cannot be a UNI-ENI isolated or UNI-ENI community VLAN. For more information about UNI-ENI VLANs, see Chapter 12, "Configuring VLANs."
- Do not configure a remote SPAN (RSPAN) VLAN as a private-VLAN primary or secondary VLAN. For more information about SPAN, see Chapter 27, "Configuring SPAN and RSPAN."
- Do not configure private-VLAN ports on interfaces configured for these other features:
  - dynamic-access port VLAN membership
  - PAgP (only NNIs or ENIs)
  - LACP (only NNIs or ENIs)
  - Multicast VLAN Registration (MVR)
- You can configure 802.1x port-based authentication on a private-VLAN port, but do not configure IEEE 802.1x with port security on private-VLAN ports.
- A private-VLAN host or promiscuous port cannot be a SPAN destination port. If you configure a SPAN destination port as a private-VLAN port, the port becomes inactive.
- If you configure a static MAC address on a promiscuous port in the primary VLAN, you must add the same static address to all associated secondary VLANs. If you configure a static MAC address on a host port in a secondary VLAN, you must add the same static MAC address to the associated primary VLAN. When you delete a static MAC address from a private-VLAN port, you must remove all instances of the configured MAC address from the private VLAN.

  Note Dynamic MAC addresses learned in one VLAN of a private VLAN are replicated in the associated VLANs. For example, a MAC address learned in a secondary VLAN is replicated in the primary VLAN. When the original dynamic MAC address is deleted or aged out, the replicated addresses are removed from the MAC address table.

- Configure Layer 3 VLAN interfaces only for primary VLANs.

Configuring and Associating VLANs in a Private VLAN

Beginning in privileged EXEC mode, follow these steps to configure a private VLAN:

Note The **private-vlan** commands do not take effect until you exit VLAN configuration mode.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	Enter VLAN configuration mode and designate or create a VLAN that will be the primary VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094. **Note** If the VLAN has been configured as a UNI-ENI community VLAN, you must enter the **no uni-vlan** VLAN configuration command before configuring a private VLAN.
Step 3	**private-vlan primary**	Designate the VLAN as the primary VLAN.
Step 4	**exit**	Return to global configuration mode.
Step 5	**vlan** *vlan-id*	(Optional) Enter VLAN configuration mode and designate or create a VLAN that will be an isolated VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.
Step 6	**private-vlan isolated**	Designate the VLAN as an isolated VLAN.
Step 7	**exit**	Return to global configuration mode.
Step 8	**vlan** *vlan-id*	(Optional) Enter VLAN configuration mode and designate or create a VLAN that will be a community VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094. **Note** If the VLAN has been configured as a UNI-ENI community VLAN, you must enter the **no uni-vlan** VLAN configuration command before configuring a private VLAN.
Step 9	**private-vlan community**	Designate the VLAN as a community VLAN.
Step 10	**exit**	Return to global configuration mode.
Step 11	**vlan** *vlan-id*	Enter VLAN configuration mode for the primary VLAN designated in Step 3.
Step 12	**private-vlan association** [**add** | **remove**] *secondary_vlan_list*	Associate the secondary VLANs with the primary VLAN.
Step 13	**end**	Return to privileged EXEC mode.
Step 14	**show vlan private-vlan** [**type**] or **show interfaces status**	Verify the configuration.
Step 15	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

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

- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.

- The *secondary_vlan_list* parameter can contain multiple community VLAN IDs but only one isolated VLAN ID.
- Enter a *secondary_vlan_list,* or use the **add** keyword with a *secondary_vlan_list* to associate secondary VLANs with a primary VLAN.
- Use the **remove** keyword with a *secondary_vlan_list* to clear the association between secondary VLANs and a primary VLAN.
- The **private-vlan association** VLAN configuration command does not take effect until you exit VLAN configuration mode.

This example shows how to configure VLAN 20 as a primary VLAN, VLAN 501 as an isolated VLAN, and VLANs 502 and 503 as community VLANs, to associate them in a private VLAN, and to verify the configuration. It assumes that VLANs 502 and 503 have previously been configured as UNI-ENI community VLANs:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# no-uni vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# no-uni vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
Switch(config)# show vlan private vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
20      501       isolated
20      502       community
20      503       community
20      504       non-operational
```

Configuring a Layer 2 Interface as a Private-VLAN Host Port

Beginning in privileged EXEC mode, follow these steps to configure a Layer 2 interface as a private-VLAN host port and to associate it with primary and secondary VLANs:

Note Isolated and community VLANs are both secondary VLANs.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode for the Layer 2 interface to be configured.

	Command	Purpose
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport mode private-vlan host**	Configure the Layer 2 port as a private-VLAN host port.
Step 5	**switchport private-vlan host-association** *primary_vlan_id secondary_vlan_id*	Associate the Layer 2 port with a private VLAN.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces** [*interface-id*] **switchport**	Verify the configuration.
Step 8	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

This example shows how to configure an interface as a private-VLAN host port, associate it with a private-VLAN pair, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/22
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
Switch# show interfaces fastethernet0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Administrative private-vlan host-association: 20 501
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 501
<output truncated>
```

