Catalystスイッチでの隔離プライベートVLANの設定

内容

はじめに

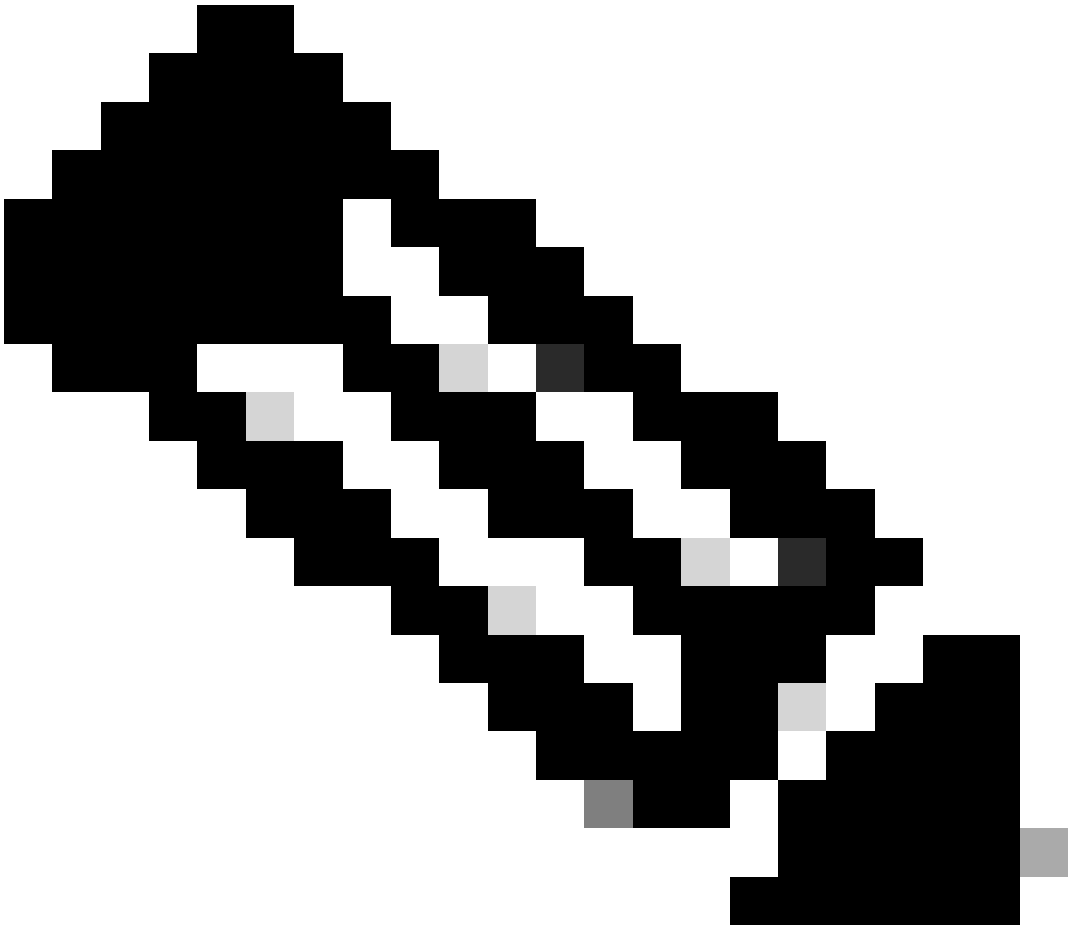
このドキュメントでは、Catalyst OS（CatOS）または Cisco IOS® ソフトウェアを使用して、Cisco Catalyst スイッチ上で隔離された PVAN を設定する手順について説明します。

前提条件

要件

このドキュメントは、ネットワークが既に存在しており、PVLAN に接続するさまざまなポート間で通信を確立できることが前提です。複数のスイッチがある場合は、スイッチ間のトランクが正しく動作し、トランク上の PVLAN が許可されていることを確認します。

すべてのスイッチとソフトウェア バージョンが PVLAN をサポートしているわけではありません。



注：一部のスイッチ (「プライベートVLAN Catalystスイッチのサポート一覧」で指定) は、現在PVLANエッジ機能のみをサポートしています。この機能は、「保護ポート」とも呼ばれています。PVLAN エッジ ポートは、同じスイッチ上の他の保護ポートとの通信が制限されています。ただし、別のスイッチ上の保護ポートとは相互に通信できます。この機能と、このドキュメントで説明する通常の PVLAN 設定と混同しないでください。保護ポートについての詳細は、『ポートベース トラフィック制御の設定』の「ポート セキュリティの設定」を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CatOS バージョン 6.3(5) が稼働しているスーパーバイザ エンジン 2 モジュールを搭載した Catalyst 4003 スイッチ
- Cisco IOS ソフトウェア リリース 12.1(12c)EW1 が稼働しているスーパーバイザ エンジン 3 を搭載した Catalyst 4006 スイッチ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

状況によっては、デバイスを異なる IP サブネットに配置しないようにして、スイッチ上のエンドデバイス間のレイヤ 2（L2）接続を防止する必要があります。この設定により IP アドレスを節約できます。プライベート VLAN（PVLAN）を使用すると、同じ IP サブネット上のデバイスをレイヤ 2 で隔離できます。デフォルト ゲートウェイ、バックアップ サーバ、または Cisco LocalDirector が接続された特定のポートだけに到達できるように、スイッチ上の一部のポートを制限することができます。

このドキュメントでは、Catalyst OS(CatOS)またはCisco IOSソフトウェアのいずれかを使用して、Cisco Catalystスイッチに隔離PVLANを設定する手順について説明します。

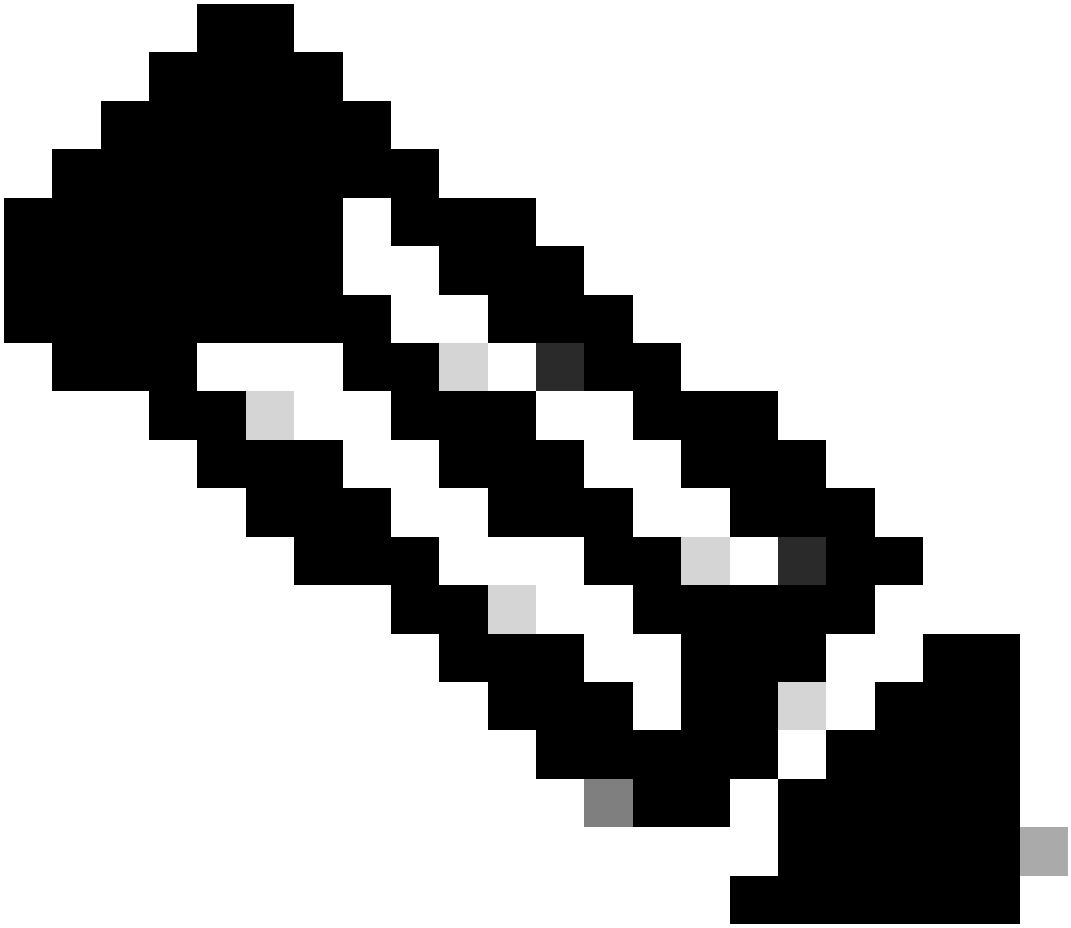
PVLAN とは、同じブロードキャスト ドメインまたはサブネット内の他のポートからレイヤ 2 で隔離するように設定された VLAN です。PVLAN 内で特定のポート セットを割り当てることができるため、レイヤ 2 でのポート間のアクセスを制御できます。PVLAN と通常の VLAN を同じスイッチ上で設定できます。

