Configurar VLANs privadas isoladas em Switches Catalyst

Contents

Introdução

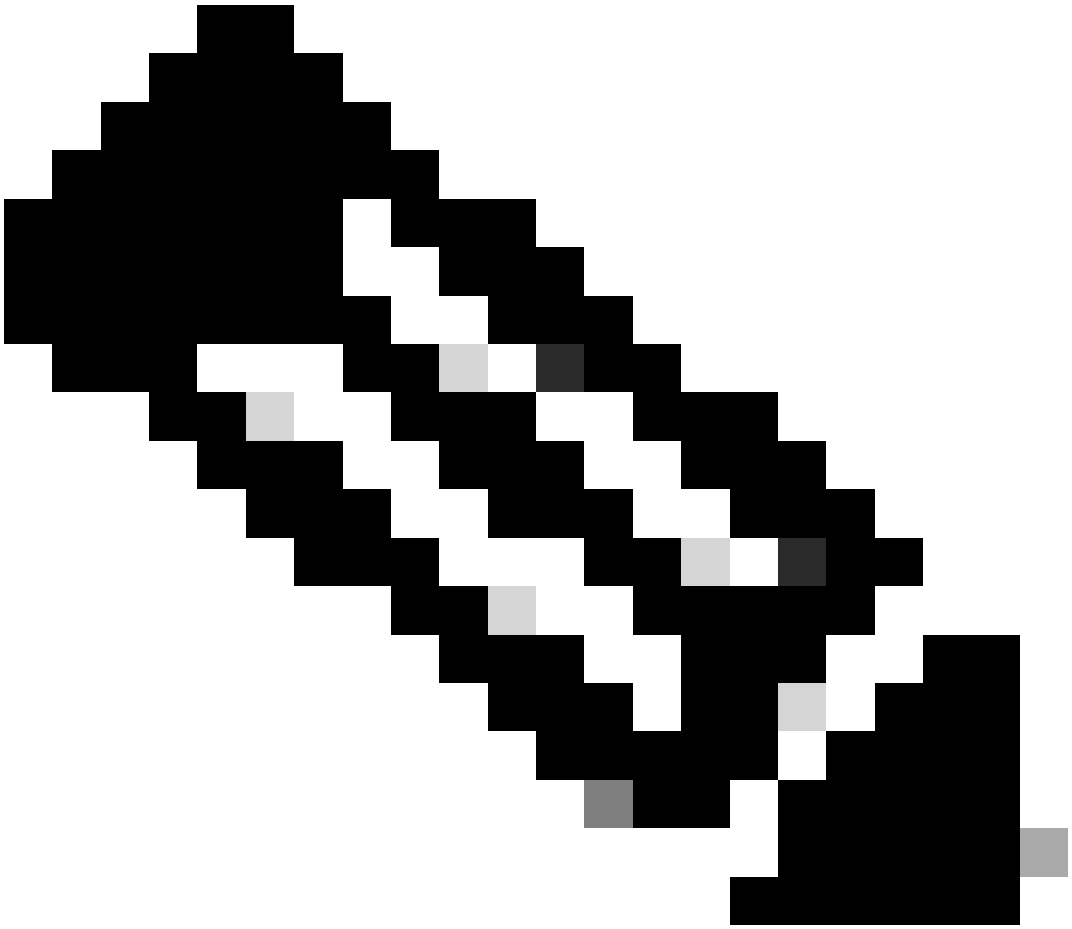
Este documento descreve o procedimento para configurar PVLANs isoladas em switches Cisco Catalyst com Catalyst OS (CatOS) ou Cisco IOS® Software.

Pré-requisitos

Requisitos

Este documento pressupõe que você tenha uma rede que já existe e seja capaz de estabelecer conectividade entre as várias portas para adição a uma PVLAN. Se você tiver vários switches, certifique-se de que o tronco entre os switches funcione corretamente e permita as PVLANs no tronco.

Nem todos os switches e versões de software oferecem suporte a PVLAN.



Observação: alguns switches (conforme especificado na Matriz de Suporte do Switch Catalyst da VLAN Privada) suportam atualmente apenas o recurso PVLAN Edge. O termo "portas protegidas" também se refere a esse recurso. As portas de borda PVLAN têm uma restrição que impede a comunicação com outras portas protegidas no mesmo switch. As portas protegidas em switches separados, no entanto, podem se comunicar entre si. Não confunda esse recurso com as configurações PVLAN normais mostradas neste documento. Para obter mais informações sobre portas protegidas, consulte a seção Configuração da Segurança de Porta do documento Configuração do Controle de Tráfego Baseado em Porta.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Switch Catalyst 4003 com módulo Supervisor Engine 2 que executa o CatOS versão 6.3(5)
- Switch Catalyst 4006 com módulo Supervisor Engine 3 que executa o Cisco IOS Software Release 12.1(12c)EW1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Em algumas situações, é necessário impedir a conectividade da Camada 2 (L2) entre dispositivos finais em um switch sem a colocação dos dispositivos em sub-redes IP diferentes. Esta instalação impede o desperdício de endereços IP. As VLAN Privadas (PVLAN) permitem o isolamento na Camada 2 de dispositivos na mesma sub-rede IP. É possível restringir algumas portas no switch para se obter apenas algumas portas específicas que têm um gateway padrão, um servidor de backup ou um Cisco LocalDirector integrado.

Este documento descreve o procedimento para configurar PVLANs isoladas em switches Cisco Catalyst com Catalyst OS (CatOS) ou Cisco IOS Software.

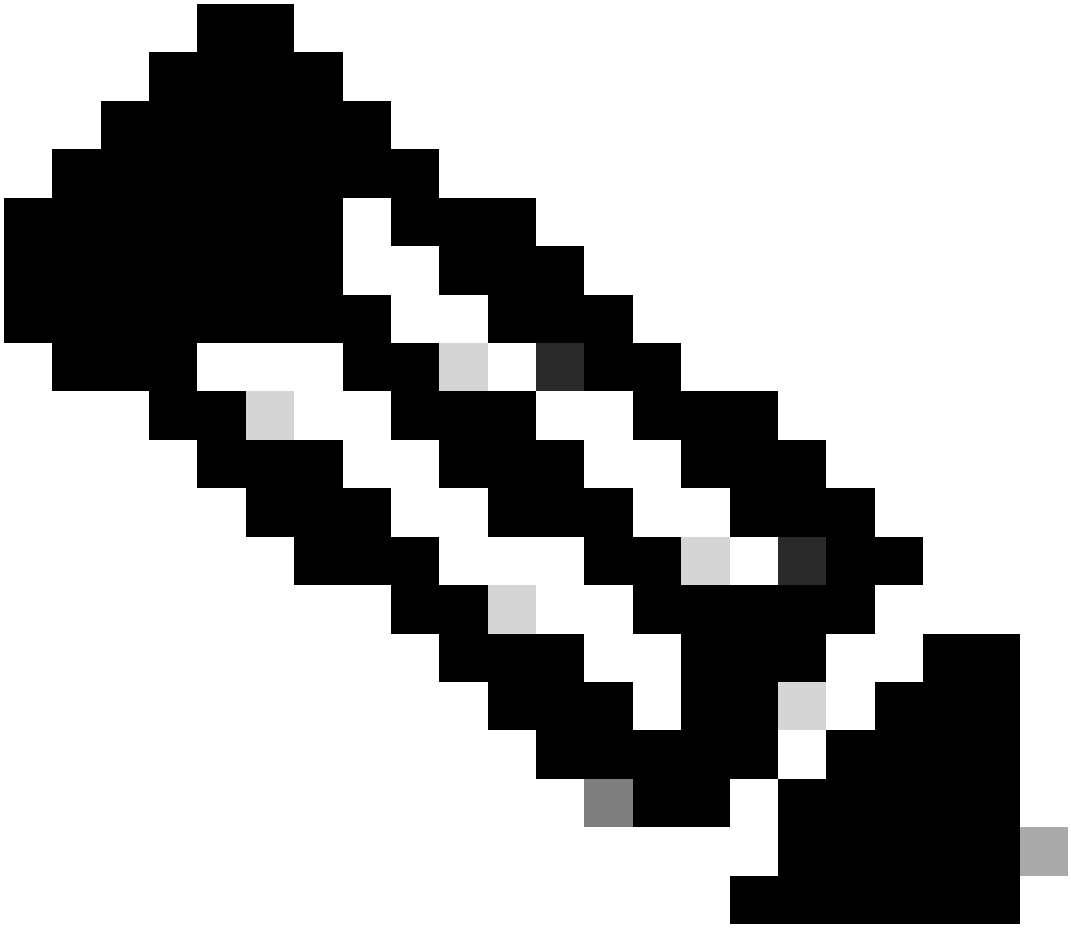
Uma PVLAN é uma VLAN com configuração para isolamento de Camada 2 de outras portas dentro do mesmo domínio de broadcast ou sub-rede. Você pode atribuir um conjunto específico de portas em uma PVLAN e, assim, controlar o acesso entre as portas na Camada 2. Você pode configurar PVLANs e VLANs normais no mesmo switch.

