CHAPTER 16

プライベート VLAN の設定

この章では、Catalyst 3750 スイッチにプライベート VLAN（仮想 LAN）を設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

（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 VTP トランスペアレント モードである必要があります。第 14 章「VTP の設定」を参照してください。

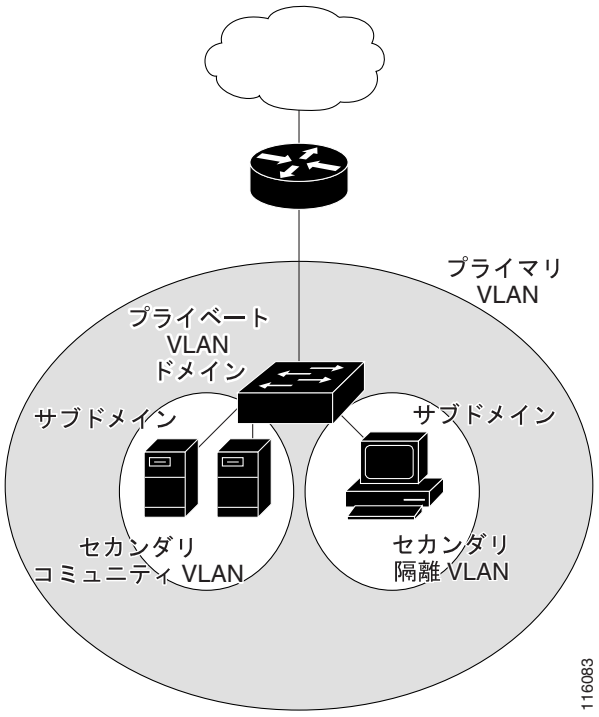
プライベート VLAN の概要

プライベート VLAN 機能は、VLAN を使用中にサービス プロバイダーが直面する次の 2 つ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 個のアクティブ VLAN をサポートします。サービス プロバイダーがお客様ごとに 1 つの VLAN を割り当てる場合、この数字ではサービス プロバイダーがサポートできるお客様の数を制限することになります。
- 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。これにより、未使用の IP アドレスを消費し、IP アドレス管理問題が発生します。

プライベート VLAN を使用することによって、スケーラビリティの問題を対処します。また、サービス プロバイダーに対して IP アドレス管理の利点を提供し、お客様に対するレイヤ 2 のセキュリティを確実にします。プライベート VLAN 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、次の VLAN ペアにより表示されます。*primary* VLAN および *secondary* VLAN です。プライベート VLAN には複数の VLAN ペアがあり、ペア 1 つあたり 1 つのサブドメインを構成します。プライベート VLAN 内の VLAN ペアすべては、同じプライマリ VLAN を共有します。セカンダリ VLAN ID は、サブドメインを相互に区別します。図 16-1 を参照してください。

図 16-1　プライベート VLAN ドメイン



セカンダリ VLAN には次があります。

- 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 内のポートは相互に通信できますが、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 内の各ポートをレイヤ 2 レベルで分離します。プライベート VLAN は、次のアクセス ポート タイプのいずれかです。

- 混合 — 混合ポートはプライマリ VLAN に属し、コミュニティおよび隔離ホスト ポート（プライマリ VLAN に対応付けられるセカンダリ VLAN に所属）を含めた、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 に所属するホスト ポートです。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 を完全に分離します。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 に所属するホスト 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、正規の VLAN、またプライマリ、隔離、コミュニティ VLAN からトラフィックを搬送します。

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 つのみ存在します。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、単一方向トラフィック ダウンストリームを混合ポートから（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搬送します。
- 隔離 VLAN — プライベート VLAN には隔離 VLAN が 1 つのみ存在します。隔離 VLAN は、単一方向トラフィック アップストリームをホストから混合ポートおよびゲートウェイに向けて搬送するセカンダリ VLAN です。
- コミュニティ VLAN — コミュニティ VLAN は、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 ポートに搬送するセカンダリ VLAN です。複数のコミュニティ VLAN をプライベート VLAN に設定できます。