PVLANポートには、無差別、隔離、およびコミュニティの3つのタイプがあります。

- 混合モード ポートは、他のすべての PVLAN ポートと通信します。通常は、外部ルータ、LocalDirector、ネットワーク管理デバイス、バックアップ サーバ、管理ワークステーションなどとの通信で使用されます。一部のスイッチでは、ルート モジュール（たとえば、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード））へのポートは、混合モード ポートである必要があります。
- 隔離ポートは、同じ PVLAN 内の他のポートからレイヤ 2 で完全に分離されています。この分離にはブロードキャストも含まれていますが、混合モード ポートだけは例外です。レイヤ 2 レベルでのプライバシーは、すべての隔離ポートへの発信トラフィックをブロックすることで実現されます。隔離ポートから受信するトラフィックは、すべての混合モード ポ

ートにだけ転送されます。

- コミュニティ ポートは、コミュニティ ポート同士、および混合モード ポートと通信できます。このポートは、他のコミュニティ内の他のすべてのポートから、または、PVLAN 内の隔離ポートから、レイヤ 2 で隔離されています。ブロードキャストは、関連するコミュニティ ポートおよび混合モード ポート間でだけ伝搬されます。



注：このドキュメントでは、コミュニティVLANの設定については説明していません。

ルールおよび制限

このセクションでは、PVLAN を実装する場合に注意する必要があるいくつかのルールと制限事項について説明します。

- PVLAN に VLAN 1 または 1002–1005 を含めることはできません。
- VLAN Trunk Protocol（VTP; VLAN トランク プロトコル）モードを transparent に設定する必要があります。

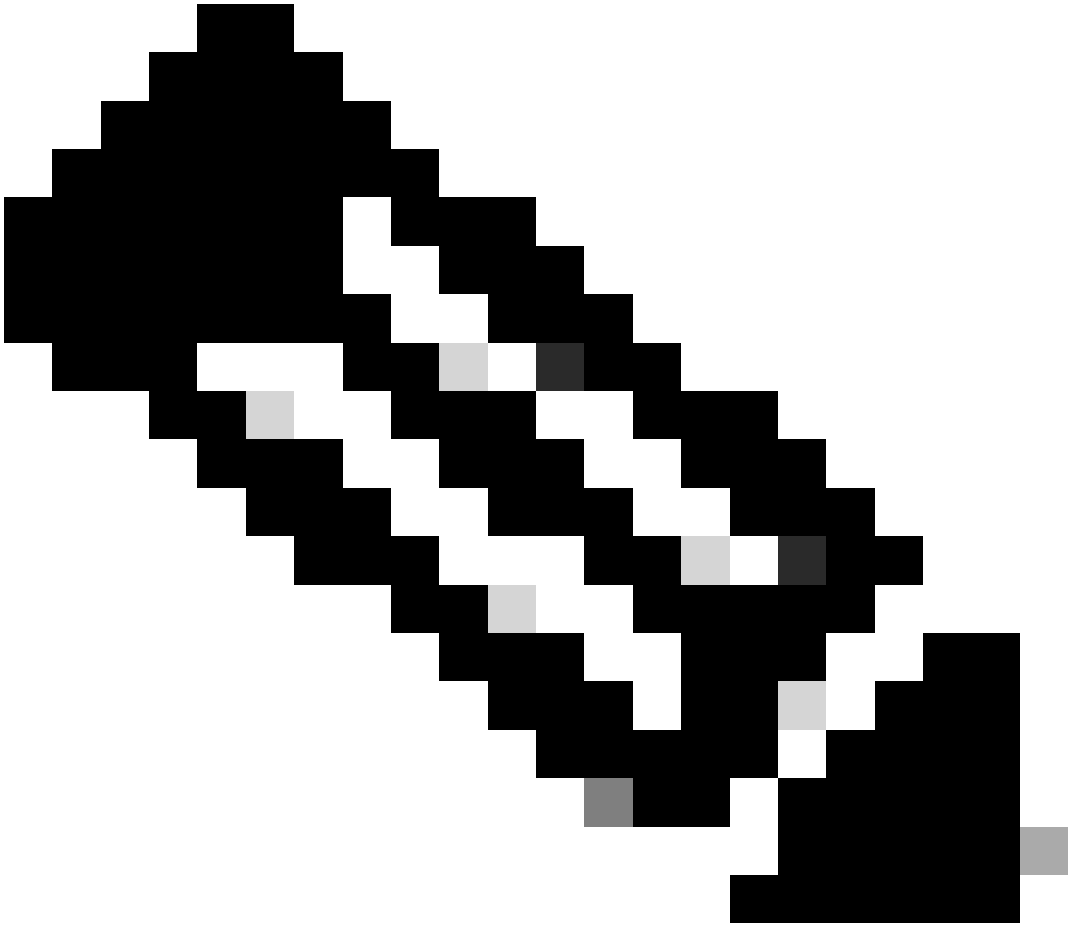
- プライマリ VLAN ごとに、隔離モード VLAN は 1 つしか指定できません。
- VLAN にアクセス ポートが割り当てられていない場合、その VLAN は PVLAN としてのみ指定できます。VLAN を PVLAN にする前に、その VLAN 内のポートを削除します。
- PVLAN ポートを EtherChannel として設定しないでください。
- ハードウェアの制約により、同じ COIL Application-Specific Integrated Circuit（ASIC; 特定用途向け集積回路）内のポートが次のいずれかの場合、Catalyst 6500/6000 ファスト イーサネット スイッチ モジュールは、隔離 VLAN ポートまたはコミュニティ VLAN ポートの設定が制限されます。
    - トランク
    - Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）の宛先
    - 混合モードの PVLAN ポート

  次の表は、Catalyst 6500/6000 ファスト イーサネット スイッチ モジュール上の同じ ASIC に属するポートの範囲を示しています。

モジュール	ASIC ごとのポート
WS-X6224-100FX-MT、WS-X6248-RJ-45、WS-X6248-TEL	ポート 1 ~ 12、13 ~ 24、25 ~ 36、37 ~ 48
WS-X6024-10FL-MT	ポート 1 ~ 12、13 ~ 24
WS-X6548-RJ-45、WS-X6548-RJ-21	ポート 1 ~ 48

また、show pvlan capability コマンド（CatOS）は、ポートを PVLAN ポートにできるかどうかを示します。Cisco IOS ソフトウェアにはこれに相当するコマンドはありません。

