Configure Isolated Private VLANs on Catalyst Switches

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

- Rules and Limitations

Configure

- Network Diagram
- Configure the Primary and Isolated VLANs
- Assign Ports to the PVLANs
- Layer 3 Configuration
- Configurations
- Private VLANs Across Multiple Switches
  - Regular Trunks
  - Private VLAN Trunks
  - Additional Information

Verify

- CatOS
- Cisco IOS Software
- Verification Procedure

Troubleshoot

- Troubleshoot PVLANs
  - Problem 1
  - Problem 2
  - Problem 3
  - Problem 4
  - Problem 5
  - Problem 6

Related Information

Introduction

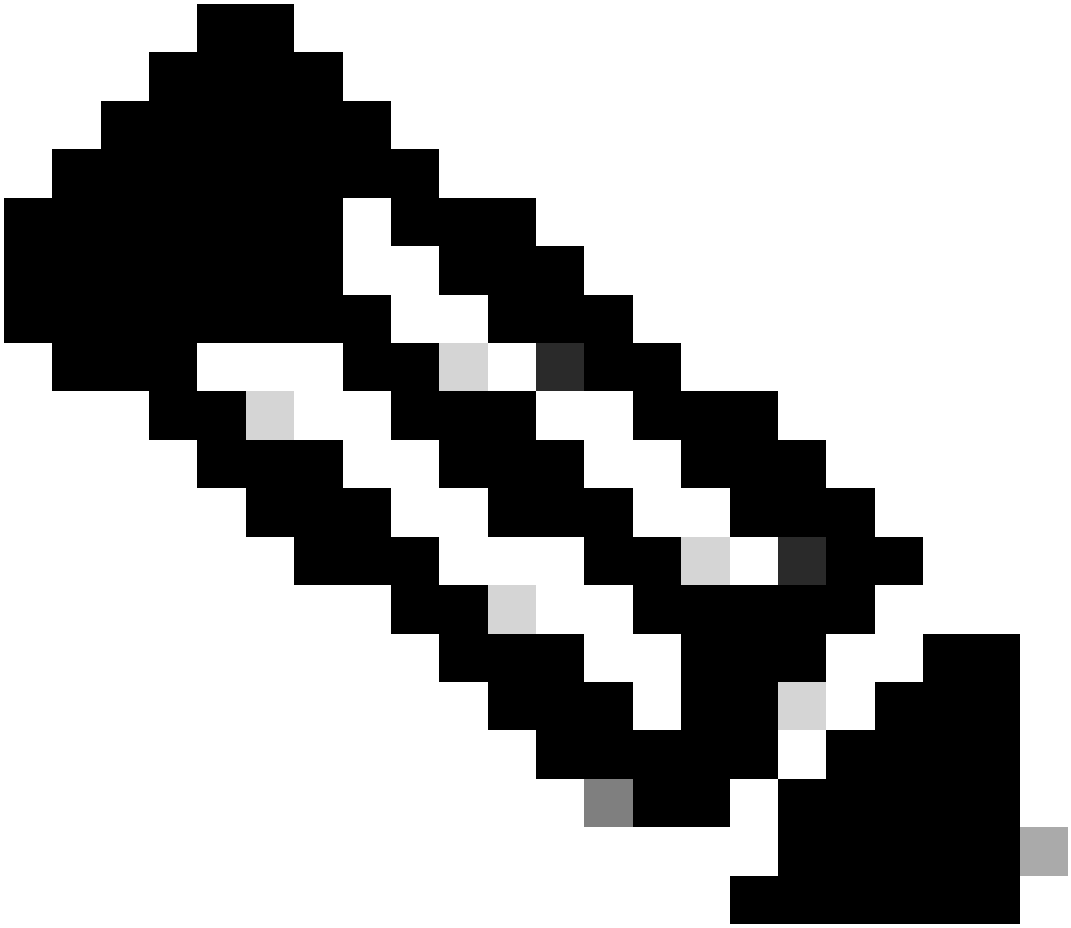
This document describes the procedure to configure isolated PVLANs on Cisco Catalyst switches with either Catalyst OS (CatOS) or Cisco IOS® Software.

Prerequisites

Requirements

This document assumes that you have a network that already exists and are able to establish connectivity among the various ports for addition to a Private VLANs (PVLANs). If you have multiple switches, make sure that the trunk between the switches functions correctly and permits the PVLANs on the trunk.

Not all switches and software versions support PVLANs.



> **Note**: Some switches (as specified in the Private VLAN Catalyst Switch Support Matrix) currently support only the PVLAN Edge feature. The term protected ports also refers to this feature. PVLAN Edge ports have a restriction that prevents communication with other protected ports on the same switch. Protected ports on separate switches, however, can communicate with each other. Do not confuse this feature with the normal PVLAN configurations that this document shows. For more information on protected ports, refer to the Configuring Port Security section of the document Configuring Port-Based Traffic Control.

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 4003 switch with Supervisor Engine 2 module that runs CatOS version 6.3(5)

- Catalyst 4006 switch with Supervisor Engine 3 module that runs Cisco IOS Software Release 12.1(12c)EW1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

In some situations, you need to prevent Layer 2 (L2) connectivity between end devices on a switch without the placement of the devices in different IP subnets. This setup prevents the waste of IP addresses. PVLANs allow the isolation at Layer 2 of devices in the same IP subnet. You can restrict some ports on the switch to reach only specific ports that have a default gateway, backup server, or Cisco LocalDirector attached.

This document describes the procedure to configure isolated PVLANs on Cisco Catalyst switches with either Catalyst OS (CatOS) or Cisco IOS Software.

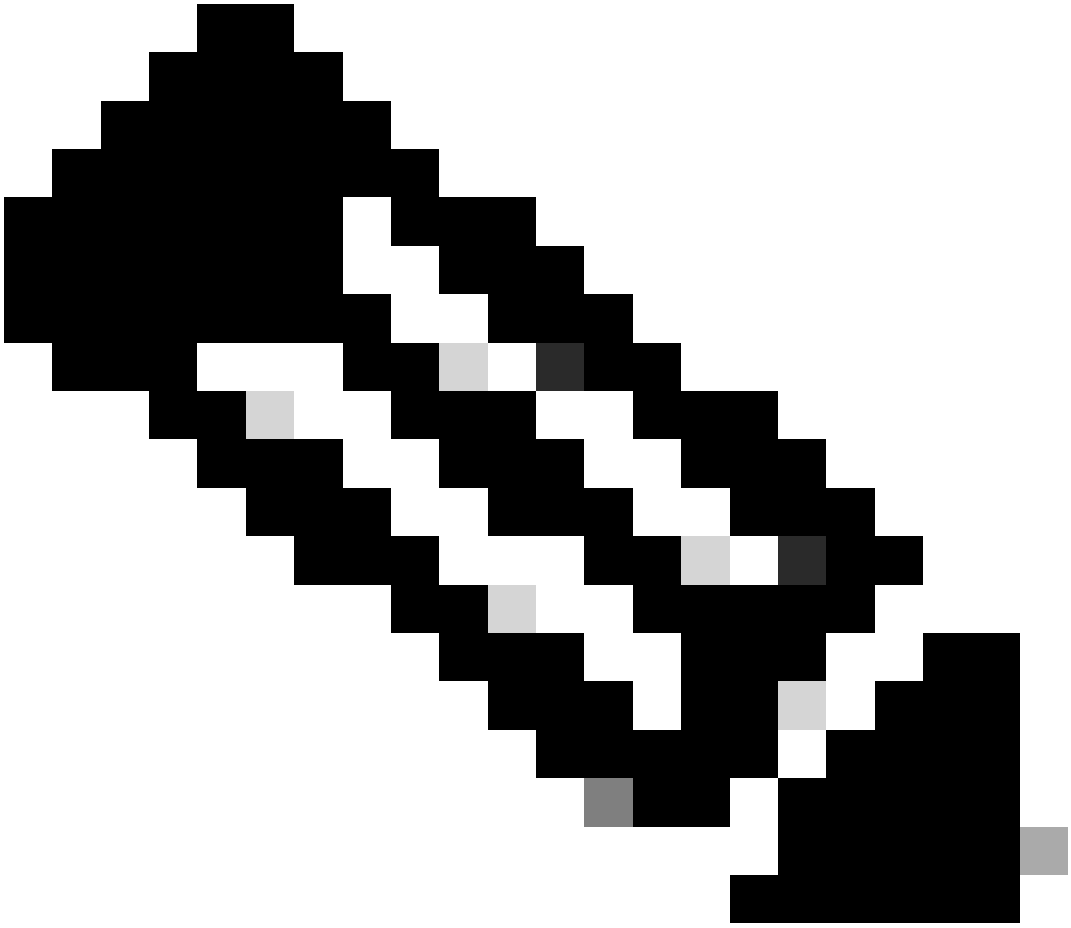
A PVLAN is a VLAN with configuration for Layer 2 isolation from other ports within the same broadcast domain or subnet. You can assign a specific set of ports within a PVLAN and thereby control access among the ports at Layer 2. You can configure PVLANs and normal VLANs on the same switch.

There are three types of PVLAN ports: promiscuous, isolated, and community.

1. A promiscuous port communicates with all other PVLAN ports. The promiscuous port is the port that you typically use to communicate with external routers, Local Directors, network management devices, backup servers, administrative workstations, and other devices. On some switches, the port to the route module (for example, Multilayer Switch Feature Card [MSFC]) needs to be promiscuous.

2. An isolated port has complete Layer 2 separation from other ports within the same PVLAN. This separation includes broadcasts, and the only exception is the promiscuous port. A privacy grant at the Layer 2 level occurs with the block of outgoing traffic to all isolated ports. Traffic that comes from an isolated port forwards to all promiscuous ports only.

3. Community ports can communicate with each other and with the promiscuous ports. These ports have Layer 2 isolation from all other ports in other communities, or isolated ports within the PVLAN. Broadcasts propagate only between associated community ports and the promiscuous port.



Note: This document does not cover community VLAN configuration.

Rules and Limitations

This section provides some rules and limitations for which you must watch when you implement PVLANs.

- PVLANs cannot include VLANs 1 or 1002–1005.
- You must set VLAN Trunk Protocol (VTP) mode to `transparent`.
- You can only specify one isolated VLAN per primary VLAN.
- You can only designate a VLAN as a PVLAN if that VLAN has no current access port assignments. Remove any ports in that VLAN before you make the VLAN a PVLAN.
- Do not configure PVLAN ports as EtherChannels.
- Due to hardware limitations, the Catalyst 6500/6000 Fast Ethernet switch modules restrict the configuration of an isolated or community VLAN port when one port within the same COIL application-specific integrated circuit (ASIC) is one of these:

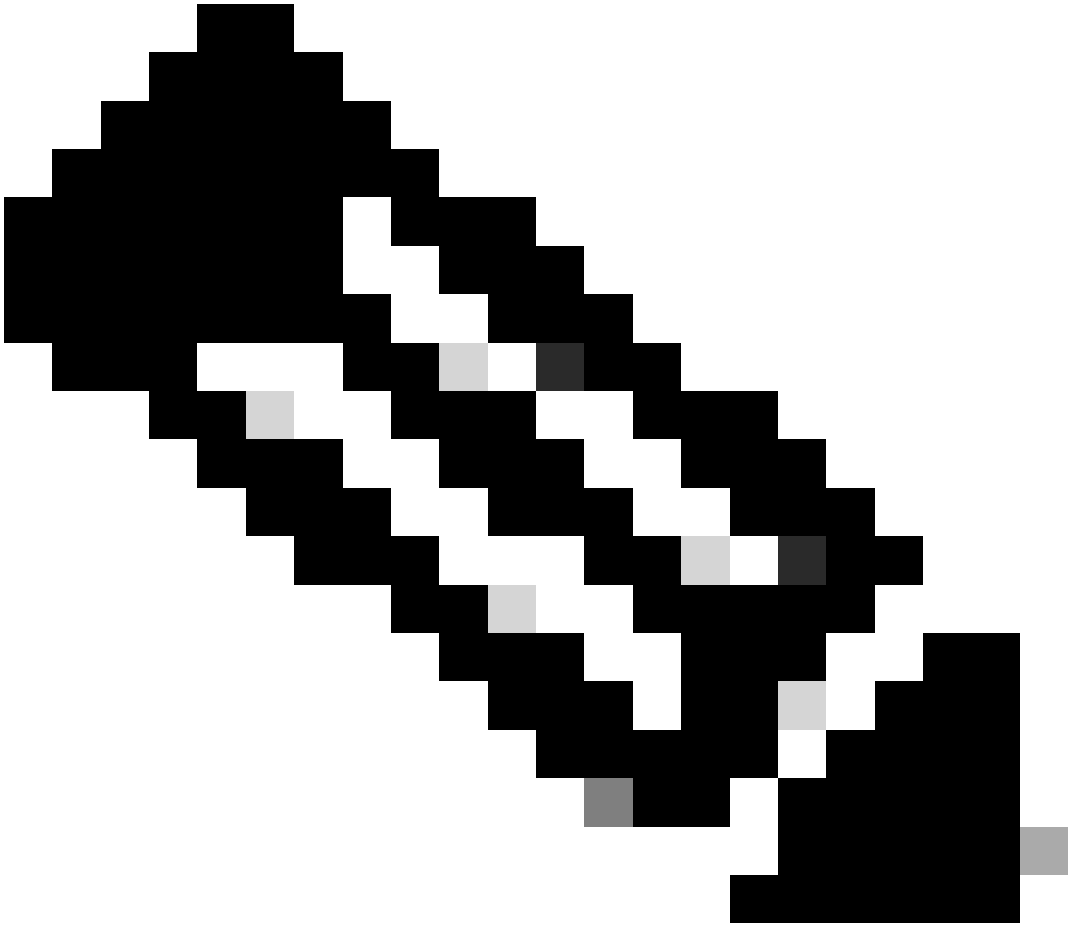
- A trunk
- A Switched Port Analyzer (SPAN) destination
- A promiscuous PVLAN port

This table indicates the range of ports that belong to the same ASIC on Catalyst 6500/6000 FastEthernet modules:

Module	Ports by ASIC
WS-X6224-100FX-MT, WS-X6248-RJ-45, WS-X6248-TEL	Ports 1-12, 13-24, 25-36, 37-48
WS-X6024-10FL-MT	Ports 1-12, 13-24
WS-X6548-RJ-45, WS-X6548-RJ-21	Ports 1-48

The **show pvlan capability** command (CatOS) also indicates if you can make a port a PVLAN port. There is no equivalent command in Cisco IOS Software.

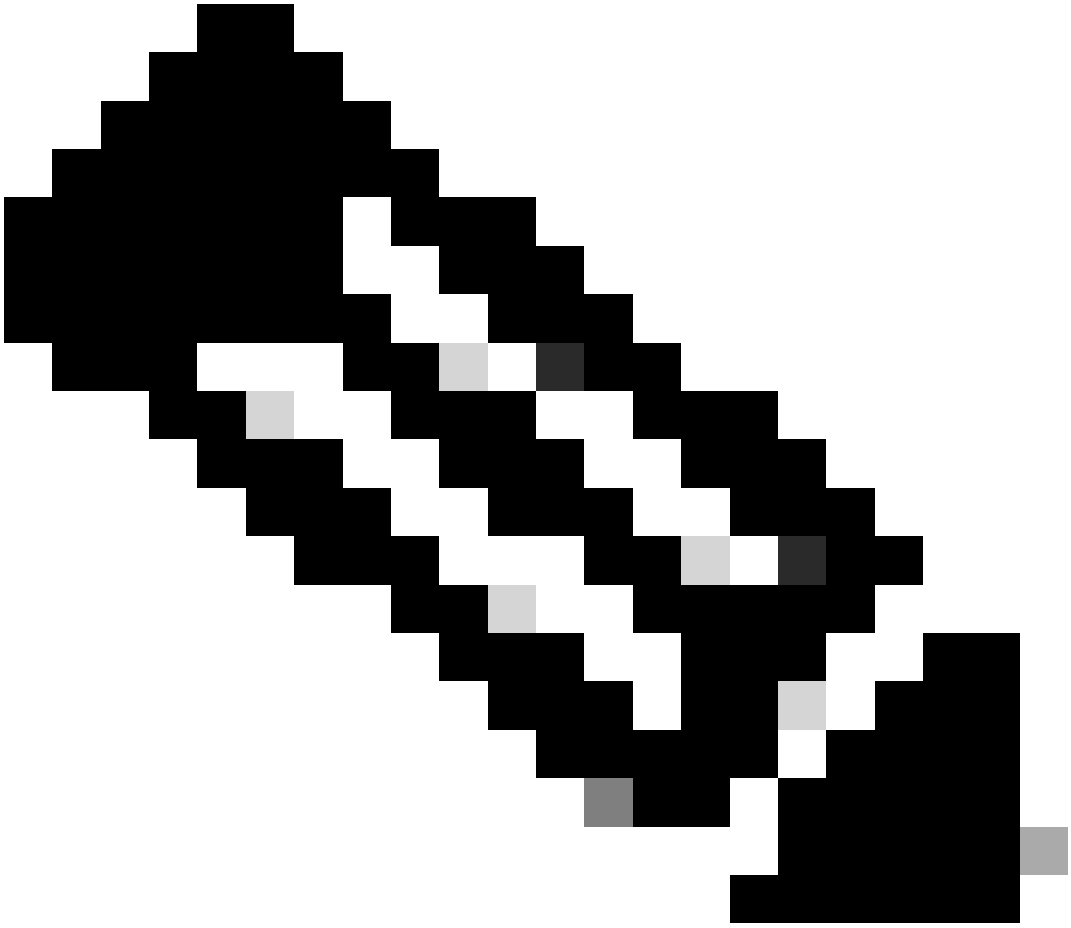
- If you delete a VLAN that you use in the PVLAN configuration, the ports that associate with the VLAN become inactive.
- Configure Layer 3 (L3) VLAN interfaces only for the primary VLANs. VLAN interfaces for isolated and community VLANs are inactive while the VLAN has an isolated or community VLAN configuration.
- You can extend PVLANs across switches with the use of trunks. Trunk ports carry traffic from regular VLANs and also from primary, isolated, and community VLANs. Cisco recommends the use of standard trunk ports if both switches that undergo trunking support PVLANs.



