CHAPTER 13

プライベート VLAN の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチにプライベート VLAN を設定する方法について説明します。

（注） この章で使用す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。

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 を使用している場合に直面する 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 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 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。

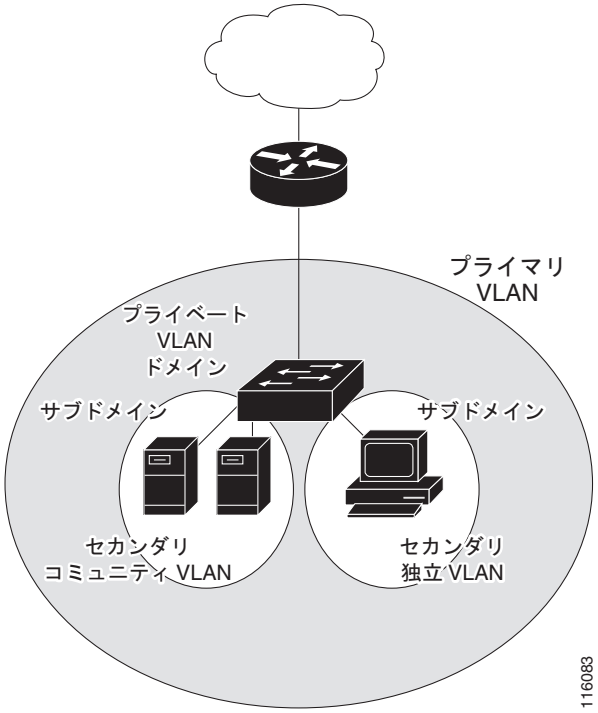
プライベート VLAN を使用することでスケーラビリティの問題に対処することができ、サービス プロバイダーにとっては IP アドレス管理上の利点が得られ、カスタマーに対してはレイヤ 2 セキュリティを提供できます。

ここでは、プライベート VLAN の機能について説明します。

プライベート VLAN およびプライベート VLAN ポートのタイプ

プライベート VLAN では、通常の VLAN ドメインはサブドメインに分割されます。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 のペアで表されます。プライベート VLAN では複数の VLAN ペアを設定でき、各サブドメインにつき 1 ペアとなります。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 13-1 を参照してください。

図 13-1　　プライベート VLAN ドメイン



セカンダリ VLAN には 2 種類あります。

- 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 レベルの他のコミュニティ内のポートとは通信できません。コミュニティ VLAN には、User Network Interface（UNI; ユーザネットワーク インターフェイス）と Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）を最大 8 つ組み合せて指定できます。

プライベート VLAN では、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、次のタイプがあります。

- プロミスキャス：プロミスキャス ポートは、プライベート VLAN に属し、プライマリ VLAN と関連しているセカンダリ VLAN に属するコミュニティ ポートや独立ホスト 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。

（注） プロミスキャス ポートは、Network Node Interface（NNI; ネットワーク ノード インターフェイス）とします。UNI または ENI は、プロミスキャス ポートとしては設定できません。

- 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。これは、プロミスキャス 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 では、プロミスキャス ポートからのトラフィックを除く、独立ポートへのすべてのトラフィックをブロックします。独立ポートで受信されるトラフィックは、プロミスキャス ポートへだけ転送されます。
- 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 にある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 内の独立ポートとレイヤ 2 で分離されます。最大 8 つの UNI と ENI を同一コミュニティ VLAN 内のコミュニティ ポートとすることができます。

（注）　トランク ポートは、通常の VLAN からのトラフィックを転送し、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転送します。

プライマリおよびセカンダリ 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 が 1 つだけあります。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、プロミスキャス 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 ポートおよび他のプロミスキャス ポートに転送します。
- 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、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プロミスキャス ポートおよびゲートウェイへ転送するセカンダリ 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 ポートへ転送するセカンダリ 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。コミュニティ VLAN は、UNI および ENI を組み合せて最大 8 つ指定できます。