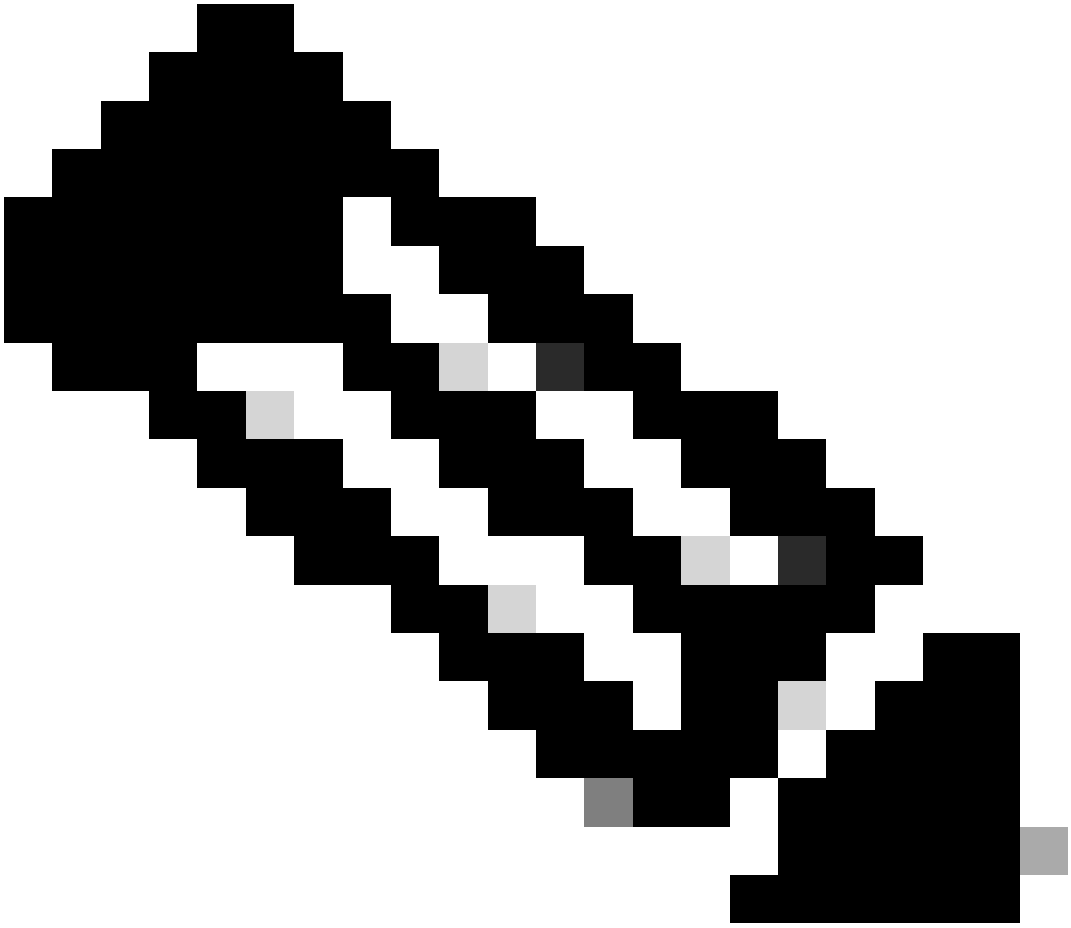
- PVLAN 設定で使用している VLAN を削除すると、その VLAN に関連付けられているポートは非アクティブになります。
- レイヤ 3（L3）VLAN インターフェイスは、プライマリ VLAN に対してだけ設定してください。VLAN が隔離 VLAN またはコミュニティ VLAN として設定されている場合、隔離 VLAN およびコミュニティ VLAN の VLAN インターフェイスは非アクティブです。
- PVLAN は、トランクを使用することでスイッチを越えて拡張できます。トランク ポートは、通常の VLAN からのトラフィックだけでなく、プライマリ VLAN、隔離 VLAN、およびコミュニティ VLAN からのトラフィックも伝送します。トランキングを実行する両方のスイッチが PVLAN をサポートする場合は、標準のトランク ポートを使用することをお勧めします。



注：関与するすべてのスイッチで同じPVLAN設定を手動で入力する必要があります。これは、トランスペアレントモードのVTPがこの情報を伝搬しないためです。

設定

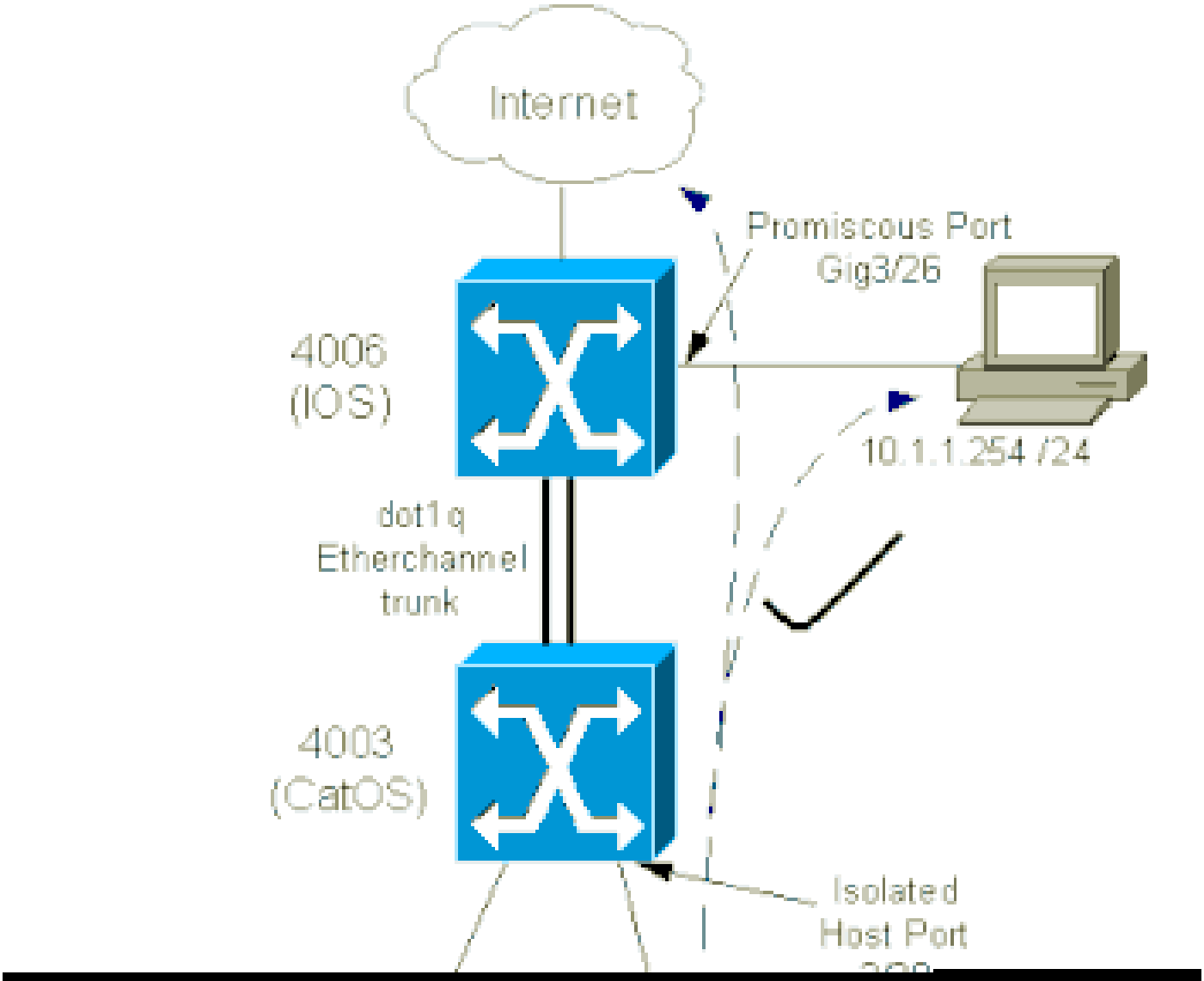
このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。



注：このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。シスコの内部ツールおよび情報にアクセスできるのは、登録ユーザのみです。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



このシナリオでは、隔離VLAN(101)内のデバイスは、レイヤ2での相互通信が制限されています。ただし、インターネットへの接続は可能です。また、4006のポートGig 3/26は無差別ポートとして認識されています。このオプションの設定により、ギガビット イーサネット 3/26 上のデバイスは、隔離 VLAN 内のすべてのデバイスに接続できます。このため、たとえば、すべての PVLAN ホスト デバイスのデータを管理ワークステーションにバックアップできます。混合モード ポートの他の使用方法として、外部ルータ、LocalDirector、ネットワーク管理デバイスなどへの接続があります。

プライマリ VLAN と隔離 VLAN の設定

プライマリ VLAN とセカンダリ VLAN を作成し、さまざまなポートをこれらの VLAN にバインドするには、次の手順を実行します。手順には、CatOSとCisco IOS®ソフトウェアの両方の例が含まれています。インストールされている OS に応じて、適切なコマンド セットを実行してください。

1. プライマリ PVLAN を作成します。

   - 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 ソフトウェア

     <#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. 隔離 VLAN を作成します。

   - 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 ソフトウェア

```
<#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. 隔離 VLAN をプライマリ VLAN にバインドします。

- 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 ソフトウェア

