CHAPTER 40

プライベート VLAN の設定

（注） Supervisor Engine 6-E は、コミュニティ PVLAN、独立 PVLAN トランク、および無差別トランク ポートをサポートしません。

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	場所
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.40-13）
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。リストに含めることができる VLAN は 1 つだけです。	「セカンダリ VLAN のプライマリ VLAN との関連付け」（P.40-15）
show vlan private-vlan [**type**]	設定を確認します。	「PVLAN としての VLAN の設定」（P.40-13） 「セカンダリ VLAN のプライマリ VLAN との関連付け」（P.40-15）

コマンド	目的	場所
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.40-22）
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.40-10）
switchport private-vlan mapping [**trunk**] *primary_vlan_ID* {*secondary_vlan_list* | **add** *secondary_vlan_list* | **remove** *secondary_vlan_list*}	PVLAN 無差別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 無差別ポートとしての設定」（P.40-16） 「無差別トランク ポートとしてのレイヤ 2 インターフェイスの設定」（P.40-20）
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。	「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.40-17）
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。	「レイヤ 2 インターフェイスの PVLAN トランク ポートとしての設定」（P.40-18）
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 PVLAN トランク ポートとしての設定」（P.40-18）
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 PVLAN トランク ポートとしての設定」（P.40-18）

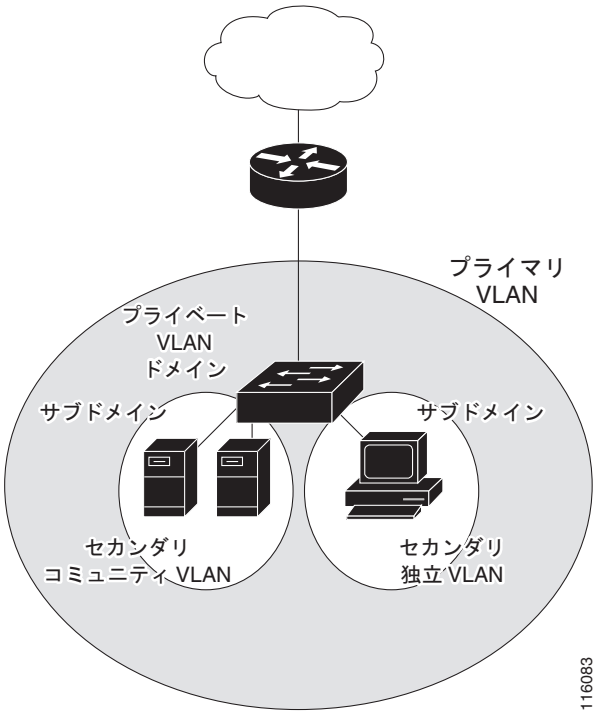
PVLAN の概要

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 1 カスタマーあたり 1 つの VLAN を割り当てる場合、サービス プロバイダーがサポートできるカスタマー数はこれに制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネット アドレス空間またはアドレス ブロックを割り当てますが、これにより、未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が起きます。

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。プライベート VLAN 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 のペアで表されます。プライベート VLAN には複数の VLAN ペアを設定可能で、各サブドメインにつき 1 ペアになります。プライベート VLAN 内のすべての 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 は、各サブドメインの区別に使用されます。図 40-1 を参照してください。

図 40-1　プライベート VLAN 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 内のポートは、レイヤ 2 レベルで相互に通信できません。
- コミュニティ VLAN：コミュニティ VLAN 内のポートは互いに通信できますが、レイヤ 2 レベルにある他のコミュニティ内のポートとは通信できません。

無差別ポートは、1 つのプライマリ VLAN、1 つの独立 VLAN、複数のコミュニティ VLAN だけで動作できます。レイヤ 3 ゲートウェイは通常無差別ポートを介してスイッチに接続されています。

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、個別のプライベート VLAN 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 ステーションはデフォルト ゲートウェイとの通信を行うだけで、プライベート VLAN の外部と通信することができます。

プライベート VLAN を使用し、次の方法でエンド ステーションへのアクセスを制御できます。

- 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選択して独立ポートとして設定し、レイヤ 2 の通信をしないようにします。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無差別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。

  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、無差別ポートを 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。無差別ポートを使用して、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。

