Catalyst スイッチにおける隔離されたプライベート VLAN の設定

目次

概要

状況によっては、スイッチ上のエンド デバイス間のレイヤ 2 (L2) 接続を、異なる IP サブネットにデバイスを配置することなく阻止する必要があります。 そうすることで、IP アドレスを無駄に使用せずに済みます。 プライベート VLAN (PVLAN) を使用すると、同じ IP サブネット内のデバイスをレイヤ 2 で隔離できます。 スイッチの一部のポートが、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にだけアクセスできるように制限できます。

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。 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。

注: スイッチによっては（『プライベート VLAN Catalyst スイッチのサポート一覧』を参照）、現在、PVLAN エッジ機能だけがサポートされています。 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くものです。

- 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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『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。

背景理論

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 ポートには次の 3 種類があります。 混合モード、隔離モード、コミュニティ モードです。

- 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ません。

PVLAN の詳細は、『*VLAN の説明と設定*』の「プライベート VLAN の設定」を参照してください。

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。 詳細なリストについては、『*VLAN の設定*』の「プライベート VLAN の設定ガイドライン」を参照してください。

- 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。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。 詳細は、『プライベート VLAN の設定』を参照してください。
- 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、transparent モードの VTP がこの情報を伝搬しないためです。

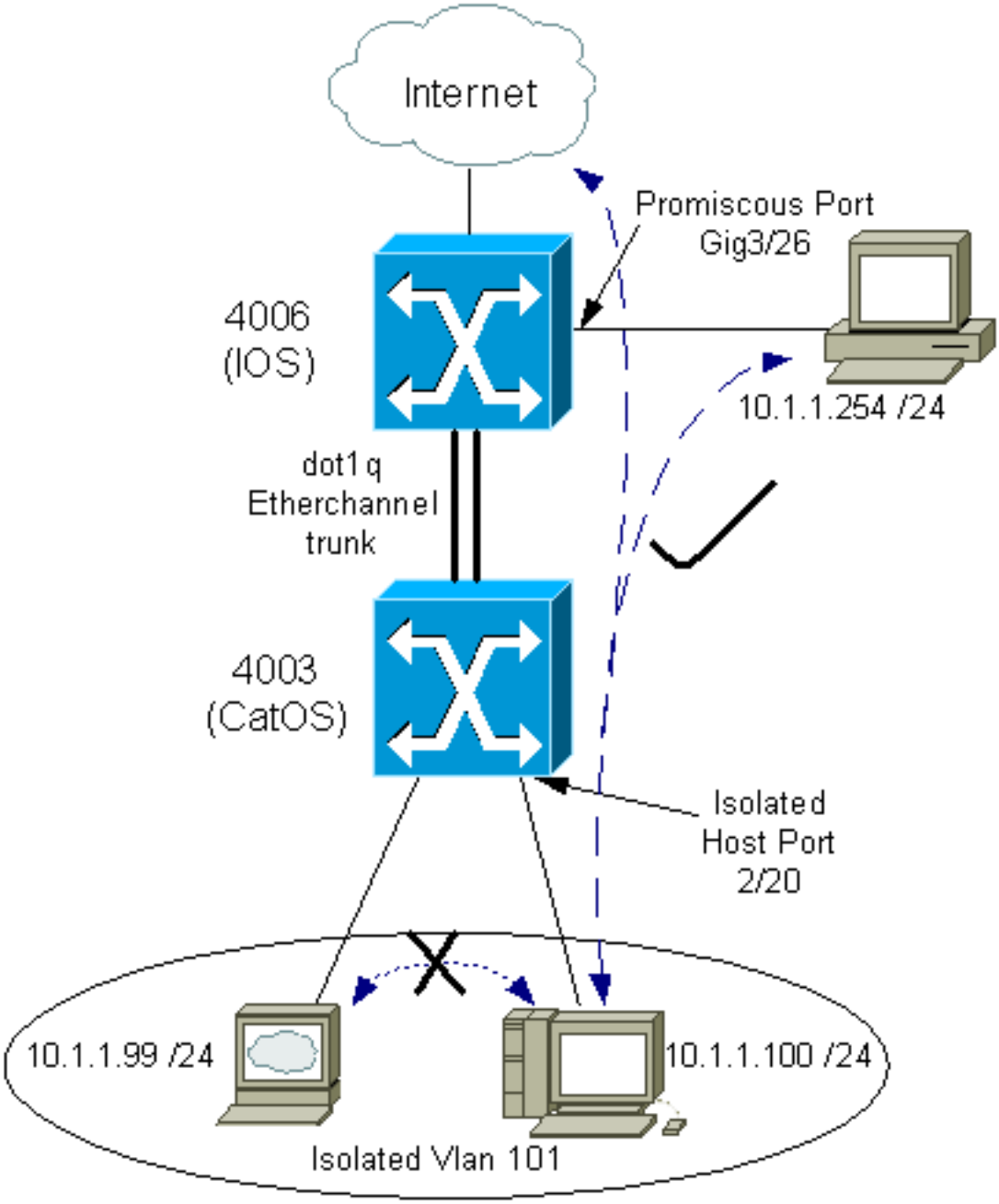
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

