CHAPTER 14

# プライベート VLAN の設定

この章では、Catalyst 3750 Metro スイッチでプライベート VLAN を設定する方法について説明します。

（注） この章で使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。



（注） プライベート VLAN を設定する場合、スイッチは VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）透過モードでなければなりません。第 13 章「VTP の設定」を参照してください。

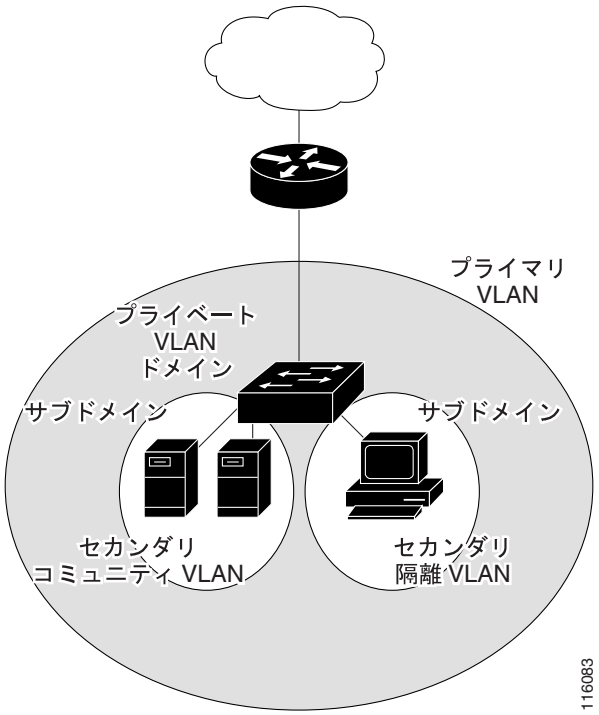
# プライベート VLAN の概要

プライベート VLAN 機能は、サービス プロバイダーが VLAN を使用している間に直面する次の問題に対処します。

- スケーラビリティ：スイッチは最大 1005 のアクティブ VLAN をサポートします。サービス プロバイダーがカスタマーあたり 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より制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN をサブネット アドレス スペース、またはアドレス ブロックに割り当てます。ただし、これにより未使用の IP アドレスが無駄に使用され、IP アドレス管理に問題が発生します。

プライベート VLAN を使用すると、スケーラビリティ問題に対処します。また、サービス プロバイダーにとっては IP アドレス管理の利点が提供され、カスタマーに対してはレイヤ 2 のセキュリティを提供します。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 および*セカンダリ* VLAN という VLAN のペアで表現されます。プライベート VLAN には複数の VLAN ペアがあり、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、あるサブドメインを別のサブドメインと区別します。図 14-1 を参照してください。

**図 14-1　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。

- 隔離 VLAN — 隔離 VLAN 内のポートは、レイヤ 2 レベルでは互いに通信できません。
- 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 レベルでの他のコミュニティのポートとは通信できません。

プライベート VLAN は、同じプライベート VLAN 内のポートの間をレイヤ 2 レベルで切り離します。プライベート VLAN は、次のいずれかのタイプのアクセス ポートです。

- 混合 — 混合ポートはプライマリ VLAN に属し、プライマリ VLAN に対応付けられたセカンダリ VLAN に属するコミュニティおよび隔離ホスト ポートなどのすべてのインターフェイスと通信できます。
- 隔離 — 隔離ポートは、隔離セカンダリ VLAN に属するホスト ポートです。これは、混合ポート以外の、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、隔離ポートに対して、混合ポートからのトラフィック以外のトラフィックすべてをブロックします。隔離ポートから受信したトラフィックは混合ポートへのみ、転送されます。
- コミュニティ — コミュニティ ポートは、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 内の他のポートおよび混合ポートと通信します。このインターフェイスはレイヤ 2 で、他のコミュニティの他のインターフェイスすべてから、また同じプライベート VLAN 内の隔離ポートから分離されます。

