Configuring Private VLANs

- Finding Feature Information, on page 1
- Prerequisites for Private VLANs, on page 1
- Restrictions for Private VLANs, on page 1
- Information About Private VLANs, on page 2
- How to Configure Private VLANs, on page 11
- Monitoring Private VLANs, on page 21
- Configuration Examples for Private VLANs, on page 21
- Where to Go Next, on page 23
- Additional References, on page 24

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Private VLANs

Private vlans are supported in transparent mode for VTP 1, 2 and 3. Private VLANS are also supported on server mode with VTP 3.

When configuring private VLANs on the device, always use the default Switch Database Management (SDM) template to balance system resources between unicast routes and Layer 2 entries. If another SDM template is configured, use the `sdm prefer default` global configuration command to set the default template.

Restrictions for Private VLANs

- Do not configure fallback bridging on devices with private VLANs.
• Do not configure a remote SPAN (RSPAN) VLAN as a private-VLAN primary or secondary VLAN.

• Do not configure private-VLAN ports on interfaces configured for these other features:
  • Dynamic-access port VLAN membership
  • Dynamic Trunking Protocol (DTP)
  • IPv6 Security Group (SG)
  • Port Aggregation Protocol (PAgP)
  • Link Aggregation Control Protocol (LACP)
  • Multicast VLAN Registration (MVR)
  • Voice VLAN
  • Web Cache Communication Protocol (WCCP)

• You can configure IEEE 802.1x port-based authentication on a private-VLAN port, but do not configure 802.1x with port security, voice VLAN, or per-user ACL 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 need not add the same static address to all associated secondary VLANs. Similarly, if you configure a static MAC address on a host port in a secondary VLAN, you need not add the same static MAC address to the associated primary VLAN. Also, when you delete a static MAC address from a private-VLAN port, you do not have to remove all instances of the configured MAC address from the private VLAN.

**Note**

Dynamic MAC addresses learned in Secondary VLAN of a private VLAN are replicated to the Primary VLANs. All mac entries are learnt on secondary VLANs, even if the traffic ingresses from primary VLAN. If a mac-address is dynamically learnt in the primary VLAN it will not get replicated in the associated secondary VLANs.

• Configure Layer 3 VLAN interfaces (SVIs) only for primary VLANs.

---

**Information About Private VLANs**

**Private VLAN Domains**

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

• When running the IP Base or IP Services image, the device supports up to 4094 active VLANs. If a service provider assigns one VLAN per customer, this limits the numbers of customers the service provider can support.
• To enable IP routing, each VLAN is assigned a subnet address space or a block of addresses, which can result in wasting the unused IP addresses, and cause IP address management problems.

Figure 1: Private VLAN Domain

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

Secondary VLANs

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.

Related Topics

Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface, on page 19
Example: Mapping Secondary VLANs to a Primary VLAN Interface, on page 23

Private VLANs Ports

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.
• 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.

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.

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs. Layer 3 gateways are typically connected to the device through a promiscuous port. With a promiscuous port, you can connect a wide range of devices as access points to a private VLAN. For example, you can use a promiscuous port to monitor or back up all the private VLAN servers from an administration workstation.

Related Topics
Configuring a Layer 2 Interface as a Private VLAN Host Port, on page 15
Configuring a Layer 2 Interface as a Private VLAN Promiscuous Port, on page 17
Example: Configuring an Interface as a Host Port, on page 22
Example: Configuring an Interface as a Private VLAN Promiscuous Port, on page 22

Private VLANs in Networks

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 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.
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 Devices**

*Figure 2: Private VLANs Across Switches*

As with regular VLANs, private VLANs can span multiple devices. A trunk port carries the primary VLAN and secondary VLANs to a neighboring device. The trunk port treats the private VLAN as any other VLAN. A feature of private VLANs across multiple devices is that traffic from an isolated port in Device A does not reach an isolated port on Device B.

