CHAPTER 26

# プライベート VLAN



（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、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

## プライベート VLAN の前提条件

なし。

## プライベート VLAN の制約事項

# セカンダリ VLAN およびプライマリ VLAN

- プライベート VLAN を設定して、VTP をトランスペアレント モードに設定した後は、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 については、第 24 章「VLAN トランキング プロトコル（VTP）」を参照してください。
- プライベート VLAN の設定後は、**copy running-config startup config** 特権 EXEC コマンドを使用して、VTP トランスペアレント モード設定およびプライベート VLAN 設定を startup-config ファイルに保存してください。スイッチがリセットした場合、プライベート VLAN をサポートするためにデフォルトで VTP トランスペアレント モードになる必要があります。
- VTP バージョン 1 および 2 では、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。VTP バージョン 3 では、VTP はプライベート VLAN 設定を自動的に伝播します。
- 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せん。イーサネット VLAN だけをプライベート VLAN に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。
- セカンダリ VLAN をプライマリ VLAN に関連付けられている場合、ブリッジ プライオリティなどのプライマリ VLAN の STP パラメータは、セカンダリ VLAN に伝播されます。ただし、STP パラメータが必ずしもその他のデバイスに伝播されるとはかぎりません。STP 設定を手動でチェックして、プライマリ VLAN、独立 VLAN、コミュニティ VLAN のスパニングツリー トポロジが一致することを確認してください。これらの VLAN が同じ転送データベースを適切に共有できるようにするためです。
- 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デバイス上で MAC アドレス リダクション機能をイネーブルにする必要があります。
- プライベート VLAN が設定されているネットワーク内で、一部のデバイスの MAC アドレス リダクション機能をイネーブルにし、他のデバイス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 リダクションは個々のレベルにしか対応せず、範囲としてはすべての中間値を内部的に使用します。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 VLAN ACL（VACL）を適用できません（第 67 章「VLAN ACL（VACL）」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 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 （第 58 章「PFC QoS」を参照）。

- プライベート VLAN を設定すると、スティッキ アドレス解決プロトコル（ARP）がデフォルトでイネーブルになり、レイヤ 3 プライベート VLAN インターフェイスで学習した ARP エントリはスティッキ 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 ポートのスティッキ ARP エントリには期限切れがありません。スティッキ ARP の設定については、「スティッキ ARP の設定」（P.69-22）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。
- スティッキ 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。スティッキ ARP はインターフェイスごとに設定できます。スティッキ ARP の設定については、「スティッキ ARP の設定」（P.69-22）を参照してください。次の注意事項および制約事項が、プライベート VLAN のスティッキ ARP に適用されます。
  - レイヤ 3 プライベート VLAN インターフェイスで学習した ARP エントリは、スティッキ ARP エントリです。
  - IP アドレスが同じでも、MAC アドレスが異なるデバイスを接続すると、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 ポートのスティッキ 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 VLAN マップを設定できます（「VLAN アクセス マップの適用」（P.67-5）を参照）。ただし、プライベート VLAN のプライマリ VLAN およびセカンダリ VLAN では、同一 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 内においてレイヤ 2 で転送されると、入力側と出力側で同じ VLAN マップが適用されます。プライベート VLAN 内部から外部ポートにフレームがルーティングされると、プライベート VLAN マップが入力側で適用されます。
  - 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。
- 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 65 章「MAC アドレスベースのトラフィック ブロッキング」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 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; VLAN ベースの SPAN）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 53 章「ローカル SPAN、RSPAN、および ERSPAN」を参照してください。

# プライベート VLAN ポート

- 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。
- 設定ミスによって STP ループが発生しないようにして、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（第 31 章「オプションの STP 機能」を参照）。イネーブルにすると、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。無差別ポートでは、PortFast および BPDU ガード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。
- 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 に関連するすべてのプライマリ VLAN、独立 VLAN、コミュニティ VLAN では、トランク間で同一トポロジーを維持する必要があります。すべての関連 VLAN で同じ STP ブリッジ パラメータとトランク ポート パラメータを設定し、同一トポロジーを維持することを強く推奨します。

# その他の機能の制限事項

- VTP バージョン 3 はプライベート VLAN（PVLAN）ポートではサポートされません。
- 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。
- ポートが現在プライベート VLAN モードになっており、ポートがプライマリ ポート、独立ポート、コミュニティ ポートのうちのいずれかであることをプライベート VLAN 設定が示している場合、ポートはプライベート VLAN 機能だけに影響されます。ダイナミック トランキング プロトコル（DTP）などのその他のモードにポートがなっている場合、ポートはプライベート ポートとして機能しません。

