



プライベート VLAN の設定

この章の内容は、次のとおりです。

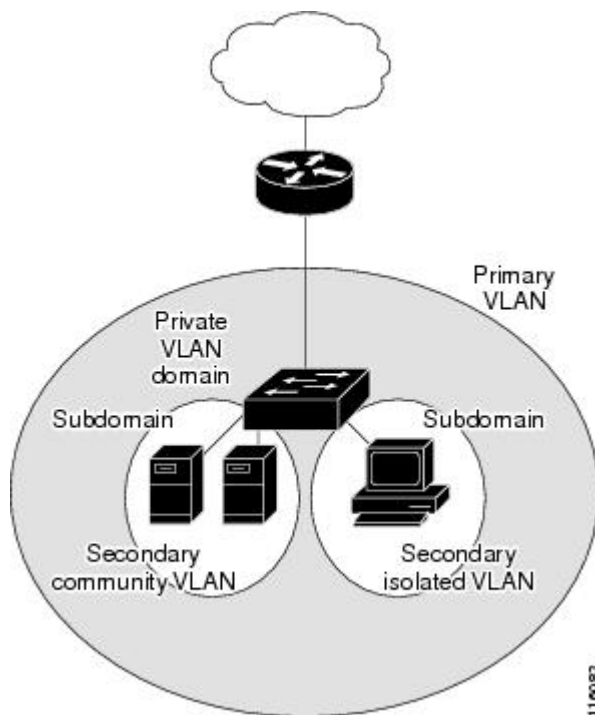
- [プライベート VLAN について, 1 ページ](#)
- [プライベート VLAN に関する注意事項および制約事項, 7 ページ](#)
- [プライベート VLAN の設定, 8 ページ](#)
- [プライベート VLAN 設定の確認, 19 ページ](#)

プライベート VLAN について

プライベート VLAN (PVLAN) では VLAN のイーサネットブロードキャストドメインがサブドメインに分割されるため、スイッチ上のポートを互いに分離することができます。サブドメインは、1つのプライマリ VLAN と 1つ以上のセカンダリ VLAN とで構成されます（次の図を参照）。1つの PVLAN に含まれる VLAN はすべて、同じプライマリ VLAN を共有します。セカンダリ VLAN ID は、各サブドメインの区別に使用されます。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかの場合があります。独立 VLAN 上のホストは、そのプライマリ VLAN 上でアソシエートされている無差別ポートのみと通信できます。コミュニティ VLAN 上の

ホストは、それぞれのホスト間およびアソシエートされている無差別ポートと通信できますが、他のコミュニティ VLAN にあるポートとは通信できません。

図 1: プライベート VLAN ドメイン



(注) VLAN をプライマリまたはセカンダリの PVLAN に変換する場合は、あらかじめその VLAN を作成しておく必要があります。

プライベート VLAN のプライマリ VLAN とセカンダリ VLAN

プライベート VLAN ドメインには、プライマリ VLAN が 1 つのみ含まれています。プライベート VLAN ドメインの各ポートは、プライマリ VLAN のメンバです。プライマリ VLAN は、プライベート VLAN ドメイン全体です。

セカンダリ VLAN は、同じプライベート VLAN ドメイン内のポート間を分離します。プライマリ VLAN 内のセカンダリ VLAN には、次の 2 つのタイプがあります。

- 独立 VLAN : 独立 VLAN 内のポートは、レイヤ 2 レベルで直接かつ相互には通信できません。
- コミュニティ VLAN : コミュニティ VLAN 内のポートは相互通信できますが、他のコミュニティ VLAN またはレイヤ 2 レベルの独立 VLAN にあるポートとは通信できません。

プライベート VLAN ポート

PVLAN ポートには、次の 3 種類があります。

- 無差別ポート：無差別ポートはプライマリ VLAN に属します。無差別ポートは、無差別ポートとアソシエートされているセカンダリ VLAN に属し、プライマリ VLAN とアソシエートされている、すべてのインターフェイスと通信でき、この通信可能なインターフェイスには、コミュニティポートと独立ポートも含まれます。プライマリ VLAN には、複数の無差別ポートを含めることができます。各無差別ポートには、複数のセカンダリ VLAN を関連付けることができるほか、セカンダリ VLAN をまったく関連付けないことも可能です。無差別ポートとセカンダリ VLAN が同じプライマリ VLAN にある限り、セカンダリ VLAN は、複数の無差別ポートとアソシエートすることができます。ロードバランシングまたは冗長性を持たせる目的で、これを行う必要が生じる場合があります。無差別ポートとアソシエートされていないセカンダリ VLAN も、含めることができます。