Private VLANs are supported in transparent mode for VTP 1, 2 and 3. Private vlan is also supported on server mode for VTP 3. If we have a server client setup using VTP 3, private vlans configured on the server should be reflected on the client.
Private-VLAN Interaction with Other Features

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 theses 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 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 VLAN multicast forwarding supports the following:

- Sender can be outside the VLAN and the Receivers can be inside the VLAN domain.
- Sender can be inside the VLAN and the Receivers can be outside the VLAN domain.
- Sender and Receiver can both be in the same community VLAN.

Private VLANs and SVIs

In a Layer 3 device, a device 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 (SVIs) 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.
Private VLANs and Device Stacks

Private VLANs can operate within the device stack, and private-VLAN ports can reside on different stack members. However, the following changes to the stack can impact private-VLAN operation:

• If a stack contains only one private-VLAN promiscuous port and the stack member that contains that port is removed from the stack, host ports in that private VLAN lose connectivity outside the private VLAN.

• If a stack master stack that contains the only private-VLAN promiscuous port in the stack fails or leaves the stack and a new stack master is elected, host ports in a private VLAN that had its promiscuous port on the old stack master lose connectivity outside of the private VLAN.

• If two stacks merge, private VLANs on the winning stack are not affected, but private-VLAN configuration on the losing device is lost when that device reboots.

Private VLAN with Dynamic Mac Address

The Mac addresses learnt in the secondary VLAN are replicated to the primary VLAN and not vice-versa. This saves the hardware l2 cam space. The primary VLAN is always used for forwarding lookups in both directions.

Dynamic MAC addresses learned in Primary VLAN of a private VLAN are then, if required, replicated in the secondary VLANs. For example, if a mac-address is dynamically received on the secondary VLAN, it will be learnt as part of primary VLAN. In case of isolated VLANs, a blocked entry for the same mac will be added to secondary VLAN in the mac address table. So, mac learnt on host ports in secondary domain are installed as blocked type entries. All mac entries are learnt on secondary VLANs, even if the traffic ingress from primary VLAN.

However, if a mac-address is dynamically learnt in the primary VLAN it will not get replicated in the associated secondary VLANS.

Private VLAN with Static Mac Address

Users are not required to replicate the Static Mac Address CLI for private VLAN hosts as compare to legacy model.

Example:

• In the legacy model, if the user configures a static mac address, they need to add same mac static mac-address in the associated VLAN too. For example, if mac-address A is user configured on port 1/0/1 in VLAN 101, where VLAN 101 is a secondary VLAN and VLAN 100 is a primary VLAN, then the user has to configure

  \texttt{mac-address static A vlan 101 interface G1/0/1}
  \texttt{mac-address static A vlan 100 interface G1/0/1}

• In this device, the user does not need to replicate the mac address to the associated VLAN. For the above example, user has to configure only

  \texttt{mac-address static A vlan 101 interface G1/0/1}

Private VLAN Interaction with VACL/QOS

Private VLANs are bidirectional in case of this device, as compared to “Unidirectional” in other platforms.
After layer-2 forward lookup, proper egress VLAN mapping happens and all the egress VLAN based feature processing happens in the egress VLAN context.

When a frame in Layer-2 is forwarded within a private VLAN, the VLAN map is applied at the ingress side and at the egress side. When a frame is routed from inside a private VLAN to an external port, the private-VLAN map is applied at the ingress side. Similarly, when the frame is routed from an external port to a Private VLAN, the private-VLAN is applied at the egress side. This is applicable to both bridged and routed traffic.

**Bridging:**

- For upstream traffic from secondary VLAN to primary VLAN, the MAP of the secondary VLAN is applied on the ingress side and the MAP of the primary VLAN is applied on the egress side.
- For downstream traffic from primary VLAN to secondary VLAN, the MAP of the primary VLAN is applied in the ingress direction and the MAP of the secondary VLAN is applied in the egress direction.

**Routing**

If we have two private VLAN domains - PV1 (sec1, prim1) and PV2 (sec2, prim2). For frames routed from PV1 to PV2:

- The MAP of sec1 and L3 ACL of prim1 is applied in the ingress port.
- The MAP of sec2 and L3 ACL of prim2 is applied in the egress port.

For packets going upstream or downstream from isolated host port to promiscuous port, the isolated VLAN’s VACL is applied in the ingress direction and primary VLAN’s VACL is applied in the egress direction. This allows user to configure different VACL for different secondary VLAN in a same primary VLAN domain.

