



NX-OS を使用したプライベート VLAN の設定

- プライベート VLAN について, [on page 1](#)
- プライベート VLAN の前提条件, [on page 10](#)
- プライベート VLAN の設定に関するガイドラインおよび制約事項 (10 ページ)
- プライベート VLAN のデフォルト設定, [on page 14](#)
- プライベート VLAN の設定, [on page 14](#)
- プライベート VLAN 設定の確認, [on page 31](#)
- プライベート VLAN の統計情報の表示とクリア, [on page 32](#)
- プライベート VLAN の設定例, [on page 32](#)
- プライベート VLAN の追加情報 (CLI バージョン) , [on page 33](#)

プライベート VLAN について



Note 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。



Note 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。

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 の関連付けです。

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 のいずれかの場合があります。独立 VLAN 上のホストは、プライマリ VLAN 内で関連付けられた無差別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

■ プライベート VLAN の概要

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。

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 ネットワークインターフェイスを割り当てることにより、ルーティングを提供できます。VLAN ネットワークインターフェイスは、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 VLAN ネットワークインターフェイス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 VLAN ネットワークインターフェイスは、すべてサービス停止状態になります。

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。



Note 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 を作成しておく必要があります。

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 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 を割り当てるに、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、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、各サブドメインの区別に使用されます。



Note 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。

セカンダリ VLAN は、同じプライベート 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：コミュニケーション 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ケーション 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



Note 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、コミュニケーション 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 ポートのタイプは、次のとおりです。

- 無差別ポート：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、無差別ポートとアソシエートされているセカンダリ VLAN に属し、プライマリ VLAN とアソシエートされている、すべてのインターフェイスと通信でき、この通信可能なインターフェイスには、コミュニケーションポートと独立ホストポートも含まれます。プライマリ VLAN には、複数の無差別ポートを含めることができます。各無差別ポートには、ポートにアソシエートされている、複数のセカンダリ VLAN を含めることができます、また、セカンダリ VLAN を含めないこともあります。無差別ポートとセカンダリ VLAN が同じプライマリ VLAN にある限り、セカンダリ VLAN は、複数の無差別ポートとアソシエートすることができます。このアソシエーションは、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ができます。セカンダリ VLAN を無差別ポートに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。



Note ベストプラクティスとして、プライマリのすべてのセカンダリ ポートをマッピングして、トラフィックの損失を最小限に抑える必要があります。

- 無差別トランク：複数のプライマリ VLAN のトラフィックを伝送するように無差別トランク ポートを設定できます。プライベート VLAN のプライマリ VLAN およびすべてまたは選択した関連付けられた VLAN を無差別トランク ポートにマップします。各プライマリ VLAN と 1 つの関連付けられたセカンダリ VLAN は、プライベート VLAN のペアとなります。最大 PVLAN のマッピングについては、『検証済み拡張性ガイド』を参照してください。

■ プライマリ、独立、およびコミュニティ プライベート VLAN

**Note**

プライマリ プライベート VLAN に加え、標準の VLAN でもプライベート VLAN 無差別トランク ポートでトラフィックが传送されます。

- 独立ポート：独立ポートは、セカンダリ独立VLANに属するホストポートです。このポートは同一プライベート VLAN ドメイン内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。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。
- 独立トランクまたはセカンダリ トランク：複数の独立 VLAN のトラフィックを伝送するように独立トランク ポートを設定できます。独立トランク ポートの各セカンダリ VLAN は、別々のプライマリ VLAN に関連付ける必要があります。同じプライマリ VLAN に関連付けられた 2 つのセカンダリ VLAN は、1 つの独立トランク ポートにはできません。各プライマリ VLAN と関連付けられた 1 つのセカンダリ VLAN は、プライベート VLAN のペアです。最大 PVLAN の関連付けについては、『*Verified Scalability Guide*』を参照してください。

**Note**

セカンダリ プライベート VLAN に加え、標準の VLAN でもプライベート VLAN 独立トランク ポートでトラフィックが传送されます。

- コミュニティ ポート：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 にある他のポートおよびアソシエートされている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。