無差別ポートは、アクセスポートまたはトランクポートとして設定できます。

- 独立ポート：独立セカンダリ VLAN に属するホストポート。このポートは、同じ PVLAN ドメイン内の他のポートから完全に独立しています。ただし、関連付けられている無差別ポートと通信することはできます。PVLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。独立ポートから受信されたトラフィックは、無差別ポートだけに転送されます。指定した独立 VLAN には、複数の独立ポートを含めることができます。各ポートは、独立 VLAN にある他のすべてのポートから、完全に隔離されています。

独立ポートは、アクセスポートまたはトランクポートとして設定できます。

- コミュニティポート：コミュニティセカンダリ VLAN に属するホストポートです。コミュニティポートは、同じコミュニティ VLAN にある他のポートおよびアソシエートされている無差別ポートと通信します。これらのインターフェイスは、他のコミュニティにあるすべてのインターフェイス、および PVLAN ドメイン内のすべての独立ポートから分離されています。

コミュニティポートは、アクセスポートとして設定する必要があります。独立トランクに対してコミュニティ VLAN をイネーブルにすることはできません。



(注) ファブリック エクステンダ (FEX) のトランクポートは、FEX トランクポートにすることも、FEX 独立トランクポートにすることもできます。



(注) トランクは、無差別ポート、独立ポート、およびコミュニティポートの間でトラフィックを伝送する VLAN をサポートできるため、独立ポートとコミュニティポートのトラフィックはトランク インターフェイスを経由してスイッチと送受信されることがあります。

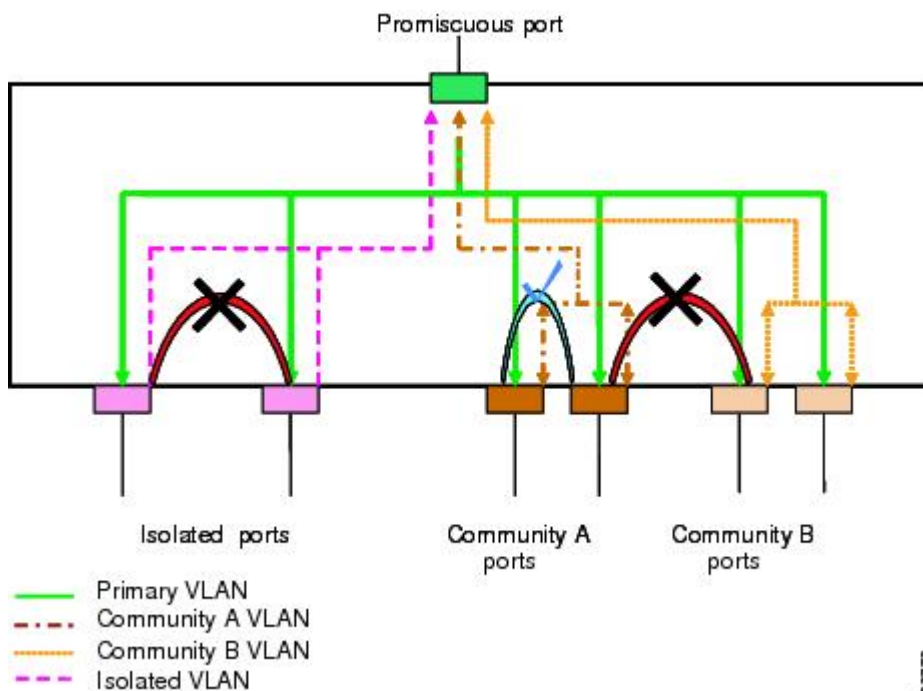
プライマリ、独立、およびコミュニティ プライベート VLAN

プライマリ VLAN および2つのタイプのセカンダリ VLAN（独立 VLAN とコミュニティ VLAN）には、次の特徴があります。

- **プライマリ VLAN**：独立ポートおよびコミュニティポートであるホストポート、および他の無差別ポートに、無差別ポートからトラフィックを伝送します。
- **独立 VLAN**：ホストから無差別ポートにアップストリームに単方向トラフィックを伝送するセカンダリ VLAN です。1つの PVLAN ドメイン内で設定できる独立 VLAN は1つだけです。独立 VLAN には、複数の独立ポートを設定できます。各独立ポートからのトラフィックも完全に隔離されたままです。
- **コミュニティ VLAN**：コミュニティ VLAN は、コミュニティポートから、無差別ポートおよび同じコミュニティにある他のホストポートへ、アップストリームトラフィックを送信するセカンダリ VLAN です。1つの PVLAN ドメインには、複数のコミュニティ VLAN を設定できます。1つのコミュニティ内のポートは相互に通信できますが、これらのポートは、他のコミュニティにあるポートとも、プライベート VLAN にある独立 VLAN とも、通信できません。