**（注）** トランク ポートは、通常の VLAN からトラフィックを伝送し、またプライマリ、隔離、コミュニティ VLAN からもトラフィックを伝送します。

プライマリおよびセカンダリ VLAN には次の特性があります。

- プライマリ VLAN — プライベート VLAN にはプライマリ VLAN が 1 つだけあります。プライベート VLAN 内の各ポートは、プライマリ VLAN のメンバーです。プライマリ VLAN は、混合ポートからの単一方向トラフィック ダウンストリームを、（隔離およびコミュニティ）ホスト ポートおよび他の混合ポートに伝送します。
- 隔離 VLAN — プライベート VLAN には隔離 VLAN が 1 つだけあります。隔離 VLAN は、ホストからの単一方向トラフィック アップストリームを混合ポートおよびゲートウェイに向けて伝送するセカンダリ VLAN です。
- コミュニティ VLAN — コミュニティ VLAN は、コミュニティ ポートからのアップストリーム トラフィックを混合ポート ゲートウェイおよび同じコミュニティ内の他のホスト ポートに伝送するセカンダリ VLAN です。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。

混合ポートでは、プライマリ VLAN を 1 つ、隔離 VLAN を 1 つ、複数のコミュニティ VLAN のみを処理できます。レイヤ 3 ゲートウェイは通常、混合ポートを介してスイッチに接続されます。混合ポートを使用すると、プライベート VLAN へのアクセス ポイントとして幅広いデバイスを接続できます。たとえば、管理ワークステーションからすべてのプライベート VLAN サーバをモニタ、またはバックアップするのに、混合ポートを使用できます。

スイッチングされた環境では、個別のプライベート VLAN と対応する IP サブネットを、個々のエンド ステーションまたはエンド ステーションの共通グループに割り当てることができます。プライベート VLAN 外で通信するには、エンド ステーションはデフォルト ゲートウェイとのみ通信する必要があります。

プライベート VLAN を使用してエンド ステーションへのアクセスを次のように制御できます。

- レイヤ 2 で通信を行わないようにするには、エンド ステーションに接続されたインターフェイスを選択して隔離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の間でレイヤ 2 通信は実施されません。
- エンド ステーションすべてがデフォルト 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 ゲートウェイと選択したエンド ステーション（バックアップ サーバなど）に接続されたインターフェイスを混合ポートとして設定します。

プライベート VLAN をサポートする他のデバイスにプライマリ、隔離、コミュニティ VLAN をトランキングすることで、プライベート VLAN を複数のデバイスに拡張できます。プライベート VLAN 設定のセキュリティを維持し、プライベート VLAN として設定された VLAN の別の使用を避けるには、すべての中間デバイス（プライベート VLAN ポートのないデバイスを含む）でプライベート VLAN を設定します。

## プライベート VLAN での IP アドレス方式

個別の VLAN を各カスタマーに割り当てると、IP アドレス方式が非効率的になります。

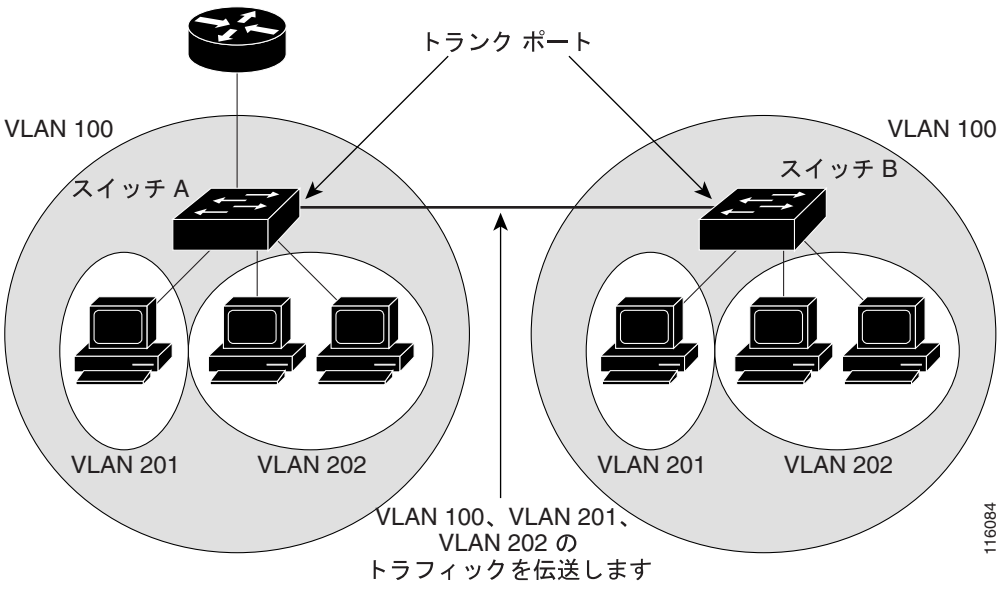
- アドレス ブロックをカスタマー VLAN に割り当てると、未使用の IP アドレスが出てきます。
- VLAN 内のデバイス数が増えた場合、それに対応するだけのアドレスを割り当てられない場合があります。

プライベート VLAN のメンバーすべてが共通のアドレス スペースを共有しているプライベート VLAN を使用することで、この問題を軽減できます。アドレス スペースはプライマリ VLAN に割り当てられています。ホストはセカンダリ VLAN に接続されます。DHCP サーバは、プライマリ VLAN に割り当てられたアドレス ブロックからホストに IP アドレスを割り当てます。後続の IP アドレスは、同じプライマリ VLAN 内の異なるセカンダリ VLAN のカスタマー デバイスに割り当てられます。新しいデバイスを追加する場合、DHCP サーバはサブネット アドレスの大きなプールから次に使用可能なアドレスをデバイスに割り当てます。

## 複数のスイッチにまたがるプライベート VLAN

通常の VLAN の場合と同様に、プライベート VLAN は複数のスイッチにまたがることができます。トランク ポートはプライマリ 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 ポートはプライベート VLAN を他の VLAN と同様に扱います。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 の隔離ポートからのトラフィックがスイッチ B の隔離ポートに到達しません。詳細については、図 14-2 を参照してください。

**図 14-2　複数のスイッチにまたがるプライベート VLAN**




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

プライベート VLAN を 2 つのスイッチの間で正しく動作させるには、トランクの両側で VLAN 変換を設定する必要があります。各スイッチの Enhanced-Services（ES）ポートで VLAN 変換を設定し、両方のスイッチのカスタマー ポートで同じプライベート VLAN ID を使用することを推奨します。こうすると、プライベート VLAN エンド ユーザ間でのデータ交換が可能となります。

VTP はプライベート VLAN をサポートしないため、レイヤ 2 ネットワーク内のすべてのスイッチ上でプライベート 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のプライマリおよびセカンダリ VLAN の関係を設定しない場合、そ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、それらのスイッチで不要なプライベート VLAN のフラッディングが発生します。

（注）　スイッチ上でプライベート VLAN を設定する場合、必ずデフォルトの Switch Database Management（SDM）テンプレートを使用して、ユニキャスト ルートとレイヤ 2 エントリの間のシステム リソースを均衡化します。別の SDM テンプレートを設定する場合、**sdm prefer default** グローバル コンフィギュレーション コマンドを使用してデフォルトのテンプレートを設定します。第 7 章「SDM テンプレートの設定」を参照してください。

## プライベート VLAN と他の機能との相互作用

プライベート VLAN と他の機能との特有な相互作用は、次のとおりです。

- プライベート VLAN と、ユニキャスト、ブロードキャスト、マルチキャスト トラフィック（p.14-5）
- プライベート VLAN および SVI（p.14-6）

「プライベート VLAN 設定時の注意事項」の章の「セカンダリおよびプライマリ VLAN の設定」（p.14-8）も参照してください。

### プライベート VLAN と、ユニキャスト、ブロードキャスト、マルチキャスト トラフィック

通常の VLAN では、同じ VLAN 内のデバイスはレイヤ 2 レベルで互いに通信できますが、別の VLAN 内のインターフェイスに接続されたデバイスはレイヤ 3 レベルで通信する必要があります。プライベート VLAN では、混合ポートはプライマリ VLAN のメンバーです。ホスト ポートはセカンダリ VLAN に所属します。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 では、ブロードキャストはその VLAN 内のすべてのポートに転送されます。プライベート VLAN ブロードキャストの転送は、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。

- 隔離ポートはブロードキャストを混合ポートまたはトランク ポートへのみ送信します。
- コミュニティポートは、ブロードキャストをすべての混合ポート、トランク　ポート、同じコミュニティ VLAN 内のポートに送信します。
- 混合ポートは、ブロードキャストをプライベート VLAN 内のすべてのポート（他の混合ポート、トランク ポート、隔離ポート、コミュニティ ポート）に送信します。

マルチキャスト トラフィックは、プライベート VLAN 境界を超え、単一のコミュニティ VLAN 内でルーティングおよびブリッジングされます。マルチキャスト トラフィックは、同じ隔離 VLAN 内のポートの間、または別のセカンダリ VLAN 内のポートの間では転送されません。

## プライベート VLAN および 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 インターフェイスになります。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 を介してのみプライベート VLAN と通信します。レイヤ 3 VLAN インターフェイス（SVI）をプライマリ VLAN にのみ設定します。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。VLAN がセカンダリ VLAN として設定されている場合、セカンダリ VLAN の SVI は非アクティブです。

- アクティブな SVI を設定した VLAN をセカンダリ VLAN として設定しようとする場合、SVI をディセーブルにするまで設定は許可されません。
- セカンダリ VLAN として設定された VLAN 上で SVI を作成しようとしてセカンダリ VLAN がすでにレイヤ 3 で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 で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 がセカンダリ VLAN に対応付けられマッピングされている場合、プライマリ VLAN の設定はセカンダリ VLAN の 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 の SVI に割り当てる場合、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。

# プライベート VLAN の設定

ここでは、プライベート VLAN 設定の注意事項と手順について説明します。内容は次のとおりです。



## プライベート VLAN の設定作業

プライベート VLAN を設定するには、次の手順を実行します。

**ステップ 1**　VTP モードを透過モードに設定します。

**ステップ 2**　プライマリおよびセカンダリ VLAN を作成し、対応付けます。「プライベート VLAN 内の VLAN の設定および対応付け」（p.14-11）を参照してください。

（注）　VLAN がまだ作成されていない場合、プライベート VLAN 設定プロセスで作成します。

**ステップ 3**　インターフェイスを隔離またはコミュニティ ホスト ポートに設定し、VLAN メンバーシップをホスト ポートに割り当てます。「プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定」（p.14-12）を参照してください。

**ステップ 4**　インターフェイスを混合ポートとして設定し、混合ポートをプライマリとセカンダリ VLAN のペアにマッピングします。「プライベート VLAN 混合ポートとしてのレイヤ 2 インターフェイスの設定」（p.14-13）を参照してください。

**ステップ 5**　VLAN 間ルーティングを使用する場合、プライマリ SVI を設定し、セカンダリ VLAN をプライマリにマッピングします。「プライマリ VLAN レイヤ 3 VLAN インターフェイスへのセカンダリ VLAN のマッピング」（p.14-14）を参照してください。

**ステップ 6**　プライベート VLAN 設定を確認します。

## プライベート VLAN のデフォルト設定

プライベート VLAN は設定されていません。

# プライベート VLAN 設定時の注意事項

プライベート VLAN の設定時の注意事項は、次のカテゴリに分類されます。



## セカンダリおよびプライマリ VLAN の設定

プライベート VLAN の設定を行うときは、次の注意事項に従ってください。

- VTP を透過モードに設定します。プライベート VLAN を設定したあと、VTP モードをクライアントまたはサーバに変更しないでください。VTP の詳細については、第 13 章「VTP の設定」を参照してください。
- プライベート VLAN を設定するには、VLAN 設定（config-vlan）モードを使用する必要があります。VLAN データベース コンフィギュレーション モードではプライベート VLAN を設定できません。VLAN 設定の詳細については、「VLAN 設定モードのオプション」（p.12-8）を参照してください。
- プライベート VLAN を設定したあと、VTP 透過モード設定およびプライベート VLAN 設定をスイッチのスタートアップ　コンフィギュレーション　ファイルに保存するには、**copy running-config startup config** 特権 EXEC コマンドを使用します。保存しないと、スイッチをリセットした場合、デフォルトの VTP サーバ モードとなり、プライベート VLAN をサポートしません。
- VTP はプライベート VLAN を伝播しません。プライベート VLAN ポートが必要な各デバイスで、プライベート VLAN を設定する必要があります。
- VLAN 1、または VLAN 1002 ～ 1005 をプライマリまたはセカンダリ VLAN として設定できません。拡張 VLAN（VLAN ID 1006 ～ 4094）はプライベート VLAN に所属できます。
- プライマリ VLAN には、1 つの隔離 VLAN と、これに対応付けられた複数のコミュニティ VLAN を設定できます。隔離またはコミュニティ VLAN には、これに対応付けられたプライマリ VLAN が 1 つのみ設定できます。
- プライベート VLAN には、1 つまたは複数の VLAN がありますが、プライベート VLAN 全体で稼働するのは Spanning-Tree Protocol（STP; スパニングツリー プロトコル）インスタンス 1 つのみです。セカンダリ VLAN がプライマリ VLAN に対応付けられている場合、プライマリ VLAN の STP パラメータはセカンダリ VLAN に伝播されます。
- プライベート VLAN で DHCP スヌーピングをイネーブルにできます。プライマリ VLAN で DHCP スヌーピングをイネーブルにすると、セカンダリ VLAN に伝播されます。セカンダリ VLAN で DHCP を設定する場合、その設定はプライマリ VLAN がすでに設定されていると有効にはなりません。
- プライベート VLAN ポートで IP ソース ガードをイネーブルにする場合は、プライマリ VLAN で DHCP スヌーピングをイネーブルにする必要があります。
- プライベート VLAN のトラフィックを伝送しないデバイスのトランクからプライベート VLAN をプルーニングすることを推奨します。
- 別の QoS（Quality of Service）設定をプライマリ VLAN、隔離 VLAN、コミュニティ VLAN に適用できます。
- プライベート VLAN を設定すると、デフォルトでは sticky Address Resolution Protocol（ARP; アドレス解決プロトコル）はイネーブルになり、レイヤ 3 プライベート VLAN インターフェイス上で学習された ARP エントリは sticky ARP エントリになります。セキュリティを確保するため、プライベート VLAN ポート sticky ARP エントリは期限切れになりません。

**（注）** プライベート VLAN 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。

MAC アドレスが違っても IP アドレスが同じデバイスに接続すると、メッセージが生成されて、ARP エントリは作成されません。プライベート VLAN ポート sticky ARP エントリは期限切れにならないため、MAC アドレスを変更する場合はプライベート VLAN ポート ARP エントリを手動で削除する必要があります。

- **no arp** *ip-address* グローバル コンフィギュレーション コマンドを使用すると、プライベート VLAN ARP エントリを削除できます。
- **arp** *ip-address hardware-address* **type** グローバル コンフィギュレーション コマンドを使用すると、プライベート VLAN ARP エントリを追加できます。

- VLAN マップをプライマリおよびセカンダリ VLAN で設定できます（「VLAN マップの設定」[p.32-31] を参照）。ただし、同じ VLAN マップをプライベート VLAN のプライマリおよびセカンダリ VLAN に設定することを推奨します。
- フレームがプライベート VLAN 内で転送されるレイヤ 2 の場合、同じ VLAN マップが入出力側で適用されます。フレームがプライベート VLAN 内部から外部ポートにルーティングされた場合、プライベート VLAN マップが入力側で適用されます。
  - ホスト ポートから混合ポートへアップストリームで送信されるフレームの場合、セカンダリ VLAN で設定された VLAN マップが適用されます。
  - 混合ポートからホスト ポートへダウンストリームで送信されるフレームの場合、プライマリ VLAN で設定された VLAN マップが適用されます。

  プライベート VLAN の特定の IP トラフィックをフィルタリングするには、VLAN マップをプライマリおよびセカンダリ VLAN 両方に適用する必要があります。
- 2 つのプライベート VLAN 間でトンネル経由でデータが交換されるようにするには、スイッチのエッジの ES ポートで VLAN 変換を設定し、スイッチのプライベート VLAN ポートで同じ VLAN ID を使用します。
- ルータ ACL（アクセス コントロール リスト）をプライマリ VLAN の SVI にのみ適用できます。ACL はプライマリおよびセカンダリ VLAN レイヤ 3 トラフィック両方に適用できます。
- プライベート VLAN はレイヤ 2 でホストを分離しますが、ホストはレイヤ 3 で互いに通信できます。
- プライベート VLAN は、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能をサポートします。
  - 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。
  - 出力または入力トラフィックを個別にモニタするには、プライマリ VLAN、隔離 VLAN、またはコミュニティ VLAN で VLAN-based SPAN（VSPAN）を使用できます。または 1 つの VLAN でのみ SPAN を使用できます。

## プライベート VLAN ポートの設定

プライベート VLAN ポートの設定を行うときは、次の注意事項に従ってください。

- プライマリ VLAN、隔離 VLAN、またはコミュニティ VLAN にポートを割り当てるには、プライベート VLAN コンフィギュレーション コマンドのみを使用します。VLAN がプライベート VLAN 設定の一部である間、プライマリ VLAN、隔離 VLAN、またはコミュニティ VLAN として設定する VLAN に割り当てられたレイヤ 2 アクセス ポートは、非アクティブです。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。
- Port Aggregation Protocol（PAgP）または Link Aggregation Control Protocol（LACP）EtherChannel に所属するポートをプライベート VLAN ポートとして設定しないでください。ポートがプライベート VLAN 設定の一部である間、ポートの EtherChannel 設定は非アクティブです。
- 誤った設定による STP ループを防ぎ、STP コンバージェンスを高速にするには、隔離およびコミュニティ ホスト ポートで、PortFast および BPDU（ブリッジ プロトコル データ ユニット）ガードをイネーブルにします（第 19 章「オプションのスパニングツリー機能の設定」を参照）。イネーブルの場合、STP は BPDU ガード機能を PortFast が設定されたレイヤ 2 LAN ポートすべてに適用します。混合ポートで、PortFast および BPDU ガードをイネーブルにしないでください。

- プライベート VLAN 設定で使用する VLAN を削除した場合、VLAN に対応付けられたプライベート VLAN ポートが非アクティブになります。
- デバイスがトランク接続され、プライマリおよびセカンダリ VLAN がトランクから削除されていない場合、プライベート VLAN ポートは別のネットワーク デバイス上に存在できます。

## 他の機能との制限

プライベート VLAN を設定する場合、他の機能との制限があることに注意してください。

（注）　エラー　メッセージが表示されずに設定が受け入れられても、コマンドが機能しない場合があります。

- プライベート VLAN を使用したスイッチ上で、代替ブリッジングを設定しないでください。
- IGMP スヌーピングがスイッチ上でイネーブル（デフォルト）の場合、スイッチでは 20 以上のプライベート VLAN ドメインがサポートされます。
- Remote SPAN（RSPAN）VLAN を、プライベート VLAN のプライマリまたはセカンダリ VLAN として設定しないでください。

  SPAN の詳細については、第 28 章「SPAN および RSPAN の設定」を参照してください。
- 次の機能が設定されたインターフェイスに、プライベート VLAN を設定しないでください。
  - ダイナミック アクセス ポート VLAN メンバーシップ
  - Dynamic Trunking Protocol（DTP）
  - PAgP
  - LACP
  - Multicast VLAN Registration（MVR）
  - 音声 VLAN
- プライベート VLAN ポートで IEEE 802.1x ポートベースの認証を設定できますが、プライベート VLAN ポートに、802.1x とポート セキュリティ、音声 VLAN、またはユーザ単位 ACL を設定できません。
- プライベート VLAN ホストまたは混合ポートは、SPAN 宛先ポートにできません。SPAN 宛先ポートをプライベート VLAN ポートとして設定すると、ポートは非アクティブになります。
- プライマリ VLAN の混合ポートにスタティック MAC アドレスを設定する場合、同じスタティック アドレスを関連するセカンダリ VLAN すべてに追加する必要があります。セカンダリ VLAN のホスト ポートにスタティック MAC アドレスを設定する場合、同じスタティック MAC アドレスを関連するプライマリ VLAN に追加する必要があります。スタティック MAC アドレスをプライベート VLAN ポートから削除する場合、設定された MAC アドレスのインスタンスをすべて、プライベート VLAN から削除する必要があります。

  （注）　プライベート VLAN のある VLAN で学習されたダイナミック MAC アドレスは、対応付けられた VLAN で複製されます。たとえば、セカンダリ VLAN で学習された MAC アドレスは、プライマリ VLAN で複製されます。元のダイナミック MAC アドレスが削除、または期限切れになった場合、複製されたアドレスが MAC アドレス テーブルから削除されます。

- レイヤ 3 VLAN インターフェイス（SVI）をプライマリ VLAN にのみ設定します。

## プライベート VLAN 内の VLAN の設定および対応付け

プライベート VLAN を設定するには、特権 EXEC モードで次の手順を行います。

（注）　VLAN コンフィギュレーション モードを終了するまで、**private-vlan** コマンドは有効になりません。

| | コマンド | 説明 |
|---|---|---|
| ステップ 1 | **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 | **vtp mode transparent** | VTP モードを透過モードに設定します（VTP をディセーブルにします）。 |
| ステップ 3 | **vlan** *vlan-id* | VLAN コンフィギュレーション モードを開始し、プライマリ VLAN となる VLAN を指定または作成します。指定できる VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。 |
| ステップ 4 | **private-vlan primary** | プライマリ VLAN として VLAN を指定します。 |
| ステップ 5 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 6 | **vlan** *vlan-id* | （任意）VLAN コンフィギュレーション モードを開始し、隔離 VLAN となる VLAN を指定または作成します。指定できる VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。 |
| ステップ 7 | **private-vlan isolated** | VLAN を隔離 VLAN として指定します。 |
| ステップ 8 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 9 | **vlan** *vlan-id* | （任意）VLAN コンフィギュレーション モードを開始し、コミュニティ VLAN となる VLAN を指定または作成します。指定できる VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。 |
| ステップ 10 | **private-vlan community** | VLAN をコミュニティ VLAN として指定します。 |
| ステップ 11 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 12 | **vlan** *vlan-id* | ステップ 2 で指定されたプライマリ VLAN 用の 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 13 | **private-vlan association** [**add** \| **remove**] *secondary_vlan_list* | セカンダリ VLAN とプライマリ VLAN を対応付けます。 |
| ステップ 14 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 15 | **show vlan private-vlan** [**type**]<br>または<br>**show interfaces status** | 設定を確認します。 |
| ステップ 16 | **copy running-config startup config** | スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。プライベート VLAN 設定を保存するには、スイッチのスタートアップ コンフィギュレーション ファイルに VTP 透過モード設定とプライベート VLAN 設定を保存する必要があります。保存しないと、スイッチをリセットした場合、デフォルトの VTP サーバ モードとなり、プライベート VLAN をサポートしません。 |

セカンダリ VLAN とプライマリ VLAN を対応付ける場合、次の構文情報に注意してください。

- *secondary_vlan_list* パラメータにスペースを含めることはできません。カンマで区切られた項目を複数指定できます。各項目は単一のプライベート VLAN ID またはプライベート VLAN ID をハイフンでつないだ範囲です。
- *secondary_vlan_list* パラメータに複数のコミュニティ VLAN ID を含めることはできますが、隔離 VLAN ID は 1 つのみです。
- セカンダリ VLAN とプライマリ VLAN を対応付けるには、*secondary_vlan_list* を入力、または *secondary_vlan_list* 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 の間の関連性を削除するには、*secondary_vlan_list* を指定して **remove** キーワードを使用します。
- VLAN コンフィギュレーション モードを終了するまで、このコマンドは有効になりません。

次に、VLAN 20 をプライマリ VLAN、VLAN 501 を隔離 VLAN、VLAN 502 および 503 をコミュニティ VLAN として設定し、プライベート VLAN 内で対応付け、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
Switch(config)# show vlan private vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
20      501       isolated
20      502       community
20      503       community
20      504       non-operational
```

## プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN ホスト ポートとして設定し、これとプライマリおよびセカンダリ VLAN を対応付けるには、特権 EXEC モードで次の手順を実行します。

（注）　隔離およびコミュニティ VLAN は両方ともセカンダリ VLAN です。

| | コマンド | 説明 |
|---|---|---|
| ステップ 1 | **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 | **interface** *interface-id* | 設定するレイヤ 2 インターフェイスを指定して、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 | **switchport mode private-vlan host** | レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。 |
| ステップ 4 | **switchport private-vlan host-association** *primary_vlan_id secondary_vlan_id* | レイヤ 2 ポートとプライベート VLAN を対応付けます。 |

| | コマンド | 説明 |
|---|---|---|
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show interfaces** [*interface-id*] **switchport** | 設定を確認します。 |
| ステップ 7 | **copy running-config startup config** | （任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。 |

次に、インターフェイスをプライベート VLAN ホスト ポートとして設定し、これをプライベート VLAN ペアと対応付け、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 1/0/22
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 25
Switch(config-if)# end
Switch# show interfaces fastethernet 1/0/22 switchport
Name: Fa1/0/22
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)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 20 (VLAN0020) 25 (VLAN0025)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
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 private VLANs: none
Operational private-vlan:
20 (VLAN0020) 25 (VLAN0025)

(テキスト出力は省略)
```

## プライベート VLAN 混合ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN 混合ポートとして設定し、これをプライマリおよびセカンダリ VLAN にマッピングするには、特権 EXEC モードで次の手順を実行します。

（注）　隔離およびコミュニティ VLAN は両方ともセカンダリ VLAN です。

| | コマンド | 説明 |
|---|---|---|
| ステップ 1 | **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 | **interface** *interface-id* | 設定するレイヤ 2 インターフェイスを指定して、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 | **switchport mode private-vlan promiscuous** | レイヤ 2 ポートをプライベート VLAN 混合ポートとして設定します。 |

| | コマンド | 説明 |
|---|---|---|
| ステップ 4 | **switchport private-vlan mapping** *primary_vlan_id* {**add** \| **remove**} *secondary_vlan_list* | プライベート VLAN 混合ポートを、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 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show interfaces** [*interface-id*] **switchport** | 設定を確認します。 |
| ステップ 7 | **copy running-config startup config** | （任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。 |

レイヤ 2 インターフェイスをプライベート VLAN 混合ポートとして設定する場合、次の構文情報に注意してください。

- *secondary_vlan_list* パラメータにスペースを含めることはできません。カンマで区切られた項目を複数指定できます。各項目は単一のプライベート VLAN ID またはプライベート VLAN ID をハイフンでつないだ範囲です。
- セカンダリ VLAN をプライベート VLAN 混合ポートにマッピングするには、*secondary_vlan_list* を入力、または *secondary_vlan_list* を指定して **add** キーワードを使用します。
- セカンダリ VLAN とプライベート VLAN 混合ポートの間のマッピングをクリアするには、*secondary_vlan_list* を指定して **remove** キーワードを使用します。

次に、インターフェイスをプライベート VLAN 混合ポートとして設定し、これをプライベート VLAN にマッピングする例を示します。このインターフェイスはプライマリ VLAN 20 のメンバーであり、セカンダリ VLAN 501 ～ 503 はこのインターフェイスにマッピングされます。

```
Switch# configure terminal
Switch(config)# interface fastethernet 1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

プライマリおよびセカンダリ VLAN とスイッチ上のプライベート VLAN ポートを表示するには、**show vlan private-vlan** または **show interface status** 特権 EXEC コマンドを使用します。

## プライマリ VLAN レイヤ 3 VLAN インターフェイスへのセカンダリ VLAN のマッピング

プライベート VLAN を VLAN 間ルーティングに使用する場合、プライマリ VLAN に SVI を設定し、セカンダリ VLAN を SVI にマッピングします。

（注）　隔離およびコミュニティ VLAN は両方ともセカンダリ VLAN です。

プライマリ VLAN の SVI にセカンダリ VLAN をマッピングして、プライベート VLAN トラフィックのレイヤ 3 スイッチングを許可するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 説明 |
|---|---|---|
| ステップ 1 | **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 | **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、VLAN を SVI として設定します。指定できる VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。 |

| | コマンド | 説明 |
|---|---|---|
| ステップ 3 | **private-vlan mapping** [**add** \| **remove**] *secondary_vlan_list* | プライマリ VLAN のレイヤ 3 VLAN インターフェイスにセカンダリ VLAN をマッピングして、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを許可します。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show interface private-vlan mapping** | 設定を確認します。 |
| ステップ 6 | **copy running-config startup config** | （任意）スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。 |

（注）　**private-vlan mapping** インターフェイス コンフィギュレーション コマンドのみが、レイヤ 3 でスイッチングされるプライベート VLAN トラフィックに影響を及ぼします。

プライマリ VLAN のレイヤ 3 VLAN インターフェイスにセカンダリ VLAN をマッピングする場合、次の構文情報に注意してください。

- *secondary_vlan_list* パラメータにスペースを含めることはできません。カンマで区切られた項目を複数指定できます。各項目は単一のプライベート VLAN ID またはプライベート VLAN ID をハイフンでつないだ範囲です。
- 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、または *secondary_vlan_list* 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 の間のマッピングをクリアするには、*secondary_vlan_list* を指定して **remove** キーワードを使用します。

次に、VLAN 501 および 502 のインターフェイスをプライマリ VLAN 10 にマッピングする例を示します。VLAN 10 ではプライベート VLAN 501 ～ 502 のセカンダリ VLAN 入力トラフィックのルーティングが許可されます。

```
Switch# configure terminal
Switch(config)# interface vlan 10
Switch(config-if)# private-vlan mapping 501-502
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan10    501            isolated
vlan10    502            community
```

# プライベート VLAN のモニタ

表 14-1 に、プライベート VLAN アクティビティ モニタ用の特権 EXEC コマンドを示します。

**表 14-1　プライベート VLAN モニタ コマンド**

| コマンド | 説明 |
|---|---|
| **show interfaces status** | インターフェイスが所属する VLAN を含めたインターフェイスのステータスを表示します。 |
| **show vlan private-vlan** [**type**] | スイッチのプライベート VLAN 情報を表示します。 |
| **show interface switchport** | インターフェイス上のプライベート VLAN 設定を表示します。 |
| **show interface private-vlan mapping** | VLAN SVI のプライベート VLAN マッピング情報を表示します。 |

次に、**show vlan private-vlan** コマンドの出力例を示します。

```
Switch(config)# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Fa1/0/1, Gi1/0/1, Gi1/0/2
10      502       community         Fa1/0/11, Gi1/0/1, Gi1/0/4
10      503       non-operational
```