**Note**

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。

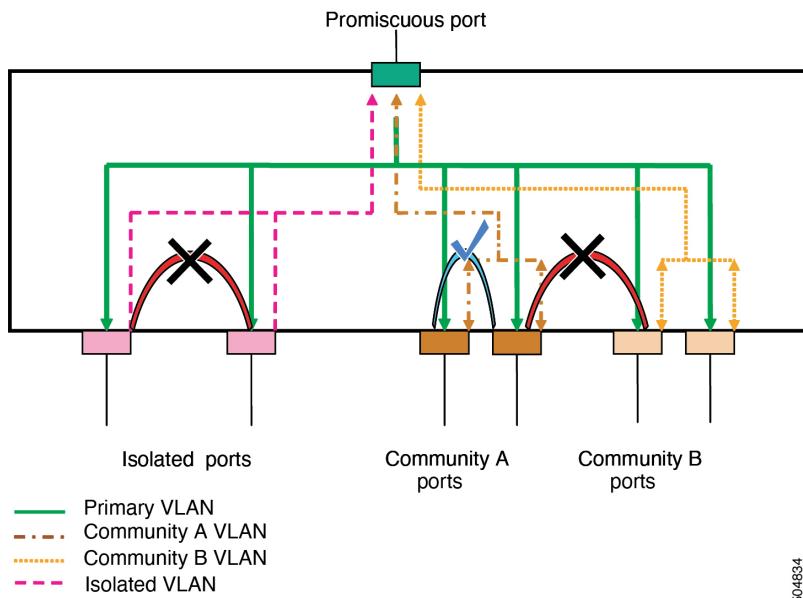
プライマリ、独立、およびコミュニティ プライベート VLAN

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。プライマリ VLAN には1つの独立 VLAN を設定できます。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。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。1つのコミュニティ内のポートは相互に通信できますが、これらのポートは、他のコミュニティにあるポートとも、プライベート VLAN にある独立 VLAN とも、通信できません。

Figure 1: プライベート VLAN のレイヤ2 トラフィック フロー

次の図に、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。



Note 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单方向です。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、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、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

■ プライマリ VLAN とセカンダリ VLAN の関連付け

接続できます。たとえば、すべてのプライベート VLAN サーバー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。



Note プライベート VLAN の無差別および独立トランク ポートを設定できます。これらの無差別トランク ポートと独立トランク ポートは、標準の VLAN に加え、複数のプライマリおよびセカンダリ VLAN のトラフィックを伝送できます。

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。



Note レイヤ 3 ゲートウェイを設定するには、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 ネットワークインターフェイスと IP アドレス設定の詳細については、『Cisco Nexus 9000 Series 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。関連付け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。



Note セカンダリ VLAN は、1 つのプライマリ VLAN のみにアソシエートすることができます。

アソシエーションの操作を可能にするには、次の条件を満たす必要があります。

- 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。



Note 関連付けが動作していることを確認するには、**show** コマンドの出力を調べます。関連付け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

プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。指定の 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。

関連付けがプライベート VLAN トランク ポートで動作していない場合、ポート全体はダウンせずに、その VLANだけがダウンします。

no private-vlan コマンドを入力すると、VLAN は通常の VLAN モードに戻ります。その VLAN 上の関連付け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 モードのままになります。

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 に関連付けされたすべてのプライベート VLAN は失われます。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、その VLAN とプライベート VLAN の関連付けは一時停止します。この VLAN を再作成してセカンダリ VLAN として設定すると元に戻ります。



Note この動作は、Catalyst デバイスの動作と異なります。

セカンダリ VLAN とプライマリ VLAN の関連付けを変更するには、現在の関連付けを削除してから目的の関連付けを追加します。

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 にあるポートからのブロードキャスト トラフィックは、次のように流れます。

- ブロードキャスト トラフィックは、すべての無差別ポートからプライマリ VLAN 内のすべてのポートにれます。このブロードキャスト トラフィックは、プライベート VLAN パラメータで設定されていないポートを含め、プライマリ VLAN 内のすべてのポートに配信されます。
- すべての独立ポートからのブロードキャスト トラフィックは、その独立ポートに関連付けられているプライマリ VLAN の無差別ポートにだけ配信されます。
- 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。

■ プライベート VLAN および VLAN インターフェイス

- 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 サーバーなど）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。

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、スイッチ仮想インターフェイス (SVI) 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 だけを介してプライベート VLAN と通信します。

VLAN ネットワークインターフェイスは、プライマリ VLAN だけに対して設定します。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 ネットワークインターフェイス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 ネットワークインターフェイスが設定された 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 ネットワークインターフェイス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 VLAN ネットワークインターフェイスに IP サブネットを割り当てるとき、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。



Note 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 アドレスの設定の詳細については、『Cisco Nexus 9000 Series 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

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ки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。

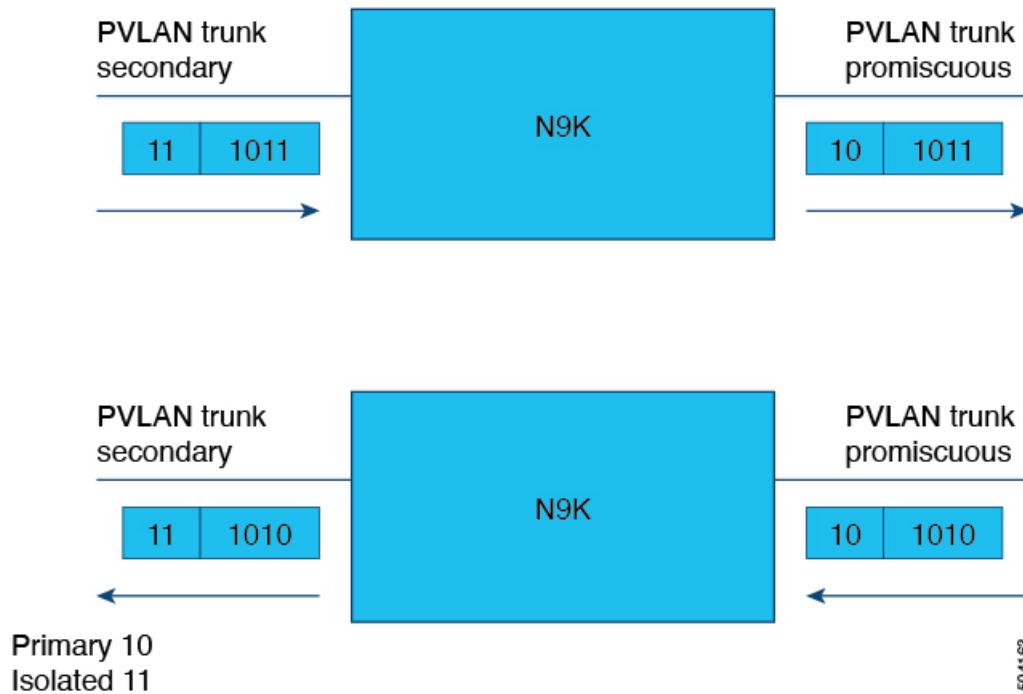
内部 VLAN タグを保持するプライベート VLAN

Cisco NX-OS リリース 10.2(3)F 以降、グローバル **system dot1q-tunnel transit <vlan>** を構成している場合トランジット ボックスとして機能するサポートされている Cisco Nexus スイッチでコマンドを実行すると、2つ以上のタグを持つプライベート VLAN トランク ポートに着信するパケットは保持され、内部タグを削除せずに送信されます。このコマンドの詳細については、cisco.com の関連リリースの『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』を参照してください。



(注) PVLAN と QinQ が同じポートで設定されている場合、内部タグの保存は機能しません。

次の図は、パケットが PVLAN セカンダリ トランクから PVLAN 無差別 トランクに移動したり、その逆に移動したりするときの、サポートされている Cisco Nexus スイッチでの内部タグの保持を示しています。



サンプル設定を次に示します。

```
vlan 10
private-vlan primary
private-vlan association 11-12
vlan 11
private-vlan isolated
vlan 12
private-vlan community

interface Ethernet1/1
switchport
switchport mode private-vlan trunk secondary
switchport private-vlan association trunk 10 11
```

■ プライベート VLAN のハイ アベイラビリティ

```
no shutdown

interface Ethernet1/2
switchport
switchport mode private-vlan trunk promiscuous
switchport private-vlan mapping trunk 10 11-12
no shutdown

(config)# system dot1q-tunnel transit vlan 10,11
```

プライベート VLAN のハイ 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、最大 3 回の再試行がサポートされます。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。



Note ハイアベイラビリティ機能、の詳細については、『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』を参照してください。

プライベート VLAN の前提条件

プライベート VLAN には次の前提条件があります。

- デバイスにログインしていること。
- 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。

プライベート VLAN の設定に関するガイドラインおよび制約事項

プライベート VLAN 設定時のガイドラインと制約事項 PVLAN は次のとおりです。

- 一つの関連付けから別の関連付けに PVLAN ホスト関連付けを変更する場合、ポートセキュリティ静的 MAC アドレスが削除されていないとエラーが表示されます。ポートセキュリティ静的 MAC アドレスを削除することをお勧めします。

ERROR: Static Port-Security Mac configured. Remove configured static port-security mac under the interfaces before changing the private-vlan

- 無差別モードで vPC ポートチャネルの PVLAN マッピングを変更すると、vPC セカンダリ の vPC PO メンバーがフラップします。
- **show** コマンド (**internal** キーワード付き) はサポートされていません。

- デバイスで PVLAN 機能を適用できるようにするには、あらかじめ PVLAN をイネーブルにしておく必要があります。
- ハードウェアおよび設定の制限により、ポートは、ポート VLAN マッピングを持つと同時に、無差別、独立、トランク、またはホストポートモードでプライベート VLAN (PVLAN) インターフェイスとして動作することはできません。PVLAN と ポート VLAN 機能は、個別のポートで独立して動作します。両方の機能に同じ VLAN を構成して使用できます。これは、これらのリリースに適用されます。
 - Cisco NX-OS リリース 10.2(9)M
 - Cisco NX-OS リリース 10.3(7)M
 - Cisco NX-OS リリース 10.4(5)M
 - Cisco NX-OS リリース 10.2 (2) F
- 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 ネットワーク インターフェイスをシャットダウンします。
- スタティック MAC が通常の VLAN で作成され、その VLAN がセカンダリ VLAN に変換されると、Cisco NX-OS はセカンダリ VLAN で設定された MAC をスタティック MAC として維持します。
- PVLAN は、次のように PVLAN ポート モードをサポートします。
 - プロミスキヤス
 - 無差別トランク
 - ホストを分離する
 - 独立ホストトランク。
 - コミュニティホスト。
- Cisco NX-OS リリース 9.2(1) 以降、PVLAN は VXLAN をサポートします。
- プライベート VLAN は、ポート チャネルのポート モードをサポートします。
- プライベート VLAN は、仮想ポートチャネル (vPC) インターフェイスのポート モード サポートを提供します。
- PVLAN 無差別トランクまたは PVLAN 独立トランクを設定する場合は、ID で指定されたリストで非 PVLAN を許可することを推奨します。 **switchport private-vlan trunk allowed** コマンドを使用します。PVLAN は、PVLAN トランクモードに応じてマッピングまたは関連付けられます。

■ プライベート VLAN の設定に関するガイドラインおよび制約事項



(注) 2番目のスイッチを無差別または隔離された PVLAN トランクに接続することはできません。PVLAN無差別トランクまたはPVLAN隔離トランクは、ホストスイッチでのみサポートされます。

- **system private-vlan fex trunk** コマンドは、Cisco Nexus 9300 -FX、-FX2、-FX3 プラットフォーム スイッチでサポートされていません。次の PVLAN モードは、シングルホーム FEX 構成の FEX ポートおよびポートチャネルでのみサポートされます (AA または ST vPC モードではサポートされません)。
 - Isolated host
 - Community host
 - Isolated trunk
 これらのモードは、シングルホーム FEX 構成の FEX ポートおよびポートチャネルでのみサポートされます (AA または ST vPC モードではサポートされません)。
- PVLANはPAACLおよびRACLをサポートします。
- PVLANは次のようにSVIをサポートします。
 - プライマリ VLAN上のSVI。
 - SVI の プライマリおよびセカンダリ IP アドレス。
 - プライマリ SVIのHSRP。
- PVLANはレイヤ2転送をサポートします。
- PVLANは次のようにSTPをサポートします。
 - RSTP
 - MST
- PVLANは、通常のトランクポートを介してスイッチ間でサポートされます。
- PVLANは、Cisco Nexus 9396PQおよび93128TXスイッチの10Gポートでサポートされます。
- PVLAN設定は、Cisco Nexus 9300シリーズスイッチのALEポートではサポートされません。
- PVLANポートモードは、Cisco Nexus 3164Qスイッチではサポートされていません。
- Network Forwarding Engine (NFE) では、PVLANはブレークアウトをサポートしません。
- PVLANは、vPCまたはポートチャネルFEXポートではサポートされません。
- PVLANは、IPマルチキャストまたはIGMPスヌーピングをサポートしません。
- Cisco NX-OS リリース9.3(3) 以降では、次の機能が C9316D-GX、C93600CD-GX、および C9364C-GX スイッチでサポートされています。

- vPC
 - 200k MAC スケール
 - Dot1x
 - ポートセキュリティ
 - 選択的 QinQ
 - マルチプルプロバイダ VLAN を装備した選択的 QinQ
-
- Cisco NX-OS リリース 9.3 (5) 以降、PVLAN は DHCP スヌーピングをサポートします。
 - Cisco NX-OS リリース 9.3(5) 以降、PVLAN は N9K-C93180YC-FX3S プラットフォームスイッチでサポートされています。
 - Cisco NX-OS リリース 9.3(9) 以降、vPC ピアリンクインターフェイスでは PVLAN 設定は許可されません。
 - PVLAN は PVLAN QoS をサポートしません。
 - PVLAN は VACL をサポートしません。
 - PVLAN は VTP をサポートしません。
 - PVLAN は トンネルをサポートしません。
 - 送信元が PVLAN VLAN の場合、PVLAN は SPAN をサポートしません。
 - PVLAN の一部になるように共有インターフェイスを設定できません。詳細については、『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』を参照してください。
 - Cisco NX-OS CLI では、PVLAN グループごとに複数の独立 VLAN 設定を設定できますが、このような設定はサポートされていません。PVLAN グループには、最大で 1 つの独立 VLAN を設定できます。
 - Cisco NX-OS Release 7.0 (3) I5 (1) 以降では、VLAN での PVLAN アソシエーションはサポートされていません。
 - PVLAN ホストポートおよび通常のトランクの MAC アドレス学習は、プライマリ VLAN で行われます。通常のトランクの場合、パケットはセカンダリ VLAN を使用して交換されますが、MAC 学習は引き続きプライマリ VLAN で実施されます。
 - PVLAN は、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ラインカードを搭載した Cisco Nexus 9500 Series スイッチではサポートされていません。
 - Cisco NX-OS リリース 10.1 (2) 以降では、vPC 孤立ポートでの PVLAN と portSec 機能の組み合わせには、ピアとトリガー間での動的な Mac 同期に制限があります。
 - Cisco NX-OS Release 10.2(2)F 以降、次の機能が Cisco N9K-9332D-GX2B プラットフォームスイッチでサポートされます。
 - PVLAN および Flex Link

■ プライベート VLAN のデフォルト設定

- VPC
- 選択的 QinQ
- マルチプル プロバイダ VLAN を装備した選択的 QinQ
- Cisco NX-OS リリース 10.2(3)F 以降では、グローバル **system dot1q-tunnel transit** コマンドがトランジット ボックスとして機能する Nexus スイッチで設定されている場合、パケットが 2 つ以上のタグで着信すると、内部 VLAN を持つプライベート VLAN タグ保存機能により、PVLAN の内部タグを保存できます。この機能は、EX、FX、FX2、FX3、GX、および GX2B ベースの Cisco Nexus 9000 シリーズ TOR スイッチでのみサポートされています。
- PVLAN と Q-in-Q が同じポートで設定されている場合、内部タグの保存は機能しません。
- Cisco NX-OS リリース 10.3(3)F 以降、IPv6 アンダーレイは、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2 スイッチおよび 9700-EX/FX/GX ラインカードを搭載した Cisco Nexus 9500 スイッチにおいて、VXLAN EVPN の PVLAN でサポートされます。
- Cisco NX-OS リリース 10.4(2)F 以降、PVLAN は Cisco Nexus C93108TC-FX3 スイッチではサポートされます。

プライベート VLAN のデフォルト設定

次の表に、プライベート VLAN のデフォルト設定を示します。

Table 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	無効化

プライベート VLAN の設定

指定した 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。

VLAN インターフェイスへの IP アドレスの割り当ての詳細については、『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』を参照してください。



Note

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 のイネーブル化 (CLI バージョン)

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。



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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	feature private-vlan Example: 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。
ステップ 3	exit Example: 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	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	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。

Example

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。

■ プライベート VLAN としての VLAN の設定 (CLI バージョン)

```
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 (CLI バージョン)



Note VLAN をセカンダリ VLAN (つまり、コミュニティ VLAN または独立 VLAN のいずれか) として設定する前に、まず VLAN ネットワーク インターフェイス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 と関連付けを設定できます。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 を削除すると、その VLAN に関連付けされたポートは非アクティブになります。

プライベート VLAN トラック ポート上でセカンダリ VLAN またはプライマリ VLAN のいずれかを削除した場合、その特定の VLAN だけが非アクティブになり、トランク ポートはアップしましたままでです。

SUMMARY STEPS

1. config t
2. vlan {vlan-id | vlan-range}
3. [no] private-vlan {community | isolated | primary}
4. exit
5. (Optional) show vlan private-vlan [type]
6. (Optional) copy running-config startup-config

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: <pre>switch# config t switch(config)# </pre>	コンフィギュレーション モードに入ります。

	Command or Action	Purpose
ステップ 2	vlan {vlan-id vlan-range} Example: switch(config)# vlan 5 switch(config-vlan)#{/td> <td>VLAN 設定サブモードにします。</td>	VLAN 設定サブモードにします。
ステップ 3	[no] private-vlan {community isolated primary} Example: 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 として設定します。プライベート VLAN には、1つのプライマリ VLAN を設定する必要があります。複数のコミュニティ VLAN と独立 VLAN を設定することができます。 または 指定した VLAN からプライベート VLAN の設定を削除し、通常の VLAN モードに戻します。プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。
ステップ 4	exit Example: switch(config-vlan)# exit switch(config)#{/td> <td>VLAN コンフィギュレーションサブモードを終了します。</td>	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	(Optional) show vlan private-vlan [type] Example: switch# show vlan private-vlan	プライベート VLAN の設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	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。

Example

次の例は、VLAN 5 をプライマリ VLAN としてプライベート VLAN に割り当てる方法を示しています。

```
switch# config t
switch(config)# vlan 5
switch(config-vlan)# private-vlan primary
switch(config-vlan)# exit
switch(config)#{/pre>

```

セカンダリ VLAN とプライマリ プライベート VLAN の関連付け (CLI バージョン)

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。各項目は、単一のセカンダリ VLAN ID、またはセカンダリ VLAN ID をハイフンでつないだ範囲にできます。
- *secondary-vlan-list* パラメータには、複数のコミュニティ VLAN ID と独立 VLAN ID を含めることができます。
- *secondary-vlan-list* を入力するか、**add** キーワード *secondary-vlan-list* を追加して、プライマリ VLAN とセカンダリ VLAN の関連付けを行います。
- **remove** を入力します キーワード *secondary-vlan-list* を削除して、セカンダリ VLAN とプライマリ VLAN との関連付けをクリアします。
- セカンダリ VLAN とプライマリ VLAN と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、次に必要な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 を削除すると、その VLAN に関連付けされたポートは非アクティブになります。

no private-vlan コマンド、VLAN は通常の VLAN モードに戻ります。その VLAN 上の関連付け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 モードのままになります。

指定の 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。

no vlan コマンドは、プライマリ VLAN に対して、その VLAN に関連付けされているすべてのプライベート VLAN が失われます。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、その VLAN とプライベート VLAN の関連付けは一時停止します。この VLAN を再作成して以前のセカンダリ VLAN として設定すると元に戻ります。

Before you begin

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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	vlan primary-vlan-id Example: switch(config)# vlan 5 switch(config-vlan)#[/pri]	プライベート VLAN の設定作業を行うプライマリ VLAN の番号を入力します。
ステップ 3	[no] private-vlan association {[add] secondary-vlan-list} remove secondary-vlan-list} Example: switch(config-vlan)# private-vlan association 100-105,109	コマンドの 1 つの形式を使用して、 セカンダリ VLAN をプライマリ VLAN に関連付けています。 または プライマリ VLAN からすべての関連付けを削除し、 通常の VLAN モードに戻します。
ステップ 4	exit Example: switch(config-vlan)# exit switch(config)#[/pri]	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	(Optional) show vlan private-vlan [type] Example: switch# show vlan private-vlan	プライベート VLAN の設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	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。

Example

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)# vlan 5
switch(config-vlan)# private-vlan association 100-105, 109
switch(config-vlan)# exit
switch(config)#[/pri]
```

■ 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 (CLI バージョン)

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 (CLI バージョン)



Note

プライベート VLN のプライマリ VLAN の VLAN インターフェイスへの IP アドレスの割り当ての詳細については、『Cisco Nexus 9000 Series 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。プライベート 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 ネットワーク インターフェイスにマッピングします。



Note

VLAN ネットワーク インターフェイスを設定する前に、VLAN ネットワーク 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 ネットワーク 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 ネットワーク インターフェイスだけです。

Before you begin

- プライベート VLAN 機能をイネーブルにする。
- VLAN インターフェイス機能をイネーブルにする。
- 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 インターフェイスで作業をしていること。

SUMMARY STEPS

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. (Optional) **show interface vlan primary-vlan-id private-vlan mapping**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	interface vlan primary-vlan-ID Example: switch(config)# interface vlan 5 switch(config-if)#	プライベート VLAN の設定作業を行うプライマリ 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	[no] private-vlan mapping {[add] secondary-vlan-list remove secondary-vlan-list} Example: 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。 または 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 Example: 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	(Optional) show interface vlan primary-vlan-id private-vlan mapping Example: switch(config)# show interface vlan 101 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。
ステップ 6	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	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。

Example

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 インターフェイスにマッピングする例を示します。

```
switch #config t
switch(config)# interface vlan 5
```

■ 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

```
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 ポートがセカンダリ VLAN の一部です。セカンダリ VLAN は、コミュニティ VLAN または独立 VLAN のいずれかです。



Note ホスト 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で、BPDU ガードをイネーブルにすることを推奨します。

次に、ホスト ポートを、プライマリ VLAN とセカンダリ VLAN の両方にアソシエートします。

Before you begin

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。

SUMMARY STEPS

1. **config t**
2. **interface type slot/port**
3. **switchport mode private-vlan host**
4. [no] **switchport private-vlan host-association {primary-vlan-id} {secondary-vlan-id}**
5. **exit**
6. (Optional) **show interface switchport**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	interface type slot/port Example:	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。

	Command or Action	Purpose
	switch(config)# interface ethernet 2/1 switch(config-if)#	
ステップ3	switchport mode private-vlan host Example: 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。
ステップ4	[no] switchport private-vlan host-association {primary-vlan-id} {secondary-vlan-id} Example: 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 のいずれかとして設定できます。 または プライベート VLAN のアソシエーションをポートから削除します。
ステップ5	exit Example: 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	(Optional) show interface switchport Example: switch# 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に関する情報を表示します。
ステップ7	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	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。

Example

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 独立トランク ポートとしてのレイヤ2インターフェイスの設定

プライベート VLAN 独立トランク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 独立トランク ポートとして設定できます。これらの独立トランク ポートは、複数のセカンダリ VLAN と通常の VLAN のトラフィックを伝送します。



(注) プライマリ VLAN とセカンダリ VLAN は、プライベート VLAN 独立トランク ポート上で動作可能になる前に関連付ける必要があります。

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。

手順の概要

1. config t
2. interface {type slot/port}
3. switchport
4. switchport mode private-vlan trunk secondary
5. (任意) switchport private-vlan trunk native vlan *vlan-id*
6. switchport private-vlan trunk allowed vlan {add *vlan-list* | all | except *vlan-list* | none | remove *vlan-list*}
7. [no] switchport private-vlan association trunk {primary-vlan-id [*secondary-vlan-id*]}
8. exit
9. (任意) show interface switchport
10. (任意) copy running-config startup-config

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ1	config t 例： <pre>switch# config t switch(config)#</pre>	コンフィギュレーション モードになります。
ステップ2	interface {type slot/port} 例： <pre>switch(config)# interface ethernet 2/11 switch(config-if)#</pre>	プライベート VLAN 独立トランク ポートとして設定するレイヤ2ポートを選択します。

	コマンドまたはアクション	目的
ステップ 3	switchport 例： <pre>switch(config-if)# switchport switch(config-if)#{/pre></pre>	レイヤ2ポートをスイッチポートとして設定します。
ステップ 4	switchport mode private-vlan trunk secondary 例： <pre>switch(config-if)# switchport mode private-vlan trunk secondary switch(config-if)#{/pre></pre>	レイヤ2ポートを、複数の独立VLANのトラフィックを伝送する独立トランクポートとして設定します。 (注) コミュニティVLANは独立トランクポートにはできません。
ステップ 5	(任意) switchport private-vlan trunk native vlan <i>vlan-id</i> 例： <pre>switch(config-if)# switchport private-vlan trunk native vlan 5#{/pre></pre>	802.1QトランクのネイティブVLANを設定します。有効値の範囲は1～3968および4048～4093です。デフォルト値は1です。 (注) プライベートVLANを独立トランクポートのネイティブVLANとして使用している場合は、セカンダリVLANまたは標準VLANの値を入力する必要があります。プライマリVLANをネイティブVLANとして設定することはできません。
ステップ 6	switchport private-vlan trunk allowed vlan {add <i>vlan-list</i> all except <i>vlan-list</i> none remove <i>vlan-list</i>} 例： <pre>switch(config-if)# switchport private-vlan trunk allowed vlan add 1 switch(config-if)#{/pre></pre>	プライベートVLAN独立トランクインターフェイスの許容VLANを設定します。有効値の範囲は1～3968および4048～4093です。 プライベートプライマリVLANおよびセカンダリVLANを独立トランクポートにマッピングすると、すべてのプライマリVLANがこのポートの許可されるVLANリストに自動的に追加されます。 (注) ネイティブVLANが許可されるVLANリストに含まれていることを確認します。このコマンドでは、デフォルトでこのインターフェイス上のVLANが許可されないため、ネイティブVLANトラフィックを通過させるには、ネイティブVLANを許可されるVLANとして設定する必要があります（関連するVLANとして追加済みでない場合）。
ステップ 7	[no] switchport private-vlan association trunk {primary-vlan-id [secondary-vlan-id]} 例：	レイヤ2独立トランクポートを、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である必要があります。各独立トランクポートに

■ プライベート VLAN 独立トランク ポートとしてのレイヤ2インターフェイスの設定

	コマンドまたはアクション	目的
	<pre>switch(config-if)# switchport private-vlan association trunk 10 101 switch(config-if)# </pre>	<p>対し、最大 16 個のプライベート VLAN のプライマリとセカンダリのペアを関連付けられます。作業中のプライマリ VLAN とセカンダリ VLAN のペアごとに、コマンドを再入力する必要があります。</p> <p>(注) 独立トランク ポートの各セカンダリ VLAN は、別々のプライマリ VLAN に関連付ける必要があります。同じプライマリ VLAN に関連付けられた 2 つの独立 VLAN を、プライベート VLAN 独立トランク ポートに接続することはできません。これを行った場合、最新のエントリが前のエントリを上書きします。</p> <p>または プライベート VLAN 独立トランク ポートからプライベート VLAN の関連付けを削除します。</p>
ステップ 8	exit 例： <pre>switch(config-if)# exit switch(config)# </pre>	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 9	(任意) show interface switchport 例： <pre>switch# show interface switchport </pre>	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に関する情報を表示します。
ステップ 10	(任意) copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config </pre>	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。

例

次に、レイヤ2ポート 2/1 を、3つの異なるプライマリ VLAN と関連セカンダリ VLAN に関連付けられたプライベート VLAN 独立トランク ポートとして設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode private-vlan trunk
switch(config-if)# switchport private-vlan trunk allowed vlan add 1
switch(config-if)# switchport private-vlan association trunk 10 101
switch(config-if)# switchport private-vlan association trunk 20 201
switch(config-if)# switchport private-vlan association trunk 30 102
```

```
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。

Before you begin

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。

SUMMARY STEPS

1. config t
2. interface {type slot/port}
3. switchport mode private-vlan promiscuous
4. [no] switchport private-vlan mapping {primary-vlan-id} {secondary-vlan-list | add secondary-vlan-list | remove secondary-vlan-list}
5. exit
6. (Optional) show interface switchport
7. (Optional) copy running-config startup-config

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ1	config t Example: <pre>switch# config t switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ2	interface {type slot/port} Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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 Example: <pre>switch(config-if)# switchport mode private-vlan promiscuous</pre>	レイヤ2ポートをプライベート VLAN の無差別ポートとして設定します。

■ プライベート VLAN 無差別トランク ポートとしてのレイヤ2インターフェイスの設定

	Command or Action	Purpose
ステップ 4	[no] switchport private-vlan mapping {primary-vlan-id} {secondary-vlan-list add secondary-vlan-list remove secondary-vlan-list} Example: 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 のいずれかとして設定できます。 または プライベート VLAN から、マッピングをクリアします。
ステップ 5	exit Example: 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	(Optional) show interface switchport Example: switch# 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に関する情報を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	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。

Example

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 無差別トランク 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 の無差別トランク ポートとして設定し、その無差別トランク ポートを複数のプライマリ VLAN に関連付けることができます。これらの無差別トランク ポートは、複数のプライマリ VLAN と通常の VLAN のトランザクションを伝送します。



(注) プライマリ VLAN とセカンダリ VLAN は、プライベート VLAN 無差別トランク ポート上で動作可能になる前に関連付ける必要があります。

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。

手順の概要

1. **config t**
2. **interface {type slot/port}**
3. **switchport**
4. **switchport mode private-vlan trunk promiscuous**
5. (任意) **switchport private-vlan trunk native vlan vlan-id**
6. **switchport mode private-vlan trunk allowed vlan {add vlan-list | all | except vlan-list | none | remove vlan-list}**
7. [no]switchport private-vlan mapping trunk primary-vlan-id [secondary-vlan-id] {add secondary-vlan-list | remove secondary-vlan-id}
8. **exit**
9. (任意) **show interface switchport**
10. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ1	config t 例： <pre>switch# config t switch(config)#</pre>	コンフィギュレーションモードになります。
ステップ2	interface {type slot/port} 例： <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	プライベート VLAN 無差別トランク 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 例： <pre>switch(config-if)# switchport switch(config-if)#</pre>	レイヤ2ポートをスイッチポートとして設定します。

■ プライベート VLAN 無差別トランク ポートとしてのレイヤ2インターフェイスの設定

	コマンドまたはアクション	目的
ステップ 4	switchport mode private-vlan trunk promiscuous 例： <pre>switch(config-if)# switchport mode private-vlan trunk promiscuous switch(config-if)# </pre>	レイヤ2ポートを、複数のプライベート VLAN と通常の VLAN のトラフィックを伝送するための無差別トランクポートとして設定します。
ステップ 5	(任意) switchport private-vlan trunk native vlan <i>vlan-id</i> 例： <pre>switch(config-if)# switchport private-vlan trunk native vlan 5 </pre>	802.1QトランクのネイティブVLANを設定します。有効値の範囲は1～3968および4048～4093です。デフォルト値は1です。 (注) プライベート VLAN を無差別トランクポートのネイティブ VLAN として使用している場合は、プライマリ VLAN または標準 VLAN の値を入力する必要があります。セカンダリ VLAN をネイティブ VLAN として設定することはできません。
ステップ 6	switchport mode private-vlan trunk allowed vlan {add <i>vlan-list</i> all except <i>vlan-list</i> none remove <i>vlan-list</i> } 例： <pre>switch(config-if)# switchport private-vlan trunk allowed vlan add 1 switch(config-if)# </pre>	プライベート VLAN 無差別トランクインターフェイスの許可 VLAN を設定します。有効値の範囲は1～3968および4048～4093です。 プライベートプライマリ VLAN およびセカンダリ VLAN を無差別トランクポートにマッピングすると、すべてのプライマリ VLAN がこのポートの許可される VLAN リストに自動的に追加されます。 (注) ネイティブ VLAN が許可される VLAN リストに含まれていることを確認します。このコマンドでは、デフォルトでこのインターフェイス上の VLAN が許可されないため、ネイティブ VLAN トラフィックを通過させるには、ネイティブ VLAN を許可される VLAN として設定する必要があります（関連する VLAN として追加済みでない場合）。
ステップ 7	[no]switchport private-vlan mapping trunk <i>primary-vlan-id</i> [<i>secondary-vlan-id</i>] { add <i>secondary-vlan-list</i> remove <i>secondary-vlan-id</i> } 例： <pre>switch(config-if)# switchport private-vlan mapping trunk 4 5 switch(config-if)# </pre>	無差別トランクポートと、プライマリ VLAN および選択した関連するセカンダリ VLAN のリストをマッピングするかマッピングを削除します。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。トラフィックを通過させるには、プライマリ VLAN とセカンダリ VLAN の間のプライベート VLAN の関連付けが動作する必要があります。各無差別トランクポートに対し、最大16個のプライベート VLAN のプライマリとセカンダリのペアをマッピングできます。

	コマンドまたはアクション	目的
		作業しているプライマリ VLAN それぞれに対してコマンドを再入力する必要があります。 または インターフェイスからプライベート VLAN 無差別トランク マッピングを削除します。
ステップ 8	exit 例： <pre>switch(config-if)# exit switch(config)#</pre>	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 9	(任意) show interface switchport 例： <pre>switch# show interface switchport</pre>	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に関する情報を表示します。
ステップ 10	(任意) copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	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。

例

次に、レイヤ 2 ポート 2/1 を、2 つのプライマリ VLAN とそれに関連するセカンダリ VLAN に関連付けられた無差別トランク ポートとして設定する例を示します。