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。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



このシナリオでは、隔離 VLAN（101）のデバイスは、レイヤ 2 での相互の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。 さらに、4006 上のポート「Gig 3/26」は混合モードとして指定されています。 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。 この手順には、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
```
Switch_CatOS> (enable) set vlan primary_vlan_id pvlan-type primary name primary_vlan
!--- Note: Thise command should be on one line.

VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 100 configuration successfulCisco IOS ソフトウェア
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
```
Switch_CatOS> (enable) set vlan secondary_vlan_id pvlan-type isolated name isolated_pvlan
!--- Note: This command should 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。CatOSSwitch_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
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。CatOSSwitch_CatOS> (enable) **show pvlan**
```
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
100     101       isolated     Cisco IOS ソフトウェア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： 次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、ポートが PVLAN ポートになるかどうかを判断します。

注: 次の手順 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。

1. 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
```
Switch_CatOS> (enable)set pvlan primary_vlan_id secondary_vlan_id mod/port
!--- Note: This command should be on one line.

Successfully set the following ports to Private Vlan 100,101: 2/20Cisco IOS ソフトウェア
Switch_IOS(config)#interface gigabitEthernet mod/port
Switch_IOS(config-if)#switchport private-vlan host
```

```
primary_vlan_id secondary_vlan_id
!--- Note: This command should be on one line.

Switch_IOS(config-if)#switchport mode private-vlan host
Switch_IOS(config-if)#exit
```

2. 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**`Switch_CatOS>`
   `(enable) set pvlan mapping primary_vlan_id secondary_vlan_id mod/port`
   `!--- Note: This command should be on one line.`

   `Successfully set mapping between 100 and 101 on 3/26`**注:** Catalyst 6500/6000 で、スーパーバイザ エンジンがシステム ソフトウェアとして CatOS を実行している場合、VLAN 間でレイヤ 3 のスイッチングを行うには、スーパーバイザ エンジンの MSFC ポート（15/1 または 16/1）が混合モードである必要があります。**Cisco IOS ソフトウェア**
   ```
   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 should 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。

1. 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。
2. 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。
   ```
   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ます。 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。
3. **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。
4. 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。`Switch_IOS(config-if)#private-vlan mapping add secondary_vlan_list`
   or
   `Switch_IOS(config-if)#private-vlan mapping remove secondary_vlan_list`

詳細については、『プライベート *VLAN* の設定』の「プライマリ VLAN のレイヤ 3 VLAN インターフェイスへのセカンダリ VLAN のマッピング」を参照してください。

注: MSFC を搭載した Catalyst 6500/6000 スイッチの場合、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（たとえば、ポート 15/1 または 16/1）が混合モードであることを確認します。

```
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。

```
cat6000> (enable) show pvlan mapping
Port Primary Secondary
---- ------- ---------
15/1  100      101
```

設定

このドキュメントでは、次の設定を使用します。

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

Access_Layer (Catalyst 4003： CatOS)

```
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 should 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 should 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）