---

**Note**

2-way community VLAN is now not required as the private VLANS on this device are always bi-directional.

---

**Private VLANs and HA Support**

PVLAN will work seamlessly with High Availability (HA) feature. The Private VLAN existing on the master before switchover should be the same after switchover (new master should have similar PVLAN configuration both on IOS side and FED side as that of the old master).

**Private-VLAN Configuration Guidelines**

**Default Private-VLAN Configurations**

No private VLANs are configured.

**Secondary and Primary VLAN Configuration**

Follow these guidelines when configuring private VLANs:

- Private VLANs are supported in transparent mode for VTP 1, 2 and 3. If the device is running VTP version 1 or 2, you must set VTP to transparent mode. After you configure a private VLAN, you should not change the VTP mode to client or server. VTP version 3 supports private VLANs in all modes.
• With VTP version 1 or 2, after you have configured private VLANs, use the `copy running-config startup config` privileged EXEC command to save the VTP transparent mode configuration and private-VLAN configuration in the device startup configuration file. Otherwise, if the device resets, it defaults to VTP server mode, which does not support private VLANs. VTP version 3 does support private VLANs.

• VTP version 1 and 2 do not propagate private-VLAN configuration. You must configure private VLANs on each device where you want private-VLAN ports unless the devices are running VTP version 3, as VTP3 propagate private vlans.

• 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.

• When copying a PVLAN configuration from a ftp server and applying it on a running-config, the PVLAN association will not be formed. You will need to check and ensure that the primary VLAN is associated to all the secondary VLANs.

You can also use `configure replace flash:config_file force` instead of `copy flash:config_file running-config`.

• 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.

• When you enable IP source guard on private-VLAN ports, you must enable DHCP snooping on the primary VLAN.

• We recommend that you prune the private VLANs from the trunks on devices that carry no traffic in the private VLANs.

• You can apply different quality of service (QoS) configurations to primary, isolated, and community VLANs.

• Note the following considerations for sticky ARP:
  • Sticky ARP entries are those learned on SVIs and Layer 3 interfaces. These entries do not age out.
  • The `ip sticky-arp` global configuration command is supported only on SVIs belonging to private VLANs.
  • The `ip sticky-arp` interface configuration command is only supported on:
    • Layer 3 interfaces
    • SVIs belonging to normal VLANs
    • SVIs belonging to private VLANs

For more information about using the `ip sticky-arp global` configuration and the `ip sticky-arp interface` configuration commands, see the command reference for this release.
Private VLAN Port Configuration

Follow these guidelines when configuring private VLAN 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 ports that belong to a PAgP or 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 isolated and community host ports to prevent STP loops due to misconfigurations and to speed up STP convergence. 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.

How to Configure Private VLANs

Configuring Private VLANs

To configure a private VLAN, perform these steps:

Note
Private vlans are supported in transparent mode for VTP 1, 2 and 3. Private VLANS are also supported on server mode with VTP 3.

SUMMARY STEPS

1. Set VTP mode to transparent.
2. Create the primary and secondary VLANs and associate them.
3. Configure interfaces to be isolated or community host ports, and assign VLAN membership to the host port.
4. Configure interfaces as promiscuous ports, and map the promiscuous ports to the primary-secondary VLAN pair.
5. If inter-VLAN routing will be used, configure the primary SVI, and map secondary VLANs to the primary.
6. Verify private-VLAN configuration.

DETAILED STEPS

Step 1
Set VTP mode to transparent.

Note
Note: For VTP3, you can set mode to either server or transparent mode.

Step 2
Create the primary and secondary VLANs and associate them.