次の図は、PVLAN 内でのトラフィックフローを VLAN およびポートのタイプ別に示したものです。

図 2：プライベート VLAN のトラフィックフロー





- (注) PVLAN のトラフィック フローは、ホスト ポートから無差別ポートへの単方向です。プライマリ VLAN で受信したトラフィックによって隔離は行われず、転送は通常の VLAN として実行されます。

無差別アクセスポートでは、1 つだけのプライマリ VLAN と複数のセカンダリ VLAN (コミュニティ VLAN および独立 VLAN) を処理できます。無差別トランク ポートでは、複数のプライマリ VLAN のトラフィックを伝送できます。指定されたプライマリ VLAN の複数のセカンダリ VLAN を無差別トランク ポートにマッピングできます。無差別ポートを使用すると、さまざまなデバイスを PVLAN への「アクセスポイント」として接続できます。たとえば、すべての PVLAN サーバを管理ワークステーションから監視したりバックアップしたりするのに、無差別ポートを使用できます。

スイッチング環境では、個々のエンドステーションに、または共通グループのエンドステーションに、個別の PVLAN や、関連する IP サブネットを割り当てることができます。プライベート VLAN の外部と通信するには、エンドステーションでは、デフォルトゲートウェイのみと通信する必要があります。

プライマリ VLAN とセカンダリ VLAN のアソシエーション

セカンダリ PVLAN 内のホスト ポートで PVLAN の外部と通信できるようにするためには、セカンダリ VLAN をプライマリ VLAN に関連付ける必要があります。アソシエーションの操作が可能ではない場合、セカンダリ VLAN のホスト ポート (コミュニティ ポートと独立ポート) は、ダウンされます。



- (注) セカンダリ VLAN は、1 つのプライマリ VLAN のみにアソシエートすることができます。

アソシエーションの操作を可能にするには、次の条件を満たす必要があります。

- プライマリ VLAN を終了し、プライマリ VLAN として設定する必要があります。
- セカンダリ VLAN を終了し、独立 VLAN またはコミュニティ VLAN として設定する必要があります。



- (注) 関連付けの操作が可能かどうかを確認する場合は、**show vlan private-vlan** コマンドを使用します。関連付けが動作していないとき、スイッチはエラー メッセージを表示しません。

プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。VLAN を通常モードに戻す場合は、**no private-vlan** コマンドを使用します。その VLAN におけるプライマリとセカンダリの関連付けはすべて一時停止されますが、インターフェイスは PVLAN モードのままです。VLAN を PVLAN モードに戻すと、関連付けも元の状態に戻ります。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN に関連付けられている PVLAN はすべて削除されます。ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN と PVLAN との関連付けは一時停止します。この VLAN を再作成して以前のセカンダリ VLAN として設定すると、関連付けは元の状態に戻ります。

セカンダリ VLAN とプライマリ VLAN の関連付けを変更するには、現在の関連付けを削除してから目的の関連付けを追加します。

プライベート VLAN 無差別トランク

無差別トランク ポートは、複数のプライマリ VLAN のトラフィックを伝送できます。無差別トランク ポートには、同じプライマリ VLAN に従属する複数のセカンダリ VLAN をマップすることができます。無差別ポートのトラフィックはプライマリ VLAN タグとともに送受信されます。

プライベート VLAN 独立トランク

Cisco Nexus 3000 シリーズのデバイスはプライベート VLAN トランク ポートをサポートしません。

独立トランク ポートでは、複数の独立 PVLAN のトラフィックを伝送することができます。コミュニティ VLAN のトラフィックは、独立トランク ポートで伝送されません。独立トランク ポートのトラフィックは、独立 VLAN タグとともに送受信されます。独立トランク ポートは、ホストサーバに接続するように設計されています。

Cisco Nexus 2000 シリーズ FEX の独立 PVLAN ポートをサポートするためには、Cisco Nexus 5000 シリーズスイッチにより FEX 上の独立ポート間の通信が回避される必要があります。転送はすべて、スイッチを経由して行われます。



