プライベート VLAN の設定

この章は、次の内容で構成されています。

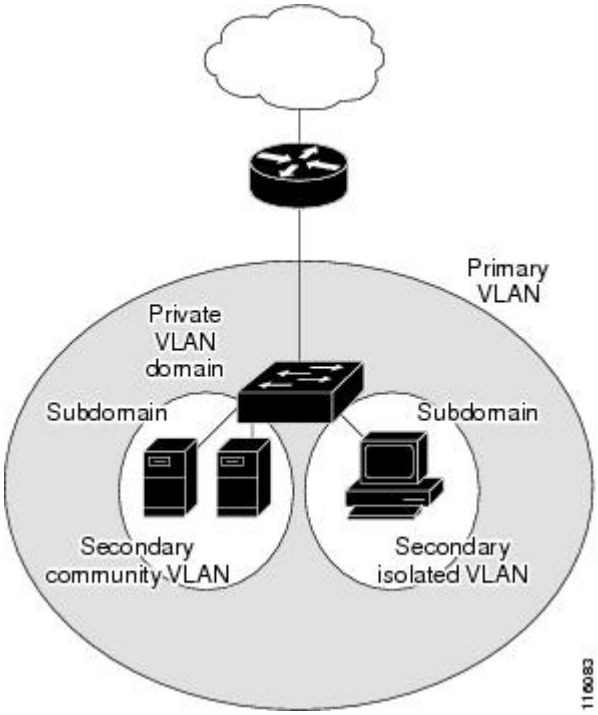
- プライベート VLAN について，1 ページ
- プライベート VLAN に関する注意事項および制約事項，6 ページ
- プライベート VLAN の設定，6 ページ
- プライベート VLAN 設定の確認，12 ページ

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ので、スイッチで相互にポートを分離できます。 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 で構成されます（次の図を参照）。 PVLAN にあるすべての VLAN は、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） まず VLAN を作成してから、プライマリまたはセカンダリの PVLAN に変換する必要があります。

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 ポートと独立ホスト 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。 各無差別ポートは、そのポートに関連付けられた複数のセカンダリ VLAN を持つことができます。または、セカンダリ VLAN を持たないこともできます。 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、関連付けられた無差別ポートと通信できることを除き、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。 VLANは、無差別ポートからのトラフィックを除き、独立ポート宛て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他のすべてのインターフェイスからも、PVLAN ドメイン内のすべての独立ポートからも独立しています。

  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。

プライマリ、独立、およびコミュニティ プライベート VLAN

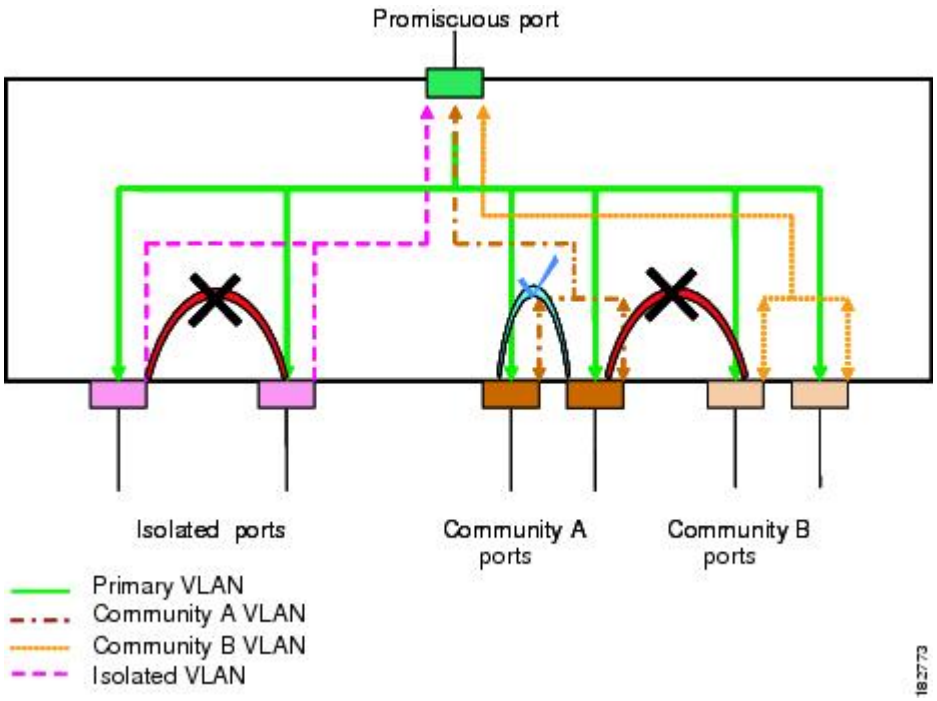
プライマリ VLAN および 2 つのタイプのセカンダリ VLAN（独立 VLAN とコミュニティ VLAN）には、次の特徴があります。

- 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。 PVLAN ドメインには、1 つの独立 VLAN だけ設定できます。 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。 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。

次の図に、PVLAN 内のトラフィック フローと、VLAN のタイプ、ポートのタイプを示します。

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 で受信するトラフィックによって隔離は行われず、転送は通常 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や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 VLAN の外部と通信するには、セカンダリ VLAN をプライマリ VLAN に関連付けます。 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） 関連付けが動作していることを確認するには、**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には、**no private-vlan** コマンドを使用します。 その VLAN におけるすべてのプライマリとセカンダリの関連付けは一時停止しますが、インターフェイスは PVLAN モードのままです。 VLAN を PVLAN モードに戻すときには、元の関連付けが戻されます。

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 に関連付けされたすべての PVLAN が削除されます。 ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力した場合、その VLAN と PVLAN の関連付けは一時停止します。この指定 VLAN を再作成して以前のセカンダリ VLAN として設定すると復元されます。

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 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。
- スイッチが PVLAN 機能を適用するには、PVLAN をイネーブルにする必要があります。
- PVLAN モードで動作しているポートがスイッチに含まれる場合、PVLAN をディセーブルにできません。
- 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。

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 機能を使用するには、スイッチの 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

	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） PVLAN モードにあるスイッチに動作しているポートがある場合、PVLAN をディセーブルにできません。

次に、スイッチの PVLAN 機能をイネーブルにする例を示します。

```
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、PVLAN になるようにその VLAN 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

	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、1 つのプライマリ VLAN を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。

	コマンドまたはアクション	目的
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。

次に、VLAN 5 をプライマリ VLAN として PVLAN に割り当てる例を示します。

```
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ています。

```
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ています。

```
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 におけるすべてのプライマリとセカンダリの関連付けは一時停止しますが、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、元の関連付けが戻されます。

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 に関連付けされたすべてのPVLANは失われます。 ただし、セカンダリ VLANに対して**no vlan**コマンドを入力した場合、その VLAN との PVLAN の関連付けは一時停止します。この指定した VLAN を再作成して以前のセカンダリ VLAN として設定すると元に戻ります。

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

	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**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}	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、*secondary-vlan-list* 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 ポートがセカンダリ VLAN の一部です。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 ホスト 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 PVLAN ホスト ポートとして定義した後で、プライマリ VLAN とセカンダリ VLAN 間のホスト関連付けを設定します。

（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

	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 ホスト ポートとして設定するポートを選択します。 このポートは、FEX（chassis オプションで識別される）上に存在できます。
ステップ 3	switch(config-if)# **switchport mode private-vlan host**	PVLAN のホスト ポートとしてポートを設定します。
ステップ 4	switch(config-if)# **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*}	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） ポートから PVLAN の関連付けを削除します。

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ています。

```
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

	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 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。 このポートは、FEX 上には設定できません。
ステップ 3	switch(config-if)# **switchport mode private-vlan promiscuous**	PVLAN の無差別ポートとしてポートを設定します。 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 の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
```

プライベート VLAN 設定の確認

PVLAN の設定情報を表示するには、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。
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。

次に、PVLAN コンフィギュレーションを表示する例を示します。

```
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
...
```