Configuración de VLAN privadas aisladas en Catalyst switches

Contenido

Introducción

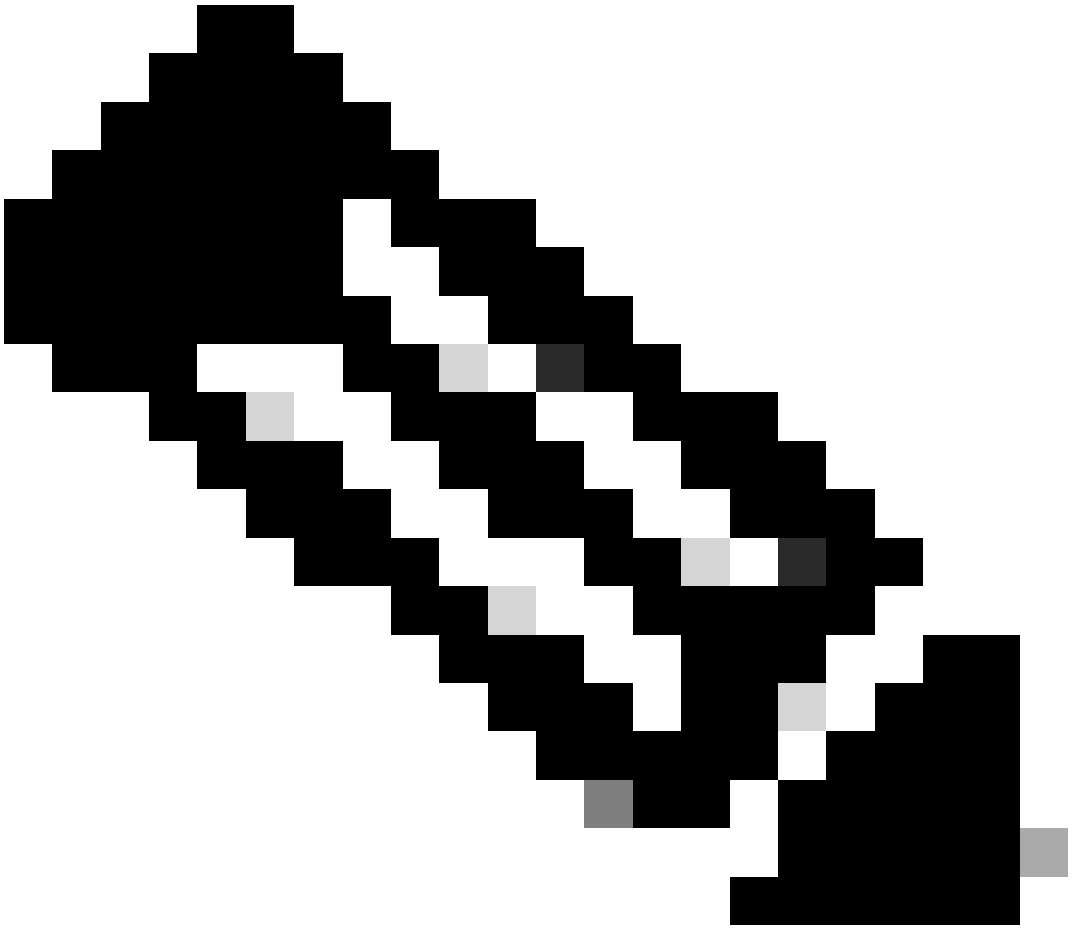
Este documento describe el procedimiento para configurar las PVLAN aisladas en los switches de Cisco Catalyst con el Catalyst OS (CatOS) o el software de Cisco IOS®.

Prerequisites

Requirements

Este documento asume que usted tiene una red que ya existe y que puede establecer la conectividad entre los diversos puertos para la adición a una VLAN privada (PVLAN). Si tiene switches múltiples, asegúrese de que el trunk entre los switches funcione correctamente y habilita las PVLAN en el trunk.

No todos los switches y las versiones de software son compatibles con PVLAN.



Nota: Algunos switches (como se especifica en la Matriz de Soporte de Switch Catalyst de VLAN Privada) actualmente soportan solamente la función PVLAN Edge. El término puertos protegidos también hace referencia a esta función. Los puertos PVLAN Edge tienen una restricción que previene la comunicación con otros puertos protegidos en el mismo switch. Los puertos protegidos en switches diferentes, sin embargo, pueden comunicarse entre sí. No confunda esta función con las configuraciones de PVLAN normales que este documento muestra. Para obtener más información sobre los puertos protegidos, consulte la sección Configuración de Seguridad del Puerto del documento Configuración del Control de Tráfico Basado en el Puerto.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 4003 switch con el módulo Supervisor Engine 2 que ejecuta CatOS version 6.3(5)
- Catalyst 4006 switch con el módulo Supervisor Engine 3 que ejecuta Cisco IOS Software Release 12.1(12c)EW1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

En algunas situaciones, debe prevenir la conectividad de la Capa 2 (L2) entre los dispositivos extremos en un switch sin la colocación de dispositivos en diversas subredes de IP. Este configuración previene la pérdida de direcciones IP. Las PVLAN permiten el aislamiento en la Capa 2 de los dispositivos en la misma subred IP. Puede restringir algunos puertos en el switch para alcanzar solamente los puertos específicos que tienen conectados un gateway predeterminado, un servidor de respaldo, o un Cisco LocalDirector.

Este documento describe el procedimiento para configurar las PVLAN aisladas en los switches Cisco Catalyst con Catalyst OS (CatOS) o Cisco IOS Software.

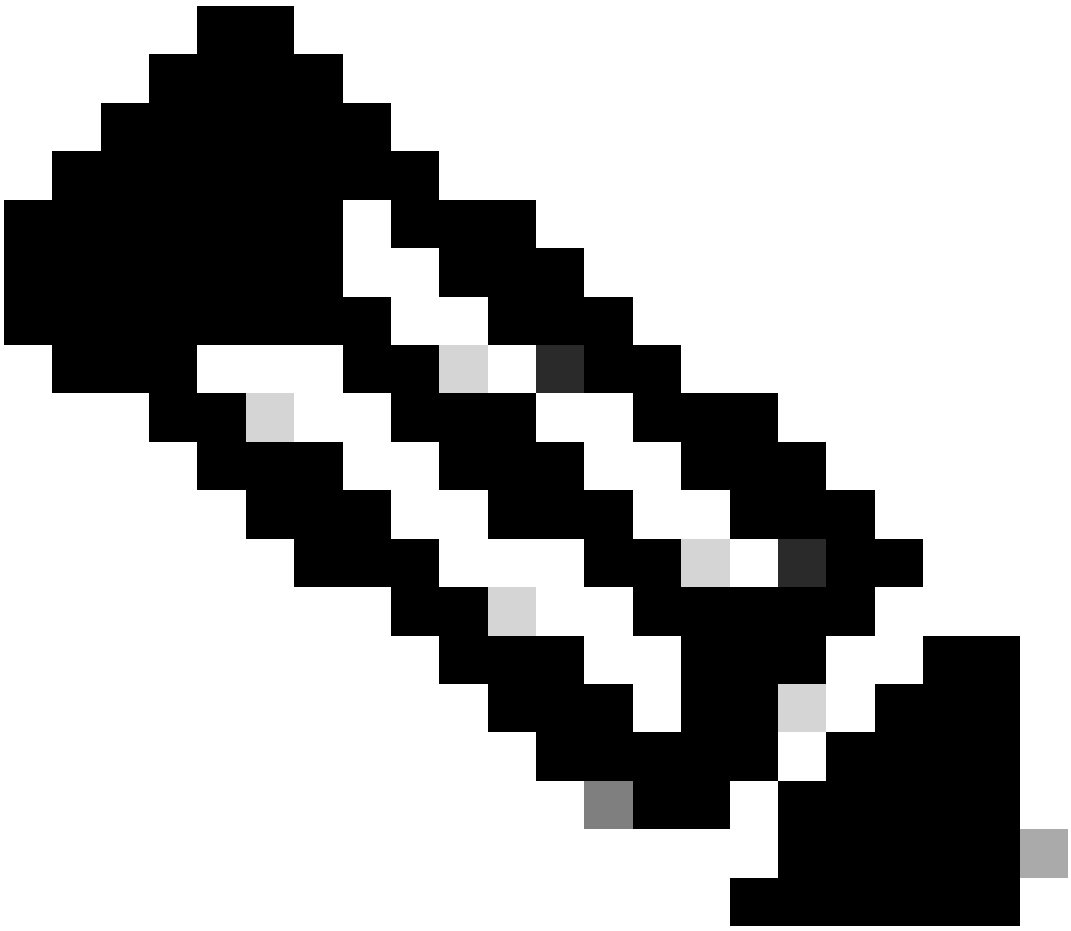
Una PVLAN es una VLAN con la configuración para el aislamiento de la Capa 2 de otros puertos dentro del mismo dominio de broadcast o subred. Puede asignar un conjunto especial de puertos dentro de una PVLAN y, así, controlar el acceso entre los puertos en la Capa 2. Puede configurar las PVLAN y las VLAN normales en el mismo switch.