```
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

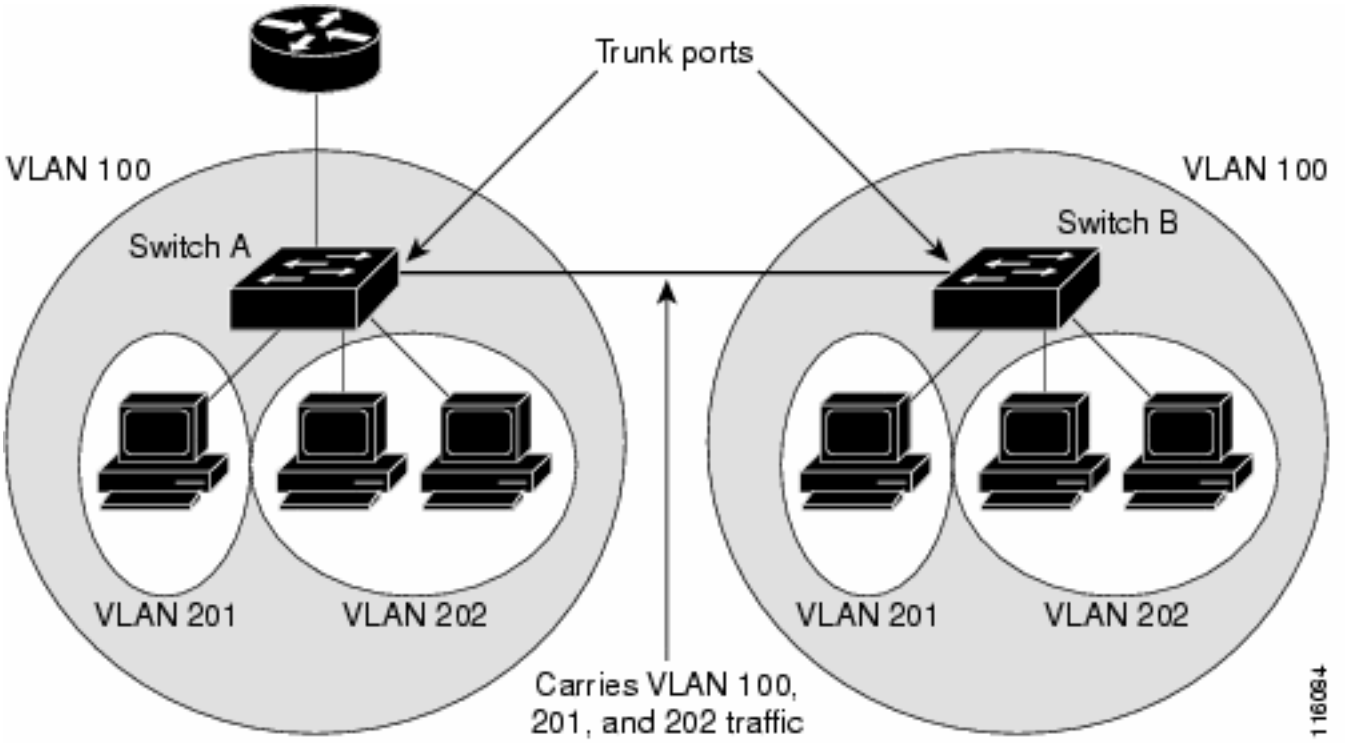
通常のトランク

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。



VLAN 100 = Primary VLAN
VLAN 201 = Secondary isolated VLAN
VLAN 202 = Secondary community VLAN

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。

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 ポートして設定する方法については、『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 ポートして設定する方法については、『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

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool (OIT) (登録ユーザ専用) では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

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 interface mod/port switchport**：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

次の手順を実行します。

1. 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。`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. 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。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. 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。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. ホスト ポート間で ICMP ping を開始します。次の例では、host_port_2 (10.1.1.99) により、host_port (10.1.1.100) への ping の実行を試みます。 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。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.
```

トラブルシューティング

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

次のエラー メッセージが表示される：「`%PM-SP-3-ERR_INCOMP_PORT: <mod/port> is set to inactive because <mod/port> is a trunk port`

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 1： ハードウェアの制約により、同じ COIL ASIC 内のポートがトランク、SPAN 宛先、または混合モード PVLAN ポートの場合、Catalyst 6500/6000 10/100 Mbps モジュールは、隔離 VLAN ポートまたはコミュニティ VLAN ポートの設定を制限します（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： 該当のポートで 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。 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* モードまたは *dynamic auto* モードに設定されている場合。

決定手順- 2: switchport mode access コマンドで、ポートを access 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 12.2(17a)SX 以降のリリースでは、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 12 ポートの制限は適用されません。 他の機能に関する PVLAN の設定制限についての詳細は、『プライベート VLAN（PVLAN）の設定』の「他の機能の制限事項」を参照してください。

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。

- `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.
```

- 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.
```

説明： ハードウェアの制約により、同じ COIL ASIC 内のポートがトランク、SPAN 宛先、または混合モード PVLAN ポートの場合、Catalyst 6500/6000 10/100 Mbps モジュールは、隔離 VLAN ポートまたはコミュニティ VLAN ポートの設定を制限します（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 12.2(17a)SX 以降のリリースでは、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 12 ポートの制限は適用されません。 他の機能に関する PVLAN の設定制限についての詳細は、『プライベート VLAN（PVLAN）の設定』の「他の機能の制限事項」を参照してください。

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 に対するポート（15/1 または 16/1）が混合モードであることを確認します。

```
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 インターフェイスは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。

```
Router(config)#no arp 11.1.3.30
IP ARP:Deleting Sticky ARP entry 11.1.3.30
Router(config)#arp 11.1.3.30 0000.5403.2356 arpa
IP ARP:Overwriting Sticky ARP entry 11.1.3.30, 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

- プライベート VLAN Catalyst スイッチのサポート一覧
- プライベート VLAN および VLAN アクセス コントロール リストによるネットワーク セキュリティの確保
- プライベート VLAN の設定
- LAN 製品に関するサポート ページ
- LAN スイッチングに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems