CHAPTER 4

プライベート VLAN の設定

この章では、プライベート VLAN を設定する手順について説明します。プライベート VLAN は、レイヤ 2 レベルでさらなる保護機能を提供します。

この章の内容は、次のとおりです。

- プライベート VLAN について（p.4-2）
- プライベート VLAN のライセンス要件（p.4-8）
- プライベート VLAN の前提条件（p.4-8）
- 注意事項および制限（p.4-9）
- プライベート VLAN の設定（p.4-12）
- プライベート VLAN 設定の確認（p.4-22）
- プライベート VLAN の統計情報の表示とクリア（p.4-22）
- プライベート VLAN の設定例（p.4-23）
- デフォルト設定（p.4-23）
- 追加情報（p.4-24）

（注） レイヤ 3 VLAN インターフェイスまたは Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）の IP アドレス指定の詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

プライベート VLAN について

（注）　レイヤ 2 ポートは、トランク ポート、アクセス ポート、またはプライベート VLAN ポートとして機能します。

（注）　この機能を設定する前に、プライベート VLAN 機能をイネーブルにする必要があります。

同様のシステム間で直接通信する必要がない特定の状況では、プライベート VLAN により、レイヤ 2 レベルの保護を強化できます。プライベート VLAN は、プライマリ VLAN とセカンダリ VLAN のアソシエーションです。

プライマリ VLAN は、セカンダリ VLAN を関連付けるブロードキャスト ドメインを定義します。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のどちらかです（独立 VLAN およびコミュニティ VLAN の詳細は、「セカンダリ VLAN およびプライマリ VLAN の設定」[p.4-9] を参照してください）。独立 VLAN 上のホストは、プライマリ VLAN 内で関連付けられた混合ポートとだけ通信します。コミュニティ VLAN 上のホストは、同じコミュニティ VLAN 上のホスト間および関連付けられた無差別ポートとだけ通信し、独立ポートまたは他のコミュニティ VLAN 内のポートとは通信しません（プライベート VLAN のポート タイプの詳細は、「プライベート VLAN ポートの設定」[p.4-10] を参照してください）。

統合スイッチングおよびルーティング機能を使用するコンフィギュレーションでは、各プライベート VLAN に単一のレイヤ 3 VLAN インターフェイスまたは SVI を割り当てることにより、ルーティングを提供できます。SVI は、プライマリ VLAN 用に作成します。このようなコンフィギュレーションでは、セカンダリ VLAN はすべて、プライマリ VLAN 上の SVI とのマッピングにより、レイヤ 3 でのみ通信します。セカンダリ VLAN 上の既存の SVI は、すべてサービス停止状態になります。

ここでは、次の内容について説明します。

- プライベート VLAN の概要（p.4-2）
- ハイ アベイラビリティ（p.4-8）
- バーチャライゼーションのサポート（p.4-8）

プライベート VLAN の概要

デバイスでプライベート VLAN 機能を適用するには、プライベート VLAN をイネーブルにする必要があります。

プライベート VLAN モードで動作しているポートがデバイスに設定されている場合は、プライベート VLAN をディセーブルにすることはできません。

（注）　特定の VLAN をプライマリまたはセカンダリのどちらかのプライベート VLAN として設定するには、事前に VLAN が作成しておく必要があります（VLAN の作成については、第 3 章「VLAN の設定」を参照してください）。

ここでは、次の内容について説明します。

- プライベート VLAN のプライマリ VLAN とセカンダリ VLAN（p.4-3）
- プライベート VLAN ポート（p.4-3）
- プライマリ、独立、およびコミュニティ プライベート VLAN（p.4-4）
- プライマリ VLAN とセカンダリ VLAN の関連付け（p.4-6）
- プライベート VLAN 内のブロードキャスト トラフィック（p.4-6）
- プライベート VLAN ポートの分離（p.4-7）
- プライベート VLAN および VLAN インターフェイス（p.4-7）
- 複数のデバイスにまたがるプライベート VLAN（p.4-7）

プライベート VLAN のプライマリ VLAN とセカンダリ VLAN

プライベート VLAN 機能では、VLAN の使用時にユーザが直面する 2 つの問題に対処できます。

- 各 Virtual Device Context（VDC）は、最大 4096 の VLAN をサポートします。各カスタマーに 1 つの VLAN を割り当てると、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が解決され、IP アドレスの管理が容易になり、カスタマーにレイヤ 2 セキュリティが提供されます。

プライベート VLAN の機能は、VLAN のレイヤ 2 ブロードキャスト ドメインをサブドメインに分割できます。サブドメインは、1 つのプライベート VLAN ペアで、プライマリ VLAN とセカンダリ VLAN で構成されます。プライベート VLAN ドメインには、各サブドメインに 1 ペアずつ、複数のプライベート VLAN ペアを設定できます。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。各サブドメインは、セカンダリ VLAN ID で識別します。

（注）　プライベート VLAN ドメインに設定できるプライマリ VLAN は 1 つだけです。

セカンダリ VLAN は、同じ VLAN 内のポートをレイヤ 2 で分離します。プライマリ VLAN 内のセカンダリ VLAN には、次の 2 つのタイプがあります。

- 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 レベルの他のコミュニティ VLAN 内または独立 VLAN 内のポートとは通信できません。

プライベート VLAN ポート

（注）　コミュニティ プライベート VLAN および独立プライベート VLAN のポートは、いずれも PVLAN ホスト ポートというラベルが付けられます。PVLAN ホスト ポートは、関連付けられているセカンダリ VLAN のタイプによって、コミュニティ PVLAN ポートまたは独立 PVLAN ポートのどちらかになります。