混合ポートでは、プライマリ VLAN を 1 つのみ、隔離 VLAN を 1 つ、コミュニティ VLAN を複数処理できます。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には、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、個々のプライベート VLAN および対応する IP サブネットが、エンド ステーションの個々の、または共通するグループにそれぞれ割り当てられます。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。

次の方法で、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、この設定ではサーバの間のレイヤ 2 通信を実施しません。
- 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。

プライマリ、隔離、コミュニティ VLAN を、プライベート VLAN をサポートする他のデバイスにトランキングすることで、複数のデバイス上にプライベート VLAN を拡張できます。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 の他の目的による使用を避けるには、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）上でプライベート VLAN を設定します。

プライベート VLAN を使用した IP アドレス指定方式

個別の VLAN を各カスタマーに割り当てると、効率の悪い IP アドレス指定方式となります。

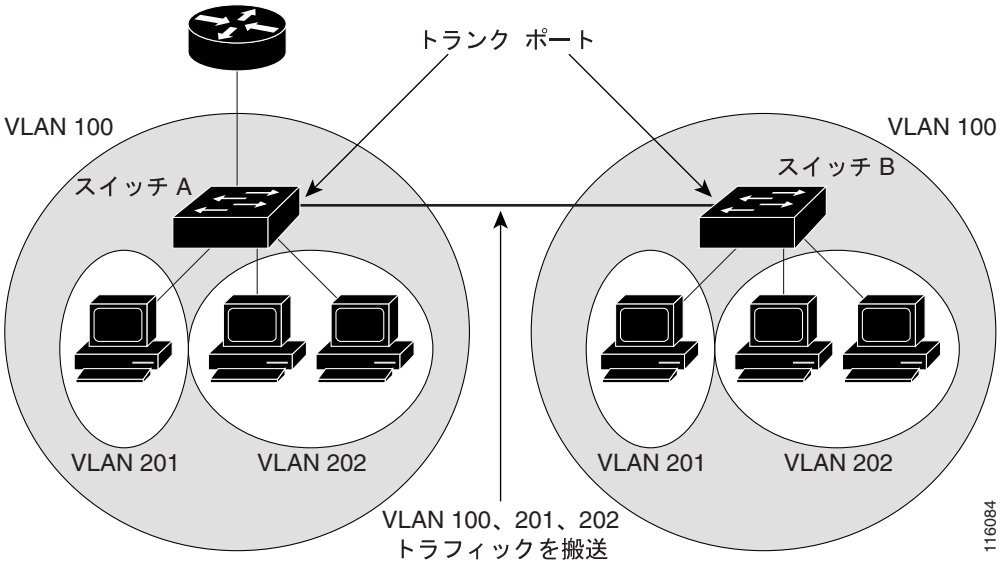
- アドレス ブロックをカスタマー VLAN に割り当てると、未使用の IP アドレスを作成できます。
- VLAN 内のデバイス数が増えた場合、割り当てられたアドレス数がこのデバイス数に対応するだけの十分な大きさでない可能性があります。

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。Dynamic Host Configuration Protocol（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 IP アドレスを割り当てます。後続の IP アドレスは、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が、同じプライマリ VLAN 内です。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利用できるアドレスにデバイスを割り当てます。

複数のスイッチにまたがるプライベート VLAN

正規 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 を近接スイッチに搬送します。トランク ポートはプライベート VLAN を他の VLAN として処理します。複数のスイッチにまたがるプライベート VLAN の機能は、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させないことです。詳細については、図 16-2 を参照してください。

図 16-2　スイッチ上のプライベート 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

VLAN Trunk Protocol（VTP;VLAN トランク プロトコル）がプライベート 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 の関連性を設定しない場合、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、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 8 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 は他の機能と特別に連動します。それについての説明は、次のとおりです。

- プライベート VLAN、およびユニキャスト、ブロードキャスト、マルチキャスト トラフィック（p.16-5）
- プライベート VLAN および SVI（p.16-6）
- プライベート VLAN およびスイッチ スタック（p.16-6）

