プライベート VLAN の設定

プライベート VLAN の前提条件

プライベート VLAN をデバイスに設定するときに、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。

（注） プライベート VLAN は、VTP 1、2、および 3 のトランスペアレント モードでサポートされます。プライベート VLAN は、VTP 3 のサーバ モードでもサポートされます。

プライベート VLAN の制約事項

（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 が設定されているデバイスでは、フォールバックブリッジングを設定しないでください。
- リモート SPAN（RSPAN）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。
- 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 トランキング プロトコル（DTP）
  - IP ソース ガード
  - Cisco IPv6 First Hop Security（FHS）
  - IPv6 Security Group（SG）
  - 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）
- Port Aggregation Protocol（PAgP）および Link Aggregation Control Protocol（LACP）は、プライベート VLAN 無差別トランクポートおよびプライベート VLAN 独立トランクポートでのみサポートされています。
- IEEE 802.1x ポートベース認証をプライベート VLAN ポートに設定できますが、802.1x とポート セキュリティ、音声 VLAN、またはポート単位のユーザ ACL は、プライベート VLAN ポートに設定できません。
- 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 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はありません。同様に、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はありません。さらに、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 から削除する必要はありません。

（注） プライベート VLAN のセカンダリ VLAN で学習したダイナミック MAC アドレスは、関連プライマリ VLAN で複製されます。プライマリ VLAN からトラフィックが入力される場合でも、すべての MAC エントリはセカンダリ VLAN で学習されます。MAC アドレスがプライマリ VLAN で動的に学習される場合は、関連セカンダリ VLAN では複製されません。

- レイヤ 3 VLAN インターフェイス（スイッチ仮想インターフェイス）はプライマリ VLAN にだけ設定してください。
- 同じ VLAN 上で MACsec または仮想プライベート LAN サービス（VPLS）または Cisco SD-Access ソリューションを使用して設定されたプライベート VLAN は機能しません。

プライベート VLAN について

ここでは、プライベート VLAN について説明します。

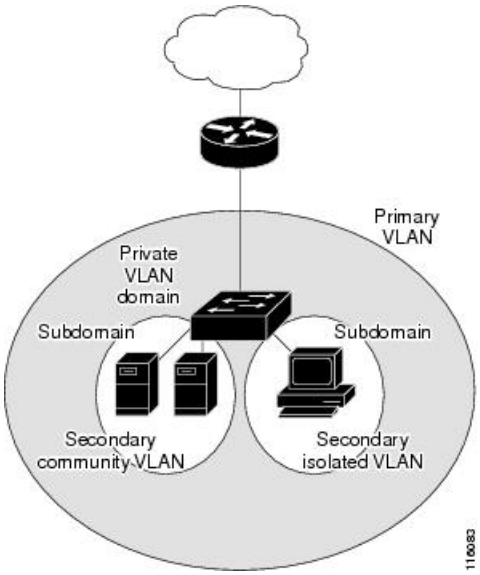
プライベート VLAN ドメイン

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。

- 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。

図 *1* : プライベート *VLAN* ドメイン

プライベート VLAN の使用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。



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、1 つのコミュニティ セカンダリ VLAN に属しているホスト 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一方向トラフィック 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、アップストリーム トラフィックをコミュニティ ポートから無差別ポート ゲートウェイおよび同じコミュニティ内の他のホスト ポートに伝送するセカンダリ VLAN です。複数のコミュニティ VLAN を 1 つのプライベート VLAN に設定できます。

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デバイスに接続されます。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。

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ンキングします。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 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。

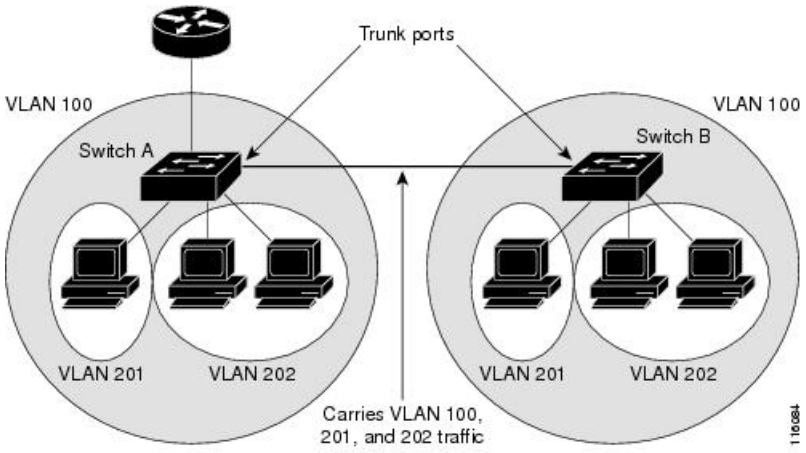
- カスタマー VLAN にアドレスのブロックを割り当てると、未使用 IP アドレスが発生することがあります。
- VLAN 内のデバイス数が増加した場合、それに対応するだけのアドレスを割り当てられない場合があります。

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。

複数のデバイスにまたがるプライベート VLAN

図 *2:* 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 の機能の特徴として、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 上の独立ポートに到達しません。



VLAN 100 = Primary VLAN
VLAN 201 = Secondary isolated VLAN
VLAN 202 = Secondary community VLAN

プライベート VLAN は、VTP 1、2、および 3 のトランスペアレント モードでサポートされます。プライベート VLAN は VTP 3 のサーバモードでもサポートされます。VTP 3 を使用して設定したサーバクライアントがある場合、サーバに設定されているプライベート VLAN をクライアント上に反映させる必要があります。

プライベート VLAN の他機能との相互作用

ここでは、プライベート VLAN の他の機能との連携について説明します。

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 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 のマルチキャスト転送は次の状況をサポートします。

- 送信側が VLAN 外に存在する可能性があり、受信側が VLAN ドメイン内に存在している可能性がある。
- 送信側が VLAN 内に存在する可能性があり、受信側が VLAN ドメイン外に存在している可能性がある。
- 送信側と受信側が同一のコミュニティ VLAN に存在している可能性がある。

プライベート VLAN と SVI

スイッチ仮想インターフェイス（SVI）は 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 だけを介してプライベート 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 ポートはスタック内のさまざまなメンバスイッチ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メンバスイッチ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 無差別ポートのみがあるアクティブスイッチに障害が発生した場合、またはスタックを残し、新しいアクティブスイッチが選択された場合、古

いアクティブスイッチ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。

ダイナミック MAC アドレスを備えたプライベート VLAN

セカンダリ VLAN で学習された MAC アドレスはプライマリ VLAN で複製されますが、その逆はありません。これにより、ハードウェアの L2 CAM スペースを節約できます。プライマリ VLAN は常に、両方向で正引きを実行するのに使用されます。

ダイナミック MAC アドレスは、プライベート VLAN のプライマリ VLAN で学習されると、必要に応じて、セカンダリ VLAN で複製されます。たとえば、MAC アドレスがセカンダリ VLAN で動的に受信されると、プライマリ VLAN の一部として学習されます。隔離 VLAN の場合、同じ MAC のブロックされたエントリは MAC アドレス テーブルのセカンダリ VLAN に追加されます。このため、セカンダリドメインのホストポートで学習された MAC は、ブロックされたタイプのエントリとしてインストールされます。プライマリ VLAN からトラフィックが入力される場合でも、すべての MAC エントリはセカンダリ VLAN で学習されます。

MAC アドレスがプライマリ VLAN で動的に学習される場合、関連セカンダリ VLAN では複製されません。

スタティック MAC アドレスを備えたプライベート VLAN

ユーザは、従来型のようにプライベート VLAN のホストにスタティック MAC アドレス CLI を複製する必要はありません。

例：

- 従来のモデルでは、ユーザはスタティック MAC アドレスを設定すると、関連 VLAN 内にも同じスタティック MAC アドレスを追加する必要がありました。たとえば、MAC アドレス A が VLAN 101 のポート 1/0/1 でユーザ設定され、VLAN 101 ではセカンダリ VLAN で、VLAN 100 がプライマリ VLAN である場合は、ユーザは設定する必要があります

```
mac-address static A vlan 101 interface G1/0/1
mac-address static A vlan 100 interface G1/0/1
```

- このデバイスでは、ユーザは関連 VLAN に MAC アドレスを複製する必要はありません。上記の例のみで、ユーザは設定する必要があります。

```
mac-address static A vlan 101 interface G1/0/1
```

プライベート VLAN と VACL/QOS との相互作用

プライベート VLAN は、このデバイスの場合、他のプラットフォームの「単方向」と比べ、双方向です。

レイヤ 2 の正引き後には、適切な出力 VLAN マッピングが行われ、すべての出力 VLAN ベースの機能による処理が出力 VLAN のコンテキストで実行されます。

レイヤ2のフレームがプライベートVLAN内で転送されると、入力側と出力側とで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マップが入力側に適用されます。同様に、フレームが外部ポートからプライベート VLAN にルーティングされると、プライベート VLAN は出力側に適用されます。これは、ブリッジされたトラフィックとルーティングされたトラフィックの両方に適用されます。

ブリッジング：

- セカンダリ VLAN からプライマリ VLAN へのアップストリーム トラフィックの場合、セカンダリ VLAN の MAP は入力側に適用され、プライマリ VLAN の MAP は出力側に適用されます。
- プライマリ VLAN からセカンダリ VLAN へのダウンストリーム トラフィックの場合は、プライマリ VLAN の MAP は入力方向で適用され、セカンダリ VLAN のMAP は出力方向で適用されます。

ルーティング

プライベート VLAN ドメインが 2 つ（PV1（sec1、prim1）および PV2（sec2、prim2））ある場合を想定します。PV1 から PV2 にルーティングされるフレームについては次のようになります。

- sec1 の MAP および prim1 の L3 ACL は、入力ポートに適用されます。
- sec2 の MAP および prim2 の L3 ACL は、出力ポートに適用されます。

分離されたホストポートから無差別ポートへのアップストリームまたはダウンストリームに従うパケットの場合、分離された VLAN の VACL は入力方向に適用され、プライマリ VLAN の VACL は出力方向に適用されます。これにより、ユーザは同じプライマリ VLAN ドメインの別のセカンダリ VLAN に異なる VACL を設定することができます。

（注） このデバイスでのプライベートVLANは常に双方向であるため、双方向のコミュニティ VLAN は不要です。

プライベート VLAN および HA サポート

PVLANは、高可用性（HA）機能とシームレスに連携します。切り替えの前に、アクティブスイッチにあるプライベート VLAN は、切り替え後と同じである必要があります（新しいアクティブスイッチはIOS側および、FED側両方で以前のアクティブスイッチと同様のPVLAN設定が必要です）。

プライベート VLAN 設定時の注意事項

ここでは、プライベート VLAN 設定時の注意事項について説明します。

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。

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 の設定時は、次の注意事項に従ってください。

- プライベート VLAN は、VTP 1、2、および 3 のトランスペアレント モードでサポートされます。デバイスで 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 設定をデバイス 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、デバイスをリセットした場合、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、VTP3 はプライベート VLAN を伝播するため、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。
- TFTP サーバから PVLAN 設定をコピーし、それを実行中の設定に適用しても、PVLAN の関連付けは形成されません。プライマリ VLAN がすべてのセカンダリ VLAN に確実に関連付けられていることを確認する必要があります。

  copy flash:config_file running-configの代わりに**configure replace flash:config_file force**を使用することもできます。
- 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。
- PVLAN は双方向です。これらは、入力側と出力側の両方に適用されます。

  レイヤ 2 のフレームがプライベート VLAN 内で転送されると、入力側と出力側で 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 マップが入力側に適用されます。同様に、フレームが外部ポートからプライベート VLAN にルーティングされると、プライベート VLAN は出力側に適用されます。

  ブリッジング

  - セカンダリ VLAN からプライマリ VLAN へのアップストリーム トラフィックの場合、セカンダリ VLAN の MAP は入力側に適用され、プライマリ VLAN の MAP は出力側に適用されます。
  - プライマリ VLAN からセカンダリ VLAN へのダウンストリーム トラフィックの場合は、プライマリ VLAN の MAP は入力方向で適用され、セカンダリ VLAN のMAP は出力方向で適用されます。

ルーティング

プライベート VLAN ドメインが 2 つ（PV1（sec1、prim1）および PV2（sec2、prim2））ある場合を想定します。PV1 から PV2 にルーティングされるフレームについては次のようになります。

- sec1 の MAP および prim1 の L3 ACL は入力ポートに適用されます。
- sec1 の MAP および prim2 の L3 ACL は出力ポートに適用されます。
- 分離されたホスト ポートから無差別ポートへのアップストリームまたはダウンストリームに従うパケットの場合、分離された VLAN の VACL は入力方向に適用され、プライマリ VLAN の VACL は出力方向に適用されます。これにより、ユーザは同じプライマリ VLAN ドメインの別のセカンダリ VLAN に異なる VACL を設定することができます。

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 の設定方法

ここでは、プライベート VLAN の設定について説明します。

プライベート VLAN の設定

プライベート VLAN を設定するには、次の手順を実行します。

（注） プライベート VLAN は、VTP 1、2、および 3 のトランスペアレント モードでサポートされます。プライベート VLAN は、VTP 3 のサーバ モードでもサポートされます。

手順

ステップ 1 VTP モードを次に設定します： **transparent**

（注） 注：VTP3 の場合、サーバまたはトランスペアレント モードのいずれにもモードを設定できます。

ステップ 2 プライマリおよびセカンダリ VLAN を作成してこれらを対応付けします。

「プライベート VLAN 内の VLAN の設定および対応付け」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 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」を参照してください

ステップ 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。

「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」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、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」を参照してください

ステップ 6 プライマリ VLAN 設定を確認します。

プライベート VLAN 内の VLAN の設定および対応付け

VLAN コンフィギュレーション モードを終了するまで、**private-vlan** コマンドは有効ではありません。

プライベート VLAN 内で VLAN を設定し、関連付けるには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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： `Device# 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： `Device(config)# 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）。 （注） VTP3 の場合、サーバまたはトランスペアレントモードのいずれにもモードを設定できます。
ステップ 4	**vlan** *vlan-id* 例：	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

	コマンドまたはアクション	目的
	`Device(config)# vlan 20`	ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 5	**private-vlan primary** 例： `Device(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： `Device(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： `Device(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： `Device(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： `Device(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： `Device(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： `Device(config-vlan)# private-vlan community`	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
ステップ 12	**exit** 例： `Device(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 13	**vlan** *vlan-id* 例： `Device(config)# vlan 503`	（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 14	**private-vlan community** 例： `Device(config-vlan)# private-vlan community`	VLAN をコミュニティ VLAN として指定します。
ステップ 15	**exit** 例： `Device(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 16	**vlan** *vlan-id* 例： `Device(config)# vlan 20`	ステップ 4 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 17	**private-vlan association** [**add** | **remove**] *secondary_vlan_list* 例： `Device(config-vlan)# private-vlan association 501-503`	セカンダリ VLAN をプライマリ VLAN に関連付けます。単一のプライベート VLAN ID でも、またはハイフンで連結したプライベート VLAN ID でもかまいません。 • *secondary_vlan_list* 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 です。

	コマンドまたはアクション	目的
		• *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 *secondary_vlan_list* で **add** キーワードを指定し、セカンダリ VLAN とプライマリ VLAN を関連付けます。 • セカンダリ VLAN とプライマリ VLAN 間の関連付けをクリアするには、*secondary_vlan_list* に **remove** キーワードを使用します。 • このコマンドは、VLAN コンフィギュレーション モードを終了するまで機能しません。
ステップ 18	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 19	**show vlan private-vlan** [**type**] or **show interfaces status** 例： `Device# show vlan private-vlan`	設定を確認します。
ステップ 20	**copy running-config startup config** 例： `Device# copy running-config startup-config`	デバイス 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 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 に関連付けるには、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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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： `Device# 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： `Device(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： `Device(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** *primary_vlan_id secondary_vlan_id* 例： `Device(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。 （注） これは、レイヤ 2 インターフェイスに PVLAN を関連付けるために必要な手順です。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： `Device# 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： `Device# 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。

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、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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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： `Device# 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： `Device(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： `Device(config-if)# switchport mode private-vlan promiscuous`	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** *primary_vlan_id* {**add** | **remove**} *secondary_vlan_list* 例： `Device(config-if)# switchport private-vlan mapping 20 add 501-503`	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。 • *secondary_vlan_list* 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。 • 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、*secondary_vlan_list*、または **add** キーワードを指定した *secondary_vlan_list* を使用します。 • 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 *secondary_vlan_list* を使用します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： `Device# show interfaces gigabitethernet1/0/2 switchport`	設定を確認します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup config** 例： `Device# copy running-config startup-config`	デバイス 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。

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、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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： `Device# 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 vlan** *primary_vlan_id* 例： `Device(config)# interface vlan 20`	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：	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

	コマンドまたはアクション	目的
	`Device(config-if)# private-vlan mapping 501-503`	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。 （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。 • *secondary_vlan_list* 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 です。 • *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *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。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces private-vlan mapping** 例： `Device# show interfaces private-vlan mapping`	設定を確認します。
ステップ 7	**copy running-config startup config** 例： `Device# copy running-config`	デバイス 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。

	コマンドまたはアクション	目的
	startup-config	

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**]	
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

次のセクションにプライベート VLAN の設定例を示します。

例：プライベート VLAN 内の VLAN の設定および関連付け

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。

```
Device# configure terminal
Device(config)# vlan 20
Device(config-vlan)# private-vlan primary
Device(config-vlan)# exit
Device(config)# vlan 501
Device(config-vlan)# private-vlan isolated
Device(config-vlan)# exit
Device(config)# vlan 502
Device(config-vlan)# private-vlan community
Device(config-vlan)# exit
Device(config)# vlan 503
Device(config-vlan)# private-vlan community
Device(config-vlan)# exit
Device(config)# vlan 20
```

```
Device(config-vlan)# private-vlan association 501-503
Device(config-vlan)# end
Device# show vlan private-vlan
Primary   Secondary      Type
--------- -------------- -----------------
20        501            isolated
20        502            community
20        503            community
```

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。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/22
Device(config-if)# switchport mode private-vlan host
Device(config-if)# switchport private-vlan host-association 20 501
Device(config-if)# end
Device# 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>
```

例：プライベート VLAN 無差別ポートとしてのインターフェイスの設定

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。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport mode private-vlan promiscuous
```

```
Device(config-if)# switchport private-vlan mapping 20 add 501-503
Device(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 とデバイス上のプライベート VLAN ポートを表示します。

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 入力トラフィックのルーティングが可能になります。

```
Device# configure terminal
Device(config)# interface vlan 20
Device(config-if)# private-vlan mapping 501-503
Device(config-if)# end
Device# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan20    501            isolated
vlan20    502            community
vlan20    503            community
```

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。

```
Device# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
20      501       isolated          Gi1/0/22, Gi1/0/2
20      502       community         Gi1/0/2
20      503       community         Gi1/0/2
```

次の作業

次の設定を行えます。

- VTP
- VLAN
- VLAN トランキング
- VLAN メンバーシップ ポリシー サーバ（VMPS）
- 音声 VLAN

その他の参考資料

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。	*Command Reference (Catalyst 9200 Series Switches)*

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	『Remote Network Monitoring Management Information Base』
RFC 2021	Remote Network Monitoring Management Information Base Version 2 using SMIv2

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB • BRIDGE-MIB（RFC1493） • CISCO-BRIDGE-EXT-MIB • CISCO-CDP-MIB • CISCO-PAGP-MIB • CISCO-PRIVATE-VLAN-MIB • CISCO-LAG-MIB • CISCO-L2L3-INTERFACE-CONFIG-MIB • CISCO-MAC-NOTIFICATION-MIB • CISCO-STP-EXTENSIONS-MIB • CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VTP-MIB • IEEE8023-LAG-MIB • IF-MIB（RFC 1573） • RMON-MIB（RFC 1757） • RMON2-MIB（RFC 2021）	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、URL http://www.cisco.com/go/mibs にある Cisco MIB Locator を使用します

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 XE Fuji 16.9.2	このコマンドが導入されました。