この項では、次のトピックについて取り上げます。

定義一覧

用語	定義
プライベート VLAN	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。コミュニティ ポートは、同一コミュニティ VLAN のその他のポート、および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、他のコミュニティの他のすべてのインターフェイスおよびプライベート VLAN 内の独立ポートとレイヤ 2 で分離されます。
コミュニティ VLAN	コミュニティ VLAN：コミュニティ VLAN はセカンダリ VLAN であり、コミュニティ ポートから同一コミュニティの無差別ポート ゲートウェイおよびその他のホスト ポートにアップストリーム トラフィックを搬送します。複数のコミュニティ VLAN を 1 つのプライベート VLAN に設定できます。 **（注）** Supervisor Engine 6-E は、コミュニティ PLAN をサポートしません。
独立ポート	独立セカンダリ VLAN に属するホスト ポート。これは、無差別ポートを除く、同じプライベート VLAN 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。プライベート 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、無差別ポートにだけ転送されます。
独立 VLAN	独立 VLAN：プライベート VLAN の独立 VLAN は 1 つだけです。独立 VLAN はセカンダリ VLAN であり、ホストから無差別ポートおよびゲートウェイに向かう単一方向トラフィック アップストリームを搬送します。

用語	定義
プライマリ VLAN	プライマリ VLAN：プライベート VLAN には、プライマリ VLAN を 1 つだけ設定できます。プライベート VLAN 内のすべてのポートは、プライマリ VLAN のメンバーです。プライマリ VLAN は、無差別ポートからの単一方向トラフィックのダウンストリームを、（独立およびコミュニティ）ホスト ポートおよび他の無差別ポートへ伝送します。
プライベート VLAN 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。
無差別ポート	無差別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。
無差別トランク ポート	無差別トランク 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、ポートは無差別アクセス 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。 **（注）** Supervisor Engine 6-E は、混合モード トランク ポートをサポートしません。

複数のスイッチの PVLAN

（注） Supervisor Engine 6-E は、コミュニティ PVLAN、独立 PVLAN トランク、および混合モード PVLAN トランク ポートをサポートしません。

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」（P.40-5）
- 「独立 PVLAN トランク ポート」（P.40-6）
- 「無差別 PVLAN トランク ポート」（P.40-8）

標準トランク ポート

通常の VLAN と同様に、プライベート VLAN を複数のスイッチにまたがるように設定できます。トランク ポートはプライマリ VLAN およびセカンダリ VLAN を隣接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 として扱います。複数のスイッチにまたがるプライベート VLAN の機能の場合、スイッチ A にある独立ポートからのトラフィックはスイッチ B に到達しませ

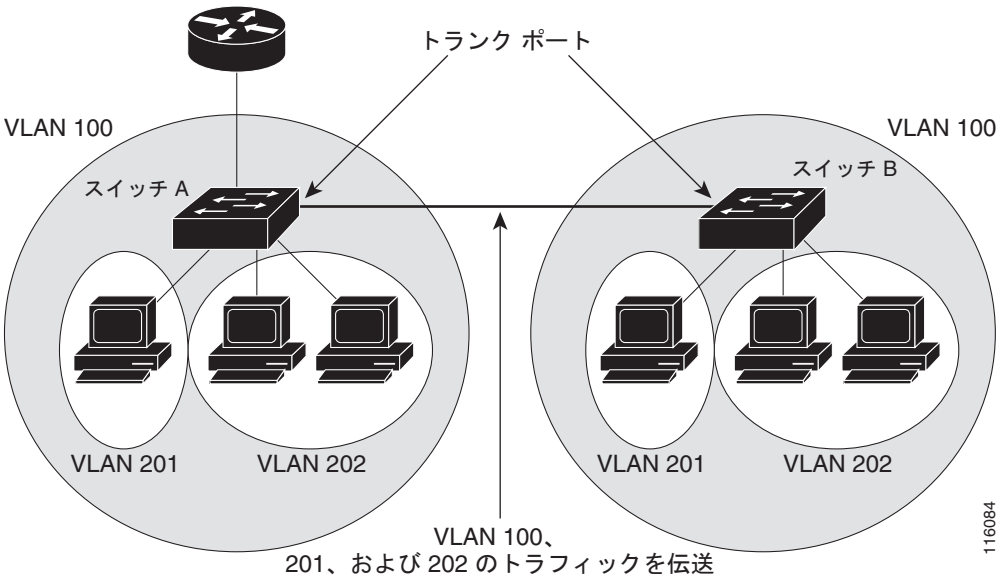
ん。図 40-2 を参照してください。

プライベート VLAN コンフィギュレーションのセキュリティを保って VLAN の他のユーザがプライベート VLAN に設定されないようにするには、プライベート VLAN ポートのないデバイスを含む、すべての中間デバイス内にプライベート VLAN を設定します。