プライベート VLAN ポートには、次のタイプがあります。

- 無差別 — 無差別ポートは、プライマリ VLAN に属します。無差別ポートは、コミュニティ ホスト ポートおよび独立ホスト ポートを含め、セカンダリ VLAN に属していて、無差別ポートとプライマリ VLAN に*関連付けられている*すべてのインターフェイスと通信できます。プライマリ VLAN には、複数の無差別ポートを設定できます。各無差別ポートには、複数のセカンダリ VLAN を関連付けることができますが、セカンダリ VLAN を関連付けなくてもかまいません。無差別ポートとセカンダリ VLAN が同じプライマリ VLAN 内にあれば、1 つのセカンダリ VLAN を複数の無差別ポートに関連付けることができます。このアソシエーション（関連付け）は、ロード バランシングまたは冗長性のために使用することもできます。セカンダリ VLAN に無差別ポートを関連付けないこともできますが、その場合、セカンダリ VLAN はレイヤ 3 インターフェイスと通信できません。
- 独立 — 独立ポートは、独立セカンダリ VLAN に属すホスト ポートです。このポートは、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が、関連付けられた無差別ポートとは通信できます。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したトラフィックは、無差別ポートにのみ転送されます。特定の独立 VLAN に複数の独立ポートを設定し、その独立 VLAN 内で各ポートを他のすべてのポートから完全に分離できます。
- 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関連付けられた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、他のコミュニティにある他のすべてのインターフェイスおよびプライベート VLAN ドメイン内のすべての独立ポートから、レイヤ 2 で分離されています。

（注）　トランクは、無差別、独立、およびコミュニティの各ポート間のトラフィックを伝送する VLAN をサポートできるので、独立ポートとコミュニティ ポートのトラフィックはトランク インターフェイスを経由してデバイスと送受信されることがあります。

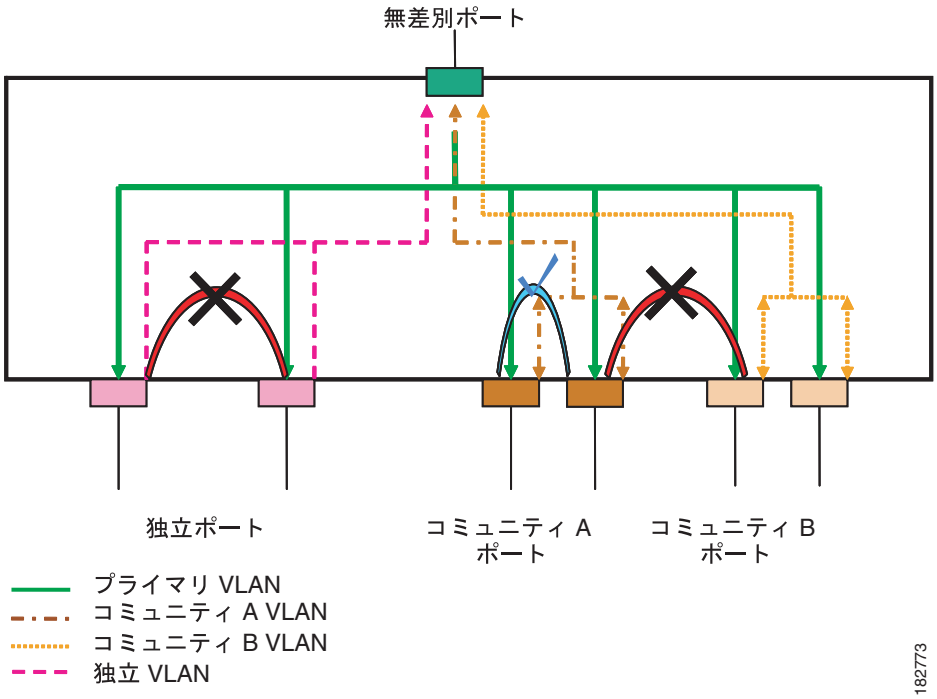
プライマリ、独立、およびコミュニティ プライベート VLAN

プライマリ VLAN にはレイヤ 3 ゲートウェイがあるので、プライベート VLAN の外部と通信するには、セカンダリ VLAN をプライマリ VLAN に関連付けます。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、無差別ポートから（独立およびコミュニティ）ホスト ポートおよび他の無差別ポートへのトラフィックを伝送します。
- 独立 VLAN — 独立 VLAN は、ホストから無差別ポートおよびレイヤ 3 ゲートウェイへの単方向アップストリーム トラフィックを伝送するセカンダリ VLAN です。プライベート VLAN ドメインに複数の独立 VLAN を設定し、各 VLAN 内のトラフィックを分離できます。また、各独立 VLAN に複数の独立ポートを設定し、各独立ポートからのトラフィックを完全に分離することもできます。
- 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。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。これらのポートは、同じコミュニティ内のポートとは相互に通信できますが、プライベート VLAN 内の他のコミュニティ VLAN 内または独立 VLAN 内のポートとは通信できません。

図 4-1 に、プライマリまたはプライベート VLAN 内のレイヤ 2 トラフィック フロー、および VLAN のタイプとポートのタイプを示します。

図 4-1　プライベート VLAN のレイヤ 2 トラフィック フロー



（注）　プライベート VLAN のトラフィック フローは、ホスト ポートから無差別ポートへの単方向です。無差別ポートから*出力*されるトラフィックは、標準 VLAN 内のトラフィックと同様に処理され、関連付けられたセカンダリ VLAN でトラフィックが分離されることはありません。