注意

FEX トランク ポートで PVLAN を設定する場合は、その前に FEX 独立トランク ポートをすべてディセーブルにしておく必要があります。FEX 独立トランク ポートと FEX トランク ポートをともにイネーブルにすると、不要なネットワーク トラフィックが発生することがあります。

ユニキャスト トラフィックに対しては、他に影響を与えることなく、こうした通信を回避することができます。

マルチキャスト トラフィックに対しては、FEX によりフレームのレプリケーションが行われます。FEX の独立 PVLAN ポート間での通信を回避するため、スイッチではマルチキャストフレームがファブリック ポート経由で返送されないようになっています。これにより、FEX 上の独立 VLAN と無差別ポートとの間での通信は行われません。ただし、ホストインターフェイスは別のスイッチやルータに接続することを目的としたものではないため、FEX で無差別ポートをイネーブルにすることはできません。

プライベート VLAN 内のブロードキャストトラフィック

プライベート VLAN にあるポートからのブロードキャストトラフィックは、次のように流れます。

- ブロードキャストトラフィックは、プライマリ VLAN で、無差別ポートからすべてのポート（コミュニティ VLAN と独立 VLAN にあるすべてのポートも含む）に流れます。このブロードキャストトラフィックは、プライベート VLAN パラメータで設定されていないポートを含め、プライマリ VLAN 内のすべてのポートに配信されます。
- 独立ポートからのブロードキャストトラフィックは、独立ポートにアソシエートされているプライマリ VLAN にある無差別ポートにのみ配信されます。
- コミュニティポートからのブロードキャストトラフィックは、そのポートのコミュニティ内のすべてのポート、およびそのコミュニティポートに関連付けられているすべての無差別ポートに配信されます。このブロードキャストパケットは、プライマリ VLAN 内の他のコミュニティまたは独立ポートには配信されません。

プライベート VLAN ポートの分離

PVLAN を使用すると、次のように、エンドステーションへのアクセスを制御できます。

- 通信を防止するには、エンドステーションに接続されているインターフェイスのうち、選択したインターフェイスを、独立ポートとして設定します。たとえば、エンドステーションがサーバの場合、この設定により、サーバ間の通信が防止されます。
- すべてのエンドステーションがデフォルトゲートウェイにアクセスできるようにするには、デフォルトゲートウェイおよび選択したエンドステーション（バックアップサーバなど）に接続されているインターフェイスを、無差別ポートとして設定します。

プライベート VLAN に関する注意事項および制約事項

PVLAN を設定する場合は、次の注意事項に従ってください。

- 指定した VLAN をプライベート VLAN として割り当てる前に、VLAN を作成しておく必要があります。
- スイッチで PVLAN 機能を適用できるようにするには、あらかじめ PVLAN をイネーブルにしておく必要があります。
- PVLAN モードで動作しているポートがスイッチにある場合、PVLAN をディセーブルにすることはできません。
- プライマリ VLAN と同じ MST インスタンスにセカンダリ VLAN マッピングするには、Multiple Spanning Tree (MST) リージョン定義内から **private-vlan synchronize** コマンドを入力します。

- FEX トランク ポートを設定する場合は、その前にすべての FEX 独立トランク ポートをディセーブルにしておく必要があります。
- Cisco NX-OS Release 5.0(2)N2(1) 以降では、各 PVLAN トランク ポートに対するマッピングの数は最大 16 です。

プライベート VLAN の設定

プライベート VLAN をイネーブルにするには

PVLAN 機能を使用するためには、スイッチ上で PVLAN をイネーブルにする必要があります。



(注) PVLAN コマンドは、PVLAN 機能をイネーブルにするまで表示されません。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature private-vlan**
3. (任意) switch(config)# **no feature private-vlan**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# feature private-vlan	スイッチの PVLAN 機能をイネーブルにします。
ステップ 3	switch(config)# no feature private-vlan	(任意) スイッチの PVLAN 機能をディセーブルにします。 (注) スイッチ上に PVLAN モードで動作しているポートがある場合は、PVLAN をディセーブルにすることはできません。

次の例は、スイッチの PVLAN 機能をイネーブルにする方法を示したものです。

```
switch# configure terminal
switch(config)# feature private-vlan
```