Note: You must manually enter the same PVLAN configuration on every switch with involvement because VTP in transparent mode does not propagate this information.

Configure

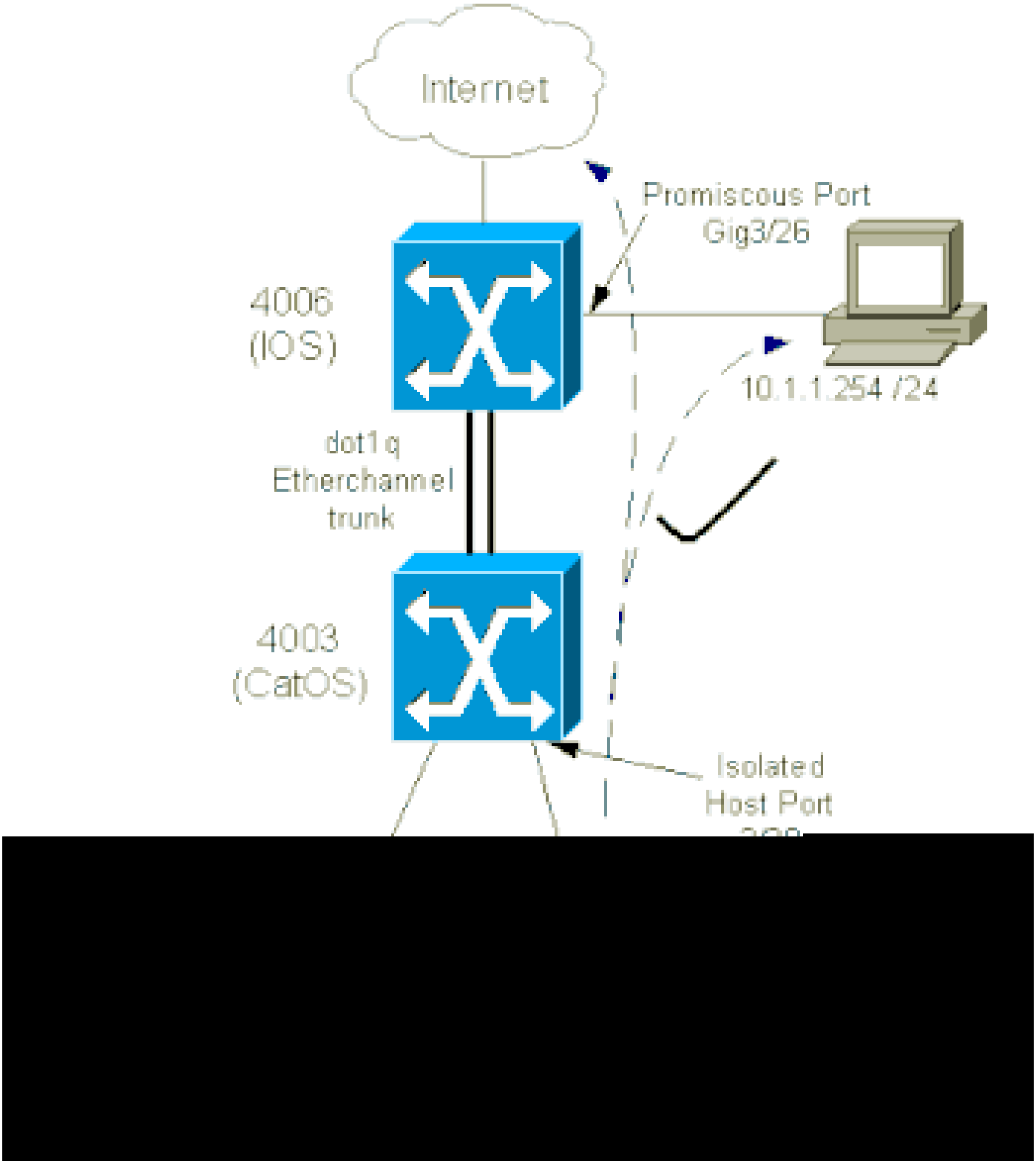
In this section, you are presented with the information to configure the features described in this document.



Note: Use the command **Lookup Tool** to find more information on the commands used in this document. Only registered users can access internal Cisco tools and information.

Network Diagram

This document uses this network setup:



In this scenario, the devices in the isolated VLAN (101) have a restriction from communication at Layer 2 with one another. However, the devices can connect to the Internet. In addition, port Gig 3/26 on the 4006 has the promiscuous designation. This optional configuration allows a device on GigabitEthernet 3/26 to connect to all devices in the isolated VLAN. This configuration also allows, for example, the backup of the data from all the PVLAN host devices to an administration workstation. Other uses for promiscuous ports include connection to an external router, LocalDirector, network management device, and other devices.

Configure the Primary and Isolated VLANs

Perform these steps to create the primary and secondary VLANs, as well as to bind the various ports to these VLANs. The steps include examples for both CatOS and Cisco IOS® Software. Issue the appropriate command set for your OS installation.

1. Create the **primary PVLAN**.

   - CatOS

```
<#root>

Switch_CatOS> (enable)

set vlan primary_vlan_id
pvlan-type primary name primary_vlan

 !--- Note: This command must be on one line.

VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 100 configuration successful
```

   - Cisco IOS Software

```
<#root>

Switch_IOS(config)#

vlan primary_vlan_id

Switch_IOS(config-vlan)#

private-vlan primary

Switch_IOS(config-vlan)#

name primary-vlan

Switch_IOS(config-vlan)#

exit
```

2. Create the i**solated VLAN** or **VLANs**.

   - CatOS

```
<#root>

Switch_CatOS> (enable)

set vlan secondary_vlan_id
pvlan-type isolated name isolated_pvlan

 !--- Note: This command must be on one line.
```

```
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 101 configuration successful
```

- Cisco IOS Software

```
<#root>

Switch_IOS(config)#

vlan secondary_vlan_id

Switch_IOS(config-vlan)#

private-vlan isolated

Switch_IOS(config-vlan)#

name isolated_pvlan

Switch_IOS(config-vlan)#

exit
```

3. Bind the **isolated VLAN/VLANs** to the **primary VLAN**.

- CatOS

```
<#root>

Switch_CatOS> (enable)

set pvlan primary_vlan_id secondary_vlan_id

Vlan 101 configuration successful
Successfully set association between 100 and 101.
```

- Cisco IOS Software

```
<#root>

Switch_IOS(config)#

vlan primary_vlan_id

Switch_IOS(config-vlan)#

private-vlan association secondary_vlan_id

Switch_IOS(config-vlan)#

exit
```

4. Verify the **private VLAN configuration**.

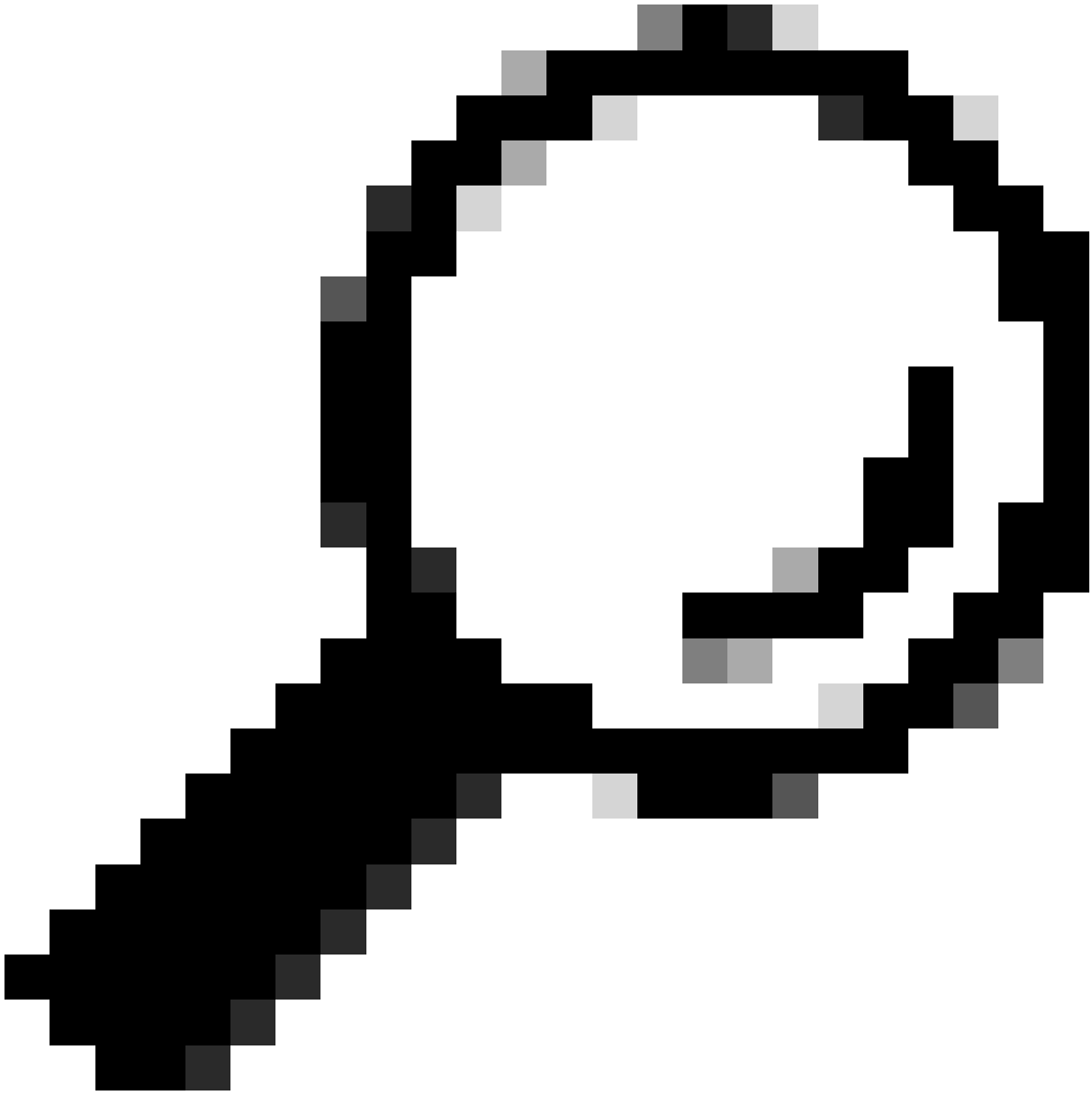
- CatOS

```
<#root>

Switch_CatOS> (enable)

show pvlan

Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
100     101       isolated
```