（注）　またスイッチは、UNI-ENI 独立 VLAN および UNI-ENI コミュニティ VLAN サポートします。作成された VLAN は、デフォルトで UNI-ENI 独立 VLAN となります。UNI-ENI 独立 VLAN に属するスイッチの UNI および ENI 間では、トラフィックはスイッチングされません。UNI-ENI VLAN の詳細については、第 12 章「VLAN の設定」を参照してください。

プロミスキャス ポートが扱えるのは、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 だけです。レイヤ 3 ゲートウェイは通常プロミスキャス ポートを介してスイッチに接続されています。プロミスキャス ポートを使用すると、幅広いデバイスをプライベート VLAN へのアクセス ポートとして接続できます。たとえば、すべてのプライベート VLAN サーバを管理ワークステーションからモニタしたりバックアップしたりするのに、プロミスキャス ポートを使用できます。

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エンド ステーションの共通グループに、個別のプライベート VLAN と関連する IP サブネットを割り当てることができます。エンド ステーションがデフォルト ゲートウェイと対話する必要があるのは、プライベート VLAN 外部と通信する場合だけです。

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。

- 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 NNI をプロミスキャス ポートとして設定します。これにより、すべてのエンド ステーションがデフォルト ゲートウェイに接続できます。

プライマリ、独立、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デバイスに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 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。

プライベート VLAN での IP アドレッシング方式

各カスタマーに個別の 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。

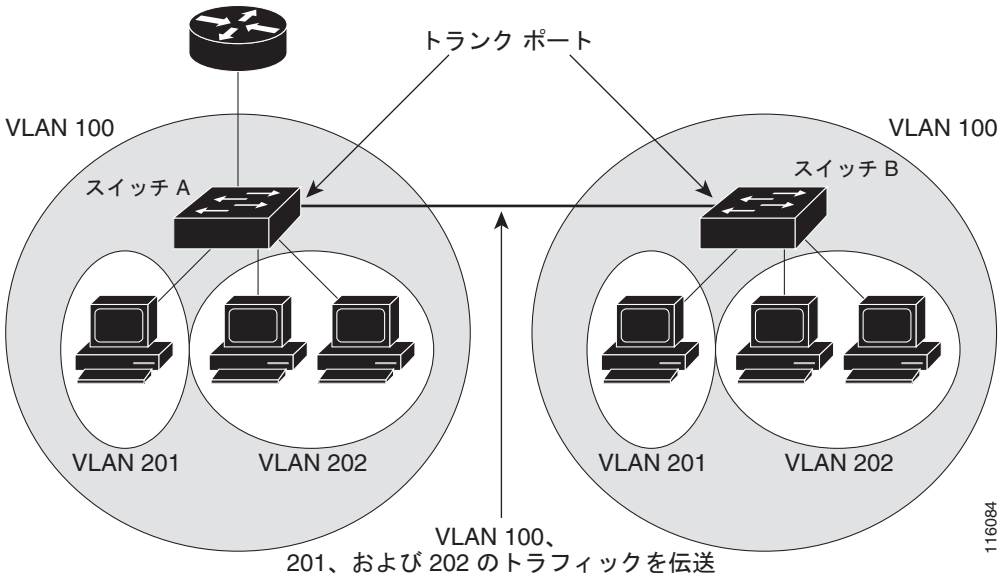
- カスタマーの VLAN にアドレス ブロックを割り当てると、未使用の IP アドレスが出てきます。
- VLAN 内のデバイス数が増加した場合、それに対応するだけのアドレスを割り当てられない場合があります。

これらの問題は、プライベート VLAN を使用することで軽減できます。この場合、プライベート VLAN 内のすべてのメンバーがプライマリ VLAN に割り当てられた共通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。後続の IP アドレスは、同じプライマリ VLAN にある別のセカンダリ VLAN にあるカスタマー デバイスに割り当てることができます。新しいデバイスが追加されると、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できる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 と同様に、プライベート VLAN を複数のスイッチ全体に設定できます。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 にある独立ポートに到達しません。図 13-2 を参照してください。

図 13-2　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

レイヤ 2 ネットワークのすべてのスイッチ上のプライベート VLAN は、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。

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 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左右されます。

- 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、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 内のポートにブロードキャストを送信します。
- プロミスキャス ポート（NNI だけ）は、プライベート VLAN 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、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 内のポート間で転送されず、また別のセカンダリ VLAN 内のポート間でも転送されません。

プライベート VLAN と SVI

レイヤ 3 スイッチ（メトロ IP アクセス イメージが稼動するスイッチ）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 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。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 は非アクティブになります。

- アクティブ 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と、SVI をディセーブルにするまで設定が許可されません。
- 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 がセカンダリ VLAN に対応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 アドレスです。

プライベート VLAN の設定

プライベート VLAN の設定手順

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　プライマリおよびセカンダリ VLAN を作成してこれらを対応付けします。「プライベート VLAN への VLAN の設定と関連付け」（P.13-10）を参照してください。

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

ステップ 2　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.13-12）を参照してください。

ステップ 3　NNI をプロミスキャス ポートを設定し、プロミスキャス ポートをプライマリおよびセカンダリ 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.13-13）を参照してください。

ステップ 4　VLAN 間ルーティングを使用している場合、プライマリ SVI を設定し、セカンダリ VLAN をプライマリ SVI 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.13-15）を参照してください。

ステップ 5　プライマリ VLAN 設定を確認します。

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。新たに作成された VLAN は、UNI-ENI 独立 VLAN になります。

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、次のカテゴリに分けられます。

- 「セカンダリおよびプライマリ VLAN の設定」（P.13-7）
- 「プライベート VLAN ポート設定」（P.13-9）
- 「他の機能との間の制限」（P.13-10）

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。

- プライベート VLAN を設定するには、VLAN 設定モードを使用します。VLAN 設定の詳細については、「VLAN の作成および変更」（P.12-7）を参照してください。
- プライベート VLAN ポートが必要な各デバイスにプライベート VLAN を設定する必要があります。
- プライベート VLAN は、UNI-ENI VLAN にできません。
  - UNI-ENI 独立 VLAN（デフォルト）をプライベート VLAN に変更するには、**private-vlan** VLAN コンフィギュレーション コマンドを入力します。これにより、デフォルトの独立 VLAN 設定は上書きされます。
  - UNI-ENI コミュニティ VLAN をプライベート VLAN に変更するには、まず **no uni-vlan** VLAN コンフィギュレーション コマンドを入力して、デフォルトの UNI 独立 VLAN 設定に戻します。
- VLAN 1 または VLAN 1002 ～ 1005 をプライマリまたはセカンダリ VLAN に設定できません。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 を 1 つだけ設定できます。
- 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 全体で実行可能な Spanning-Tree Protocol（STP; スパニングツリー プロトコル）インスタンスは 1 つだけです。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。

- 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場合、セカンダリ VLAN に伝播されます。セカンダリ VLAN に 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ないと有効になりません。
- 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には、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。
- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN に別々の QoS（Quality of Service）設定を適用できます。
- スティッキ ARP について、スイッチでメトロ IP アクセス イメージが稼動している場合
  - 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 *global* コンフィギュレーションおよび **ip sticky-arp** *interface* コンフィギュレーション コマンドの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。
- プライマリおよびセカンダリ VLAN で VLAN マップを設定できます（「VLAN マップの設定」（P.32-30）を参照）。ただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ 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 を介して転送される場合、同じ VLAN マップが受信側と送信側の両方に適用されます。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 マップが受信側に適用されます。

  - 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 に設定されている 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 に設定されている 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 の両方に適用します。

- スイッチでメトロ IP アクセス イメージが稼動している場合、ルータ ACL はプライマリ VLAN SVI 上でだけ適用できます。ACL はプライマリおよびセカンダリ 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 でホストを分離していても、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、次の Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能をサポートします。
  - プライベート VLAN を SPAN 送信元ポートとして設定できます。
  - VLAN-based SPAN（VSPAN）はプライマリ VLAN、独立 VLAN、およびコミュニティ VLAN で使用できます。また、送信または受信トラフィックを別々にモニタするために、1 つの VLAN でだけ SPAN を使用できます。

プライベート VLAN ポート設定

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。

- プロミスキャス ポートは NNI である必要があり、UNI および ENI はプロミスキャス ポートとして設定できません。
- プライマリ VLAN、独立 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 設定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 として設定した VLAN に割り当てられたレイヤ 2 アクセス ポートは、VLAN がプライベート VLAN 設定の一部の間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。
- Port Aggregation Protocol（PAgP; ポート集約プロトコル）または Link Aggregation Control Protocol（LACP; リンク集約制御プロトコル）EtherChannel に属する NNI ポートは、プライベート VLAN ポートとして設定できません。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。
- 誤った設定による STP ループを発生させず、STP コンバージェンスを高速にするために、NNI 独立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 17 章「オプションのスパニング ツリー機能の設定方法」を参照）。イネーブルの場合、STP はすべての PortFast が設定されたレイヤ 2 LAN ポートに BPDU ガード機能を適用します。PortFast および BPDU ガードをプロミスキャス ポートでイネーブルにしないでください。
- プライベート VLAN 設定で 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に接続されていて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 ポートを別のネットワーク デバイス上に設定できます。
- コミュニティ プライベート VLAN には、最大 8 つの UNI および ENI を含めることができます。9 つ以上の UNI および ENI を追加しようとした場合、設定は許可されません。9 つ以上の UNI および ENI の組み合せを含む VLAN をコミュニティ プライベート VLAN として設定しようとしても、設定は許可されません。

他の機能との間の制限

プライベート VLAN を設定する際、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）　エラー メッセージなしで設定が受け入れられていてもコマンドが機能しない場合があります。

- IGMP スヌーピングがスイッチでイネーブルの場合（デフォルト）、スイッチでサポートされるプライベート VLAN ドメインの数は 20 までです。
- プライベート VLAN は、UNI-ENI 独立 VLAN または UNI-ENI コミュニティ VLAN にはできません。UNI-ENI VLAN の詳細については、第 12 章「VLAN の設定」を参照してください。
- Remote SPAN（RSPAN; リモート SPAN）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 27 章「SPAN および RSPAN の設定」を参照してください。
- 次のような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
  - PAgP（NNI または ENI だけ）
  - LACP（NNI または ENI だけ）
  - マルチキャスト VLAN レジストレーション（MVR）
- プライベート VLAN ポートでは 802.1x ポートベース認証を設定できますが、このポートで、ポート セキュリティと同時に IEEE 802.1x を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 ポートに設定した場合、ポートは非アクティブになります。
- プライマリ VLAN 内のプロミスキャス ポートにスタティック MAC アドレスを設定した場合、同じスタティック アドレスをすべての関連セカンダリ VLAN に追加する必要があります。セカンダリ VLAN 内ホスト ポートにスタティック MAC アドレスを設定した場合、同じスタティック アドレスをすべての関連プライマリ 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際に、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 LAN 上にある 1 つの VLAN で学習されたダイナミック MAC アドレスは、関連 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たり期限が切れた場合、複製アドレスは 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。

プライベート VLAN への VLAN の設定と関連付け

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行います。

（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機能しません。

	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	**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 を指定するか作成します。指定できる VLAN ID 範囲は 2 ～ 1001 および 1006 ～ 4094 です。 **（注）** VLAN が UNI-ENI コミュニティ VLAN として設定されている場合、**no uni-vlan** VLAN コンフィギュレーション コマンドを入力してから、プライベート VLAN を設定する必要があります。
ステップ 3	**private-vlan primary**	VLAN をプライマリ VLAN として指定します。
ステップ 4	**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 5	**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 を指定するか作成します。指定できる VLAN ID 範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 6	**private-vlan isolated**	VLAN を独立 VLAN として指定します。
ステップ 7	**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 8	**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 を指定するか作成します。指定できる VLAN ID 範囲は 2 ～ 1001 および 1006 ～ 4094 です。 **（注）** VLAN が UNI-ENI コミュニティ VLAN として設定されている場合、**no uni-vlan** VLAN コンフィギュレーション コマンドを入力してから、プライベート VLAN を設定する必要があります。
ステップ 9	**private-vlan community**	VLAN をコミュニティ VLAN として指定します。
ステップ 10	**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 11	**vlan** *vlan-id*	ステップ 3 で指定したプライマリ 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 12	**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 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show vlan private-vlan** [**type**] または **show interfaces status**	設定を確認します。
ステップ 15	**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。