```
<#root>

Switch_IOS(config)#
```

```
vlan primary_vlan_id
Switch_IOS(config-vlan)#
private-vlan association secondary_vlan_id
Switch_IOS(config-vlan)#
exit
```

4. プライベート VLAN 設定を確認します。

- CatOS

<#root>

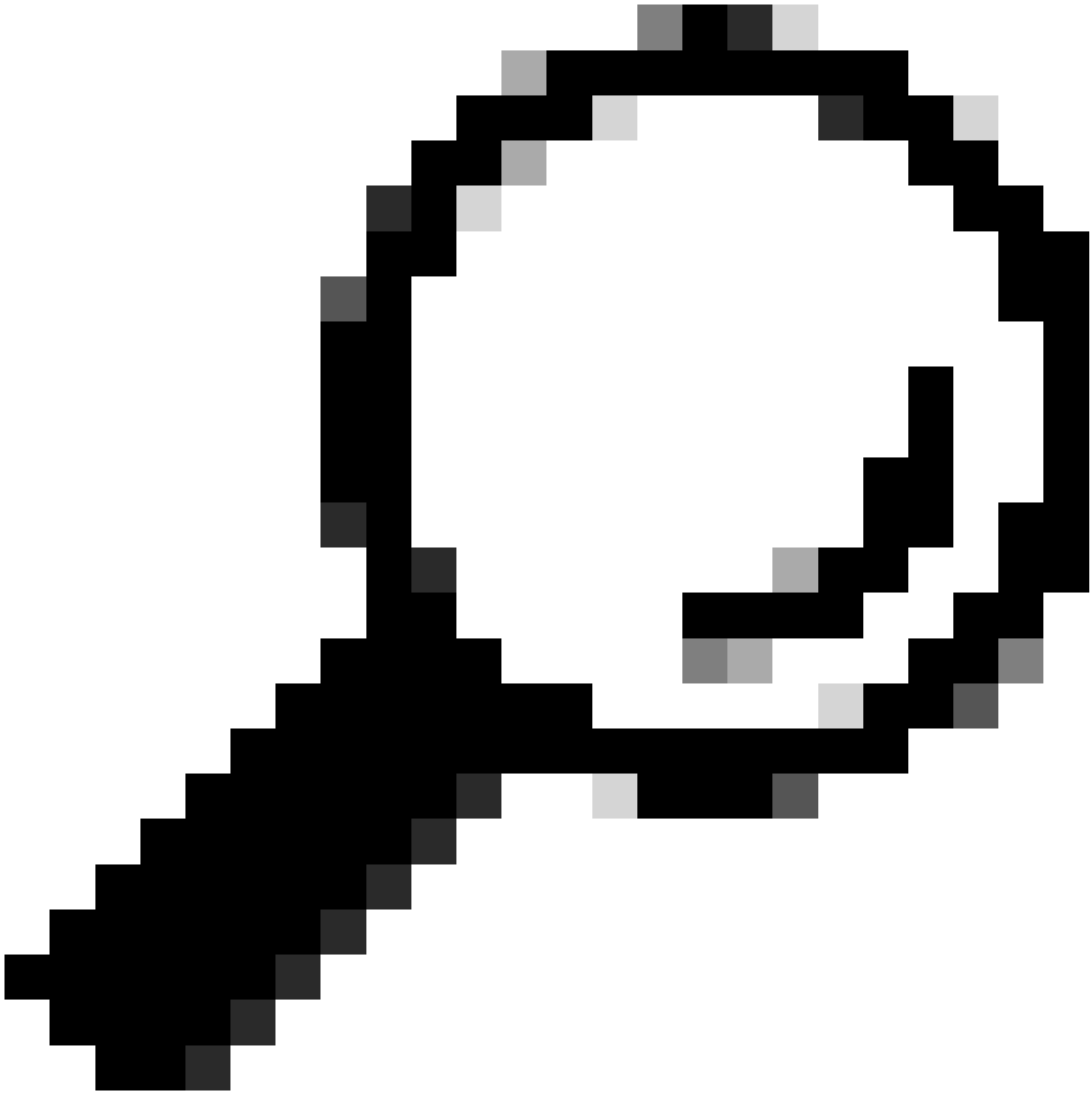
```
Switch_CatOS> (enable)
show pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
100     101       isolated
```

- Cisco IOS ソフトウェア

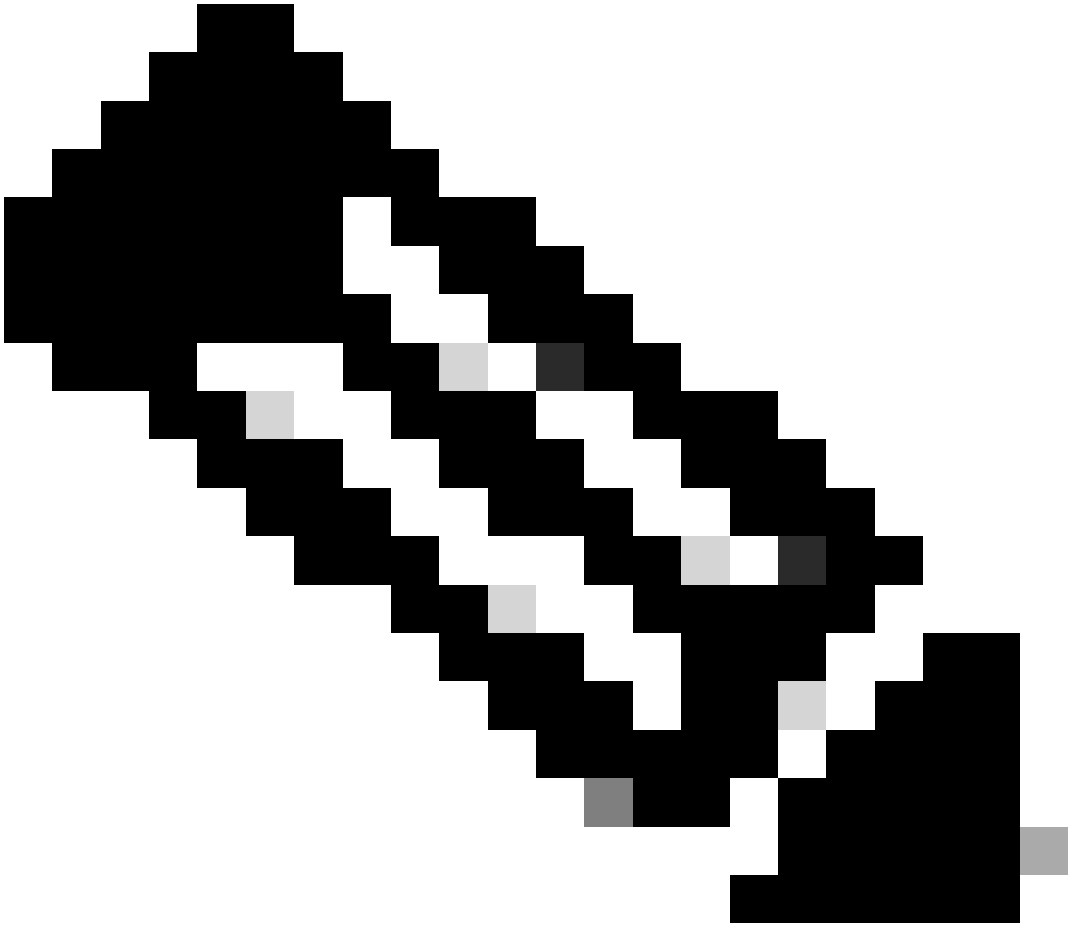
<#root>

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

PVLAN へのポートの割り当て



ヒント：この手順を実行する前に、show PVLAN capability mod/portコマンド(CatOSの場合)を発行して、ポートをPVLANポートにできるかどうか確認してください。



注：この手順1を実行する前に、インターフェイス設定モードでswitchportコマンドを発行して、ポートをレイヤ2スイッチインターフェイスとして設定します。

-

該当するすべてのスイッチ上でホスト ポートを設定します。

  - **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 ソフトウェア

<#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

- いずれか 1 つのスイッチで、混合モード ポートを設定します。

  - **CatOS**

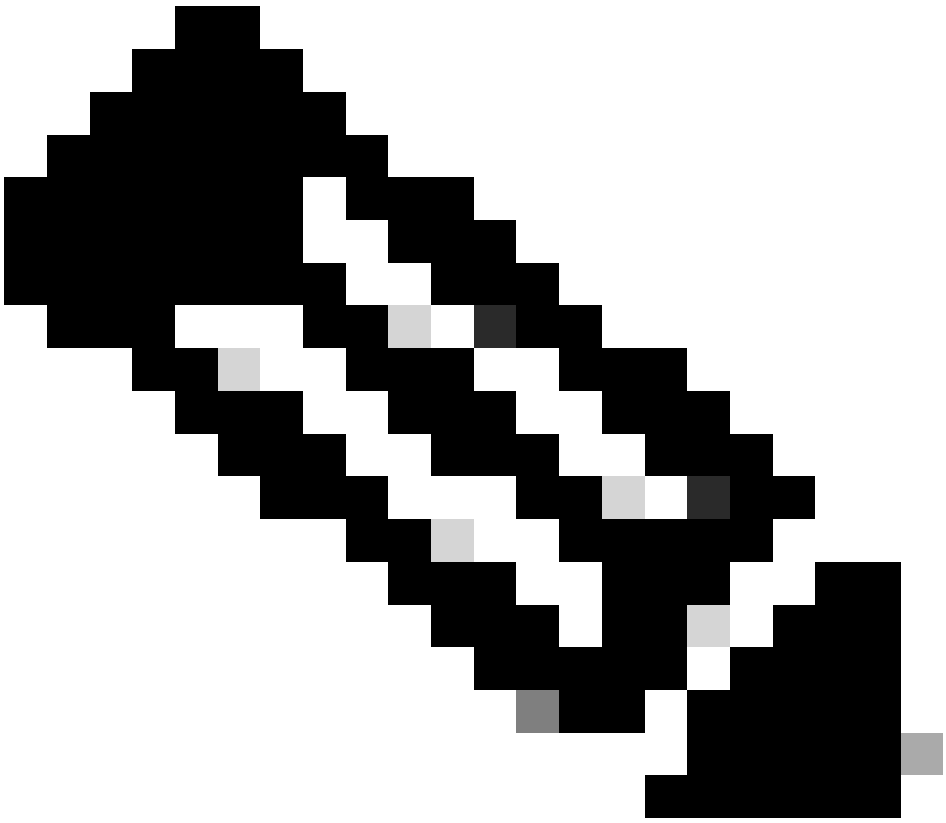
    <#root>

    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



注：スーパーバイザエンジンでシステムソフトウェアとしてCatOSが稼働しているCatalyst 6500/6000の場合、VLAN間でレイヤ3スイッチングを行うには、スーパーバイザエンジン（15/1または16/1）のMSFCポートが混合モードである必要があります。

-

Cisco IOS ソフトウェア

<#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
```

レイヤ 3 の設定

このオプションのセクションでは、PVLAN の入トラフィックのルーティングを許可する設定手順について説明します。レイヤ 2 接続だけを有効にする必要がある場合は、この手順は省略できます。

- 通常のレイヤ 3 ルーティングの場合と同様に VLAN インターフェイスを設定します。

この設定には、次のものが含まれます。

- IP アドレスの設定

- **no shutdown** コマンドによるインターフェイスのアクティブ化

- VLAN データベースに目的の VLAN が存在することの確認

設定例については、『VLAN/VTP テクニカル サポート』を参照してください。

- ルーティングするセカンダリ VLAN をプライマリ VLAN にマップします。

<#root>

Switch_IOS(config)#

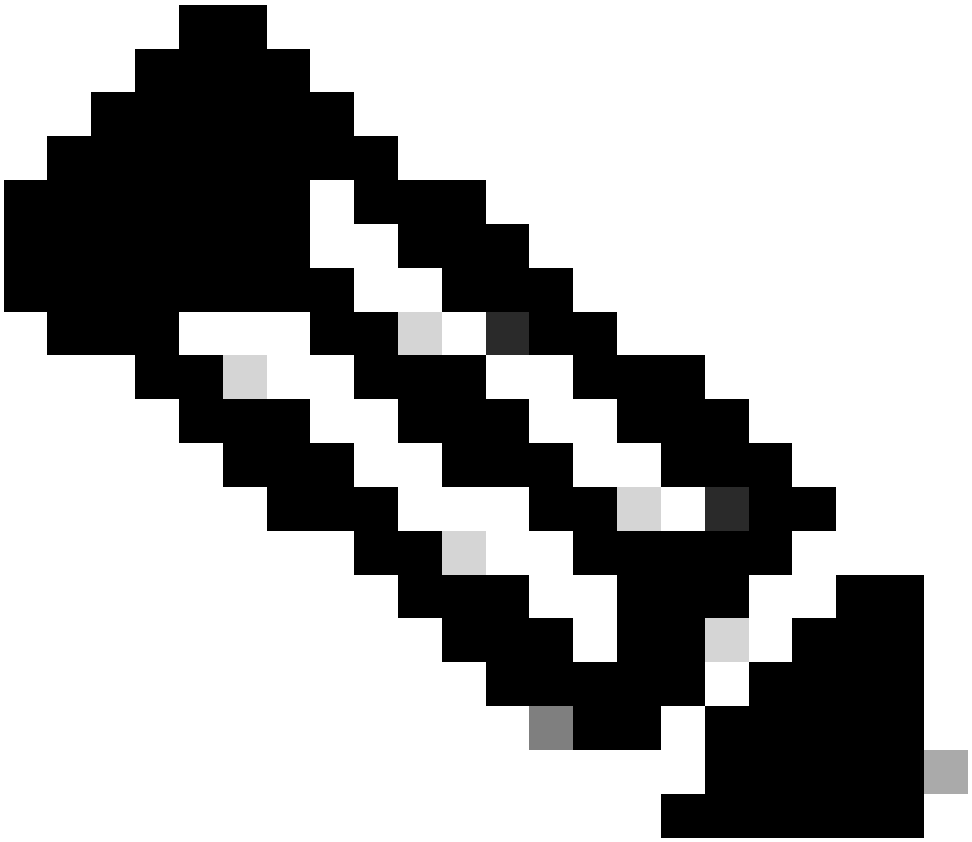
interface vlan primary_vlan_id

Switch_IOS(config-if)#

private-vlan mapping secondary_vlan_list

Switch_IOS(config-if)#

end



注：レイヤ3 VLANインターフェイスは、プライマリVLANに対してだけ設定してください。隔離 VLAN またはコミュニティ VLAN として設定されている場合、隔離 VLAN およびコミュニティ VLAN の VLAN インターフェイスは非アクティブです。

-

show interfaces private-vlan

mapping（Cisco IOS ソフトウェア）コマンドまたは **show pvlan mapping**（**CatOS**）コマンドを発行して、マッピングを確認します。

-

マッピングの設定後にセカンダリ VLAN リストを変更する必要がある場合は、**add** キーワードまたは **remove** キーワードを使用します。

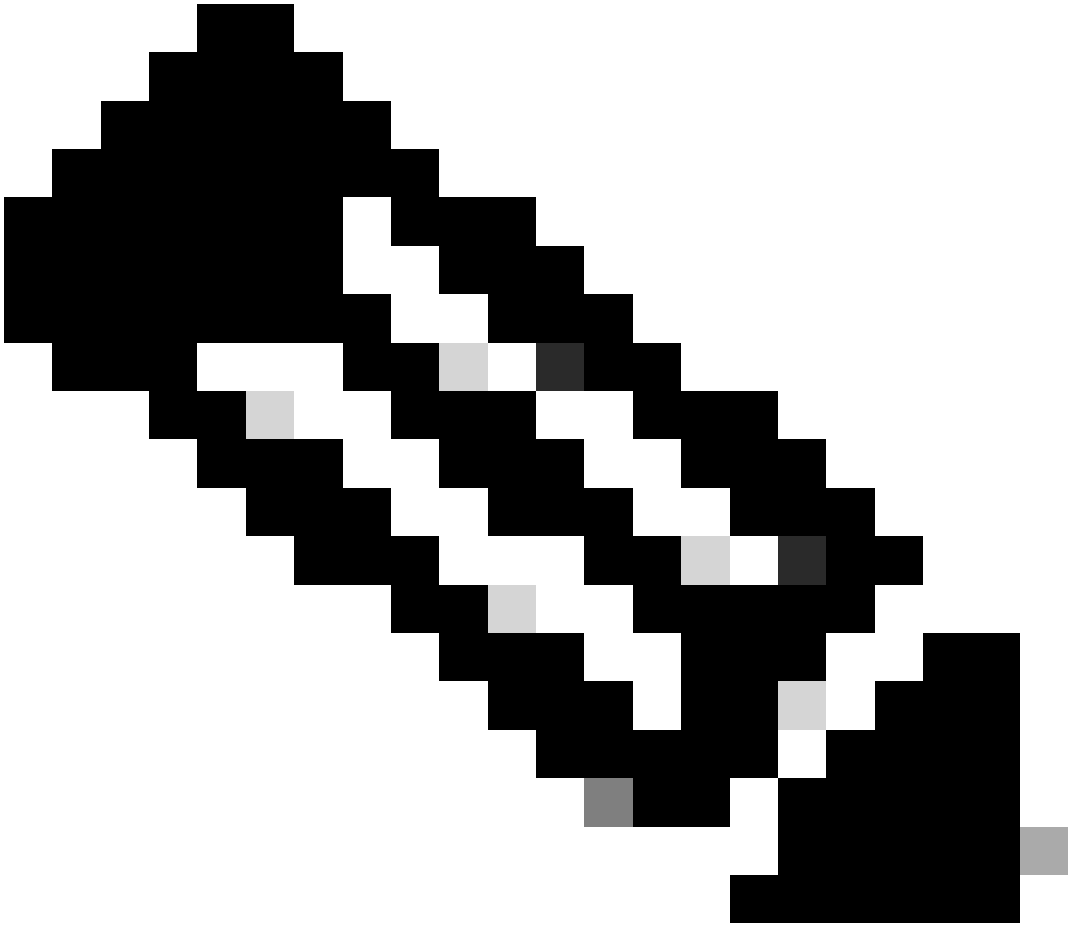
<#root>

Switch_IOS(config-if)#

private-vlan mapping add secondary_vlan_list

or
Switch_IOS(config-if)#

private-vlan mapping remove secondary_vlan_list



注:MSFCを搭載したCatalyst 6500/6000スイッチの場合は、スーパーバイザエンジンからルーティングエンジンへのポート（ポート15/1や16/1など）が混合モードであることを確認してください。