Existen tres tipos de puertos PVLAN: promiscuos, aislados y de comunidad.

1. Un puerto promiscuo se comunica con el resto de los puertos PVLAN. El puerto promiscuo es el puerto que se utiliza habitualmente para comunicarse con los routers externos, los directores locales, los dispositivos de administración de redes, los servidores de respaldo, las estaciones de trabajo administrativas y otros dispositivos. En algunos switches, el puerto al módulo de la ruta (por ejemplo, Tarjeta de Función de Switch Multicapa [MSFC]) debe ser promiscuo.
2. Un puerto aislado tiene separación completa de la Capa 2 de otros puertos dentro de la misma PVLAN. Esta separación incluye los broadcasts, y la única excepción es el puerto

promiscuo. Una concesión del aislamiento en el nivel de la Capa 2 se produce con el bloqueo del tráfico saliente a todos los puertos aislados. El tráfico que se proviene de un puerto aislado se reenvía a todos los puertos promiscuos solamente.

3. Los puertos de comunidad pueden comunicarse entre sí y con los puertos promiscuos. Estos puertos tienen el aislamiento de la Capa 2 del resto de los puertos en otras comunidades, o puertos aislados dentro de la PVLAN. Las difusiones se propagan sólo entre los puertos de comunidades asociadas y en el puerto promiscuo.



Nota: Este documento no cubre la configuración de VLAN de comunidad.

Reglas y limitaciones

Esta sección proporciona algunas reglas y limitaciones que debe tener en cuenta al implementar las PVLAN.

- Las PVLAN no pueden incluir las VLAN 1 o 1002-1005.

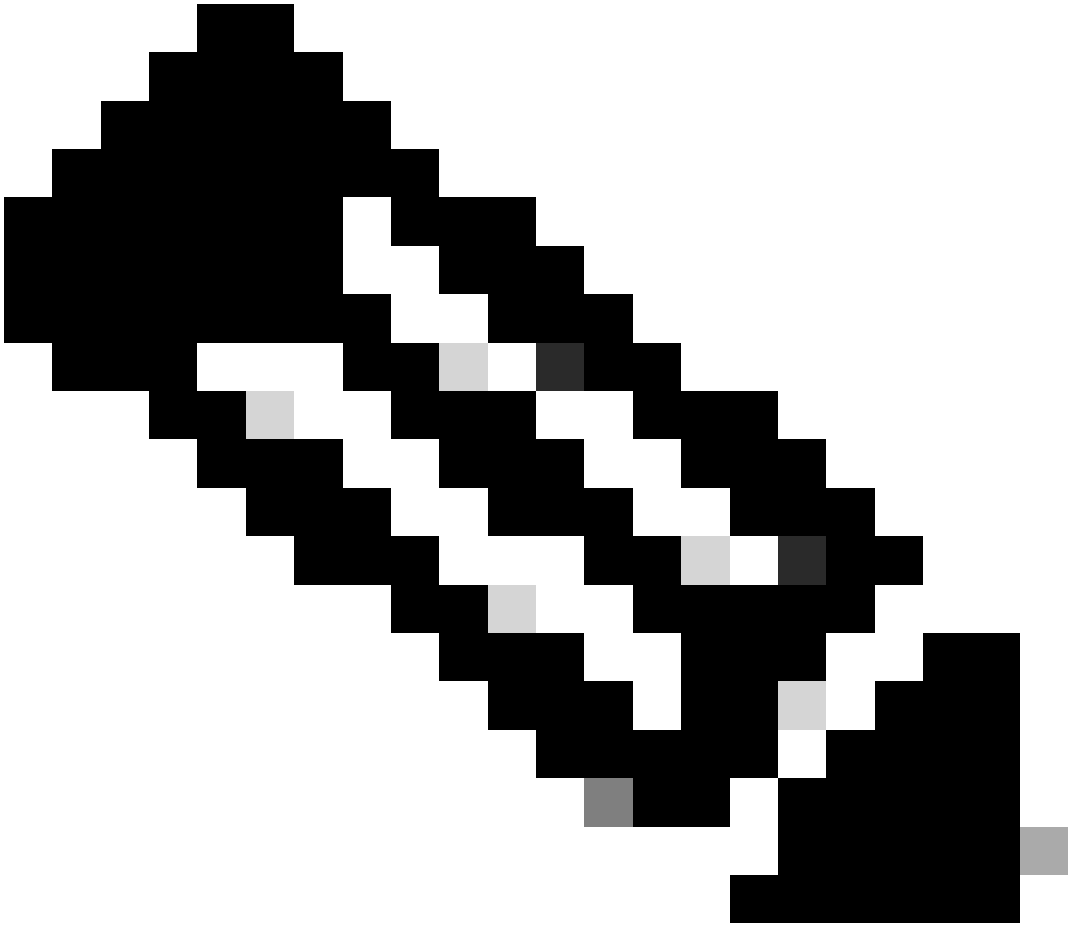
- Debe configurar el modo de VLAN Trunk Protocol (VTP) como transparente.
- Sólo puede especificar una VLAN aislada por VLAN principal.
- Puede señalar solamente una VLAN como PVLAN si esa VLAN no tiene ninguna asignación actual del puerto de acceso. Quite cualquier puerto en esa VLAN antes de que convierta la VLAN en PVLAN.
- No configure los puertos PVLAN como EtherChannels.
- Debido a las limitaciones del hardware, los módulos de switch Fast Ethernet del Catalyst 6500/6000 restringen la configuración de un puerto de VLAN de comunidad o aislada cuando un puerto dentro del mismo circuito específico de la aplicación COIL (ASIC) es uno de lo siguientes:
    - Un trunk
    - Un destino de Analizador de Puerto Conmutado (SPAN Port)
    - Un puerto promiscuo PVLAN

Esta tabla indica el rango de puertos que pertenece al mismo ASIC en los módulos de FastEthernet del Catalyst 6500/6000:

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

El comando show pvlan capability (CatOS) también indica si puede convertir a un puerto en puerto PVLAN. No hay comando equivalentes en Cisco IOS Software.

