CHAPTER 39

プライベート VLAN（PVLAN）の設定

この章では、Catalyst 4500 シリーズ スイッチ上の Private VLAN（PVLAN; プライベート VLAN）について説明します。また、注意事項、手順、設定例についても示します。

この章の主な内容は、次のとおりです。

（注） この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

コマンド リスト

この表には、主に PVLAN で共通に使用されるコマンドを示します。

コマンド	目的	参照先
private-vlan {**community** | **isolated** | **primary**}	VLAN を PVLAN として設定します。	「PVLAN としての VLAN の設定」（P.39-14）
private-vlan association {*secondary_vlan_list* | **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。 リストには、独立 VLAN ID を 1 つだけ含めることができ、リストに複数のコミュニティ VLAN ID を含めることもできます。	「セカンダリ VLAN のプライマリ VLAN との関連付け」（P.39-15）
show vlan private-vlan [**type**]	設定を確認します。	「PVLAN としての VLAN の設定」（P.39-14） 「セカンダリ VLAN のプライマリ VLAN との関連付け」（P.39-15）
show interface private-vlan mapping	設定を確認します。	「セカンダリ VLAN 入力トラフィックのルーティングの許可」（P.39-21）

コマンド	目的	参照先
switchport mode private-vlan {**host** | **promiscuous** | **trunk promiscuous** | **trunk [secondary]**}	レイヤ 2 インターフェイスを PVLAN ポートとして設定します。	「PVLAN の設定」（P.39-10）
switchport private-vlan mapping [**trunk**] *primary_vlan_ID* {*secondary_vlan_list* | **add** *secondary_vlan_list* | **remove** *secondary_vlan_list*}	PVLAN 混合モード ポートをプライマリ VLAN および選択したセカンダリ VLAN にマッピングします。	「レイヤ 2 インターフェイスの PVLAN 混合モード ポートとしての設定」（P.39-16） 「レイヤ 2 インターフェイスの混合モード PVLAN トランク ポートとしての設定」（P.39-19）
Switch(config-if)# **switchport private-vlan host-association** *primary_vlan_ID secondary_vlan_ID*	レイヤ 2 インターフェイスを PVLAN に関連付けます。 **（注）** 独立ポートに関連付けることができるのは、1 つのプライマリ/セカンダリ VLAN ペアだけです。	「レイヤ 2 インターフェイスの PVLAN ホスト ポートとしての設定」（P.39-17）
switchport private-vlan association trunk *primary_vlan_ID secondary_vlan_ID*	プライマリ VLAN とセカンダリ VLAN のアソシエーションを設定し、PVLAN トランク ポートを PVLAN に関連付けます。 **（注）** 独立トランク ポートは、複数のプライマリ/セカンダリ ペアを使用して設定できます。	「レイヤ 2 インターフェイスの独立 PVLAN トランク ポートとしての設定」（P.39-18）
switchport private-vlan trunk allowed vlan *vlan_list* **all** | **none** | [**add** | **remove** | **except**] *vlan_atom*[,*vlan_atom*...]	PVLAN トランク ポートで許容される通常の VLAN のリストを設定します。	「レイヤ 2 インターフェイスの独立 PVLAN トランク ポートとしての設定」（P.39-18）
switchport private-vlan trunk native vlan *vlan_id*	PVLAN トランク ポートに（IEEE 802.1Q タグとしての）タグなしパケットが割り当てられる VLAN を設定します。	「レイヤ 2 インターフェイスの独立 PVLAN トランク ポートとしての設定」（P.39-18）

PVLAN

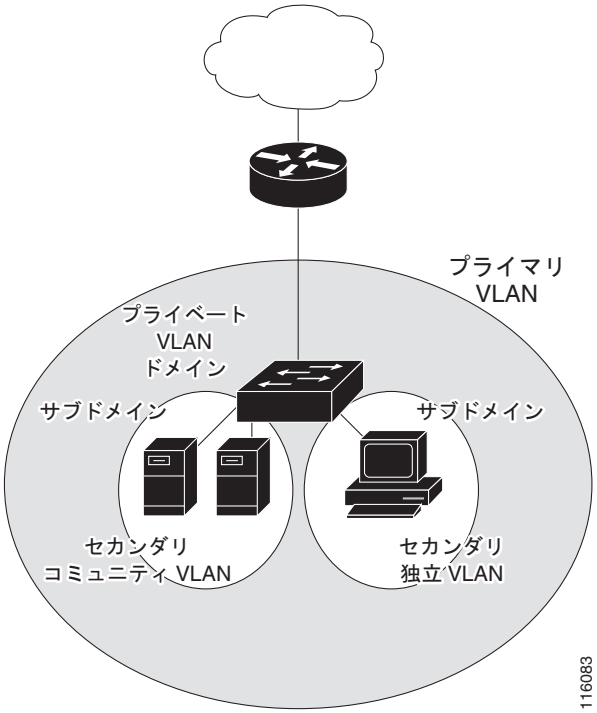
PVLAN 機能を使用すると、サービス プロバイダーが VLAN を使用したときに直面する 2 つの問題に対処できます。

- スイッチがサポートするアクティブ VLAN は最大で 1005 です。サービス プロバイダーが顧客ごとに VLAN を 1 つ割り当てる場合、サポートできる顧客数に限界が生じます。
- IP ルーティングをイネーブルにするために、各 VLAN にサブネット アドレス スペースを割り当てるかアドレス ブロックを割り当てます。このために未使用の IP アドレスが増え、IP アドレスの管理に問題が発生します。

PVLAN の使用により、サービス プロバイダーにはスケーラビリティと IP アドレス管理上の利点がもたらされ、顧客にはレイヤ 2 セキュリティが提供されます。PVLAN では、通常の VLAN ドメインをサブドメインに分割します。サブドメインは、*プライマリ* VLAN と *セカンダリ* VLAN という VLAN のペアで表されます。PVLAN には複数の VLAN のペアがあり、各サブドメインに 1 組のペアが対応

します。PVLAN のすべての VLAN ペアは、同じプライマリ VLAN を共有します。セカンダリ VLAN ID によって各サブドメインは識別されます。図 39-1 を参照してください。

図 39-1　PVLAN のドメイン



セカンダリ VLAN には次の 2 種類があります。

- 独立 VLAN：独立 VLAN のポートは、レイヤ 2 レベルでは相互に通信できません。
- コミュニティ VLAN：コミュニティ VLAN のポートは相互に通信できますが、レイヤ 2 レベルでは他のコミュニティのポートとは通信できません。

混合モード ポートは、1 つの PVLAN、1 つの独立 VLAN、および複数のコミュニティ VLAN だけで使用できます。レイヤ 3 ゲートウェイは、通常、混合モード ポート経由でスイッチに接続されます。

スイッチング環境では、個々のエンド ステーションまたは一連のエンド 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。エンド ステーションが PVLAN の外とやり取りする際に通信する必要があるのは、デフォルト ゲートウェイのみです。

PVLAN を使用して端末へのアクセスをコントロールするには、次の方法があります。

- 端末に接続する選択したインターフェイスを独立ポートとして設定し、レイヤ 2 での通信ができないようにします。たとえば、端末がサーバであれば、サーバ間のレイヤ 2 通信ができなくなります。
- デフォルト ゲートウェイおよび選択した端末（バックアップ サーバなど）に接続するインターフェイスを混合モード ポートとして設定して、すべての端末をデフォルト ゲートウェイにアクセスさせることができます。
- VLAN および IP サブネット内のトラフィック量を減らせば、端末が同じ VLAN および IP サブネット内にある場合でも端末間のトラフィックを防止できます。

  混合モード 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、混合モード ポートを LocalDirector のサーバ ポートに接続して、サーバに独立 VLAN または多数のコミュニティ VLAN を接続できます。LocalDirector は、独立また

はコミュニティ VLAN 内にあるサーバのロード バランシングを行います。混合モード ポートを使用して、管理ワークステーションからすべての PVLAN サーバのモニタまたはバックアップを行うことも可能です。

ここでは、次の内容について説明します。

定義一覧

用語	定義
PVLAN	プライマリ ID を共有し、ポート間をレイヤ 2 で分離しながら 1 つのレイヤ 3 ルータ ポートおよび IP サブネットを共有するメカニズムを提供する VLAN ペアのセット。
セカンダリ VLAN	PVLAN を実装するために使用する VLAN の種類。プライマリ VLAN に関連付けられており、ホストから他の許容ホストおよびルータにトラフィックを送信します。
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。同一コミュニティ VLAN 内の他のポートや混合モード ポートと通信します。これらのインターフェイスは、他のコミュニティのすべてのインターフェイスから、および自身の PVLAN 内の独立ポートから、レイヤ 2 で隔離されています。
コミュニティ VLAN	アップストリーム トラフィックをコミュニティ ポートから混合モード ポート ゲートウェイおよび同一コミュニティ内の他のホスト ポートに送信するセカンダリ VLAN。PVLAN には複数のコミュニティ VLAN を設定できます。
独立ポート	独立セカンダリ VLAN に属するホスト ポート。同一の PVLAN 内の他のポートからは、混合モード ポートを除き、レイヤ 2 で完全に分離されています。PVLAN は、混合モード ポートからのトラフィックを除く、独立ポートへのすべてのトラフィックをブロックします。独立ポートから受信したトラフィックは、混合モード ポートにのみ転送されます。
独立 VLAN	PVLAN には独立 VLAN が 1 つだけあります。独立 VLAN とは、ホストから混合モード ポートおよびゲートウェイに単方向トラフィック アップストリームを送信するセカンダリ VLAN です。
プライマリ VLAN	PVLAN にはプライマリ VLAN が 1 つだけあります。PVLAN のどのポートもプライマリ VLAN のメンバです。プライマリ VLAN は、混合モード ポートから（独立およびコミュニティ）ホスト ポートおよび他の混合モード ポートに単方向トラフィック ダウンストリームを送信します。

用語	定義
PVLAN トランク ポート	PVLAN トランク ポートは、複数のセカンダリ（独立のみ）PVLAN および非 PVLAN を伝送します。パケットは、PVLAN トランク ポートでセカンダリ VLAN タグまたは通常の VLAN タグとともに送受信されます。 （注）　IEEE 802.1Q カプセル化方式のみサポートされています。
混合モード ポート	混合モード ポートはプライマリ VLAN に属し、すべてのインターフェイスと通信できます。これらのインターフェイスには、コミュニティおよび独立ホスト ポートと、プライマリ VLAN に関連付けられたセカンダリ VLAN に属する PVLAN トランク ポートが含まれます。
混合モード トランク ポート	混合モード トランク ポートは、複数のプライマリ VLAN および通常の VLAN を伝送します。プライマリ VLAN タグまたは通常の VLAN タグを持つパケットが送受信されます。これ以外は、ポートは混合モード アクセス ポートと同じように動作します。 （注）　IEEE 802.1Q カプセル化方式のみサポートされています。

複数のスイッチの PVLAN

ここでは、次の内容について説明します。

標準トランク ポート

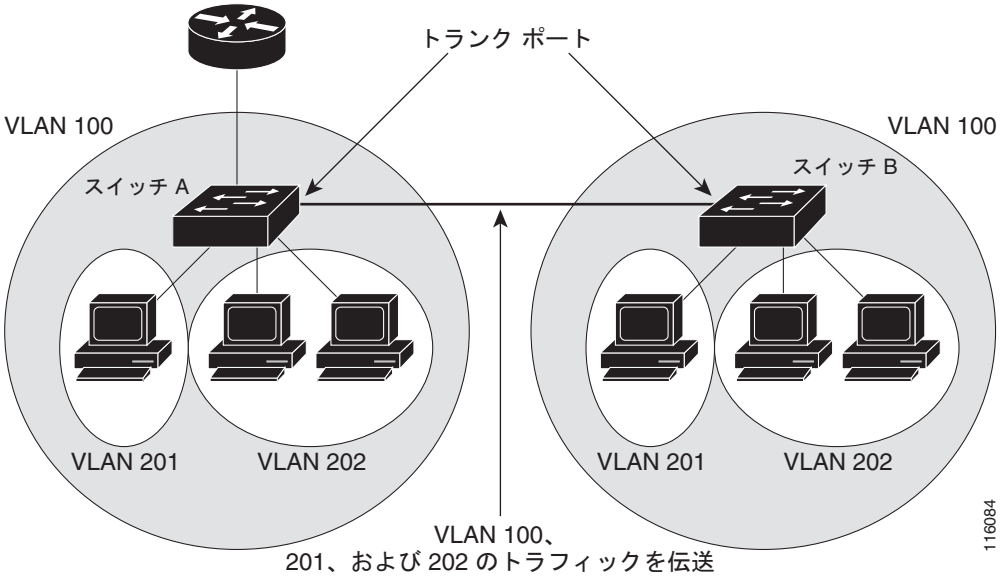
通常の VLAN と同じく、PVLAN も複数のスイッチにまたがって使用できます。1 つのトランク ポートが、プライマリ VLAN およびセカンダリ VLAN を近接スイッチに伝送します。トランク ポートは、PVLAN をその他の VLAN として扱います。複数のスイッチにまたがる PVLAN では、スイッチ A の独立ポートからのトラフィックはスイッチ B の独立ポートに到達しません。図 39-2 を参照してください。