<#root>

cat6000> (enable)

set pvlan mapping primary_vlan secondary_vlan 15/1

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

show pvlan mappingコマンドを発行して、マッピングを確認します。

```
<#root>

cat6000> (enable)

show pvlan mapping

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

コンフィギュレーション

このドキュメントでは、次のコンフィギュレーションを使用します。

- Access_Layer(Catalyst 4003:CatOS)
- コア（Catalyst 4006:Cisco IOSソフトウェア）

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
```

コア（Catalyst 4006:Cisco IOSソフトウェア）

<#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.
```

複数のスイッチにまたがるプライベート VLAN

プライベート VLAN は、2 つの方法で複数のスイッチにまたがって構成できます。このセクションでは、その方法について説明します。

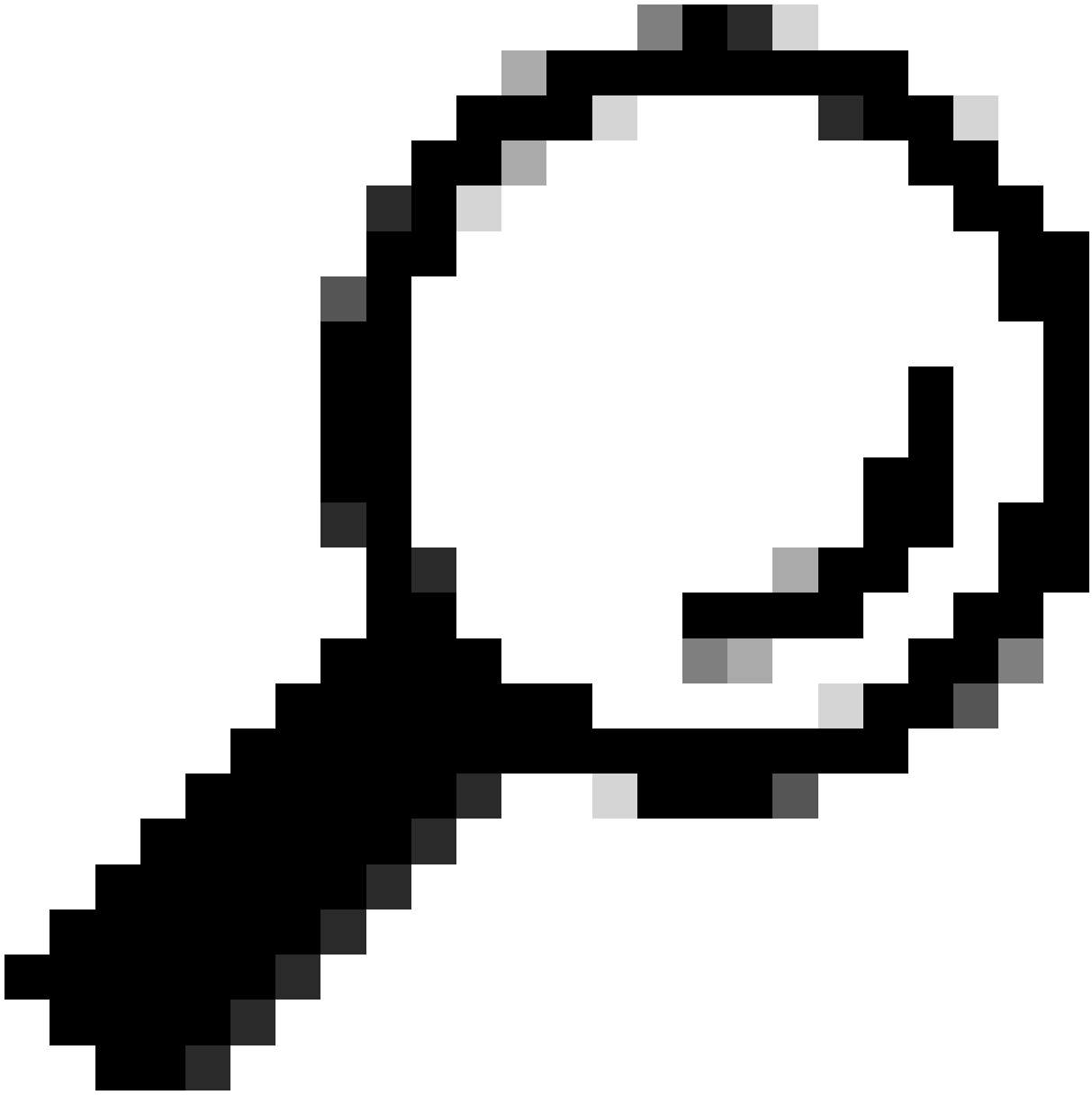
- 通常のトランク
- プライベート VLAN トランク

通常のトランク

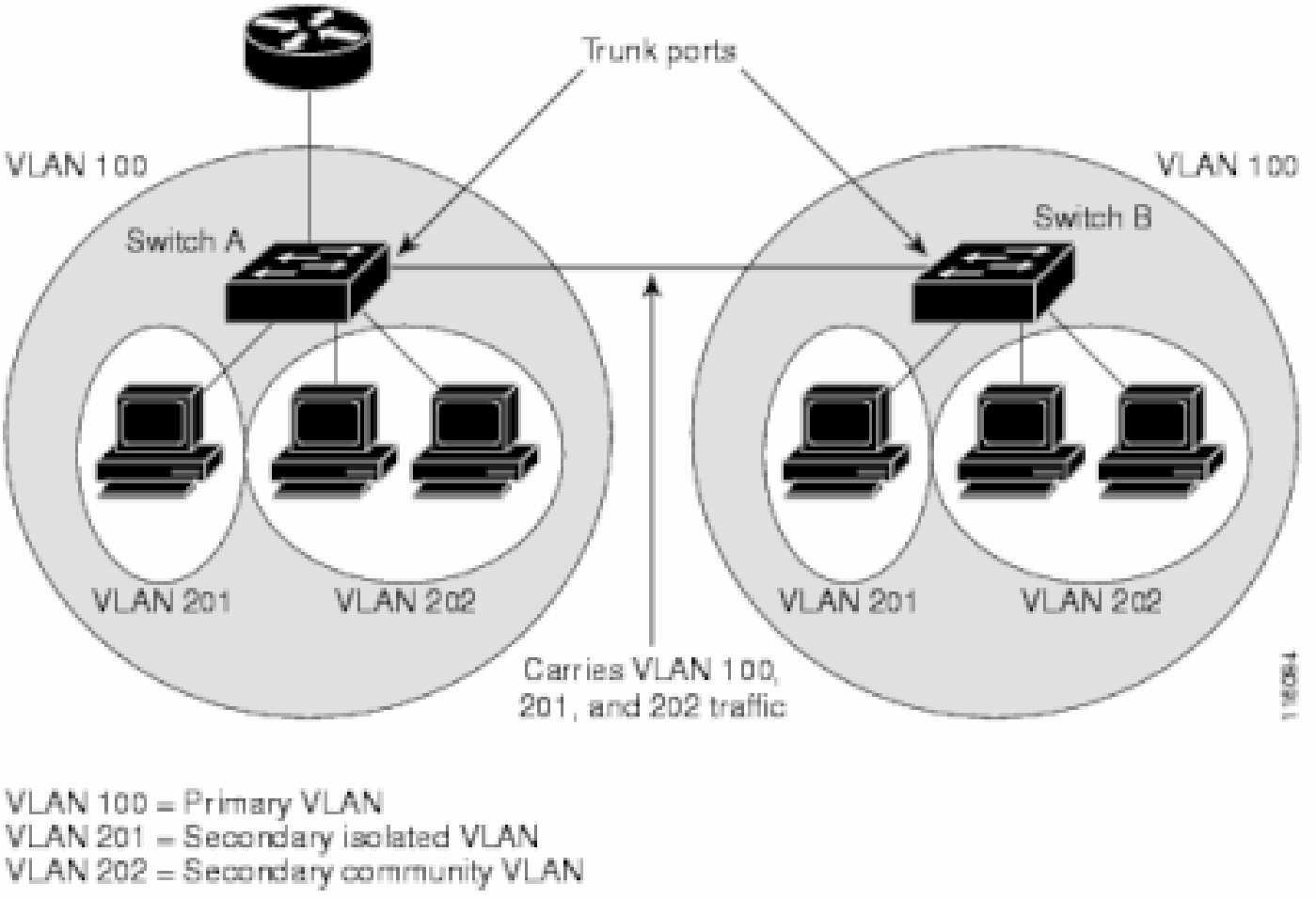
PVLAN は、通常の VLAN と同様、複数のスイッチにまたがることができます。トランク ポートが、プライマリ VLAN とセカンダリ VLAN を隣接するスイッチに伝送します。トランク ポートは、プライベート VLAN を他の VLAN と同じように処理します。複数のスイッチにまたがる PVLAN の特徴は、あるスイッチ内の隔離ポートからのトラフィックが、別のスイッチの隔離ポートに到達しないことです。

PVLAN 設定のセキュリティを保持し、PVLAN として設定されている VLAN が他の目的で使用されないようにするためには、PVLAN ポートを持たないデバイスも含めて、すべての中継デバイスで、PVLAN を設定します。

トランク ポートは、通常の VLAN からのトラフィックだけでなく、プライマリ VLAN、隔離 VLAN、およびコミュニティ VLAN からのトラフィックも伝送します。



ヒント：トランキングを実行する両方のスイッチがPVLANをサポートしている場合は、標準トランクポートを使用することをお勧めします。



レイヤ2ネットワーク内のすべてのスイッチでの*PVLAN*の手動設定

VTP は PVLAN をサポートしないため、レイヤ 2 ネットワーク内のすべてのスイッチで、PVLAN を手動で設定する必要があります。ネットワーク内のスイッチでプライマリ VLAN およびセカンダリ VLAN の関連付けを行わないと、そのスイッチ内のレイヤ 2 データベースが統合されません。この場合、該当のスイッチで PVLAN トラフィックの不要なフラッディングが発生する可能性があります。

プライベート VLAN トランク

PVLAN トランク ポートは、複数のセカンダリ PVLAN および PVLAN 以外を伝送できます。PVLAN トランク ポートでは、セカンダリまたは通常の VLAN タグを使用してパケットが送受信されます。

IEEE 802.1q カプセル化だけがサポートされています。隔離されたトランク ポートを使用すると、トランク経由のすべてのセカンダリ ポートのトラフィックを結合できます。混合モードのトランク ポートを使用すると、このトポロジで必要な複数の混合モード ポートを、複数のプライマリ VLAN を伝送する 1 つのトランク ポートに結合できます。

複数の VLAN (通常の VLAN または複数のプライベート VLAN ドメイン) を伝送するのに、プライベート VLAN の隔離ホスト ポートの使用が予想される場合は、隔離されたプライベート VLAN トランク ポートを使用します。これは、プライベート VLAN をサポートしないダウンストリーム スイッチの接続で役立ちます。

プライベート VLAN の混合モード トランクは、プライベート VLAN の混合モード ホスト ポートが通常は使用されるが、複数の VLAN (通常の VLAN または複数のプライベート VLAN ドメイン) を伝送する必要がある状況で使用されます。これは、プライベート VLAN をサポートしないアップストリーム ルータの接続で役立ちます。

追加情報

詳細は、『プライベート VLAN トランク』を参照してください。

インターフェイスをPVLANトランクポートとして設定するには、『レイヤ2インターフェイスをPVLANトランクポートとして設定』を参照してください。

インターフェイスを混合モードトランクポートとして設定するには、『レイヤ2インターフェイスを混合モードトランクポートとして設定』を参照してください。

確認

このセクションでは、設定が正常に動作していることを確認します。

CatOS

- **show pvlan**：PVLAN 設定を表示します。隔離 VLAN とプライマリ VLAN が互いに関連付けられていることを確認します。ホスト ポートが表示されることも確認します。
- **show pvlan mapping**：混合モード ポートで設定されている PVLAN マッピングを表示します。

Cisco IOS ソフトウェア

- **show vlan private-vlan**：関連付けられているポートなど、PVLAN 情報を表示します。
- **show interfacemod/portswitchport**：インターフェイス固有の情報を表示します。動作モードと、動作している PVLAN 設定が正しいことを確認します。
- **show interfaces private-vlan mapping**：設定した PVLAN マッピングを表示します。

確認手順

次のステップを実行します。

- スイッチの PVLAN 設定を確認します。

  プライマリ PVLAN とセカンダリ PVLAN が互いに関連付けられているか、またはマッピングされているかどうかを確認します。また、必要なポートが含まれていることも確認します。