無差別ポートは 1 つのプライマリ VLAN の専用ポートになりますが、複数の独立 VLAN および複数のコミュニティ VLAN で使用できます（レイヤ 3 ゲートウェイは通常、無差別ポート経由でデバイスに接続されます）。無差別ポートを使用すると、さまざまなデバイスをアクセス 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、無差別ポートを使用して、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。

プライマリ VLAN には複数の無差別ポートを設定できますが、各プライマリ VLAN に設定できるレイヤ 3 ゲートウェイは *1* つだけです。

スイッチング環境では、個々の端末または共通グループの端末に、個別のプライベート VLAN および関連する IP サブネットを割り当てることができます。端末は、プライベート VLAN の外側と通信する場合、デフォルト ゲートウェイのみと通信する必要があります。

（注）　レイヤ 3 ゲートウェイまたは SVI を設定するには、VLAN インターフェイス機能をイネーブルにしておく必要があります。SVI および IP アドレス指定の詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

プライマリ VLAN とセカンダリ VLAN の関連付け

セカンダリ VLAN 内のホスト ポートでプライベート VLAN 外と通信するには、セカンダリ VLAN をプライマリ VLAN に関連付ける必要があります。アソシエーションが正常に動作していない場合、セカンダリ VLAN のホスト ポート（独立ポートおよびコミュニティ ポート）はダウン ステートになります。

（注）　セカンダリ VLAN は、1 つのプライマリ VLAN にのみ関連付けることができます。

アソシエーションを正常に動作させるには、次の条件が満たされている必要があります。

- プライマリ VLAN が存在する。
- セカンダリ VLAN が存在する。
- プライマリ VLAN がプライマリ VLAN として設定されている。
- セカンダリ VLAN が、独立 VLAN またはコミュニティ VLAN として設定されている。

（注）　アソシエーションが動作しているかどうかを確認するには、**show** コマンドの出力を調べます。アソシエーションが動作していなくても、エラー メッセージは発行されません（設定の確認については、「プライベート VLAN 設定の確認」[p.4-22] を参照してください）。

プライマリ VLAN またはセカンダリ VLAN のどちらかを削除すると、その VLAN に関連付けられているポートは非アクティブになります。**no private-vlan** コマンドを入力すると、VLAN は標準 VLAN モードに戻ります。その VLAN 上のアソシエーションはすべて一時停止されますが、インターフェイスはプライベート VLAN モードのままです。特定の VLAN をプライベート VLAN モードに再変換すると、元のアソシエーションが復元されます。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN のすべてのプライベート VLAN アソシエーションが削除されます。ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力した場合には、その VLAN のプライベート VLAN アソシエーションは一時停止するだけです。VLAN を再作成して、元のセカンダリ VLAN として設定すると、アソシエーションが再開されます。

セカンダリ VLAN とプライマリ VLAN 間のアソシエーションを変更するには、最初に現在のアソシエーションを削除してから、新しいアソシエーションを追加します。

プライベート VLAN 内のブロードキャスト トラフィック

プライベート VLAN 内のポートからのブロードキャスト トラフィックは、次のように伝送されます。

- 無差別ポートからのブロードキャスト トラフィックは、プライマリ VLAN 内のすべてのポートに伝送されます。このブロードキャスト トラフィックは、プライベート VLAN パラメータが設定されていないポートも含め、プライマリ VLAN 内のすべてのポートに配信されます。
- 独立ポートからのブロードキャスト トラフィックは、その独立ポートが関連付けられているプライマリ VLAN 内の無差別ポートだけに配信されます。
- コミュニティ ポートからのブロードキャスト トラフィックは、そのポートのコミュニティ内のすべてのポート、およびそのコミュニティ ポートに関連付けられているすべての無差別ポートに配信されます。このブロードキャスト パケットは、プライマリ VLAN 内の他のコミュニティまたは独立ポートには配信されません。

プライベート VLAN ポートの分離

プライベート VLAN を使用して、端末へのアクセスを次のように制御できます。

- 端末に接続している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 での通信が阻止されます。たとえば、端末がサーバである場合、この設定により、サーバ間のレイヤ 2 通信が阻止されます。
- デフォルト ゲートウェイおよび特定の端末（バックアップ サーバなど）に接続しているインターフェイスを無差別ポートとして設定すると、すべての端末からデフォルト ゲートウェイへのアクセスが許可されます。

プライベート VLAN および VLAN インターフェイス

レイヤ 2 VLAN への VLAN インターフェイスは、Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）とも呼ばれます。レイヤ 3 デバイスは、セカンダリ VLAN ではなく、プライマリ VLAN を介してのみプライベート VLAN と通信します。

VLAN インターフェイスは、プライマリ VLAN に対してのみ設定します。セカンダリ VLAN には 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 VLAN インターフェイスまたは SVI は非アクティブになります。VLAN インターフェイスの設定が正しくない場合、次のような状況になります。

- アクティブな VLAN インターフェイスまたは 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、VLAN インターフェイス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 上で VLAN インターフェイスまたは SVI を作成してイネーブルにしようとすると、その VLAN インターフェイスはディセーブルのままで、システムからエラーが返されます。

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 に伝播されます。たとえば、プライマリ VLAN 上のレイヤ 3 VLAN インターフェイスまたは 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。