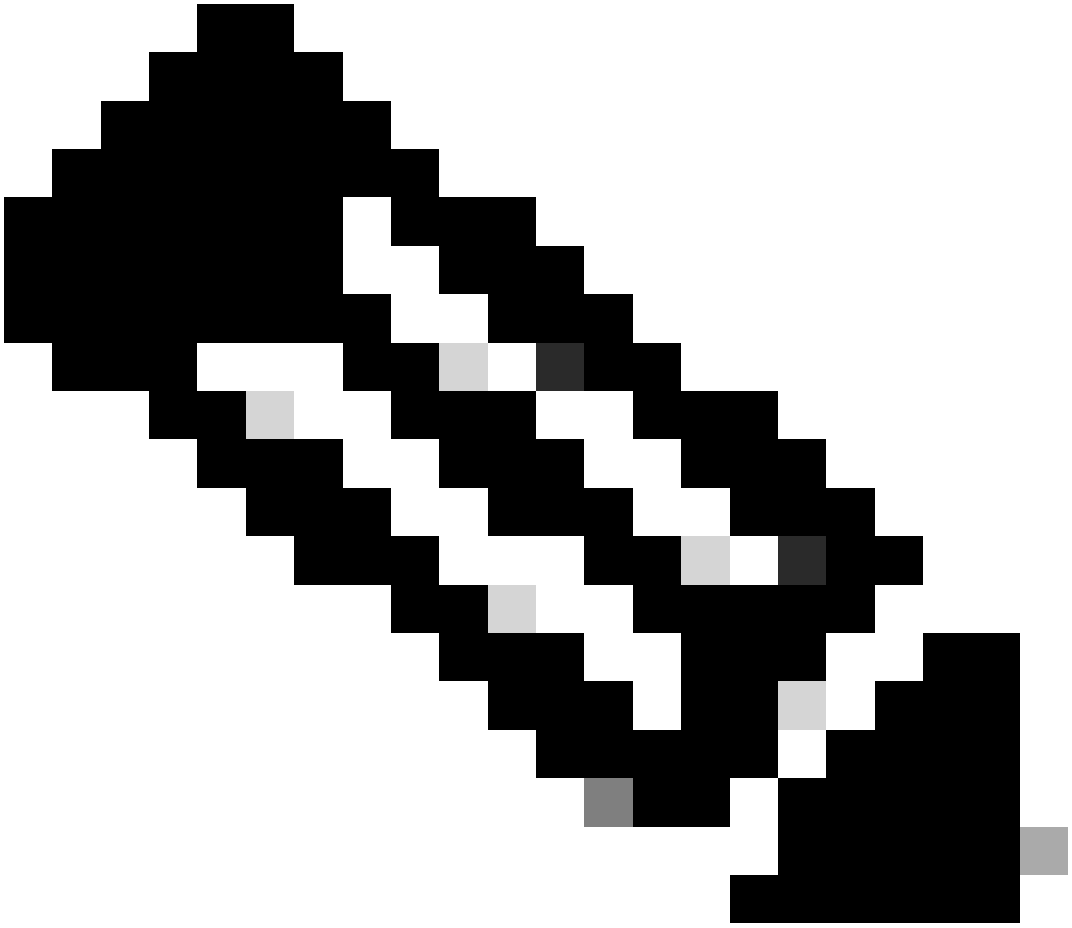
- Si borra una VLAN que utiliza en la configuración de PVLAN, los puertos que se asocian con la VLAN se vuelven inactivos.
- Configure las interfaces VLAN de la Capa 3 (L3) solamente para las VLAN principales. Las interfaces VLAN para las VLANs de comunidad y aisladas están inactivas mientras la VLAN tiene una configuración de VLAN de comunidad o aislada.
- Puede ampliar las PVLANs a través de los switches con el uso de los trunks. Los puertos trunk llevan el tráfico de las VLANs regulares y también de las VLANs de comunidad, primarias y aisladas. Cisco recomienda el uso de los puertos trunk estándar si ambos switches que experimenten el trunking soportan las PVLANs.



Nota: Debe ingresar manualmente la misma configuración PVLAN en cada switch con participación porque el VTP en modo transparente no propaga esta información.

Configurar

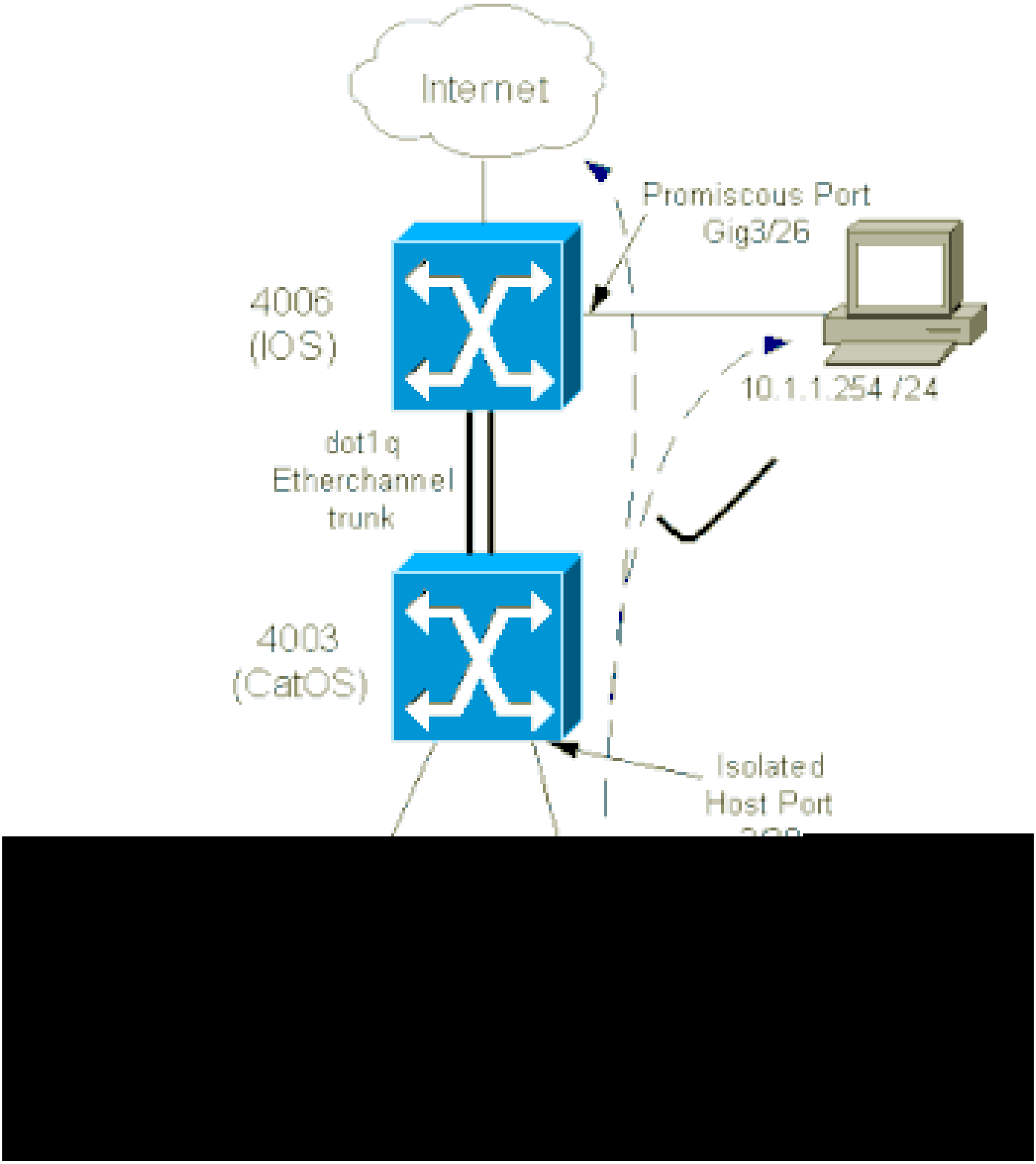
En esta sección encontrará la información para configurar las funciones descritas en este documento.



Nota: Utilice el comando Herramienta de Búsqueda para encontrar más información sobre los comandos utilizados en este documento. Solo los usuarios registrados pueden acceder a la información y las herramientas internas de Cisco.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



En este escenario, los dispositivos en la VLAN aislada (101) tienen una restricción de comunicación en la Capa 2 entre sí. Sin embargo, los dispositivos pueden conectarse con Internet. Además, el puerto Gig 3/26 en el 4006 tiene la designación promiscua. Esta configuración optativa permite que un dispositivo GigabitEthernet 3/26 se conecte con todos los dispositivos en la VLAN aislada. Esta configuración también permite, por ejemplo, realizar una copia de seguridad de los datos de todos los dispositivos host PVLAN en una estación de trabajo de administración. Otras aplicaciones para los puertos promiscuos incluyen la conexión a un router externo, a un LocalDirector, a un dispositivo de administración de red y a otros dispositivos.

Configure las VLANS Principales y Aisladas

Siga estos pasos para crear las VLANs principales y secundarias, y para unir varios puertos a estas VLANs. Los pasos incluyen ejemplos para CatOS y Cisco IOS® Software. Ejecute el comando adecuado configurado para la instalación de su sistema operativo.

1. Cree la PVLAN principal.

    - 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. Cree una o varias VLANsaisladas.

    - 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. Una la/s VLAN/s aislada/s a la VLAN principal.

- 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. Verifique la configuración de la VLAN privada.

