CHAPTER 19

プライベート VLAN の設定

この章では、IE 3000 スイッチにプライベート VLAN を設定する手順について説明します。プライベート VLAN は、IP サービス イメージが稼動しているスイッチでだけサポートされます。

（注） この章で使用してい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。

- 「プライベート VLAN の概要」（P.19-1）
- 「プライベート VLAN の設定」（P.19-6）
- 「プライベート VLAN のモニタ」（P.19-15）

（注） プライベート VLAN を設定する場合は、スイッチが VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）トランスペアレント モードになっている必要があります。第 17 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 機能では、サービス プロバイダーが VLAN を使用する際に直面する 2 つの問題に対処します。

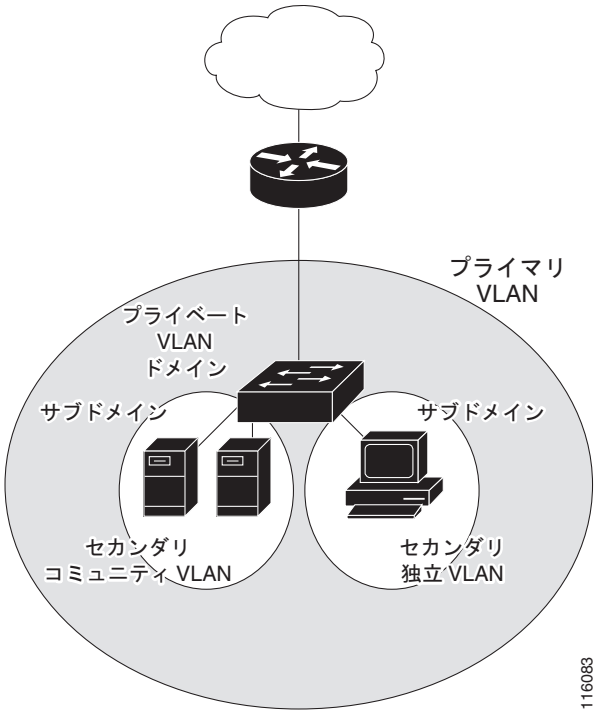
- スケーラビリティ：スイッチは最大 1005 個のアクティブ VLAN をサポートします。サービス プロバイダーがカスタマーごとに 1 つの VLAN を割り当てる場合、サービス プロバイダーがサポートできるカスタマー数は制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネット アドレス空間またはアドレス ブロックを割り当てます。これにより未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が生じます。

プライベート VLAN を使用することにより、スケーラビリティの問題が対処され、サービス プロバイダーにとっては IP アドレスの管理が便利になり、カスタマーにはレイヤ 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 ドメインがサブドメインに分割され、複数の VLAN ペア（サブドメインごとに 1 つのペア）を設定できます。サブドメインは、*プライマリ* VLAN と *セカンダリ* VLAN で表されます。

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 では、あるサブドメインを他のサブドメインと区別します。図 19-1 を参照してください。

図 19-1　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、相互に通信できますが、レイヤ 2 レベルの他のコミュニティ上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 内のポート間をレイヤ 2 で分離します。プライベート VLAN ポートには、次の 3 種類のアクセス ポートがあります。

- プロミスキャス：プロミスキャス ポートはプライマリ VLAN に属し、プライマリ VLAN に関連付けられているセカンダリ VLAN に属するコミュニティ ホスト ポートおよび独立ホスト 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。
- 独立：独立ポートは、独立セカンダリ VLAN に属するホスト ポートです。このポートは、プロミスキャス 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、プロミスキャス 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、プロミスキャス ポートにだけ転送されます。
- 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プロミスキャス 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 内の独立ポートからレイヤ 2 で分離されています。

（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。

プライマリ VLAN およびセカンダリ VLAN には、次のような特性があります。

- プライマリ VLAN：プライベート VLAN には、プライマリ VLAN 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、単一方向のトラフィックのダウンストリームをプロミスキャス ポートから（独立およびコミュニティ）ホスト ポートおよび他のプロミスキャス ポートに伝送します。
- 独立 VLAN：プライベート VLAN には、独立 VLAN を 1 つだけ設定できます。独立 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へ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、アップストリーム トラフィックをコミュニティ ポートからプロミスキャス 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。1 つのプライベート VLAN 内に複数のコミュニティ VLAN を設定できます。

プロミスキャス ポートでは、1 つのプライマリ VLAN、1 つの独立 VLAN、および複数のコミュニティ VLAN だけを処理できます。レイヤ 3 ゲートウェイは、通常プロミスキャス ポート経由でスイッチに接続されます。プロミスキャス ポートを使用すると、さまざまな装置をアクセス ポイントとしてプライベート VLAN に接続できます。たとえば、プロミスキャス ポートを使用すると、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できます。

スイッチング環境では、個々のエンド ステーション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、関連付けられている IP サブネットを割り当てることができます。エンド ステーションがプライベート VLAN の外部と通信するには、デフォルト ゲートウェイだけと通信する必要があります。

プライベート VLAN を使用すると、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。

- エンド ステーションに接続された特定のインターフェイスを独立ポートとして設定すると、レイヤ 2 での通信が禁止されます。たとえば、エンド ステーションがサーバの場合は、サーバ間のレイヤ 2 通信が禁止されます。
- デフォルト ゲートウェイおよび選択されたエンド ステーション（たとえば、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プロミスキャス ポートとして設定すると、すべてのエンド ステーションがデフォルト ゲートウェイにアクセスできます。

複数の装置にわたるようにプライベート VLAN を拡張するには、プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN を、プライベート VLAN をサポートする他の装置にトランキングします。使用するプライベート VLAN の設定のセキュリティを確保して、プライベート VLAN 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、プライベート VLAN ポートがない装置を含めて、すべての中間装置でプライベート VLAN を設定します。

プライベート VLAN による IP アドレッシング方式

カスタマーごとに個別の VLAN を割り当てると、次のように IP アドレッシング方式が非効率的になります。

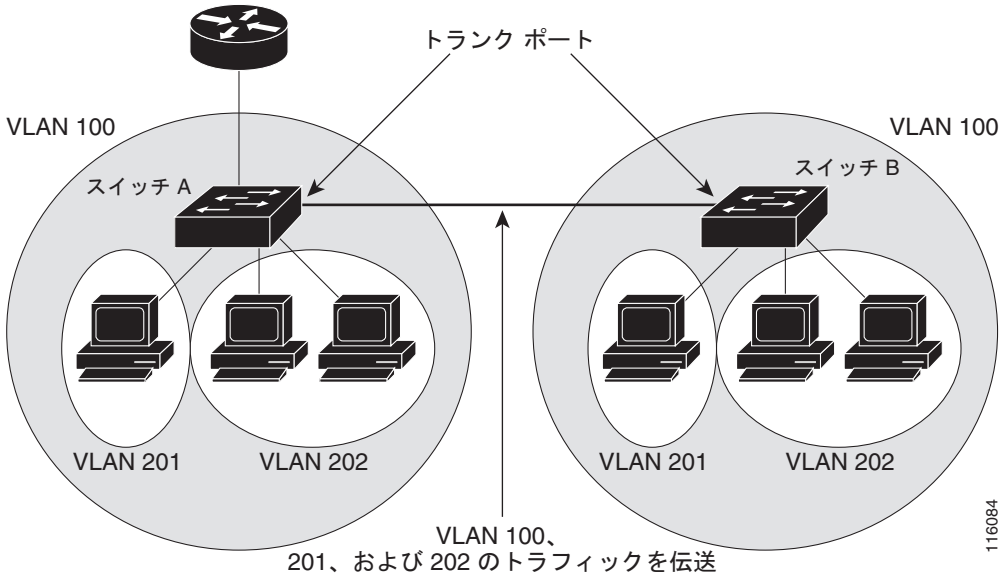
- カスタマー VLAN に アドレス ブロックを割り当てると、未使用の IP アドレスが生じます。
- VLAN 内の装置数が増加した場合、割り当てられるアドレス数はそれに対応できるほど多くはない場合があります。

これらの問題は、プライベート VLAN を使用することで軽減されます。この場合、プライベート VLAN 内のすべてのメンバーは、プライマリ VLAN に割り当てられる共通のアドレス空間を共有します。ホストはセカンダリ VLAN に接続され、Dynamic Host Configuration Protocol（DHCP）サーバが 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。同じプライマリ VLAN 内の別のセカンダリ VLAN 内のカスタマー装置に後続の IP アドレスを割り当てられます。新しい装置が追加された場合、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装置に割り当てます。

複数のスイッチにまたがるプライベート VLAN

通常の VLAN 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 をネイバー 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 19-2 を参照してください。

図 19-2　　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 ネットワークのすべてのスイッチではプライベート 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 VLAN とセカンダリ VLAN のアソシエーションを設定しない場合、これらのスイッチ内のレイヤ 2 データベースは結合されません。これより、これらのスイッチ上のプライベート VLAN トラフィックが不要にフラッディングする可能性があります。

（注） スイッチにプライベート VLAN を設定するときには、ユニキャスト ルートとレイヤ 2 エントリとの間のシステム リソースのバランスを取るために、必ずデフォルトの Switch Database Management（SDM）テンプレートを使用してください。別の SDM テンプレートが設定されている場合は、**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 10 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 の他の機能との相互作用

プライベート VLAN には、次の各項で説明するように、他の機能との特殊な相互作用があります。

- 「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」（P.19-5）
- 「プライベート VLAN および SVI」（P.19-5）

「プライベート VLAN 設定時の注意事項」の「セカンダリ VLAN およびプライマリ VLAN の設定」（P.19-7）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、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 内の装置はレイヤ 2 レベルで相互に通信できますが、異なる VLAN のインターフェイスに接続されている装置とは、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 では、プロミスキャス ポートはプライマリ VLAN のメンバーで、ホスト ポートはセカンダリ VLAN に属しています。セカンダリ VLAN はプライマリ VLAN に関連付けられているため、これらの VLAN のメンバーはレイヤ 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 内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転送は、ブロードキャストを送信するポートにより異なります。

- 独立ポートは、ブロードキャストをプロミスキャス ポートまたはトランク ポートにだけ送信します。
- コミュニティ ポートは、ブロードキャストをすべてのプロミスキャス ポート、トランク ポート、および同じコミュニティ VLAN 内のポートに送信します。
- プロミスキャス 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（他のプロミスキャス 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）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 境界を越えて、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、同じ独立 VLAN 内のポート間または異なるセカンダリ VLAN 内のポート間で転送されません。

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 インターフェイスを表します。レイヤ 3 装置は、セカンダリ VLAN ではなく、プライマリ VLAN を介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。

- アクティブな SVI が設定された VLAN をセカンダリ VLAN として設定しようとする場合、SVI をディセーブルにしなければ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 上に SVI を作成しようとした場合、セカンダリ VLAN がレイヤ 3 ですでにマッピングされていると、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 に関連付けられていて、マッピングされている場合、プライマリ VLAN 上のすべての設定はセカンダリ 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 アドレスとなります。

プライベート VLAN の設定

ここでは、次の設定情報について説明します。

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 VLAN およびセカンダリ VLAN を作成して、これらを関連付けします。「VLAN の設定およびプライベート VLAN への関連付け」（P.19-10）を参照してください。

（注）　VLAN がまだ作成されていない場合は、プライベート VLAN の設定プロセスを実行して、VLAN を作成します。

ステップ 3　インターフェイスを独立ポートまたはコミュニティ ホスト ポートに設定して、ホスト ポートに VLAN メンバーシップを割り当てます。「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.19-12）を参照してください。

ステップ 4　インターフェイスをプロミスキャス ポートに設定して、プロミスキャス ポートをプライマリ VLAN およびセカンダリ VLAN のペアにマッピングします。「プライベート VLAN プロミスキャス ポートとしてのレイヤ 2 インターフェイスの設定」（P.19-13）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している場合は、プライマリ SVI を設定して、セカンダリ VLAN をプライマリにマッピングします。「セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング」（P.19-14）を参照してください。

ステップ 6　プライベート VLAN の設定を確認します。

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 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 VLAN およびプライマリ VLAN の設定

プライベート VLAN の設定時には、次の注意事項に従ってください。

- スイッチで VTP バージョン 1 または 2 が稼動している場合は、VTP をトランスペアレント モードに設定する必要があります。プライベート VLAN を設定したあとで、VTP モードをクライアントまたはサーバに変更できません。VTP の詳細については、第 17 章「VTP の設定」を参照してください。VTP バージョン 3 では、すべてのモードでプライベート VLAN がサポートされます。
- VTP バージョン 1 または 2 では、プライベート VLAN を設定したあと、**copy running-config startup config** 特権 EXEC コマンドを使用して、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 スタートアップ コンフィギュレーション ファイルに保存します。そうしないと、スイッチをリセットしたときにデフォルトの VTP サーバ モードになり、プライベート VLAN がサポートされなくなります。VTP バージョン 3 では、プライベート VLAN がサポートされます。
- VTP バージョン 1 およびバージョン 2 では、プライベート VLAN 設定が伝播されません。装置で VTP バージョン 3 が稼動していない場合は、プライベート VLAN ポートを使用する装置ごとに、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 VLAN 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 に属することができます。
- プライマリ VLAN には、1 つの隔離 VLAN および複数のコミュニティ VLAN を関連付けることができます。独立 VLAN またはコミュニティ VLAN には、1 つのプライマリ VLAN だけを関連付けることができます。
- プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行されるのは 1 つの Spanning Tree Protocol（STP; スパニング ツリー プロトコル）インスタンスだけです。セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の STP パラメータがセカンダリ VLAN に伝播されます。
- DHCP スヌーピングはプライベート VLAN 上で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場合、セカンダリ VLAN に伝播されます。セカンダリ VLAN で DHCP を設定する際、プライマリ VLAN がすでに設定されている場合は、設定が有効になりません。
- 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 でトラフィックを伝送しない装置のトランクから、プライベート VLAN をプルーニングすることを推奨します。
- 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; サービス品質）を適用できます。
- スティッキ ARP
  - スティッキ ARP エントリは、SVI およびレイヤ 3 インターフェイスで学習されるエントリです。これらのエントリは、期限切れになりません。

  - **ip sticky-arp** グローバル コンフィギュレーション コマンドは、プライベート VLAN に属している SVI でだけサポートされます。
  - **ip sticky-arp** インターフェイス コンフィギュレーション コマンドは、次のものでだけサポートされます。

    レイヤ 3 インターフェイス

    通常の VLAN に属している SVI

    プライベート VLAN に属している SVI

  ip sticky-arp *グローバル* コンフィギュレーション コマンドと **ip sticky-arp** *インターフェイス* コンフィギュレーション コマンドの使用の詳細については、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。

- プライマリ VLAN およびセカンダリ VLAN では VLAN マップを設定できます（「VLAN マップの設定」（P.38-31）を参照）。ただし、プライベート VLAN のプライマリ VLAN とセカンダリ VLAN には、同じ VLAN マップを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 転送される場合、入力側と出力側で同じ VLAN マップが適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップは入力側で適用されます。
  - ホスト ポートからプロミスキャス ポートへの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。
  - プロミスキャス ポートからホスト ポートへの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、プライマリ VLAN とセカンダリ VLAN の両方に VLAN マップを適用する必要があります。
- ルータ ACL はプライマリ VLAN SVI にだけ適用できます。ACL はプライマリ VLAN およびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。
- プライベート VLAN がレイヤ 2 でホストを独立していても、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 では、次の 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）を使用したり、単一の VLAN 上で SPAN を使用したりして、出力トラフィックまたは入力トラフィックを個別にモニタすることができます。