（注）　VLAN インターフェイスを設定するには、VLAN インターフェイス機能をイネーブルにしておく必要があります。VLAN インターフェイスおよび IP アドレス指定の詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

複数のデバイスにまたがるプライベート VLAN

プライベート VLAN を複数の装置にわたるように拡張するには、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。プライベート VLAN 設定のセキュリティを保持して、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 ポートが設定されていないデバイスを含め、すべての中間デバイスにプライベート VLAN を設定します。

ハイ アベイラビリティ

このソフトウェアは、コールド リブート時に、プライベート VLAN のステートフルおよびステートレスの両方の再起動において、ハイ アベイラビリティをサポートしています。ステートフルな再起動では、再試行は最大 3 回までサポートされます。再起動から 10 秒以内に 4 回以上の再試行を行うと、スーパーバイザ モジュールがリロードされます。

プライベート VLAN ごとに、ソフトウェアのアップグレードまたはダウングレードをシームレスに実行できます。

（注）　ハイ アベイラビリティ機能の詳細については、『*Cisco NX-OS High Availability and Redundancy Configuration Guide* 』を参照してください。

バーチャライゼーションのサポート

ソフトウェアは、Virtual Device Context（VDC）をサポートしています。

（注）　VDC およびリソース割り当ての詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』を参照してください。

各 VLAN は、プライマリ VLAN およびすべてのセカンダリ VLAN のプライベート VLAN ポートが、すべて同じ VDC に属している必要があります。プライベート VLAN は、複数の VDC に対しては設定できません。

プライベート VLAN のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
NX-OS	プライベート VLAN のライセンスは不要です。ライセンス パッケージに含まれていない機能は Cisco NX-OS システム イメージにバンドルされ、追加料金なしで提供されます。NX-OS ライセンス機構の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ただし、VDC を使用するには、Advanced Services ライセンスが必要です。

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。

- デバイスにログオンしている必要があります。
- 必要に応じて、Advanced Services ライセンスをインストールし、特定の VDC を開始します。
- プライベート VLAN 機能をイネーブルにする必要があります。

注意事項および制限

プライベート VLAN 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（p.4-9）
- プライベート VLAN ポートの設定（p.4-10）
- 他の機能に関連する制限（p.4-10）

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。

- デフォルト VLAN（VLAN1）または内部的に割り当てられた VLAN を、プライマリ VLAN またはセカンダリ VLAN として設定することはできません。
- 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。
- 1 つのプライマリ VLAN に、複数の独立 VLAN およびコミュニティ 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 は、1 つのプライマリ VLAN だけに関連付けることができます。
- プライベート VLAN により、ホストはレイヤ 2 で分離されますが、レイヤ 3 で相互に通信できます。
- 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、他のデバイスに STP パラメータを伝播する必要はありません。プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN のスパニング ツリー トポロジが正確に一致し、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かどうかを確認するには、STP 設定を手動でチェックする必要があります。
- 標準トランク ポートの場合、次の事項に注意してください。
  - プライベート VLAN 内の各 VLAN に、個別の STP インスタンスが存在します。
  - プライマリ VLAN およびすべてのセカンダリ VLAN の STP パラメータが一致している必要があります。
  - プライマリ VLAN および関連付けられたすべてのセカンダリ VLAN が、同じ Multiple Spanning Tree（MST）インスタンス内に存在している必要があります。
- 非トランク ポートの場合、次の事項に注意してください。
  - STP が認識するのは、プライベート VLAN ホスト ポートのプライマリ VLAN だけです。STP は、ホスト ポート上のセカンダリ VLAN では実行されません。

（注）　ホスト ポートとして設定するすべてのポート上で BPDU ガードをイネーブルにすることを推奨します。この機能は、無差別ポート上ではイネーブルにしないでください。BPDU ガードの設定情報については、第 7 章「STP 拡張機能の設定」を参照してください。

- 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
- すべてのプライベート VLAN トラフィックに VACL を適用するには、プライマリ VLAN のレイヤ 3 VLAN インターフェイスまたは SVI にセカンダリ VLAN をマッピングしてから、プライマリ VLAN の SVI 上に VACL を設定します。
- プライマリ VLAN の、レイヤ 3 VLAN インターフェイスまたは SVI に適用した VACL は、マッピングが設定されている場合にのみ、関連付けられた独立 VLAN およびコミュニティ VLAN に自動的に適用されます。

- プライマリ VLAN のレイヤ 3 インターフェイスまたは SVI にセカンダリ VLAN をマッピング*せずに*、プライマリ VLAN とセカンダリ VLAN に異なる VACL を設定すると、問題が生じることがあります。
- プライベート VLAN のトラフィックは、異なる VLAN では異なる方向に伝送されるので、マッピングを設定する前に、入力トラフィック用と出力トラフィック用にそれぞれ異なる VACL を設定できます。

（注）　プライベート VLAN 内のプライマリ VLAN とすべてのセカンダリ VLAN では、同じ VACL を保持する必要があります。

- 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 上で DHCP スヌーピングをイネーブルにすると、DHCP 設定がセカンダリ VLAN に伝播されます。セカンダリ VLAN 上に DHCP を設定しても、プライマリ VLAN 上で DHCP がすでに設定されている場合、セカンダリ VLAN 上での設定は有効になりません。
- VLAN をセカンダリ VLAN として設定する前に、セカンダリ VLAN 用のレイヤ 3 インターフェイスまたは SVI をシャットダウンする必要があります。
- 無差別ポートが設定された独立プライベート VLAN 内でのホスト間通信を防ぐには、そのサブネット内のホストの相互通信を拒否する Role-Based ACL（RBACL; ロールベース ACL）を設定します。