```
switch# config t  
switch(config)# interface ethernet 2/1  
switch(config-if)# switchport  
switch(config-if)# switchport mode private-vlan trunk promiscuous  
switch(config-if)# switchport private-vlan trunk allowed vlan add 1  
switch(config-if)# switchport private-vlan mapping trunk 10 20  
switch(config-if)# switchport private-vlan mapping trunk 11 21  
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 <i>vlan-id</i>	VLAN 情報を表示します。
show vlan private-vlan [type]	プライベート VLAN に関する情報を表示します。

■ プライベート VLAN の統計情報の表示とクリア

コマンド	目的
show interface private-vlan mapping	プライベート VLAN マッピングのインターフェイスの情報を表示します。
show interface vlan <i>primary-vlan-id</i> private-vlan mapping	プライベート VLAN マッピングのインターフェイスの情報を表示します。
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に関する情報を表示します。

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 <i>vlan-id</i>] 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)# exit
switch(config)# vlan 3
switch(config-vlan)# private-vlan community
switch(config-vlan)# exit
switch(config)# vlan 4
switch(config-vlan)# private-vlan isolated
switch(config-vlan)# exit

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

```

```

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

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

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

```

プライベート VLAN の追加情報 (CLI バージョン)

関連資料

関連項目	マニュアルタイトル
VLAN インターフェイス、IP アドレス指定	『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』
スタティック MAC アドレス、セキュリティ	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』
Cisco NX-OS の基礎	『Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide』
高可用性	『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』
システム管理	『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』
ライセンス	『Cisco NX-OS Licensing Guide』
リリースノート	『Cisco Nexus 9000 Series NX-OS Release Notes』

■ プライベート VLAN の追加情報 (CLI バージョン)**標準**

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
• CISCO-PRIVATE-VLAN-MIB	詳細については、 https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html を参照してください。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。