Há três tipos de portas PVLAN: promíscuas, isoladas e comunitárias.

- Uma porta misturada se comunica com todas as outras portas PVLAN. A porta promíscua é a porta que você normalmente usa para se comunicar com roteadores externos, LocalDirectors, dispositivos de gerenciamento de rede, servidores de backup, estações de trabalho administrativas e outros dispositivos. Em alguns switches, a porta para o módulo de rota (por exemplo, Multilayer Switch Feature Card [MSFC]) precisa ser promíscua.
- Uma porta isolada tem separação completa da Camada 2 de outras portas dentro da mesma PVLAN. Essa separação inclui broadcasts e a única exceção é a porta misturada. Uma concessão de privacidade no nível da Camada 2 ocorre com o bloqueio do tráfego de saída para todas as portas isoladas. O tráfego proveniente de uma porta isolada é

encaminhado somente para todas as portas promíscuas.

- Os portos comunitários podem comunicar entre si e com os portos promíscuos. Essas portas têm isolamento de Camada 2 de todas as outras portas em outras comunidades ou portas isoladas dentro da PVLAN. As difusões são propagadas apenas entre as portas de comunidade associadas e a porta heterogênea (sem restrições).



Observação: este documento não aborda a configuração da comunidade VLAN.

Regras e limitações

Esta seção fornece algumas regras e limitações que você deve observar ao implementar PVLANs.

- As PVLANs não podem incluir as VLANs 1 ou 1002-1005.
- Você deve definir o modo do VLAN Trunk Protocol (VTP) como `transparente`.

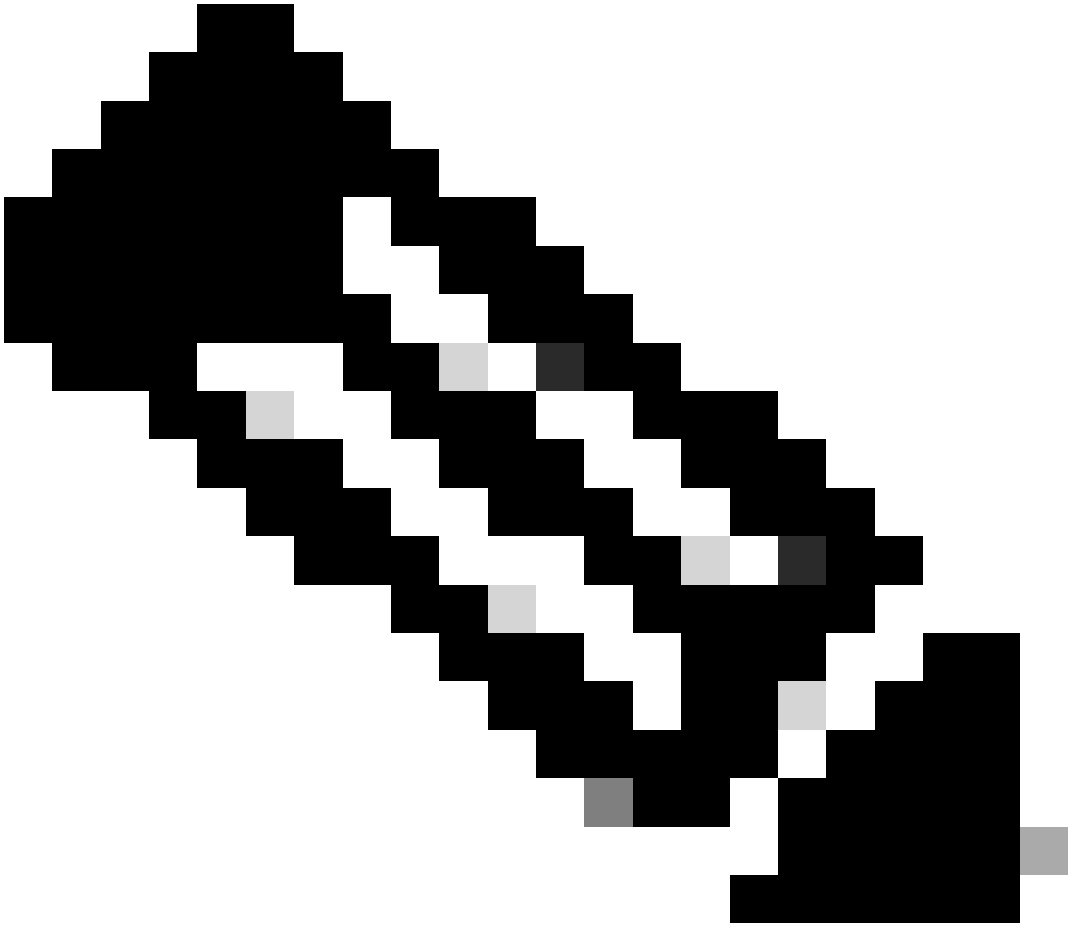
- Você só pode especificar uma VLAN isolada por VLAN primária.
- Você só pode designar uma VLAN como uma PVLAN se essa VLAN não tiver atribuições de porta de acesso atuais. Remova todas as portas dessa VLAN antes de tornar a VLAN uma PVLAN.
- Não configure portas PVLAN como EtherChannels.
- Devido a limitações de hardware, os módulos de switch Fast Ethernet do Catalyst 6500/6000 restringem a configuração de uma porta VLAN isolada ou de comunidade quando uma porta dentro do mesmo circuito integrado específico da aplicação (ASIC) do COIL é uma destas:
    - Um tronco
    - Um destino do Switched Port Analyzer (SPAN)
    - Uma porta PVLAN misturada

  Esta tabela indica o intervalo de portas que pertencem ao mesmo ASIC nos módulos FastEthernet do Catalyst 6500/6000:

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

O comando show pvlan capability (CatOS) também indica se você pode tornar uma porta PVLAN. Não há nenhum comando equivalente no Cisco IOS Software.