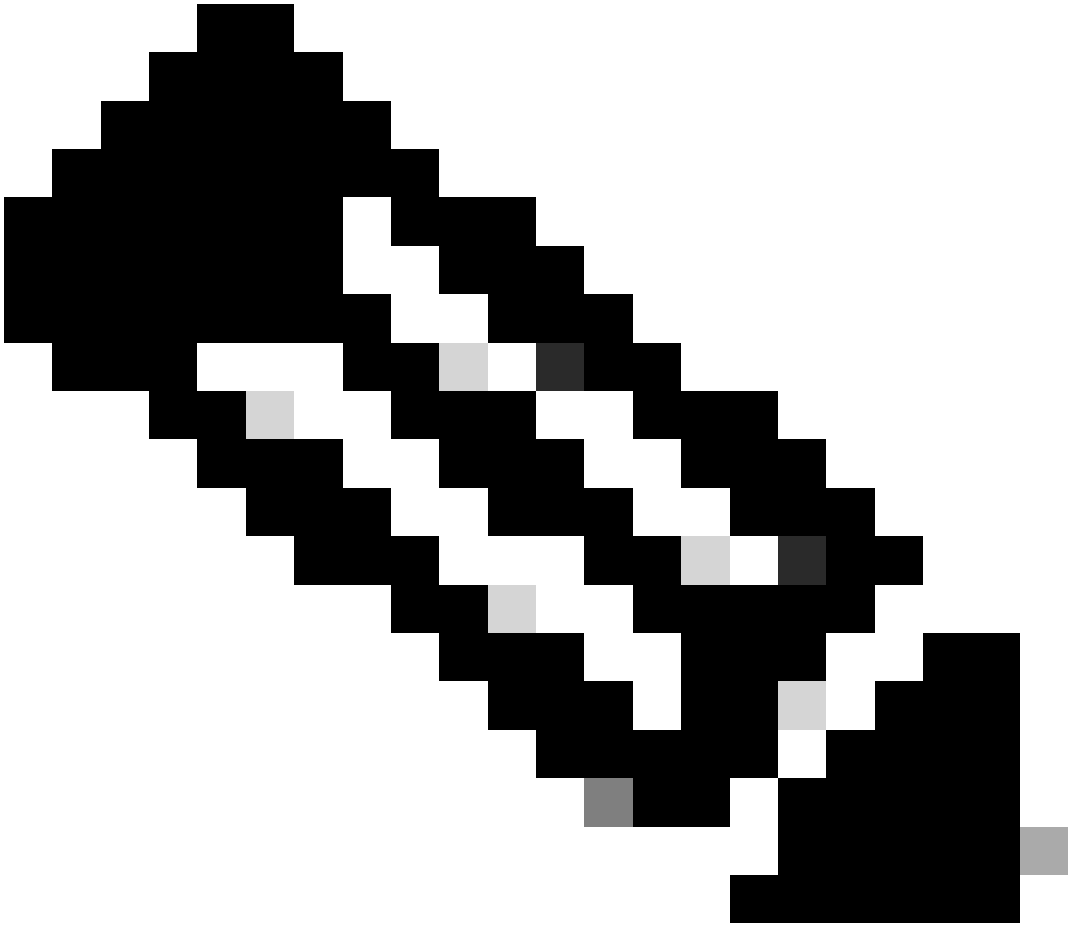
- Cisco IOS Software

```
<#root>

Switch_IOS#

show vlan private-vlan

Primary  Secondary  Type              Ports
------- --------- ----------------- -------
100     101       isolated
```

Assign Ports to the PVLANs



Tip: Before you implement this procedure, issue the show PVLAN capability mod/port command (for CatOS) to determine if a port can become a PVLAN port.



Note: Before you perform Step 1 of this procedure, issue the **switchport** command in interface configuration mode to configure the port as a Layer 2 switched interface.

- Configure the **host ports** on all the appropriate switches.
  - CatOS

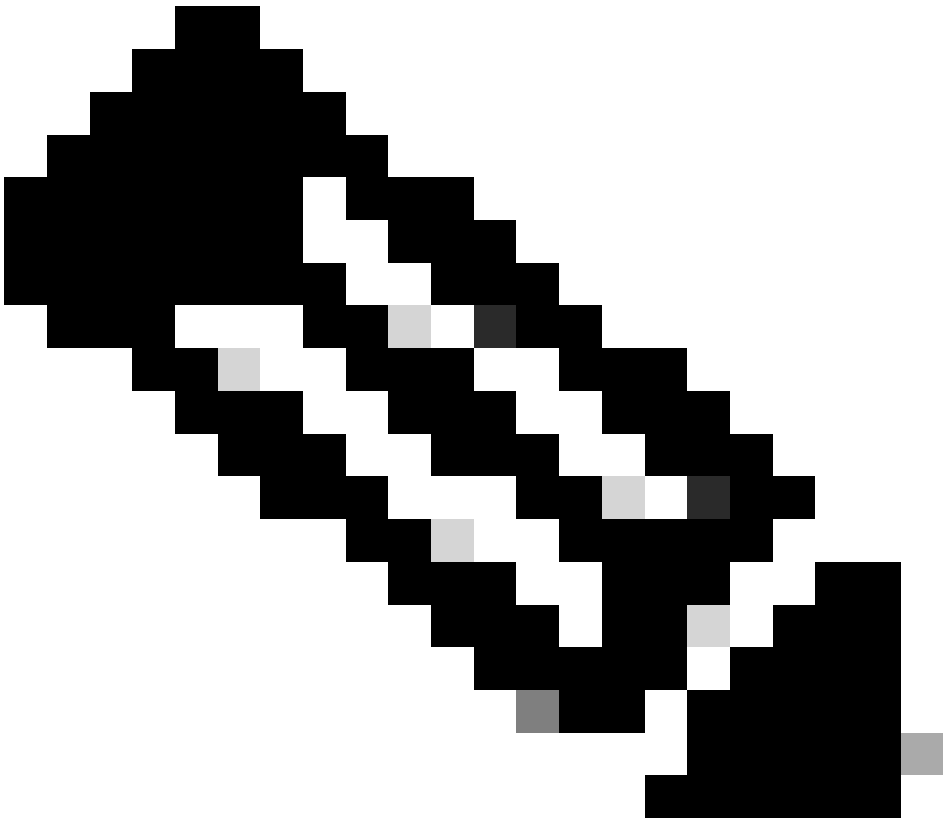
```
<#root>

Switch_CatOS> (enable)

 set pvlan primary_vlan_id secondary_vlan_id mod/port


!--- Note: This command must be on one line.

Successfully set the following ports to Private Vlan 100,101: 2/20
```

  - Cisco IOS Software

```
<#root>

Switch_IOS(config)#

interface gigabitEthernet mod/port

Switch_IOS(config-if)#

switchport private-vlan host
primary_vlan_id secondary_vlan_id


 !--- Note: This command must be on one line.

Switch_IOS(config-if)#

switchport mode private-vlan host

Switch_IOS(config-if)#

exit
```

- Configure the **promiscuous port** on one of the switches.
  - CatOS

```
<#root>

Switch_CatOS> (enable)

set pvlan mapping primary_vlan_id secondary_vlan_id mod/port


!--- Note: This command must be on one line.

Successfully set mapping between 100 and 101 on 3/26
```



Note: For Catalyst 6500/6000 when the Supervisor Engine runs CatOS as the system software, the MSFC port on the Supervisor Engine (15/1 or 16/1) must be promiscuous if you wish to Layer 3 switch between the VLANs.

- Cisco IOS Software

```
<#root>

Switch_IOS(config)#

interface interface_type mod/port

Switch_IOS(config-if)#

switchport private-vlan
mapping primary_vlan_id secondary_vlan_id


 !--- Note: This command must be on one line.

Switch_IOS(config-if)#

switchport mode private-vlan promiscuous


Switch_IOS(config-if)#
```

```
end
```

Layer 3 Configuration

This optional section describes the configuration steps to permit the route of PVLAN ingress traffic. If you only need to enable Layer 2 connectivity, you can omit this phase.