```
    <#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
```

- 混合モード ポートが適切に設定されていることを確認します。

  次の出力は、ポートの動作モードが **promiscuous** であり、動作している **VLAN** が **100** および **101** であることを示しています。

<#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

•

Internet Control Message Protocoll（ICMP; インターネット制御メッセージ プロトコル）ping パケットを、ホスト ポートから混合モード ポートへ発信します。

両方のデバイスは同じプライマリ VLAN にあるため、これらは同じサブネット内に存在する必要があることに注意してください。

```
    <#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.
```

- ホスト ポート間で ICMP ping を開始します。

この例では、host_port_2(10.1.1.99)により、host_port(10.1.1.100)へのpingが試行されます。この ping は失敗します。ただし、別のホスト ポートから混合モード ポートへの ping は成功します。

```
    <#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.
```

トラブルシュート

PVLAN のトラブルシューティング

このセクションでは、PVLAN 設定に関して発生する一般的な問題について説明します。

問題 1

%PM-SP-3-ERR_INCOMP_PORT: <mod/port>はトランクポートであるため、inactiveに設定されています()。

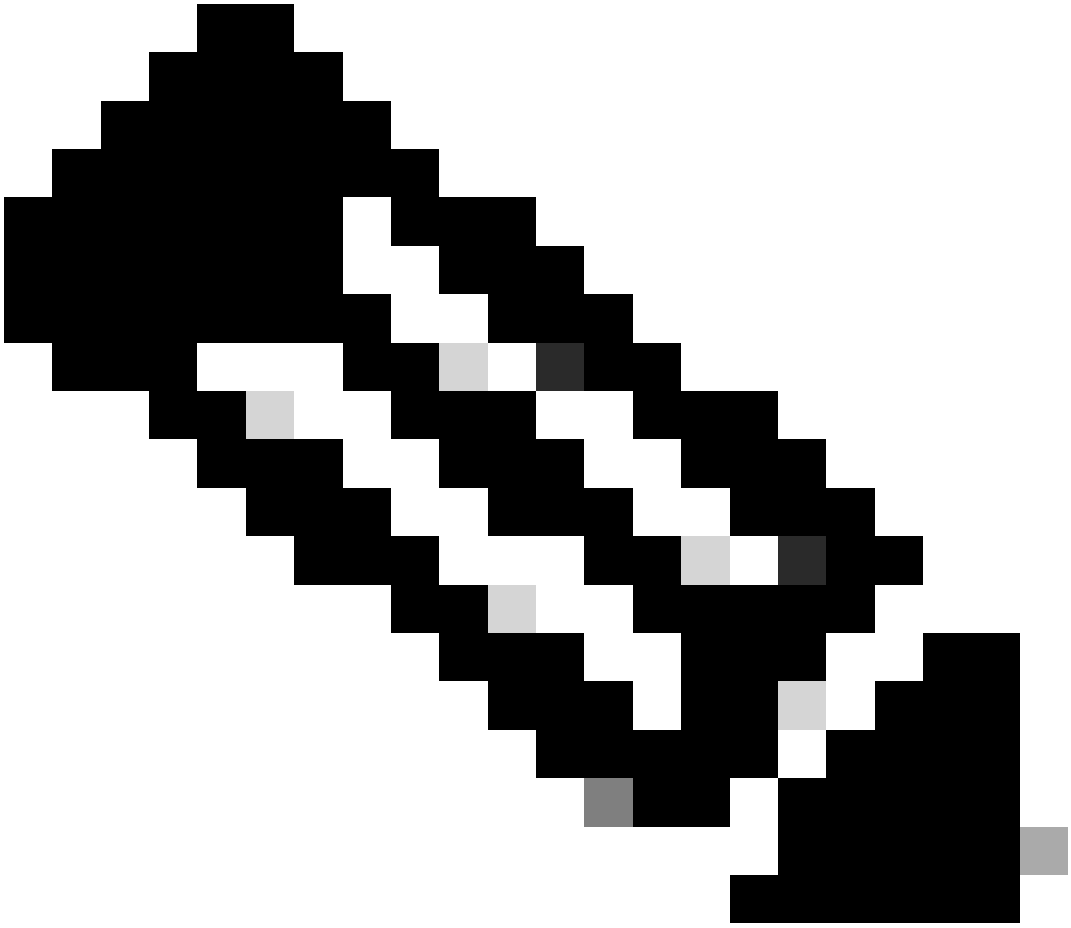
このエラー メッセージは、次に示すいくつかの理由が原因で表示されることがあります。

説明：同じCOIL ASIC内の1つのポートがトランク、SPAN宛先、または混合PVLANポートの場合、**1:**ハードウェアの制限により、Catalyst 6500/6000 10/100 Mbpsモジュールでは隔離VLANポートまたはコミュニティVLANポートの設定が制限されます。（COIL ASIC は、ほとんどのモジュールで 12 ポートを制御し、Catalyst 6548 モジュールで 48 ポートを制御します）。 このドキュメントの「ルールと制限事項」にある表に、Catalyst 6500/6000 10/100 Mbps モジュールのポート制限が詳しく記載されています。

解決手順 – 1:そのポートでPVLANがサポートされていない場合は、モジュール上の別のASIC上のポートか、別のモジュール上のポートを選択します。ポートを再度アクティブにするには、隔離 VLAN ポートまたはコミュニティ VLAN ポートの設定を削除し、**shutdown** コマンドと **no shutdown** コマンドを発行します。

説明：2:ポートが手動またはデフォルトで*dynamic desirable*モードか *dynamic auto*モードに設定されている場合。

解決手順2:switchport mode accessコマンドで、ポートをアクセスモードとして設定します。ポートを再度アクティブにするには、**shutdown** コマンドと **no shutdown** コマンドを発行します。



注:Cisco IOSソフトウェアリリース12.2(17a)SX以降のリリースでは、12ポートの制限はWS-X6548-RJ-45、WS-X6548-RJ-21、およびWS-X6524-100FX-MMイーサネットスイッチングモジュールには適用されません。

問題 2

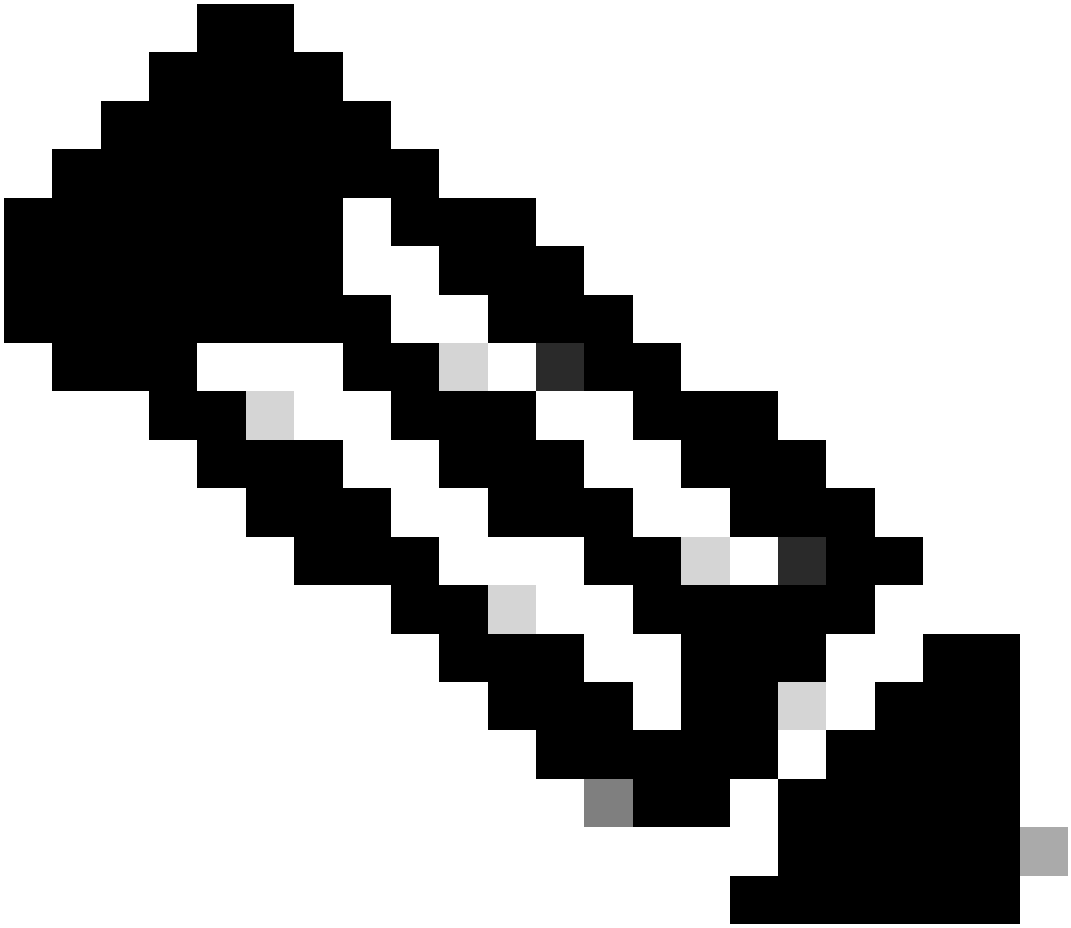
PVLAN の設定中に、次のいずれかのメッセージが表示される。

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.