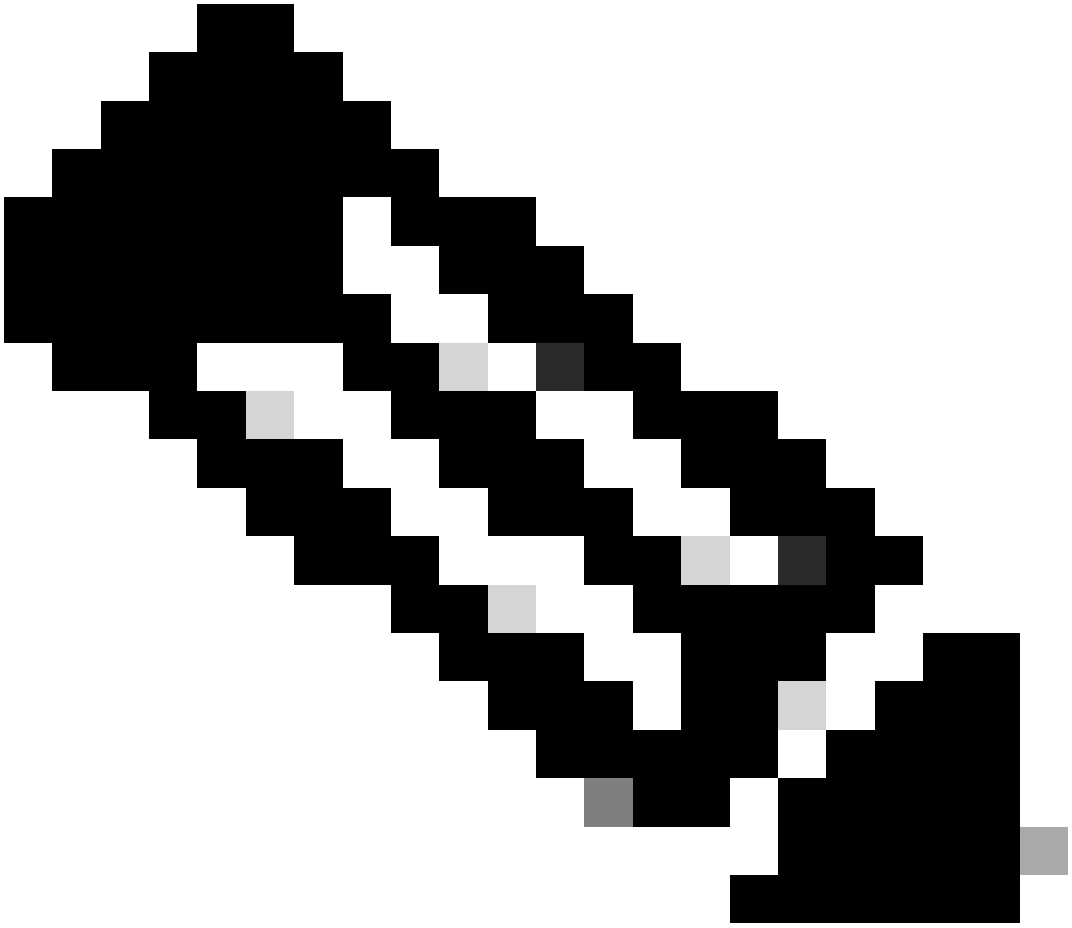
- Se você excluir uma VLAN usada na configuração PVLAN, as portas associadas à VLAN ficarão inativas.
- Configure interfaces VLAN de Camada 3 (L3) somente para as VLANs primárias. As interfaces de VLAN para VLANs isoladas e de comunidade ficam inativas enquanto a VLAN tem uma configuração de VLAN isolada ou de comunidade.
- Você pode estender PVLANs através de switches com o uso de troncos. As portas de tronco transportam o tráfego de VLANs regulares e também de VLANs primárias, isoladas e de comunidade. A Cisco recomenda o uso de portas de tronco padrão se ambos os switches que passam por entroncamento suportam PVLANs.



Observação: você deve inserir manualmente a mesma configuração de PVLAN em cada switch com envolvimento, pois o VTP no modo transparente não propaga essas informações.

Configurar

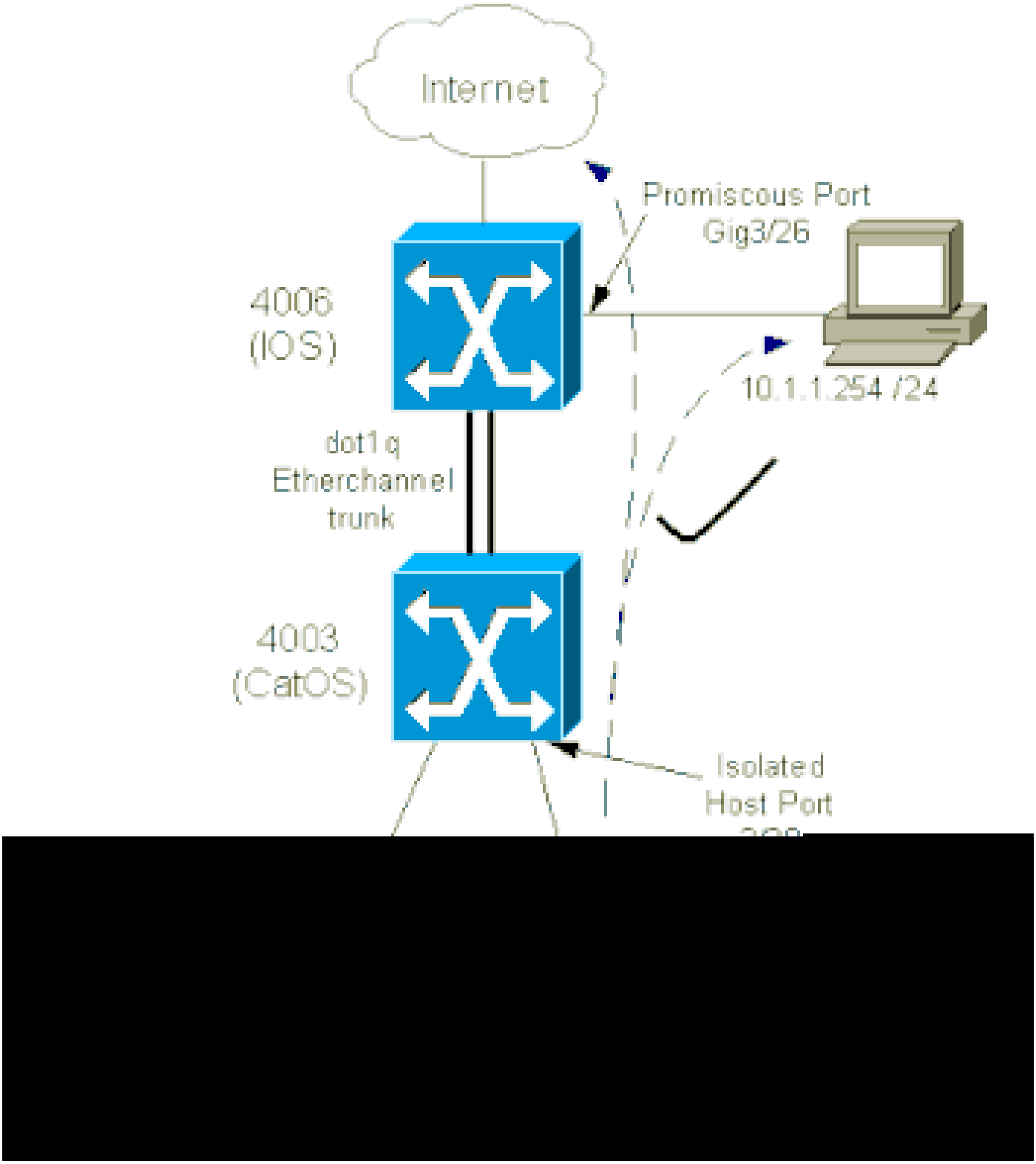
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.



Observação: use a Command Lookup Tool para obter mais informações sobre os comandos usados neste documento. Somente usuários registrados podem acessar as ferramentas e informações internas da Cisco.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Neste cenário, os dispositivos na VLAN isolada (101) têm uma restrição de comunicação na Camada 2 uns com os outros. No entanto, os dispositivos podem se conectar à Internet. Além disso, a porta Gig 3/26 no 4006 tem a designação promíscua. Essa configuração opcional permite que um dispositivo em GigabitEthernet 3/26 se conecte a todos os dispositivos na VLAN isolada. Essa configuração também permite, por exemplo, o backup dos dados de todos os dispositivos de host PVLAN para uma estação de trabalho administrativa. Outros usos para portas promíscuas incluem conexão a um roteador externo, LocalDirector, dispositivo de gerenciamento de rede e outros dispositivos.

Configurar as VLANs primária e isolada

Execute estas etapas para criar as VLANs primária e secundária, bem como para vincular as várias portas a essas VLANs. As etapas incluem exemplos para o CatOS e o Cisco IOS® Software. Emita o conjunto de comandos apropriado para a instalação do SO.

1. Crie a 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. Crie a VLAN ou VLANs isoladas.

    - 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. Vincule as VLANs/VLANs isoladas à 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 a configuração da VLAN privada.

