CHAPTER 13

プライベート VLAN の設定

この章では、Catalyst 6500 シリーズ 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。

（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、次の URL で『*Catalyst Supervisor Engine 32 PISA Cisco IOS Command Reference*, Release 12.2ZY』を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/cmdref.html

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 の機能概要

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 ドメイン

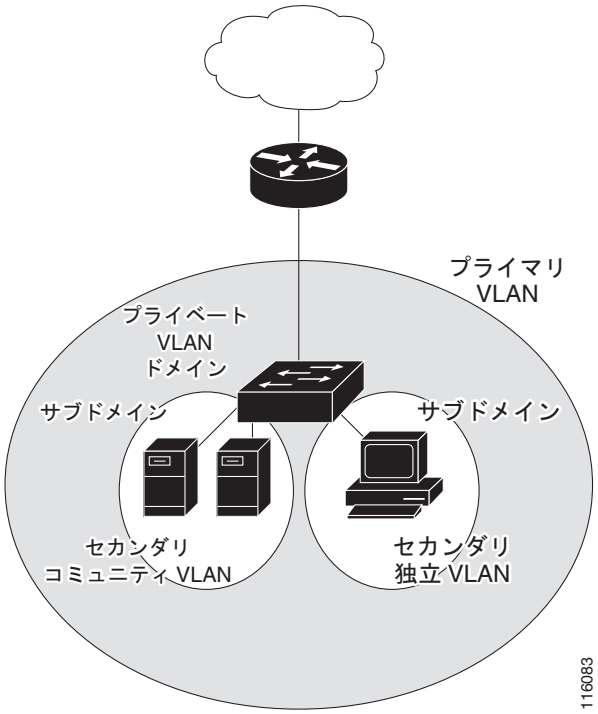
プライベート VLAN 機能では、サービス プロバイダー が VLAN を使用する際に直面する 2 つの問題に対処します。

- スイッチは、最大 4096 の 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は解決され、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 機能により、VLAN のレイヤ 2 ブロードキャスト 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 1 つの プライベート VLAN ペアです。プライベート VLAN ドメインには、複数のプライベート VLAN ペアが設定可能で、各サブドメインに 1 つのペアとなります。プライベート VLAN ドメイン内のすべての 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 13-1 を参照）。

図 13-1　プライベート VLAN ドメイン



プライベート VLAN ドメインには、プライマリ VLAN を 1 つだけ設定できます。プライベート VLAN ドメイン内のすべてのポートは、プライマリ VLAN のメンバーです。言い換えると、プライマリ VLAN はプライベート VLAN ドメイン全体となります。

セカンダリ VLAN は、同じ プライベート VLAN ドメイン内のポート間をレイヤ 2 で分離します。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 ポート

プライベート VLAN ポートには 3 つの種類があります。

- 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 に対応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 ドメイン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、独立ポート宛て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 ポートだけに転送されます。
- 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 ドメイン内の独立ポートからレイヤ 2 で分離されています。

（注）　トランクは独立ポート、コミュニティ ポート、およびプロミスキャス ポート間でトラフィックを伝達する VLAN をサポートできます。したがって、独立ポートおよびコミュニティ ポートのトラフィックはトランク インターフェイスを介してスイッチに送受信できます。

プライマリ、独立、およびコミュニティ VLAN

プライマリ VLAN および 2 種類のセカンダリ VLAN（独立 VLAN およびコミュニティ VLAN）には、次の特性があります。

- プライマリ VLAN：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 ドメインの独立 VLAN は、1 つだけです。独立 VLAN は、単一方向のトラフィックのアップストリームをホストからプロミスキャス ポートおよびゲートウェイに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 ドメイン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 ポートの独立

