



プライベート VLAN の設定

- 機能情報の確認, 1 ページ
- プライベート VLAN の前提条件, 1 ページ
- プライベート VLAN の制約事項, 4 ページ
- プライベート VLAN について, 6 ページ
- プライベート VLAN の設定方法, 12 ページ
- プライベート VLAN のモニタ, 22 ページ
- プライベート VLAN の設定例, 22 ページ
- 次の作業, 25 ページ
- その他の関連資料, 25 ページ
- プライベート VLAN の機能履歴と情報, 26 ページ

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェアリリースの **Bug Search Tool** およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

プライベート VLAN の前提条件

プライベート VLAN 設定時の前提条件は、次のとおりです。

- VTP を実行しているスイッチにプライベート VLAN を設定した場合、スイッチは VTP トランスペアレント モードでなければなりません。
- プライベート VLAN をスイッチに設定するときに、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、常にデフォルトの 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、デフォルトテンプレートを設定するのに **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 の設定を行うときは、次の注意事項に従ってください。

- switch で VTP バージョン 1 または 2 が稼働している場合は、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 を設定した後で、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 バージョン 3 は、すべてのモードでプライベート VLAN をサポートします。
- VTP バージョン 1 または 2 でプライベート VLAN を設定した後、**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 モード設定とプライベート VLAN 設定を switch 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。保存しないと、switch をリセットした場合にデフォルトの VTP サーバモードになり、プライベート VLAN をサポートしなくなります。VTP バージョン 3 ではプライベート VLAN をサポートします。
- VTP バージョン 1 および 2 では、プライベート VLAN 設定の伝播は行われません。プライベート VLAN ポートが必要なデバイスで VTP バージョン 3 が実行されていない場合は、そのデバイス上でプライベート 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 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 つの独立 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 全体で実行可能なスパンニングツリープロトコル (STP) 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。
- 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と、DHCP スヌーピングはセカンダリ VLAN に伝播されます。セカンダリ VLAN で DHCP を設定しても、プライマリ VLAN をすでに設定している場合、DHCP 設定は有効になりません。
- 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。
 - 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
 - sticky ARP には、次の考慮事項があります。
 - sticky ARP エントリとは、SVI およびレイヤ 3 インターフェイス上で学習されるエントリです。これらのエントリは、期限切れになることはありません。
 - **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 に属する 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、以下でのみサポートされます。
 - レイヤ 3 インターフェイス
 - 標準 VLAN に属する SVI
 - プライベート VLAN に属する SVI
- ip sticky-arp** グローバル コンフィギュレーション コマンドおよび **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 VLAN マップを設定できます。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 内で転送されるレイヤ 2 の場合、同じ VLAN マップが入力側と出力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 マップが入力側に適用されます。
 - フレームがホストポートから無差別ポートにアップストリームで送信される場合は、セカンダリ VLAN で設定された VLAN マップが適用されます。
 - フレームが無差別ポートからホストポートにダウンストリームで送信される場合は、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 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 およびセカンダリ VLAN の両方に VLAN マップを適用する必要があります。
- プライマリ VLAN SVI にだけルータ ACL を適用できます。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 では、次のスイッチドポートアナライザ (SPAN) 機能がサポートされます。

- プライベート VLAN を SPAN 送信元ポートとして設定できます。
- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN 上で VLAN ベースの 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監視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 ポートの設定時は、次の注意事項に従ってください。

- 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 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。
- PAgP または 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 の設定に含まれている間は、そのポートの EtherChannel 設定はいずれも非アクティブです。
- 設定ミスによる STP ループの発生を防ぎ、STP コンバージェンスを高速化するには、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 BPDU ガードをイネーブルにします。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 ガードを無差別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 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。
- ネットワーク デバイスをトランク接続し、プライマリ VLAN 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 ポートはさまざまなネットワーク デバイス上で使用できます。

プライベート VLAN の制約事項

プライベート VLAN を設定する際の前提条件は、次のとおりです。

- プライベート VLAN は、IP Lite イメージを実行するスイッチ上でのみサポートされます。

その他の機能の制限事項

プライベート VLAN を設定する際に、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) 一部の状況では、エラーメッセージが表示されずに設定が受け入れられますが、コマンドには効果がありません。

- 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。
- 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、スイッチまたはスイッチスタックでは 20 個までしかプライベート VLAN ドメインをサポートしません。
- 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、Remote SPAN (RSPAN) VLAN を設定しないでください。
- 次のようなその他の機能用に設定したインターフェイスでは、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 トランッキング プロトコル (DTP)
 - ポート集約プロトコル (PAgP)
 - リンク集約制御プロトコル (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)
- IEEE 802.1x ポートベース認証をプライベート VLAN ポートで設定できますが、ポートセキュリティ、音声 VLAN、またはユーザごとの ACL と一緒に 802.1x をプライベート VLAN ポートに設定しないでください。
- プライベート VLAN ホストまたは無差別ポートは、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 の無差別ポートでスタティック MAC アドレスを設定する場合は、すべての関連セカンダリ VLAN に同じスタティック アドレスを追加する必要があります。セカンダリ VLAN のホストポートでスタティック MAC アドレスを設定する場合は、関連プライマリ VLAN に同じスタティック 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 アドレスを削除する場合は、設定した 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 で学習したダイナミック MAC アドレスは、関連 VLAN で複製されます。たとえば、セカンダリ VLAN で学習した 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 アドレスが削除されるか期限切れになると、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 (SVI) 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 について

プライベート VLAN ドメイン

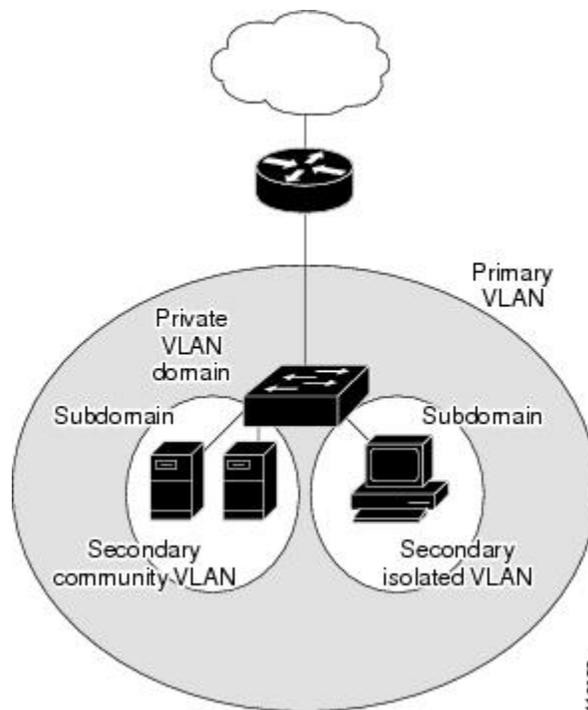
PVLAN 機能を使用すると、サービス プロバイダーが VLAN を使用したときに直面する 2 つの問題に対処できます。

- 最大 1005 個のアクティブ VLAN が switch でサポートされます。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得がもたらされ、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。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 1: プライベート VLAN ドメイン



関連トピック

[プライベート VLAN 内の VLAN の設定および対応付け](#), (12 ページ)

[例: プライマリ VLAN、独立 VLAN、および VLAN コミュニティの設定](#), (22 ページ)

セカンダリ VLAN

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。

プライベート VLAN ポート

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 ポートは、次のいずれかの種類に属するアクセス ポートです。

- 無差別：無差別ポートは、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。
- 独立：独立ポートは、独立セカンダリ VLAN に属しているホストポートです。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。
- 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。



(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、無差別ポートからの単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。
- 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方向トラフィックアップストリームを搬送します。
- 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。

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switchに接続されます。無差別ポートでは、広範囲なデバイスをプライベート VLAN のアクセスポイン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監視したりバックアップしたりするのに、無差別ポートを使用できます。

関連トピック

[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](#), (16 ページ)

[例：ホストポートとしてのインターフェイスの設定](#), (23 ページ)

[プライベート VLAN 無差別ポートとしてのレイヤ2インターフェイスの設定](#), (18 ページ)

[例：インターフェイスをプライベート VLAN 無差別ポートとして設定する](#), (24 ページ)

ネットワーク内のプライベート VLAN

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）に接続されているインターフェイスを無差別ポートとして設定し、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るようにします。

複数のデバイス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デバイスにトラッキングします。使用するプライベート VLAN 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 ポートがないデバイスを含めて、すべての中間デバイスでプライベート VLAN を設定します。

プライベート VLAN による IP アドレス指定方式

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。

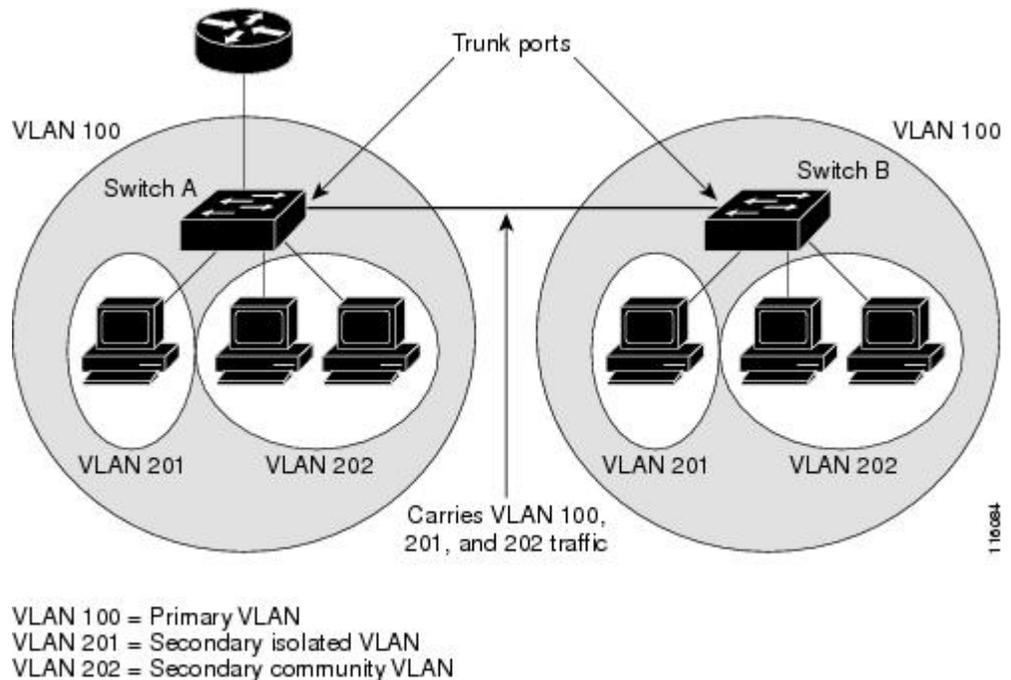
- カスタマー VLAN にアドレスのブロックを割り当てると、未使用 IP アドレスが発生することがあります。
- VLAN 内のデバイス数が増加した場合、それに対応するだけのアドレスを割り当てられない場合があります。

この問題は、プライベート VLAN を使用すると軽減します。プライベート VLAN では、プライベート VLAN のすべてのメンバーが、プライマリ VLAN に割り当てられている共通アドレス空間を共有するためです。ホストはセカンダリ VLAN に接続され、プライマリ VLAN に割り当てられているアドレスのブロックから IP アドレスが DHCP サーバによってホストに割り当てられますが、同一プライマリ VLAN 内のセカンダリ VLAN には割り当てられません。さまざまなセカンダリ VLAN のカスタマー デバイスには後続 IP アドレスが割り当てられます。新しいデバイスを追加すると、サブネット アドレスの巨大プールから次に使用できるアドレスが、DHCP サーバによって割り当てられます。

複数のSwitches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switches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switch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switchesにまたがるプライベート VLAN の機能の特徴として、Switch A にある独立ポートからのトラフィックはSwitch B に到達しません。

図 2: 複数のスイッチにまたがるプライベート 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switches 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switches で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switches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switchesでプライベート VLAN トラフィックの不要なフラディングが発生する可能性があります。

プライベート VLAN とその他の機能の相互作用

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。

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のルーティングとブリッジングは、プライベート VLAN 境界を横断して行われ、単一コミュニティ VLAN 内でも行われます。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。

プライベート VLAN と Switch スタック

プライベート VLAN は switch 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存在することができます。ただし、スタックを次のように変更すると、プライベート VLAN の動作に影響が及ぶ可能性があります。

- スタックにプライベート VLAN 無差別ポートが1つだけ含まれ、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 無差別ポートが1つだけあるスタックマスターに障害が発生した場合、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無差別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された場合、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、switchを再起動したときに、権利を獲得しなかったswitchのプライベート VLAN 設定が失われます。

プライベート VLAN の設定タスク

プライベート VLAN を設定するには、次の手順を実行します。

- 1 VTP モードをトランスペアレントに設定します。
- 2 プライマリおよびセカンダリ VLAN を作成してこれらに対応付けします。



(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。

- 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。
- 4 インターフェイスを無差別ポートとして設定し、無差別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。
- 5 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 をプライマリにマッピングします。
- 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 の設定方法

プライベート VLAN 内の VLAN の設定および対応付け

`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。

手順の概要

1. **enable**
2. **configure terminal**
3. **vtp mode transparent**
4. **vlan *vlan-id***
5. **private-vlan primary**
6. **exit**
7. **vlan *vlan-id***
8. **private-vlan isolated**
9. **exit**
10. **vlan *vlan-id***
11. **private-vlan community**
12. **exit**
13. **vlan *vlan-id***
14. **private-vlan association [add | remove] *secondary_vlan_list***
15. **end**
16. **show vlan private-vlan [type] または show interfaces status**
17. **copy running-config startup config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Switch> enable	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : 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 3	vtp mode transparent 例 : Switch(config)# vtp mode transport	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）。

	コマンドまたはアクション	目的
ステップ 4	vlan vlan-id 例： Switch(config)# vlan 20	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 の範囲は 2 ~ 1001 および 1006 ~ 4094 です。
ステップ 5	private-vlan primary 例： Switch(config-vlan)# private-vlan primary	VLAN をプライマリ VLAN として指定します。
ステップ 6	exit 例： Switch(config-vlan)# 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 7	vlan vlan-id 例： Switch(config)# vlan 501	(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 の範囲は 2 ~ 1001 および 1006 ~ 4094 です。
ステップ 8	private-vlan isolated 例： Switch(config-vlan)# private-vlan isolated	VLAN を独立 VLAN として指定します。
ステップ 9	exit 例： Switch(config-vlan)# 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 10	vlan vlan-id 例： Switch(config)# vlan 502	(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 の範囲は 2 ~ 1001 および 1006 ~ 4094 です。
ステップ 11	private-vlan community 例： Switch(config-vlan)# private-vlan	VLAN をコミュニティ VLAN として指定します。