セカンダリ VLAN をプライマリ VLAN に関連付ける際に、構文に関して次のことに留意してください。

- *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 を含められますが、独立 VLAN ID は 1 つだけです。
- *secondary_vlan_list* を入力するか、またはキーワード **add** を指定した *secondary_vlan_list* を使用してセカンダリ VLAN とプライマリ VLAN を関連付けます。

- **remove** キーワードとともに *secondary_vlan_list* を使用して、セカンダリ VLAN とプライマリ VLAN の関連付けを解除します。
- **private-vlan association** VLAN コンフィギュレーション コマンドは、VLAN コンフィギュレーション モードを終了しないかぎり、有効になりません。

次に、VLAN 20 をプライマリ VLAN、VLAN 501 を独立 VLAN、VLAN 502 および VLAN 503 をコミュニティ VLAN として設定し、これらをプライベート VLAN 内で関連付けして、設定を確認する例を示します。VLAN 502 および VLAN 503 は、事前に UNI-ENI コミュニティ VLAN として設定されていると想定します。

```
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)# no-uni vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# no-uni vlan
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、これをプライマリおよびセカンダリ VLAN と関連付けるには、特権 EXEC モードで次の手順を実行します。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ 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*	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。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。

	コマンド	目的
ステップ 4	**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 5	**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 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport**	設定を確認します。
ステップ 8	**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、これにプライベート VLAN ペアを関連付けて、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/22
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
Switch# show interfaces fastethernet0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Administrative private-vlan host-association: 20 501
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:
20 501
<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

プロミスキャス ポートとして設定できるのは、NNI に限られます。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）　独立およびコミュニティ VLAN はいずれもセカンダリ 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*	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。インターフェイスは、NNI である必要があります。 **（注）** インターフェイスが UNI または ENI の場合は、プロミスキャス ポートとして設定する前に、**port-type nni** インターフェイス コンフィギュレーション コマンドを入力する必要があります。
ステップ 3	**switchport mode private-vlan promiscuous**	レイヤ 2 NNI 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 と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 ポートとして設定した場合、構文に関して次のことに留意してください。

- *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* を入力するか、またはキーワード **add** を指定した *secondary_vlan_list* を使用してセカンダリ VLAN とプライマリ 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します。
- **remove** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN とプライベート VLAN プロミスキャス ポートのマッピングを解除します。

次に、NNI をプライベート VLAN プロミスキャス ポートとして設定して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 gigabitethernet0/1
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

show vlan private-vlan または **show interface status** 特権 EXEC コマンドを使用して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

スイッチでメトロ IP アクセス イメージが稼動していて、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）　独立およびコミュニティ VLAN はいずれもセカンダリ 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 でインターフェイス コンフィギュレーション モードを開始して VLAN を SVI として設定します。指定できる 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 着信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 を介してスイッチングされているプライベート VLAN トラフィックにだけ影響します。

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、構文について次の点に留意してください。

- *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* を入力するか、またはキーワード **add** を指定した *secondary_vlan_list* を使用してセカンダリ VLAN をプライマリ VLAN にマッピングします。
- **remove** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN とプライマリ VLAN のマッピングを解除します。

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 から 502 へのセカンダリ VLAN 着信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 のモニタリング

表 13-1 に、プライベート VLAN モニタ用の特権 EXEC コマンドを示します。

表 13-1　プライベート VLAN モニタリング 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 インターフェイスのプライベート VLAN マッピングに関する情報を表示します。

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

```
Switch(config)# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Fa0/1, Gi0/1, Gi0/2
10      502       community         Fa0/11, Fa0/12, Gi0/1
10      503       non-operational
```