「プライベート VLAN 設定時の注意事項」の下にある「セカンダリおよびプライマリ VLAN の設定」（p.16-8）も参照してください。

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

正規 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ので、VLAN のメンバーはレイヤ 2 レベルで相互に通信できます。

正規 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 境界を超えて、および単一のコミュニティ 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、同じ隔離 VLAN 内のポート、または別のセカンダリ VLAN 内のポート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 Intertface（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 を介してのみプライベート VLAN と通信します。レイヤ 3 の 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 を持つ VLAN をセカンダリ VLAN として設定しようとしても、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、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 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 およびスイッチ スタック

プライベート VLAN はスイッチ スタック内で動作することができ、プライベート VLAN ポートはさまざまなスタック メンバーに常駐できます。ただし、スイッチ スタックを変更するとプライベート VLAN 動作に影響を与えます。

- スタックにプライベート VLAN 混合ポートのみが含まれ、このポートを含めたスタック メンバーがスタックから削除された場合、プライベート VLAN のホスト ポートとプライベート VLAN 外との接続が不能になります。
- スタック内にプライベート VLAN 混合ポートが 1 つのみあるスタック マスターに障害が発生した、またはスタックを残し、新しいスタック マスターが選択された場合、古いスタック マスターに混合ポートがあるプライベート VLAN のホスト ポートとプライベート VLAN 外との接続が不能になります。
- 2 つのスタックが統合した場合、権利を獲得したスタックのプライベート VLAN は影響を受けませんが、スイッチを再起動したときに、権利を獲得しなかったスイッチのプライベート VLAN 設定が失われます。

スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

プライベート VLAN の設定

ここでは、次の設定について説明します。

プライベート VLAN 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 モードをトランスペアレントに設定します。

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.16-11）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　分離インターフェイスまたはコミュニティ ホスト ポートを設定し、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.16-12）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 / セカンダリ VLAN 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.16-13）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.16-14）を参照してください。

ステップ 6　プロセス 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 の設定時は、次の注意事項に従ってください。

- VTP をトランスペアレント 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 14 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 モードにプライベート 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.13-8）を参照してください。
- プライベート VLAN を設定したあと、VTP トランスペアレント 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** イネーブル EXEC コマンドを使用します。そうしないと、スイッチがリセットした場合、スイッチはデフォルトで VTP サーバ モードが設定されます。このモードではプライベート VLAN をサポートしません。
- VTP はプライベート VLAN 設定を伝播しません。プライベート VLAN ポートを設定したいデバイスそれぞれで、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 があります。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 つあるだけです。
- 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 つだけです。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、プライマリ VLAN がすでに設定されていると設定は有効になりません。
- プライベート VLAN ポート上で IP 送信元ガードをイネーブルにする場合、プライマリ VLAN 上で 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 のトラフィックを搬送しないデバイスで、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。
- 異なる Quality of Service（QoS; サービス品質）設定をプライマリ、隔離、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、デフォルトでは固定 Address Resolution Protocol（ARP）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 エントリは固定 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 ポート固定 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、表示および確認することを推奨します。

異なる MAC（メディア アクセス制御）アドレスがあり、同じ IP アドレスを持つ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 ポート固定 ARP エントリは期限切れにならないので、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 で設定することを推奨します。
- フレームがプライベート VLAN 内でレイヤ 2 転送された場合、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のアップストリーム方向に移動するフレームの場合、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 ポートへのダウンストリーム方向に移動するフレームの場合、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 用に特定の 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。
- ルータ Access Control List（ACL; アクセス制御リスト）をプライマリ VLAN 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 でホストを切り離しますが、ホストはレイヤ 3 で相互に通信できます。
- 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、隔離、コミュニティ VLAN で VLAN-based SPAN（VSPAN）を使用するか、または 1 つの VLAN だけで SPAN を使用します。

プライベート VLAN ポートの設定

プライベート VLAN ポートの設定時は、次の注意事項に従ってください。

- プライマリ、隔離、またはコミュニティ VLAN 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 設定に含まれている場合、プライマリ、隔離、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; ポート集約プロトコル）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 設定に含まれている場合、EtherChannel 設定はすべて非アクティブです。
- 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 Bridge Protocol Data Unit（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 20 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 PortFast が設定されたレイヤ 2 LAN ポートすべてに BPDU ガード機能を適用します。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。

- ネットワーク 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）　一部の設定はエラー メッセージなしで受け入れられ、コマンドに影響しません。

- 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。
- Internet Group Management Protocol（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 スタックがサポートするプライベート VLAN ドメインは、20 個だけです。
- Remote SPAN（RSPAN; リモート SPAN）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。
- 次の別の機能用に設定されたインターフェイスで、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 ポートはセキュア ポートになれません。また、保護ポートとして設定してはいけません。
- 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。ただし、プライベート VLAN ポート上で、802.1x とポート セキュリティ、音声 VLAN、またはユーザ単位 ACL を設定しないでください。
- プライベート VLAN ホストまたは混合ポートは、SPAN 宛先ポートになれません。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 の混合ポートでスタティック MAC アドレスを設定する場合、同じスタティック MAC アドレスを対応付けられたセカンダリ 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 ポートでスタティック MAC アドレスを設定する場合、同じスタティック MAC アドレスを対応付けられたプライマリ 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 の 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、イネーブル 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 モードをトランスペアレントに設定します（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 として設定します。
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 として設定します。
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 用に、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**	イネーブル EXEC モードに戻ります。
ステップ 15	**show vlan private-vlan** [**type**] または **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 トランスペアレント 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。そうしないと、スイッチがリセットした場合、スイッチはデフォルトで VTP サーバ モードが設定されます。このモードではプライベート 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は使用できません。カンマで区切られた項目を複数、使用できます。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を示します。
- *secondary_vlan_list* パラメータに複数のコミュニティ VLAN ID は使用できません。1 つの隔離 VLAN ID のみ使用できます。
- 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 間のアソシエーションを削除するには、*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、コマンドは有効になりません。

次に、VLAN 20 をプライマリ VLAN として、VLAN 501 を隔離 VLAN として、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、インターフェイスをプライマリおよびセカンダリ VLAN と対応付けるには、イネーブル EXEC モードで次の手順を実行します。

（注）　隔離 VLAN 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*	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、設定するレイヤ 2 インターフェイスを指定します。

	コマンド	説明
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。
ステップ 5	**end**	イネーブル 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 fastethernet1/0/22
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 fastethernet1/0/22 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、イネーブル EXEC モードで次の手順を実行します。

（注）　隔離 VLAN 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*	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、設定するレイヤ 2 インターフェイスを指定します。

	コマンド	説明
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。
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**	イネーブル 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は使用できません。カンマで区切られた項目を複数、使用できます。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 混合ポート間のマッピングを削除するには、*secondary_vlan_list* を指定して **remove** キーワードを使用します。

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 はこのメンバーにマッピングされます。

```
Switch# configure terminal
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

スイッチ上のプライマリおよびセカンダリ VLAN と、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** イネーブル 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 の 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 VLAN 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 をスイッチングさせるには、イネーブル 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。
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、レイヤ 3 のプライベート VLAN 入力トラフィックのスイッチングを許可します。
ステップ 4	**end**	イネーブル 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 が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は使用できません。カンマで区切られた項目を複数、使用できます。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を示します。
- 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。

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。これにより、プライベート VLAN 501 ～ 502 からセカンダリ 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 16-1 に、プライベート VLAN アクティビティ モニタ用のイネーブル EXEC コマンドを示します。

表 16-1　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 スタックのプライベート 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** コマンドからの出力例を示します。

```
Switch(config)# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Fa2/0/1, Gi3/0/1, Gi3/0/2
10      502       community         Fa2/0/11, Gi3/0/1, Gi3/0/4
10      503       non-operational
```