	コマンドまたはアクション	目的
	<code>community</code>	
ステップ 12	exit 例： <code>Switch(config-vlan)# exit</code>	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 13	vlan vlan-id 例： <code>Switch(config)# vlan 503</code>	ステップ 2 で指定したプライマリ VLAN に関して 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 14	private-vlan association [add remove] secondary_vlan_list 例： <code>Switch(config-vlan)# private-vlan association 501-503</code>	セカンダリ VLAN をプライマリ VLAN に関連付けます。
ステップ 15	end 例： <code>Switch(config-vlan)# end</code>	特権 EXEC モードに戻ります。
ステップ 16	show vlan private-vlan [type] または show interfaces status 例： <code>Switch(config)# show vlan private vlan</code>	設定を確認します。
ステップ 17	copy running-config startup config 例： <code>Switch# copy running-config startup-config</code>	switch スタートアップ コンフィギュレーション ファイルに設定項目を保存します。 プライベート VLAN 設定を保存するには、switch 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。保存しないと、switch をリセットした場合にデフォルトの VTP サーバモードになり、プライベート VLAN をサポートしなくなります。

関連トピック

[プライベート VLAN ドメイン, \(6 ページ\)](#)

[例: プライマリ VLAN、独立 VLAN、および VLAN コミュニティの設定, \(22 ページ\)](#)

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **switchport mode private-vlan host**
5. **switchport private-vlan host-association *primary_vlan_id secondary_vlan_id***
6. **end**
7. **show interfaces [*interface-id*] switchport**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Switch> enable	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : 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。

	コマンドまたはアクション	目的
ステップ 3	interface <i>interface-id</i> 例 : Switch(config)# interface gigabitethernet1/0/22	設定するレイヤ2 インターフェイスに対して、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 4	switchport mode private-vlan host 例 : Switch(config-if)# 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 <i>primary_vlan_id secondary_vlan_id</i> 例 : Switch(config-if)# switchport private-vlan host-association 20 501	レイヤ2 ポートをプライベート VLAN と関連付けます。
ステップ 6	end 例 : Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 7	show interfaces [<i>interface-id</i>] switchport 例 : Switch# show interfaces gigabitethernet1/0/22 switchport	設定を確認します。
ステップ 8	copy running-config startup-config 例 : Switch# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

関連トピック

[プライベート VLAN ポート, \(7 ページ\)](#)

[例 : ホストポートとしてのインターフェイスの設定, \(23 ページ\)](#)

プライベート VLAN 無差別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 無差別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。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface interface-id**
4. **switchport mode private-vlan promiscuous**
5. **switchport private-vlan mapping primary_vlan_id {add | remove} secondary_vlan_list**
6. **end**
7. **show interfaces [interface-id] switchport**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Switch> enable	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： 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 3	interface interface-id 例： Switch(config)# interface gigabitethernet1/0/2	設定するレイヤ2 インターフェイスに対して、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。

	コマンドまたはアクション	目的
ステップ 4	switchport mode private-vlan promiscuous 例 : <pre>Switch(config-if)# switchport mode private-vlan promiscuous</pre>	レイヤ 2 ポートをプライベート VLAN 無差別ポートとして設定します。
ステップ 5	switchport private-vlan mapping <i>primary_vlan_id</i> { add remove } <i>secondary_vlan_list</i> 例 : <pre>Switch(config-if)# switchport private-vlan mapping 20 add 501-503</pre>	<p>プライベート VLAN 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。</p> <p><i>secondary_vlan_list</i> 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。</p> <p>セカンダリ VLAN とプライマリ VLAN をプライベート VLAN 無差別ポートにマッピングするには、<i>secondary_vlan_list</i> を入力するか、または add キーワードを指定した <i>secondary_vlan_list</i> を使用します。</p> <p>セカンダリ VLAN とプライベート VLAN 無差別ポートのマッピングを解除するには、remove キーワードを指定した <i>secondary_vlan_list</i> を使用します。</p>
ステップ 6	end 例 : <pre>Switch(config-if)# end</pre>	特権 EXEC モードに戻ります。
ステップ 7	show interfaces [<i>interface-id</i>] switchport 例 : <pre>Switch# show interfaces gigabitethernet1/0/2 switchport</pre>	設定を確認します。
ステップ 8	copy running-config startup-config 例 : <pre>Switch# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

関連トピック

[プライベート VLAN ポート, \(7 ページ\)](#)

[例: インターフェイスをプライベート VLAN 無差別ポートとして設定する, \(24 ページ\)](#)

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。

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。

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 スイッチングされているプライベート VLAN トラフィックにだけ影響を与えます。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface vlan *primary_vlan_id***
4. **private-vlan mapping [add | remove] *secondary_vlan_list***
5. **end**
6. **show interface private-vlan mapping**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例: Switch> enable	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例: 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。

	コマンドまたはアクション	目的
ステップ 3	interface vlan primary_vlan_id 例 : Switch(config)# interface vlan 10	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。VLAN ID の範囲は 2 ~ 1001 および 1006 ~ 4094 です。
ステップ 4	private-vlan mapping [add remove] secondary_vlan_list 例 : Switch(config-if)# private-vlan mapping 501-502	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。 <i>secondary_vlan_list</i> 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。 <i>secondary_vlan_list</i> を入力するか、または add キーワードを指定した <i>secondary_vlan_list</i> 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 <i>secondary_vlan_list</i> 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。
ステップ 5	end 例 : Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	show interface private-vlan mapping 例 : Switch# show interfaces private-vlan mapping	設定を確認します。
ステップ 7	copy running-config startup-config 例 : Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

関連トピック

例 : セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする, (24 ページ)

プライベート VLAN のモニタ

次の表に、プライベート VLAN をモニタするために使用するコマンドを記載します。

表 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]	スイッチまたはスイッチ 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 マッピングに関する情報を表示します。

プライベート VLAN の設定例

例：プライマリ VLAN、独立 VLAN、および VLAN コミュニティの設定

次に、VLAN 20 をプライマリ VLAN、VLAN 501 を独立 VLAN、VLAN 502 および 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。

```
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
```

関連トピック

[プライベート VLAN 内の VLAN の設定および対応付け](#), (12 ページ)

[プライベート VLAN ドメイン](#), (6 ページ)

例：ホストポートとしてのインターフェイスの設定

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、それをプライベート VLAN ペアに関連付けて、その設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/22
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 gigabitethernet1/0/22 switchport
Name: Gi1/0/22
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: 20 501
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>
```

関連トピック

[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](#), (16 ページ)

[プライベート VLAN ポート](#), (7 ページ)

例：インターフェイスをプライベート VLAN 無差別ポートとして設定する

次の例では、インターフェイスをプライベート VLAN 無差別ポートとして設定し、それをプライベート VLAN にマッピングする方法を示します。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 gigabitethernet1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

関連トピック

[プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定, \(18 ページ\)](#)

[プライベート VLAN ポート, \(7 ページ\)](#)

例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする

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 および 502 からのセカンダリ VLAN 入カトラフィックのルーティングが可能になります。

```
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
```

関連トピック

[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, \(20 ページ\)](#)

例：プライベート VLAN のモニタリング

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      Gi2/0/1, Gi3/0/1, Gi3/0/2
```

```

10      502      community      Gi2/0/11, Gi3/0/1, Gi3/0/4
10      503      non-operational

```

次の作業

次の設定を行えます。

- VTP
- VLAN
- VLAN トランッキング
- VLAN メンバーシップ ポリシー サーバ (VMPS)
- トンネリング
- 音声 VLAN

その他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Catalyst 2960-XR Switch VLAN Management Command Reference</i>

標準および RFC

標準/RFC	タイトル
—	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	<p>選択したプラットフォーム、Cisco IOS リリース、およびフィチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p>http://www.cisco.com/go/mibs</p>

テクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/support</p>

プライベート VLAN の機能履歴と情報

リリース	変更内容
Cisco IOS 15.0(2)EX1	この機能が導入されました。