PVLAN 構成のセキュリティを保持し、PVLAN として設定された VLAN が他の目的で利用されないようにするために、PVLAN ポートを持たないデバイスを含むすべての中継デバイスに PVLAN を設定します。

（注）　トランク ポートは通常の VLAN のトラフィックを伝送します。また、プライマリ、独立、およびコミュニティ VLAN のトラフィックも伝送します。

（注）　トランキングを実行するスイッチが両方とも PVLAN をサポートする場合は、標準トランク ポートを使用します。

図 39-2　スイッチのプライベート VLAN



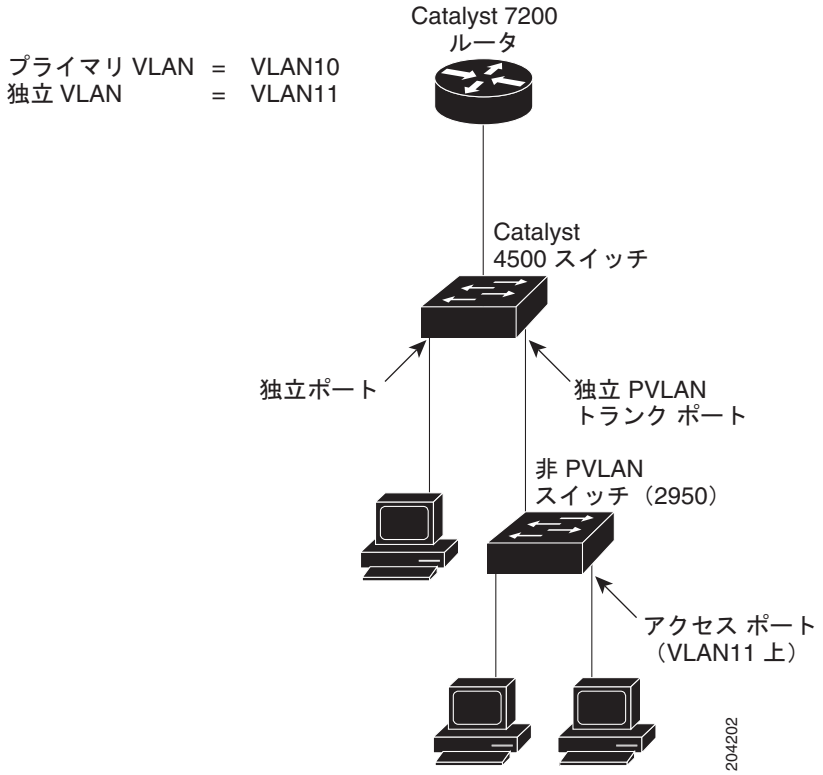
VLAN 100 = プライマリ VLAN
VLAN 201 = セカンダリ独立 VLAN
VLAN 202 = セカンダリ コミュニティ VLAN

VTP（可変端末プロトコル）は PVLAN をサポートしないので、レイヤ 2 ネットワーク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。ネットワークの一部のスイッチにプライマリ/セカンダリ VLAN アソシエーションを設定しなかった場合、これらのスイッチのレイヤ 2 データベースは統合されません。その結果、これらのスイッチで PVLAN トラフィックのフラッディングが発生します。

独立 PVLAN トランク ポート

PVLAN 独立ホスト ポートを使用して、通常の VLAN を複数伝送するか、複数の PVLAN ドメインで VLAN を複数伝送する場合、独立 PVLAN トランク ポートを使用します。これは、PVLAN をサポートしないダウンストリーム スイッチ（Catalyst 2950 など）を接続する場合に役立ちます。

図 39-3　独立 PVLAN トランク ポート



この図では、PVLAN をサポートしないダウンストリーム スイッチの接続に Catalyst 4500 スイッチが使用されています。

ルータから host1 へのダウンストリーム方向に送信されるトラフィックは、混合モード ポート上のプライマリ VLAN （VLAN 10）内の Catalyst 4500 シリーズ スイッチによって受信されます。そして、パケットは独立 PVLAN トランクからスイッチングされますが、プライマリ VLAN（VLAN 10）にタグ付けされずに独立 VLAN （VLAN 11）にタグ付けされて送信されます。このように、パケットが非 PVLAN スイッチに着信すると、宛先ホストのアクセス ポートにブリッジングされます。

アップストリーム方向のトラフィックは、host1 から非 PVLAN スイッチへ送信され、VLAN 11 に着信します。そしてパケットは、トランク ポート経由でこの VLAN （VLAN 11）のタグにタグ付けされる Catalyst 4500 シリーズ スイッチに送信されます。Catalyst 4500 シリーズ スイッチでは、VLAN 11 が独立 VLAN として設定され、トラフィックは独立ホスト ポートから送信されたかのように転送されます。

（注）　このように独立トランクを使用すると、Catalyst 4500 シリーズ スイッチは独立トランクと直接接続しているホスト（host3 など）とを分離することができますが、非 PVLAN スイッチに接続しているホスト（host1 および host2 など）を分離することはできません。これらのホストの分離は、Catalyst 2950 上の保護ポートなどの機能を使用して、非 PVLAN スイッチによって行う必要があります。

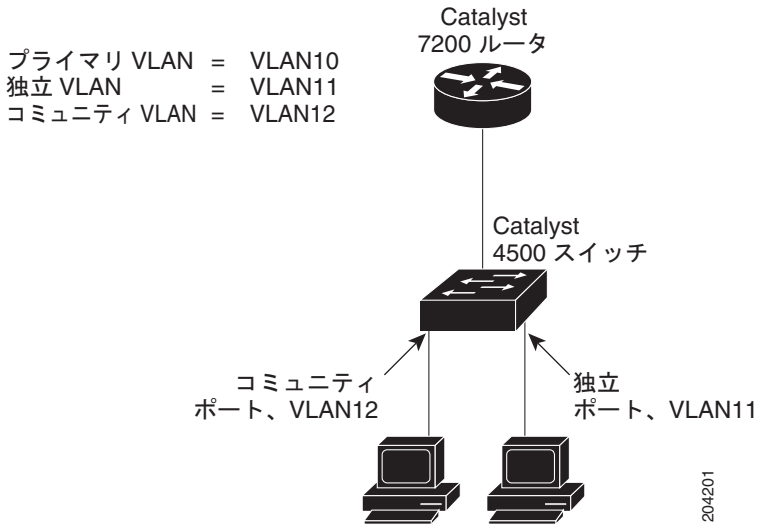
保護ポートの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_22_ea11x/configuration/guide/swtrafc.html#wp1158863