プライベート VLAN ポートの設定

プライベート VLAN ポートの設定時には、次の注意事項に従ってください。

- 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、プライベート VLAN コンフィギュレーション コマンドだけを使用します。プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN として設定する VLAN に割り当てられているレイヤ 2 アクセス ポートは、この VLAN がプライベート VLAN の設定に含まれている場合、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と、ポートの EtherChannel 設定が非アクティブになります。

- 設定ミスによって STP ループが発生しないようにするため、および STP コンバージェンスを高速化するためには独立ホスト ポートおよびコミュニティ ホスト ポート上で 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 23 章「オプションのスパニング ツリー機能の設定」を参照）。STP をイネーブルに設定すると、STP によってすべての PortFast 設定済みレイヤ 2 LAN ポートに BPDU ガード機能が適用されます。プロミスキャス ポートでは、PortFast および BPDU をイネーブルにしないでください。
- プライベート VLAN の設定で使用される VLAN を削除すると、この VLAN に関連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。
- プライベート VLAN ポートは、ネットワーク装置をトランク接続し、トランクからプライマリ VLAN およびセカンダリ VLAN が削除されていない限りさまざまなネットワーク装置上で使用できます。

他の機能との制限事項

プライベート VLAN を設定する場合、他の機能との間で次のような制限があることに留意してください。

（注）　場合によっては、エラー メッセージなしで設定が受け入れられますが、コマンドは無効になります。

- プライベート VLAN が設定されたスイッチにフォールバック ブリッジングを設定しないでください。
- スイッチで IGMP スヌーピングがイネーブルになっている場合（デフォルト）、スイッチでサポートされるプライベート VLAN ドメインは 20 個までです。
- Remote SPAN（RSPAN; リモート SPAN）VLAN をプライベート VLAN のプライマリ VLAN 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 30 章「SPAN および RSPAN の設定」を参照してください。
- 次のその他の機能が設定されているインターフェイスに、プライベート VLAN ポート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
  - ダイナミック トランキング プロトコル（DTP）
  - ポート集約プロトコル（PagP）
  - Link Aggregation Control Protocol（LACP）
  - マルチキャスト VLAN レジストレーション（MVR）
  - 音声 VLAN
  - Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）
- プライベート VLAN ポートはセキュア ポートにはなれないので、保護ポートとして設定はできません。
- プライベート VLAN ポートに IEEE 802.1x ポートベース認証を設定できますが、IEEE 802.1x をポート セキュリティ、音声 VLAN、またはユーザ単位 ACL と一緒にプライベート VLAN ポートに設定しないでください。
- プライベート VLAN ホストまたはプロミスキャス ポートは、SPAN 宛先ポートにはできません。SPAN 宛先ポートをプライベート VLAN ポートとして設定した場合、ポートは非アクティブとなります。

- プライマリ VLAN のプロミスキャス ポート上でスタティック MAC アドレスを設定する場合は、すべての関連するセカンダリ VLAN にこれと同じスタティック アドレスを追加する必要があります。セカンダリ VLAN のホスト ポート上でスタティック MAC アドレスを設定する場合は、関連するプライマリ VLAN にこれと同じスタティック MAC アドレスを追加する必要があります。プライベート VLAN ポートからスタティック MAC アドレスを削除した場合は、設定されている MAC アドレスのすべてのインスタンスをプライベート VLAN から削除する必要があります。

（注）　プライベート VLAN の 1 つの VLAN で学習されたダイナミック MAC アドレスは、関連する VLAN に複製されます。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 に複製されます。元のダイナミック MAC アドレスが削除されるか、期限切れになった場合は、複製されたアドレスは MAC アドレス テーブルから削除されます。

- レイヤ 3 VLAN インターフェイスはプライマリ VLAN にだけ設定してください。

VLAN の設定およびプライベート VLAN への関連付け

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実行します。

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

	コマンド	目的
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 モードを開始して、プライマリ VLAN となる VLAN を指定または作成します。VLAN ID 範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 4	**private-vlan primary**	VLAN をプライマリ VLAN として指定します。
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 モードを開始して、独立 VLAN となる VLAN を指定または作成します。VLAN ID 範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 7	**private-vlan isolated**	VLAN を独立 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 モードを開始して、コミュニティ VLAN となる VLAN を指定または作成します。VLAN ID 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 で指定したプライマリ 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 13	**private-vlan association** [**add** | **remove**] *secondary_vlan_list*	セカンダリ VLAN をプライマリ VLAN に関連付けます。
ステップ 14	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
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 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 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、スイッチをリセットしたときにデフォルトの VTP サーバ モードになり、プライベート VLAN がサポートされなくなります。

セカンダリ VLAN をプライマリ VLAN と関連付ける際には、次の構文情報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 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が、独立 VLAN ID は 1 つしか含めることができません。
- セカンダリ VLAN をプライマリ VLAN に関連付けるには、*secondary_vlan_list* を入力するか、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 の関連付けを消去するには、*secondary_vlan_list* を指定して **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 モードを終了するまで有効になりません。

次に、VLAN 20 をプライマリ VLAN に、VLAN 501 を独立 VLAN に、VLAN 502 および 503 をコミュニティ VLAN に設定し、それらの VLAN をプライベート VLAN に関連付けて、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、それをプライマリ VLAN およびセカンダリ VLAN に関連付けるには、特権 EXEC モードで次の手順を実行します。

（注）　独立 VLAN およびコミュニティ VLAN はセカンダリ VLAN です。

	コマンド	目的
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	**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 ポートをプライベート VLAN に関連付けます。
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。

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、それをプライマリ VLAN のペアに関連付けて、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigatibethernet1/2
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 gigabitethernet1/2 switchport
Name: Gi1/2
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)

<output truncated>
```

プライベート VLAN プロミスキャス 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 プロミスキャス ポートとして設定し、それをプライマリ VLAN 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）　独立 VLAN およびコミュニティ VLAN はセカンダリ VLAN です。

	コマンド	目的
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	**switchport mode private-vlan promiscuous**	レイヤ 2 ポートをプライベート VLAN プロミスキャス 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 プロミスキャス 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 プロミスキャス ポートとして設定する際には、次の構文情報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 です。
- セカンダリ VLAN をプライベート VLAN プロミスキャス 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* 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 プロミスキャス ポートの間のマッピングを消去するには、*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 プロミスキャス ポートとして設定し、それをプライベート VLAN にマッピングする例を示します。インターフェイスは、プライマリ VLAN 20 のメンバーで、セカンダリ VLAN 501 ～ 503 がマッピングされます。

```
Switch# configure terminal
Switch(config)# interface gigatibethernet1/2
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 VLAN 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。

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

プライベート VLAN が VLAN 間ルーティングに使用される場合、SVI をプライマリ VLAN に設定して、セカンダリ VLAN を SVI にマッピングできます。

（注）　独立 VLAN およびコミュニティ VLAN はセカンダリ VLAN です。

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

	コマンド	目的
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。VLAN ID 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*	セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングして、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にします。
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 コマンドは、レイヤ 3 スイッチングされるプライベート VLAN トラフィックにだけ作用します。

セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングする際には、次の構文情報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 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* 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消去するには、*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。プライマリ VLAN 10 では、プライベート VLAN 501 から 502 へのセカンダリ 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 19-1　プライベート VLAN のモニタ コマンド

コマンド	目的
show interfaces status	所属する VLAN を含む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 マッピングに関する情報を表示します。

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           Gi1/1, Gi1/3
10      502       community          Gi1/5, Gi1/4

10      503       non-operational
```