1. Configure the VLAN interface in the same way that you configure for normal Layer 3 routing.

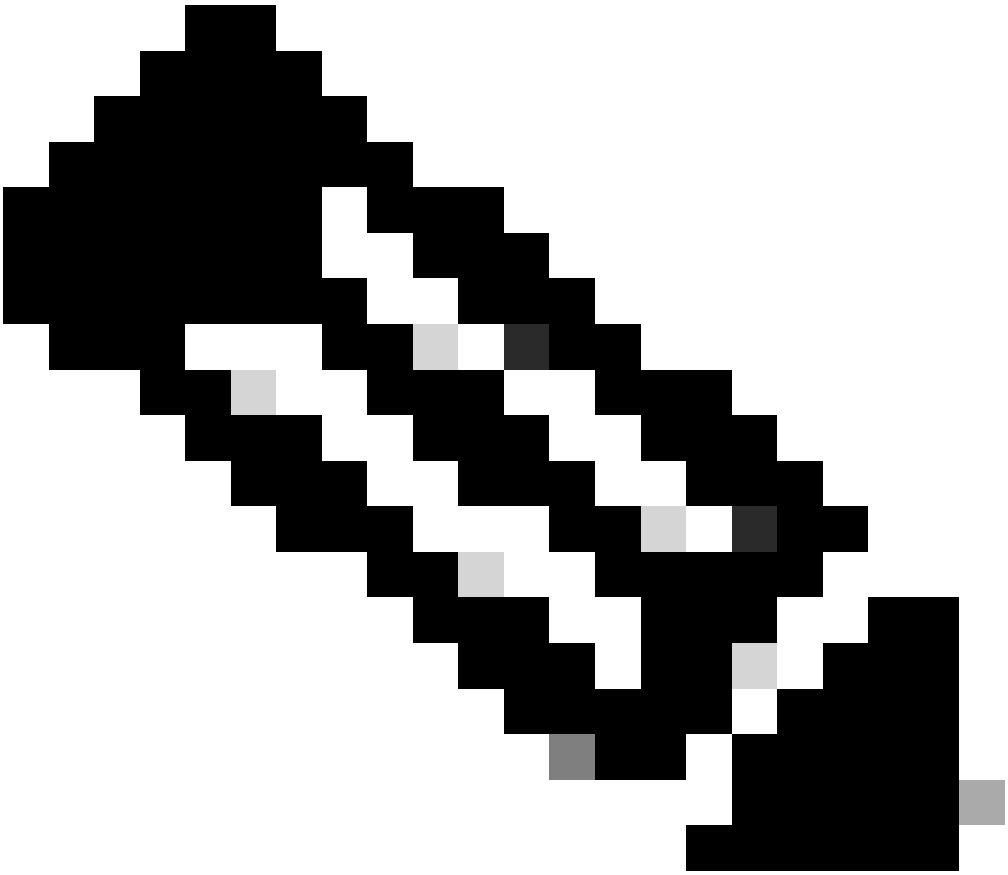
   This configuration involves:

   - Configuration of an IP address
   - Activation of the interface with the **no shutdown** command
   - Verification that the VLAN exists in the VLAN database

   Refer to VLANs/VTP Technical Support for configuration examples.

2. Map the secondary VLANs that you wish to route with the primary VLAN.

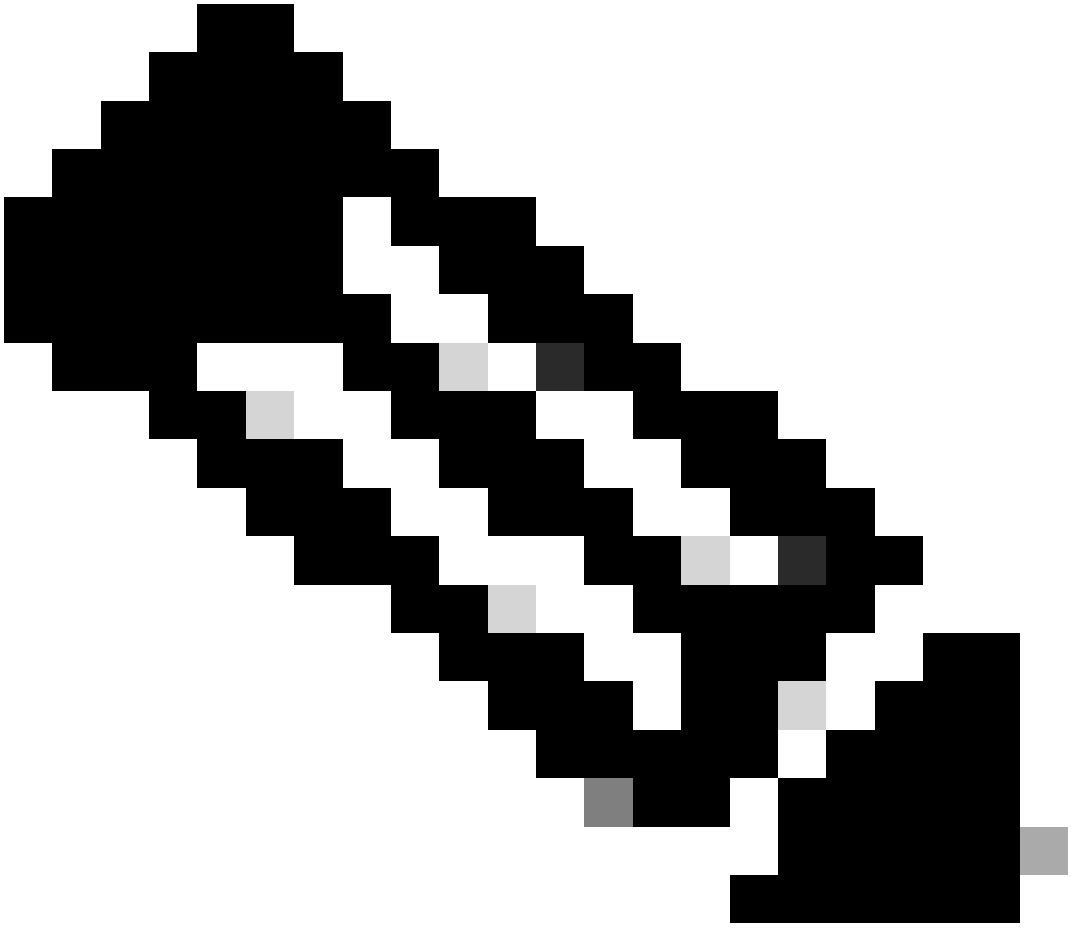
```
<#root>

Switch_IOS(config)#

interface vlan primary_vlan_id

Switch_IOS(config-if)#

private-vlan mapping secondary_vlan_list


Switch_IOS(config-if)#

end
```



Note: Configure Layer 3 VLAN interfaces only for primary VLANs. VLAN interfaces for isolated and community VLANs are inactive with an isolated or community VLAN configuration.

3. Issue the **show interfaces private-vlan mapping** (Cisco IOS Software) or **show pvlan mapping** (CatOS) command to verify the mapping.
4. If you need to modify the secondary VLAN list after the configuration of mapping, use the **add** or **remove** keyword.

```
<#root>

Switch_IOS(config-if)#

private-vlan mapping add secondary_vlan_list

or
Switch_IOS(config-if)#

private-vlan mapping remove secondary_vlan_list
```



Note: For Catalyst 6500/6000 switches with MSFC, ensure that the port from the Supervisor Engine to the routing engine (for example, port 15/1 or 16/1) is promiscuous.

```
<#root>

cat6000> (enable)

set pvlan mapping primary_vlan secondary_vlan 15/1

Successfully set mapping between 100 and 101 on 15/1
```

Issue the command **show pvlan mapping** to verify the mapping.

```
<#root>

cat6000> (enable)

show pvlan mapping
```

```
Port Primary Secondary
---- ------- ---------
15/1  100      101
```

Configurations

This document uses these configurations:

- Access_Layer (Catalyst 4003: CatOS)
- Core (Catalyst 4006: Cisco IOS Software)

Access_Layer (Catalyst 4003: CatOS)

```
<#root>

Access_Layer> (enable)

show config

 This command shows non-default configurations only.
 Use 'show config all' to show both default and non-default configurations.
 ............


!--- Output suppressed.


 #system
 set system name  Access_Layer
 !
 #frame distribution method
 set port channel all distribution mac both
 !
 #vtp
 set vtp domain Cisco
 set vtp mode transparent
 set vlan 1 name default type ethernet mtu 1500 said 100001 state active
 set vlan 100 name primary_for_101 type ethernet pvlan-type primary mtu 1500
 said 100100 state active

!--- This is the primary VLAN 100.
!--- Note: This command must be on one line.

 set vlan 101 name isolated_under_100 type ethernet pvlan-type isolated mtu
 1500 said 100101 state active

!--- This is the isolated VLAN 101.
!--- Note: This command must be on one line.

 set vlan 1002 name fddi-default type fddi mtu 1500 said 101002 state active


!--- Output suppressed.


 #module 1 : 0-port Switching Supervisor
 !
```

```
 #module 2 : 24-port 10/100/1000 Ethernet

set pvlan 100 101 2/20

!--- Port 2/20 is the PVLAN host port in primary VLAN 100, isolated
!--- VLAN 101.

 set trunk 2/3  desirable dot1q 1-1005
 set trunk 2/4  desirable dot1q 1-1005
 set trunk 2/20 off dot1q 1-1005

!--- Trunking is automatically disabled on PVLAN host ports.

 set spantree portfast    2/20 enable

!--- PortFast is automatically enabled on PVLAN host ports.

 set spantree portvlancost 2/1  cost 3


!--- Output suppressed.


 set spantree portvlancost 2/24 cost 3
 set port channel 2/20 mode off

!--- Port channeling is automatically disabled on PVLAN !--- host ports.

 set port channel 2/3-4 mode desirable silent
 !
 #module 3 : 34-port 10/100/1000 Ethernet
 end
```