プライベート VLAN としての VLAN の設定

PVLAN を作成するには、まず VLAN を作成したうえで、その VLAN を PVLAN として設定します。

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vlan** {vlan-id | vlan-range}
3. switch(config-vlan)# **private-vlan** {community | isolated | primary}
4. (任意) switch(config-vlan)# **no private-vlan** {community | isolated | primary}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# vlan {vlan-id vlan-range}	VLAN 設定サブモードにします。
ステップ 3	switch(config-vlan)# private-vlan {community isolated primary}	VLAN を、コミュニティ PVLAN、独立 PVLAN、またはプライマリ PVLAN として設定します。PVLAN には、プライマリ VLAN を 1 つ設定する必要があります。複数のコミュニティ VLAN と独立 VLAN を設定することができます。
ステップ 4	switch(config-vlan)# no private-vlan {community isolated primary}	(任意) 指定した VLAN から PVLAN の設定を削除し、通常の VLAN モードに戻します。プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。

次の例は、VLAN 5 をプライマリ VLAN として PVLAN に割り当てる方法を示したものです。

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# private-vlan primary
```

次の例は、VLAN 100 をコミュニティ VLAN として PVLAN に割り当てる方法を示したものです。

```
switch# configure terminal
switch(config)# vlan 100
switch(config-vlan)# private-vlan community
```

次の例は、VLAN 200 を独立 VLAN として PVLAN に割り当てる方法を示したものです。

```
switch# configure terminal
switch(config)# vlan 200
switch(config-vlan)# private-vlan isolated
```

セカンダリ VLAN のプライマリ プライベート VLAN とのアソシエーション

セカンダリ VLAN をプライマリ VLAN とアソシエートするときには、次の事項に注意してください。

- *secondary-vlan-list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目は、単一のセカンダリ VLAN ID、またはセカンダリ VLAN ID をハイフンでつないだ範囲にできます。
- *secondary-vlan-list* パラメータには、複数のコミュニティ VLAN ID と 1 つの独立 VLAN ID を指定できます。
- セカンダリ VLAN をプライマリ VLAN にアソシエートするには、*secondary-vlan-list* と入力するか、*secondary-vlan-list* に **add** キーワードを使用します。
- セカンダリ VLAN とプライマリ VLAN とのアソシエーションをクリアするには、*secondary-vlan-list* に **remove** キーワードを使用します。
- セカンダリ VLAN とプライマリ VLAN とのアソシエーションを変更するには、既存のアソシエーションを削除し、次に必要なアソシエーションを追加します。

プライマリまたはセカンダリ VLAN のいずれかを削除すると、VLAN はアソシエーションが設定されたポートで非アクティブになります。 **no private-vlan** コマンドを入力すると、VLAN は通常の VLAN モードに戻ります。その VLAN におけるプライマリとセカンダリの関連付けはすべて一時停止されますが、インターフェイスは PVLAN モードのままです。指定した VLAN を PVLAN モードに再変換すると、関連付けも元の状態に戻ります。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN に関連付けられている PVLAN はすべて失われます。ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN と PVLAN との関連付けは一時停止します。この VLAN を再作成して以前のセカンダリ VLAN として設定すると、関連付けは元の状態に戻ります。

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vlan primary-vlan-id**
3. switch(config-vlan)# **private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}
4. (任意) switch(config-vlan)# **no private-vlan association**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# vlan primary-vlan-id	PVLAN の設定作業を行うプライマリ VLAN の番号を入力します。
ステップ 3	switch(config-vlan)# private-vlan association {[add] <i>secondary-vlan-list</i> remove <i>secondary-vlan-list</i> }	セカンダリ VLAN をプライマリ VLAN に関連付けます。セカンダリ VLAN とプライマリ VLAN とのアソシエーションをクリアするには、 <i>secondary-vlan-list</i> に remove キーワードを使用します。
ステップ 4	switch(config-vlan)# no private-vlan association	(任意) プライマリ VLAN からすべてのアソシエーションを削除し、通常の VLAN モードに戻します。

次に、コミュニティ VLAN 100 ~ 110 および独立 VLAN 200 をプライマリ VLAN 5 に関連付ける例を示します。

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# private-vlan association 100-110, 200
```

インターフェイスをプライベート VLAN ホストポートとして設定するには

PVLAN では、ホストポートはセカンダリ VLAN の一部であり、セカンダリ VLAN はコミュニティ VLAN または独立 VLAN のいずれかです。PVLAN のホストポートを設定する手順には2つのステップがあります。1つ目はポートを PVLAN のホストポートとして定義すること、2つ目はプライマリ VLAN とセカンダリ VLAN のホストアソシエーションを設定することです。



(注) ホストポートとして設定したすべてのインターフェイスで BPDU ガードをイネーブルにすることを推奨します。

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type [chassis/]slot/port**
3. switch(config-if)# **switchport mode private-vlan host**
4. switch(config-if)# **switchport private-vlan host-association {primary-vlan-id} {secondary-vlan-id}**
5. (任意) switch(config-if)# **no switchport private-vlan host-association**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface type [chassis/]slot/port	PVLAN のホスト ポートとして設定するポートを選択します。このポートとしては、FEX のポートを選択できます (chassis オプションで指定)。
ステップ 3	switch(config-if)# switchport mode private-vlan host	選択したポートを PVLAN のホストポートとして設定します。
ステップ 4	switch(config-if)# switchport private-vlan host-association {primary-vlan-id} {secondary-vlan-id}	選択したポートを、PVLAN のプライマリ VLAN とセカンダリ VLAN に関連付けます。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。
ステップ 5	switch(config-if)# no switchport private-vlan host-association	(任意) PVLAN の関連付けをポートから削除します。

次の例は、PVLAN のホスト ポートとしてイーサネット ポート 1/12 を設定し、プライマリ VLAN 5 とセカンダリ VLAN 101 にそのポートを関連付ける方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/12
switch(config-if)# switchport mode private-vlan host
switch(config-if)# switchport private-vlan host-association 5 101
```

インターフェイスをプライベート VLAN 無差別ポートとして設定するには

PVLAN ドメインでは、無差別ポートはプライマリ VLAN の一部です。無差別ポートの設定には、2 つの手順が必要です。最初にポートを無差別ポートに定義した後で、セカンダリ VLAN とプライマリ VLAN 間のマッピングを設定します。

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **switchport mode private-vlan promiscuous**
4. switch(config-if)# **switchport private-vlan mapping {primary-vlan-id} {secondary-vlan-list | add secondary-vlan-list | remove secondary-vlan-list}**
5. (任意) switch(config-if)# **no switchport private-vlan mapping**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface type slot/port	PVLAN の無差別ポートとして設定するポートを選択します。物理インターフェイスが必要です。このポートとして、FEX のポートを選択することはできません。
ステップ 3	switch(config-if)# switchport mode private-vlan promiscuous	選択したポートを PVLAN の無差別ポートとして設定します。物理イーサネットポートのみを、無差別ポートとしてイネーブルにできます。
ステップ 4	switch(config-if)# switchport private-vlan mapping {primary-vlan-id} {secondary-vlan-list add secondary-vlan-list remove secondary-vlan-list}	ポートを無差別ポートとして設定し、プライマリ VLAN と、セカンダリ VLAN の選択リストに、指定したポートをアソシエートします。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。
ステップ 5	switch(config-if)# no switchport private-vlan mapping	(任意) PVLAN から、マッピングをクリアします。

次の例は、無差別ポートとしてイーサネット インターフェイス 1/4 を設定し、プライマリ VLAN 5 およびセカンダリ独立 VLAN 200 にそのポートを関連付ける方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# switchport private-vlan mapping 5 200
```

無差別トランク ポートの設定

PVLAN ドメインでは、無差別トランク ポートはプライマリ VLAN の一部です。無差別トランク ポートは、複数のプライマリ VLAN を伝送できます。指定されたプライマリ VLAN の複数のセカンダリ VLAN を無差別トランク ポートにマッピングできます。

無差別ポートの設定には、2つの手順が必要です。最初にポートを無差別ポートに定義した後で、セカンダリ VLAN とプライマリ VLAN 間のマッピングを設定します。複数のプライマリ VLAN は複数のマッピングを設定することでイネーブルにできます。



(注) 各 PVLAN トランク ポートに対するマッピングの数は最大 16 です。

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順の概要

1. `switch# configure terminal`
2. `switch(config)# interface type slot/port`
3. `switch(config-if)# switchport mode private-vlan trunk promiscuous`
4. `switch(config-if)# switchport private-vlan mapping trunk {primary-vlan-id} {secondary-vlan-id}`
5. (任意) `switch(config-if)# no switchport private-vlan mapping trunk [primary-vlan-id]`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</code>	コンフィギュレーション モードを開始します。
ステップ 2	<code>switch(config)# interface type slot/port</code>	PVLAN の無差別トランク ポートとして設定するポートを選択します。
ステップ 3	<code>switch(config-if)# switchport mode private-vlan trunk promiscuous</code>	選択したポートを PVLAN の無差別トランク ポートとして設定します。物理イーサネット ポートのみを、無差別ポートとしてイネーブルにできます。このポートとして、FEX のポートを選択することはできません。
ステップ 4	<code>switch(config-if)# switchport private-vlan mapping trunk {primary-vlan-id} {secondary-vlan-id}</code>	PVLAN のプライマリ VLAN およびセカンダリ VLAN に、選択したトランク ポートに関連付けます。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。