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場合には、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てください。
- 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、非アクティブになります。プライベート VLAN を伝送するレイヤ 2 トランク インターフェイスはアクティブで、STP データベースの一部として保持されます。
- ポートチャネル グループに属すポートを、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場合、そのポートのポート チャネル設定は非アクティブになります。
- プライベート VLAN 設定に使用される VLAN を削除すると、その VLAN に関連付けられたプライベート VLAN ポートは非アクティブになります。

他の機能に関連する制限

プライベート VLAN の設定時は、他の機能に関連する設定上の制限を考慮してください。

（注）　状況によっては、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、コマンドは無効になります。

- IGMP は、プライマリ VLAN 上でのみ実行され、すべてのセカンダリ VLAN にプライマリ VLAN の設定が使用されます。
- セカンダリ VLAN 内の IGMP 加入要求は、プライマリ VLAN で受信されたものとして処理されます。

- プライベート VLAN は、次の Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能をサポートします。
  - プライベート VLAN 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。
- 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。
- 宛先 SPAN ポートを、独立ポートにすることはできません（ただし、送信元 SPAN ポートは独立ポートにできます）。
- SPAN は、プライマリ VLAN およびセカンダリ VLAN の両方に対して設定できます。また、出力トラフィックまたは入力トラフィックのうち、どちらか一方だけに対して設定することもできます。
- プライマリ VLAN とセカンダリ VLAN 間のアソシエーションを設定すると、セカンダリ VLAN を学習したダイナミック MAC アドレスがすぐに消去されます。
- プライマリ VLAN とセカンダリ VLAN 間のアソシエーションを設定すると、セカンダリ VLAN 上で作成されたすべてのスタティック MAC アドレスが、プライマリ VLAN に挿入されます。アソシエーションを削除すると、スタティック MAC アドレスはセカンダリ VLAN だけの設定に戻ります。
- プライマリ VLAN とセカンダリ VLAN 間のアソシエーションの設定後に、セカンダリ VLAN 用のスタティック MAC アドレスを作成することはできません。
- プライマリ VLAN とセカンダリ VLAN 間のアソシエーションの設定後、このアソシエーションを削除すると、プライマリ VLAN 上に作成されたすべてのスタティック MAC アドレスは、プライマリ VLAN 上でのみ存続します。
- プライベート VLAN では、ポート セキュリティ機能はサポートされません。

（注） スタティック MAC アドレスの設定の詳細については、『*Cisco NX-OS Security Configuration Guide*』を参照してください。

プライベート VLAN の設定

（注）　特定の VLAN をプライベート VLAN として割り当てる前に、VLAN を作成しておく必要があります。

+ ここでは、次の内容について説明します。

- プライベート VLAN の設定時の注意事項（p.4-12）
- プライベート VLAN のイネーブル化（p.4-13）
- プライベート VLAN としての VLAN の設定（p.4-14）
- プライマリ プライベート VLAN へのセカンダリ VLAN の関連付け（p.4-15）
- プライマリ VLAN の VLAN インターフェイスへのセカンダリ VLAN のマッピング（p.4-17）
- 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.4-19）
- 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.4-20）

（注）　レイヤ 3 VLAN インターフェイス（SVI）の IP アドレス指定の詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

プライベート VLAN の設定時の注意事項

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。

- セカンダリ VLAN をプライマリ VLAN と同じ MST にマップするには、**private-vlan synchronize** コマンドを入力します。
- デバイスでプライベート VLAN 機能を適用するには、プライベート VLAN をイネーブルにする必要があります。
- デバイスでこの機能を適用するには、VLAN インターフェイス機能をイネーブルにする必要があります。
- セカンダリ VLAN を設定する前に、セカンダリ VLAN として設定するすべての VLAN の VLAN インターフェイスまたは SVI をシャットダウンします。
- プライベート VLAN 機能の設定を開始する前に、「注意事項および制限」（p.4-9）を参照してください。
- プライベート VLAN モードで動作しているポートがデバイスに設定されている場合は、プライベート VLAN をディセーブルにすることはできません。

プライベート VLAN のイネーブル化

プライベート VLAN 機能を使用するには、デバイス上でプライベート VLAN をイネーブルにする必要があります。

（注）　プライベート VLAN 機能をイネーブルにするまでは、プライベート VLAN コマンドは表示されません。

手順の要約

1. **config t**
2. **feature private-vlan**
3. **exit**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	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	**feature private-vlan** **例：** switch(config)# feature private-vlan switch(config)#	デバイス上でプライベート VLAN 機能をイネーブルにします。 （注）　デバイス上にプライベート VLAN モードで動作しているポートが設定されている場合、**no feature private-vlan** コマンドは適用できません。
ステップ 3	**exit** **例：** switch(config)# exit switch#	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	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、デバイス上でプライベート VLAN 機能をイネーブルにする例を示します。

```
switch# config t
switch(config)# feature private-vlan
switch(config)#
```

プライベート VLAN としての VLAN の設定

（注）　VLAN をセカンダリ VLAN（コミュニティ VLAN または独立 VLAN のどちらか）として設定する前に、その VLAN のレイヤ 3 VLAN インターフェイスまたは SVI をシャットダウンする必要があります。