See the Configuring and Associating VLANs in a Private VLAN, on page 12

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

Step 3
Configure interfaces to be isolated or community host ports, and assign VLAN membership to the host port.
Configuring and Associating VLANs in a Private VLAN

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

To configure and associate VLANs in a Private VLAN, perform these steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `vtp mode transparent`
4. `vlan vlan-id`
5. `private-vlan primary`
6. `exit`
7. `vlan vlan-id`
8. `private-vlan isolated`
9. `exit`
10. `vlan vlan-id`
11. `private-vlan community`
12. `exit`
13. `vlan vlan-id`
14. `private-vlan community`
15. `exit`
16. `vlan vlan-id`
17. `private-vlan association [add | remove] secondary_vlan_list`
18. `end`
19. `show vlan private-vlan [type]` or `show interfaces status`
20. `copy running-config startup config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

See the Configuring a Layer 2 Interface as a Private VLAN Host Port, on page 15

**Step 4** Configure interfaces 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, on page 17

**Step 5** 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, on page 19

**Step 6** Verify private-VLAN configuration.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device&gt; enable</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vtp mode transparent</td>
<td>Sets VTP mode to transparent (disable VTP).</td>
</tr>
<tr>
<td>Example:</td>
<td>Note: For VTP3, you can set mode to either server or transparent mode.</td>
</tr>
<tr>
<td>Device(config)# vtp mode transport</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> vlan vlan-id</td>
<td>Enters VLAN configuration mode and designates or creates a VLAN that will be the primary VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# vlan 20</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> private-vlan primary</td>
<td>Designates the VLAN as the primary VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-vlan)# private-vlan primary</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-vlan)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> vlan vlan-id</td>
<td>(Optional) Enters VLAN configuration mode and designates or creates a VLAN that will be an isolated VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# vlan 501</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> private-vlan isolated</td>
<td>Designates the VLAN as an isolated VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-vlan)# private-vlan isolated</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-vlan)# exit</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Device(config-vlan)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>(Optional) Enters VLAN configuration mode and designates or creates a VLAN that will be a community VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# vlan 502</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Designates the VLAN as a community VLAN.</td>
</tr>
<tr>
<td>private-vlan community</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-vlan)# private-vlan community</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-vlan)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>(Optional) Enters VLAN configuration mode and designates or creates a VLAN that will be a community VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# vlan 503</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>Designates the VLAN as a community VLAN.</td>
</tr>
<tr>
<td>private-vlan community</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-vlan)# private-vlan community</td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-vlan)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td>Enters VLAN configuration mode for the primary VLAN designated in Step 4.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# vlan 20</td>
<td></td>
</tr>
<tr>
<td><strong>Step 17</strong></td>
<td>Associates the secondary VLANs with the primary VLAN. It can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.</td>
</tr>
<tr>
<td>private-vlan association [add</td>
<td>remove] secondary_vlan_list</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| Device(config-vlan)# private-vlan association 501–503 | • 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 command does not take effect until you exit VLAN configuration mode. |

**Step 18**  
**Example:**  
Device(config)# end  
Returns to privileged EXEC mode.

**Step 19**  
**Example:**  
Device# show vlan private-vlan  
Verifies the configuration.

**Step 20**  
**Example:**  
Device# copy running-config startup-config  
Saves your entries in the device startup configuration file.

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

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.
### SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. switchport mode private-vlan host
5. switchport private-vlan host-association primary_vlan_id secondary_vlan_id
6. end
7. show interfaces [interface-id] switchport
8. copy running-config startup-config

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
<td>Enters interface configuration mode for the Layer 2 interface to be configured.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# interface gigabitethernet1/0/22</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>switchport mode private-vlan host</td>
<td>Configures the Layer 2 port as a private-VLAN host port.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# switchport mode private-vlan host</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>switchport private-vlan host-association primary_vlan_id secondary_vlan_id</td>
<td>Associates the Layer 2 port with a private VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# switchport private-vlan host-association 20 501</td>
<td><strong>Note</strong> This is a required step to associate the PVLAN to a Layer 2 interface.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Private VLANs

**Purpose**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config)# end</code></td>
<td>Verifies the configuration.</td>
</tr>
</tbody>
</table>

**Step 7**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces [interface-id] switchport</code></td>
<td>Verifies the configuration.</td>
</tr>
</tbody>
</table>

**Example:**

```
Device# show interfaces gigabitethernet1/0/22 switchport
```

**Step 8**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**Example:**

```
Device# copy running-config startup-config
```

**Related Topics**

- [Private VLANs Ports](#), on page 3
- [Example: Configuring an Interface as a Host Port](#), on page 22
- [Example: Configuring an Interface as a Private VLAN Promiscuous Port](#), on page 22

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

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.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `switchport mode private-vlan promiscuous`
5. `switchport private-vlan mapping primary_vlan_id {add | remove} secondary_vlan_list`
6. `end`
7. `show interfaces [interface-id] switchport`
8. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
</tbody>
</table>

**Example:**

```
Device# enable
```
### Configuring a Layer 2 Interface as a Private VLAN Promiscuous Port

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

configure terminal

*Example:*

Device# configure terminal

**Step 3**

interface interface-id

*Example:*

Device(config)# interface gigabitethernet1/0/2

**Step 4**

switchport mode private-vlan promiscuous

*Example:*

Device(config-if)# switchport mode private-vlan promiscuous

**Step 5**

switchport private-vlan mapping primary_vlan_id {add | remove} secondary_vlan_list

*Example:*

Device(config-if)# switchport private-vlan mapping 20 add 501-503

- 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.

**Step 6**

end

*Example:*

Device(config)# end

**Step 7**

show interfaces [interface-id] switchport

*Example:*

Device# show interfaces gigabitethernet1/0/2 switchport

Verifies the configuration.
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 8 copy running-config startup config</td>
<td>Saves your entries in the device startup configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

- Private VLANs Ports, on page 3
- Example: Configuring an Interface as a Host Port, on page 22
- Example: Configuring an Interface as a Private VLAN Promiscuous Port, on page 22

### Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface

If 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.

Follow these steps to map secondary VLANs to the SVI of a primary VLAN to allow Layer 3 switching of private VLAN traffic:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface vlan primary_vlan_id`
4. `private-vlan mapping [add | remove] secondary_vlan_list`
5. `end`
6. `show interface private-vlan mapping`
7. `copy running-config startup config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<p>| Step 2 configure terminal    | Enters the global configuration mode.             |
| Example:                     |                                                   |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# configure terminal</td>
<td>Enters interface configuration mode for the primary VLAN, and configures the VLAN as an SVI. The VLAN ID range is 2 to 1001 and 1006 to 4094.</td>
</tr>
</tbody>
</table>

**Step 3**  
**interface vlan primary_vlan_id**  
**Example:**  
Device(config)# interface vlan 20

**Step 4**  
**private-vlan mapping [add | remove] secondary_vlan_list**  
**Example:**  
Device(config-if)# private-vlan mapping 501-503

Maps the secondary VLANs to the Layer 3 VLAN interface of a primary VLAN to allow Layer 3 switching of private VLAN ingress traffic.  

**Note**  
The **private-vlan mapping** interface configuration command only affects private VLAN traffic that is Layer 3 switched.  
- 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 a primary VLAN.  
- Use the **remove** keyword with a **secondary_vlan_list** to clear the mapping between secondary VLANs and a primary VLAN.

**Step 5**  
**end**  
**Example:**  
Device(config)# end

Returns to privileged EXEC mode.

**Step 6**  
**show interface private-vlan mapping**  
**Example:**  
Device# show interfaces private-vlan mapping

Verifies the configuration.

**Step 7**  
**copy running-config startup config**  
**Example:**  
Device# copy running-config startup-config

Saves your entries in the device startup configuration file.

**Related Topics**  
VTP Domain
Monitoring Private VLANs

The following table displays the commands used to monitor private VLANs.

**Table 1: Private VLAN Monitoring Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces status</code></td>
<td>Displays the status of interfaces, including the VLANs to which they belong.</td>
</tr>
<tr>
<td><code>show vlan private-vlan [type]</code></td>
<td>Displays the private VLAN information for the Device or Device stack.</td>
</tr>
<tr>
<td><code>show interface switchport</code></td>
<td>Displays private VLAN configuration on interfaces.</td>
</tr>
<tr>
<td><code>show interface private-vlan mapping</code></td>
<td>Displays information about the private VLAN mapping for VLAN SVIs.</td>
</tr>
<tr>
<td><code>show platform vlan pvlan</code></td>
<td>Displays PVLAN information on FED side</td>
</tr>
<tr>
<td><code>show platform vlan pvlan hardware</code></td>
<td>Displays all the hardware resources held by PVLANs on FED side</td>
</tr>
</tbody>
</table>