- CatOS

<#root>

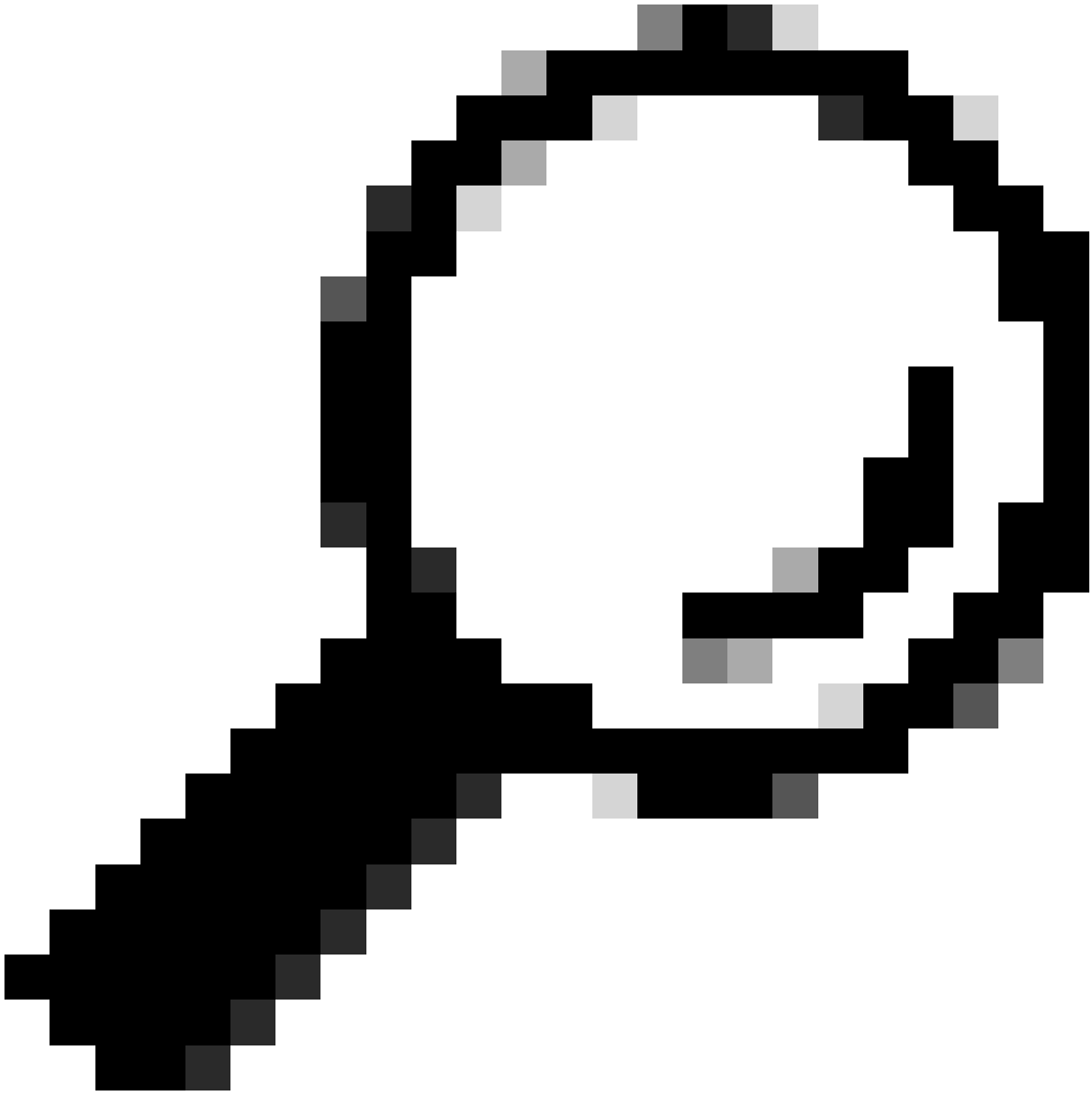
```
Switch_CatOS> (enable)
show pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
100     101       isolated
```

- Cisco IOS Software

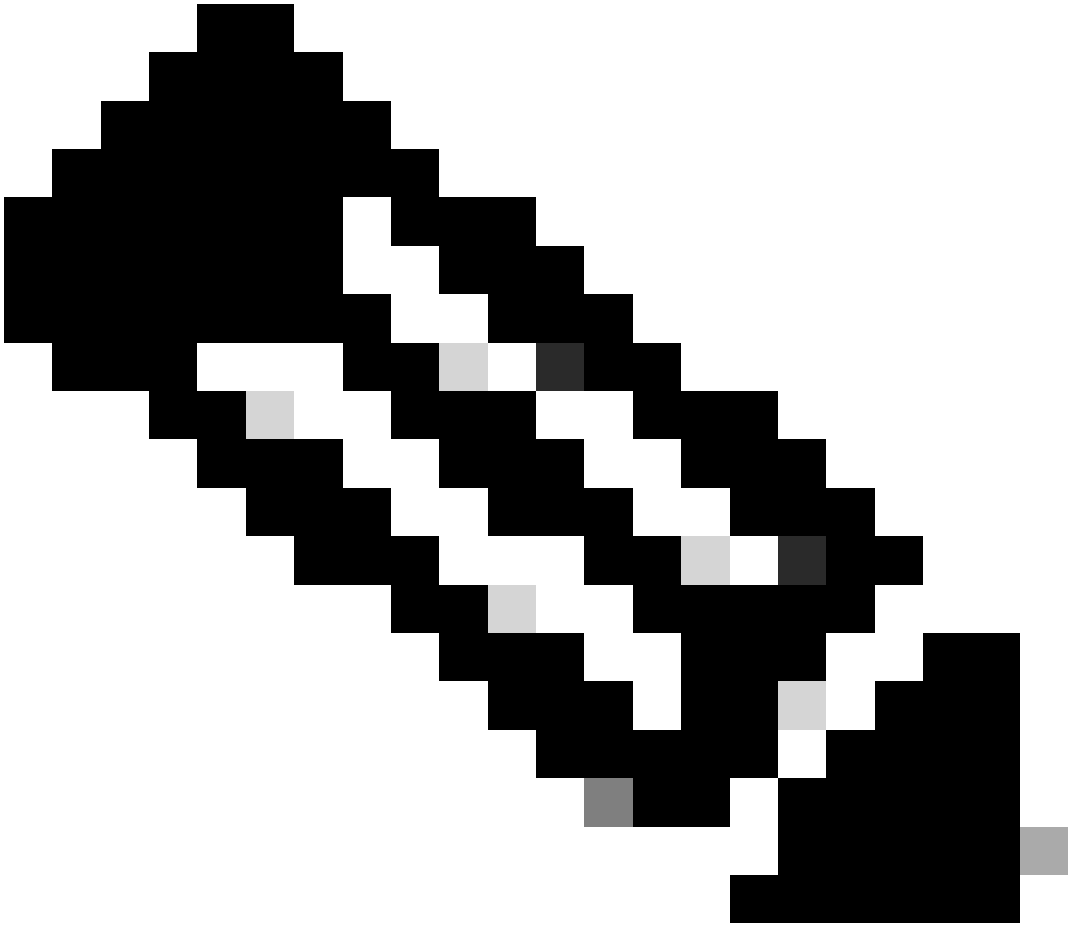
<#root>

```
Switch_IOS#
show vlan private-vlan
Primary  Secondary  Type              Ports
------- --------- ----------------- -------
100     101       isolated
```

Asigne los puertos a las PVLAN



Sugerencia: Antes de implementar este procedimiento, ejecute el`show PVLAN capability mod/port`comando (para CatOS) para determinar si un puerto puede convertirse en un puerto PVLAN.



Nota: Antes de realizar el Paso 1 de este procedimiento, ejecute el comando switchport en el modo de configuración de la interfaz para configurar el puerto como una interfaz conmutada de Capa 2.

- Configurar los puertos del host en todos los switches correspondientes.
  - 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 el puerto promiscuo en uno de los switches.
  - CatOS

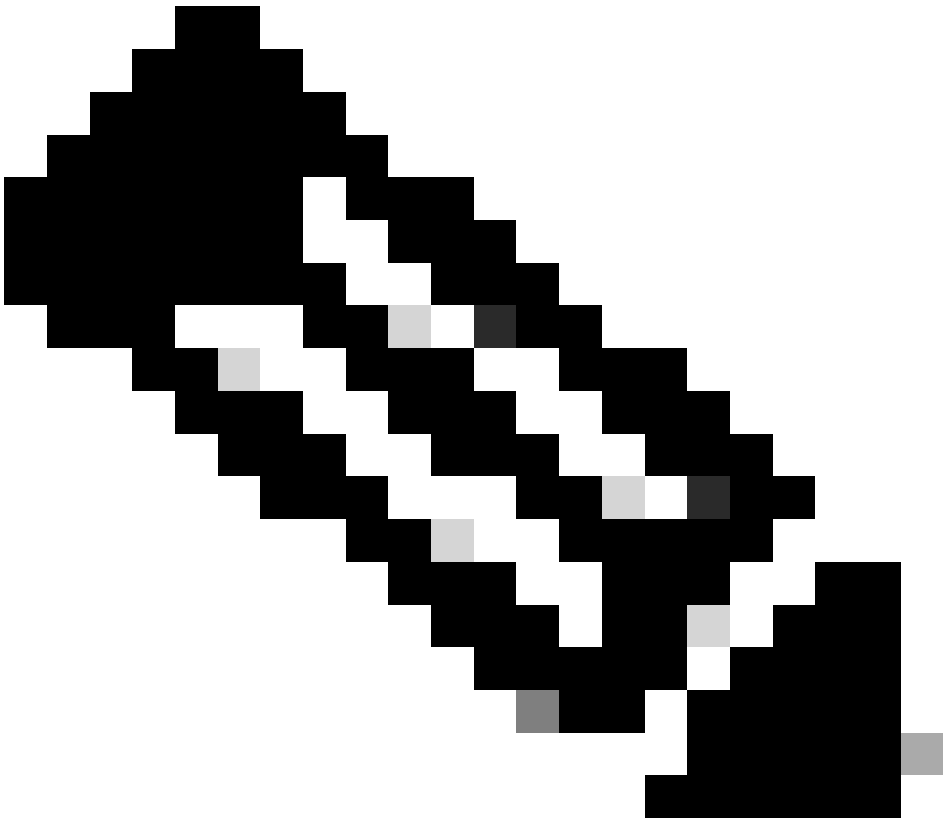
```
<#root>

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
```