	コマンドまたはアクション	目的
ステップ 5	<code>switch(config-if)# no switchport private-vlan mapping trunk [primary-vlan-id]</code>	(任意) ポートから PVLAN のマッピングを削除します。 <i>primary-vlan-id</i> が指定されない場合は、PVLAN のすべてのマッピングがポートから削除されます。

次の例は、イーサネット インターフェイス 1/1 を、PVLAN の無差別トランク ポートとして設定し、セカンダリ VLAN をプライマリ VLAN にマップする方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport mode private-vlan trunk promiscuous
switch(config-if)# switchport private-vlan mapping trunk 5 100
switch(config-if)# switchport private-vlan mapping trunk 5 200
switch(config-if)# switchport private-vlan mapping trunk 6 300
```

独立トランク ポートの設定

PVLAN ドメインでは、独立トランクはセカンダリ VLAN の一部です。独立トランク ポートは、複数の独立 VLAN を送受信できます。指定されたプライマリ VLAN の 1 つの独立 VLAN のみを、独立トランク ポートに関連付けることができます。独立トランク ポートの設定には、2 つの手順が必要です。最初に、独立トランク ポートとしてポートを定義した後で、独立 VLAN とプライマリ VLAN との関連付けを設定します。複数の独立 VLAN は複数の関連付けを設定することでイネーブルにできます。

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順の概要

1. `switch# configure terminal`
2. `switch(config)# interface type [chassis/]slot/port`
3. `switch(config-if)# switchport mode private-vlan trunk [secondary]`
4. `switch(config-if)# switchport private-vlan association trunk {primary-vlan-id} {secondary-vlan-id}`
5. (任意) `switch(config-if)# no switchport private-vlan association trunk [primary-vlan-id]`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</code>	コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	<code>switch(config)# interface type [chassis/]slot/port</code>	PVLAN の独立トランク ポートとして設定するポートを選択します。このポートとしては、FEX のポートを選択できます (<i>chassis</i> オプションで指定)。
ステップ 3	<code>switch(config-if)# switchport mode private-vlan trunk [secondary]</code>	選択したポートを PVLAN のセカンダリ トランク ポートとして設定します。 (注) secondary キーワードがない場合は、それが仮定されます。
ステップ 4	<code>switch(config-if)# switchport private-vlan association trunk {primary-vlan-id} {secondary-vlan-id}</code>	PVLAN のプライマリ VLAN およびセカンダリ VLAN に、独立トランク ポートを関連付けます。セカンダリ VLAN は独立 VLAN である必要があります。指定されたプライマリ VLAN では、1 つの独立 VLAN だけがマッピングできます。
ステップ 5	<code>switch(config-if)# no switchport private-vlan association trunk [primary-vlan-id]</code>	(任意) PVLAN の関連付けをポートから削除します。 <i>primary-vlan-id</i> が指定されない場合は、PVLAN のすべての関連付けがポートから削除されます。

次の例は、イーサネット インターフェイス 1/1 を、PVLAN の無差別トランク ポートとして設定し、セカンダリ VLAN をプライマリ VLAN にマップする方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport mode private-vlan trunk secondary
switch(config-if)# switchport private-vlan association 5 100
switch(config-if)# switchport private-vlan association 6 200
```

FEX トランク ポートでのプライベート VLAN の設定

FEX トランク ポートでは PVLAN をイネーブルにしたりディセーブルにしたりすることができます。FEX トランク ポートにより、PVLAN ドメインは、そこに接続されているすべてのホストに拡張されます。FEX トランク ポートを設定すると、Cisco NX-OS 5000 シリーズ スイッチに接続されているすべての FEX ポートがグローバルにその影響を受けます。



- (注) FEX インターフェイスでは、無差別ポートを含む設定はサポートされていません。また、FEX インターフェイスでは、無差別ポートを持つデバイスへの接続もサポートされていません。無差別機能が必要な場合は、Nexus 1000V などのデバイスを Cisco NX-OS 5000 シリーズ スイッチのベース ポートに接続する必要があります。



注意

FEX トランク ポートで PVLAN を設定する場合は、その前に FEX 独立トランク ポートをすべてディセーブルにしておく必要があります。FEX 独立トランク ポートと FEX トランク ポートをともにイネーブルにすると、不要なネットワーク トラフィックが発生することがあります。