Core (Catalyst 4006: Cisco IOS Software)

```
<#root>

Core#

show running-config

 Building configuration...


!--- Output suppressed.

 !
 hostname Core
 !
 vtp domain Cisco
 vtp mode transparent

!--- VTP mode is transparent, as PVLANs require.

 ip subnet-zero
 !
 vlan 2-4,6,10-11,20-22,26,28
 !
 vlan 100
  name primary_for_101
```

```
   private-vlan primary
   private-vlan association 101
 !
 vlan 101
  name isolated_under_100
   private-vlan isolated
 !
 interface Port-channel1

!--- This is the port channel for interface GigabitEthernet3/1
!--- and interface GigabitEthernet3/2.

  switchport
  switchport trunk encapsulation dot1q
  switchport mode dynamic desirable
 !
 interface GigabitEthernet1/1
 !
 interface GigabitEthernet1/2
 !
 interface GigabitEthernet3/1

!--- This is the trunk to the Access_Layer switch.

  switchport trunk encapsulation dot1q
  switchport mode dynamic desirable
  channel-group 1 mode desirable
 !
 interface GigabitEthernet3/2

!--- This is the trunk to the Access_Layer switch.

  switchport trunk encapsulation dot1q
  switchport mode dynamic desirable
  channel-group 1 mode desirable
 !
 interface GigabitEthernet3/3
 !

!--- There is an omission of the interface configuration
!--- that you do not use.

 !
 interface GigabitEthernet3/26


  switchport private-vlan mapping 100 101
  switchport mode private-vlan promiscuous


!--- Designate the port as promiscuous for PVLAN 101.

 !

!--- There is an omission of the interface configuration
!--- that you do not use.

 !

!--- Output suppressed.

 interface Vlan25
```

```
!--- This is the connection to the Internet.

  ip address 10.25.1.1 255.255.255.0
 !
 interface Vlan100

!--- This is the Layer 3 interface for the primary VLAN.

  ip address 10.1.1.1 255.255.255.0
  private-vlan mapping 101

!--- Map VLAN 101 to the VLAN interface of the primary VLAN (100).
!--- Ingress traffic for devices in isolated VLAN 101 routes
!--- via interface VLAN 100.
```

Private VLANs Across Multiple Switches

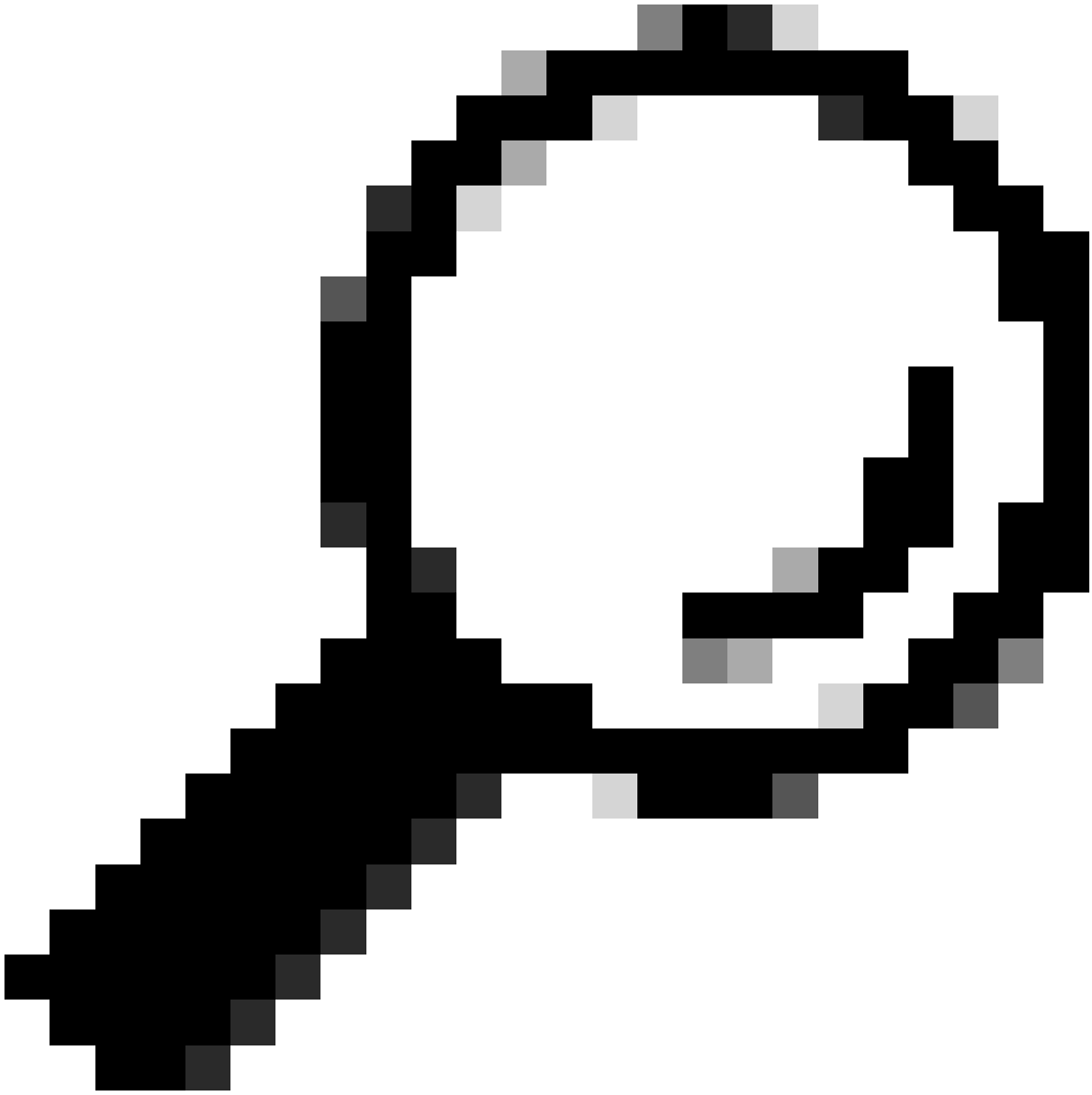
Private VLANs can be taken across multiple switches in two methods. This section discusses these methods:

- Regular Trunks
- Private VLAN Trunks

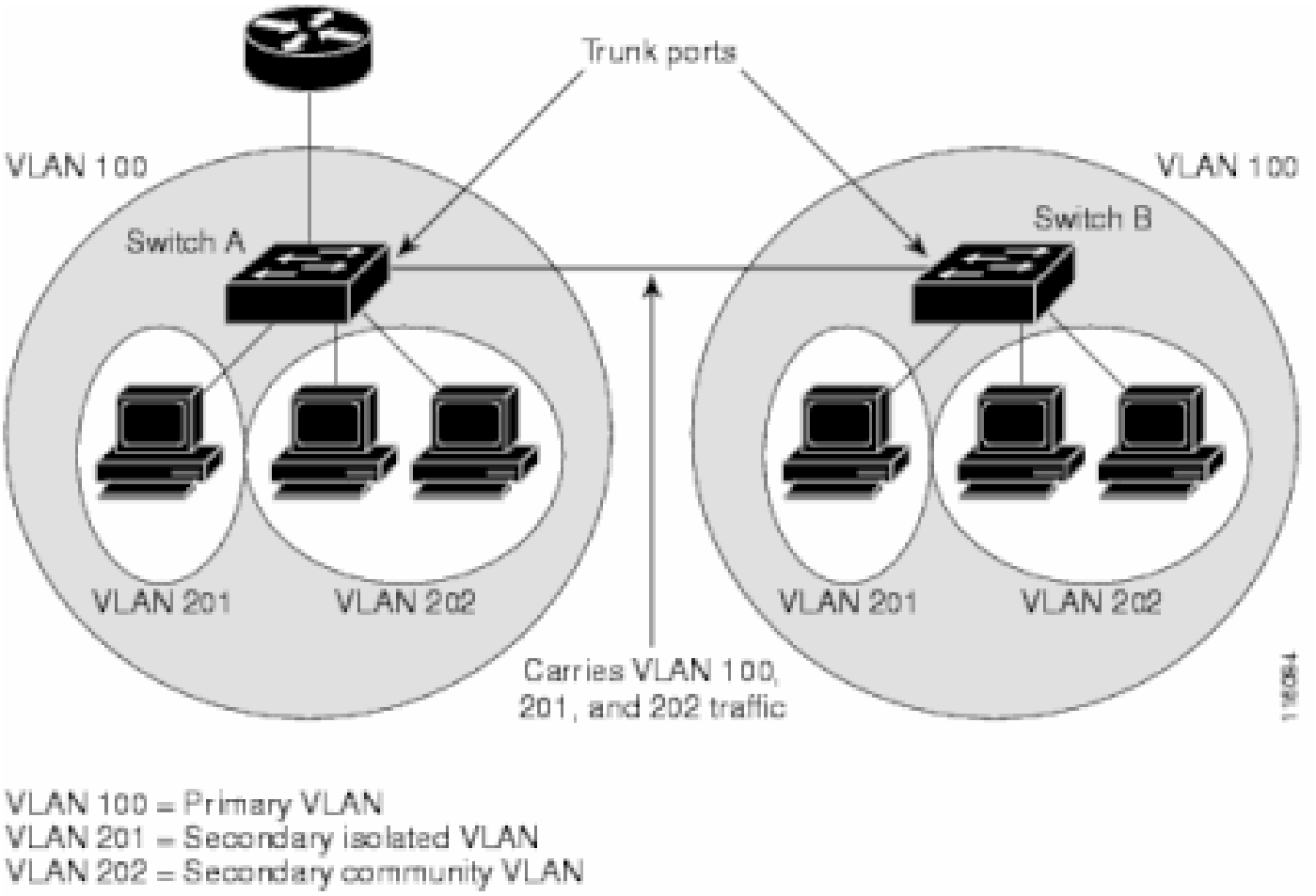
Regular Trunks

As with regular VLANs, PVLANs can span multiple switches. A trunk port carries the primary VLAN and secondary VLANs to a neighboring switch. The trunk port deals with the private VLAN as any other VLAN. A feature of PVLANs across multiple switches is that traffic from an isolated port in one switch does not reach an isolated port on another switch.

Configure PVLANs on all intermediate devices, which includes devices that have no PVLAN ports, in order to maintain the security of your PVLAN configuration and avoid other use of the VLANs configured as PVLANs. Trunk ports carry traffic from regular VLANs, and also from primary, isolated, and community VLANs.



Tip: Cisco recommends the use of standard trunk ports if both switches that undergo trunking support PVLANs.



Manually Configure PVLANS on all Switches in the Layer 2 Network

Because VTP does not support PVLANs, you must manually configure PVLANs on all switches in the Layer 2 network. If you do not configure the primary and secondary VLAN association in some switches in the network, the Layer 2 databases in these switches are not merged. This situation can result in unnecessary flooding of PVLAN traffic on those switches.

Private VLAN Trunks

A PVLAN trunkport can carry multiple secondary and non-PVLANs. Packets are received and transmitted with secondary or regular VLAN tags on the PVLAN trunk ports.

Only IEEE 802.1q encapsulation is supported. Isolated trunk ports allow you to combine traffic for all secondary ports over a trunk. Promiscuous trunk ports allow you to combine the multiple promiscuous ports required in this topology in a single trunk port that carries multiple primary VLANs.

Use isolated Private VLAN trunk ports when you anticipate the use of Private VLAN isolated host ports to carry multiple VLANs, either normal VLANs or for multiple Private VLAN domains. This makes it useful for connecting a downstream switch that does not support Private VLANs.

Private VLAN Promiscuous Trunks are used in situations where a Private VLAN promiscuous host port is normally used but where it is necessary to carry multiple vlans, either normal vlans or for multiple Private VLAN domains. This makes it useful for connecting an upstream router that does not support Private VLANs.

Additional Information

Refer to Private VLAN Trunks for more information.

In order to configure an interface as PVLAN trunk port, refer to Configuring a Layer 2 Interface as a PVLAN Trunk Port .

In order to configure an interface as a promiscuous trunk port, refer to Configuring a Layer 2 Interface as a Promiscuous Trunk Port .

Verify

Use this section to confirm that your configuration works properly.

CatOS

- **show pvlan**—Displays the PVLAN configuration. Verify that the isolated and primary VLANs associate with each other. Also, verify that any host ports appear.
- **show pvlan mapping**—Displays the PVLAN mapping with configuration on promiscuous ports.

Cisco IOS Software

- **show vlan private-vlan**—Displays PVLAN information, which includes ports that associate.
- **show interfacemod/portswitchport**—Displays interface-specific information. Verify that the operational mode as well as the operational PVLAN settings are correct.
- **show interfaces private-vlan mapping**—Displays the PVLAN mapping that you have configured.

Verification Procedure

Complete these steps:

1. Verify the **PVLAN configuration** on the switches.

   Check to determine if the primary and secondary PVLANs associate/map to each other. Also, verify the inclusion of the necessary ports.

```
<#root>

Access_Layer> (enable)

show pvlan

Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
 100     101       isolated         2/20

Core#

show vlan private-vlan


Primary Secondary Type             Ports
------- --------- ---------------- -----------
100     101       isolated         Gi3/26
```

2. Verify the **correct configuration** of the promiscuous port.

   This output indicates that the port operational mode is **promiscuous** and that the operational VLANs are 100 and 101.

```
<#root>

Core#

show interface gigabitEthernet 3/26 switchport

Name: Gi3/26
Switchport: Enabled
Administrative Mode: private-Vlan promiscuous

Operational Mode: private-vlan promiscuous

Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative Private VLAN Host Association: none

Administrative Private VLAN Promiscuous Mapping: 100
(primary_for_101) 101 (isolated_under_100)

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 VLANs:
100 (primary_for_101) 101 (isolated_under_100)

Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

3. Initiate an Internet Control Message Protocol (ICMP) ping packet from the host port to the promiscuous port.

   Keep in mind that, since both devices are in the same primary VLAN, the devices must be in the same subnet.

```
<#root>

host_port#

show arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.100              -   0008.a390.fc80  ARPA   FastEthernet0/24

!--- The Address Resolution Protocol (ARP) table on the client indicates
```

```
!--- that no MAC addresses other than the client addresses are known.

host_port#
ping 10.1.1.254


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.254, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms

!--- The ping is successful. The first ping fails while the
!--- device attempts to map via ARP for the peer MAC address.


host_port#
show arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.100              -   0008.a390.fc80  ARPA   FastEthernet0/24
Internet  10.1.1.254              0   0060.834f.66f0  ARPA   FastEthernet0/24


!--- There is now a new MAC address entry for the peer.
```

4. Initiate an ICMP ping between host ports.

   In this example, `host_port_2` (10.1.1.99) attempts to ping > `host_port` (10.1.1.100). This ping fails. A ping from another host port to the promiscuous port, however, still succeeds.

```
<#root>

host_port_2#
ping 10.1.1.100


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

!--- The ping between host ports fails, which is desirable.


host_port_2#
ping 10.1.1.254


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

!--- The ping to the promiscuous port still succeeds.
```

```
host_port_2#

show arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.99               -   0005.7428.1c40  ARPA   Vlan1
Internet  10.1.1.254              2   0060.834f.66f0  ARPA   Vlan1

!--- The ARP table includes only an entry for this port and
!--- the promiscuous port.
```

Troubleshoot

Troubleshoot PVLANs

This section addresses some common problems that occur with PVLAN configurations.

Problem 1

You get this error message: "`%PM-SP-3-ERR_INCOMP_PORT: <mod/port> is set to inactive because <mod/port> is a trunk port.`"

This error message can be displayed for multiple reasons, as discussed here.

Explanation - 1

Due to hardware limitations, Catalyst 6500/6000 10/100-Mbps modules restrict the configuration of an isolated or community VLAN port when one port within the same COIL ASIC is a trunk, a SPAN destination, or a promiscuous PVLAN port. (The COIL ASIC controls 12 ports on most modules and 48 ports on the Catalyst 6548 module.) The table in the Rules and Limitations section of this document provides a breakdown of the port restriction on the Catalyst 6500/6000 10/100-Mbps modules.

Resolution Procedure - 1

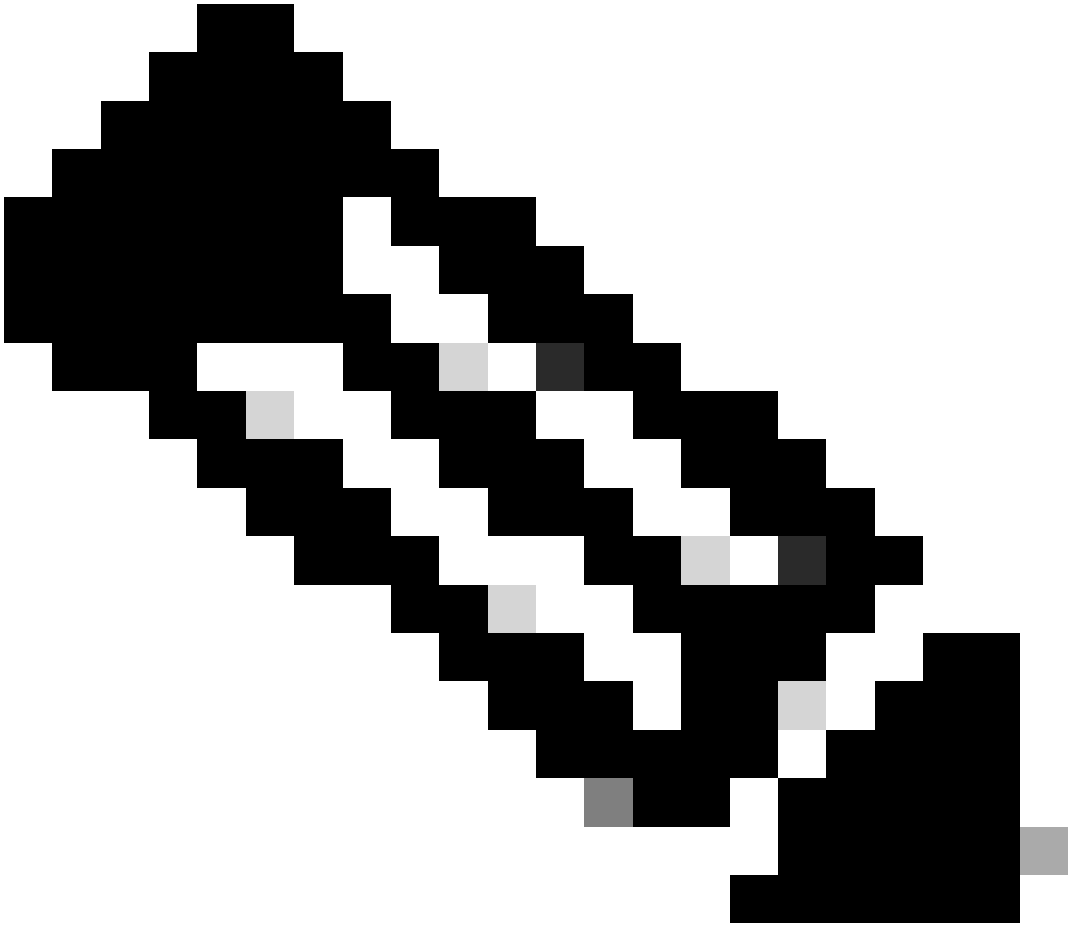
If there is no support for PVLAN on that port, pick a port on a different ASIC on the module or on a different module. In order to reactivate the ports, remove the isolated or community VLAN port configuration and issue the **shutdown** command and **no shutdown** command.

Explanation - 2

If the ports are configured manually or by default to dynamic desirable or dynamic auto mode.

Resolution Procedure - 2

Configure the ports as access mode with the **switchport mode access** command. In order to reactivate the ports, issue the **shutdown** command and **no shutdown** command.



Note: In Cisco IOS Software Release 12.2(17a)SX and later releases, the 12 port restriction does not apply to WS-X6548-RJ-45, WS-X6548-RJ-21 and WS-X6524-100FX-MM Ethernet switching modules.

Problem 2

During PVLAN configuration, you encounter *one* of these messages:

```
Cannot add a private vlan mapping to a port with another Private port in
the same ASIC.
Failed to set mapping between <vlan> and <vlan> on <mod/port>
```

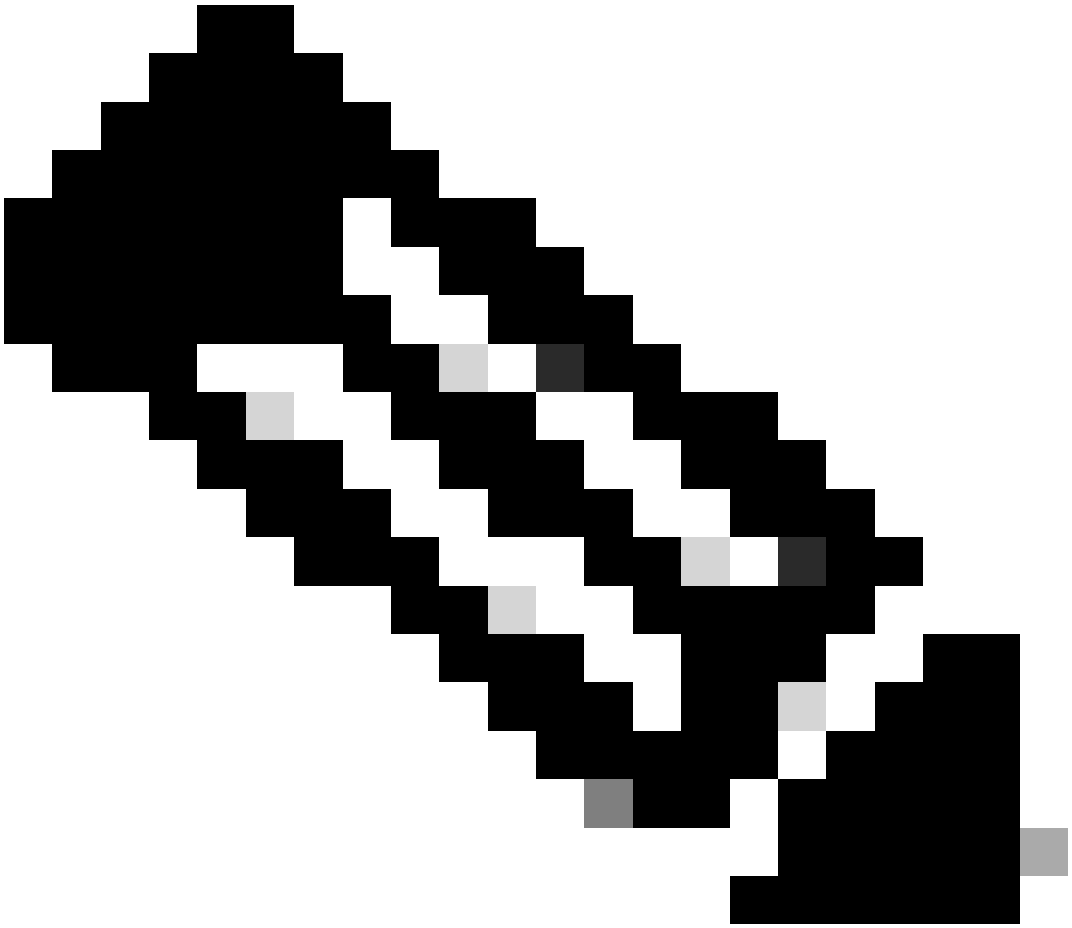
```
Port with another Promiscuous port in the same ASIC cannot be made
Private port.
Failed to add ports to association.
```

Explanation

Due to hardware limitations, Catalyst 6500/6000 10/100-Mbps modules restrict the configuration of an isolated or community VLAN port when one port within the same COIL ASIC is a trunk, a SPAN destination, or a promiscuous PVLAN port. (The COIL ASIC controls 12 ports on most modules and 48 ports on the Catalyst 6548 module.) The table in the Rules and Limitations section of this document provides a breakdown of the port restriction on the Catalyst 6500/6000 10/100-Mbps modules.

Resolution Procedure

Issue the **show pvlan capability** command (CatOS), which indicates if a port can become a PVLAN port. If there is no support for PVLAN on that particular port, pick a port on a different ASIC on the module or on a different module.



Note: In Cisco IOS Software Release 12.2(17a)SX and later releases, the 12 port restriction does not apply to WS-X6548-RJ-45, WS-X6548-RJ-21 and WS-X6524-100FX-MM Ethernet switching modules.

Problem 3

You cannot configure PVLANs on some platforms.

Resolution

Verify that the platform supports PVLANs. Refer to Private VLAN Catalyst Switch Support Matrix to determine if your platform and software version support PVLANs before you begin the configuration.

Problem 4

On a Catalyst 6500/6000 MSFC, you cannot ping a device that connects to the isolated port on the switch.

Resolution

On the Supervisor Engine, verify that the port to the MSFC (15/1 or 16/1) is promiscuous.

```
<#root>

cat6000> (enable)

set pvlan mapping primary_vlan secondary_vlan 15/1

Successfully set mapping between 100 and 101 on 15/1
```

Also, configure the VLAN interface on the MSFC as the Layer 3 Configuration section of this document specifies.

Problem 5

With issue of the **no shutdown** command, you cannot activate the VLAN interface for isolated or community VLANs.

Resolution

Due to the nature of PVLANs, you cannot activate the VLAN interface for isolated or community VLANs. You can only activate the VLAN interface that belongs to the primary VLAN.

Problem 6

On Catalyst 6500/6000 devices with MSFC/MSFC2, ARP entries learned on Layer 3 PVLAN interfaces do not age out.

Resolution

ARP entries that are learned on Layer 3 private VLAN interfaces are sticky ARP entries and do not age out. The connection of new equipment with the same IP address generates a message, and there is no creation of the ARP entry. Therefore, you must manually remove PVLAN port ARP entries if a MAC address changes. In order to add or remove PVLAN ARP entries manually, issue these commands:

```
<#root>
```

```
Router(config)#
no arp 10.1.3.30

IP ARP:Deleting Sticky ARP entry 10.1.3.30
Router(config)#
arp 10.1.3.30 0000.5403.2356 arpa

IP ARP:Overwriting Sticky ARP entry 10.1.3.30, hw:00d0.bb09.266e by
hw:0000.5403.2356
```

Another option is to issue the **no ip sticky-arp** command in Cisco IOS Software Release 12.1(11b)E and later.

Related Information

- Secure Networks with PVLANs and VACLs
- LAN Switching Technology Support
- Cisco Technical Support & Downloads