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。

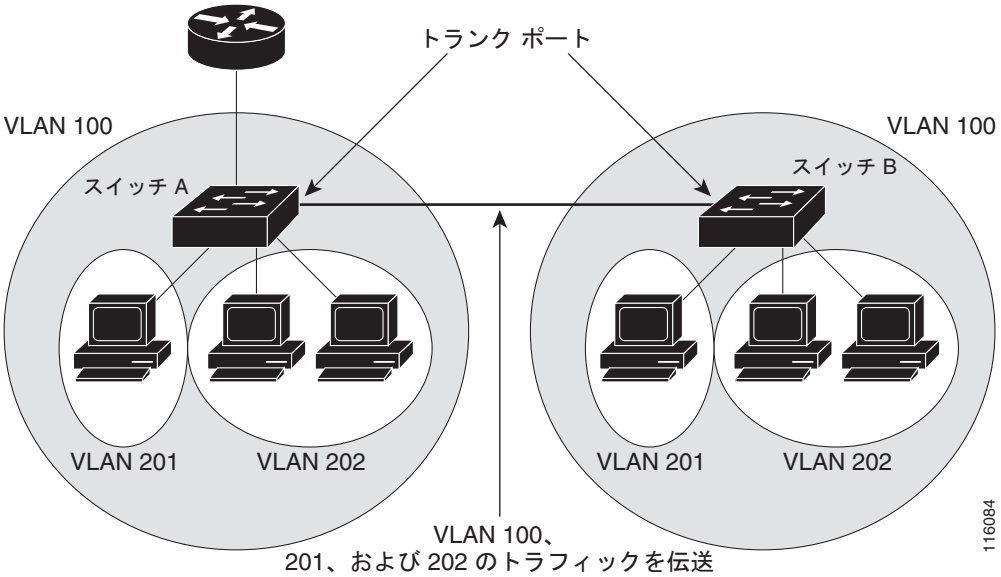
これらの問題は、プライベート VLAN を使用することで軽減されます。この場合、プライベート VLAN 内のすべてのメンバーは、プライマリ VLAN に割り当てられる共通のアドレス空間を共有します。ホストはセカンダリ VLAN に接続され、Dynamic Host Configuration Protocol（DHCP）サーバが プライマリ VLAN に割り当てられたアドレス ブロックから IP アドレスを割り当てます。同じプライマリ VLAN 内の別のセカンダリ VLAN 内のカスタマー装置に後続の IP アドレスを割り当てられます。新しい装置が追加された場合、DHCP サーバはサブネット 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 を近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 13-2 を参照）。

図 13-2　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

VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）は、プライベート VLAN をサポートしないため、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。この状況により、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。

プライベート VLAN の他の機能との相互作用

ここでは、プライベート VLAN の他の機能との相互作用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」（P.13-6）
- 「プライベート VLAN および SVI」（P.13-6）

「プライベート VLAN 設定時の注意事項および制約事項」（P.13-7）を参照してください。

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 ポートだけに送信します。
- 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

スイッチ仮想インターフェイス（SVI）は、レイヤ 2 VLAN のレイヤ 3 インターフェイスです。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。プライマリ VLAN に対してだけ、レイヤ 3 VLAN SVI を設定します。セカンダリ VLAN 用にレイヤ 3 VLAN インターフェイスを設定しないでください。VLAN がセカンダリ VLAN として設定されている場合、セカンダリ VLAN の SVI は非アクティブです。

- アクティブな SVI 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 設定時の注意事項および制約事項

プライベート VLAN の設定時の注意事項の内容は、次のとおりです。

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 を設定する場合、次の注意事項を考慮してください。

- プライベート VLAN を設定して、VTP をトランスポート モードに設定したあとは、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 11 章「VLAN トランキング プロトコル（VTP）の設定」を参照してください。
- プライベート VLAN を設定するには、VLAN コンフィギュレーション（config-vlan）モードを使用する必要があります。VLAN データベース コンフィギュレーション モードの場合は、プライベート VLAN を設定できません。VLAN 設定の詳細については、「VLAN の設定方法」（P.12-9）を参照してください。
- プライベート VLAN を設定後、**copy running-config startup config** イネーブル 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 startup-config ファイルに保存します。スイッチをリセットした場合は、プライベート VLAN をサポートするため、デフォルトの VTP トランスペアレント モードにする必要があります。
- VTP は、プライベート VLAN 設定を伝播しません。プライベート VLAN ポートを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。プライベート VLAN にできるのは、イーサネット VLAN に限られます。
- 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。
- 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 Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）パラメータ（ブリッジ プライオリティなど）はセカンダリ VLAN に伝播されます。ただし、他の装置に STP パラメータを伝播する必要はありません。VLAN が同一の転送データベースを適切に共有できるように、プライマリ、独立、およびコミュニティ VLAN のスパニング ツリー トポロジの一致を確認するには、STP 設定を手動で検証する必要があります。
- スイッチの MAC アドレス リダクション機能をイネーブルにする場合は、プライベート VLAN の STP トポロジが一致するように、ネットワーク内のすべての装置の MAC アドレス リダクション機能をイネーブルにするよう推奨します。