説明：ハードウェアの制限により、同じCOIL ASIC内の1つのポートがトランク、SPAN宛先、または混合PVLANポートの場合、Catalyst 6500/6000 10/100 Mbpsモジュールでは隔離VLANポートまたはコミュニティVLANポートの設定が制限されます。（COIL ASIC は、ほとんどのモジュールで 12 ポートを制御し、Catalyst 6548 モジュールで 48 ポートを制御します）。 このドキュメントの「ルールと制限事項」にある表に、Catalyst 6500/6000 10/100 Mbps モジュールのポート制限が詳しく記載されています。

解決手順：show pvlan capabilityコマンド(CatOS)を発行します。ポートをPVLANポートにできるかどうかが示されます。その特定のポートで PVLAN がサポートされていない場合は、そのモジュールの別の ASIC 上のポートか、別のモジュールのポートを選択します。



注:Cisco IOSソフトウェアリリース12.2(17a)SX以降のリリースでは、12ポートの制限はWS-X6548-RJ-45、WS-X6548-RJ-21、およびWS-X6524-100FX-MMイーサネットスイッチングモジュールには適用されません。

問題 3

一部のプラットフォームで PVLAN を設定できない。

解決策：プラットフォームがPVLANをサポートしていることを確認します。設定を開始する前に、『プライベート VLAN Catalyst スイッチのサポート一覧』を参照して、ご使用のプラットフォームとソフトウェア バージョンが PVLAN をサポートしているかどうかを確認してください。

問題 4

Catalyst 6500/6000 MSFC で、スイッチの隔離ポートに接続されているデバイスに対して ping を実行できない。

解決策：スーパーバイザエンジンで、MSFC（15/1または16/1）へのポートが混合モードであることを確認します。

```
<#root>

cat6000> (enable)

set pvlan mapping primary_vlan secondary_vlan 15/1

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

また、このドキュメントの「レイヤ 3 の設定」に従って、MSFC で VLAN インターフェイスを設定します。

問題 5

no shutdown コマンドを発行しても、隔離 VLAN またはコミュニティ VLAN の VLAN インターフェイスをアクティブにできない。

解決策：PVLANの性質上、隔離VLANまたはコミュニティVLANのVLANインターフェイスをアクティブにできません。アクティ

ブにできるのは、プライマリ VLAN に属している VLAN インターフェイスだけです。

問題 6

MSFC/MSFC2 を搭載した Catalyst 6500/6000 デバイスで、レイヤ 3 PVLAN インターフェイスで学習された ARP エントリがエージング アウトしない。

解決策：レイヤ3プライベートVLANインターフェイスで学習されたARPエントリは、スティッキARPエントリであり、エージングアウトしません。同じ IP アドレスに新しい機器を接続するとメッセージが生成され、ARP エントリは作成されません。したがって、MAC アドレスを変更した場合は、PVLAN ポートの ARP エントリを手動で削除する必要があります。PVLAN ARP エントリを追加または削除するには、次のコマンドを発行します。

```
<#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
```

Cisco IOS ソフトウェア 12.1(11b)E 以降のリリースでは、**no ip sticky-arp** コマンドを発行する方法もあります。

関連情報

- **Cisco Catalyst 2955シリーズスイッチ – 廃止通知**

- **PVLANとVACLを使用したセキュアネットワーク**
- **LAN スイッチングに関するサポート ページ**
- **シスコのテクニカルサポートとダウンロード**

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。