Configuration Examples for Private VLANs

**Example: Configuring and Associating VLANs in a Private VLAN**

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:

```
Device# configure terminal
Device(config)# vlan 20
Device(config-vlan)# private-vlan primary
Device(config-vlan)# exit
Device(config)# vlan 501
Device(config-vlan)# private-vlan isolated
Device(config-vlan)# exit
Device(config)# vlan 502
Device(config-vlan)# private-vlan community
Device(config-vlan)# exit
Device(config)# vlan 503
Device(config-vlan)# private-vlan community
Device(config-vlan)# exit
Device(config)# vlan 20
Device(config-vlan)# private-vlan association 501-503
Device(config-vlan)# end
```
### Example: Configuring an Interface as a Host Port

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:

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/22
Device(config-if)# switchport mode private-vlan host
Device(config-if)# switchport private-vlan host-association 20 501
Device(config-if)# end
Device# show interfaces gigabitethernet1/0/22 switchport
```

### Related Topics
- Private VLANs Ports, on page 3
- Configuring a Layer 2 Interface as a Private VLAN Host Port, on page 15
- Configuring a Layer 2 Interface as a Private VLAN Promiscuous Port, on page 17

### Example: Configuring an Interface as a Private VLAN Promiscuous Port

This example shows how to configure an interface 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.

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport mode private-vlan promiscuous
```
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 Device.

**Related Topics**
- Private VLANs Ports, on page 3
- Configuring a Layer 2 Interface as a Private VLAN Host Port, on page 15
- Configuring a Layer 2 Interface as a Private VLAN Promiscuous Port, on page 17

**Example: Mapping Secondary VLANs to a Primary VLAN Interface**

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

```
Device(config-if)# switchport private-vlan mapping 20 add 501-503
Device(config-if)# end
```

```
Device(config)# configure terminal
Device(config)# interface vlan 20
Device(config-if)# private-vlan mapping 501-503
Device(config-if)# end
Device(config)# show interfaces private-vlan mapping
```

```
Interface Secondary VLAN Type
---------- -------------- -----------------
vlan20 501 isolated
vlan20 502 community
vlan20 503 community
```

**Related Topics**
- VTP Domain
- Secondary VLANs, on page 3
- Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface, on page 19

**Example: Monitoring Private VLANs**

This example shows output from the `show vlan private-vlan` command:

```
Device(config)# show vlan private-vlan
```

```
Primary Secondary Type Ports
---------- ------------- ----------------- ------------------------------------------
20 501 isolated   Gi1/0/22, Gi1/0/2
20 502 community  Gi1/0/2
20 503 community  Gi1/0/2
```

**Where to Go Next**

You can configure the following:

- VTP
- VLANs
- VLAN trunking
- VLAN Membership Policy Server (VMPS)
- Voice VLANs

## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI commands</td>
<td>LAN Switching Command Reference, Cisco IOS Release</td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1573</td>
<td></td>
</tr>
<tr>
<td>RFC 1757</td>
<td></td>
</tr>
<tr>
<td>RFC 2021</td>
<td></td>
</tr>
</tbody>
</table>
### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>• BRIDGE-MIB (RFC1493)</td>
<td></td>
</tr>
<tr>
<td>• CISCO-BRIDGE-EXT-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-CDP-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-PAGP-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-PRIVATE-VLAN-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-LAG-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-L2L3-INTERFACE-CONFIG-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-MAC-NOTIFICATION-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-STP-EXTENSIONS-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-VLAN-MEMBERSHIP-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-VTP-MIB</td>
<td></td>
</tr>
<tr>
<td>• IEEE8023-LAG-MIB</td>
<td></td>
</tr>
<tr>
<td>• IF-MIB (RFC 1573)</td>
<td></td>
</tr>
<tr>
<td>• RMON-MIB (RFC 1757)</td>
<td></td>
</tr>
<tr>
<td>• RMON2-MIB (RFC 2021)</td>
<td></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>