- CatOS

<#root>

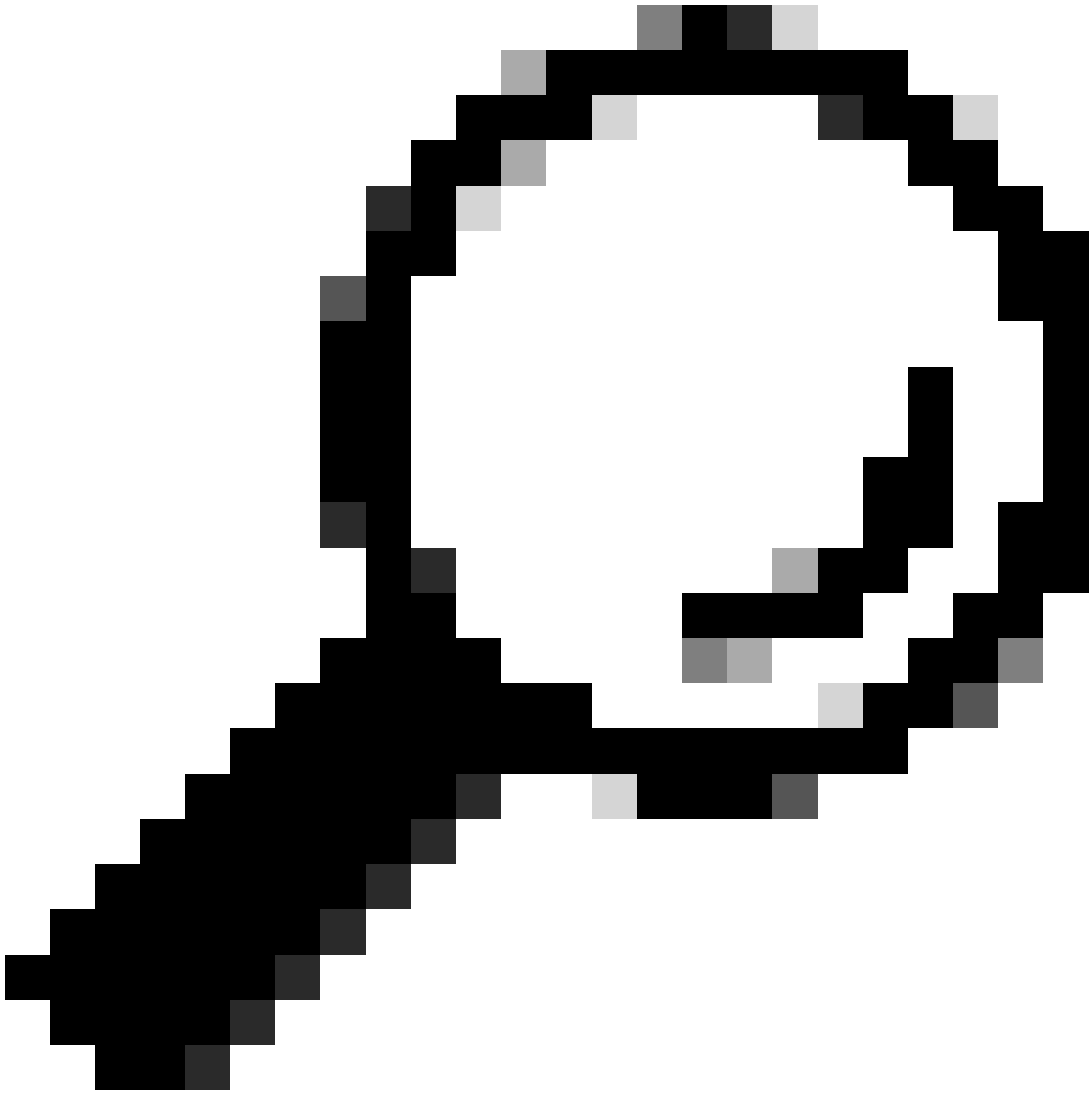
```
Switch_CatOS> (enable)
show pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
100     101       isolated
```

- Cisco IOS Software

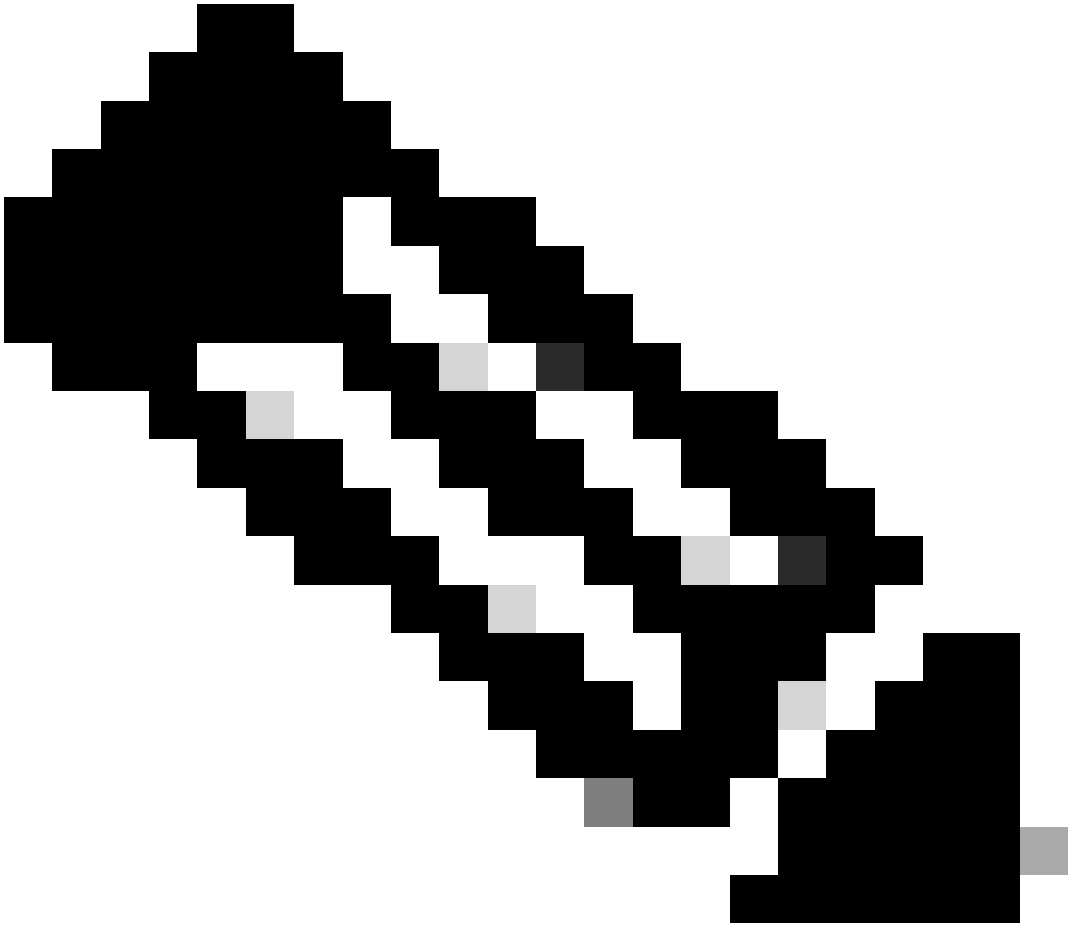
<#root>

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

Atribuir portas às PVLANs



Dica: antes de implementar esse procedimento, emita o comando`show PVLAN capability mod/port` (para CatOS) para determinar se uma porta pode se tornar uma porta PVLAN.



Observação: antes de executar a Etapa 1 deste procedimento, emita o comando switchport no modo de configuração de interface para configurar a porta como uma interface comutada de Camada 2.

-

Configure as portas do host em todos os Switches adequados.

  - **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.

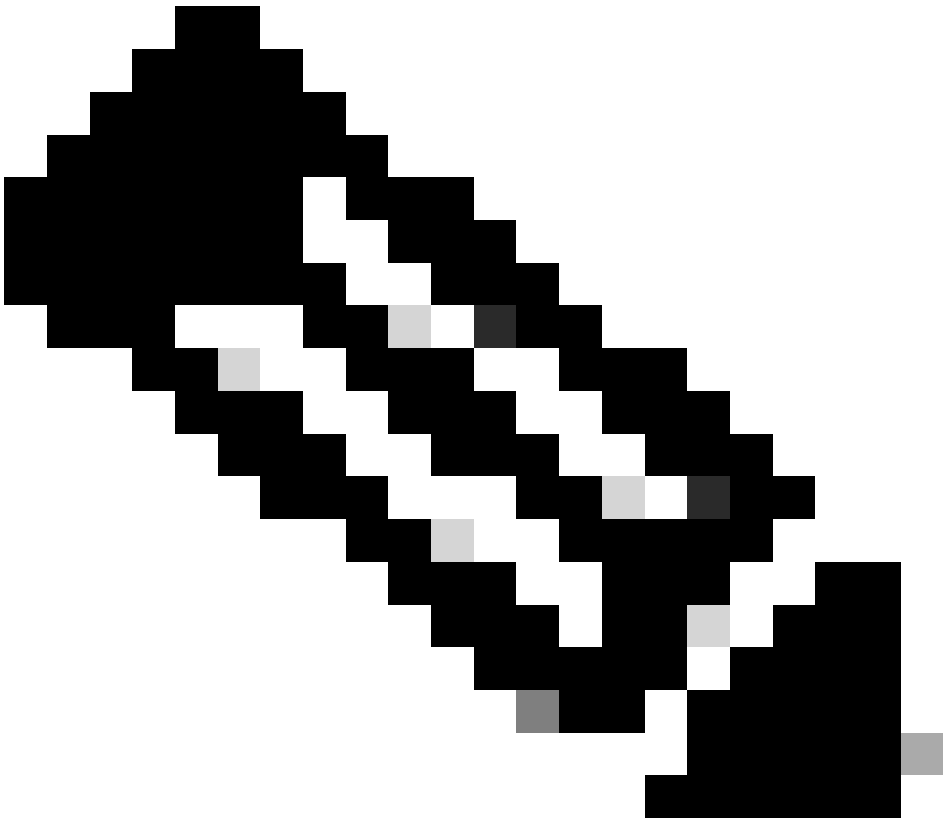
  - **CatOS**

```
<#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
```