混合モード PVLAN トランク ポート

PVLAN 混合モード トランクが使用されるのは、一般的には PVLAN 混合モード ホスト ポートを使用する場合ですが、通常の VLAN を複数伝送するか、複数の PVLAN ドメインで VLAN を複数伝送する必要がある場合です。これは、Cisco 7200 などの PVLAN をサポートしないアップストリーム ルータを接続する場合に役立ちます。

図 39-4　　混合モード PVLAN トランク ポート



この図では、PVLAN ドメインを PVLAN をサポートしないアップストリーム ルータに接続するために Catalyst 4500 シリーズ スイッチが使用されています。host1 によってアップストリームに送信されるトラフィックは、コミュニティ VLAN（VLAN 12）の Catalyst 4500 シリーズ スイッチに着信します。このトラフィックは、このルータ宛てに混合モード PVLAN トランクにブリッジングされる場合にプライマリ VLAN（VLAN 10）にタグ付けされ、ルータで設定された正しいサブインターフェイス経由でルーティングされます。

ダウンストリーム方向のトラフィックは、混合モード ホスト ポートによって受信されるように、プライマリ VLAN（VLAN 10）の Catalyst 4500 スイッチによって混合モード PVLAN トランク ポートで受信されます。そして、PVLAN ドメイン内にあるかのように、宛先ホストにブリッジングされます。

PVLAN 混合モード トランクは、VLAN QoS と相互に作用します。「PVLAN と VLAN ACL/QoS」（P.39-9）を参照してください。

PVLAN と他の機能との相互作用

PVLAN には他の機能との相互作用があります。詳しくは次のセクションで説明します。

- 「PVLAN と VLAN ACL/QoS」（P.39-9）
- 「PVLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック」（P.39-9）
- 「PVLAN と SVI」（P.39-10）
- 「PVLAN 上での Virtial Port（VP; 仮想ポート）ごとの errdisable」（P.39-10）

詳細については、「PVLAN 設定時の注意事項および制約事項」（P.11）を参照してください。

PVLAN と VLAN ACL/QoS

PVLAN ポートは、次のようにプライマリおよびセカンダリ VLAN を使用します。

- PVLAN ホスト ポートで受信されたパケットは、セカンダリ VLAN に属します。
- セカンダリ VLAN によりパケットにタグが設定されている場合、またはパケットのタグが解除され、ポートのネイティブ VLAN がセカンダリ VLAN の場合、PVLAN トランク ポートで受信されたパケットはセカンダリ VLAN に属します。

PVLAN ホストまたはトランク ポートで受信され、セカンダリ VLAN に割り当てられているパケットは、セカンダリ VLAN 上でブリッジングされます。このブリッジングにより、セカンダリ VLAN ACL（アクセス コントロール リスト）と（入力方向の）セカンダリ VLAN QoS（Quality Of Service）が適用されます。

パケットが PVLAN ホストまたはトランク ポートから送信される場合、パケットは論理的にはプライマリ VLAN に属します。この関係は、セカンダリ VLAN によるタグ付けが PVLAN 用であった場合にも適用されます。この状況では、出力時のプライマリ VLAN ACL およびプライマリ VLAN QoS がパケットに適用されます。

- 同様に、PVLAN 混合モード アクセス ポートで受信されるパケットもプライマリ VLAN に属します。
- 着信 VLAN によっては、PVLAN 混合モード トランク ポートで受信されるパケットがプライマリ VLAN または通常の VLAN に属することもあります。

混合モード トランク ポートに着信する、通常の VLAN へのトラフィックの場合、通常の VLAN ACL および QoS ポリシーが適用されます。PVLAN ドメインへのトラフィックの場合、混合モード ポートで受信するパケットはプライマリ VLAN にブリッジングされます。このため、入力ではプライマリ VLAN ACL および QoS ポリシーが適用されます。

パケットが混合モード トランク ポートから送信される場合、セカンダリ ポートから受信されたパケットであればセカンダリ VLAN に論理的に属し、別の混合モード ポートからブリッジングされたパケットであればプライマリ VLAN に属します。パケットは区別できないので、混合モード トランク ポートから出力するパケットについては、VLAN QoS ポリシーはすべて無視されます。

PVLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック

通常の VLAN では、同じ VLAN のデバイスはレイヤ 2 レベルで相互に通信できますが、別の VLAN のインターフェイスに接続されているデバイスはレイヤ 3 レベルで通信します。PVLAN の場合、混合モード ポートはプライマリ VLAN のメンバですが、ホスト ポートはセカンダリ VLAN に属します。セカンダリ VLAN はプライマリ VLAN に関連付けられているので、これらの VLAN のメンバはレイヤ 2 レベルで相互に通信できます。

通常の VLAN では、ブロードキャストはその VLAN のすべてのポートに転送されます。PVLAN ブロードキャストの場合の転送先は、ブロードキャストを送信するポートによって異なります。

- 独立ポートは、混合モード ポートまたはトランク ポートにのみブロードキャストを送信します。
- コミュニティ ポートは、すべての混合モード ポート、トランク ポート、および同じコミュニティ VLAN のポートにブロードキャストを送信します。
- 混合モード ポートは、PVLAN のすべてのポートにブロードキャストを送信します（他の混合モード ポート、トランク ポート、独立ポート、およびコミュニティ ポート）。

マルチキャスト トラフィックは、PVLAN の境界を超えて、1 つのコミュニティ VLAN 内で、ルーティングまたはブリッジングされます。マルチキャスト トラフィックは、同じ独立 VLAN のポート間または異なるセカンダリ VLAN のポート間では転送されません。

PVLAN と SVI

レイヤ 3 スイッチでは、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）が VLAN のレイヤ 3 インターフェイスとなります。レイヤ 3 デバイスと PVLAN の通信は、セカンダリ VLAN ではなく、プライマリ VLAN を介してのみ行われます。レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。セカンダリ VLAN には、レイヤ 3 VLAN インターフェイスを設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI は非アクティブになります。

- アクティブ SVI をセカンダリ VLAN として VLAN に設定しようとしても、SVI をディセーブルにしなければ設定できません。
- VLAN がセカンダリ VLAN として設定されており、そのセカンダリ VLAN がレイヤ 3 でマップされている場合は、この VLAN に SVI を作成しようとしても SVI は作成されず、エラー メッセージが表示されます。SVI がレイヤ 3 でマップされていなければ SVI は作成されますが、自動的にシャット ダウンされます。

プライマリ VLAN がセカンダリ VLAN に関連付けられ、マップされている場合、プライマリ VLAN の設定はセカンダリ VLAN SVI に伝播されます。たとえば、IP サブネットをプライマリ VLAN SVI に割り当てると、このサブネットは PVLAN 全体の IP サブネット アドレスになります。