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

You can configure only NNIs as promiscuous ports. Beginning in privileged EXEC mode, follow these steps to configure a Layer 2 interface as a private-VLAN promiscuous port and map it to primary and secondary VLANs:

Note Isolated and community VLANs are both secondary VLANs.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode for the Layer 2 interface to be configured. The interface must be an NNI. **Note** If the interface is a UNI or ENI, you must enter the **port-type nni** interface configuration command before configuring it as a promiscuous port.
Step 3	**switchport mode private-vlan promiscuous**	Configure the Layer 2 NNI port as a private-VLAN promiscuous port.
Step 4	**switchport private-vlan mapping** *primary_vlan_id* {**add** | **remove**} *secondary_vlan_list*	Map the private-VLAN promiscuous port to a primary VLAN and to selected secondary VLANs.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interfaces** [*interface-id*] **switchport**	Verify the configuration.
Step 7	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

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

- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
- Enter a *secondary_vlan_list*, or use the **add** keyword with a *secondary_vlan_list* to map the secondary VLANs to the private-VLAN promiscuous port.
- Use the **remove** keyword with a *secondary_vlan_list* to clear the mapping between secondary VLANs and the private-VLAN promiscuous port.

This example shows how to configure an NNI as a private-VLAN promiscuous port and map it to a private VLAN. The interface is a member of primary VLAN 20 and secondary VLANs 501 to 503 are mapped to it.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

Use the **show vlan private-vlan** or the **show interface status** privileged EXEC command to display primary and secondary VLANs and private-VLAN ports on the switch.

Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface

If the switch is running the metro IP access image and the private VLAN will be used for inter-VLAN routing, you configure an SVI for the primary VLAN and map secondary VLANs to the SVI.

Note Isolated and community VLANs are both secondary VLANs.

Beginning in privileged EXEC mode, follow these steps to map secondary VLANs to the SVI of a primary VLAN to allow Layer 3 switching of private-VLAN traffic:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface vlan** *primary_vlan_id*	Enter interface configuration mode for the primary VLAN, and configure the VLAN as an SVI. The VLAN ID range is 2 to 1001 and 1006 to 4094.
Step 3	**private-vlan mapping** [**add** | **remove**] *secondary_vlan_list*	Map the secondary VLANs to the Layer 3 VLAN interface of a primary VLAN to allow Layer 3 switching of private-VLAN incoming traffic.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interface private-vlan mapping**	Verify the configuration.
Step 6	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

Note The **private-vlan mapping** interface configuration command only affects private-VLAN traffic that is switched through Layer 3.

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

- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
- Enter a *secondary_vlan_list,* or use the **add** keyword with a *secondary_vlan_list* to map the secondary VLANs to the primary VLAN.
- Use the **remove** keyword with a *secondary_vlan_list* to clear the mapping between secondary VLANs and the primary VLAN.

This example shows how to map the interfaces of VLANs 501 and 502 to primary VLAN 10, which permits routing of secondary VLAN incoming traffic from private VLANs 501 to 502:

```
Switch# configure terminal
Switch(config)# interface vlan 10
Switch(config-if)# private-vlan mapping 501-502
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan10    501            isolated
vlan10    502            community
```

Monitoring Private VLANs

Table 13-1 shows the privileged EXEC commands for monitoring private-VLAN activity.

Table 13-1 Private VLAN Monitoring Commands

Command	Purpose
show interfaces status	Displays the status of interfaces, including the VLANs to which they belong.
show vlan private-vlan [**type**]	Display the private-VLAN information for the switch.
show interface switchport	Display the private-VLAN configuration on interfaces.
show interface private-vlan mapping	Display information about the private-VLAN mapping for VLAN interfaces.

This is an example of the output from the **show vlan private-vlan** command:

```
Switch(config)# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Fa0/1, Gi0/1, Gi0/2
10      502       community         Fa0/11, Fa0/12, Gi0/1
10      503       non-operational
```