- 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。
  - ポート集約プロトコル（PAgP）
  - リンク集約制御プロトコル（LACP）
  - 音声 VLAN
- 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 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。SPAN の詳細については、第 53 章「ローカル SPAN、RSPAN、および ERSPAN」を参照してください。
- 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。
- 宛先 SPAN ポートを独立ポートにしないでください。送信元 SPAN ポートを独立ポートにすることはできます。VSPAN を設定して、プライマリ VLAN およびセカンダリ VLAN の両方を拡張するか、入力トラフィックまたは出力トラフィックだけが重要な場合はそのどちらかを拡張できます。
- 各 VLAN 間でショートカットを使用する場合（このうちいずれかの VLAN がプライベート VLAN である場合）は、プライマリ VLAN、独立 VLAN、コミュニティ VLAN を考慮してください。プライマリ VLAN は、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。セカンダリ VLAN（真の送信元）が、レイヤ 2 FID テーブルでプライマリ VLAN に常に再マッピングされるからです。
- 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。

- 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。ポートはプライベート VLAN 設定の一部にすることができますが、ポートの EtherChannel 設定はいずれも非アクティブになります。

# プライベート VLAN について

# プライベート VLAN ドメイン

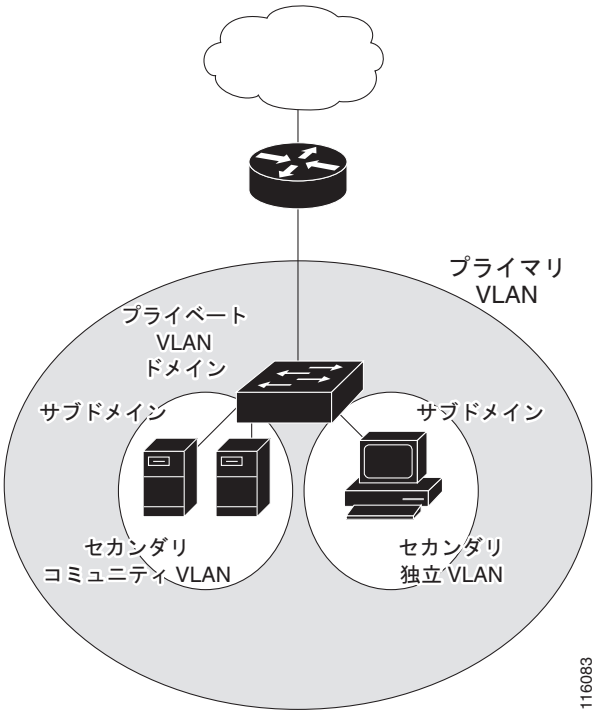
プライベート VLAN 機能では、サービス プロバイダーが VLAN の使用時に直面する、次の 2 つの問題に対処します。

- スイッチがサポートする VLAN は最大で 4096 です。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 とセカンダリ VLAN で構成されるプライベート VLAN のペアで表されます。プライベート VLAN ドメインには複数のプライベート VLAN のペアを設定でき、それぞれのペアを各サブドメインに割り当てることができます。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 は、サブドメインを識別します（図 26-1 を参照）。

**図 26-1　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 が 1 つのみ含まれています。プライベート VLAN ドメインのポートはすべて、プライマリ VLAN のメンバです。言い換えれば、プライマリ VLAN はプライベート VLAN ドメイン全体です。

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 内のポートは相互に通信できますが、レイヤ 2 レベルでその他のコミュニティ内のポートと通信できません。

# プライベート VLAN ポート

プライベート VLAN ポートには 3 種類があります。

- 無差別：無差別ポートはプライマリ VLAN に属し、プライマリ VLAN に関連付けられたセカンダリ 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 ポートも含めて、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、無差別ポートを除く、同一プライベート VLAN ドメインのそ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 ドメイン内の独立ポートとレイヤ 2 で分離されます。

（注）　トランクは独立ポート、コミュニティ ポート、および無差別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 VLAN、独立 VLAN、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：無差別ポートからホスト ポート（独立とコミュニティ）およびその他の無差別ポートへの単一方向トラフィック ダウンストリームを搬送します。
- 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。プライベート VLAN には、複数のコミュニティ VLAN を設定できます。