PVLAN 上での Virtial Port（VP; 仮想ポート）ごとの errdisable

PVLAN では、VP ごとの errdisable 動作が次のように定義されます。

- PVLAN 混合モード ポート上または PVLAN 混同モード トランク ポート上では、プライマリ VLAN 上で違反が発生した場合に errdisable になります。
- PVLAN ホスト上または PVLAN トランク ポート上では、セカンダリ VLAN 上で違反が発生した場合に、関連付けられたプライマリ VLAN が errdisable になります。
- プライマリ VLAN およびセカンダリ VLAN の両方を伝送する標準トランク ポート上では、プライマリ VLAN 上で違反が発生した場合に、その VLAN と VLAN に関連付けられたすべてのセカンダリ VLAN が errdisable になります。セカンダリ VLAN 上で違反が発生した場合は、関連付けられたプライマリ VLAN と プライマリ VLAN に関連付けられたすべてのセカンダリ VLAN が errdisable になります。

PVLAN の設定

ここでは、PVLAN の設定手順について説明します。

PVLAN の設定手順

PVLAN を設定する手順は、次のとおりです。

ステップ 1　VTP を透過モードに設定します。「VLAN トランキング プロトコル」（P.14-8）を参照してください。

ステップ 2　セカンダリ VLAN を作成します。「PVLAN としての VLAN の設定」（P.39-14）を参照してください。

ステップ 3　プライマリ VLAN を作成します。「PVLAN としての VLAN の設定」（P.39-14）を参照してください。

ステップ 4　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 のプライマリ VLAN との関連付け」（P.39-15）を参照してください。

（注）　プライマリ VLAN にマッピングできる独立 VLAN は 1 つだけですが、コミュニティ VLAN は複数をマッピングできます。

ステップ 5　インターフェイスを、独立ホスト、コミュニティ ホスト、またはトランク ポートとして設定します。「レイヤ 2 インターフェイスの PVLAN ホスト ポートとしての設定」（P.39-17）および「レイヤ 2 インターフェイスの独立 PVLAN トランク ポートとしての設定」（P.39-18）を参照してください。

ステップ 6　独立ポートまたはコミュニティ ポートをプライマリ/セカンダリ VLAN ペアに関連付けます。「セカンダリ VLAN のプライマリ VLAN との関連付け」（P.39-15）を参照してください。

ステップ 7　インターフェイスを混合モード ポートとして設定します。「レイヤ 2 インターフェイスの PVLAN 混合モード ポートとしての設定」（P.39-16）を参照してください。

ステップ 8　混合モード ポートをプライマリ/セカンダリ VLAN ペアにマッピングします。「レイヤ 2 インターフェイスの PVLAN 混合モード ポートとしての設定」（P.39-16）を参照してください。

ステップ 9　VLAN 間ルーティングを使用する場合は、プライマリ SVI を設定し、セカンダリ VLAN をマッピングします。「セカンダリ VLAN 入力トラフィックのルーティングの許可」（P.39-21）を参照してください。

ステップ 10　PVLAN の設定を確認します。「Switch#」（P.39-22）を参照してください。

PVLAN のデフォルト設定

PVLAN は設定されていません。

PVLAN 設定時の注意事項および制約事項

PVLAN の設定時には、次の注意事項に従ってください。

- PVLAN を正しく設定するには、VTP バージョン 1 および VTP バージョン 2 のトランスペアレント モードで VTP をイネーブルにします（VTP バージョン 3 を使用すると、サーバ モードで PVLAN を作成できます）。

  VTP モードを PVLAN のクライアントまたはサーバに変更することはできません。
- PVLAN に VLAN 1 または VLAN 1002 ～ 1005 を設定しないでください。
- ポートをプライマリ VLAN、独立 VLAN、またはコミュニティ VLAN に割り当てる場合は、PVLAN コマンドのみを使用します。

プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN 上のレイヤ 2 インターフェイスは、PVLAN では非アクティブになります。レイヤ 2 トランク インターフェイスは、STP（スパニング ツリー プロトコル）フォワーディング ステートのままです。

- セカンダリ VLAN には、レイヤ 3 VLAN インターフェイスを設定できません。

  独立 VLAN およびコミュニティ（セカンダリ）VLAN のレイヤ 3 VLAN インターフェイスは、VLAN が独立 VLAN またはコミュニティ VLAN として設定されている場合、非アクティブです。

- VLAN ポートを、EtherChannel として設定しないでください。ポートが PVLAN の設定に含まれる場合、これに対応する EtherChannel の設定は非アクティブです。
- プライマリ VLAN には、ダイナミック Access Control Entry（ACE; アクセス コントロール エントリ）を適用できません。

  プライマリ VLAN に適用されている Cisco IOS ダイナミック ACL 設定は、VLAN が PVLAN の設定に含まれている場合、非アクティブです。

- 不正な設定によるスパニングツリー ループを防止するために、**spanning-tree portfast trunk** コマンドを使用して PVLAN トランク上で PortFast をイネーブルにします。
- セカンダリ VLAN に設定された VLAN ACL は、すべて入力方向で有効です。また、セカンダリ VLAN に関連付けられたプライマリ VLAN に設定された VLAN ACL はすべて出力方向で有効です。
- 独立 VLAN またはコミュニティ VLAN のレイヤ 3 スイッチングを停止する場合は、その VLAN のプライマリ VLAN へのマッピングを削除します。
- デバイスがトランク接続され、プライマリ VLAN およびセカンダリ VLAN がトランクに関連付けられている限り、異なるネットワーク デバイス上に PVLAN ポートを設定できます。
- 2 つの異なるデバイス上の独立ポートは相互通信できませんが、コミュニティ VLAN ポートの場合は可能です。
- PVLAN は、次の SPAN 機能をサポートしています。
  - PVLAN ポートを SPAN 送信元ポートとして設定できます。
  - プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN 上で VLAN-based SPAN（VSPAN）を使用して、または単一の VLAN 上で SPAN を使用して、入力および出力トラフィックを個別にモニタリングできます。

  SPAN の詳細については、第 50 章「SPAN と RSPAN の設定」を参照してください。
- プライマリ VLAN には複数のコミュニティ VLAN を関連付けできますが、独立 VLAN は 1 つだけです。
- 独立 VLAN またはコミュニティ VLAN には、1 つのプライマリ VLAN のみを関連付けることができます。
- PVLAN の設定で使用された VLAN を削除すると、この VLAN に関連付けられた PVLAN ポートは非アクティブになります。
- VTP は、PVLAN をサポートしていません。PVLAN ポートを使用する場合は、デバイスごとに PVLAN を設定する必要があります。
- 使用する PVLAN の設定のセキュリティを確保して、PVLAN として設定された VLAN が他の目的に使用されないようにするには、PVLAN ポートがないデバイスを含めて、すべての中間デバイスで PVLAN を設定します。
- PVLAN でトラフィックを伝送しないデバイスのトランクから、PVLAN をプルーニングします。
- ポート ACLS 機能が使用できる場合、セカンダリ VLAN ポートに Cisco IOS ACLS を、および PVLAN（VACL）に Cisco IOS ACLS を適用できます。VACL の詳細については、第 47 章「ACL によるネットワーク セキュリティの設定」を参照してください。

- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN には、さまざまな QoS 設定を適用できます（第 37 章「QoS の設定」を参照）。プライマリ VLAN のレイヤ 3 VLAN インターフェイスに適用された Cisco IOS ACL は、関連する独立 VLAN およびコミュニティ VLAN にも自動的に適用されます。
- PVLAN トランク ポートでは、入力トラフィックにセカンダリ VLAN ACL、出力トラフィックにプライマリ VLAN ACL が適用されます。
- 混合モード ポートでは、入力トラフィックにプライマリ VLAN ACL が適用されます。
- PVLAN セカンダリ トランク ポートと混合モード トランク ポートはどちらも IEEE 802.1q カプセル化だけをサポートします。
- PVLAN トランク上では、コミュニティ VLAN を伝播または伝送できません。
- レイヤ 3 PVLAN インターフェイス上で学習された ARP エントリは、「sticky」ARP エントリといいます（PVLAN インターフェイス ARP エントリを表示して確認することを推奨します）。
- セキュリティ上の理由から、PVLAN ポート sticky ARP エントリは期限切れになりません。異なる MAC アドレスでも同じ IP アドレスを持つデバイスを接続すると、エラー メッセージが生成されて ARP エントリは作成されません。
- PVLAN ポート sticky ARP エントリは期限切れしないので、MAC アドレスを変更する場合は手動でエントリを削除する必要があります。sticky ARP エントリを上書きするには、まず **no arp** コマンドでエントリを削除してから、**arp** コマンドでエントリを上書きします。
- DHCP 環境では、PC をシャットダウンしても自分の IP アドレスを他人に譲ることはできません。この問題を解決するために、Catalyst 4500 シリーズ スイッチでは **no ip sticky-arp** コマンドをサポートしています。このコマンドを使用すると、DHCP 環境での IP アドレスの上書きおよび再使用ができます。
- 通常の VLAN は混合モード トランク ポートまたは独立トランク ポートで伝送されます。
- 混合モード トランク ポートのデフォルト ネイティブ VLAN は VLAN 1 で、管理 VLAN です。タグのないパケットはすべてネイティブ VLAN で転送されます。プライマリ VLAN または通常の VLAN をネイティブ VLAN として設定できます。
- 混合モード トランクは、セカンダリ VLAN を伝送するようには設定できません。許容 VLAN リストでセカンダリ VLAN を指定した場合、設定は受け入れられますが、セカンダリ VLAN のポートは動作せず、転送しません。これは、セカンダリ VLAN ではあってもプライマリ VLAN に関連付けられていない VLAN のポートの場合にも当てはまります。
- 混合モード トランク ポートでは、プライマリ VLAN に着信する入力トラフィックにプライマリ VLAN ACL および QoS が適用されます。
- VLAN ACL または QoS は、混合モード トランク ポートの出力トラフィックには適用されません。PVLAN のトラフィックのアップストリームは、論理的にセカンダリ VLAN に向かうからです。ハードウェアの VLAN 変換により、受信したセカンダリ VLAN の情報は失われます。このため、ポリシーは適用されません。この制約は、同じプライマリ VLAN の他のポートからブリッジングされるトラフィックにも当てはまります。
- PVLAN 混合モード トランク ポートでポート セキュリティを設定しないでください。逆の場合も行わないでください。

  混合モード トランク ポートのポートセキュリティをイネーブルにした場合、この機能はサポートされていないので、ポートは予測できない動作をする可能性があります。
- PVLAN 混合モード トランク ポートに IEEE 802.1X を設定しないでください。

（注）　コミュニティ PVLAN トランク ポートはサポートされていません。

PVLAN としての VLAN の設定

VLAN を PVLAN として設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	設定モードを開始します。
ステップ 2	`Switch(config)# vlan vlan_ID`	VLAN コンフィギュレーション モードを開始します。
ステップ 3	`Switch(config-vlan)# private-vlan {community | isolated | primary}`	VLAN を PVLAN として設定します。 • このコマンドは、VLAN コンフィギュレーション サブモードを終了するまで有効になりません。 PVLAN のステータスをクリアするには、**no** キーワードを使用します。
ステップ 4	`Switch(config-vlan)# end`	VLAN コンフィギュレーション モードを終了します。
ステップ 5	`Switch# show vlan private-vlan [type]`	設定を確認します。

次に、VLAN 202 をプライマリ VLAN として設定し、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# end
Switch# show vlan private-vlan
Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
```

次に、VLAN 303 をコミュニティ VLAN として設定し、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 303
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
        303       community
```

次に、VLAN 440 を独立 VLAN として設定し、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 440
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
        303       community
        440       isolated
```

セカンダリ VLAN のプライマリ VLAN との関連付け

セカンダリ VLAN をプライマリ VLAN に関連付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	設定モードを開始します。
ステップ 2	`Switch(config)# vlan primary_vlan_ID`	プライマリ VLAN の VLAN コンフィギュレーション モードを開始します。
ステップ 3	`Switch(config-vlan)# private-vlan association {secondary_vlan_list | 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。リストには、独立 VLAN ID を 1 つだけ含めることができ、リストに複数のコミュニティ VLAN ID を含めることもできます。 すべてのセカンダリ アソシエーションをクリアするには、**no** キーワードを使用します。
ステップ 4	`Switch(config-vlan)# end`	VLAN コンフィギュレーション モードを終了します。
ステップ 5	`Switch# show vlan private-vlan [type]`	設定を確認します。

セカンダリ VLAN をプライマリ VLAN と関連付ける場合、次の点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。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一の PVLAN ID またはハイフンで連結した PVLAN ID の範囲です。
- *secondary_vlan_list* パラメータには、複数のコミュニティ VLAN ID を含めることができます。
- *secondary_vlan_list* パラメータには、独立 VLAN ID を 1 つだけ含めることができます。
- セカンダリ VLAN を PVLAN に関連付けるには、*secondary_vlan_list* を入力するか、または **secondary_vlan_list** と *add* キーワードを使用します。
- セカンダリ VLAN と PVLAN 間のアソシエーションをクリアするには、**secondary_vlan_list** と *remove* キーワードを使用します。
- これらのコマンドは、VLAN コンフィギュレーション サブモードを終了するまで有効になりません。

次に、プライマリ VLAN 202 にコミュニティ VLAN 303 ～ 307 および 309、独立 VLAN 440 を関連付け、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan association 303-307,309,440
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202     303       community
202     304       community
202     305       community
202     306       community
202     307       community
202     309       community
202     440       isolated
        308       community
```

（注）　セカンダリ VLAN 308 は、プライマリ VLAN と関連付けされません。

レイヤ 2 インターフェイスの PVLAN 混合モード ポートとしての設定

レイヤ 2 インターフェイスを PVLAN 混合モード ポートとして設定するには、次の作業を行います。

	コマンド	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)# interface {fastethernet | gigabitethernet | tengigabitethernet} slot/port`	設定する LAN インターフェイスを指定します。
ステップ 3	`Switch(config-if)# switchport mode private-vlan {host | promiscuous | trunk promiscuous | trunk [secondary]}`	レイヤ 2 インターフェイスを PVLAN 混合モード ポートとして設定します。
ステップ 4	`Switch(config-if)# [no] switchport private-vlan mapping [trunk] primary_vlan_ID {secondary_vlan_list | add secondary_vlan_list | remove secondary_vlan_list}`	PVLAN 混合モード ポートをプライマリ VLAN および選択したセカンダリ VLAN にマッピングします。
ステップ 5	`Switch(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 6	`Switch# show interfaces {fastethernet | gigabitethernet | tengigabitethernet} slot/port switchport`	設定を確認します。

（注）　**switchport private-vlan mapping** コマンドでサポートされる一意の PVLAN ペアの最大数は 1000 です。

レイヤ 2 インターフェイスを PVLAN 混合モード ポートとして設定する場合、次の点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。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一の PVLAN ID またはハイフンで連結した PVLAN ID の範囲です。
- セカンダリ VLAN を PVLAN 混合モード ポートにマッピングするには、*secondary_vlan_list* を入力するか、または **secondary_vlan_list** と *add* キーワードを使用します。
- セカンダリ VLAN と PVLAN 混合モード ポート間のマッピングをクリアするには、**secondary_vlan_list** と *remove* キーワードを使用します。

次に、ファスト イーサネット インターフェイス 5/2 を PVLAN 混合モード ポートとして設定し、PVLAN にマッピングして、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 200 2
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name:Fa5/2
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:200 (VLAN0200) 2 (VLAN0002)
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:
  200 (VLAN0200) 2 (VLAN0002)
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Capture Mode Disabled
Capture VLANs Allowed:ALL
```

レイヤ 2 インターフェイスの PVLAN ホスト ポートとしての設定

レイヤ 2 インターフェイスを PVLAN ホスト ポートとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# **configure terminal**	設定モードを開始します。
ステップ 2	Switch(config)# **interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port*	設定する LAN ポートを指定します。
ステップ 3	Switch(config-if)# **switchport mode private-vlan** {**host** | **promiscuous** | **trunk promiscuous | trunk [secondary]**}	レイヤ 2 インターフェイスを PVLAN ホスト ポートとして設定します。
ステップ 4	Switch(config-if)# [**no**] **switchport private-vlan host-association** *primary_vlan_ID secondary_vlan_ID*	レイヤ 2 インターフェイスを PVLAN に関連付けます。 プライマリ VLAN からすべてのアソシエーションを削除するには、**no** キーワードを使用します。
ステップ 5	Switch(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 6	Switch# **show interfaces** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* **switchport**	設定を確認します。

次に、ファスト イーサネット インターフェイス 5/1 を PVLAN ホスト ポートとして設定し、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end

Switch# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
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
Appliance trust: none
Administrative Private Vlan
  Host Association: 202 (VLAN0202) 440 (VLAN0440)
```

```
  Promiscuous Mapping: none
  Trunk encapsulation : dot1q
  Trunk vlans:
Operational private-vlan(s):
  202 (VLAN0202) 440 (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

レイヤ 2 インターフェイスの独立 PVLAN トランク ポートとしての設定

レイヤ 2 インターフェイスを独立 PVLAN トランク ポートとして設定するには、次の作業を行います。

	コマンド	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)# **interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port*	設定する LAN インターフェイスを指定します。
ステップ 3	Switch(config-if)# **switchport mode private-vlan** {**host** | **promiscuous** | **trunk promiscuous | trunk [secondary]**}	レイヤ 2 インターフェイスを PVLAN トランク ポートとして設定します。
ステップ 4	Switch(config-if)# [**no**] **switchport private-vlan association trunk** *primary_vlan_ID secondary_vlan_ID*	プライマリ VLAN とセカンダリ VLAN のアソシエーションを設定し、PVLAN トランク ポートを PVLAN に関連付けます。 **（注）** PVLAN トランク ポートが複数のセカンダリ VLAN を伝送できるように、このコマンドを使用して複数の PVLAN ペアを指定できます。既存のプライマリ VLAN にアソシエーションを指定した場合、既存のアソシエーションと置き換えられます。トランクにアソシエーションが指定されていない場合、セカンダリ VLAN で受信されたパケットはすべてドロップされます。 プライマリ VLAN からすべてのアソシエーションを削除するには、**no** キーワードを使用します。
ステップ 5	Switch(config-if)# [**no**] **switchport private-vlan trunk allowed vlan** *vlan_list* **all** | **none** | [**add** | **remove** | **except**] *vlan_atom*[,*vlan_atom*...]	PVLAN トランク ポートで許容される通常の VLAN のリストを設定します。 PVLAN トランク ポートで許容される通常の VLAN をすべて削除するには、**no** キーワードを使用します。
ステップ 6	Switch(config-if)# **switchport private-vlan trunk native vlan** *vlan_id*	PVLAN トランク ポートに（IEEE 802.1Q タグとしての）タグなしパケットが割り当てられる VLAN を設定します。 ネイティブ VLAN が設定されていない場合、タグなしのパケットはすべてドロップされます。 ネイティブ VLAN がセカンダリ VLAN で、ポートにセカンダリ VLAN の関連付けが指定されていない場合、タグなしパケットはドロップされます。 You can use the **no** keyword to remove all native VLANs on a PVLAN trunk port.

	コマンド	目的
ステップ 7	`Switch(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 8	`Switch# show interfaces {fastethernet | gigabitethernet | tengigabitethernet} slot/port switchport`	設定を確認します。

次に、ファスト イーサネット インターフェイス 5/2 をセカンダリ トランク ポートとして設定し、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10. 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
    Switchport: Enabled
    Administrative Mode: private-vlan trunk secondary
    Operational Mode: private-vlan trunk secondary
    Administrative Trunking Encapsulation: negotiate
    Operational Trunking Encapsulation: dot1q
    Negotiation of Trunking: On
    Access Mode VLAN: 1 (default)
    Trunking Native Mode VLAN: 1 (default)
    Administrative Native VLAN tagging: enabled
    Voice VLAN: none
    Administrative private-vlan host-association: none A
    dministrative private-vlan mapping: none
    Administrative private-vlan trunk native VLAN: 10
    Administrative private-vlan trunk Native VLAN tagging: enabled
    Administrative private-vlan trunk encapsulation: dot1q
    Administrative private-vlan trunk normal VLANs: none
    Administrative private-vlan trunk associations:
        3 (VLAN0003) 301 (VLAN0301)
    Administrative private-vlan trunk mappings: none
    Operational private-vlan: none
    Operational Normal VLANs: none
    Trunking VLANs Enabled: ALL
    Pruning VLANs Enabled: 2-1001
    Capture Mode Disabled Capture VLANs Allowed: ALL

    Unknown unicast blocked: disabled
    Unknown multicast blocked: disabled
    Appliance trust: none
```

レイヤ 2 インターフェイスの混合モード PVLAN トランク ポートとしての設定

レイヤ 2 インターフェイスを混合モード PVLAN トランク ポートとして設定するには、次の作業を行います。

	コマンド	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)# interface {fastethernet | gigabitethernet | tengigabitethernet} slot/port`	設定する LAN インターフェイスを指定します。
ステップ 3	`Switch(config-if)# switchport mode private-vlan {host | promiscuous | trunk promiscuous | trunk [secondary]}`	レイヤ 2 インターフェイスを PVLAN 混合モード トランク ポートとして設定します。
ステップ 4	`Switch(config-if)# [no] switchport private-vlan mapping [trunk] primary_vlan_ID {secondary_vlan_list | add secondary_vlan_list | remove secondary_vlan_list}`	混合モード PVLAN ポートをプライマリ VLAN および選択したセカンダリ VLAN にマッピングします。 このコマンドの削除には 3 つのレベルがあります。この表に続く例を参照してください。
ステップ 5	`Switch(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 6	`Switch# show interfaces {fastethernet | gigabitethernet | tengigabitethernet} slot/port switchport`	設定を確認します。

（注）　**switchport private-vlan mapping trunk** コマンドでサポートされる一意の PVLAN ペアの最大数は 500 です。プライマリ VLAN ごとに 1 つだけの独立 VLAN のアソシエーションがサポートされるため、たとえば、500 の独立セカンダリ VLAN を 500 のプライマリ VLAN にマッピングできます。または、500 のコミュニティ セカンダリ VLAN を 1 つのプライマリ VLAN にマッピングできます。または、250 のコミュニティ セカンダリ VLAN を 1 つのプライマリ VLAN にマッピングし、他の 250 のコミュニティ セカンダリ VLAN を他のプライマリ VLAN にマッピングして、合計 500 のペアを作成できます。

（注）　デフォルトでは、PVLAN トランク**混合モード**に設定すると、ネイティブ VLAN は 1 に設定されます。

[**no**] **switchport private-vlan mapping** コマンドには、次の 3 つの削除レベルがあります。

- リストから 1 つまたは複数のセカンダリ VLAN を削除するレベル。次に例を示します。

  ```
  Switch(config-if)# switchport private-vlan mapping trunk 2 remove 222
  ```

- PVLAN 混合モード トランク ポートから指定したプライマリ VLAN（およびそれ自身の選択したセカンダリ VLAN）へのマッピングをすべて削除するレベル。次に例を示します。

  ```
  Switch(config-if)# no switchport private-vlan mapping trunk 2
  ```

- PVLAN 混合モード トランク ポートから事前に設定されていたすべてのプライマリ VLAN（およびそれら自身の選択したセカンダリ VLAN）へのマッピングを削除するレベル。次に例を示します。

  ```
  Switch(config-if)# no switchport private-vlan mapping trunk
  ```

レイヤ 2 インターフェイスを PVLAN 混合モード ポートとして設定する場合、次の点に注意してください。

- 混合モード トランク ポートで複数のプライマリ VLAN を伝送できるようにするには、**switchport private-vlan mapping trunk** コマンドを使用して複数の PVLAN ペアを指定します。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一の PVLAN ID またはハイフンで連結した PVLAN ID の範囲です。
- セカンダリ VLAN を PVLAN 混合モード ポートにマッピングするには、*secondary_vlan_list* を入力するか、または **secondary_vlan_list** と *add* キーワードを使用します。
- セカンダリ VLAN と PVLAN 混合モード ポート間のマッピングをクリアするには、**secondary_vlan_list** と *remove* キーワードを使用します。

次に、ファスト イーサネット インターフェイス 5/2 を混合モード トランク ポートとして設定し、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan mapping trunk 3 301, 302
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 3-4,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    3 (VLAN0003) 301 (VLAN0301)  302 (VLAN0302)
Operational private-vlan:
  3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

セカンダリ VLAN 入力トラフィックのルーティングの許可

（注）　独立 VLAN とコミュニティ VLAN は、いずれもセカンダリ VLAN と呼ばれます。

セカンダリ VLAN 入力トラフィックのルーティングを許可するには、次の作業を行います。

	コマンド	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)# interface vlan primary_vlan_ID`	プライマリ VLAN のインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`Switch(config-if)# [no] private-vlan mapping primary_vlan_ID {secondary_vlan_list | add secondary_vlan_list | remove secondary_vlan_list}`	セカンダリ VLAN 入力トラフィックのルーティングを許可するために、セカンダリ VLAN をプライマリ VLAN にマッピングします。 プライマリ VLAN からすべてのアソシエーションを削除するには、**no** キーワードを使用します。
ステップ 4	`Switch(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Switch# show interface private-vlan mapping`	設定を確認します。

セカンダリ VLAN 入力トラフィックのルーティングを許可する場合、次の点に注意してください。

- **private-vlan mapping** インターフェイス コンフィギュレーション コマンドは、レイヤ 3 スイッチングされた PVLAN 入力トラフィックのみに影響します。
- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。各項目として入力できるのは、単一の PVLAN ID またはハイフンで連結した PVLAN ID の範囲です。
- セカンダリ VLAN をプライマリ VLAN にマッピングするには、*secondary_vlan_list* を入力するか、または **secondary_vlan_list** と *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 間のマッピングを消去するには、**secondary_vlan_list** パラメータと *remove* キーワードを使用します。

次に、PVLAN 303 ～ 307、309、および 440 からのセカンダリ VLAN 入力トラフィックのルーティングを許可し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface vlan 202
Switch(config-if)# private-vlan mapping add 303-307,309,440
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan202   303            community
vlan202   304            community
vlan202   305            community
vlan202   306            community
vlan202   307            community
vlan202   309            community
vlan202   440            isolated

Switch#
```