- プライベート VLAN が設定されているネットワーク内で、一部の装置の MAC アドレス リダクション機能をイネーブルにし、他の装置でディセーブルにした場合は（混在環境）、プライマリ VLAN や、関連付けられたすべての独立 VLAN およびコミュニティ VLAN に対してルート ブリッジが共通となるように、デフォルトのブリッジ プライオリティを使用します。MAC アドレス リダクション機能がシステム上でイネーブルであるかどうかに関係なく、この機能の対象範囲に矛盾がないようにしてください。MAC アドレス リダクション機能では個々のレベルだけが許可されています。すべての中間値は、範囲として内部的に使用されます。プライベート VLAN および MAC アドレス リダクション機能を持つルート ブリッジをディセーブルにし、ルート ブリッジとする装置に、ルート ブリッジ以外で使用される最も高いプライオリティの範囲よりもさらに高いプライオリティを設定する必要があります。
- セカンダリ VLAN には VACL を適用できません（第 32 章「VLAN アクセス制御リスト（VACL）の設定」を参照）。
- 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、その設定がプライマリ VLAN ですでに設定されている場合有効になりません。
- 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 QoS（Quality of Service）を適用できます （第 38 章「PFC QoS の設定」を参照）。
- プライベート VLAN を設定する場合に、sticky Address Resolution Protocol（ARP; アドレス解決プロトコル）がデフォルトでイネーブルとなり、レイヤ 3 プライベート VLAN インターフェイスで学習される ARP エントリは、sticky ARP エントリになります。セキュリティ上の理由から、プライベート VLAN ポートの sticky ARP エントリには期限切れがありません。sticky ARP の設定については、「sticky ARP の設定」（P.33-27）を参照してください。
- プライベート VLAN インターフェイスの ARP エントリを表示して確認することを推奨します。
- sticky ARP は、ARP エントリ（IP アドレス、MAC アドレス、および送信元 VLAN）が期限切れしないようにすることにより、MAC アドレス スプーフィングを防ぎます。sticky ARP はインターフェイス単位で設定できます。sticky ARP の設定については、「sticky ARP の設定」（P.33-27）を参照してください。プライベート VLAN sticky ARP には、次の注意事項および制約事項が適用されます。
  - レイヤ 3 プライベート VLAN インターフェイスで学習される ARP エントリは、sticky ARP エントリです。
  - MAC アドレスは違っても、IP アドレスが同じ装置を接続すると、メッセージが表示され、ARP エントリは作成されません。
  - プライベート VLAN ポートの sticky ARP エントリには期限がないため、MAC アドレスが変更された場合は、プライベート VLAN ポートの ARP エントリを手動で削除する必要があります。プライベート VLAN の ARP エントリを手動で追加または削除する方法は、次のとおりです。

```
Router(config)# no arp 11.1.3.30
IP ARP:Deleting Sticky ARP entry 11.1.3.30

Router(config)# arp 11.1.3.30 0000.5403.2356 arpa
IP ARP:Overwriting Sticky ARP entry 11.1.3.30, hw:00d0.bb09.266e by
hw:0000.5403.2356
```

- 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 アクセス マップの適用」（P.32-8）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。
- 発信されるすべてのプライベート VLAN トラフィックに Cisco IOS 出力 ACL を適用するには、プライマリ VLAN のレイヤ 3 VLAN インターフェイス上でこの ACL を設定します（第 30 章「ネットワーク セキュリティの設定」を参照）。
- プライマリ VLAN のレイヤ 3 VLAN インターフェイスに適用された Cisco IOS ACL は、関連する独立 VLAN およびコミュニティ VLAN にも自動的に適用されます。
- Cisco IOS ACL を独立 VLAN またはコミュニティ VLAN には適用しないでください。独立 VLAN およびコミュニティ VLAN に適用される Cisco IOS ACL の設定は、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。
- 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。
  - SPAN の詳細については、第 48 章「ローカル スイッチド ポート アナライザ（SPAN）、Remote SPAN（RSPAN）、および Encapsulated RSPAN（ERSPAN）の設定」を参照してください。

プライベート VLAN ポートの設定

プライベート VLAN ポートを設定する場合、次の注意事項を考慮してください。

- 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）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 の設定に含まれている間は、そのポートの EtherChannel 設定は非アクティブです。

- 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 18 章「オプションのスパニングツリー プロトコル（STP）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かぎりさまざまなネットワーク装置上で使用できます。
- プライベート VLAN 内で関連付けられているすべてのプライマリ、独立、およびコミュニティ VLAN は、トランク間で同じトポロジを維持する必要があります。同じトポロジを維持するためには、関連付けられた VLAN すべてで、同じ STP ブリッジ パラメータおよびトランク ポート パラメータを設定することを強く推奨します。

他の機能との制限事項

プライベート VLAN を設定する場合、次の他の機能との設定上の制限事項を考慮してください。

（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では、代替ブリッジングを設定しないでください。
- ポートが現在プライベート VLAN モードで、そのプライベート VLAN 設定では、ポートがプライマリ、独立、またはコミュニティ ポートであると示されている場合、ポートはプライベート VLAN 機能によってだけ影響されます。ポートがそれ以外のモード（Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）など）の場合、プライベート ポートとして機能しません。
- 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。
  - PAgP
  - LACP
  - 音声 VLAN
- 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、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。
- IEEE 802.1q マッピングは、通常どおり動作します。トラフィックは設定のとおり dot1Q ポートとの間で、Inter-Switch Link（ISL; スイッチ間リンク）VLAN から受信したかのように、再マッピングされます。
- プライベート VLAN のポート上でポート セキュリティを設定できます。
- Remote SPAN（RSPAN）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 48 章「ローカル スイッチド ポート アナライザ（SPAN）、Remote SPAN（RSPAN）、および Encapsulated RSPAN（ERSPAN）の設定」を参照してください。

- 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。
- 宛先 SPAN ポートを、独立ポートにしないでください（ただし、送信元 SPAN ポートは独立ポートにできます)。VSPAN は、プライマリ VLAN またはセカンダリ VLAN の両方にまたがるように設定できます。またはユーザが入力トラフィックか出力トラフィックだけに関係する場合は、いずれか 1 つを補うように設定することもできます。
- Supervisor Engine 1 でプロトコル フィルタリングがイネーブルである場合、プライベート VLAN ポートの必要な Local Target Logic（LTL）バケットすべてを適切なセカンダリ VLAN インデックスを使用してプログラミングする必要があります。
- 異なる VLAN 間でショートカットを使用する場合（これらの VLAN のいずれかがプライベートである場合)、プライマリ VLAN と独立 VLAN、コミュニティ VLAN の両方を考慮してください。セカンダリ VLAN（実際の送信元）は常にレイヤ 2 FID テーブルのプライマリ VLAN に再マッピングされるため、プライマリ VLAN を宛先および仮想送信元の両方として使用する必要があります。
- 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。

- プライベート VLAN ポートを EtherChannel 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 設定は非アクティブです。
- 12 ポートのグループをセカンダリ ポートとして設定する場合は、いくつかの制限事項があります。
  - 「12 ポート制限」が次の 10 Mb、10/100 Mb、100 Mb イーサネット スイッチング モジュールに適用されます。WS-X6324-100FX、WS-X6348-RJ-45、WS-X6348-RJ-45V、WS-X6348-RJ-21V、WS-X6248-RJ-45、WS-X6248A-TEL、WS-X6248-TEL、WS-X6148-RJ-45、WS-X6148-RJ-45V、WS-X6148-45AF、WS-X6148-RJ-21、WS-X6148-RJ-21V、WS-X6148-21AF、WS-X6024-10FL-MT (CSCea67876)

12 のポートからなるグループ（1 ～ 12、13 ～ 24、25 ～ 36、37 ～ 48）内のポートの 1 つが以下のいずれかである場合は、ポートを独立ポートまたはコミュニティ VLAN ポートとして設定しないでください。

- トランク ポート
- SPAN 宛先ポート
- プロミスキャス プライベート VLAN ポート
- CSCsb44185 が解決されているリリースの、**switchport mode dynamic auto** または **switchport mode dynamic desirable** コマンドで設定されているポート

12 個のポートの 1 つが上記のいずれかの場合、および上記の特性がある場合、他の 11 個のポートの独立またはコミュニティ VLAN 設定は非アクティブです。これらのポートを再びアクティブにするには、独立 VLAN ポートまたはコミュニティ VLAN ポートの設定を削除して、**shutdown** および **no shutdown** コマンドを入力します。

- 24 ポートのグループをセカンダリ ポートとして設定する場合は、いくつかの制限事項があります。

  すべてのリリースで、「24 ポート制限」が WS-X6548-GE-TX および WS-X6148-GE-TX 10/100/1000Mb イーサネット スイッチング モジュールに適用されます。

  24 のポートからなるグループ（1 ～ 24、25 ～ 48）内のポートの 1 つが以下のいずれかである場合は、ポートを独立ポートまたはコミュニティ VLAN ポートとして設定しないでください。

  - トランク ポート
  - SPAN 宛先ポート
  - プロミスキャス プライベート VLAN ポート
  - CSCsb44185 が解決されているリリースの、**switchport mode dynamic auto** または **switchport mode dynamic desirable** コマンドで設定されているポート

  24 個のポートの 1 つが上記のいずれかの場合、および上記の特性がある場合、他の 23 個のポートの独立またはコミュニティ VLAN 設定は非アクティブです。これらのポートを再びアクティブにするには、独立 VLAN ポートまたはコミュニティ VLAN ポートの設定を削除して、**shutdown** および **no shutdown** コマンドを入力します。

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。

（注） VLAN がまだ定義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 を定義します。

プライベート VLAN としての VLAN の設定

VLAN をプライベート VLAN として設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# vlan vlan_ID`	VLAN コンフィギュレーション サブモードを開始します。
ステップ 2	`Router(config-vlan)# private-vlan {community | isolated | primary}`	VLAN をプライベート VLAN として設定します。
	`Router(config-vlan)# no private-vlan {community | isolated | primary}`	プライベート VLAN の設定を消去します。 **（注）** これらのコマンドは、VLAN コンフィギュレーション サブモードを終了するまで有効になりません。
ステップ 3	`Router(config-vlan)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show vlan private-vlan [type]`	設定を確認します。

次に、VLAN 202 をプライマリ VLAN として設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# vlan 202
Router(config-vlan)# private-vlan primary
Router(config-vlan)# end
Router# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
```

次に、VLAN 303 をコミュニティ VLAN として設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# vlan 303
Router(config-vlan)# private-vlan community
Router(config-vlan)# end
Router# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
        303       community
```

次に、VLAN 440 を独立 VLAN として設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# vlan 440
Router(config-vlan)# private-vlan isolated
Router(config-vlan)# end
Router# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
        303       community
        440       isolated
```

セカンダリ VLAN とプライマリ VLAN の関連付け

セカンダリ VLAN をプライマリ VLAN に関連付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# vlan primary_vlan_ID`	プライマリ VLAN の VLAN コンフィギュレーション サブモードを開始します。
ステップ 2	`Router(config-vlan)# private-vlan association {secondary_vlan_list | add secondary_vlan_list | remove secondary_vlan_list}`	セカンダリ VLAN をプライマリ VLAN に関連付けます。
	`Router(config-vlan)# no private-vlan association`	セカンダリ VLAN の関連付けをすべて消去します。
ステップ 3	`Router(config-vlan)# end`	VLAN コンフィギュレーション モードを終了します。
ステップ 4	`Router# show vlan private-vlan [type]`	設定を確認します。

セカンダリ VLAN をプライマリ VLAN と関連付ける際、次の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入れないでください。カンマで区切って複数の項目を入力できます。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。
- *secondary_vlan_list* パラメータには、複数のコミュニティ VLAN ID を入れることができます。
- *secondary_vlan_list* パラメータには、1 つの独立 VLAN ID を入れることができます。
- 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 サブモードを終了するまで有効になりません。

次に、コミュニティ VLAN 303 ～ 307、309、および独立 VLAN 440 をプライマリ VLAN 202 に関連付けて、設定を確認する方法を示します。

```
Router# configure terminal
Router(config)# vlan 202
Router(config-vlan)# private-vlan association 303-307,309,440
Router(config-vlan)# end
Router# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202     303       community
202     304       community
202     305       community
202     306       community
202     307       community
202     309       community
202     440       isolated
        308       community
```

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

（注）　独立 VLAN およびコミュニティ VLAN は、ともにセカンダリ VLAN と呼ばれます。

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するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# 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 モードを開始します。
ステップ 2	`Router(config-if)# private-vlan mapping {secondary_vlan_list | add secondary_vlan_list | 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。
	`Router(config-if)# [no] private-vlan mapping`	セカンダリ VLAN とプライマリ VLAN の間のマッピングを消去します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show interface private-vlan mapping`	設定を確認します。

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は、次の情報に注意してください。

- **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 入力トラフィックにだけ作用します。
- *secondary_vlan_list* パラメータにはスペースを入れないでください。カンマで区切って複数の項目を入力できます。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 をプライマリ VLAN にマッピングするには、*secondary_vlan_list* パラメータを入力するか、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* パラメータを指定して **remove** キーワードを使用します。

次に、プライベート VLAN 303 ～ 307、309、および 440 からのセカンダリ VLAN 入力トラフィックのルーティングを許可して、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface vlan 202
Router(config-if)# private-vlan mapping add 303-307,309,440
Router(config-if)# end
Router# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan202   303            community
vlan202   304            community
vlan202   305            community
vlan202   306            community
vlan202   307            community
vlan202   309            community
vlan202   440            isolated

Router#
```