Nota: Para Catalyst 6500/6000 cuando Supervisor Engine ejecuta CatOS como software del sistema, el puerto MSFC en Supervisor Engine (15/1 o 16/1) debe ser promiscuo si desea conmutar la Capa 3 entre las VLAN.

- 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
```

Configuración de capa 3

Esta sección opcional describe los pasos de configuración para permitir la ruta del tráfico de ingreso PVLAN. Si necesita solamente habilitar la conectividad de la Capa 2, puede omitir esta fase.

1. Configure la interfaz VLAN de la misma manera que configura el ruteo habitual de la Capa 3.

   Esta configuración incluye:

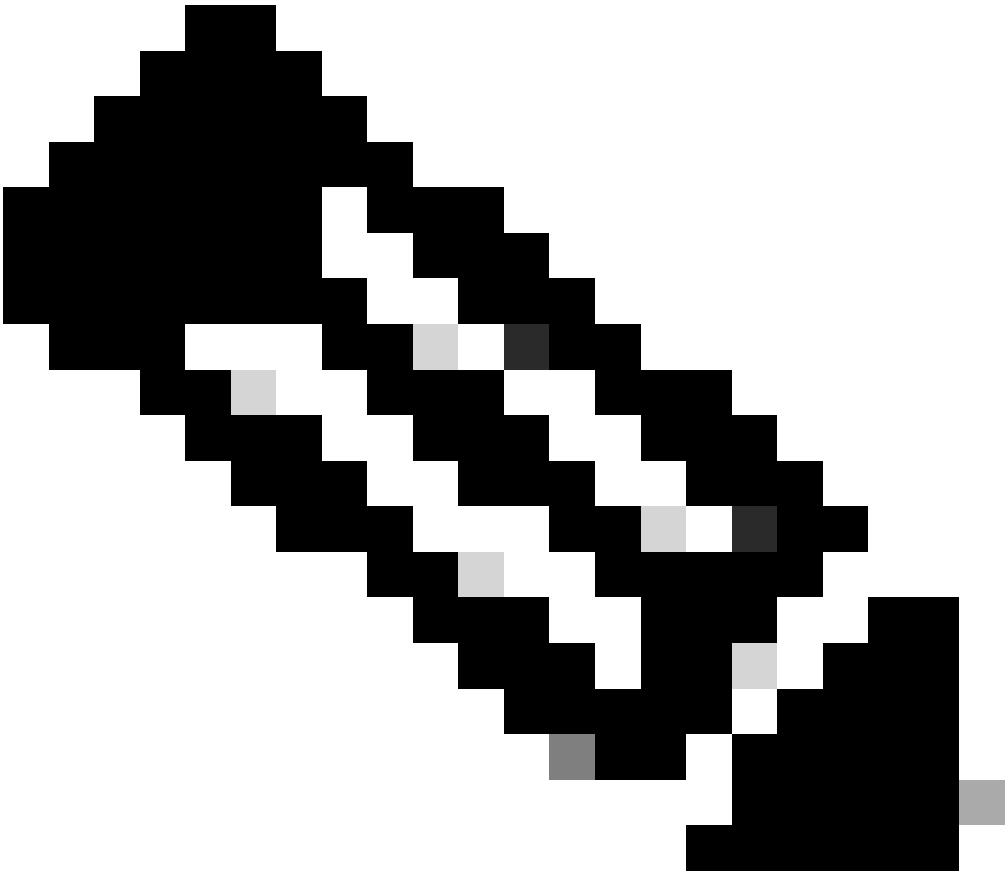
   - Configuración de una dirección IP
   - Activación de la interfaz con el comando no shutdown
   - Verificación que la VLAN existe en las bases de datos de VLAN

   Consulte Soporte Técnico de VLANs/VTP para obtener ejemplos de configuración.

2. Mapee las VLANs secundarias que desea rutear con la VLAN principal.

```
<#root>
Switch_IOS(config)#
interface vlan primary_vlan_id
Switch_IOS(config-if)#
private-vlan mapping secondary_vlan_list

Switch_IOS(config-if)#
end
```



Nota: Configure las interfaces VLAN de Capa 3 solamente para las VLAN primarias. Las interfaces VLAN para las VLANs de comunidad y aisladas están inactivas con una configuración de VLAN de comunidad o aislada.

3. Ejecute el comando show interfaces private-vlan mapping (Cisco IOS Software) o el comando show pvlan mapping (CatOS) para verificar el mapping.
4. Si necesita modificar la lista de VLAN secundaria después de la configuración de mapping, utilice la palabra clave add o remove.

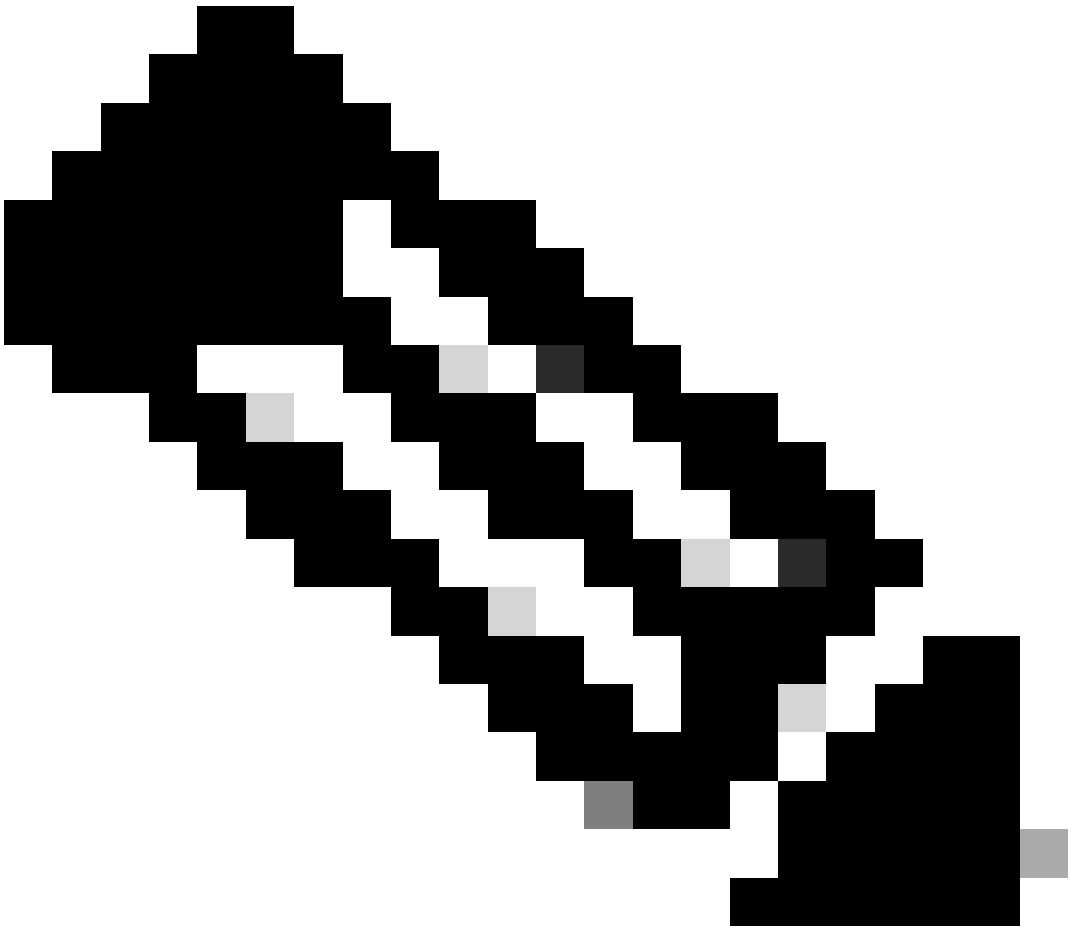
<#root>

```
Switch_IOS(config-if)#
```

private-vlan mapping add secondary_vlan_list

```
or
Switch_IOS(config-if)#
```

private-vlan mapping remove secondary_vlan_list



Nota: Para los switches Catalyst 6500/6000 con MSFC, asegúrese de que el puerto del Supervisor Engine al motor de ruteo (por ejemplo, el puerto 15/1 o 16/1) sea promiscuo.

<#root>

```
cat6000> (enable)
set pvlan mapping primary_vlan secondary_vlan 15/1
Successfully set mapping between 100 and 101 on 15/1
```

Ejecute el comando show pvlan mapping para verificar la correlación.

<#root>

```
cat6000> (enable)
```

```
show pvlan mapping

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

Configuraciones

En este documento, se utilizan estas configuraciones:

- Capa_acceso (Catalyst 4003: CatOS)
- Núcleo (Catalyst 4006: Cisco IOS Software)

Capa_acceso (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
```

Núcleo (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.
```

VLANs privadas a través de switches múltiples

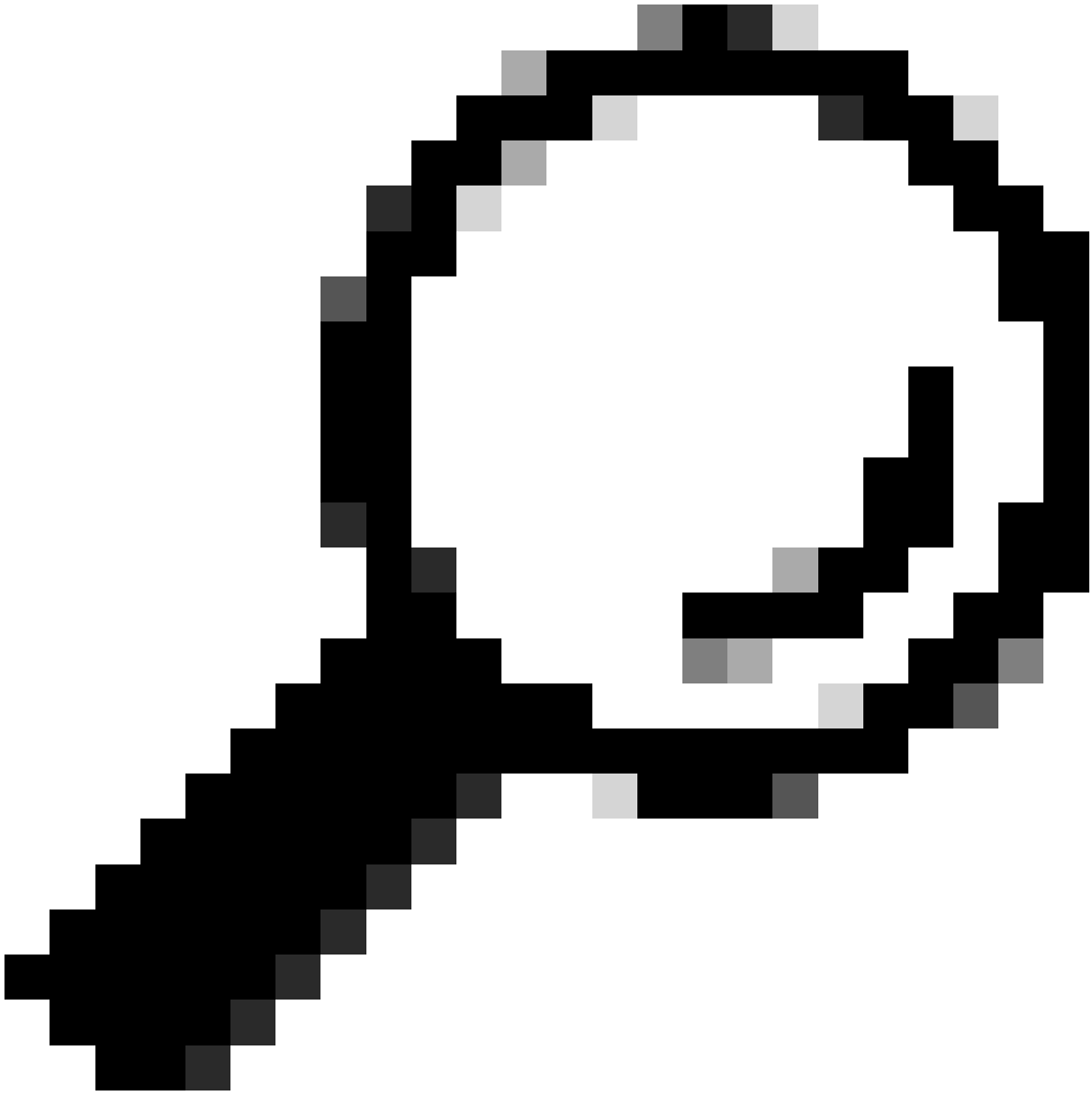
Las VLANs privadas se pueden tomar a través de switches múltiples con dos métodos. Esta sección discute estos métodos:

- Trunks Regulares
- Trunks de VLAN Privada

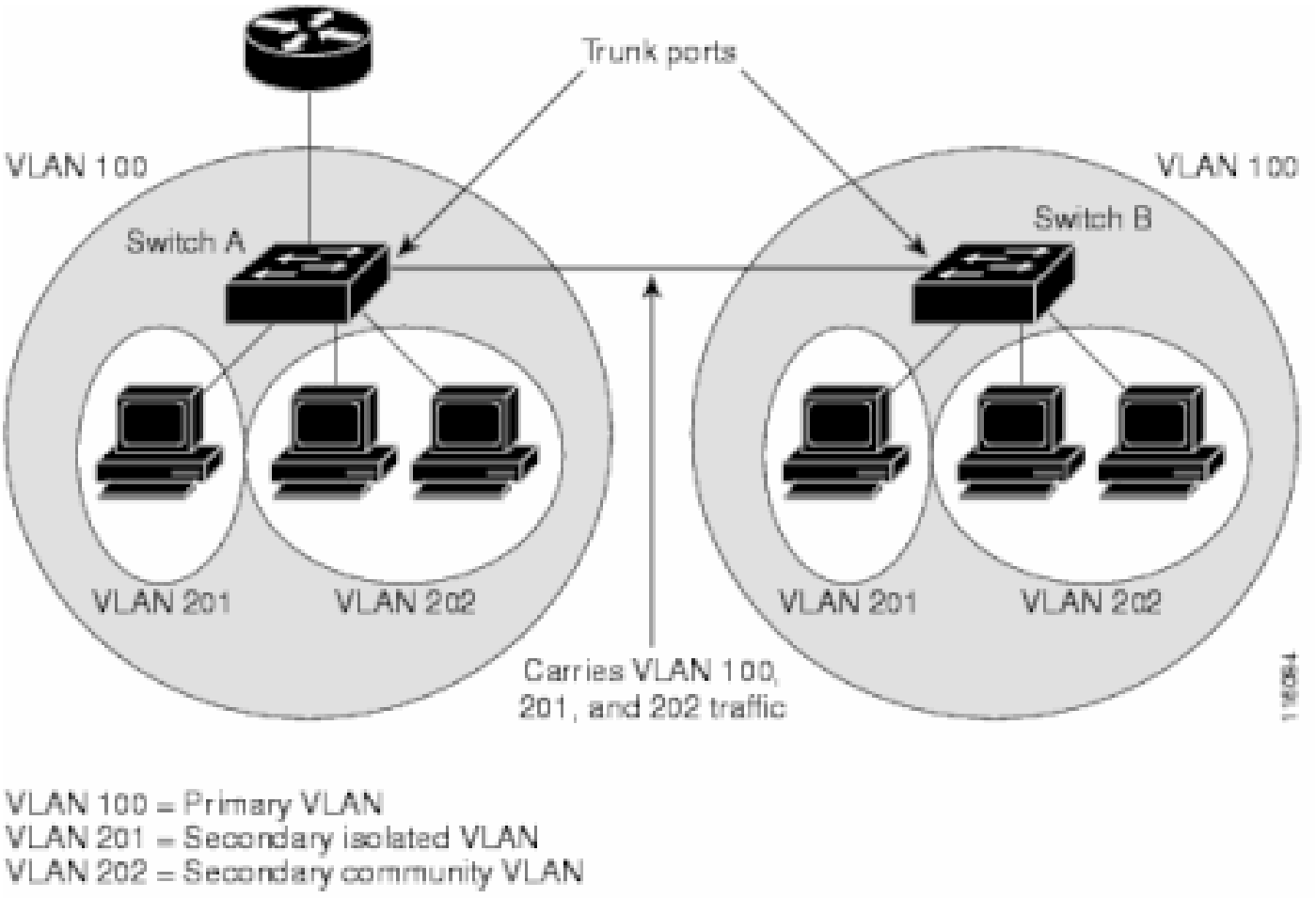
Trunks Regulares

Como con las VLANs regulares, las PVLAN pueden atravesar los switches múltiples. Un puerto trunk lleva la VLAN principal y las VLANs secundarias a un switch vecino. El puerto trunk trata la VLAN privada como cualquier otra VLAN. Una función de las PVLAN a través de los switches múltiples es que el tráfico de un puerto aislado en un switch no alcanza un puerto aislado en otro switch.

Configure las PVLAN en todos los dispositivos intermedios, que incluyen los dispositivos que no tienen ningún puerto PVLAN, para mantener la seguridad de su configuración de PVLAN y evitar otro uso de las VLANs configuradas como PVLANs. Los puertos troncales transportan el tráfico de las VLAN regulares y también de las VLAN primarias, aisladas y de comunidad.



Consejo: Cisco recomienda el uso de puertos troncales estándar si ambos switches que se someten a trunking soportan PVLAN.



Configuración manual de PVLAN en todos los switches de la red de capa 2

Debido a que el VTP no soporta las PVLANs, debe configurar manualmente las PVLANs en todos los switches en la red de la Capa 2. Si no configura la asociación de VLAN primaria y secundaria en algunos switches en la red, las bases de datos de la Capa 2 en estos switches no se combinan. Esta situación puede dar lugar a la inundación innecesaria del tráfico PVLAN en esos switches.

Trunks de VLAN Privada

Un puerto trunk PVLAN puede transportar varias PVLANS secundarias y VLANs que no sean PVLANs. Los paquetes se reciben y se transmiten con etiquetas VLANs secundarias o regulares en los puertos trunk de PVLAN.

Solamente se soporta la encapsulación del IEEE 802.1Q. Los puertos trunk aislados permiten que combine el tráfico para todos los puertos secundarios sobre un trunk. Los puertos trunk promiscuos permiten que combine los puertos promiscuos múltiples requeridos en esta topología en un solo puerto trunk que transportan VLANs principales múltiples.

Utilice los puertos trunk de VLAN Privada cuando anticipa el uso de los puertos de host DE VLAN privada para transportar las VLAN múltiples, las VLAN normales o para los dominios múltiples de VLAN Privada. Esto facilita la conexión de un switch descendente que no soporta VLANs Privadas.

Los Trunks Promiscuos de VLAN Privada se utilizan en las situaciones donde un puerto de host promiscuo de VLAN Privada se utiliza normalmente pero cuando es necesario transportar VLAN múltiples, vlans normales o para los dominios múltiples de VLAN privada. Esto facilita la conexión a un router ascendente que no soporte las VLAN privadas.

Additional Information

Consulte los Trunks de VLAN Privada para obtener más información.

Para configurar una interfaz como puerto troncal PVLAN, consulte Configuración de una Interfaz de Capa 2 como puerto troncal PVLAN .

Para configurar una interfaz como puerto trunk promiscuo, consulte Configuración de una Interfaz de Capa 2 como Puerto Trunk Promiscuo .

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

CatOS

- show pvlan—Muestra la configuración de PVLAN. Verifique que las VLAN principales y aisladas estén asociadas. También, verifique si aparecen puertos host.
- show pvlan mapping: muestra el mapping de PVLAN con la configuración en los puertos promiscuos.

Cisco IOS Software

- show vlan private-vlan: muestra la información de PVLAN, que incluye puertos que se asocian.
- show interfacemod/portswitchport—Muestra información específica de la interfaz. Verifique que el modo de operación y las configuraciones operativas PVLAN sean correctas.
- show interfaces private-vlan mapping: muestra el mapping de PVLAN que ha configurado.

Procedimiento de verificación

Complete estos pasos:

1. Verifique la configuración de PVLAN en los switches.

   Verifique para determinar si las PVLAN principales y secundarias se asocian/mapean. También, verifique la inclusión de los puertos necesarios.

   <#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. Verifique la configuración correcta del puerto promiscuo.

   Este resultado indica que el modo de operación del puerto es promiscuo y que las VLANs operativas son 100 y 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. Inicie un paquete ping del Protocolo de control de mensaje de Internet (ICMP) desde el puerto host hacia el puerto promiscuo.

   Tenga presente que, puesto que ambos dispositivos están en la misma VLAN principal, los dispositivos deben estar en la misma subred.

```
<#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. Inicie un ping de ICMP entre los puertos de host.

   En este ejemplo, `host_port_2` (10.1.1.99) intenta hacer ping a > `host_port` (10.1.1.100). Este ping falla. Sin embargo, el ping de otro puerto de host al puerto promiscuo aún es exitoso.

```
<#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

Troubleshooting de PVLAN

Esta sección aborda algunos problemas comunes que se producen con las configuraciones de PVLAN.

Problema 1

Recibe este mensaje de error: "`%PM-SP-3-ERR_INCOMP_PORT: <mod/port> está configurado como inactivo porque <mod/port> es un puerto trunk.`"

Este mensaje de error puede generarse por diferentes razones, según lo discutido aquí.

Explicación - 1

Debido a las limitaciones del hardware, los módulos de Catalyst 6500/6000 10/100-Mbps restringen la configuración de un puerto de VLAN de comunidad o aislada cuando un puerto dentro del mismo ASIC COIL es un trunk, un destino de SPAN, o un puerto promiscuo PVLAN. (El ASIC COIL controla 12 puertos en la mayoría de los módulos y 48 puertos en el módulo Catalyst 6548). La tabla en la sección Reglas y Limitaciones de este documento proporciona una

descripción de la restricción del puerto en los módulos de Catalyst 6500/6000 10/100-Mbps.

Procedimiento de resolución - 1

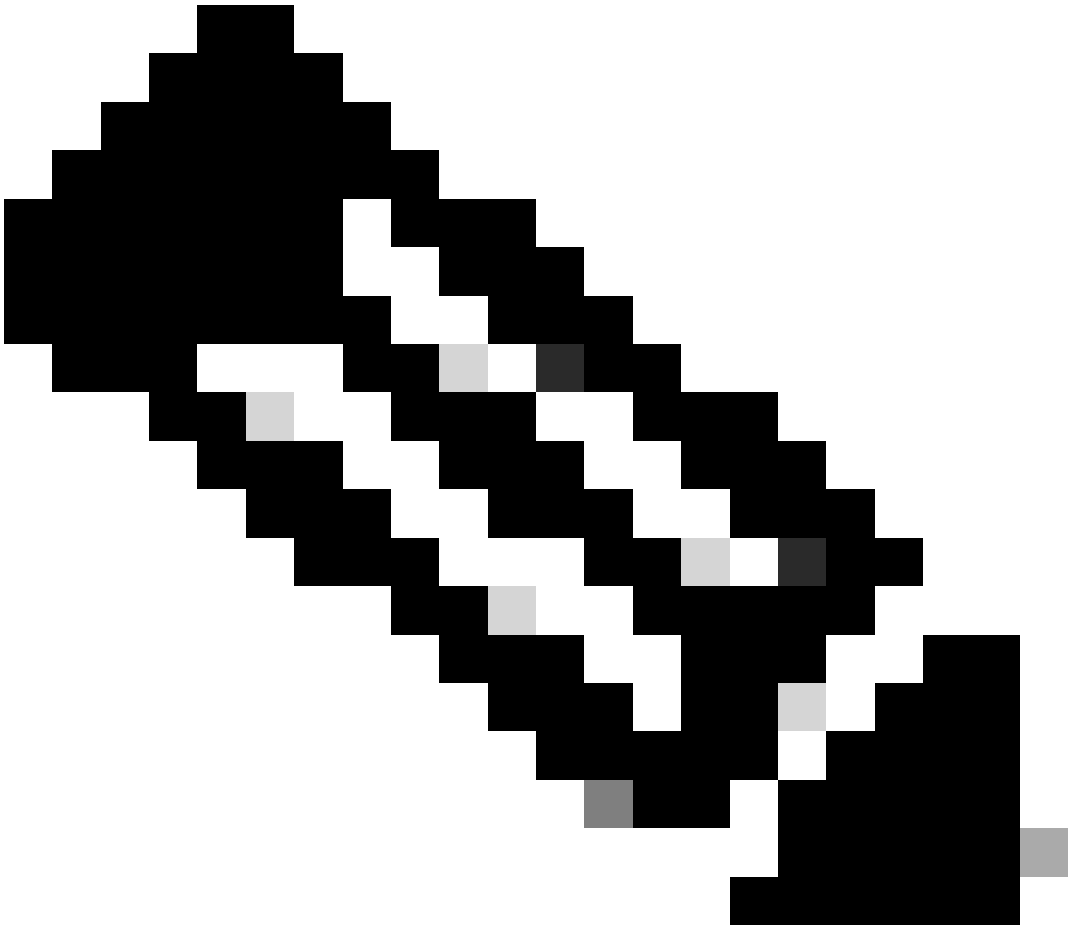
Si no hay soporte para la PVLAN en ese puerto, escoja un puerto en un ASIC diferente en el módulo o en otro módulo. Para reactivar los puertos, quite la configuración del puerto de VLAN de comunidad o aislada y ejecute el comando shutdown y el comando no shutdown.

Explicación - 2

Si los puertos se configuran manualmente o de forma predeterminada al modo deseable o al modo automático dinámico.

Procedimiento de resolución - 2

Configure los puertos como modo de acceso con el comando switchport mode access. Para reactivar los puertos, ejecute el comando shutdown y el comando no shutdown.



Nota: En Cisco IOS Software Release 12.2(17a)SX y versiones posteriores, la restricción

---

de 12 puertos no se aplica a los módulos de switching Ethernet WS-X6548-RJ-45, WS-X6548-RJ-21 y WS-X6524-100FX-MM.

Problema 2

Durante la configuración de PVLAN, obtiene uno de estos mensajes:

```
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>
```

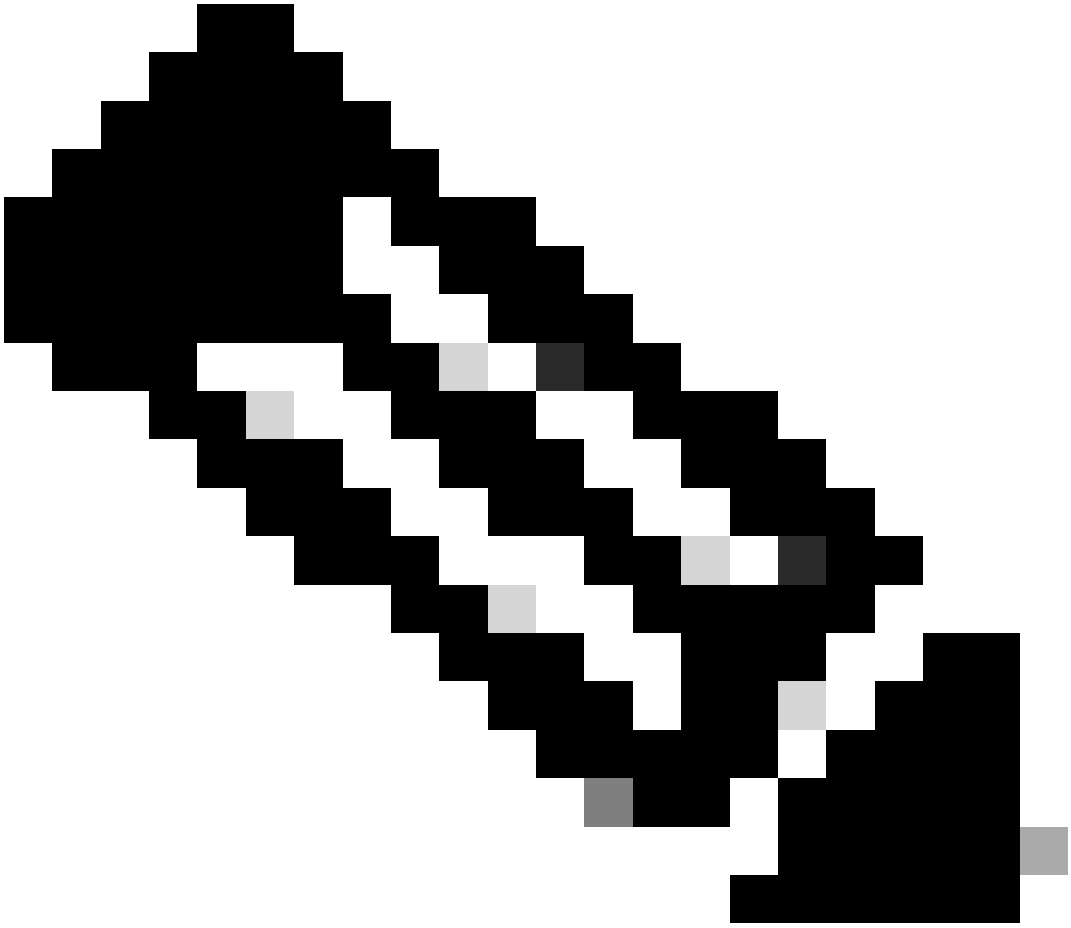
```
Port with another Promiscuous port in the same ASIC cannot be made
Private port.
Failed to add ports to association.
```

Explicación

Debido a las limitaciones del hardware, los módulos de Catalyst 6500/6000 10/100-Mbps restringen la configuración de un puerto de VLAN de comunidad o aislada cuando un puerto dentro del mismo ASIC COIL es un trunk, un destino de SPAN, o un puerto promiscuo PVLAN. (El ASIC COIL controla 12 puertos en la mayoría de los módulos y 48 puertos en el módulo Catalyst 6548). La tabla en la sección Reglas y Limitaciones de este documento proporciona una descripción de la restricción del puerto en los módulos de Catalyst 6500/6000 10/100-Mbps.

Procedimiento de resolución

Ejecute el comando show pvlan capability (CatOS), que indica si un puerto puede convertirse en un puerto PVLAN. Si no hay soporte para la PVLAN en ese puerto determinado, escoja un puerto en un ASIC diferente en el módulo o en otro módulo.



Nota: En Cisco IOS Software Release 12.2(17a)SX y versiones posteriores, la restricción de 12 puertos no se aplica a los módulos de switching Ethernet WS-X6548-RJ-45, WS-X6548-RJ-21 y WS-X6524-100FX-MM.

Problema 3

No puede configurar PVLAN en algunas plataformas.

Resolución

Verifique que la plataforma soporte las PVLANs. Consulte Matriz de Soporte del Switch Catalyst de VLAN Privada para determinar si su plataforma y versión de software soportan las PVLANs antes de comenzar con la configuración.

Problema 4

En un Catalyst 6500/6000 MSFC, no puede hacer ping a un dispositivo que se conecta con el

puerto aislado en el switch.

Resolución

En Supervisor Engine, verifique que el puerto al MSFC (15/1 o 16/1) sea promiscuo.

<#root>

```
cat6000> (enable)
set pvlan mapping primary_vlan secondary_vlan 15/1
Successfully set mapping between 100 and 101 on 15/1
```

También, configure la interfaz VLAN en el MSFC como especifica la sección Configuración de Capa 3 de este documento.

Problema 5

Con la aplicación el comando no shutdown, no puede activar la interfaz VLAN para VLANs de comunidad o aisladas.

Resolución

Debido a la naturaleza de las PVLAN, no es posible activar la interfaz de VLAN para VLAN aisladas o comunitarias. Puede activar solamente la interfaz VLAN que pertenece a la VLAN principal.

Problema 6

En los dispositivos Catalyst 6500/6000 con MSFC/MSFC2, las entradas ARP aprendidas en las interfaces PVLAN de la Capa 3 no envejecen.

Resolución

Las entradas ARP que se aprenden en las interfaces de VLAN privada de la Capa 3 son entradas ARP permanentes y no envejecen. La conexión del nuevo equipo con la misma dirección IP genera un mensaje, y no hay creación de la entrada ARP. En consecuencia, debe eliminar en forma manual las entradas ARP del puerto PVLAN si una dirección MAC cambia. Para agregar o quitar las entradas ARP PVLAN manualmente, ejecute estos comandos:

<#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
```

Otra opción es ejecutar el comando no ip sticky-arp en el Cisco IOS Software Release 12.1(11b)E y posterior.

Información Relacionada

- Redes seguras con PVLAN y VACL
- Soporte de Tecnología de LAN Switching
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).