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **system private-vlan fex trunk**
3. (任意) switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# system private-vlan fex trunk	FEX トランク ポートで PVLAN をイネーブルにします。
ステップ 3	switch(config)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次の例は、FEX トランク ポートで PVLAN を設定する方法を示したものです。

```
switch# configure terminal
switch(config)# system private-vlan fex trunk
switch(config)# copy running-config startup-config
```

PVLAN トランキング ポートの許可 VLAN の設定

独立トランク ポートおよび無差別トランク ポートでは、PVLAN とともに通常の VLAN のトラフィックを伝送することができます。

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type [chassis/]slot/port**
3. switch(config-if)# **switchport private-vlan trunk allowed vlan {vlan-list | all | none [add | except | none | remove {vlan-list}]}**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# interface type [chassis/]slot/port	PVLAN のホストポートとして設定するポートを選択します。このポートとしては、FEX のポートを選択できます (chassis オプションで指定)。
ステップ 3	switch(config-if)# switchport private-vlan trunk allowed vlan {vlan-list all none [add except none remove {vlan-list}]}	<p>プライベート トランク インターフェイスの許可 VLAN を設定します。デフォルトの場合、PVLAN トランク インターフェイスで許可されるのは、マップされた VLAN または関連付けられた VLAN のみです。</p> <p>(注) プライマリ VLAN は、許容 VLAN リストに明示的に追加する必要はありません。プライマリ VLAN とセカンダリ VLAN との間で1回マッピングされると、自動的に追加されます。</p>

次の例は、イーサネット PVLAN トランク ポートの許可 VLAN のリストにいくつかの VLAN を追加する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport private-vlan trunk allowed vlan 15-20
```

プライベート VLAN のネイティブ 802.1Q VLAN の設定

通常は、ネイティブ VLAN ID で 802.1Q トランクを設定します。これによって、その VLAN 上のすべてのパケットからタグングが取り除かれます。この設定は、タグなしトラフィックと制御トラフィックが Cisco Nexus 5000 シリーズ スイッチを通過するようにします。セカンダリ VLAN は、無差別 トランク ポートではネイティブ VLAN ID で設定できません。プライマリ VLAN は、独立 トランク ポートではネイティブ VLAN ID で設定できません。



(注) トランクは、複数の VLAN のトラフィックを伝送できます。ネイティブ VLAN に属するトラフィックはトランクを通過するようにカプセル化されません。他の VLAN のトラフィックは、それが属している VLAN を識別するためのタグでカプセル化されます。

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type [chassis/]slot/port**
3. switch(config-if)# **switchport private-vlan trunk native {vlan vlan-id}**
4. (任意) switch(config-if)# **no switchport private-vlan trunk native {vlan vlan-id}**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# interface type [chassis/]slot/port	PVLAN のホストポートとして設定するポートを選択します。このポートとしては、FEX のポートを選択できます (chassis オプションで指定)。
ステップ 3	switch(config-if)# switchport private-vlan trunk native {vlan vlan-id}	PVLAN トランクのネイティブ VLAN ID を設定します。デフォルトは VLAN 1 です。
ステップ 4	switch(config-if)# no switchport private-vlan trunk native {vlan vlan-id}	(任意) PVLAN トランクからネイティブ VLAN ID を削除します。

プライベート VLAN 設定の確認

PVLAN の設定情報を表示する場合は、次のコマンドを使用します。

コマンド	目的
switch# show feature	スイッチでイネーブルになっている機能を表示します。

コマンド	目的
switch# show interface switchport	スイッチポートとして設定されているすべてのインターフェイスに関する情報を表示します。
switch# show vlan private-vlan [type]	PVLAN のステータスを表示します。

次の例は、PVLAN 設定の表示方法を示したものです。

```
switch# show vlan private-vlan
Primary Secondary Type Ports
-----
5 100 community
5 101 community Eth1/12, Eth100/1/1
5 102 community
5 110 community
5 200 isolated Eth1/2
switch# show vlan private-vlan type
Vlan Type
-----
5 primary
100 community
101 community
102 community
110 community
200 isolated
```

次に、イネーブルの機能を表示する例を示します（出力の一部を割愛してあります）。

```
switch# show feature
Feature Name Instance State
-----
fcsp 1 enabled
...
interface-vlan 1 enabled
private-vlan 1 enabled
udld 1 disabled
...
```