VLAN は、プライベート VLAN として設定できます。

プライベート VLAN を作成するには、最初に VLAN を作成して、その VLAN をプライベート VLAN として設定します。

プライベート VLAN 内で、プライマリ VLAN、コミュニティ VLAN、または独立 VLAN として使用するすべての VLAN を作成します。そのあとで、複数の独立 VLAN および複数のコミュニティ VLAN を 1 つのプライマリ VLAN に関連付けます。複数のプライマリ VLAN とアソシエーションを設定できます。つまり、複数のプライベート VLAN を設定できます。

プライマリ VLAN またはセカンダリ VLAN のどちらかを削除すると、その VLAN に関連付けられているポートは非アクティブになります。

始める前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。異なる VDC で同じ VLAN 名と ID を繰り返し使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の要約

1. **config t**
2. **vlan** {*vlan-id* | *vlan-range*}
3. **private-vlan** {**community** | **isolated** | **primary**}
4. **exit**
5. **show vlan private-vlan** [*type*]
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**vlan** {*vlan-id*	*vlan-range*}
		
		例：
		`switch(config)# vlan 5`
		`switch(config-vlan)#`
			VLAN コンフィギュレーション サブモードを開始します。

	コマンド	目的
ステップ 3	**private-vlan** {**community** | **isolated** | **primary**} **例**： switch(config-vlan)# private-vlan primary	VLAN を、コミュニティ VLAN 、独立 VLAN、またはプライマリ プライベート VLAN のいずれかに設定します。プライベート VLAN には、1 つのプライマリ VLAN が必要です。コミュニティ VLAN と独立 VLAN は、複数設定できます。
	no private-vlan {**community** | **isolated** | **primary**} **例**： switch(config-vlan)# no private-vlan primary	指定した VLAN からプライベート VLAN 設定を削除し、標準 VLAN モードに戻します。プライマリ VLAN またはセカンダリ VLAN のどちらかを削除すると、その VLAN に関連付けられているポートは非アクティブになります。
ステップ 4	**exit** **例**： switch(config-vlan)# exit switch(config)#	VLAN コンフィギュレーション サブモードを終了します。
ステップ 5	**show vlan private-vlan** [*type*] **例**： switch# show vlan private-vlan	(オプション) プライベート VLAN の設定を表示します。
ステップ 6	**copy running-config startup-config** **例**： switch(config)# copy running-config startup-config	(オプション) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、VLAN 5 をプライマリ VLAN としてプライベート VLAN に割り当てる例を示します。

```
switch# config t
switch(config)# vlan 5
switch(config-vlan)# private-vlan primary
switch(config-vlan)# exit
switch(config)#
```

プライマリ プライベート VLAN へのセカンダリ VLAN の関連付け

セカンダリ VLAN をプライマリ VLAN に関連付けるときは、次の注意事項に従ってください。

- *secondary-vlan-list* パラメータには、スペースを挿入しないでください。複数の項目は、カンマで区切って入力できます。各項目に、単一のセカンダリ VLAN ID、またはハイフンで連結したセカンダリ VLAN ID の範囲を指定します。
- *secondary-vlan-list* パラメータに、複数のコミュニティ VLAN ID および独立 VLAN ID を指定できます。
- 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、**add** キーワードと *secondary-vlan-list* を入力します。
- セカンダリ VLAN とプライマリ VLAN 間のアソシエーションを消去するには、**remove** キーワードと *secondary-vlan-list* を入力します。
- セカンダリ VLAN とプライマリ VLAN 間のアソシエーションを変更するには、既存のアソシエーションを削除して、新しいアソシエーションを追加します。

プライマリ VLAN またはセカンダリ VLAN のどちらかを削除すると、その VLAN に関連付けられているポートは非アクティブになります。

no private-vlan コマンドを入力すると、VLAN は標準 VLAN モードに戻ります。その VLAN 上のアソシエーションはすべて一時停止されますが、インターフェイスはプライベート VLAN モードのままです。

特定の VLAN をプライベート VLAN モードに再変換すると、元のアソシエーションが復元されます。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN のすべてのプライベート VLAN アソシエーションが削除されます。ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力した場合には、その VLAN のプライベート VLAN アソシエーションは一時停止するだけです。VLAN を再作成して、元のセカンダリ VLAN として設定すると、アソシエーションが再開されます。

始める前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。異なる VDC で同じ VLAN 名と ID を繰り返し使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の要約

1. **config t**
2. **vlan** *primary-vlan-id*
3. [**no**] **private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}
4. **exit**
5. **show vlan private-vlan** [*type*]
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**vlan** *primary-vlan-id*
	
	例：
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		プライベート VLAN の設定を行うプライマリ VLAN の番号を入力します。

ステップ 3	**private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*} **例：** `switch(config-vlan)# private-vlan association 100-105, 109`	セカンダリ VLAN をプライマリ VLAN に関連付けます。
	no private-vlan association **例：** `switch(config-vlan)# no private-vlan association`	プライマリ VLAN からすべてのアソシエーションを削除し、標準 VLAN モードに戻ります。

ステップ 4	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN コンフィギュレーション サブモードを終了します。

	コマンド	目的
ステップ 5	**show vlan private-vlan** [**type**] **例**： switch# show vlan private-vlan	（オプション）プライベート VLAN の設定を表示します。
ステップ 6	**copy running-config startup-config** **例**： switch(config)# copy running-config startup-config	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、コミュニティ VLAN 100 ～ 105 および独立 VLAN 109 をプライマリ VLAN 5 に関連付ける例を示します。

```
switch# config t
switch(config)# vlan 5
switch(config-vlan)# private-vlan association 100-105, 109
switch(config-vlan)# exit
switch(config)#
```

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

（注） プライベート VLAN のプライマリ VLAN 上のレイヤ 3 インターフェイス（SVI）への IP アドレス指定の詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

セカンダリ VLAN を、プライマリ VLAN の VLAN インターフェイスにマッピングします。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。プライマリ VLAN の入力トラフィックをレイヤ 3 で処理するには、セカンダリ VLAN をプライマリ VLAN の VLAN インターフェイスにマッピングします。

（注） VLAN インターフェイスまたは SVI を設定する前に、VLAN インターフェイスをイネーブルにする必要があります。プライマリ VLAN に関連付けられたコミュニティ VLAN または独立 VLAN 上の VLAN インターフェイスは、アウト オブ サービスになります。稼働するのは、プライマリ VLAN 上の VLAN インターフェイスだけです。

始める前に

作業を開始する前に、次の設定を確認してください。

- プライベート VLAN 機能がイネーブルである。
- VLAN インターフェイスまたは SVI 機能がイネーブルである。
- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。異なる VDC で同じ VLAN 名と ID を繰り返し使用できるので、正しい VDC で作業していることを確認する必要があります。
- セカンダリ VLAN のマッピング先となる正しいプライマリ VLAN レイヤ 3 インターフェイス、または SVI で作業をしている。

手順の要約

1. **config t**
2. **interface vlan** *primary-vlan-ID*
3. [**no**] **private-vlan mapping** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}
4. **exit**
5. **show interface private-vlan mapping**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *primary-vlan-ID* **例：** switch(config)# interface vlan 5 switch(config-if)#	プライベート VLAN の設定を行うプライマリ VLAN の番号を入力します。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 モードが開始されます。
ステップ 3	**private-vlan mapping** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*} **例：** switch(config-if)# private-vlan mapping 100-105, 109	セカンダリ VLAN を、プライマリ VLAN の SVI またはレイヤ 3 インターフェイスにマッピングします。これにより、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングが可能になります。
	no private-vlan mapping **例：** switch(config-if)# no private-vlan mapping	セカンダリ VLAN とプライマリ VLAN 間のレイヤ 3 インターフェイスへのマッピングを消去します。
ステップ 4	**exit** **例：** switch(config-if)# exit switch(config)#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	**show interface vlan private-vlan mapping** **例：** switch(config)# show interface vlan private-vlan mapping	（オプション）インターフェイスのプライベート VLAN 情報を表示します。
ステップ 6	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、セカンダリ VLAN 100 ～ 105 および 109 を、プライマリ VLAN 5 のレイヤ 3 インターフェイスまたは SVI にマッピングする例を示します。

```
switch# config t
switch(config)# interface vlan 5
switch(config-if)# private-vlan mapping 100-105, 109
switch(config-if)# exit
switch(config)#
```

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 のホスト ポートとして設定できます。プライベート VLAN では、ホスト ポートはセカンダリ VLAN（コミュニティ VLAN または独立 VLAN のどちらか）に含まれます。

（注）　ホスト ポートとして設定したすべてのインターフェイス上で BPDU ガードをイネーブルにすることを推奨します。BPDU ガードの設定情報については、第 7 章「STP 拡張機能の設定」を参照してください。

設定したホスト ポートを、プライマリ VLAN とセカンダリ VLAN の両方に関連付けます。

始める前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。異なる VDC で同じ VLAN 名と ID を繰り返し使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の要約

1. **config t**
2. **interface** *type slot/port*
3. **switchport mode private-vlan host**
4. **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*}
5. **exit**
6. **show interface switchport**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		プライベート VLAN ホスト ポートとして設定するレイヤ 2 ポートを選択します。

ステップ 3	**switchport mode private-vlan host**
	
	例：
	`switch(config-if)# switchport mode private-vlan host`
	`switch(config-if)#`
		レイヤ 2 ポートをプライベート VLAN のホスト ポートとして設定します。