Observação: para o Catalyst 6500/6000 quando o Supervisor Engine executa o CatOS como o software do sistema, a porta MSFC no Supervisor Engine (15/1 ou 16/1) deve ser promíscua se você desejar comutar a Camada 3 entre as 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
```

Configuração de camada 3

Esta seção opcional descreve as etapas de configuração para permitir a rota do tráfego de entrada de PVLAN. Se você só precisa habilitar a conectividade da Camada 2, você pode omitir essa fase.

- Configure a interface VLAN da mesma maneira que você configura para o roteamento normal da camada 3.

Essa configuração envolve:

- Configuração de um endereço IP

- Ativação da interface com o comando **no shutdown**

- Verificação de que a VLAN existe no banco de dados da VLAN

Consulte o Suporte Técnico de VLANs/VTP para obter exemplos de configuração.

- Mapeie as VLANs secundárias que você deseja rotear com a VLAN principal.

<#root>

Switch_IOS(config)#

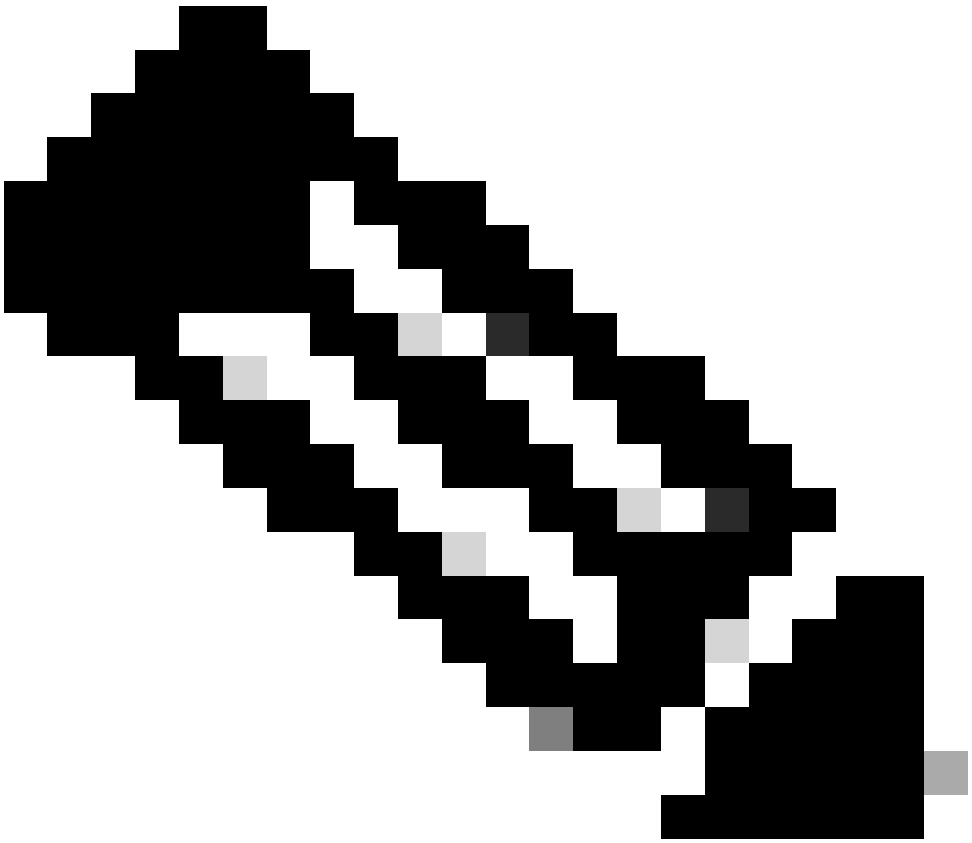
interface vlan primary_vlan_id

Switch_IOS(config-if)#

private-vlan mapping secondary_vlan_list

Switch_IOS(config-if)#

end



Observação: configure interfaces VLAN de Camada 3 somente para VLANs primárias. As interfaces de VLAN para VLANs isoladas e de comunidade estão inativas com uma configuração de VLAN isolada ou de comunidade.

•

Emita o comando **show interfaces private-vlan mapping** (Cisco IOS Software) ou **show pvlan mapping** (CatOS) para verificar o mapeamento.

•

Se você precisar modificar a lista de VLANs secundárias após a configuração do mapeamento, use a palavra-chave **add** ou **remove** .

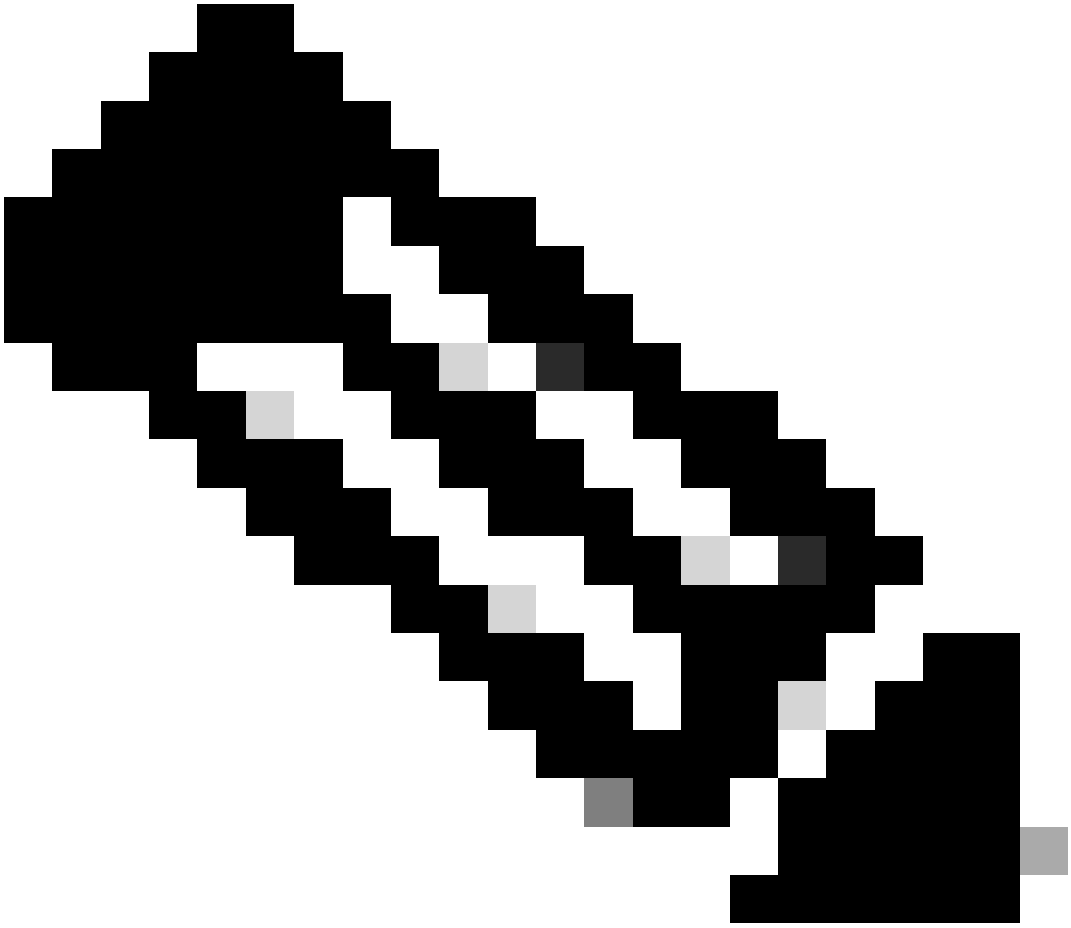
<#root>

Switch_IOS(config-if)#

private-vlan mapping add secondary_vlan_list

or
Switch_IOS(config-if)#

private-vlan mapping remove secondary_vlan_list



Observação: para switches Catalyst 6500/6000 com MSFC, certifique-se de que a porta do Supervisor Engine para o mecanismo de roteamento (por exemplo, porta 15/1 ou 16/1) seja promíscua.

<#root>

cat6000> (enable)

set pvlan mapping primary_vlan secondary_vlan 15/1

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

Emita o comando **show pvlan mapping** para verificar o mapeamento.

```
<#root>

cat6000> (enable)

show pvlan mapping

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

Configurações

Este documento utiliza as seguintes configurações:

- Access_Layer (Catalyst 4003: CatOS)
- Principal (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
```

Principal (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.
```

As VLANs privadas podem ser obtidas através de vários switches de dois métodos. Esta seção aborda estes métodos:

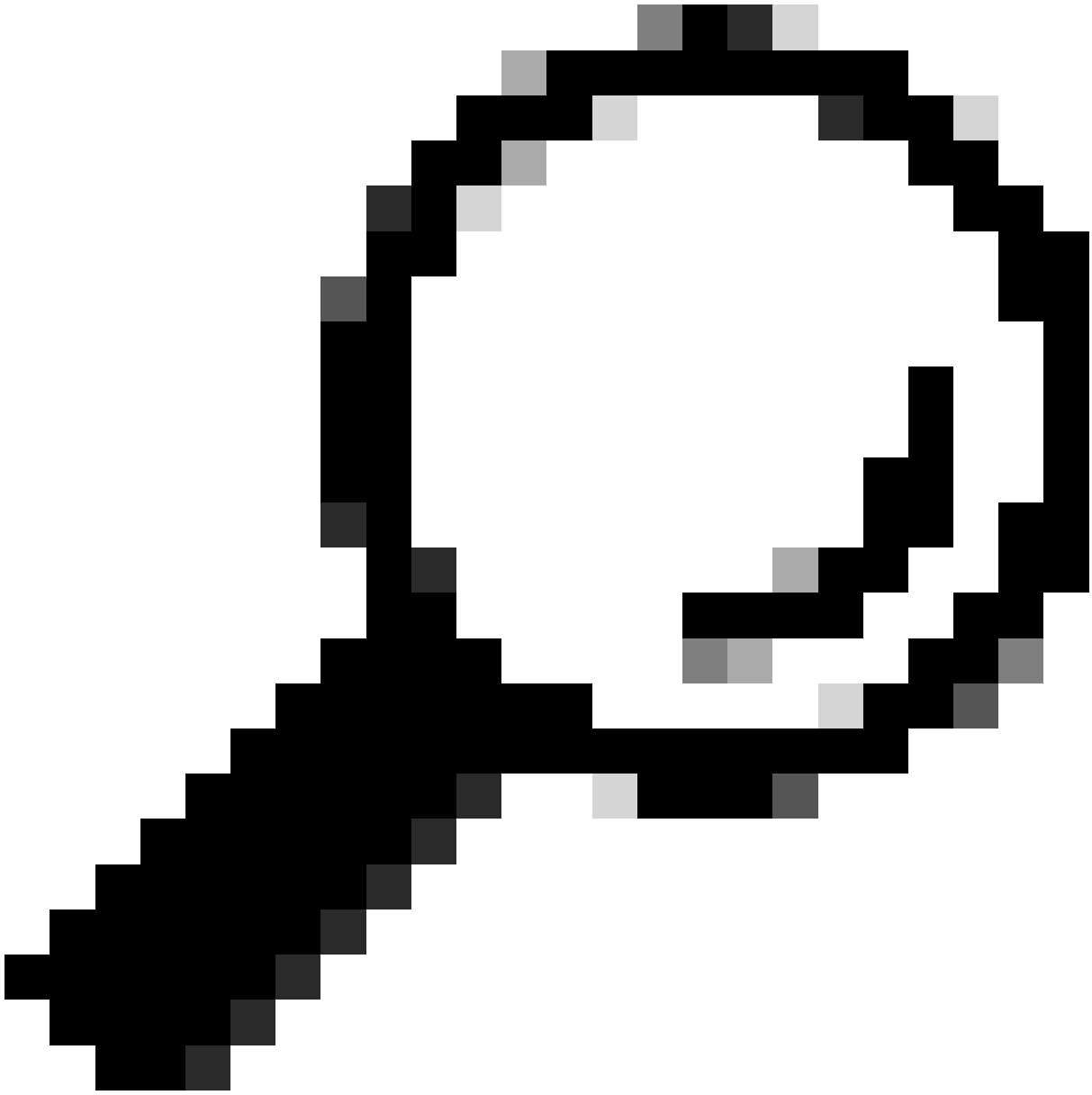
- Troncos Regulares
- Troncos VLAN Privados

Troncos Regulares

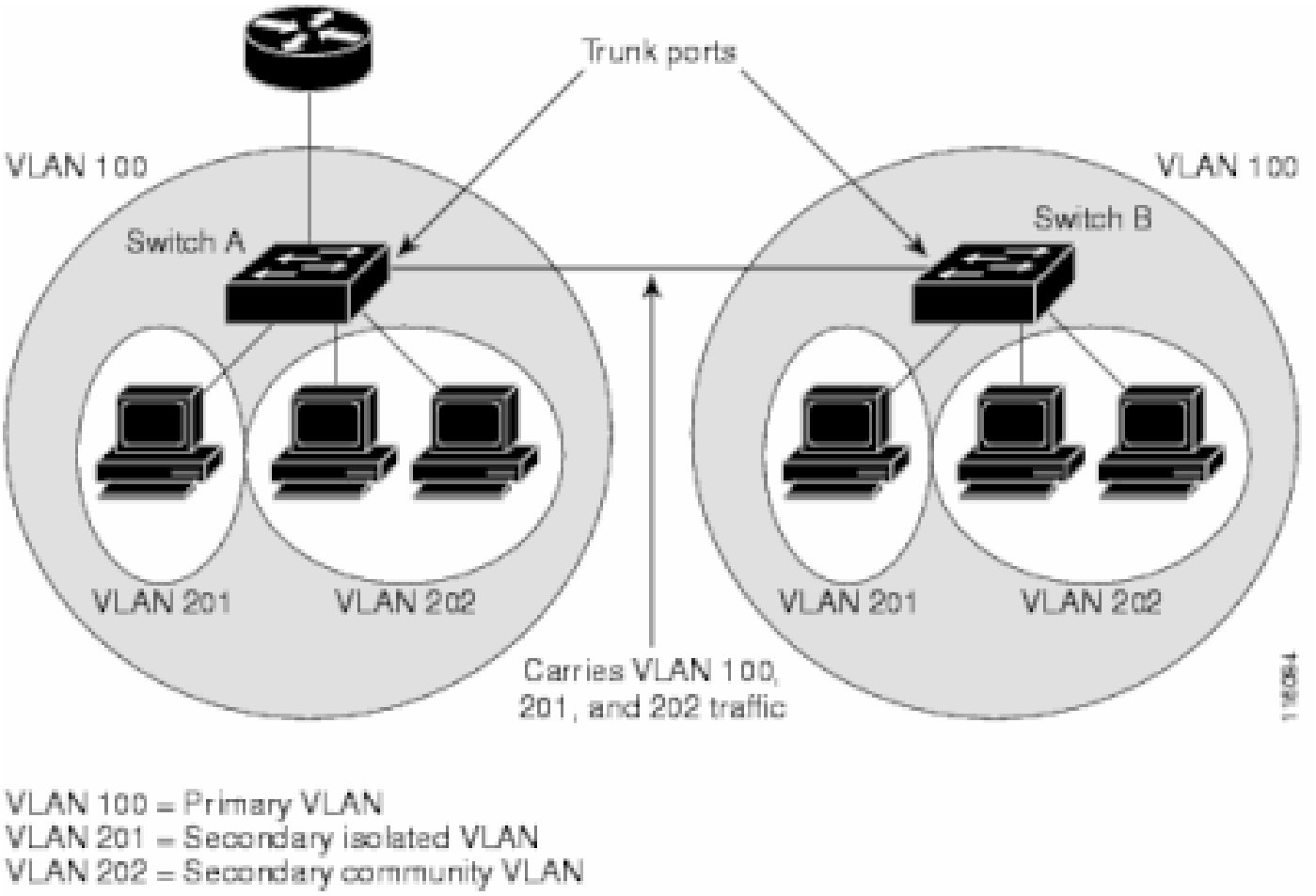
Como ocorre com as VLANs normais, as PVLANs podem abranger vários switches. Uma porta de tronco transporta a VLAN principal e as VLANs secundárias para um switch vizinho. A porta de tronco lida com a VLAN privada como qualquer outra VLAN. Um recurso de PVLANs através de vários switches é que o tráfego de uma porta isolada em um switch não alcança uma porta isolada em outro switch.

Configure PVLANs em todos os dispositivos intermediários, o que inclui dispositivos que não têm portas PVLAN, para manter a segurança da sua configuração PVLAN e evitar outro uso das VLANs configuradas como PVLANs.

As portas de tronco transportam o tráfego de VLANs regulares e também de VLANs primárias, isoladas e de comunidade.



Dica: a Cisco recomenda o uso de portas de tronco padrão se ambos os switches que passam por entroncamento suportam PVLANs.



Configurar manualmente as PVLANS em todos os Switches na rede de Camada 2

Como o VTP não suporta PVLANs, você deve configurar manualmente as PVLANs em todos os switches na rede de Camada 2. Se você não configurar a associação de VLAN primária e secundária em alguns switches na rede, os bancos de dados de Camada 2 nesses switches não serão mesclados. Essa situação pode resultar em inundação desnecessária de tráfego de PVLAN nesses switches.

Troncos VLAN Privados

Uma porta de tronco PVLAN pode transportar vários PVLANs secundários e não PVLANs. Os pacotes são recebidos e transmitidos com marcas de VLAN secundárias ou regulares nas portas de tronco PVLAN.

Somente o encapsulamento IEEE 802.1q é suportado. As portas de tronco isoladas permitem combinar o tráfego de todas as portas secundárias em um tronco. As portas de tronco promíscuas permitem combinar as várias portas promíscuas necessárias nessa topologia em uma única porta de tronco que transporta várias VLANs primárias.

Use portas de tronco VLAN privadas isoladas ao prever o uso de portas de host isoladas de VLAN privada para transportar várias VLANs, sejam VLANs normais ou para vários domínios de VLAN privada. Isso o torna útil para conectar um switch downstream que não suporta VLANs privadas.

Troncos promíscuos de VLAN privada são usados em situações onde uma porta de host promíscua de VLAN privada é normalmente usada, mas onde é necessário transportar várias vlans, seja vlans normais ou para vários domínios de VLAN privada. Isso o torna útil para conectar um roteador upstream que não suporta VLANs privadas.

Informações adicionais

Consulte Troncos VLAN Privados para obter mais informações.

Para configurar uma interface como porta de tronco PVLAN, consulte Configuração de uma Interface de Camada 2 como uma Porta de Tronco PVLAN .

Para configurar uma interface como uma porta de tronco promíscua, consulte Configuração de uma Interface de Camada 2 como uma Porta de Tronco Promiscua .

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

CatOS

- **show pvlan** — Exibe a configuração de PVLAN. Verifique se as VLANs isoladas e primárias se associam. Além disso, verifique se todas as portas de host são exibidas.

- **show pvlan mapping** — Exibe o mapeamento PVLAN com configuração em portas misturadas.

Cisco IOS Software

- **show vlan private-vlan** — Exibe informações de PVLAN, que incluem portas que se associam.

- **show interfacemod/portswitchport** — Exibe informações específicas da interface. Verifique se o modo operacional e as configurações de PVLAN operacionais estão corretos.

- **show interfaces private-vlan mapping** — Exibe o mapeamento PVLAN que você configurou.

Procedimento de verificação

Conclua estes passos:

•

Verifique a configuração da PVLAN nos switches.

Verifique se as PVLANs principal e secundária se associam/mapeiam umas às outras. Verifique também a inclusão das portas necessárias.

<#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
```

•

Verifique a configuração correta da porta misturada.

Essa saída indica que o modo operacional da porta é **promíscuo** e que as VLANs operacionais são 100 e 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

•

Inicie um pacote de ping do ICMP (Protocolo de Mensagens de Controle da Internet) da porta do host para a porta misturada.

Tenha em mente que, como ambos os dispositivos estão na mesma VLAN principal, os dispositivos devem estar na mesma sub-rede.

<#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.

•

Inicie um ping ICMP entre portas de host.

Neste exemplo, `host_port_2` (10.1.1.99) tenta fazer ping > `host_port` (10.1.1.100). Esse ping falha. Um ping de outra porta de host para a porta promíscua, no entanto, ainda é bem-sucedido.

<#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.
```

Troubleshooting

Solucionar problemas de PVLANs

Esta seção aborda alguns problemas comuns que ocorrem com as configurações de PVLAN.

Problema 1

Você recebe esta mensagem de erro: `%PM-SP-3-ERR_INCOMP_PORT: <mod/port> está definido como inativo porque <mod/port> é uma porta de tronco`.

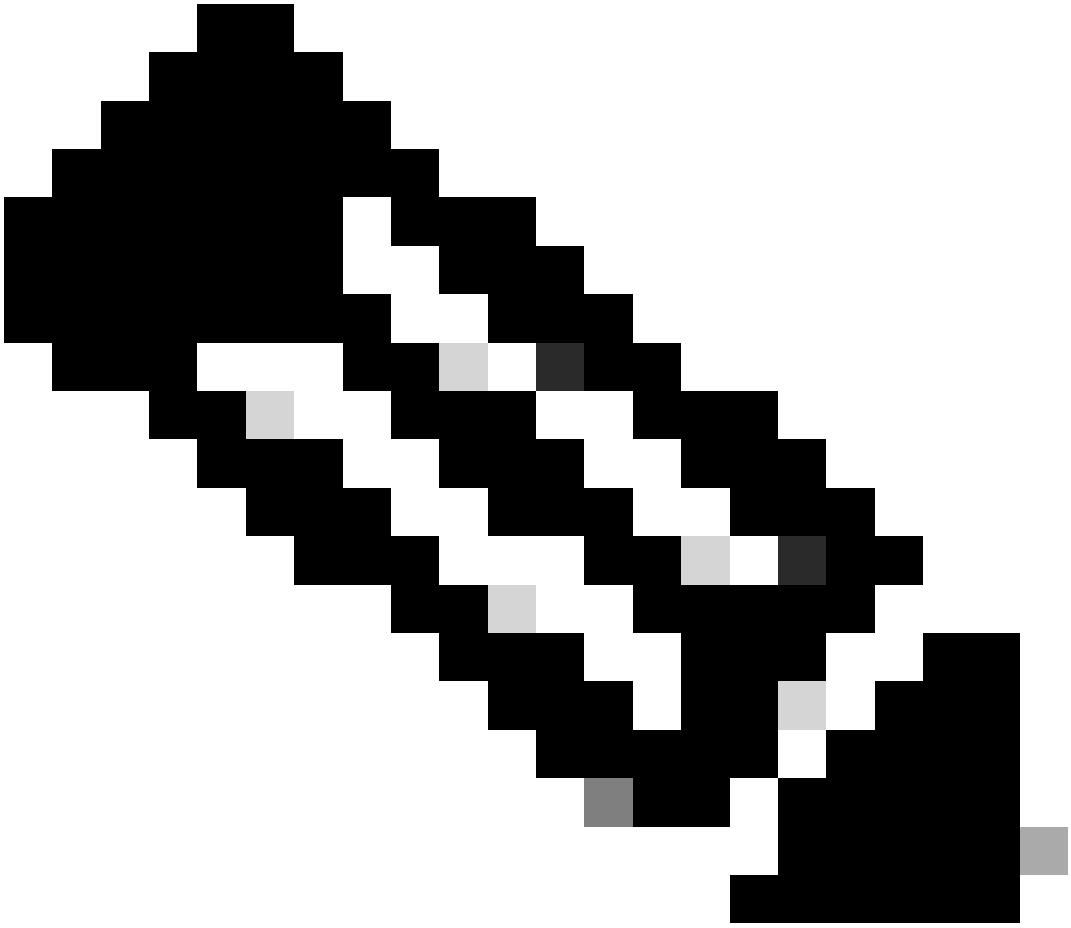
Essa mensagem de erro pode ser exibida por vários motivos, conforme discutido aqui.