無差別ポートは、1 つのみのプライマリ VLAN、1 つの独立 VLAN、複数のコミュニティ VLAN を処理できます。レイヤ 3 ゲートウェイは一般的に、無差別ポートを介してスイッチに接続されます。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モニタ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。

スイッチド環境では、個々の VLAN および対応する IP サブネットを、個々のステーションまたはステーションの共通のグループに割り当てることができます。エンド ステーションは、プライベート VLAN の外部にアクセスするために、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 ポートの分離

プライベート VLAN を使用すると、次のようにエンド 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 による IP アドレス指定方式

それぞれのカスタマーに別々の VLAN を割り当てると、次のように非効率的な IP アドレス指定方式が作成されます。

- 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 におけるデバイス数が増加する場合、割り当て済みアドレス数が増加に対応できるだけ十分に大きくないことがあります。

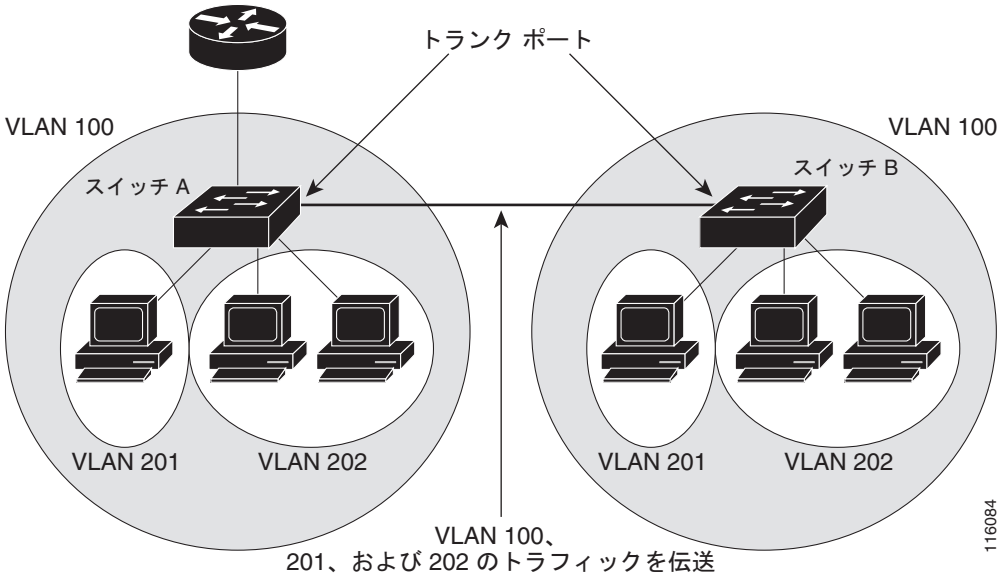
この問題は、プライベート VLAN を使用すると軽減します。プライベート VLAN では、プライベート VLAN のすべてのメンバが、プライマリ VLAN に割り当てられている共通アドレス空間を共有するためです。ホストはセカンダリ VLAN に接続され、プライマリ VLAN に割り当てられているアドレスのブロックから IP アドレスが DHCP サーバによってホストに割り当てられますが、同一プライマリ VLAN 内のセカンダリ VLAN には割り当てられません。さまざまなセカンダリ VLAN のカスタマー デバイスには後続 IP アドレスが割り当てられます。新しいデバイスを追加すると、サブネッ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

達しません。（図 26-2 を参照）。

**図 26-2　　複数のスイッチにまたがるプライベート VLAN**




VLAN 100 = プライマリ VLAN
VLAN 201 = セカンダリ独立 VLAN
VLAN 202 = セカンダリ コミュニティ VLAN

VTP バージョン 1 および 2 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。

VTP バージョン 3 はプライベート VLAN をサポートしているため、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はありません。

# 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 の場合、同一 VLAN の各デバイスはレイヤ 2 レベルで相互に通信できますが、別々の VLAN のインターフェイスに接続しているデバイスはレイヤ 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、無差別ポートはプライマリ VLAN のメンバであり、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 に関連付けられているので、これらの VLAN のメンバはレイヤ 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 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、無差別ポートまたはトランク ポートのみ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、同じコミュニティ 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（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、同じ独立 VLAN のポート間、または別々のセカンダリ VLAN のポート間では転送されません。