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 ポートとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport`	LAN ポートをレイヤ 2 スイッチング用に設定します。 • LAN ポートをレイヤ 2 インターフェイスとして設定するには、キーワードを指定せずに **switchport** コマンドを 1 度入力する必要があります。そのあとで、キーワードとともにさらに **switchport** コマンドを入力してください。 • インターフェイスに対して **switchport** コマンドを一度も入力していない場合に限り、必須です。
ステップ 3	`Router(config-if)# switchport mode private-vlan {host | promiscuous}`	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。
	`Router(config-if)# no switchport mode private-vlan`	プライベート VLAN ポートの設定を消去します。
ステップ 4	`Router(config-if)# 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 と関連付けます。
	`Router(config-if)# no switchport private-vlan host-association`	関連付けを消去します。
ステップ 5	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 6	`Router# show interfaces` [*type*[1] *slot/port*] `switchport`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、インターフェイス FastEthernet 5/1 をプライベート VLAN ホスト ポートとして設定して、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport mode private-vlan host
Router(config-if)# switchport private-vlan host-association 202 303
Router(config-if)# end
Router# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
→ Administrative Mode: private-vlan host
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
→ Administrative private-vlan host-association: 202 (VLAN0202) 303 (VLAN0303)
Administrative private-vlan mapping: none
→ Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

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 ポートとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定する LAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# switchport`	LAN インターフェイスをレイヤ 2 スイッチング用に設定します。 • LAN インターフェイスをレイヤ 2 インターフェイスとして設定するには、キーワードを指定せずに **switchport** コマンドを 1 度入力する必要があります。そのあとで、キーワードとともにさらに **switchport** コマンドを入力してください。 • インターフェイスに対して **switchport** コマンドを一度も入力していない場合に限り、必須です。
ステップ 3	`Router(config-if)# switchport mode private-vlan {host | 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。
	`Router(config-if)# no switchport mode private-vlan`	プライベート VLAN ポートの設定を消去します。
ステップ 4	`Router(config-if)# switchport private-vlan mapping` *primary_vlan_ID* {*secondary_vlan_list* | **add** *secondary_vlan_list* | **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。
	`Router(config-if)# no switchport private-vlan mapping`	プライベート VLAN プロミスキャス ポートと、プライマリ VLAN やセカンダリ VLAN の間のマッピングを消去します。

	コマンド	目的
ステップ 5	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 6	`Router# show interfaces [type[1] slot/port] switchport`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

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、次の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入れないでください。カンマで区切って複数の項目を入力できます。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 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* の値を入力するか、または *secondary_vlan_list* の値を指定して **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* の値を指定して **remove** キーワードを使用します。

次に、インターフェイス FastEthernet 5/2 をプライベート VLAN プロミスキャス ポートとして設定し、そのインターフェイスをプライベート VLAN にマッピングする例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/2
Router(config-if)# switchport mode private-vlan promiscuous
Router(config-if)# switchport private-vlan mapping 202 303,440
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
→ Administrative Mode: private-vlan promiscuous
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none ((Inactive))
→ Administrative private-vlan mapping: 202 (VLAN0202) 303 (VLAN0303) 440 (VLAN0440)
→ Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

プライベート VLAN のモニタ

表 13-1 に、プライベート VLAN のアクティビティをモニタするためのイネーブル EXEC コマンドを示します。

表 13-1　プライベート VLAN のモニタ コマンド

コマンド	目的
show interfaces status	インターフェイス（それが属する VLAN を含む）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          Fa2/1, Gi3/1, Gi3/2
10      502       community         Fa2/11, Gi3/1, Gi3/4
10      503       non-operational
```