Explicação - 1: Devido a limitações de hardware, os módulos de 10/100 Mbps do Catalyst 6500/6000 restringem a configuração de uma porta isolada ou de VLAN de comunidade quando uma porta dentro do mesmo ASIC COIL é um tronco, um destino de SPAN ou uma porta PVLAN misturada. (O ASIC COIL controla 12 portas na maioria dos módulos e 48 portas no módulo Catalyst 6548.) A tabela na seção Regras e Limitações deste documento fornece uma divisão da restrição de porta nos módulos Catalyst 6500/6000 de 10/100 Mbps.

Procedimento de resolução - 1: se não houver suporte para PVLAN nessa porta, escolha uma porta em um ASIC diferente no módulo ou em um módulo diferente. Para reativar as portas, remova a configuração de porta VLAN isolada ou de comunidade e execute o comando **shutdown** e o comando **no shutdown**.

Explicação - 2: Se as portas forem configuradas manualmente ou por padrão para o modo *dynamic desirable* ou **dynamic auto** .

Procedimento de resolução - 2: Configure as portas como modo de acesso com o comando **switchport mode access**. Para reativar as portas, execute os comandos **shutdown** e **no shutdown**.



Observação: no Cisco IOS Software Release 12.2(17a)SX e versões posteriores, a restrição de 12 portas não se aplica aos módulos de switching Ethernet WS-X6548-RJ-45, WS-X6548-RJ-21 e WS-X6524-100FX-MM.

Problema 2

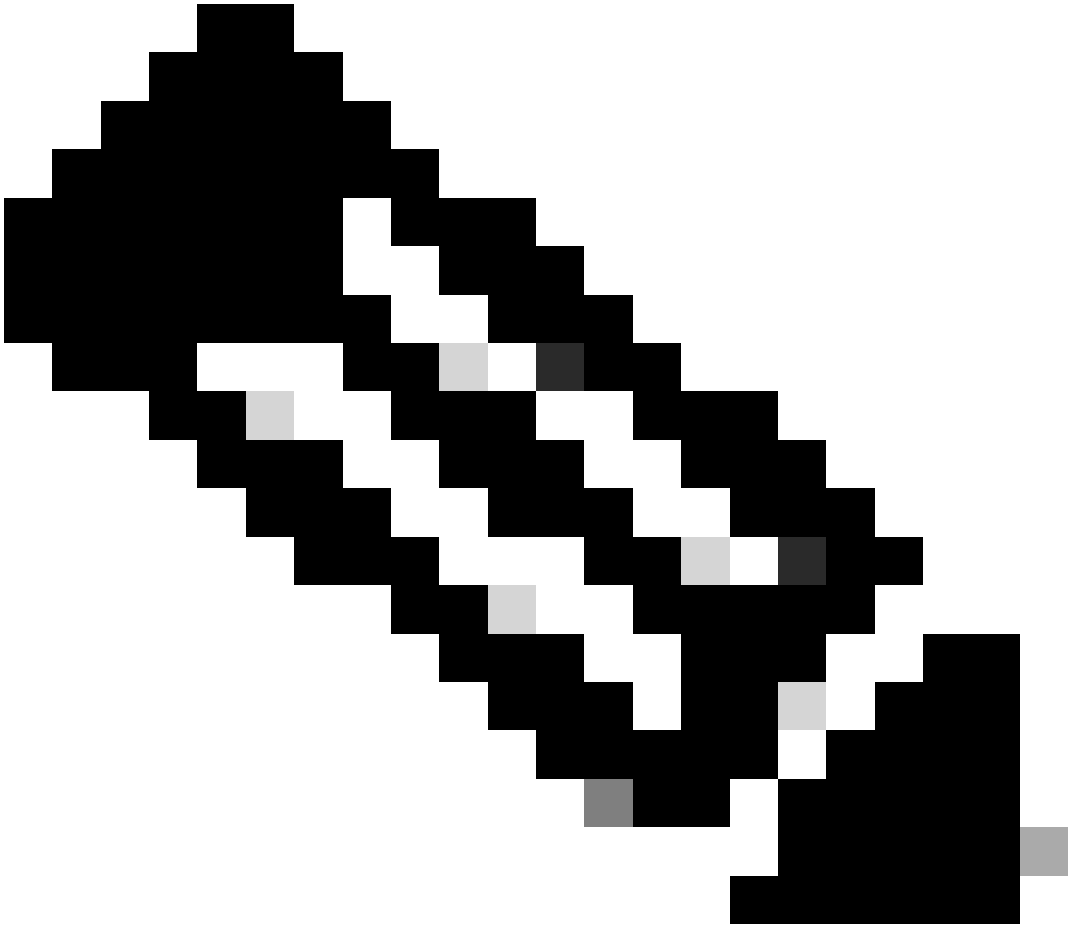
Durante a configuração de PVLAN, você encontra *uma* destas mensagens:

```
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.
```

Explicação: Devido a limitações de hardware, os módulos 10/100 Mbps do Catalyst 6500/6000 restringem a configuração de uma porta VLAN isolada ou de comunidade quando uma porta dentro do mesmo ASIC COIL é um tronco, um destino de SPAN ou uma porta PVLAN misturada. (O ASIC COIL controla 12 portas na maioria dos módulos e 48 portas no módulo Catalyst 6548.) A tabela na seção Regras e Limitações deste documento fornece uma divisão da restrição de porta nos módulos Catalyst 6500/6000 de 10/100 Mbps.

Procedimento de Resolução: Emita o comando **show pvlan capability** (CatOS), que indica se uma porta pode se tornar uma porta PVLAN. Se não houver suporte para PVLAN nessa porta específica, escolha uma porta em um ASIC diferente no módulo ou em um módulo diferente.



Observação: no Cisco IOS Software Release 12.2(17a)SX e versões posteriores, a restrição de 12 portas não se aplica aos módulos de switching Ethernet WS-X6548-RJ-45, WS-X6548-RJ-21 e WS-X6524-100FX-MM.

Problema 3

Não é possível configurar PVLANs em algumas plataformas.

Resolução: Verifique se a plataforma suporta PVLANs. Consulte a Matriz de Suporte do Switch Catalyst de VLAN Privada para determinar se a sua plataforma e versão de software suportam PVLANs antes de começar a configuração.

Problema 4

Em um Catalyst 6500/6000 MSFC, você não pode fazer ping em um dispositivo que se conecta à porta isolada no switch.

Resolução: no Supervisor Engine, verifique se a porta para o MSFC (15/1 ou 16/1) é promíscua.

<#root>

```
cat6000> (enable)
```

set pvlan mapping primary_vlan secondary_vlan 15/1

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

Além disso, configure a interface VLAN no MSFC conforme especificado na seção Configuração da Camada 3 deste documento.

Problema 5

Com a emissão do comando **no shutdown**, você não pode ativar a interface VLAN para VLANs isoladas ou de comunidade.

Resolução: Devido à natureza das PVLANs, você não pode ativar a interface VLAN para VLANs isoladas ou de comunidade. Você só pode ativar a interface VLAN que pertence à VLAN principal.

Problema 6

Nos dispositivos Catalyst 6500/6000 com MSFC/MSFC2, as entradas ARP aprendidas nas interfaces PVLAN de Camada 3 não envelhecem.

Resolução: as entradas ARP aprendidas nas interfaces VLAN privadas da Camada 3 são entradas ARP aderentes e não envelhecem. A conexão de novos equipamentos com o mesmo endereço IP gera uma mensagem e não há criação da entrada ARP. Portanto, é necessário remover as entradas ARP da porta PVLAN manualmente caso um endereço MAC seja alterado. Para adicionar ou remover manualmente as entradas ARP de PVLAN, execute estes 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
```

Outra opção é executar o comando **no ip sticky-arp** no Cisco IOS Software Release 12.1(11b)E e posteriores.

Informações Relacionadas

- **Switches Cisco Catalyst série 2955 - Notificação de desativação**
- **Redes seguras com PVLANs e VACLs**
- **Suporte de tecnologia de switching de LAN**
- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.