### 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、レイヤ 2 VLAN のレイヤ 3 インターフェイスです。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。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 にはレイヤ 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間、セカンダリ VLAN の SVI は非アクティブになります。

- アクティブな SVI が設定された VLAN をセカンダリ VLAN として設定しようとすると、SVI をディセーブルにするまでは、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 で SVI を作成し、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場合、SVI は作成されずに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、マッピングされている場合、プライマリ VLAN 上のすべての設定がセカンダリ VLAN SVI に伝播されます。たとえば、プライマリ VLAN 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 のデフォルト設定

なし。

# プライベート VLAN の設定方法

- 「プライベート VLAN としての VLAN の設定」（P.26-11）
- 「セカンダリ VLAN とプライマリ VLAN の関連付け」（P.26-12）
- 「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」（P.26-13）
- 「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.26-14）
- 「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」（P.26-15）

（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。<br>（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実行されません。 |
| 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。 |

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、次の作業を実行します。

| | 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。 |
| 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。 |

セカンダリ VLAN をプライマリ VLAN と関連付ける際は、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 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 を含めることができます。
- *secondary_vlan_list* パラメータには、独立 VLAN ID を 1 つだけ含めることができます。
- セカンダリ VLAN とプライマリ VLAN を関連付けるには、*secondary_vlan_list* を入力するか、*secondary_vlan_list* に **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 間の関連付けを消去するには、*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 サブモードを終了しない限り、有効になりません。

次の例は、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。 |

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 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、*secondary_vlan_list* パラメータに **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 間のマッピングを消去するには、*secondary_vlan_list* パラメータに **remove** キーワードを使用します。

次の例は、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 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。<br>• 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。<br>• 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かぎり、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。 |
| 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。<br>**（注）** VLAN のロックがイネーブルになっている場合は、VLAN の番号の代わりに VLAN の名前を入力します。詳細については、「VLAN ロック」（P.25-5）を参照してください。 |
| 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。 |

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

```
Router# configure terminal
Router(config)# interface gigabitethernet 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 gigabitethernet 5/1 switchport | include private-vlan
Administrative Mode: private-vlan host
Administrative private-vlan host-association: 202 (VLAN0202) 303 (VLAN0303)
Administrative private-vlan mapping: none
Operational private-vlan: none
```

# 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 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。<br>• 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** コマンドを一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。<br>• 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かぎり、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 無差別ポートとして設定します。 |
| 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 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。<br>（注）　VLAN のロックがイネーブルになっている場合は、VLAN の番号の代わりに VLAN の名前を入力します。詳細については、「VLAN ロック」（P.25-5）を参照してください。 |
| | `Router(config-if)# no switchport private-vlan mapping` | プライベート VLAN 無差別ポートと、プライマリ VLAN および任意のセカンダリ VLAN 間のすべてのマッピングを消去します。 |
| 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。 |

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する際は、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 の範囲です。
- VLAN ロックがイネーブルになっている場合は、VLAN の番号の代わりに VLAN の名前を *secondary_vlan_list* に入力します。VLAN の名前の範囲を入力する場合は、VLAN の名前とダッシュの間にスペースを入力してください。
- セカンダリ 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* 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 無差別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 GigabitEthernet 5/2 をプライベート VLAN 無差別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 gigabitethernet 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 gigabitethernet 5/2 switchport | include private-vlan
Administrative Mode: private-vlan promiscuous
Administrative private-vlan host-association: none ((Inactive))
Administrative private-vlan mapping: 202 (VLAN0202) 303 (VLAN0303) 440 (VLAN0440)
Operational private-vlan: none
```

# プライベート VLAN のモニタ

表 26-1 は、プライベート VLAN アクティビティをモニタするための特権 EXEC コマンドを示しています。

**表 26-1　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** | インターフェイスが属している VLAN を含めて、インターフェイスのステータスを表示します。 |
| **show vlan private-vlan** [**type**] | スイッチのプライベート VLAN 情報を表示します。 |
| **show interface switchport** | インターフェイス上のプライベート VLAN 設定を表示します。 |
| **show interface private-vlan mapping** | VLAN SVI のプライベート VLAN マッピングに関する情報を表示します。 |

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

```
Switch(config)# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Gi2/1, Gi3/1, Gi3/2
10      502       community         Gi2/11, Gi3/1, Gi3/4
10      503       non-operational
```

**ヒント** Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する