（注）　トランク ポートは、通常の VLAN からのトラフィックを伝送し、またプライマリ、独立、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。

（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 40-2　　スイッチ間の PVLAN



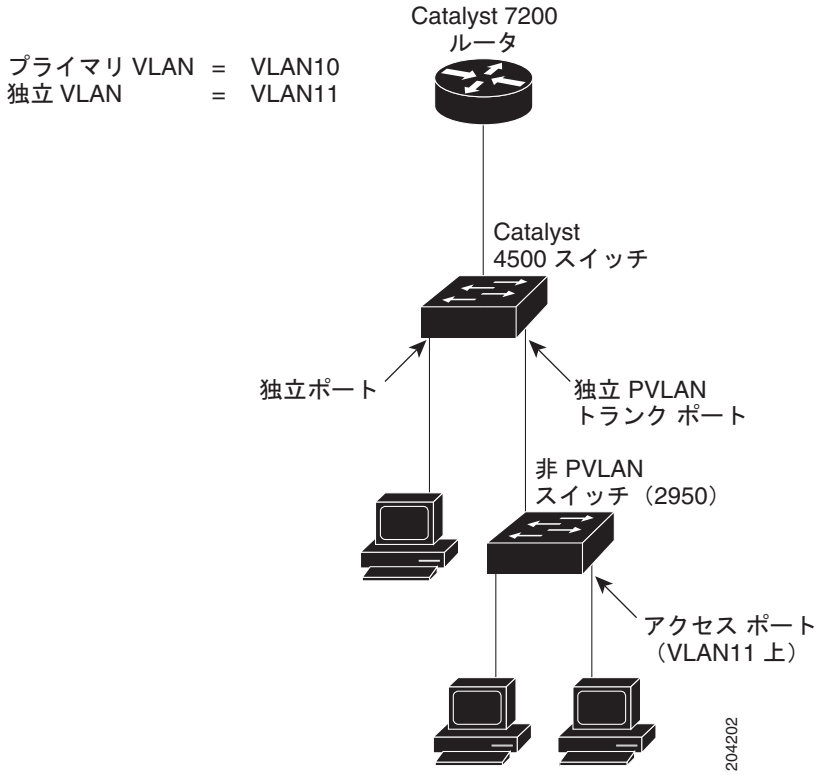
VLAN 100 = プライマリ VLAN
VLAN 201 = セカンダリ独立 VLAN
VLAN 202 = セカンダリ コミュニティ VLAN

VTP はプライベート VLAN をサポートしないので、レイヤ 2 ネットワーク内のすべてのスイッチにプライベート VLAN を手動で設定する必要があります。ネットワーク内の一部のスイッチにプライマリおよびセカンダリ VLAN の関連を設定しない場合、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。これにより、これらのスイッチにプライベート VLAN 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。

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 40-3　　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、無差別ポートとプライマリ VLAN（VLAN 10）の Catalyst 4500 シリーズ スイッチによって受信されます。その後、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。その後、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。

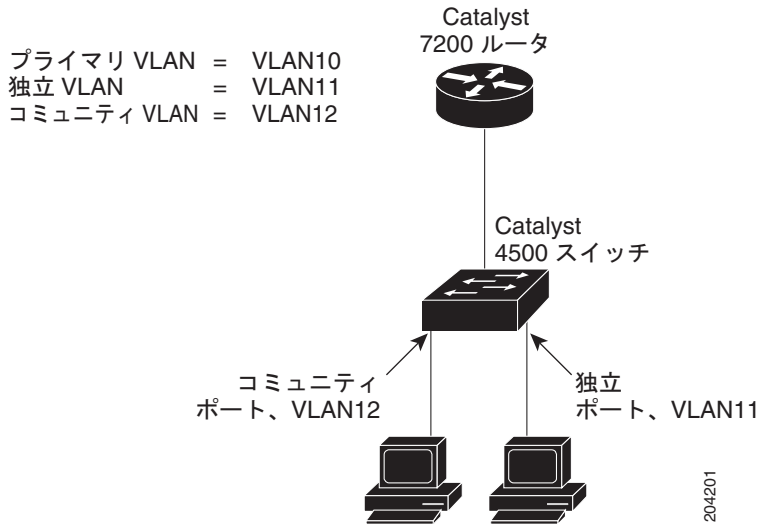
保護ポートの詳細については、次の URL を参照してください。

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

無差別 PVLAN トランク ポート

PVLAN 無差別トランクが使用されるのは、一般的には PVLAN 無差別ホスト 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 ルータを接続する場合に役立ちます。

図 40-4　　無差別 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 スイッチに到達します。このトラフィックは、このルータ宛てに無差別 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 ポートで受信された場合と同様に、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 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 無差別トランクは、VLAN QoS と相互に作用します。「PVLAN と VLAN ACL/QoS」（P.40-9）を参照してください。

PVLAN と他の機能との相互作用

プライベート VLAN には、次のように他の機能と相互作用があります。

- 「PVLAN と VLAN ACL/QoS」（P.40-9）
- 「プライベート VLAN 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.40-9）
- 「プライベート VLAN と SVI」（P.40-10）

詳細については、「PVLAN 設定時の注意事項および制約事項」（P.40-11）も参照してください。

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 無差別アクセス 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 無差別トランク 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。

無差別トランク 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、無差別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。

パケットが無差別トランク 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、別の無差別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、無差別トランク 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。

プライベート VLAN 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 にあるデバイスはレイヤ 2 レベルで互いに通信しますが、別の VLAN にあるインターフェイスに接続されたデバイスとはレイヤ 3 レベルで通信する必要があります。プライベート VLAN の場合、無差別ポートはプライマリ VLAN のメンバーであり、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 に対応付けられているため、これらの VLAN のメンバーはレイヤ 2 レベルで互いに通信できます。

通常の VLAN の場合、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。プライベート VLAN のブロードキャストの転送は、次のようにブロードキャストを送信するポートによって決まります。

- 独立ポートは、無差別ポートまたはトランク ポートだけにブロードキャストを送信します。
- コミュニティ ポートは、すべての無差別ポート、トランク ポート、同一コミュニティ VLAN のポートにブロードキャストを送信します。
- 無差別ポートは、プライベート VLAN のすべてのポート（その他の無差別ポート、トランク ポート、独立ポート、コミュニティ ポート）にブロードキャストを送信します。

マルチキャスト トラフィックは、プライベート VLAN 境界を越えて単一のコミュニティ VLAN 内に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、同一独立 VLAN のポート間、または別々のセカンダリ VLAN のポート間で転送されません。

プライベート VLAN と SVI

レイヤ 3 スイッチでは、スイッチ仮想インターフェイス（SVI）が VLAN のレイヤ 3 インターフェイスを表します。レイヤ 3 デバイスは、セカンダリ VLAN ではなく、プライマリ VLAN を通してだけプライベート VLAN と通信します。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。レイヤ 3 VLAN インターフェイスをセカンダリ VLAN 用に設定できません。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 はアクティブになりません。

- SVI がアクティブである VLAN をセカンダリ VLAN として設定する場合、SVI をディセーブルにしないと、この設定は許可されません。
- セカンダリ VLAN として設定されている VLAN に SVI を作成しようとしてセカンダリ VLAN がすでにレイヤ 3 にマッピングされている場合、SVI は作成されず、エラーが返されます。SVI がレイヤ 3 にマッピングされていない場合、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 をセカンダリ VLAN と関連付けてマッピングすると、プライマリ VLAN の設定がセカンダリ VLAN の SVI に伝播されます。たとえば、プライマリ VLAN の SVI に IP サブネットを割り当てると、このサブネットは、プライベート VLAN 全体の IP サブネット アドレスになります。

PVLAN の設定

ここでは、PVLAN の設定手順について説明します。

プライベート VLAN 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 モードをトランスペアレントに設定します。「VTP のディセーブル化（VTP トランスペアレント モード）」（P.13-16）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.40-13）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.40-13）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.40-15）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.40-17）および「レイヤ 2 インターフェイスの PVLAN トランク ポートとしての設定」（P.40-18）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.40-15）を参照してください。

ステップ 7　インターフェイスを無差別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 無差別ポートとしての設定」（P.40-16）を参照してください。

ステップ 8　無差別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 無差別ポートとしての設定」（P.40-16）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.40-22）を参照してください。

ステップ 10　プライマリ VLAN 設定を確認します。「Switch#」（P.40-22）を参照してください。

デフォルトのプライベート VLAN 設定

プライベート VLAN 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 のトランスペアレント モードでイネーブルにします。

  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 フォワーディング ステートのままです。
- レイヤ 3 VLAN インターフェイスをセカンダリ VLAN 用に設定できません。

  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。
- プライベート 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 アクセス コントロール エントリ（ACE）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。
  - プライベート VLAN 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 43 章「SPAN および 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 はプライベート VLAN をサポートしません。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 39 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、別々の Quality of Service（QoS）設定を適用できます（第 32 章「Quality of Service 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。
- 無差別ポートでは、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 ポートと無差別トランク 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る ARP エントリは、「sticky」ARP エントリです（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 は無差別トランク ポートで伝送されます。
- 無差別トランク 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。
- 無差別トランクは、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。
- 無差別トランク 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、無差別トランク 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 無差別トランク 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。

  無差別トランク 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 無差別トランク ポートに IEEE 802.1X を設定しないでください。

PVLAN としての VLAN の設定

（注） Supervisor Engine 6-E は、コミュニティ PLAN をサポートしません。

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`	コンフィギュレーション モードに入ります。
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。

	コマンド	目的
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。 （注）　Supervisor Engine 6-E は、コミュニティ VLAN と独立 PVLAN トランク ポートをサポート*しません*。
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**	コンフィギュレーション モードに入ります。
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。リストに含めることができる VLAN は 1 つだけです。 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。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN 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 を入れることができます。
- *secondary_vlan_list* パラメータには、独立 VLAN ID を 1 つだけ入れることができます。
- セカンダリ VLAN をプライマリ VLAN に関連付けるには、*secondary_vlan_list* パラメータを入力するか、または *secondary_vlan_list* パラメータを指定して **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 間の関連付けを消去するには、*secondary_vlan_list* パラメータを指定して **remove** キーワードを使用します。
- 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実行されません。

次に、コミュニティ VLAN 303 ～ 307、309、および独立 VLAN 440 をプライマリ VLAN 202 に関連付けて、設定を確認する方法を示します。

```
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 無差別ポートとしての設定

レイヤ 2 インターフェイスを PVLAN 無差別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 無差別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 無差別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）　上記の **switchport private-vlan mapping trunk** コマンドでサポートされる一意のプライベート VLAN ペアの最大数は 500 です。たとえば、1000 のセカンダリ VLAN を 1 つのプライマリ VLAN にマッピングしたり、1000 のセカンダリ VLAN を 1000 のプライマリ VLAN に 1 対 1 でマッピングしたりすることができます。

レイヤ 2 インターフェイスを PVLAN 無差別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。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 無差別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 無差別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 無差別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**	コンフィギュレーション モードに入ります。
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 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 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 VLAN 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 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。

	コマンド	目的
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。 PVLAN トランク ポートですべてのネイティブ VLAN を削除するには、**no** キーワードを使用します。
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
```

無差別トランク ポートとしてのレイヤ 2 インターフェイスの設定

（注）　Supervisor Engine 6-E は、無差別モード トランク ポートをサポート*しません*。

レイヤ 2 インターフェイスを PVLAN 無差別トランク 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 無差別トランク 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}`	PVLAN 無差別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）　上記の **switchport private-vlan mapping trunk** コマンドでサポートされる一意のプライベート VLAN ペアの最大数は 500 です。たとえば、1000 のセカンダリ VLAN を 1 つのプライマリ VLAN にマッピングしたり、1000 のセカンダリ VLAN を 1000 のプライマリ VLAN に 1 対 1 でマッピングしたりすることができます。

（注）　デフォルトでは、プライベート VLAN トランク無差別に設定すると、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 無差別トランク 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 無差別トランク 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 無差別ポートとして設定する場合、次の点に注意してください。

- 無差別トランク 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。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 無差別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 無差別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 を無差別トランク 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 およびコミュニティ VLAN は、ともにセカンダリ 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。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN 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* パラメータを入力するか、または *secondary_vlan_list* パラメータを指定して **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* パラメータを指定して **remove** キーワードを使用します。

次に、プライベート VLAN 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て、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#
```