	コマンド	目的
ステップ 4	**switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*} **例**： switch(config-if)# switchport private-vlan host-association 10 50	レイヤ 2 ホスト ポートを、プライベート VLAN のプライマリ VLAN およびセカンダリ VLAN に関連付けます。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のどちらでもかまいません。
	no switchport private-vlan host-association **例**： switch(config-if)# no switchport private-vlan host-association	ポートからプライベート VLAN のアソシエーションを削除します。
ステップ 5	**exit** **例**： switch(config-if)# exit switch(config)#	インターフェイス 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	**show interface switchport** **例**： switch# show interface switchport	（オプション）スイッチ ポートとして設定されているすべてのインターフェイスの情報を表示します。
ステップ 7	**copy running-config startup-config** **例**： switch(config)# copy running-config startup-config	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 ポート 2/1 をプライベート VLAN のホスト ポートとして設定し、プライマリ VLAN 10 およびセカンダリ VLAN 50 に関連付ける例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode private-vlan host
switch(config-if)# switchport private-vlan host-association 10 50
switch(config-if)# exit
switch(config)#
```

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 の無差別ポートとして設定し、その無差別ポートをプライマリ VLAN およびセカンダリ VLAN に関連付けることができます。

始める前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。異なる VDC で同じ VLAN 名と ID を繰り返し使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の要約

1. **config t**
2. **interface** *type slot/port*
3. **switchport mode private-vlan promiscuous**
4. **switchport private-vlan mapping** {*primary-vlan-id*} {*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*}

5. **exit**
6. **show interface switchport**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **例**： switch# config t switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface** {*type slot/port*} **例**： switch(config)# interface ethernet 2/1 switch(config-if)#	プライベート VLAN 無差別ポートとして設定するレイヤ 2 ポートを選択します。
ステップ 3	**switchport mode private-vlan promiscuous** **例**： switch(config-if)# switchport mode private-vlan promiscuous	レイヤ 2 ポートをプライベート VLAN の無差別ポートとして設定します。
ステップ 4	**switchport private-vlan mapping** {*primary-vlan-id*} {*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*} **例**： switch(config-if)# switchport private-vlan mapping 10 50	レイヤ 2 ポートを無差別ポートとして設定し、このポートをプライマリ VLAN および選択したセカンダリ VLAN のリストに関連付けます。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のどちらでもかまいません。
	no switchport private-vlan mapping **例**： switch(config-if)# no switchport private-vlan mapping	プライベート VLAN からマッピングを消去します。
ステップ 5	**exit** **例**： switch(config-if)# exit switch(config)#	インターフェイス 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	**show interface switchport** **例**： switch# show interface switchport	（オプション）スイッチ ポートとして設定されているすべてのインターフェイスの情報を表示します。
ステップ 7	**copy running-config startup-config** **例**： switch(config)# copy running-config startup-config	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 ポート 2/1 を無差別ポートとして設定し、プライマリ VLAN 10 とセカンダリ独立 VLAN 50 に関連付ける例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# switchport private-vlan mapping 10 50
switch(config-if)# exit
switch(config)#
```

プライベート VLAN 設定の確認

プライベート VLAN の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config vlan *vlan-id*	VLAN 情報を表示します。
show vlan private-vlan [*type*]	プライベート VLAN の情報を表示します。
show interface private-vlan mapping	インターフェイスのプライベート VLAN 情報を表示します。
show interface switchport	スイッチ ポートとして設定されているすべてのインターフェイスの情報を表示します。

これらのコマンドの出力フィールドの詳細については、『*Cisco NX-OS Lauer 2 Switching Command Reference*』を参照してください。

プライベート VLAN の統計情報の表示とクリア

プライベート VLAN の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
clear vlan [**id** *vlan-id*] **counters**	すべての VLAN または指定した VLAN のカウンタをクリアします。
show vlan counters	各 VLAN のレイヤ 2 パケット情報を表示します。

プライベート VLAN の設定例

次に、3 種類のプライベート VLAN を作成し、セカンダリ VLAN をプライマリ VLAN に関連付け、プライベート VLAN のホスト ポートと無差別ポートを作成して適正な VLAN に関連付け、VLAN インターフェイスまたは SVI を作成して、プライマリ VLAN がネットワーク全体と通信できるように設定する例を示します。

```
switch# configure terminal
switch(config)# vlan 2
switch(config-vlan)# private-vlan primary
switch(config-vlan)# vlan 3
switch(config-vlan)# private-vlan community
switch(config-vlan)# vlan 4
switch(config-vlan)# private-vlan isolated

switch(config-vlan)# vlan 2
switch(config-vlan)# private-vlan association 3,4

switch(config-vlan)# interface ethernet 1/11
switch(config-if)# switchport
switch(config-if)# switchport mode private-vlan host
switch(config-if)# interface ethernet 1/12
switch(config-if)# switchport
switch(config-if)# switchport mode private-vlan promiscuous

switch(config-if)# interface ethernet 1/11
switch(config-if)# switchport private-vlan host-association 2 3
switch(config-if)# interface ethernet 1/12
switch(config-if)# switchport private-vlan mapping 2 3,4

switch(config-if)# interface vlan 2
switch(config-if)# private-vlan mapping 3,4
```

デフォルト設定

表 4-1 に、プライベート VLAN のデフォルト設定を示します。

表 4-1　プライベート VLAN のデフォルト設定

パラメータ	デフォルト
プライベート VLAN	ディセーブル

追加情報

プライベート VLAN の実装に関する追加情報は、次のセクションを参照してください。

- 関連資料（p.4-24）
- 標準規格（p.4-24）
- MIB（p.4-24）

関連資料

関連トピック	マニュアル名
VLAN	第 3 章「VLAN の設定」
レイヤ 2 MAC アドレス	第 2 章「レイヤ 2 スイッチングの設定」
STP 拡張機能	第 7 章「STP 拡張機能の設定」
コマンド リファレンス	『*Cisco NX-OS Layer 2 Switching Command Reference*』
DCNM レイヤ 2 スイッチング コンフィギュレーション	『*Cisco DCNM Layer 2 Switching Configuration Guide*』
VLAN インターフェイス、IP アドレス指定	『*Cisco NX-OS Interfaces Configuration Guide*』
スタティック MAC アドレス、セキュリティ	『*Cisco NX-OS Security Configuration Guide*』
NX-OS の基本情報	『*Cisco NX-OS Security Configuration Guide*』
ハイ アベイラビリティ	『*Cisco NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco NX-OS System Management Configuration Guide*』
VDC	『*Cisco NX-OS Virtual Device Context Configuration Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco NX-OS Release Notes*』Release 4.0

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

MIB

MIB	MIB リンク
• CISCO-PRIVATE-VLAN-MIB	次の URL から、MIB の検索およびダウンロードができます。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml