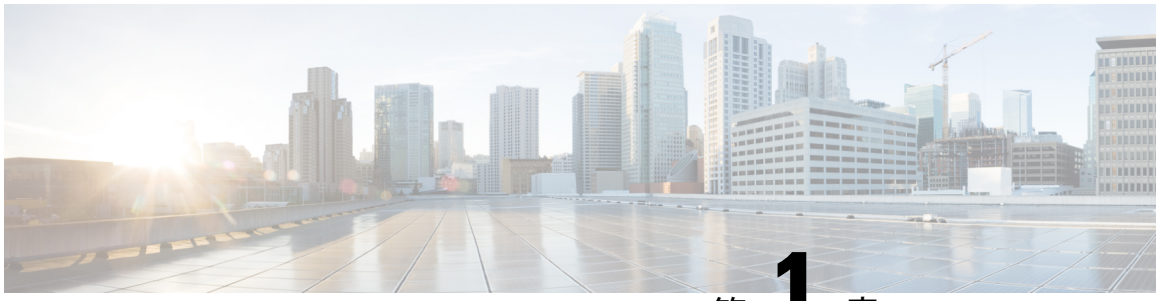
Cisco IOS XE Bengaluru 17.6.x（Catalyst 9300 スイッチ）VLAN コンフィギュレーション ガイド

初版：2021 年 7 月 31 日

最終更新：2023 年 7 月 25 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

VTP の設定

VTP の前提条件

VLAN を作成する前に、ネットワークで VLAN Trunking Protocol（VTP）を使用するかどうかを決定する必要があります。VTP を使用すると、1 台または複数のデバイス上で集中的に設定変更を行い、その変更を自動的にネットワーク上の他のデバイスに伝達できます。VTP を使用しない場合、VLAN 情報を他のデバイスに送信することはできません。

VTP は、1 つのデバイスで行われた更新が VTP を介してドメイン内の他のデバイスに送信される環境で動作するように設計されています。VLAN データベースに対する複数の更新が同一ドメイン内のデバイス上で同時に発生する環境の場合、VTP は適切に機能せず、VLAN データベースの不整合が生じます。

[**no**] **vtp** インタフェイス コンフィギュレーション コマンドを使用すると、ポート単位で VTP をイネーブルまたはディセーブルにできます。トランク ポート上で VTP をディセーブルにすると、そのポートのすべての VTP インスタンスがディセーブルになります。VTP の設定を、MST データベースには *off* にする一方で、同じポートの VLAN データベースには *on* にすることはできません。

グローバルに VTP モードをオフに設定すると、システムのすべてのトランク ポートにこの設定が適用されます。ただし、VTP インスタンス ベースでこのモードのオンまたはオフを指定することはできます。たとえば、VLAN データベースには、デバイスを VTP サーバーとして設定する一方で、MST データベースには VTP を *off* に設定することができます。

トランクポートは VTP アドバタイズを送受信するので、デバイスまたはデバイススタック上で少なくとも 1 つのトランクポートが設定されており、そのトランクポートが別のデバイスのトランクポートに接続されていることを確認する必要があります。そうでない場合、デバイスは VTP アドバタイズを受信できません。

VTP の制約事項

次に、VTP に関する制約事項を示します。

⚠

注意 VTP クライアントデバイスを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のデバイスのコンフィギュレーション リビジョン番号より小さいことを確認してください。VTP ドメイン内のデバイスは常に、VTP コンフィギュレーション リビジョン番号が最大のデバイスの VLAN コンフィギュレーションを使用します。VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つデバイスを追加すると、VTP サーバーおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。

VTP の概要

ここでは、VTP および VTP の設定について説明します。

VTP

VTP は、レイヤ 2 のメッセージ プロトコルであり、ネットワーク全体にわたって VLAN の追加、削除、名前の変更を管理することにより、VLAN 設定の整合性を維持します。VTP により、VLAN 名の重複、誤った VLAN タイプの指定、セキュリティ違反など、さまざまな問題を引き起こしかねない設定の誤りや矛盾が最小限に抑えられます。

VTP 機能はスタック全体でサポートされており、スタック内のすべてのデバイスが、アクティブデバイスから継承した同一の VLAN および VTP コンフィギュレーションを保持します。デバイスが VTP メッセージを通じて新しい VLAN について学習したり、ユーザーが新しい VLAN を設定したりすると、新しい VLAN 情報がスタック内のすべてのデバイスに伝達されます。

デバイスがスタックに参加するか、またはスタックの結合が発生すると、新しいデバイスはアクティブデバイスから VTP 情報を取得します。

VTP ドメイン

VTP ドメイン（別名 VLAN 管理ドメイン）は、1 つのデバイス、または複数の相互接続されたデバイス、または同じ VTP ドメイン名を共有して同一管理下にあるデバイスで構成されます。デバイスは、1 つの VTP ドメインにしか入ることができません。そのドメインに対してグローバル VLAN の設定を変更します。

デフォルトの設定では、トランクリンク（複数 VLAN のトラフィックを伝送するリンク）を介してドメインについてのアドバタイズを受信しない限り、またはユーザーがドメイン名を設定しない限り、デバイスはVTP非管理ドメインステートです。ドメイン名を指定しなくても、VTP サーバーで VLAN を作成または変更できます。ただし、管理ドメイン名が指定されていない場合、VLAN 情報はネットワークを介して伝播されません。

デバイスが、トランクリンクを介して VTP アドバタイズを受信した場合、管理ドメイン名および VTP 設定のリビジョン番号を継承します。その後デバイスは、別のドメイン名または古いコンフィギュレーション リビジョン番号が指定されたアドバタイズについては、すべて無視します。

VTP サーバー上の VLAN 設定を変更すると、その変更は VTP ドメイン内のすべてのデバイスに伝播されます。VTP アドバタイズは、IEEE 802.1Q を含め、すべての IEEE トランク接続に送信されます。VTP は、複数の LAN タイプにわたり、固有の名前と内部インデックスの対応によって VLAN を動的にマッピングします。このマッピングにより、ネットワーク管理者がデバイスを管理するための作業負担が大幅に軽減されます。

VTP トランスペアレントモードでデバイスを設定した場合、VLANの作成および変更は可能ですが、その変更はドメイン内の他のデバイスには送信されません。また、変更が作用するのは、個々のデバイスに限られます。ただし、デバイスがこのモードのときに設定を変更すると、変更内容がデバイスの実行コンフィギュレーションに保存されます。この変更はデバイスのスタートアップ コンフィギュレーション ファイルに保存することもできます。

VTP モード

表 *1 : VTP* モード

VTP モード	説明
VTP サーバ	VTP サーバ モードでは、VLAN の作成、変更、削除ができます。また、VTP ドメイ 他のコンフィギュレーション パラメータ（VTP バージョンなど）を指定できます。 は、同一 VTP ドメイン内の他のデバイスに自身の VLAN 設定をアドバタイズし、ト 介して受信したアドバタイズに基づいて、自身の VLAN 設定を他のデバイスと同期 VTP サーバがデフォルトのモードです。 VTP サーバ モードでは、VLAN 設定は NVRAM に保存されます。デバイスがコンフ ンを NVRAM に書き込んでいる間に障害を検出すると、VTP モードはサーバーモー ントモードに自動的に移行します。この場合、NVRAM が正常に動作するまで、デ サーバーモードに戻すことはできません。
VTP クライアント	VTP クライアントは VTP サーバと同様に機能し、そのトランクで VTP アップデー すが、VTP クライアント上で VLAN の作成、変更、削除を行うことはできません。 インに含まれる、他のサーバーモードのデバイスで設定します。 VTP バージョン 1 および 2 の VTP クライアント モードでは、VLAN 設定は NVRAM せん。VTP バージョン 3 では、VLAN 設定はクライアント モードで NVRAM に保存

VTP モード	説明
VTP トランスペアレント	VTP トランスペアレントデバイスは、VTP に参加しません。VTP トランスペアレントデ 身の VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて自身の VLAN 設 せることもありません。ただし、VTP バージョン 2 またはバージョン 3 では、トランス デバイスは、トランクインターフェイスを介して他のデバイスから受信した VTP アドバ 送します。VTP トランスペアレントモードでは、デバイス上の VLAN を作成、変更、削 す。 VTP バージョン 1 および 2 では、プライベート VLAN を作成するときに、デバイスは V ペアレントモードにする必要があります。また、このプライベート VLAN の設定後は V トランスペアレントモードからクライアントモードやサーバーモードに変更しないでくだ バージョン 3 では、クライアント モードとサーバー モードでもプライベート VLAN をサ す。プライベート VLAN が設定されている場合、VTP モードをトランスペアレントから ト モードやサーバー モードに変更しないでください。 デバイスが VTP トランスペアレントモードの場合、VTP および VLAN の設定は NVRA れますが、他のデバイスにはアドバタイズされません。このモードでは、VTP モードお ン名はデバイスの実行コンフィギュレーションに保存されます。この情報をデバイスのス プ コンフィギュレーション ファイルに保存するには、**copy running-config startup-confi** コマンドを使用します。 デバイススタックでは、実行コンフィギュレーションと保存されているコンフィギュレー スタック内のすべてのデバイスについて同じです。
VTP オフ	VTP オフモードでのデバイスの機能は、トランクを介して VTP アドバタイズを転送しな くと VTP トランスペアレントデバイスとしての機能と同じです。

VTP アドバタイズ

VTP ドメイン内の各デバイスは、専用のマルチキャストアドレスに対して、それぞれのトランクポートからグローバル コンフィギュレーション アドバタイズを定期的に送信します。ネイバーデバイスは、このようなアドバタイズを受信し、必要に応じて各自の VTP および VLAN 設定をアップデートします。

トランク ポートは VTP アドバタイズを送受信するので、スイッチ スタック上で少なくとも 1 つのトランクポートが設定されており、そのトランク ポートが別のスイッチのトランク ポートに接続されていることを確認する必要があります。そうでない場合、スイッチは VTP アドバタイズを受信できません。

VTP アドバタイズにより、次のグローバル ドメイン情報が配信されます。

- VTP ドメイン名
- VTP 設定のリビジョン番号
- アップデート ID およびアップデート タイムスタンプ

- 各 VLAN の最大伝送単位（MTU）サイズを含む MD5 ダイジェスト VLAN コンフィギュレーション
- フレーム形式

VTP アドバタイズではさらに、設定されている各 VLAN について、次の VLAN 情報が配信されます。

- VLAN ID（IEEE 802.1Q を含む）
- VLAN 名
- VLAN タイプ
- VLAN ステート
- VLAN タイプ固有のその他の VLAN 設定情報

VTP バージョン 3 では、VTP アドバタイズにはプライマリ サーバ ID、インスタンス番号、および開始インデックスも含まれます。

VTP バージョン 2

ネットワークで VTP を使用する場合、VTP のどのバージョンを使用するかを決定する必要があります。デフォルトでは、バージョン 1 の VTP が動作します。

VTP バージョン 1 でサポートされず、バージョン 2 でサポートされる機能は、次のとおりです。

- トークンリング サポート：VTP バージョン 2 は、トークンリング ブリッジ リレー機能（TrBRF）およびトークンリング コンセントレータ リレー機能（TrCRF）VLAN をサポートします。
- 認識不能な Type-Length-Value（TLV）のサポート：VTP サーバまたは VTP クライアントは、TLV が解析不能であっても、設定の変更を他のトランクに伝播します。認識されなかった TLV は、デバイスが VTP サーバーモードで動作している場合、NVRAM に保存されます。
- バージョン依存型トランスペアレントモード：VTP バージョン 1 の場合、VTP トランスペアレントデバイスが VTP メッセージ中のドメイン名およびバージョンを調べ、バージョンおよびドメイン名が一致する場合に限りメッセージを転送します。VTP バージョン 2 がサポートするドメインは 1 つだけですが、VTP バージョン 2 トランスペアレントデバイスは、ドメイン名が一致した場合のみメッセージを転送します。
- 整合性検査：VTP バージョン 2 では、CLI または SNMP を介して新しい情報が入力された場合に限り、VLAN 整合性検査（VLAN 名、値など）を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージの MD5 ダイジェストが有効であれば、情報を受け入れます。

VTP バージョン 3

VTP バージョン 1 または 2 でサポートされず、バージョン 3 でサポートされる機能は、次のとおりです。

- 拡張認証：認証を **hidden** または **secret** として設定できます。設定を **hidden** にした場合、パスワード文字列からの秘密鍵は VLAN のデータベースファイルに保存されますが、設定においてプレーンテキストで表示されることはありません。代わりに、パスワードに関連付けられているキーが 16 進表記で実行コンフィギュレーションに保存されます。ドメインにテイクオーバー コマンドを入力する際は、パスワードを再入力する必要があります。**secret** キーワードを入力する場合、パスワードに秘密鍵を直接設定できます。
- 拡張範囲 VLAN （VLAN 1006 ～ 4094）データベース伝播のサポート：VTP バージョン 1 および 2 では VLAN 1 ～ 1005 だけが伝播されます。

（注） VTP プルーニングは引き続き VLAN 1 ～ 1005 にだけ適用され、VLAN 1002 ～ 1005 は予約されたままで変更できません。

- プライベート VLAN のサポート。
- ドメイン内のデータベースのサポート：VTP 情報の伝播に加え、バージョン 3 では、Multiple Spanning Tree（MST）プロトコル データベース情報も伝播できます。VTP プロトコルの個別インスタンスが VTP を使用する各アプリケーションで実行されます。
- VTP プライマリ サーバと VTP セカンダリ サーバ：VTP プライマリ サーバは、データベース情報を更新し、システム内のすべてのデバイスに適用されるアップデートを送信します。VTP セカンダリ サーバで実行できるのは、プライマリ サーバから NVRAM に受け取ったアップデート済み VTP コンフィギュレーションのバックアップだけです。

  デフォルトでは、すべてのデバイスはセカンダリ サーバとして起動します。**vtp primary** 特権 EXEC コマンドを入力して、プライマリサーバを指定することができます。プライマリ サーバのステータスは、管理者がドメインでテイクオーバー メッセージを発行する場合、データベースのアップデート用に必要となるだけです。プライマリ サーバなしで実用 VTP ドメインを持つことができます。プライマリサーバーのステータスは、デバイスにパスワードが設定されている場合でも、装置がリロードしたり、ドメインのパラメータが変更したりすると失われます。
- サーバーモードの VTP バージョン 3 では、VLAN 構成は vlan.dat ファイルに保存されます。トランスペアレントモードの場合のように、VLAN 構成は NVRAM に保存されません。スイッチ構成のバックアップを作成するときに、vlan.dat ファイルのバックアップも作成する必要があります。

（注） VTP バージョン 1 および 2 は標準 VLAN（VLAN 1 ー 1001）のみをパブリッシュでき、拡張 VLAN（VLAN 1006 ー 4094）はフラッシュドライブまたは実行コンフィギュレーションにローカルに保存されます。VTP バージョン 3 は、VTP ドメイン全体に拡張 VLAN をパブリッシュでき、拡張 VLAN はローカルに保存されません。

VTP プルーニング

VTP プルーニングを使用すると、トラフィックが宛先デバイスに到達するために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されるので、使用可能なネットワーク帯域幅が増えます。VTP プルーニングを使用しない場合、デバイスは受信側のデバイスで廃棄される可能性があっても、VTP ドメイン内のすべてのトランクリンクに、ブロードキャスト、マルチキャスト、および不明のユニキャストトラフィックをフラッディングします。VTP プルーニングはデフォルトでディセーブルです。

VTP プルーニングは、プルーニング適格リストに指定された VLAN トランク ポートへの不要なフラッディング トラフィックを阻止します。プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。デフォルトでは、VLAN 2 ～ 1001 がプルーニング適格デバイストランクポートです。プルーニング不適格として設定した VLAN については、引き続きフラッディングが行われます。VTP プルーニングはすべてのバージョンの VTP でサポートされます。

図 *1 : VTP* プルーニングを使用しない場合のフラッディング トラフィック

VTP プルーニングは、スイッチド ネットワークでは無効です。デバイス A のポート 1 およびデバイス D のポート 2 は、Red という VLAN に割り当てられています。デバイス A に接続されたホストからブロードキャストが送信された場合、デバイス A は、このブロードキャストをフラッディングします。Red VLAN にポートを持たないデバイス C、E、F も含めて、ネットワーク内のすべてのデバイスがこのブロードキャストを受信します。

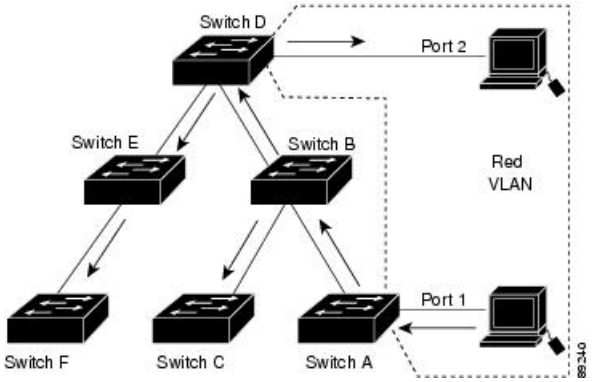
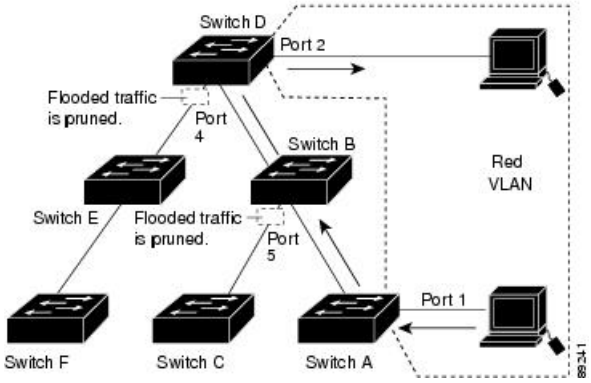


図 *2: VTP* プルーニングによるフラッディング トラフィックの最適化

VTP プルーニングは、スイッチドネットワークでは有効です。デバイス A からのブロードキャスト トラフィックは、デバイス C、E、F には転送されません。図に示されているリンクポート（デバイス B のポート 5、およびデバイス D のポート 4）で、Red VLAN のトラフィックがプルーニングされるからです。



VTP バージョン 1 および 2 では、VTP サーバーでプルーニングをイネーブルにすると、その VTP ドメイン全体でプルーニングがイネーブルになります。VTP バージョン 3 では、ドメイン内の各デバイス上で手動によってプルーニングを有効にする必要があります。VLAN をプルーニング適格または不適格として設定する場合、影響を受けるのは、そのトランク上の VLAN のプルーニングだけです（VTP ドメイン内のすべてのデバイスに影響するわけではありません）。

VTP プルーニングは、イネーブルにしてから数秒後に有効になります。VTP プルーニング不適格の VLAN からのトラフィックは、プルーニングの対象になりません。VLAN 1 および VLAN 1002 ～ 1005 は常にプルーニング不適格です。これらの VLAN からのトラフィックはプルーニングできません。拡張範囲 VLAN（1005 を超える VLAN ID）もプルーニング不適格です。

VTP とデバイススタック

VTP 設定は、デバイススタックのすべてのメンバで同一です。デバイススタックが VTP サーバーまたはクライアントモードになっている場合は、スタック内のすべてのデバイスの VTP 設定が同一になります。VTP モードがトランスペアレントの場合は、スタックは VTP には加入しません。

- スタックに参加したデバイスは、VTP および VLAN のプロパティをアクティブデバイスから継承します。
- すべての VTP アップデートが、スタック全体で保持されます。
- スタック内のデバイスの VTP モードが変更されると、そのスタック内のその他のデバイスも VTP モードを変更し、デバイスの VLAN データベースの一貫性が保たれます。

VTP バージョン 3 は、スタンドアロンデバイスでもスタックでも同じように機能しますが、スイッチスタックが VTP データベースのプライマリサーバーである場合だけは例外です。この場合は、アクティブデバイスの MAC アドレスがプライマリサーバー ID として使用されます。

アクティブデバイスがリロードまたは電源オフになると、新しいアクティブデバイスが選択されます。

- 固定 MAC アドレス機能を設定しない場合、新しいアクティブデバイスが選択されると、プライマリサーバーとして新しいアクティブな MAC アドレスが記述されたテイクオーバーメッセージを送信します。
- 固定 MAC アドレスが設定されている場合、新しいアクティブデバイスは設定されているタイマー値の間待機します。この時間内に以前のアクティブデバイスがスタックに再参加しなければ、新しいアクティブデバイスがテイクオーバーメッセージを発行します。

VTP 設定時の注意事項

ここでは、VTP 設定時の注意事項について説明します。

VTP の設定要件

VTP を設定する場合は、デバイスがドメイン内の他のデバイスと VTP アドバタイズを送受信できるように、トランクポートを設定する必要があります。

VTP バージョン 1 および 2 ではプライベート VLAN をサポートしません。VTP バージョン 3 ではプライベート VLAN をサポートします。プライベート VLAN を設定した場合、デバイスは VTP トランスペアレントモードでなければなりません。プライベート VLAN がデバイスに設定されている場合、VTP モードをトランスペアレントモードからクライアントモードやサーバーモードに変更しないでください。

VTP の設定

VTP 情報は VTP VLAN データベースに保存されます。VTP モードが透過的である場合、VTP ドメイン名およびモードはデバイス実行コンフィギュレーション ファイルに保存されます。この情報をデバイス スタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを入力します。デバイスをリセットした場合にも、VTP モードをトランスペアレントとして保存するには、このコマンドを使用する必要があります。

デバイスのスタートアップ コンフィギュレーション ファイルに VTP 情報を保存して、デバイスを再起動すると、デバイスの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

VTP 設定のためのドメイン名

VTP を初めて設定するときは、必ずドメイン名を割り当てる必要があります。また、VTP ドメイン内のすべてのデバイスを、同じドメイン名で設定しなければなりません。VTP トランスペアレントモードのデバイスは、他のデバイスと VTP メッセージを交換しません。これらのコントローラについては VTP ドメイン名を設定する必要はありません。

（注） NVRAM および DRAM の記憶域が十分にある場合は、VTP ドメイン内のすべてのデバイスを VTP サーバーモードにする必要があります。

注意 すべてのデバイスが VTP クライアントモードで動作している場合は、VTP ドメインを設定しないでください。ドメインを設定すると、そのドメインの VLAN 設定を変更できなくなります。VTP ドメイン内の少なくとも 1 台のデバイスを VTP サーバーモードに設定してください。

VTP ドメインのパスワード

VTP ドメインのパスワードは設定できますが、必須ではありません。ドメインパスワードを設定する場合は、すべてのドメインデバイスで同じパスワードを共有し、管理ドメイン内のデバイスごとにパスワードを設定する必要があります。パスワードのないデバイス、またはパスワードが不正なコントローラは、VTP アドバタイズを拒否します。

ドメインに VTP パスワードを設定する場合、VTP 設定なしで起動したデバイスは、正しいパスワードを使用して設定しない限り、VTP アドバタイズを受信しません。設定後、デバイスは同じパスワードおよびドメイン名を使用した次の VTP アドバタイズを受信します。

VTP 機能を持つ既存のネットワークに新しいデバイスを追加した場合、その新しいデバイスに適切なパスワードを設定して初めて、そのコントローラはドメイン名を学習します。

注意 VTP ドメインパスワードを設定したにもかかわらず、ドメイン内の各デバイスに管理ドメインパスワードを割り当てなかった場合には、管理ドメインが正常に動作しません。

VTP バージョン

実装する VTP バージョンを決定する場合は、次の注意事項に従ってください。

- VTP ドメイン内のすべてのデバイスは同じドメイン名を使用する必要がありますが、すべてが同じ VTP バージョンを実行する必要はありません。
- VTP バージョン 2 対応のデバイス上で VTP バージョン 2 がディセーブルに設定されている場合、VTP バージョン 2 対応デバイスは、VTP バージョン 1 を実行しているデバイスと同じ VTP ドメインで動作できます（デフォルトでは VTP バージョン 2 はディセーブルになっています）。

- VTP バージョン 1 を実行しているものの、VTP バージョン 2 に対応可能なデバイスが VTP バージョン 3 アドバタイズを受信すると、このコントローラは VTP バージョン 2 に自動的に移行します。
- VTP バージョン 3 を実行しているデバイスが VTP バージョン 1 を実行しているデバイスに接続すると、VTP バージョン 1 のデバイスは VTP バージョン 2 に移行し、VTP バージョン 3 のデバイスは、スケールダウンしたバージョンの VTP パケットを送信するため、VTP バージョン 2 デバイスは自身のデータベースをアップデートできます。
- VTP バージョン 3 を実行するデバイスは、拡張 VLAN を持つ場合はバージョン 1 または 2 に移行できません。
- 同一 VTP ドメイン内のすべてのデバイスがバージョン 2 に対応する場合を除き、デバイス上で VTP バージョン 2 をイネーブルにしないでください。1 つのデバイスでバージョン 2 をイネーブルにすると、ドメイン内のすべてのバージョン 2 対応デバイスでバージョン 2 がイネーブルになります。バージョン 1 専用のデバイスがドメインに含まれている場合、そのコントローラはバージョン 2 対応デバイスとの間で VTP 情報を交換できません。
- VTP バージョン 1 および 2 デバイスは、VTP バージョン 3 アドバタイズメントを転送できないため、ネットワークのエッジに配置することをお勧めします。
- 使用環境に TrBRF および TrCRF トークンリング ネットワークが含まれている場合に、トークンリング VLAN スイッチング機能を正しく動作させるには、VTP バージョン 2 またはバージョン 3 をイネーブルにする必要があります。トークンリングおよびトークンリング Net を実行する場合は、VTP バージョン 2 をディセーブルにします。
- VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN（VLAN 1006 ～ 4094）の設定情報を伝播しません。これらの VLAN は各装置で手動によって設定する必要があります。VTP バージョン 3 は拡張範囲 VLAN と、拡張範囲 VLAN データベースの伝播をサポートします。
- VTP バージョン 3 装置のトランク ポートが VTP バージョン 2 装置からのメッセージを受信した場合、この装置は、VLAN データベースをスケールダウンし、その特定のトランク上で VTP バージョン 2 フォーマットを使用して送信します。VTP バージョン 3 装置は、最初にそのトランク ポートで VTP バージョン 2 パケットを受信しない限り、VTP バージョン 2 フォーマットのパケットを送信しません。
- VTP バージョン 3 装置が、あるトランク ポートで VTP バージョン 2 装置を検出した場合、両方のネイバーが同一トランク上で共存できるように、VTP バージョン 2 パケットだけでなく VTP バージョン 3 パケットの送信も継続します。
- VTP バージョン 3 装置は、VTP バージョン 2 またはバージョン 1 の装置からの設定情報は受け入れません。
- 2 つの VTP バージョン 3 リージョンは、VTP バージョン 1 リージョンまたはバージョン 2 リージョンでは、トランスペアレント モードでだけ通信できます。
- VTP バージョン 1 にだけ対応する装置は、VTP バージョン 3 装置との相互運用はできません。

- VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN（VLAN 1006 ～ 4094）の設定情報を伝播しません。これらの VLAN を各装置上に手動で設定する必要があります。

VTP の設定方法

ここでは、VTP の設定について説明します。

VTP モードの設定

次のいずれかに VTP モードを設定できます。

- VTP サーバー モード：VTP サーバー モードでは、VLAN の設定を変更し、ネットワーク全体に伝播させることができます。
- VTP クライアント モード：VTP クライアント モードでは、VLAN の設定を変更できません。クライアントデバイスは、VTP ドメイン内の VTP サーバーから VTP アップデート情報を受信し、それに基づいて設定を変更します。
- VTP トランスペアレントモード：VTP トランスペアレントモードでは、デバイスで VTP がディセーブルになります。デバイスは VTP アップデートを送信せず、他のデバイスから受信した VTP アップデートにも反応しません。ただし、VTP バージョン 2 を実行する VTP トランスペアレントモードのデバイスは、対応するトランクリンクで、受信した VTP アドバタイズを転送します。
- VTP オフ モード：VTP オフ モードは、VTP アドバタイズが転送されない以外は、VTP トランスペアレント モードと同じです。

設定したドメイン名は、削除できません。別のドメインにデバイスを再び割り当てるしかありません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**vtp domain** *domain-name* 例： `Device(config)# vtp domain eng_group`	VTP 管理ドメイン名を設定します。1 ～ 32 文字の名前を使用できます。同一管理下にある VTP サーバーモードまたはクライアントモードのデバイスは、すべて同じドメイン名に設定する必要があります。 サーバ モード以外にはこのコマンドは任意です。VTP サーバ モードではドメイン名が必要です。デバイスが VTP ドメインにトランク接続されている場合、デバイスはドメイン内の VTP サーバーからドメイン名を取得します。 他の VTP パラメータを設定する前に、VTP ドメインを設定する必要があります。
ステップ 4	**vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**} 例： `Device(config)# vtp mode server`	VTP モード（クライアント、サーバー、トランスペアレント、またはオフ）のデバイスの設定。 • **vlan**：何も設定されていない場合は VLAN データベースがデフォルトです。 • **mst**：マルチ スパニング ツリー（MST）データベース。 • **unknown**：データベース タイプは不明です。
ステップ 5	**vtp password** *password* 例： `Device(config)# vtp password mypassword`	（任意）VTP ドメイン用のパスワードを設定します。パスワードに使用できる文字数は 8 ～ 64 文字です。VTP パスワードを設定したにもかかわらず、ドメイン内の各デバイスに同じパスワードを割り当てなかった場合には、VTP ドメインが正常に動作しません。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show vtp status** 例： `Device# show vtp status`	表示された *[VTP Operating Mode]* および *[VTP Domain Name]* フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）スタートアップ コンフィギュレーション ファイルに設定を保存します。 デバイスの実行コンフィギュレーションに保存され、スタートアップ コンフィギュレーション ファイルにコピーできるのは、VTP モードおよびドメイン名だけです。

VTP バージョン 3 のパスワードの設定

デバイスで VTP バージョン 3 のパスワードを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp version 3** 例： `Device(config)# vtp version 3`	デバイスで VTP バージョン 3 を有効にします。デフォルトは VTP バージョン 1 です。
ステップ 4	**vtp password** *password* [**hidden** | **secret**] 例： `Device(config)# vtp password mypassword`	（任意）VTP ドメイン用のパスワードを設定します。パスワードに使用できる文字数は 8 ～ 64 文字です。

	コマンドまたはアクション	目的
	hidden	• （任意）**hidden**：パスワード文字列から生成される秘密キーが、nvram:vlan.dat ファイルに保存されます。VTP プライマリ サーバーを設定してテイクオーバーを設定しようとすると、パスワードの再入力を要求されます。 • （任意）**secret**：パスワードを直接設定します。シークレットパスワードには 16 進数文字を 32 個含める必要があります。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show vtp password** 例： `Device# show vtp password`	VTP パスワードが設定されているかどうかを確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

VTP バージョン 3 のプライマリ サーバの設定

VTP サーバを VTP プライマリ サーバとして設定すると、テイクオーバー操作が開始されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**vtp version 3** 例： `Device(config)# vtp version 3`	デバイスで VTP バージョン 3 を有効にします。デフォルトは VTP バージョン 1 です。

	コマンドまたはアクション	目的
ステップ 2	**vtp primary** [**vlan** | **mst**] [**force**] 例： `Device# vtp primary vlan force`	デバイスの動作ステートをセカンダリサーバー（デフォルト）からプライマリサーバーに変更し、その設定をドメインにアドバタイズします。デバイスのパスワードが **hidden** に設定されている場合は、パスワードの再入力を要求されます。 • （任意）**vlan**：テイクオーバー機能として VLAN データベースを選択します。これはデフォルトです。 • （任意）**mst**：テイクオーバー機能としてマルチスパニングツリー（MST）データベースを選択します • （任意）**force**：競合するサーバの設定が上書きされます。**force** を入力しない場合、テイクオーバーの実行前に確認を求められます。

VTP バージョンのイネーブル化

デフォルトで VTP バージョン 2 およびバージョン 3 はディセーブルになっています。

- 1 つのデバイス上で VTP バージョン 2 をイネーブルにすると、VTP ドメイン内の VTP バージョン 2 に対応可能なすべてのデバイスでバージョン 2 がイネーブルになります。VTP バージョン 3 をイネーブルにするには、各デバイス上で手動によって設定する必要があります。
- VTP バージョン 1 および 2 では、このバージョンを設定できるのは、VTP サーバーモードまたはトランスペアレントモードのデバイスだけです。デバイスが VTP バージョン 3 を実行し、かつデバイスがクライアントモードの場合、既存の拡張 VLAN や既存のプライベート VLAN がなく、パスワードが非表示に設定されていないときであれば、バージョン 2 に変更できます。

⚠

注意 同一 VTP ドメイン内のデバイス上で、VTP バージョン 1 と VTP バージョン 2 は相互運用できません。VTP ドメイン内のすべてのデバイスが VTP バージョン 2 をサポートしている場合を除き、VTP バージョン 2 をイネーブルにはしないでください。

- TrCRF および TrBRF トークンリング環境では、トークンリング VLAN スイッチング機能を正しく動作させるために、VTP バージョン 2 または VTP バージョン 3 をイネーブルに

する必要があります。トークンリングおよびトークンリング Net メディアの場合は、VTP バージョン 2 をディセーブルにします。

注意　VTP バージョン 3 では、プライマリ サーバとセカンダリ サーバの両方がドメイン内の 1 つのインスタンスに存在できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp version** {**1** | **2** | **3**} 例： `Device(config)# vtp version 2`	デバイスで VTP バージョンを有効にします。デフォルトは VTP バージョン 1 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status** 例： `Device# show vtp status`	設定された VTP バージョンがイネーブルであることを確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

VTP プルーニングのイネーブル化

始める前に

VTP プルーニングは VTP トランスペアレント モードでは機能しないように設計されています。ネットワーク内に VTP トランスペアレントモードのデバイスが 1 台または複数存在する場合は、次のいずれかの操作を実行する必要があります。

- ネットワーク全体の VTP プルーニングをオフにします。
- VTP トランスペアレントデバイスのアップストリーム側にあるデバイスのトランク上で、すべての VLAN をプルーニング不適格にすることによって、VTP プルーニングをオフにします。

インターフェイスに VTP プルーニングを設定するには、**switchport trunk pruning vlan** インターフェイス コンフィギュレーション コマンドを使用します。VTP プルーニングは、インターフェイスがトランキングを実行している場合に作用します。VLAN プルーニングの適格性は、VTP ドメインで VTP プルーニングがイネーブルであるかどうか、特定の VLAN が存在するかどうか、およびインターフェイスが現在トランキングを実行しているかどうかにかかわらず、設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp pruning** 例： `Device(config)# vtp pruning`	VTP 管理ドメインでプルーニングをイネーブルにします。 プルーニングは、デフォルトではディセーブルに設定されています。VTP サーバーモードの 1 台のデバイス上に限ってプルーニングをイネーブルにする必要があります。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 5	**show vtp status** 例： `Device# show vtp status`	表示された [VTP Pruning Mode] フィールドの設定を確認します。

ポート単位の VTP の設定

VTP バージョン 3 では、ポート単位で VTP をイネーブルまたはディセーブルにできます。VTP は、トランク モードのポート上でだけイネーブルにできます。VTP トラフィックの着信または発信はブロックされ、転送されません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**vtp** 例： `Device(config-if)# vtp`	指定したポートの VTP をイネーブルにします。
ステップ 5	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 6	**show running-config interface** *interface-id* 例： `Device# show running-config interface gigabitethernet 1/0/1`	ポートの変更を確認します。
ステップ 7	**show vtp status** 例： `Device# show vtp status`	設定を確認します。

VTP ドメインへの VTP クライアントの追加

VTP ドメインに追加する前にデバイス上で VTP コンフィギュレーション リビジョン番号を確認およびリセットするには、次の手順に従います。

始める前に

VTP クライアントを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のデバイスのコンフィギュレーション リビジョン番号より小さいことを確認してください。VTP ドメイン内のデバイスは常に、VTP コンフィギュレーション リビジョン番号が最大のデバイスの VLAN コンフィギュレーションを使用します。VTP バージョン 1 および 2 では、VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つデバイスを追加すると、VTP サーバーおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。VTP バージョン 3 では、VLAN 情報が消去されることはありません。

デバイス上で VTP をディセーブルにし、VTP ドメイン内の他のデバイスに影響を与えることなく VLAN 情報を変更するには、**vtp mode transparent** グローバル コンフィギュレーション コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**show vtp status** 例： `Device# show vtp status`	VTP コンフィギュレーション リビジョン番号をチェックします。 番号が 0 の場合は、デバイスを VTP ドメインに追加します。 番号が 0 より大きい場合は、次の手順に従います。 • ドメイン名を書き留めます。 • コンフィギュレーション リビジョン番号を書き留めます。 • 次のステップに進んで、デバイスのコンフィギュレーション リビジョン番号をリセットします。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**vtp domain** *domain-name* 例： `Device(config)# vtp domain domain123`	ドメイン名を、ステップ 1 で表示された元の名前から新しい名前に変更します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。デバイスの VLAN 情報が更新され、コンフィギュレーション リビジョン番号が 0 にリセットされます。
ステップ 6	**show vtp status** 例： `Device# show vtp status`	コンフィギュレーション リビジョン番号が 0 にリセットされていることを確認します。
ステップ 7	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 8	**vtp domain** *domain-name* 例： `Device(config)# vtp domain domain012`	デバイスの元のドメイン名を入力します。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。デバイスの VLAN 情報が更新されます。
ステップ 10	**show vtp status** 例： `Device# show vtp status`	（任意）ドメイン名がステップ 1 のものと同じであり、コンフィギュレーション リビジョン番号が 0 であることを確認します。

VTP のモニタ

ここでは、VTPの設定を表示およびモニタリングするために使用するコマンドについて説明します。

VTPの設定情報（ドメイン名、現在のVTPバージョン、VLAN数）を表示することによって、VTPをモニタします。デバイスで送受信されたアドバタイズに関する統計情報を表示することもできます。

表 *2*：*VTP* モニタ コマンド

コマンド	目的
show vtp counters	送受信された VTP メッセージに関
show vtp devices [**conflict**]	ドメイン内のすべての VTP バージ ライマリ サーバと競合する VTP ノ **devices** コマンドは、デバイスがト きは情報を表示しません。
show vtp interface [*interface-id*]	すべてのインターフェイスまたは テータスおよび設定を表示します。
show vtp password	VTP パスワードが設定されている
show vtp status	VTP デバイス設定情報を表示しま

VTP の設定例

次に、VTP の設定例を示します。

例：デバイスをプライマリサーバーとして設定する

次に、パスワードが非表示またはシークレットに設定されている場合に、VLANデータベースのプライマリサーバー（デフォルト）としてデバイスを設定する方法の例を示します。

```
Device# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP  domain

VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- --------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7

Do you want to continue (y/n) [n]? y
```

次の作業

VTP を設定したら、次の項目を設定できます。

- VLAN
- VLAN トランキング
- 音声 VLAN
- プライベート VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9300 Series Switches)*

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

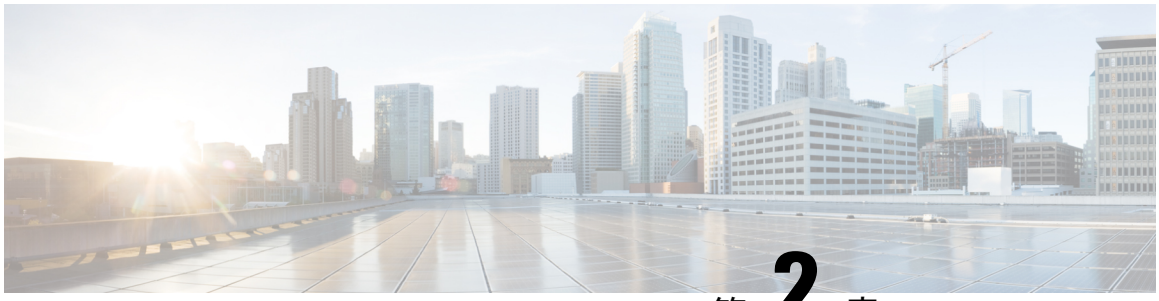
VTP の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	VLAN トランキングプロトコル（VTP）	VTP は、レイヤ 2 のメッセージ プロトコルであり、ネットワーク全体にわたってVLANの追加、削除、名前の変更を管理することにより、VLAN設定の整合性を維持します。VTPにより、VLAN名の重複、誤ったVLANタイプの指定、セキュリティ違反など、さまざまな問題を引き起こしかねない設定の誤りや矛盾が最小限に抑えられます。
Cisco IOS XE Gibraltar 16.12.4	VTP **show vtp password** コマンド出力の修正	**show vtp password** コマンドの出力は、パスワードが設定されているかどうかを表示します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 2 章

VLAN の設定

VLAN の前提条件

VLAN 設定時の前提条件と考慮事項を次に示します。

- VLANを作成する前に、VLANトランキングプロトコル（VTP）を使用してネットワークのグローバルな VLAN 設定を維持するかどうかを決定する必要があります。
- デバイスで多数の VLAN を設定し、ルーティングを有効にしない予定の場合は、Switch Database Management（SDM）機能を Access テンプレートに設定します。これにより、最大数のユニキャスト MAC アドレスをサポートするようにシステムリソースが設定されます。
- VLAN グループに VLAN を追加できるようにするため、VLAN がデバイスに存在している必要があります。

VLAN の制約事項

次に、VLAN の制約事項を示します。

- Per-VLAN Spanning-Tree（PVST）モードまたは Rapid PVST モードのスパニングツリープロトコル（STP）仮想ポートの数は、トランクの数にアクティブなVLANの数を掛けて、アクセスポートの数を足した値に基づきます。

STP 仮想ポート = トランク X トランク上のアクティブな VLAN + 非トランクポートの数。

次の例について考えてみます。

- スイッチに 40 個のトランクポート（各トランクに 100 個のアクティブな VLAN）と 8 個のアクセスポートがある場合、このスイッチの STP 仮想ポートの数は 40 X 100 + 8 = 4,008 です。
- スイッチに 8 つのトランクポート（各トランクに 200 個のアクティブな VLAN）と 40 個のアクセスポートがある場合、このスイッチの STP 仮想ポートの数は 8 X 200 + 40 = 1,640 です

STP 仮想ポートでサポートされている拡張性については、を参照してください。Cisco Catalyst 9300 シリーズ スイッチ データ シート。

- デバイスは、イーサネット ポート経由の VLAN トラフィック送信方式として IEEE 802.1Q トランキングをサポートします。
- インターフェイス VLAN にはデフォルトですでに MAC アドレスが割り当てられています。インターフェイス VLAN の MAC アドレスは、**mac-address** コマンドを使用して上書きできます。このコマンドが、レイヤ 3 のインジェクトされたパケットを必要とする単一の SVI またはルータポートで設定されている場合、デバイス上の他のすべての SVI またはルーテッドポートも、MAC アドレスの最初の 4 つの最上位ビット（4MSB）で設定する必要があります。たとえば、SVI の MAC アドレスを xxxx.yyyy.zzzz に設定する場合、他のすべての SVI の MAC アドレスは xxxx.yyyy で始まるように設定します。レイヤ 3 のインジェクトされたパケットが使用されない場合、この制限は適用されません。

（注） これは、すべてのレイヤ 3 ポート、SVI、およびルーテッドポートに適用されます。これは GigabitEthernet0/0 ポートには適用されません。

- インターフェイスの範囲がバンドルされると、VLAN インターフェイスの構成変更はポートチャネルでのみ行う必要があります。そうしないと、インターフェイスが一時停止します。
- 接続先デバイスの MAC アドレスが学習されていないか削除されており、複数のポートが特定の VLAN にマッピングされている場合、デバイスで受信された traceroute 要求に対して複数の ICMP 応答が送信されます。

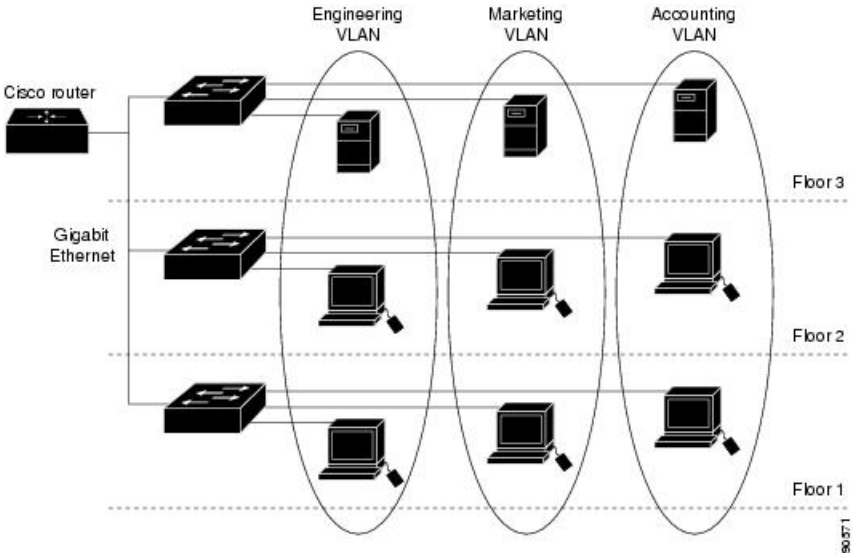
VLAN について

ここでは、VLAN に関する情報について説明します。

論理ネットワーク

VLANは、ユーザの物理的な位置に関係なく、機能、プロジェクトチーム、またはアプリケーションなどで論理的に分割されたスイッチドネットワークです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンドステーションもグループ化できます。どのようなデバイスポートでも VLAN に属することができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN 内のエンドステーションだけに転送またはフラッディングされます。各VLANは1つの論理ネットワークと見なされ、VLANに属さないステーション宛のパケットは、ルータまたはフォールバックブリッジングをサポートするデバイスを経由して伝送しなければなりません。スイッチスタックでは、VLANはスタック全体にまたがる複数のポートに設定できます。VLANはそれぞれが独立した論理ネットワークと見なされるので、VLAN ごとに独自のブリッジ管理情報ベース（MIB）情報があり、スパニングツリーの独自の実装をサポートできます。

図 *3*：論理的に定義されたネットワークとしての *VLAN*



VLAN は通常、IP サブネットワークに対応付けられます。たとえば、特定の IP サブネットに含まれるエンドステーションはすべて同じ VLAN に属します。デバイス上のインターフェイスの VLAN メンバーシップは、インターフェイスごとに手動で割り当てます。この方法でデバイスインターフェイスを VLAN に割り当てた場合、これをインターフェイスベース（またはスタティック）VLAN メンバーシップと呼びます。

VLAN 間のトラフィックは、ルーティングする必要があります。

デバイスは、デバイス仮想インターフェイス（SVI）を使用して、VLAN 間でトラフィックをルーティングできます。VLAN 間でトラフィックをルーティングするには、SVI を明示的に設定して IP アドレスを割り当てる必要があります。

サポートされる VLAN

デバイスは、VTP クライアント、サーバー、およびトランスペアレントの各モードで VLAN をサポートしています。VLAN は、1 ～ 4094 の番号で識別します。VLAN 1 はデフォルト VLAN で、システム初期化中に作成されます。

最大 4094 の VLAN をデバイスに設定できます。ただし、すべての VLAN を同時にアクティブにできるわけではありません。

MSTP モードでは、任意の時点で 1000 のアクティブ VLAN を設定できます。

VLAN ID 1002 ～ 1005 は、トークンリングおよびファイバ分散データインターフェイス（FDDI）VLAN 専用です。1002 ～ 1005 を除くすべての VLAN がユーザー設定のために使用できます。

VTP バージョン 1、バージョン 2、およびバージョン 3 の 3 つの VTP バージョンがあります。すべての VTP バージョンが標準および拡張範囲 VLAN の両方をサポートしますが、VTP バージョン 3 のみがデバイス伝播拡張範囲 VLAN 設定情報を実行します。拡張範囲 VLAN が VTP バージョン 1 および 2 で作成された場合、設定情報は伝播されません。デバイス上のローカル VTP データベースエントリも更新されませんが、拡張範囲 VLAN 設定情報が作成され、実行コンフィギュレーション ファイルに保存されます。

VLAN ポート メンバーシップ モード

VLAN に所属するポートは、メンバーシップ モードを割り当てることで設定します。メンバーシップ モードは、各ポートが伝送できるトラフィックの種類、および所属できる VLAN の数を指定します。

ポートが VLAN に所属すると、デバイスは VLAN 単位で、ポートに対応するアドレスを学習して管理します。

表 *3:* ポートのメンバーシップ モードとその特性

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
スタティック アクセス	スタティック アクセス ポートは、手動で割り当てられ、1つの VLAN だけに所属します。	VTP は必須ではありません。VTP にグローバルに情報を伝播させないようにする場合は、VTP モードをトランスペアレント モードに設定します。VTP に加入するには、別のデバイスまたはデバイススタックのトランクポートに接続されているデバイスまたはデバイススタック上に少なくとも 1 つのトランクポートが必要です。

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
トランク（IEEE 802.1Q）： • IEEE 802.1Q：業界標準のトランキング カプセル化方式です。	デフォルトで、トランク ポートは拡張範囲 VLAN を含むすべての VLAN のメンバです。ただし、メンバーシップは許可 VLAN リストを設定して制限できます。また、プルーニング適格リストを変更して、リストに指定したトランク ポート上の VLAN へのフラッディング トラフィックを阻止することもできます。	VTP を推奨しますが、必須ではありません。VTP は、ネットワーク全体にわたって VLAN の追加、削除、名前変更を管理することにより、VLAN 設定の整合性を維持します。VTP はトランクリンクを通じて他のデバイスと VLAN コンフィギュレーション メッセージを交換します。
音声 VLAN	音声 VLAN ポートは、Cisco IP Phone に接続し、電話に接続されたデバイスからの音声トラフィックに 1 つの VLAN を、データ トラフィックに別の VLAN を使用するように設定されたアクセス ポートです。	VTP は不要です。VTP は音声 VLAN に対して無効です。

VLAN コンフィギュレーション ファイル

VLAN ID 1 ～ 1005 の設定は vlan.dat ファイル（VLAN データベース）に書き込まれます。この設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。vlan.dat ファイルはフラッシュ メモリに格納されます。VTP モードがトランスペアレント モードの場合、それらの設定もデバイスの実行コンフィギュレーション ファイルに保存されます。

デバイススタックでは、スタック全体が同一の vlan.dat ファイルと実行コンフィギュレーションを使用します。一部のデバイスでは、vlan.dat ファイルがアクティブデバイスのフラッシュ メモリに保存されます。

さらに、インターフェイス コンフィギュレーション モードを使用して、ポートのメンバーシップ モードの定義、VLAN に対するポートの追加および削除を行います。これらのコマンドの実行結果は、実行コンフィギュレーション ファイルに書き込まれます。このファイルを表示するには、**show running-config** 特権 EXEC コマンドを入力します。

VLAN および VTP 情報（拡張範囲 VLAN 設定情報を含む）をスタートアップ コンフィギュレーション ファイルに保存して、デバイスを再起動すると、デバイスの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントで、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使

用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。

- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。
- VTP バージョン 1 および 2 では、VTP モードがサーバである場合、VLAN ID 1 ～ 1005 のドメイン名と VLAN 設定で VLAN データベース情報が使用されます。VTP バージョン 3 は、VLAN 1006 ～ 4094 もサポートします。

（注） スイッチの設定をリセットする前に、**write erase** コマンドを使用して、必ずコンフィギュレーション ファイルと一緒に vlan.dat ファイルを削除してください。これにより、リセット時にスイッチが正しく再起動します。

標準範囲 VLAN 設定時の注意事項

標準範囲 VLAN は、ID が 1 ～ 1005 の VLAN です。

ネットワーク内で標準範囲 VLAN を作成または変更する場合には、次の注意事項に従ってください。

- 標準範囲 VLAN は、1 ～ 1001 の番号で識別します。VLAN 番号 1002 ～ 1005 は、トークンリングおよび FDDI VLAN 専用です。
- VLAN 1 ～ 1005 の VLAN 設定は、常に VLAN データベースに格納されます。VTP モードがトランスペアレントモードの場合、VTP と VLAN の設定もデバイスの実行コンフィギュレーション ファイルに保存されます。
- デバイスが VTP サーバーモードまたは VTP トランスペアレントモードの場合は、VLAN データベース内の VLAN 2 ～ 1001 の設定を追加、変更、または削除できます。（VLAN ID 1 および 1002 ～ 1005 は自動作成され、削除できません）。
- VLAN を作成する前に、デバイスを VTP サーバーモードまたは VTP トランスペアレントモードにする必要があります。デバイスが VTP サーバーである場合には、VTP ドメインを定義する必要があります。VTP ドメインを定義しないと、VTP は機能しません。
- デバイスは、トークンリングまたはFDDIメディアをサポートしません。デバイスはFDDI、FDDI-Net、TrCRF、または TrBRF トラフィックを転送しませんが、 VTP を介して VLAN 設定を伝播します。
- 固定数のスパニング ツリー インスタンスがデバイスでサポートされています（最新情報については、『Cisco Catalyst 9300 Series Switches Data Sheet』を参照）。デバイスのアクティブな VLAN 数が、サポートされているスパニング ツリー インスタンス数より多い場合でも、スパニングツリーはサポートされている数の VLAN でのみ有効になり、残りの VLAN ではスパニングツリーは無効になります。

デバイス上の使用可能なスパニングツリー インスタンスをすべて使い切ってしまった後に、VTP ドメインの中にさらに別の VLAN を追加すると、そのデバイス上にスパニングツリーが稼働しない VLAN が生成されます。そのデバイスのトランクポート上でデフォルトの許可リスト（すべての VLAN を許可するリスト）が設定されていると、すべてのトランクポート上に新しい VLAN が割り当てられます。ネットワークトポロジによっては、新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接デバイスでスパニングツリーインスタンスをすべて使用してしまっている場合には注意が必要です。スパニングツリーインスタンスの割り当てを使い果たしたデバイスのトランクポートに許可リストを設定することにより、このような可能性を防ぐことができます。

デバイス上の VLAN の数がサポートされているスパニングツリー インスタンスの最大数を超える場合、デバイス上に IEEE 802.1s Multiple STP（MSTP）を設定して、複数の VLAN を単一のスパニングツリー インスタンスにマッピングすることを推奨します。

拡張範囲 VLAN 設定時の注意事項

拡張範囲 VLAN は、ID が 1006 ～ 4094 の VLAN です。

拡張範囲 VLAN を作成するときは次の注意事項に従ってください。

- 拡張範囲の VLAN ID は、デバイスが VTP バージョン 3 を実行していない場合は VLAN データベースに保存されず、VTP で認識されません。
- プルーニング適格範囲に拡張範囲 VLAN を含めることはできません。
- VTP バージョン 1 または 2 では、グローバル コンフィギュレーション モードで、VTP モードをトランスペアレントに設定できます。VTP トランスペアレントモードでデバイスが始動するように、この設定をスタートアップ コンフィギュレーションに保存する必要があります。このようにしないと、デバイスをリセットした場合に、拡張範囲 VLAN 設定が失われます。VTP バージョン 3 で拡張範囲 VLAN を作成する場合は、VTP バージョン 1 または 2 に変更できません。
- スイッチ スタックでは、スタック全体が同一の実行コンフィギュレーションと保存されているコンフィギュレーションを使用しており、拡張範囲 VLAN 情報はスタック全体で共有されます。

VLAN の設定方法

ここでは、標準範囲 VLAN および拡張範囲 VLAN の設定について説明します。

標準範囲 VLAN の設定方法

VLAN データベースに新しい標準範囲 VLAN を作成したり、VLAN データベース内の既存の VLAN を変更したりする場合、次のパラメータを設定できます。

- VLAN ID
- VLAN 名
- VLAN タイプ
  - イーサネット
  - Fiber Distributed Data Interface [FDDI]
  - FDDI ネットワーク エンティティ タイトル [NET]
  - TrBRF または TrCRF
  - トークンリング
  - トークンリング Net
- VLAN ステート（アクティブまたは中断）
- Security Association Identifier（SAID）
- TrBRF VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- TrCRF VLAN の親 VLAN 番号
- TrCRF VLAN のスパニングツリー プロトコル（STP）タイプ
- ある VLAN タイプから別の VLAN タイプに変換するときに使用する VLAN 番号

vlan.dat ファイルを手動で削除しようとすると、VLAN データベースに不整合が生じる可能性があります。VLAN 設定を変更する場合は、この項の手順に従ってください。

イーサネット VLAN の作成または変更

始める前に

VTP バージョン 1 および 2 でデバイスが VTP トランスペアレントモードの場合は、1006 を超える VLAN ID を割り当てることができますが、それらを VLAN データベースに追加できません。

デバイスは、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。FDDI およびトークンリング VLAN は、ローカルではサポートされないので、FDDI およびトークンリングメディア固有の特性は、他のデバイスに対する VTP グローバルアドバタイズにのみ設定します。

このデバイスはトークンリング接続をサポートしていませんが、トークンリング接続を行っているリモートデバイスを、サポート対象デバイスのうちの 1 台から管理できます。VTP バージョン 2 が稼働しているデバイスは、次のトークンリング VLAN に関する情報をアドバタイズします。

- トークンリング TrBRF VLAN

- トークンリング TrCRF VLAN

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id* 例： `Device(config)# vlan 20`	VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。新規の VLAN ID を入力して VLAN を作成するか、または既存の VLAN ID を入力してその VLAN を変更します。 （注） このコマンドで指定できる VLAN ID 範囲は 1 ～ 4094 です。
ステップ 3	**name** *vlan-name* 例： `Device(config-vlan)# name test20`	（任意）VLAN の名前を入力します。VLAN名を指定しなかった場合には、デフォルトとして、VLANという語の後ろに先行ゼロを含めた *vlan-id* 値が付加されます。たとえば、VLAN4 のデフォルトの VLAN 名は VLAN0004 になります。 次の追加 VLAN コンフィギュレーション コマンド オプションが使用可能です。 • **are**：この VLAN の All-Route Explorer（ARE）ホップの最大数を設定します。 • **backupcrf**：VLAN のバックアップ コンセントレータ リレー機能（CRF）モードをイネーブルまたはディセーブルにします。 • **bridge**：FDDI-Net またはトークンリング ネット タイプの VLAN にブリッジ番号の値を設定します。 • **exit**：変更を適用し、リビジョン番号を増分して、終了します。

	コマンドまたはアクション	目的
		• **media**：VLAN のメディア タイプを設定します。 • **no**：コマンドまたはデフォルトを拒否します。 • **parent**：FDDI の親 VLAN やトークン リング タイプの VLAN に ID の値を設定します。 • **remote-span**：リモート SPAN VLAN を設定します。 • **ring**：FDDI またはトークン リング タイプの VLAN にリング番号値を設定します。 • **said**：IEEE 802.10 SAID の値を設定します。 • **shutdown**：VLAN スイッチングをシャットダウンします。 • **state**：運用上の VLAN ステートを実行中または停止中に設定します。 • **ste**：VLAN のスパニングツリー エクスプローラ（STE）のホップの最大数を設定します。 • **stp**：VLAN のスパニングツリー特性を設定します。
ステップ 4	**media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** } 例： `Device(config-vlan)# media ethernet`	VLAN のメディア タイプを設定します。コマンドオプションは次のとおりです。 • **ethernet**：VLAN のメディア タイプをイーサネットに設定します。 • **fd-net**：VLAN のメディア タイプを FDDI-net に設定します。 • **fddi**：VLAN のメディア タイプを FDDI に設定します。 • **tokenring**：VLAN メディア タイプをトークン リングに設定します。

	コマンドまたはアクション	目的
		• **trn-net**：VLAN メディア タイプをトークン リング ネットに設定します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ステップ 7	**show vlan** { **name** *vlan-name* | **id** *vlan-id*}
	例：
	`Device# show vlan name test20`
	`or`
	`Device# show vlan id 20`
		入力を確認します。

VLAN の削除

VTP サーバモードのデバイスから VLAN を削除すると、VTP ドメイン内のすべてのデバイスの VLAN データベースから、その VLAN が削除されます。VTP トランスペアレントモードのデバイスから VLAN を削除した場合、その特定のデバイス上に限り VLAN が削除されます。

イーサネット VLAN 1 および FDDI、またはトークンリング VLAN 1002 ～ 1005 の、メディアタイプ別のデフォルト VLAN は削除できません。

⚠

注意 VLAN を削除すると、その VLAN に割り当てられていたすべてのポートが非アクティブになります。これらのポートは、新しい VLAN に割り当てられるまで、元の VLAN に（非アクティブで）対応付けられたままです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no vlan** *vlan-id* 例： `Device(config)# no vlan 4`	VLAN ID を入力して、VLAN を削除します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vlan brief** 例： `Device# show vlan brief`	VLANが削除されたことを確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN へのスタティック アクセス ポートの割り当て

VTP をディセーブルにすることによって（VTP トランスペアレント モード）、VTP に VLAN 設定情報をグローバルに伝播させずに、スタティック アクセス ポートを VLAN に割り当てることができます。

存在しない VLAN にインターフェイスを割り当てると、新しい VLAN が作成されます

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	VLANに追加するインターフェイスを入力します。
ステップ 4	**switchport mode access** 例： `Device(config-if)# switchport mode access`	ポート（レイヤ 2 アクセス ポート）の VLAN メンバーシップ モードを定義します。
ステップ 5	**switchport access vlan** *vlan-id* 例： `Device(config-if)# switchport access vlan 2`	VLANにポートを割り当てます。指定できる VLAN ID の範囲は 1 ～ 4094 です。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config interface** *interface-id* 例： `Device# show running-config interface gigabitethernet2/0/1`	インターフェイスのVLANメンバーシップ モードを確認します。
ステップ 8	**show interfaces** *interface-id* **switchport** 例： `Device# show interfaces gigabitethernet2/0/1 switchport`	表示された [Administrative Mode] フィールドおよび [Access Mode VLAN] フィールドの設定を確認します。

	コマンドまたはアクション	目的
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

拡張範囲 VLAN の設定方法

サービス プロバイダーは拡張範囲 VLAN を使用することにより、インフラストラクチャを拡張して、多数の顧客に対応できます。拡張範囲 VLAN ID は、VLAN ID が許可されている **switchport** コマンドで使用できます。

VTP バージョン 1 または 2 での拡張範囲 VLAN の設定は VLAN データベースに格納されません。ただし、VTP モードがトランスペアレントであるため、デバイスの実行コンフィギュレーション ファイルに格納されます。また、設定をスタートアップ コンフィギュレーション ファイルに保存できます。VTP バージョン 3 で作成された拡張範囲 VLAN は、VLAN データベースに保存されます。

拡張範囲 VLAN については MTU サイズ、プライベート VLAN、およびリモート SPAN 設定ステートしか変更できません。残りのすべての特性はデフォルト状態のままでなければなりません。

拡張範囲 VLAN の作成

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan** *vlan-id* 例： `Device(config)# vlan 2000`	拡張範囲 VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 1006 ～ 4094 です。

	コマンドまたはアクション	目的
	`Device(config-vlan)#`	
ステップ 4	**remote-span** 例： `Device(config-vlan)# remote-span`	（任意）RSPAN VLAN として VLAN を設定します。

ステップ 5	**exit**
	例：
	`Device(config-vlan)# exit`
	`Device(config)#`
		コンフィギュレーション モードに戻ります。

ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show vlan id** *vlan-id* 例： `Device# show vlan id 2000`	VLANが作成されたことを確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN のモニタリング

表 *4 :* 特権 *EXEC* 表示コマンド

コマンド	目的
show interfaces [**vlan** *vlan-id*]	デバイス上に設定されたすべてのインターフェイスまたは特定の VLAN の特性を表示します。

コマンド	目的
show vlan [**access-map** *name* | **brief** | **dot1q** { **tag native** } | **filter** [**access-map** | **vlan**] | **group** [**group-name** *name*] | **id** *vlan-id* | **ifindex** | **mtu** | **name** *name* | **private-vlan** **remote-span** | **summary**]	デバイス上のすべての VLAN または特定の VLAN のパラメータを表示します。次のコマンド オプションが使用可能です。 • **access-map**：VLAN アクセスマップを表示します。 • **brief**：VTP VLAN のステータス概要を表示します。 • **dot1q**：dot1q パラメータを表示します。 • **filter**：VLAN フィルタ情報を表示します。 • **group**：VLAN グループをグループ名と使用可能な接続済みの VLAN と一緒に表示します。 • **id**：識別番号別に VTP VLAN ステータスを表示します。 • **ifindex**：SNMP ifIndex を表示します。 • **mtu**：VLAN MTU 情報を表示します。 • **name**：指定された名前の VTP VLAN 情報を表示します。 • **private-vlan**：プライベート VLAN 情報を表示します。 • **remote-span**：リモート SPAN VLAN を表示します。 • **summary**：VLAN 情報の要約を表示します。 （注） デバイスの CLI に表示される **private-vlan** コマンド オプションはサポートされません。

次の作業

VLAN を設定したら、次の項目を設定できます。

- VLAN トランキング プロトコル（VTP）
- VLAN トランク
- プライベート VLAN
- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9300 Series Switches)*

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

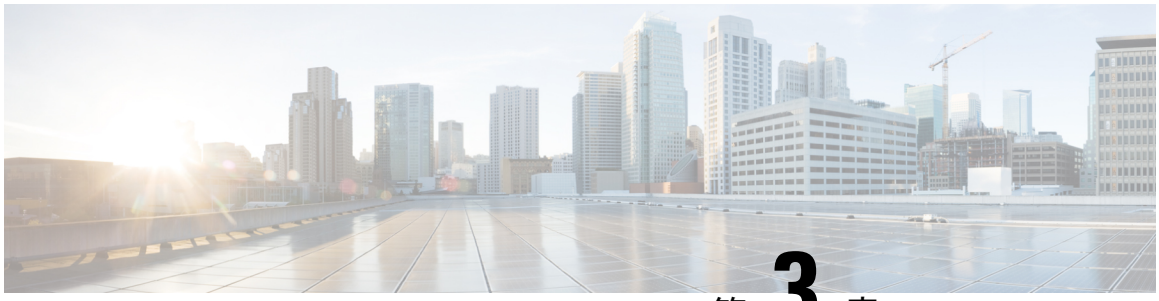
VLAN の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	VLAN	VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。VLAN は、物理LAN と同じ属性をすべて備えていますが、同じLANセグメントに物理的に配置されていないエンド ステーションもグループ化できます。
Cisco IOS XE Gibraltar 16.11.1	スパニング ツリー インスタンスの数の増加のサポート。	このリリース以降、PVST+ または Rapid PVST+ モードでは、デバイスまたはデバイススタックは最大 256 のスパニングツリーインスタンスをサポートします。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/ に進みます。



第 3 章

VLAN トランクの設定

VLAN トランクについて

ここでは、VLAN トランクについて説明します。

トランキングの概要

トランクとは、1つまたは複数のイーサネットインターフェイスと他のネットワーキングデバイス（ルータ、コントローラなど）の間のポイントツーポイントリンクです。イーサネットトランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張できます。

IEEE 802.1Q（業界標準のトランキングカプセル化方式）が、すべてのイーサネットポートで使用できます。

トランキング モード

イーサネット トランク インターフェイスは、さまざまなトランキング モードをサポートします。インターフェイスをトランキングまたは非トランキングとして設定したり、ネイバーインターフェイスとトランキングのネゴシエーションを行ったりするように設定できます。トランキングを自動ネゴシエーションするには、インターフェイスが同じ VTP ドメインに存在する必要があります。

トランク ネゴシエーションは、ポイントツーポイント プロトコル（PPP）であるダイナミック トランキング プロトコル（DTP）によって管理されます。ただし、一部のインターネットワーキング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。

レイヤ 2 インターフェイス モード

表 *5:* レイヤ *2* インターフェイス モード

モード	機能
switchport mode access	インターフェイス（アクセス ポート）を永続的な非トランキング モードにして、リンクの非トランク リンクへの変換をネゴシエートします。インターフェイスは、ネイバー インターフェイスがトランク インターフェイスかどうかに関係なく、非トランク インターフェイスになります。
switchport mode dynamic auto	インターフェイスがリンクをトランク リンクに変換できるようにします。インターフェイスは、ネイバーインターフェイスが **trunk**または **desirable** モードに設定されている場合、トランクインターフェイスになります。すべてのイーサネットインターフェイスのデフォルトのスイッチポート モードは **dynamic auto**です。
switchport mode dynamic desirable	インターフェイスがリンクのトランク リンクへの変換をアクティブに実行するようにします。インターフェイスは、ネイバーインターフェイスが **trunk**、 **desirable** または **auto** モードに設定されている場合、トランクインターフェイスになります。
switchport mode trunk	インターフェイスを永続的なトランキング モードにして、ネイバー リンクのトランク リンクへの変換をネゴシエートします。インターフェイスは、ネイバー インターフェイスがトランク インターフェイスでない場合でも、トランク インターフェイスになります。
switchport nonegotiate	インターフェイスが DTP フレームを生成しないようにします。このコマンドは、インターフェイス スイッチポート モードが **access** または **trunk** の場合だけ使用できます。トランク リンクを確立するには、手動でネイバー インターフェイスをトランク インターフェイスとして設定する必要があります。
switchport mode private-vlan	プライベート VLAN モードを設定します。

トランクでの許可 VLAN

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランクですべての VLAN ID（1～4094）が許可されます。ただし、許可リストから VLAN

を削除することにより、それらの VLAN からのトラフィックがトランク上を流れないようにすることができます。

スパニングツリー ループまたはストームのリスクを減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにできます。トランク ポートから VLAN 1 を削除した場合、インターフェイスは引き続き VLAN 1 内で Cisco Discovery Protocol（CDP）、ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、DTP、および VTP などの管理トラフィックを送受信します。

VLAN 1 をディセーブルにしたトランク ポートが非トランク ポートになると、そのポートはアクセス VLAN に追加されます。アクセス VLAN が 1 に設定されると、**switchport trunk allowed** の設定には関係なく、ポートは VLAN 1 に追加されます。ポート上でディセーブルになっている任意の VLAN について同様のことが当てはまります。

トランク ポートは、VLAN がイネーブルになっており、VTP が VLAN を認識し、なおかつポートの許可リストにその VLAN が登録されている場合に、VLAN のメンバになることができます。VTP が新しくイネーブルにされた VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されている場合、トランク ポートは自動的にその VLAN のメンバになります。VTP が新しい VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されていない場合には、トランク ポートはその VLAN のメンバにはなりません。

トランク ポートでの負荷分散

負荷分散により、デバイスに接続しているパラレルトランクの提供する帯域幅が分割されます。STP は通常、ループを防止するために、デバイス間で 1 つのパラレルリンク以外のすべてのリンクをブロックします。負荷分散を行うと、トラフィックの所属する VLAN に基づいて、リンク間でトラフィックが分散されます。

トランク ポートで負荷分散を設定するには、STP ポート プライオリティまたは STP パス コストを使用します。STP ポートプライオリティを使用して負荷分散を設定する場合には、両方の負荷分散リンクを同じデバイスに接続する必要があります。STP パスコストを使用して負荷分散を設定する場合には、それぞれの負荷分散リンクを同一のデバイスに接続することも、2 台の異なるデバイスに接続することもできます。

STP プライオリティによるネットワーク負荷分散

同一のデバイス上の 2 つのポートがループを形成すると、デバイスは STP ポートプライオリティを使用して、どのポートをイネーブルとし、どのポートをブロッキングステートとするかを判断します。パラレル トランク ポートにプライオリティを設定することにより、そのポートに、特定の VLAN のすべてのトラフィックを伝送させることができます。VLAN に対するプライオリティの高い（値の小さい）トランク ポートがその VLAN のトラフィックを転送します。同じ VLAN に対してプライオリティの低い（値の大きい）トランク ポートは、その VLAN に対してブロッキング ステートのままです。1 つのトランク ポートが特定の VLAN に関するすべてのトラフィックを送受信することになります。

STP パス コストによるネットワーク負荷分散

トランクにそれぞれ異なるパス コストを設定し、各パス コストをそれぞれ異なる VLAN 群に対応付け、各 VLAN でポートをブロックすることによって、VLAN トラフィックを分散するパラレル トランクを設定できます。VLAN はトラフィックを分離し、リンクが失われた場合に備えて冗長性を維持します。

機能の相互作用

トランキングは他の機能と次のように相互作用します。

- トランク ポートをセキュア ポートにすることはできません。
- トランク ポートをまとめて EtherChannel ポート グループにすることはできますが、グループ内のすべてのトランクに同じ設定をする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次に示すパラメータのいずれかの設定を変更すると、デバイスは、入力された設定をグループ内のすべてのポートに伝播します。
  - 許可 VLAN リスト。
  - 各 VLAN の STP ポート プライオリティ。
  - STP PortFast の設定値。
  - トランク ステータス：

    ポート グループ内の 1 つのポートがトランクでなくなると、すべてのポートがトランクでなくなります。
- トランク ポートで IEEE 802.1X をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミックに変更しようとしても、ポート モードは変更されません。

VLAN トランクの前提条件

IEEE 802.1Q トランクは、ネットワークのトランキング方式について次の制約があります。

- IEEE 802.1Q トランクを使用して接続している Cisco デバイスのネットワークでは、デバイスはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持します。他社製のデバイスは、すべての VLAN でスパニングツリー インスタンスを 1 つサポートする場合があります。

IEEE 802.1Q トランクを使用して Cisco デバイスを他社製のデバイスに接続する場合、Cisco デバイスは、トランクの VLAN のスパニングツリーインスタンスを、他社製の IEEE 802.1Q デバイスのスパニングツリー インスタンスと結合します。ただし、各 VLAN のスパニングツリー情報は、他社製の IEEE 802.1Q デバイスからなるクラウドにより分離された Cisco デバイスによって維持されます。Cisco デバイスを分離する他社製の IEEE 802.1Q クラウドは、デバイス間の単一トランクリンクとして扱われます。

- IEEE 802.1Q トランクに対応するネイティブVLANが、トランク リンクの両側で一致していなければなりません。トランクの片側のネイティブ VLAN と反対側のネイティブ VLAN が異なっていると、スパニングツリー ループが発生する可能性があります。
- ネットワーク上のすべてのネイティブ VLAN についてスパニングツリーをディセーブルにせずに、IEEE 802.1Q トランクのネイティブ VLAN 上のスパニングツリーをディセーブルにすると、スパニングツリー ループが発生することがあります。IEEE 802.1Q トランクのネイティブ VLAN 上でスパニングツリーをイネーブルのままにしておくか、またはネットワーク上のすべての VLAN でスパニングツリーをディセーブルにすることを推奨します。また、ネットワークにループがないことを確認してから、スパニングツリーをディセーブルにしてください。

VLAN トランクの制約事項

次に、VLAN トランクに関する制約事項を示します。

- トランク ポートをセキュア ポートにすることはできません。
- トランク ポートをまとめて EtherChannel ポート グループにすることはできますが、グループ内のすべてのトランクに同じ設定をする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次に示すパラメータのいずれかの設定を変更すると、デバイスは、入力された設定をグループ内のすべてのポートに伝播します。
  - 許可 VLAN リスト。
  - 各 VLAN の STP ポート プライオリティ。
  - STP PortFast の設定値。
  - トランク ステータス：

    ポート グループ内の 1 つのポートがトランクでなくなると、すべてのポートがトランクでなくなります。

- トランク ポートで IEEE 802.1X をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x をイネーブルにしようとすると、

エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミックに変更しようとしても、ポート モードは変更されません。

- ダイナミック トランキング プロトコル（DTP）はトンネルポートではサポートされていません。
- デバイスはレイヤ3トランクをサポートしません。したがって、サブインターフェイスを設定したり、レイヤ 3 インターフェイスで **encapsulation** キーワードを使用したりすることはできません。ただし、デバイスは、同等の機能を備えたレイヤ2トランクおよびレイヤ 3 VLAN インターフェイスをサポートします。

VLAN トランクの設定方法

トランクの誤設定を避けるために、DTPをサポートしないデバイスに接続されたインターフェイスが DTP フレームを転送しないように（つまり DTP をオフにするように）設定してください。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTPをサポートしていないデバイスへのトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

トランク ポートとしてのイーサネット インターフェイスの設定

ここでは、イーサネットインターフェイスをトランクポートとして設定する方法について説明します。

トランク ポートの設定

トランクポートは VTP アドバタイズを送受信するので、VTP を使用する場合は、デバイス上で少なくとも1つのトランクポートが設定されており、そのトランクでポートが別のデバイスのトランクポートに接続されていることを確認する必要があります。そうでない場合、デバイスは VTP アドバタイズを受信できません。

始める前に

デフォルトでは、インターフェイスはレイヤ 2 モードです。レイヤ 2 インターフェイスのデフォルトモードは、**switchport mode dynamic auto** です。隣接インターフェイスがトランキングをサポートし、トランキングを許可するように設定されている場合、リンクはレイヤ2トランクです。また、インターフェイスがレイヤ 3 モードの場合は、**switchport** インターフェイス コンフィギュレーション コマンドを入力するとレイヤ 2 トランクになります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	トランクに設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**} 例： `Device(config-if)# switchport mode dynamic desirable`	インターフェイスをレイヤ 2 トランクとして設定します（インターフェイスがレイヤ 2 アクセス ポートまたはトンネル ポートであり、トランキング モードを設定する場合に限り必要となります）。 • **dynamic auto**：ネイバー インターフェイスが trunk または desirable モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。これはデフォルトです。 • **dynamic desirable**：ネイバー インターフェイスが trunk、desirable、または auto モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。 • **trunk**：ネイバー インターフェイスがトランク インターフェイスでない場合でも、インターフェイスを永続的なトランキング モードに設定して、リンクをトランク リン

	コマンドまたはアクション	目的
		クに変換するようにネゴシエートします。
ステップ 5	**switchport access vlan** *vlan-id* 例： `Device(config-if)# switchport access vlan 200`	（任意）インターフェイスがトランキングを停止した場合に使用するデフォルト VLAN を指定します。
ステップ 6	**switchport trunk native vlan** *vlan-id* 例： `Device(config-if)# switchport trunk native vlan 200`	IEEE 802.1Q トランク用のネイティブ VLAN を指定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** *interface-id* **switchport** 例： `Device# show interfaces gigabitethernet 1/0/2 switchport`	インターフェイスのスイッチポート設定を表示します。[Administrative Mode] および [Administrative Trunking Encapsulation] フィールドに表示されます。
ステップ 9	**show interfaces** *interface-id* **trunk** 例： `Device# show interfaces gigabitethernet 1/0/2 trunk`	インターフェイスのトランクの設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

トランクでの許可 VLAN の定義

VLAN 1 は、すべての Cisco デバイスのすべてのトランクポートのデフォルト VLAN です。以前は、すべてのトランクリンクで VLAN 1 を必ずイネーブルにする必要がありました。VLAN

1 の最小化機能を使用して、個々の VLAN トランク リンクで VLAN 1 をディセーブルに設定できます。これにより、ユーザ トラフィック（スパニングツリーアドバタイズなど）はVLAN 1 で送受信されなくなります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 5	**switchport trunk allowed vlan** { *word* | **add** | **all** | **except** | **none** | **remove**} *vlan-list* 例： `Device(config-if)# switchport trunk allowed vlan remove 2`	（任意）トランク上で許容される VLAN のリストを設定します。 *vlan-list* パラメータは、1 ～ 4094 の単一の VLAN 番号、または 2 つの VLAN 番号（小さい方が先、ハイフンで区切る）で指定された VLAN 範囲です。カンマで区切った VLAN パラメータの間、またはハイフンで指定した範囲の間には、スペースを入れないでください。 デフォルトでは、すべての VLAN が許可されます。
ステップ 6	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 7	**show interfaces** *interface-id* **switchport** 例： `Device# show interfaces gigabitethernet 1/0/1 switchport`	表示された [Trunking VLANs Enabled] フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

プルーニング適格リストの変更

プルーニング適格リストは、トランク ポートだけに適用されます。トランク ポートごとに独自の適格リストがあります。この手順を有効にするには、VTPプルーニングがイネーブルに設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet0/1`	VLANプルーニングを適用するトランク ポートを選択し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan* [,*vlan* [,,,]]	トランクからのプルーニングを許可する VLAN のリストを設定します。 **add**、**except**、**none** および **remove** キーワードの使用方法については、このリリースに対応するコマンドリファレンスを参照してください。 連続していない VLAN ID は、カンマ（スペースなし）で区切ります。ID の範囲はハイフンで指定します。有効な ID 範囲は 2 ～ 1001 です。拡張範囲 VLAN（VLAN ID 1006 ～ 4094）はプルーニングできません。 プルーニング不適格の VLAN は、フラッディング トラフィックを受信します。 デフォルトでは、プルーニングが許可される VLAN のリストには、VLAN 2 ～ 1001 が含まれます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id* **switchport** 例： `Device# show interfaces gigabitethernet 1/0/1 switchport`	表示された [Pruning VLANs Enabled] フィールドの設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

タグなしトラフィック用ネイティブ VLAN の設定

IEEE 802.1Q タギングが設定されたトランク ポートは、タグ付きトラフィックおよびタグなしトラフィックの両方を受信できます。デフォルトでは、デバイスはタグなしトラフィックを、ポートに設定されたネイティブ VLAN に転送します。ネイティブ VLAN は、デフォルトでは VLAN 1 です。

ネイティブ VLAN には任意の VLAN ID を割り当てることができます。

パケットの VLAN ID が出力ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、デバイスはそのパケットをタグ付きで送信します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	IEEE 802.1Q トランクとして設定するインターフェイスを定義して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport trunk native vlan** *vlan-id* 例： `Device(config-if)# switchport trunk native vlan 12`	トランク ポート上でタグなしトラフィックを送受信する VLAN を設定します。 *vlan-id* に指定できる範囲は 1 ～ 4094 です。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id* **switchport** 例： `Device# show interfaces gigabitethernet 1/0/2 switchport`	[Trunking Native Mode VLAN] フィールドの設定を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

トランク ポートの負荷分散の設定

ここでは、負荷分散用のトランクポートの設定について説明します。

STP ポート プライオリティによる負荷分散の設定

スイッチがスイッチスタックのメンバーである場合、**spanning-tree** [**vlan** *vlan-id*] **cost** *priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree** [**vlan** *vlan-id*] **port-priority** *cost* インターフェイス コンフィギュレーション コマンドを使用して、フォワーディングステートにするインターフェイスを選択する必要があります。最初に選択させるインターフェイスには、低いコスト値を割り当て、最後に選択させるインターフェイスには高いコスト値を割り当てます。

次の手順では、STP ポート プライオリティを使用した負荷分散を指定してネットワークを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	デバイス A でグローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp domain** *domain-name* 例： `Device(config)# vtp domain workdomain`	VTP 管理ドメインを設定します。 1 ～ 32 文字のドメイン名を使用できます。

	コマンドまたはアクション	目的
ステップ 4	**vtp mode server** 例： `Device(config)# vtp mode server`	デバイス A を VTP サーバーとして設定します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show vtp status** 例： `Device# show vtp status`	デバイス A とデバイス B の両方で VTP 設定を確認します。 表示された *VTP Operating Mode* および *VTP Domain Name* フィールドをチェックします。
ステップ 7	**show vlan** 例： `Device# show vlan`	デバイス A のデータベースに VLAN が存在していることを確認します。
ステップ 8	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 9	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	トランクとして設定するインターフェイスを定義し、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 10	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	ポートをトランク ポートとして設定します。
ステップ 11	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-if)# end`	
ステップ 12	**show interfaces** *interface-id* **switchport** 例： `Device# show interfaces gigabitethernet 1/0/1 switchport`	VLAN の設定を確認します。
ステップ 13	デバイスの 2 番目のポートに対して、デバイス A で上記の手順を繰り返します。	
ステップ 14	デバイス B で前述の手順を繰り返し、デバイス A で設定したトランクポートに接続するトランクポートを設定します。	
ステップ 15	**show vlan** 例： `Device# show vlan`	トランクリンクがアクティブになると、VTP がデバイス B に VTP および VLAN 情報を渡します。このコマンドは、デバイス B が VLAN 設定を学習したことを確認します。
ステップ 16	**configure terminal** 例： `Device# configure terminal`	デバイス A でグローバル コンフィギュレーション モードを開始します。
ステップ 17	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	STP のポート プライオリティを設定するインターフェイスを定義し、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 18	**spanning-tree vlan** *vlan-range* **port-priority** *priority-value* 例： `Device(config-if)# spanning-tree vlan 8-10 port-priority 16`	指定された VLAN 範囲にポート プライオリティを割り当てます。0 ～ 240 のポート プライオリティ値を入力します。ポート プライオリティ値は 16 ずつ増分します。
ステップ 19	**exit** 例：	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-if)# exit`	
ステップ 20	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	STP のポート プライオリティを設定するインターフェイスを定義し、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 21	**spanning-tree vlan** *vlan-range* **port-priority** *priority-value* 例： `Device(config-if)# spanning-tree vlan 3-6 port-priority 16`	指定された VLAN 範囲にポート プライオリティを割り当てます。0 ～ 240 のポート プライオリティ値を入力します。ポート プライオリティ値は 16 ずつ増分します。
ステップ 22	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 23	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 24	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

STP パス コストによる負荷分散の設定

次の手順では、STP パス コストを使用した負荷分散を指定してネットワークを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	`Device> enable`	パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	デバイス A でグローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	ポートをトランク ポートとして設定します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	デバイス A またはデバイス A スタック内の別のインターフェイスでステップ 2 ～ 4 を繰り返します。	
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。画面で、インターフェイスがトランク ポートとして設定されていることを確認してください。
ステップ 9	**show vlan** 例：	トランクリンクがアクティブになると、デバイス A がもう一方のデバイスから VTP 情報を受信します。このコマ

	コマンドまたはアクション	目的
	`Device# show vlan`	ンドは、デバイス A が VLAN コンフィギュレーションを学習したことを確認します。
ステップ 10	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 11	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	STP コストを設定するインターフェイスを定義し、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 12	**spanning-tree vlan** *vlan-range* **cost** *cost-value* 例： `Device(config-if)# spanning-tree vlan 2-4 cost 30`	VLAN 2 ～ 4 のスパニングツリー パスコストを 30 に設定します。
ステップ 13	**end** 例： `Device(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	デバイス A に設定したもう一方のトランクインターフェイスでステップ 9 ～ 13 を繰り返し、VLAN 8、9、および 10 のスパニングツリーパスコストを 30 に設定します。	
ステップ 15	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 16	**show running-config** 例： `Device# show running-config`	入力を確認します。両方のトランクインターフェイスに対してパスコストが正しく設定されていることを表示で確認します。

	コマンドまたはアクション	目的
ステップ 17	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

VLAN トランクを設定したら、次の項目を設定できます。

- VLAN
- 音声 VLAN
- プライベート VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9300 Series Switches)*

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

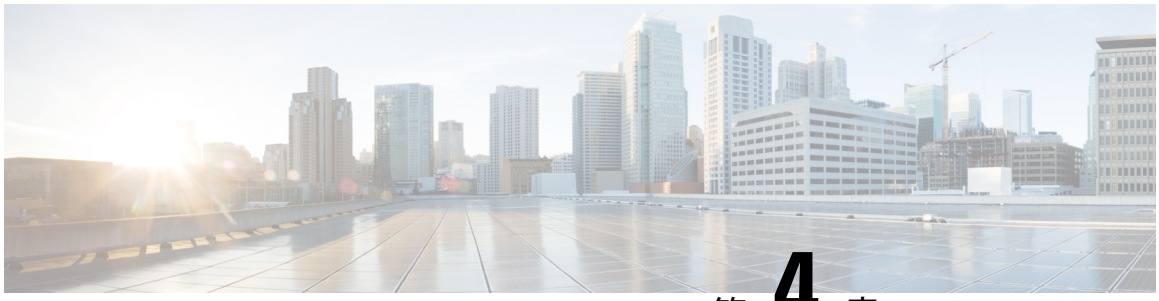
VLAN トランクの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	VLAN トランク	この機能が導入されました。 トランクとは、1つまたは複数のイーサネット インターフェイスと他のネットワーキング デバイス（ルータ、コントローラなど）の間のポイントツーポイントリンクです。イーサネット トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/ に進みます。



第 4 章

音声 VLAN の設定

音声 VLAN の前提条件

音声 VLAN の前提条件は、次のとおりです。

- 音声 VLAN 設定はデバイスのアクセスポートだけでサポートされており、トランクポートではサポートされていません。

（注） トランク ポートは、標準 VLAN と同様に、任意の数の音声 VLAN を伝送できます。トランク ポートでは、音声 VLAN の設定がサポートされません。

- 音声 VLAN を有効にする前に、 **trust device cisco-phone** インターフェイス コンフィギュレーション コマンドを入力し、デバイス上の QoS を有効にします。Auto QoS 機能を使用すると、これらは自動的に設定されます。
- Cisco IP Phone にコンフィギュレーションを送信するために、Cisco IP Phone に接続するデバイスポート上で CDP をイネーブルにする必要があります。（デフォルト設定では、CDP がすべてのデバイスインターフェイスでグローバルにイネーブルです。）

音声 VLAN の制約事項

音声 VLAN には、スタティック セキュア MAC アドレスを設定できません。

音声 VLAN に関する情報

ここでは、音声 VLAN について説明します。

音声 VLAN

音声 VLAN 機能を使用すると、アクセス ポートで IP Phone からの IP 音声トラフィックを伝送できます。デバイスを Cisco 7960 IP Phone に接続すると、IP Phone はレイヤ 3 IP 値およびレイヤ 2 サービスクラス（CoS）値を使用して、音声トラフィックを送信します。どちらの値もデフォルトでは 5 に設定されます。データ送信が均質性に欠ける場合、IP Phone の音質が低下することがあります。そのため、このデバイスは IEEE 802.1p CoS に基づく Quality of Service（QoS）をサポートしています。QoS は、分類およびスケジューリングを使用して、デバイスからのネットワークトラフィックを予測可能な方法で送信します。

Cisco 7960 IP Phone は設定可能なデバイスであり、IEEE 802.1p の優先度に基づいてトラフィックを転送するように設定できます。Cisco IP Phone によって割り当てられたトラフィックの優先度を信頼したり、オーバーライドしたりするようにデバイスを設定できます。

Cisco IP Phone の音声トラフィック

Cisco IP Phone と接続するアクセス ポートを、1 つの VLAN は音声トラフィック用に、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータ トラフィック用に使用するように設定できます。Cisco Discovery Protocol（CDP）パケットを送信するよう、デバイス上のアクセスポートを設定できます。CDP パケットは、接続する IP Phone に対して、次のいずれかの方法で音声トラフィックをデバイスに送信するよう指示します。

- レイヤ 2 CoS プライオリティ値のタグ付き音声 VLAN による送信
- レイヤ 2 CoS プライオリティ値のタグ付きアクセス VLAN による送信
- タグなし（レイヤ 2 CoS プライオリティ値なし）のアクセス VLAN による送信

（注） いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（音声トラフィックはデフォルトで 5、音声制御トラフィックは 3）を伝送します。

Cisco IP Phone のデータ トラフィック

デバイスは、Cisco IP Phone のアクセスポートに接続されたデバイスから送られる、タグ付きデータトラフィック（IEEE 802.1Q または IEEE 802.1p フレームタイプのトラフィック）を処理することもできます。CDP パケットを送信するよう、デバイス上のレイヤ 2 アクセスポートを設定できます。CDP パケットは、接続する IP Phone に対して、次のいずれかのモードで IP Phone アクセスポートを設定するよう指示します。

- trusted（信頼性がある）モードでは、Cisco IP Phone のアクセス ポート経由で受信したすべてのトラフィックがそのまま IP Phone を通過します。
- untrusted（信頼性がない）モードでは、Cisco IP Phone のアクセス ポート経由で受信した IEEE 802.1Q および IEEE 802.1p フレームのすべてのトラフィックに、設定されたレイヤ 2 CoS 値を与えます。デフォルトのレイヤ 2 CoS 値は 0 です。信頼できないモードがデフォルト設定です。

（注） Cisco IP Phone に接続されたデバイスからのタグなしトラフィックは、IP Phone のアクセス ポートの信頼状態に関係なく、そのまま IP Phone を通過します。

音声 VLAN 設定時の注意事項

- Cisco 7960 IP Phone は、PC やその他のデバイスとの接続もサポートしているので、デバイスを Cisco IP Phone に接続するポートは、さまざまな種類のトラフィックを伝送できます。ポートを設定することによって、Cisco IP Phone による音声トラフィックおよびデータ トラフィックの伝送方法を決定できます。
- IP Phone で音声 VLAN 通信が適切に行われるには、デバイス上に音声 VLAN が存在し、アクティブになっている必要があります。VLAN が存在しているかどうかを確認するには、**show vlan** 特権 EXEC コマンドを使用します（リストで表示されます）。VLAN がリストされていない場合は、音声 VLAN を作成します。
- Power Over Ethernet（PoE）デバイスは、シスコ先行標準の受電デバイスまたは IEEE 802.3af 準拠の受電デバイスが AC 電源から電力を供給されていない場合に、それらの受電デバイスに自動的に電力を供給できます。
- 音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。
- Cisco IP Phone とその IP Phone に接続されたデバイスが同じ VLAN 上にある場合、両方とも同じ IP サブネットに属していなければなりません。次の条件が満たされている場合は、同じ VLAN 上にあります。
  - 両方とも IEEE 802.1p またはタグなしフレームを使用する。
  - Cisco IP Phone が IEEE 802.1p フレームを使用し、デバイスがタグなしフレームを使用する。

- Cisco IP Phone がタグなしフレームを使用し、デバイスが IEEE 802.1p フレームを使用する。
- Cisco IP Phone が IEEE 802.1Q フレームを使用し、音声 VLAN がアクセス VLAN と同じである。

- Cisco IP Phone と IP Phone に接続されたデバイスは、同一 VLAN、同一サブネット上にあっても、使用するフレーム タイプが異なる場合は通信できません。トラフィックは同一サブネット上でルーティングされないからです（ルーティングによってフレーム タイプの相違が排除されます）。
- 音声 VLAN ポートには次のポート タイプがあります。
  - ダイナミック アクセス ポート。
  - IEEE 802.1x 認証ポート。

（注） 音声 VLAN が設定され Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x を有効にした場合、その IP Phone からデバイスへの接続が最大 30 秒間失われます。

  - 保護ポート。
  - SPAN または RSPAN セッションの送信元ポートまたは宛先ポート。
  - セキュア ポート。

（注） 音声 VLAN も設定しているインターフェイス上でポート セキュリティをイネーブルにする場合、ポートで許容されるセキュア アドレスの最大数を、アクセス VLAN におけるセキュア アドレスの最大数に 2 を足した数に設定する必要があります。ポートを Cisco IP Phone に接続している場合、IP Phone に最大で 2 つの MAC アドレスが必要になります。IP Phone のアドレスは、音声 VLAN で学習され、アクセス VLAN でも学習される場合があります。PC を IP Phone に接続する場合、追加の MAC アドレスが必要になります。

音声 VLAN の設定方法

ここでは、音声 VLAN の設定について説明します。

Cisco IP Phone の音声トラフィックの設定

Cisco IP Phone に CDP パケットを送信して IP Phone による音声トラフィックの送信方法を設定するように、IP Phone に接続するポートを設定できます。IP Phone は指定された音声 VLAN に、レイヤ 2 CoS 値を使用して、IEEE 802.1Q フレームの音声トラフィックを伝送できます。IEEE 802.1p のプライオリティ タグを使用すると、音声トラフィックにさらに高いプライオリティを与え、すべての音声トラフィックをネイティブ（アクセス）VLAN 経由で転送できます。Cisco IP Phone はタグなしの音声トラフィックを送信する、または独自の設定を使用してアクセス VLAN で音声トラフィックを送信することもできます。いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（デフォルトは 5）を伝送します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	IP Phone に接続するインターフェイスを指定し、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 3	**trust device cisco-phone** 例： `Device(config-if)# trust device cisco-phone`	Cisco IP Phone の着信トラフィック パケットを信頼するようにインターフェイスを設定します。
ステップ 4	**switchport voice vlan** {*vlan-id* | **dot1p** | **none** | **untagged**} 例： `Device(config-if)# switchport voice vlan dot1p`	音声 VLAN を設定します。 • *vlan-id*：すべての音声トラフィックが特定の VLAN を経由して転送されるように IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。指定できる VLAN ID の範囲は 1 ～ 4094 です。 • **dot1p**：VLAN ID 0（ネイティブ VLAN）のタグが付けられた音声およびデータ IEEE 802.1p プライオリティフレームを受け入れるよう、デ

	コマンドまたはアクション	目的
		バイスを設定します。デフォルトでは、デバイスはVLAN 0のタグが付いたすべての音声およびデータトラフィックをドロップします。802.1pに対応するよう設定されると、Cisco IP Phone は IEEE 802.1p プライオリティ5を使用してトラフィックを転送します。 • **none**：IP Phoneが独自の設定を使用してタグなしの音声トラフィックを送信するようにします。 • **untagged**：タグなしの音声トラフィックを送信するように電話を設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

ステップ 6	次のいずれかを使用します。
	• **show interfaces** *interface-id* **switchport**
	• **show running-config interface** *interface-id*
	例：
	`Device# show interfaces gigabitethernet1/0/1 switchport`
	または
	`Device# show running-config interface gigabitethernet1/0/1`
		音声 VLAN の設定、または QoS および音声 VLAN の設定を確認します。

ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

着信データ フレームのプライオリティ設定

PC またはその他のデータ デバイスを Cisco IP Phone ポートに接続できます。タグ付きデータ トラフィック（IEEE 802.1Q または IEEE 802.1p フレーム）を処理するために、CDP パケットを送信するようデバイスを設定できます。CDP パケットは Cisco IP Phone に対して、IP Phone 上のアクセスポートに接続されたデバイスからのデータパケット送信方法を指示します。PC は、CoS 値が割り当てられたパケットを生成できます。接続デバイスから IP Phone のポートに届いたフレームのプライオリティを変更しない（信頼する）または変更する（信頼しない）ように、IP Phone を設定できます。

Cisco IP Phone で非音声ポートから受信するデータ トラフィックのプライオリティを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	Cisco IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport priority extend** { **cos** *value* | **trust**} 例： `Device(config-if)# switchport priority extend trust`	Cisco IP Phone のアクセス ポートから受信したデータ トラフィックのプライオリティを次のように設定します。 • **cos** *value*：PC または接続しているデバイスから受信したプライオリティを、指定の CoS 値にオーバーライドするよう、IP Phone を設定します。値は 0 ～ 7 です。7 が最高のプライオリティです。デフォルトのプライオリティは、**cos** 0 です。

	コマンドまたはアクション	目的
		• **trust**：PC または接続しているデバイスから受信したプライオリティを信頼するよう IP Phone アクセスポートを設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id* **switchport** 例： `Device# show interfaces gigabitethernet1/0/1 switchport`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

音声 VLAN のモニタリング

インターフェイスの音声 VLAN 設定を表示するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを使用します。

次の作業

音声 VLAN を設定した後は、次の設定を行うことができます。

- VLAN
- VLAN トランキング
- VTP

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9300 Series Switches)*

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

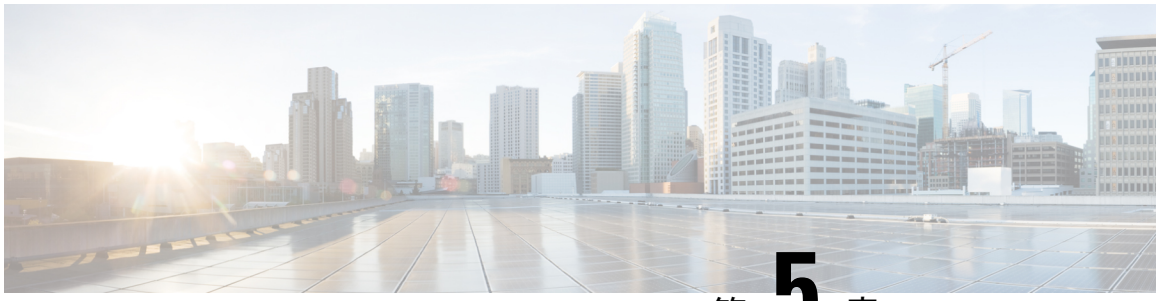
音声 VLAN の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	Voice VLAN	この機能が導入されました。 音声 VLAN 機能を使用すると、アクセスポートで IP Phone からの IP 音声トラフィックを伝送できます。Cisco IP Phone に CDP パケットを送信して IP Phone による音声トラフィックの送信方法を設定するように、IP Phone に接続するポートを設定できます。IP Phone は指定された音声 VLAN に、レイヤ 2 CoS 値を使用して、IEEE 802.1Q フレームの音声トラフィックを伝送できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/ に進みます。



第 5 章

プライベート VLAN の設定

プライベート VLAN の前提条件

プライベート VLAN をデバイスに設定するときに、ユニキャストルートとレイヤ 2 エントリとの間のシステムリソースのバランスを取るために、常にデフォルトの Switch Database Management（SDM）テンプレートを使用してください。別の SDM テンプレートが設定されている場合は、**sdm prefer default** グローバル コンフィギュレーション コマンドを使用してデフォルトのテンプレートを設定します。

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

プライベート VLAN の制約事項

（注） 一部の状況では、エラー メッセージが表示されずに設定が受け入れられますが、コマンドには効果がありません。

- プライベート VLAN が設定されているデバイスでは、フォールバックブリッジングを設定しないでください。
- リモート SPAN（RSPAN）をプライベート VLAN のプライマリまたはセカンダリ VLAN として設定しないでください。
- 次のようなその他の機能用に設定したインターフェイスでは、プライベート VLAN ポートを設定しないでください。
  - ダイナミック アクセス ポート VLAN メンバーシップ
  - ダイナミック トランキング プロトコル（DTP）
  - IP ソース ガード
  - Cisco IPv6 First Hop Security（FHS）
  - IPv6 Security Group（SG）
  - マルチキャスト VLAN レジストレーション（MVR）
  - 音声 VLAN
  - Web Cache Communication Protocol（WCCP）
- Port Aggregation Protocol（PAgP）および Link Aggregation Control Protocol（LACP）は、プライベート VLAN 無差別トランクポートおよびプライベート VLAN 独立トランクポートでのみサポートされています。
- IEEE 802.1x ポートベース認証をプライベート VLAN ポートに設定できますが、802.1x とポート セキュリティ、音声 VLAN、またはポート単位のユーザー ACL は、プライベート VLAN ポートに設定できません。
- プライベート VLAN ホストまたは無差別ポートは SPAN 宛先ポートにはできません。SPAN 宛先ポートをプライベート VLAN ポートに設定した場合、ポートは非アクティブになります。
- プライマリ VLAN の無差別ポートでスタティック MAC アドレスを設定する場合は、すべての関連セカンダリ VLAN に同じスタティック アドレスを追加する必要はありません。同様に、セカンダリ VLAN のホスト ポートでスタティック MAC アドレスを設定する場合は、関連プライマリ VLAN に同じスタティック MAC アドレスを追加する必要はありません。さらに、スタティック MAC アドレスをプライベート VLAN ポートから削除する際に、設定されている MAC アドレスのすべてのインスタンスをプライベート VLAN から削除する必要はありません。

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

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

プライベート VLAN について

ここでは、プライベート VLAN について説明します。

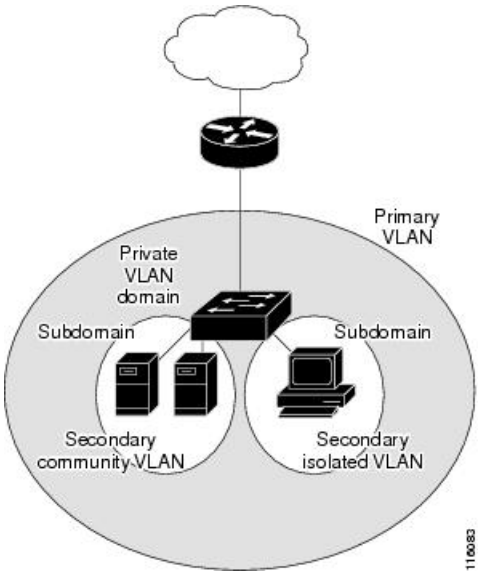
プライベート VLAN ドメイン

PVLAN 機能を使用すると、サービス プロバイダが VLAN を使用したときに直面する 2 つの問題に対処できます。

- Network Essentials または Network Advantage ライセンスを実行している場合、最大で 4094 個のアクティブ VLAN がデバイスでサポートされます。サービス プロバイダーが 1 カスタマーあたり 1 つの VLAN を割り当てる場合、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これに制限されます。
- 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が、これにより、未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が起きます。

図 *4:* プライベート *VLAN* ドメイン

プライベートVLANの使用でスケーラビリティの問題に対処でき、サービスプロバイダにとってはIP アドレス管理上の利得がもたらされ、カスタマーに対してはレイヤ 2 セキュリティを提供できます。プライベート VLAN では、通常の VLAN ドメインをサブドメインに分割します。サブドメインは、プライマリ VLANとセカンダリ VLANのペアで表されます。プライベート VLAN には複数の VLAN ペアを設定可能で、各サブドメインにつき 1 ペアになります。プライベート VLAN 内のすべての VLAN ペアは同じプライマリ VLAN を共有します。セカンダリ VLAN ID は、各サブドメインの区別に使用されます。



セカンダリ VLAN

セカンダリ VLAN には、次の 2 種類があります。

- 独立 VLAN：独立 VLAN 内のポートは、レイヤ 2 レベルでは相互に通信できません。
- コミュニティ VLAN：コミュニティ VLAN 内のポートは互いに通信できますが、レイヤ 2 レベルにある他のコミュニティ内のポートとは通信できません。

プライベート VLAN ポート

プライベート VLAN では、同じプライベート VLAN 内のポート間をレイヤ 2 で分離します。プライベート VLAN ポートは、次のいずれかの種類に属するアクセス ポートです。

- 無差別：無差別ポートは、プライベート VLAN に属し、プライマリ VLAN と関連しているセカンダリ VLAN に属するコミュニティ ポートや独立ホスト ポートなどの、すべてのインターフェイスと通信できます。
- 独立：独立ポートは、独立セカンダリ VLAN に属しているホスト ポートです。これは、無差別ポートを除く、同じプライベート VLAN 内の他のポートからレイヤ 2 で完全に分離されています。プライベート VLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。独立ポートから受信されたトラフィックは、無差別ポートにだけ転送されます。
- コミュニティ：コミュニティ ポートは、1 つのコミュニティ セカンダリ VLAN に属しているホスト ポートです。コミュニティ ポートは、同一コミュニティ VLAN のその他のポート、および無差別ポートと通信します。これらのインターフェイスは、他のコミュニティの他のすべてのインターフェイスおよびプライベート VLAN 内の独立ポートとレイヤ 2 で分離されます。

（注） トランク ポートは、通常の VLAN からのトラフィックを伝送し、またプライマリ、独立、およびコミュニティ VLAN からのトラフィックも伝送します。

プライマリおよびセカンダリ VLAN には次のような特性があります。

- プライマリ VLAN：プライベート VLAN には、プライマリ VLAN を 1 つだけ設定できます。プライベート VLAN 内のすべてのポートは、プライマリ VLAN のメンバーです。プライマリ VLAN は、無差別ポートからの単一方向トラフィックのダウンストリームを、（独立およびコミュニティ）ホスト ポートおよび他の無差別ポートへ伝送します。
- 独立 VLAN：プライベート VLAN の独立 VLAN は 1 つだけです。独立 VLAN はセカンダリ VLAN であり、ホストから無差別ポートおよびゲートウェイに向かう単一方向トラフィック アップストリームを搬送します。
- コミュニティ VLAN：コミュニティ VLAN は、アップストリーム トラフィックをコミュニティ ポートから無差別ポート ゲートウェイおよび同じコミュニティ内の他のホスト ポートに伝送するセカンダリ VLAN です。複数のコミュニティ VLAN を 1 つのプライベート VLAN に設定できます。

無差別ポートは、1 つのプライマリ VLAN、1 つの独立 VLAN、複数のコミュニティ VLAN だけで動作できます。レイヤ 3 ゲートウェイは通常、無差別ポートを介してデバイスに接続されます。無差別ポートでは、広範囲なデバイスをプライベート VLAN のアクセス ポイントとして接続できます。たとえば、すべてのプライベート VLAN サーバ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。

ネットワーク内のプライベート VLAN

スイッチング環境では、個々のエンド ステーションに、または共通グループのエンド ステーションに、個別のプライベート VLAN や、関連する IP サブネットを割り当てることができます。エンド ステーションはデフォルト ゲートウェイとの通信を行うだけで、プライベート VLAN の外部と通信することができます。

プライベート VLAN を使用し、次の方法でエンド ステーションへのアクセスを制御できます。

- エンド ステーションに接続されているインターフェイスを選択して独立ポートとして設定し、レイヤ 2 の通信をしないようにします。たとえば、エンド ステーションがサーバーの場合、この設定によりサーバー間のレイヤ 2 通信ができなくなります。
- デフォルト ゲートウェイおよび選択したエンド ステーション（バックアップ サーバーなど）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。

複数のデバイスにわたるようにプライベート VLAN を拡張するには、プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN を、プライベート VLAN をサポートする他のデバイスにトランキングします。使用するプライベート VLAN 設定のセキュリティを確保して、プライベート VLAN として設定された VLAN が他の目的に使用されないようにするには、プライ

ベート VLAN ポートがないデバイスを含めて、すべての中間デバイスでプライベート VLAN を設定します。

プライベート VLAN での IP アドレッシング方式

各カスタマーに個別の VLAN を割り当てると、次のように IP アドレッシング方式が非効率的になります。

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

この問題は、プライベート VLAN を使用すると軽減します。プライベート VLAN では、プライベート VLAN のすべてのメンバーが、プライマリ VLAN に割り当てられている共通アドレス空間を共有するためです。ホストはセカンダリ VLAN に接続され、プライマリ VLAN に割り当てられているアドレスのブロックから IP アドレスが DHCP サーバー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 サーバー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

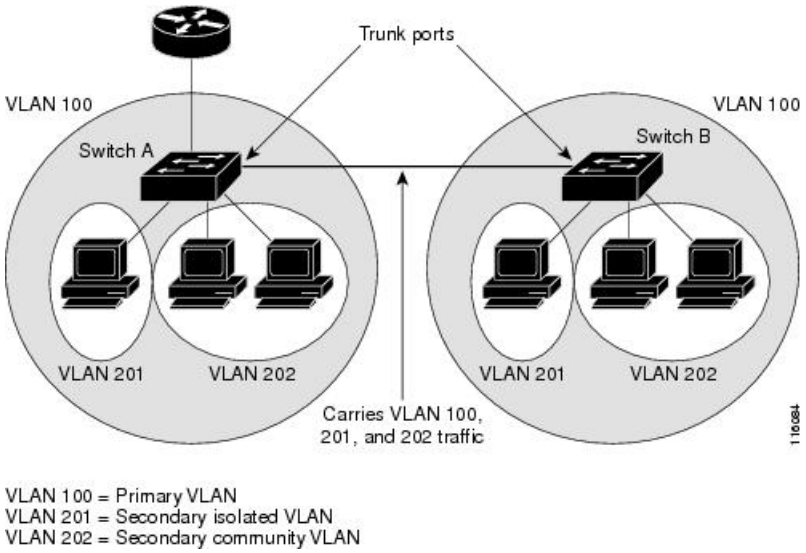
ここでは、次の内容について説明します。

- 標準トランク ポート
- 独立 PVLAN トランク ポート
- 無差別 PVLAN トランク ポート

標準トランク ポート

通常の VLAN と同様に、プライベート VLAN を複数のスイッチにまたがるように設定できます。トランク ポートはプライマリ VLAN およびセカンダリ VLAN を隣接スイッチに伝送します。トランク ポートはプライベート VLAN を他の VLAN として扱います。複数のスイッチにまたがるプライベート VLAN の機能の特徴として、スイッチ A にある独立ポートからのトラフィックはスイッチ B 上の独立ポートに到達しません。

図 *5 :* 複数のスイッチにまたがるプライベート *VLAN*

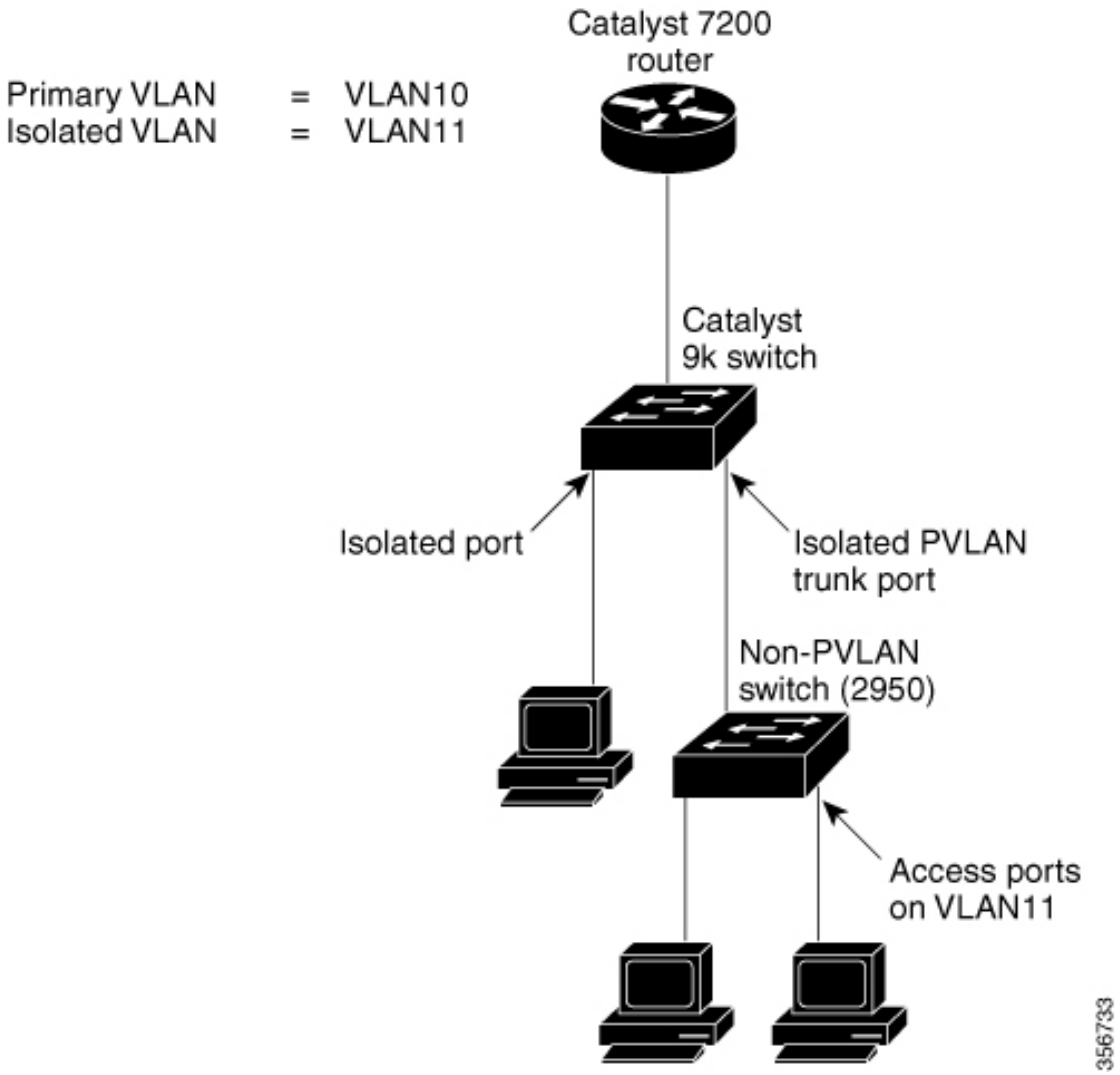


プライベート VLAN は、VTP 1、2、および 3 のトランスペアレント モードでサポートされます。プライベート VLAN は VTP 3 のサーバーモードでもサポートされます。VTP 3 を使用して設定したサーバークライアントがある場合、サーバーに設定されているプライベート VLAN をクライアント上に反映させる必要があります。

独立 PVLAN トランク ポート

PVLAN 独立ホストポートを使用して、通常の VLAN を複数伝送するか、複数の PVLAN ドメインで VLAN を複数伝送する場合、独立 PVLAN トランクポートを使用します。PVLAN をサポートしないダウンストリームスイッチ（Catalyst 2950 など）を接続できます。

図 *6 :* 独立 *PVLAN* トランク ポート



この図では、Catalyst 9k スイッチで、PVLAN をサポートしないダウンストリームスイッチに接続しています。

ルータから host1 へのダウン ストリーム方向に送信されるトラフィックは、

無差別ポートとプライマリ VLAN（VLAN 10）の Catalyst 9k シリーズ スイッチによって受信されます。そして、パケットは独立 PVLAN トランクからスイッチングされますが、プライマリ VLAN（VLAN 10）にタグ付けされずに独立 VLAN（VLAN 11）にタグ付けされて送信されます。パケットが非 PVLAN スイッチに着信すると、宛先ホストのアクセスポートにブリッジングされます。

アップストリーム方向のトラフィックは、host1 から非 PVLAN スイッチへ送信され、VLAN 11 に着信します。そしてパケットは、トランクポート経由でこの VLAN（VLAN 11）のタグにタグ付けされる Catalyst 9k シリーズ スイッチに送信されます。Catalyst 9k シリーズ スイッ

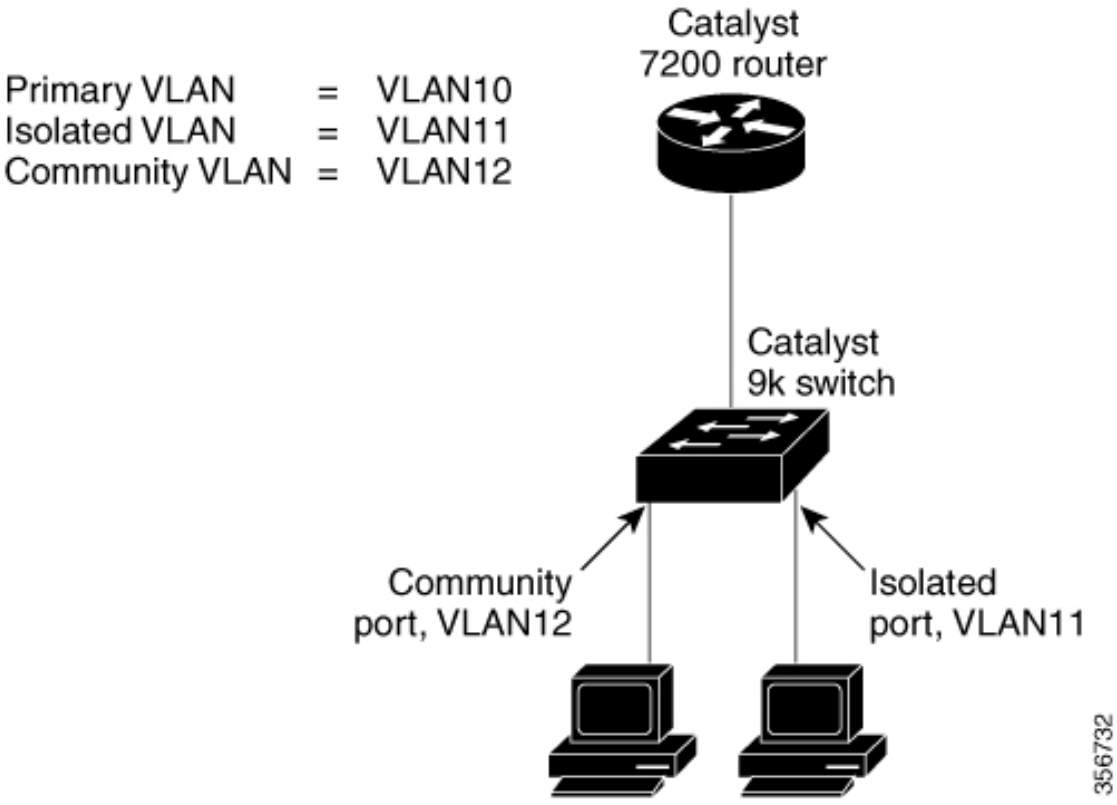
チでは、VLAN 11 が独立 VLAN として設定され、トラフィックは独立ホストポートから送信されたかのように転送されます。

（注） Catalyst 9k シリーズ スイッチは独立トランクと直接接続しているホスト（host3 など）とを分離することができますが、非 PVLAN スイッチに接続しているホスト（host1 および host2 など）を分離することはできません。これらのホストの分離は、Catalyst 2950 上の保護ポートなどの機能を使用して、非 PVLAN スイッチによって行う必要があります。

無差別 PVLAN トランク ポート

無差別プライベート VLAN トランクポートが使用されるのは、一般的には PVLAN 無差別ホストポートを使用する場合ですが、通常の VLAN を複数伝送するか、複数の PVLAN ドメインで VLAN を複数伝送する必要がある場合です。Cisco 7200 ルータなどの PVLAN をサポートしないアップストリームルータを接続できます。

図 *7*: 無差別 *PVLAN* トランク ポート



この図では、Catalyst 9k シリーズ スイッチで、PVLAN ドメインを PVLAN をサポートしないアップストリームルータに接続しています。host1 によってアップ ストリームに送信されるトラフィックは、

コミュニティ VLAN（VLAN 12）の Catalyst 9k シリーズ スイッチに到達します。このトラフィックは、このルータ宛てに無差別 PVLAN トランクにブリッジングされる場合にプライマリ VLAN（VLAN 10）にタグ付けされ、ルータで設定された正しいサブインターフェイスを使用してルーティングされます。

ダウン ストリーム方向のトラフィックは、

無差別ホストポートで受信された場合と同様に、プライマリ VLAN（VLAN 10）の Catalyst 9k スイッチによって無差別 PVLAN トランクポートで受信されます。トラフィックは PVLAN ドメイン内にあるかのように、宛先ホストにブリッジングされます。

PVLAN 無差別トランクは、VLAN QoS と相互に作用します。

プライベート VLAN の他機能との相互作用

ここでは、プライベート VLAN の他の機能との連携について説明します。

プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック

通常の VLAN では、同じ VLAN にあるデバイスはレイヤ 2 レベルで互いに通信しますが、別の VLAN にあるインターフェイスに接続されたデバイスとはレイヤ 3 レベルで通信する必要があります。プライベート VLAN の場合、無差別ポートはプライマリ VLAN のメンバーであり、ホスト ポートはセカンダリ VLAN に属します。セカンダリ VLAN はプライマリ VLAN に対応付けられているため、これらの VLAN のメンバはレイヤ 2 レベルで互いに通信できます。

通常の VLAN の場合、ブロードキャストはその VLAN のすべてのポートに転送されます。プライベート VLAN のブロードキャストの転送は、次のようにブロードキャストを送信するポートによって決まります。

- 独立ポートは、無差別ポートまたはトランク ポートだけにブロードキャストを送信します。
- コミュニティ ポートは、すべての無差別ポート、トランク ポート、同一コミュニティ VLAN のポートにブロードキャストを送信します。
- 無差別ポートは、プライベート VLAN のすべてのポート（その他の無差別ポート、トランク ポート、独立ポート、コミュニティ ポート）にブロードキャストを送信します。

マルチキャスト トラフィックのルーティングとブリッジングは、プライベート VLAN 境界を横断して行われ、単一コミュニティ VLAN 内でも行われます。マルチキャスト トラフィックは、同一独立 VLAN のポート間、または別々のセカンダリ VLAN のポート間で転送されません。

プライベート VLAN のマルチキャスト転送は次の状況をサポートします。

- 送信側が VLAN 外に存在する可能性があり、受信側が VLAN ドメイン内に存在している可能性がある。

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

プライベート VLAN と SVI

スイッチ仮想インターフェイス（SVI）は VLAN のレイヤ 3 インターフェイスを表します。レイヤ 3 デバイスは、セカンダリ VLAN ではなく、プライマリ VLAN だけを介してプライベート VLAN と通信します。レイヤ 3 VLAN インターフェイス（SVI）はプライマリ VLAN にだけ設定してください。レイヤ 3 VLAN インターフェイスをセカンダリ VLAN 用に設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI はアクティブになりません。

- SVI がアクティブである VLAN をセカンダリ VLAN として設定する場合、SVI をディセーブルにしないと、この設定は許可されません。
- セカンダリ VLAN として設定されている VLAN に SVI を作成しようとしてセカンダリ VLAN がすでにレイヤ 3 にマッピングされている場合、SVI は作成されず、エラーが返されます。SVI がレイヤ 3 にマッピングされていない場合、SVI は作成されますが、自動的にシャットダウンされます。

プライマリ VLAN をセカンダリ VLAN と関連付けてマッピングすると、プライマリ VLAN の設定がセカンダリ VLAN の SVI に伝播されます。たとえば、プライマリ VLAN の SVI に IP サブネットを割り当てると、このサブネットは、プライベート VLAN 全体の IP サブネット アドレスになります。

プライベート VLAN とスイッチ スタック

プライベート VLAN はスイッチスタック内で動作することができ、プライベート VLAN ポートはスタック内のさまざまなメンバスイッチに存在することができます。ただし、スタックを次のように変更すると、プライベート VLAN の動作に影響が及ぶ可能性があります。

- スタックにプライベート VLAN 無差別ポートが 1 つだけ含まれ、このポートを含めたメンバスイッチがスタックから削除された場合、プライベート VLAN のホストポートとプライベート VLAN 外との接続が不能になります。
- スタック内にプライベート VLAN 無差別ポートのみがあるアクティブスイッチに障害が発生した場合、またはスタックを残し、新しいアクティブスイッチが選択された場合、古いアクティブスイッチに無差別ポートがあるプライベート VLAN のホストポートとプライベート VLAN 外との接続が不能になります。
- 2 つのスタックが統合した場合、権利を獲得したスタックのプライベート VLAN は影響を受けませんが、スイッチを再起動したときに、権利を獲得しなかったスイッチのプライベート VLAN 設定が失われます。

ダイナミック MAC アドレスを備えたプライベート VLAN

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

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

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

スタティック MAC アドレスを備えたプライベート VLAN

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

例：

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

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

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

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

プライベート VLAN と VACL/QOS との相互作用

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

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

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

れます。これは、ブリッジされたトラフィックとルーティングされたトラフィックの両方に適用されます。

ブリッジング：

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

ルーティング

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

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

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

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

プライベート VLAN および HA サポート

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

プライベート VLAN 設定時の注意事項

ここでは、プライベート VLAN 設定時の注意事項について説明します。

プライベート VLAN のデフォルト設定

プライベート VLAN は設定されていません。

セカンダリ VLAN およびプライマリ VLAN の設定

プライベート VLAN の設定時は、次の注意事項に従ってください。

- プライベート VLAN は、VTP 1、2、および 3 のトランスペアレント モードでサポートされます。デバイスで VTP バージョン 1 または 2 が稼働している場合は、VTP をトランスペアレントモードに設定する必要があります。プライベート VLAN を設定した後で、VTP モードをクライアントまたはサーバーに変更できません。VTP バージョン 3 は、すべてのモードでプライベート VLAN をサポートします。
- VTP バージョン 1 または 2 でプライベート VLAN を設定した後、**copy running-config startup config** 特権 EXEC コマンドを使用して、VTP トランスペアレントモード設定とプライベート VLAN 設定をデバイス スタートアップ コンフィギュレーション ファイルに保存します。保存しないと、デバイスをリセットした場合、デフォルトの VTP サーバーモードになり、プライベート VLAN をサポートしなくなります。VTP バージョン 3 ではプライベート VLAN をサポートします。
- VTP バージョン 1 および 2 では、プライベート VLAN 設定の伝播は行われません。プライベート VLAN ポートが必要なデバイスで VTP バージョン 3 が実行されていない場合は、VTP3 はプライベート VLAN を伝播するため、そのデバイス上でプライベート VLAN を設定する必要があります。
- VLAN 1 または VLAN 1002 ～ 1005 をプライマリ VLAN またはセカンダリ VLAN として設定できません。拡張 VLAN（VLAN ID 1006 ～ 4094）はプライベート VLAN に属することができます。
- プライマリ VLAN には、1 つの独立 VLAN および複数のコミュニティ VLAN を関連付けることができます。独立 VLAN またはコミュニティ VLAN には、1 つのプライマリ VLAN だけを関連付けることができます。
- プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行可能なスパニングツリー プロトコル（STP）インスタンスは 1 つだけです。セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の STP パラメータがセカンダリ VLAN に伝播されます。
- TFTP サーバーから PVLAN 設定をコピーし、それを実行中の設定に適用しても、PVLAN の関連付けは形成されません。プライマリ VLAN がすべてのセカンダリ VLAN に確実に関連付けられていることを確認する必要があります。

  copy flash:config_file running-configの代わりに**configure replace flash:config_file force**を使用することもできます。
- DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。プライマリ VLAN で DHCP スヌーピングをイネーブルにすると、DHCP スヌーピングはセカンダリ VLAN に伝播されます。セカンダリ VLAN で DHCP を設定しても、プライマリ VLAN をすでに設定している場合、DHCP 設定は有効になりません。
- プライベート VLAN ポートで IP ソース ガードをイネーブルにする場合は、プライマリ VLAN で DHCP スヌーピングをイネーブルにする必要があります。

- プライベート VLAN でトラフィックを伝送しないデバイスのトランクから、プライベート VLAN をプルーニングすることを推奨します。
- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN には、別々の Quality of Service（QoS）設定を適用できます
- sticky ARP には、次の考慮事項があります。
  - sticky ARP エントリとは、SVI およびレイヤ 3 インターフェイス上で学習されるエントリです。これらのエントリは、期限切れになることはありません。
  - **ip sticky-arp** グローバル コンフィギュレーション コマンドは、プライベート VLAN に属する SVI でだけサポートされます。
  - **ip sticky-arp** インターフェイス コンフィギュレーション コマンドは、以下でのみサポートされます。
    - レイヤ 3 インターフェイス
    - 標準 VLAN に属する SVI
    - プライベート VLAN に属する SVI

    ip sticky-arp グローバルコンフィギュレーションおよび **ip sticky-arp interface** コンフィギュレーション コマンドの使用の詳細については、このリリースのコマンドリファレンスを参照してください。
- プライマリ VLAN およびセカンダリ VLAN で VLAN マップを設定できますただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ VLAN マップを設定することを推奨します。
- PVLAN は双方向です。これらは、入力側と出力側の両方に適用されます。

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

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

  ルーティング

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

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

プライベート VLAN の特定 IP トラフィックをフィルタリングするには、プライマリ VLAN およびセカンダリ VLAN の両方に VLAN マップを適用する必要があります。

- プライマリ VLAN SVI にだけルータ ACL を適用できます。ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。
- プライベート VLAN がレイヤ 2 でホストを分離していても、ホストはレイヤ 3 で互いに通信できます。
- プライベート VLAN では、次のスイッチド ポート アナライザ（SPAN）機能がサポートされます。
  - プライベート VLAN を SPAN 送信元ポートとして設定できます。
  - プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN 上で VLAN ベースの SPAN（VSPAN）を使用したり、単一の VLAN 上で SPAN を使用したりして、出力トラフィックまたは入力トラフィックを個別に監視することができます。

プライベート VLAN ポートの設定

プライベート VLAN ポートの設定時は、次の注意事項に従ってください。

- プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN にポートを割り当てるには、プライベート VLAN コンフィギュレーション コマンドだけを使用します。プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN として設定する VLAN に割り当てられているレイヤ 2 アクセス ポートは、この VLAN がプライベート VLAN の設定に含まれている場合、非アクティブです。レイヤ 2 トランク インターフェイスは STP フォワーディング ステートのままです。
- PAgP または LACP EtherChannel に属するポートを、プライベート VLAN ポートとして設定しないでください。ポートがプライベート VLAN の設定に含まれている間は、そのポートの EtherChannel 設定はいずれも非アクティブです。
- 設定ミスによる STP ループの発生を防ぎ、STP コンバージェンスを高速化するには、独立ホスト ポートおよびコミュニティ ホスト ポート上で PortFast および BPDU ガードをイネーブルにします。イネーブルの場合、STP はすべての PortFast が設定されたレイヤ 2 LAN

ポートに BPDU ガード機能を適用します。PortFast および BPDU ガードを無差別ポートでイネーブルにしないでください。

- プライベート VLAN の設定で使用される VLAN を削除すると、この VLAN に関連付けられたプライベート VLAN ポートが非アクティブになります。
- ネットワーク デバイスをトランク接続し、プライマリ VLAN およびセカンダリ VLAN がトランクから削除されていない場合、プライベート VLAN ポートはさまざまなネットワーク デバイス上で使用できます。

プライベート VLAN の設定方法

ここでは、プライベート VLAN の設定について説明します。

プライベート VLAN の設定

プライベート VLAN を設定するには、次の手順を実行します。

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

手順

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

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

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

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

（注） VLAN がまだ作成されていない場合、プライベート VLAN 設定プロセスでこれを作成します。

ステップ 3 インターフェイスを独立ポートまたはコミュニティ ホスト ポートに設定して、ホスト ポートに VLAN メンバーシップを割り当てます。

「プライベート VLAN ホストポートとしてのレイヤ 2 インターフェイスの設定」を参照してください

ステップ 4 インターフェイスを無差別ポートとして設定し、無差別ポートをプライマリおよびセカンダリ VLAN のペアにマッピングします。

「プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定」を参照してください

ステップ 5 VLAN 間ルーティングを使用している場合、プライマリ SVI を設定し、セカンダリ VLAN をプライマリ SVI にマッピングします。

「セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング」を参照してください

ステップ 6 プライマリ VLAN 設定を確認します。

プライベート VLAN 内の VLAN の設定および対応付け

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp mode transparent** 例： `Device(config)# vtp mode transparent`	VTP モードをトランスペアレントに設定します（VTP をディセーブルにします）。 （注） VTP3 の場合、サーバーまたはトランスペアレント モードのいずれにもモードを設定できます。
ステップ 4	**vlan** *vlan-id* 例： `Device(config)# vlan 20`	VLAN コンフィギュレーション モードを開始して、プライマリ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 5	**private-vlan primary** 例：	VLAN をプライマリ VLAN として指定します。

	コマンドまたはアクション	目的
	`Device(config-vlan)# private-vlan primary`	
ステップ 6	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**vlan** *vlan-id* 例： `Device(config)# vlan 501`	（任意）VLAN コンフィギュレーション モードを開始して、独立 VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 8	**private-vlan isolated** 例： `Device(config-vlan)# private-vlan isolated`	VLAN を独立 VLAN として指定します。
ステップ 9	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**vlan** *vlan-id* 例： `Device(config)# vlan 502`	（任意）VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 11	**private-vlan community** 例： `Device(config-vlan)# private-vlan community`	VLAN をコミュニティ VLAN として指定します。
ステップ 12	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 13	**vlan** *vlan-id* 例： `Device(config)# vlan 503`	（任意）VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 14	**private-vlan community** 例： `Device(config-vlan)# private-vlan community`	VLAN をコミュニティ VLAN として指定します。
ステップ 15	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**vlan** *vlan-id* 例： `Device(config)# vlan 20`	ステップ 4 で指定したプライマリ VLAN に関して VLAN コンフィギュレーション モードを開始します。
ステップ 17	**private-vlan association** [**add** | **remove**] *secondary_vlan_list* 例： `Device(config-vlan)# private-vlan association 501-503`	セカンダリ VLAN をプライマリ VLAN に関連付けます。単一のプライベート VLAN ID でも、またはハイフンで連結したプライベート VLAN ID でもかまいません。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。 • *secondary_vlan_list* パラメータには複数のコミュニティ VLAN ID を含められますが、独立 VLAN ID は 1 つだけです。 • *secondary_vlan_list* を入力するか、または *secondary_vlan_list* で **add**

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

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN ホスト ポートとして設定し、これをプライマリおよびセカンダリ VLAN に関連付けるには、次の手順を実行します。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/22`	設定するレイヤ2インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode private-vlan host** 例： `Device(config-if)# switchport mode private-vlan host`	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 5	**switchport private-vlan host-association** *primary_vlan_id secondary_vlan_id* 例： `Device(config-if)# switchport private-vlan host-association 20 501`	レイヤ 2 ポートをプライベート VLAN と関連付けます。 （注） これは、レイヤ 2 インターフェイスに PVLAN を関連付けるために必要な手順です。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： `Device# show interfaces gigabitethernet1/0/22 switchport`	設定を確認します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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

レイヤ 2 インターフェイスをプライベート VLAN 無差別ポートとして設定し、これをプライマリおよびセカンダリ VLAN にマッピングするには、次の手順を実行します。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	設定するレイヤ2インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode private-vlan promiscuous** 例： `Device(config-if)# switchport mode private-vlan promiscuous`	レイヤ 2 ポートをプライベート VLAN 無差別ポートとして設定します。

	コマンドまたはアクション	目的
ステップ 5	**switchport private-vlan mapping** *primary_vlan_id* {**add** | **remove**} *secondary_vlan_list* 例： `Device(config-if)# switchport private-vlan mapping 20 add 501-503`	プライベート VLAN 無差別ポートをプライマリ VLAN、および選択したセカンダリ VLAN にマッピングします。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。 • セカンダリ VLAN とプライマリ VLAN をプライベート VLAN 無差別ポートにマッピングするには、*secondary_vlan_list*、または **add** キーワードを指定した *secondary_vlan_list* を使用します。 • セカンダリ VLAN とプライベート VLAN 無差別ポートのマッピングを解除するには、**remove** キーワードを指定した *secondary_vlan_list* を使用します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： `Device# show interfaces gigabitethernet1/0/2 switchport`	設定を確認します。
ステップ 8	**copy running-config startup config** 例： `Device# copy running-config startup-config`	デバイス スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

独立プライベートVLAN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独立 PVLAN トランク ポートとして設定するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	設定するレイヤ2インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode private-vlan** { **host** | **promiscuous** | **trunk promiscuous** | **trunk** [**secondary**]} 例： `Device(config-if)# switchport mode private-vlan trunk secondary`	独立プライベート VLAN トランクポートとしてレイヤ2インターフェイスを設定します。
ステップ 4	**switchport private-vlan association trunk** *primary_vlan_id secondary_vlan_id* 例： `Device(config-if)# switchport private-vlan association trunk 3 301`	プライベート VLAN トランク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。
ステップ 5	**switchport private-vlan trunk allowed vlan** { *word* | **add** |**all** | **except** |**none** | **remove** } *vlan_list* 例： `Device(config-if)# switchport private-vlan trunk allowed vlan 10. 3-4`	PVLAN トランクポートで許容される VLANのリストを設定します。リストにはプライマリ VLAN を含める必要があります。また、通常の VLAN も設定できます。 no キーワードを使用すると、PVLAN トランクポートで許容される VLAN をすべて削除できます。

	コマンドまたはアクション	目的
ステップ 6	**switchport private-vlan trunk native vlan** *vlan_id* 例： `Device(config-if)# switchport private-vlan trunk native vlan 10`	PVLAN トランク ポートに（IEEE 802.1Q タグとしての）タグなしパケットが割り当てられる VLAN を設定します。 no キーワードを使用すると、独立 PVLAN トランクポートでネイティブ VLAN 設定を削除できます。ネイティブ VLAN がデフォルトの VLAN1 に設定されます。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** [*interface-id*] **switchport** 例： `Device# show interfaces gigabitethernet1/0/2 switchport`	設定を確認します。
ステップ 9	**copy running-config startup config** 例： `Device# copy running-config startup-config`	デバイス スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

無差別プライベート VLAN 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無差別プライベートVLANトランクポートとして設定するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	設定するレイヤ2インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode private-vlan** { **host** | **promiscuous** | **trunk promiscuous** | **trunk** [**secondary**]} 例： `Device(config-if)# switchport mode private-vlan trunk promiscuous`	レイヤ 2 ポートを無差別プライベート VLAN トランクポートとして設定します。
ステップ 4	**switchport private-vlan mapping trunk** *primary_vlan_id* [**add** | **remove**] *secondary_vlan_list* 例： `Device(config-if)# switchport private-vlan mapping trunk 20 add 501-503`	無差別プライベートVLANトランクポートをプライマリ VLAN、および選択したセカンダリ VLANにマッピングします。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。 • セカンダリ VLAN を無差別プライベートVLANトランクポートにマッピングするには、*secondary_vlan_list*、または **add** キーワードを指定した *secondary_vlan_list* を使用します。 • セカンダリ VLAN と無差別プライベートVLANトランクポートのマッピングを解除するには、**remove** キーワードを指定した *secondary_vlan_list* を使用します。
ステップ 5	**switchport private-vlan trunk allowed vlan** { *word* | **add** |**all** | **except** |**none** | **remove** } *vlan_list* 例：	PVLAN トランクポートで許容されるVLANのリストを設定します。リストにはプライマリ VLAN を含める必要があります。また、通常の VLAN も設定できます。

	コマンドまたはアクション	目的
	`Device(config-if)# switchport private-vlan trunk allowed vlan 10 3-4`	no キーワードを使用すると、PVLAN 無差別トランクポートで許可されているすべての VLAN を削除できます。
ステップ 6	**switchport private-vlan trunk native vlan** *vlan_id* 例： `Device(config-if)# switchport private-vlan trunk native vlan 10`	PVLAN トランク ポートに（IEEE 802.1Q タグとしての）タグなしパケットが割り当てられる VLAN を設定します。 no キーワードを使用すると、PVLAN 無差別トランクポートのネイティブ VLAN 設定を削除できます。ネイティブ VLAN がデフォルトの VLAN1 に設定されます。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** [*interface-id*] **switchport** 例： `Device# show interfaces gigabitethernet1/0/2 switchport`	設定を確認します。
ステップ 9	**copy running-config startup config** 例： `Device# copy running-config startup-config`	デバイス スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

ポートチャネル上の独立プライベート VLAN 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ポートチャネルの独立プライベート VLAN トランクポートとして設定するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface range* 例： `Device(config)# int range g5/0/17, g5/0/22, g6/0/12`	設定するレイヤ2インターフェイス範囲に対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode private-vlan** { **host** | **promiscuous** | **trunk promiscuous** | **trunk** [**secondary**]} 例： `Device(config-if)# switchport mode private-vlan trunk`	プライベート VLAN 独立トランクポートとしてのレイヤ2インターフェイス範囲の設定
ステップ 4	**switchport private-vlan association trunk** *primary_vlan_id secondary_vlan_id* 例： `Device(config-if)# switchport private-vlan association trunk 20 503`	プライベート VLAN トランク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。
ステップ 5	**switchport private-vlan trunk allowed vlan** { *word* | **add** |**all** | **except** |**none** | **remove** } *vlan_list* 例： `Device(config-if)# switchport private-vlan trunk allowed vlan 20`	PVLAN トランクポートで許容される VLANのリストを設定します。リストにはプライマリ VLAN を含める必要があります。また、通常の VLAN も設定できます。 no キーワードを使用すると、独立プライベート VLAN トランクポートで許可されているすべての VLAN を削除できます。
ステップ 6	**channel-group** *channel group number* **mode** { **active** | **auto** | **desirable** | **on** | **passive** } 例：	チャネル グループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ～ 128 です。ポートチャネルがない場合は、このチャネル

	コマンドまたはアクション	目的
	`Device(config-if)# channel-group 1 mode active`	グループに関連付けられたポート チャネルが自動的に作成されます。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	show etherchannel summary 例： `Device# show etherchannel summary`	設定を確認します。
ステップ 9	**copy running-config startup config** 例： `Device# copy running-config startup-config`	デバイス スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

ポートチャネル上の無差別プライベート VLAN 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ポートチャネルの無差別プライベート VLAN トランクポートとして設定するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface range* 例： `Device(config)# interface g5/0/17, g5/0/22, g6/0/12`	設定するレイヤ2インターフェイス範囲に対して、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**switchport mode private-vlan** { **host** | **promiscuous** | **trunk promiscuous** | **trunk** [**secondary**]} 例： `Device(config-if)# switchport mode private-vlan trunk promiscuous`	レイヤ 2 ポートをプライベート VLAN 無差別トランクポートとして設定します。
ステップ 4	**switchport private-vlan mapping trunk** *primary_vlan_id* [**add** | **remove**] *secondary_vlan_list* 例： `Device(config-if)# switchport private-vlan mapping trunk 20 501-503`	プライベート VLAN 無差別トランクポートをプライマリ VLAN、および選択したセカンダリ VLAN にマッピングします。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。 • セカンダリ VLAN とプライマリ VLAN をプライベート VLAN 無差別ポートにマッピングするには、*secondary_vlan_list*、または **add** キーワードを指定した *secondary_vlan_list* を使用します。 • セカンダリ VLAN とプライベート VLAN 無差別ポートのマッピングを解除するには、**remove** キーワードを指定した *secondary_vlan_list* を使用します。
ステップ 5	**switchport private-vlan trunk allowed vlan** { *word* | **add** |**all** | **except** |**none** | **remove** } *vlan_list* 例： `Device(config-if)# switchport private-vlan trunk allowed vlan 20`	PVLAN トランクポートで許容される VLAN のリストを設定します。リストにはプライマリ VLAN を含める必要があります。また、通常の VLAN も設定できます。 no キーワードを使用すると、無差別プライベート VLAN トランクポートで許可されているすべての VLAN を削除できます。

	コマンドまたはアクション	目的
ステップ 6	**channel-group** *channel group number* **mode** { **active** | **auto** | **desirable** | **on** | **passive** } 例： `Device(config-if)# channel-group 1 mode active`	チャネルグループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ～ 128 です。ポートチャネルがない場合は、このチャネルグループに関連付けられたポート チャネルが自動的に作成されます。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	show etherchannel summary 例： `Device# show etherchannel summary`	設定を確認します。
ステップ 9	**copy running-config startup config** 例： `Device# copy running-config startup-config`	デバイス スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

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

プライベート VLAN が VLAN 間ルーティングに使用される場合、SVI をプライマリ VLAN に設定してセカンダリ VLAN を SVI にマッピングできます。

（注） 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

セカンダリ VLAN をプライマリ VLAN の SVI にマッピングしてプライベート VLAN トラフィックのレイヤ 3 スイッチングを可能にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface vlan** *primary_vlan_id* 例： `Device(config)# interface vlan 20`	プライマリ VLAN でインターフェイス コンフィギュレーション モードを開始して、VLAN を SVI として設定します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 4	**private-vlan mapping** [**add** | **remove**] *secondary_vlan_list* 例： `Device(config-if)# private-vlan mapping 501-503`	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。 （注） **private-vlan mapping** インターフェイス コンフィギュレーション コマンドは、レイヤ 3 スイッチングされているプライベート VLAN トラフィックにだけ影響を与えます。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。 • *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN をプライマリ VLAN にマッピングします。

	コマンドまたはアクション	目的
		• **remove** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN とプライマリ VLAN のマッピングを解除します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces private-vlan mapping** 例： `Device# show interfaces private-vlan mapping`	設定を確認します。
ステップ 7	**copy running-config startup config** 例： `Device# copy running-config startup-config`	デバイス スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

プライベート VLAN のモニター

次の表に、プライベート VLAN をモニターするために使用するコマンドを記載します。

表 *6:* プライベート *VLAN* モニタリング コマンド

コマンド	目的
show interfaces status	所属する VLAN を含む、インター
show vlan private-vlan [**type**]	スイッチスタックのプライベート V
show interface switchport	インターフェイス上のプライベート
show interface private-vlan mapping	VLAN SVI のプライベート VLAN マ

プライベート VLAN の設定例

次のセクションにプライベート VLAN の設定例を示します。

例：プライベート VLAN 内の VLAN の設定および関連付け

次に、VLAN 20 をプライマリ VLAN、VLAN 501 を独立 VLAN、VLAN 502 および 503 をコミュニティ VLAN として設定し、これらをプライベート VLAN 内で関連付けして、設定を確認する例を示します。

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

例：ホスト ポートとしてのインターフェイスの設定

次に、インターフェイスをプライベートVLANホストポートとして設定し、それをプライベート VLAN ペアに関連付けて、その設定を確認する例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/22
Device(config-if)# switchport mode private-vlan host
Device(config-if)# switchport private-vlan host-association 20 501
Device(config-if)# end
Device# show interfaces gigabitethernet1/0/22 switchport
Name: Gi1/0/22
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 20 501
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
```

```
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 501

<output truncated>
```

例：プライベート VLAN 無差別ポートとしてのインターフェイスの設定

次の例では、インターフェイスをプライベート VLAN 無差別ポートとして設定し、それをプライベート VLAN にマッピングする方法を示します。インターフェイスは、プライマリ VLAN 20 のメンバで、セカンダリ VLAN 501 ～ 503 がマッピングされます。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport mode private-vlan promiscuous
Device(config-if)# switchport private-vlan mapping 20 add 501-503
Device(config-if)# end
```

show vlan private-vlan または **show interface status** 特権 EXEC コマンドを使用してプライマリおよびセカンダリ VLAN とデバイス上のプライベート VLAN ポートを表示します。

例：セカンダリ VLAN をプライマリ VLAN インターフェイスにマッピングする

次に、VLAN 501 および 502 のインターフェイスをプライマリ VLAN 10 にマッピングする例を示します。これにより、プライベート VLAN 501 および 502 からのセカンダリ VLAN 入力トラフィックのルーティングが可能になります。

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

例：独立プライベートVLAN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

次に、インターフェイスを独立プライベート VLAN トランクポートとして設定し、その設定を確認する例を示します。

```
Device# configure terminal
Device(config)# interface GigabitEthernet5/0/1
Device(config-if)# switchport private-vlan trunk allowed vlan 20
Device(config-if)# switchport private-vlan association trunk 20 503
Device(config-if)# switchport mode private-vlan trunk
Device(config-if)# end

Device# show interface GigabitEthernet5/0/1 switchport
Name: GigabitEthernet5/0/1
Switchport: Enabled
Administrative Mode: private-vlan trunk secondary
Operational Mode: private-vlan trunk secondary
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 20
Administrative private-vlan trunk associations:
20 (VLAN0020) 503 (VLAN0503)
Administrative private-vlan trunk mappings: none
Operational private-vlan:
20 (VLAN0020) 503 (VLAN0503)
Operational Normal VLANs: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Vepa Enabled: false
Appliance trust: none
```

例：無差別プライベート VLAN 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

次に、インターフェイスを無差別プライベート VLAN トランクポートとして設定し、その設定を確認する例を示します。

```
Device# configure terminal
Device(config)# interface GigabitEthernet6/0/4
Device(config-if)# switchport private-vlan trunk native vlan 20
```

```
Device(config-if)# switchport private-vlan trunk allowed vlan 20
Device(config-if)# switchport private-vlan mapping trunk 20 501-503
Device(config-if)# switchport mode private-vlan trunk promiscuous
Device(config-if)# end

Device# show interface GigabitEthernet6/0/4 switchport
Name: Gi6/0/4
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 20
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 20
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
20 (VLAN0020) 501 (VLAN0501)
502 (VLAN0502)
503 (VLAN0503)

Operational private-vlan:
20 (VLAN0020) 501 (VLAN0501) 502 (VLAN0502) 503 (VLAN0503)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Vepa Enabled: false
Appliance trust: none
```

例：ポートチャネル上の独立プライベート VLAN 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

次に、インターフェイスをポートチャネルの独立プライベート VLAN トランクポートとして設定し、その設定を確認する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface range g5/0/17, g5/0/22, g6/0/12
Device(config-if-range)# switchport mode private-vlan trunk
Device(config-if-range)# switchport private-vlan trunk allowed vlan 20
Device(config-if-range)# switchport private-vlan association trunk 20 503
Device(config-if-range)# channel-group 1 mode active
Device(config-if-range)# end


Device# show etherchannel summary
```

```
Dec 10 13:51:28.423 PST: %SYS-5-CONFIG_I: Configured from console by consolesumm
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------+-------------+-----------+-----------------------------------------------
1 Po1(SU) LACP Gi5/0/17(P) Gi5/0/22(P) Gi6/0/12(P)


Device# show vlan private-vlan
Primary Secondary Type Ports
------- --------- ----------------- ------------------------------------------
20 501 community
20 502 community
20 503 isolated Po1
```

例：ポートチャネル上の無差別プライベート VLAN 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

次に、インターフェイスをポートチャネルの無差別プライベート VLAN トランクポートとして設定し、その設定を確認する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface range g5/0/17, g5/0/22, g6/0/12
Device(config-if-range)# switchport mode private-vlan trunk promiscuous
Device(config-if-range)# switchport private-vlan trunk allowed vlan 20
Device(config-if-range)# switchport private-vlan mapping trunk 20 501-503
Device(config-if-range)# channel-group 1 mode active
Device(config-if-range)# end


Device# show etherchannel summary
Dec 10 13:51:28.423 PST: %SYS-5-CONFIG_I: Configured from console by consolesumm
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------+-------------+-----------+-----------------------------------------------
1 Po1(SU) LACP Gi5/0/17(P) Gi5/0/22(P) Gi6/0/12(P)
```

```
Device# show vlan private-vlan
Primary Secondary Type Ports
------- --------- ----------------- ------------------------------------------
20 501 community Po1
20 502 community Po1
20 503 isolated Po1
```

例：プライベート VLAN のモニタリング

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

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

次の作業

次の設定を行えます。

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

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9300 Series Switches)*

標準および RFC

標準/RFC	タイトル
RFC 1573	Evolution of the Interfaces Group of MIB-II

標準/RFC	タイトル
RFC 1757	『Remote Network Monitoring Management Information Base』
RFC 2021	Remote Network Monitoring Management Information Base Version 2 using SMIv2

MIB

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

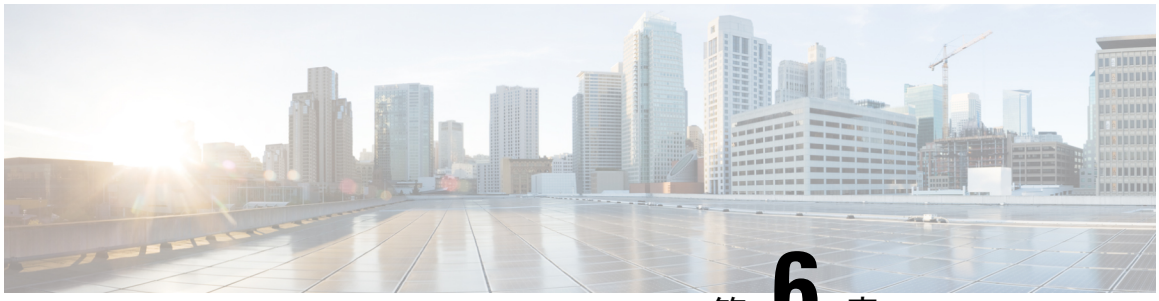
プライベート VLAN の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	プライベート VLAN	この機能が導入されました。 VLAN 機能を使用すると、サービスプロバイダが VLAN を使用したときに直面する問題に対処できます。 • Network Essential または Network Advantage ライセンスを実行している場合、最大で 4094 個のアクティブ VLAN がデバイスでサポートされます。サービス プロバイダが 1 カスタマーあたり 1 つの VLAN を割り当てる場合、サービス プロバイダがサポートできるカスタマー数はこれに制限されます。 • 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が、これにより、未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が起きます。
Cisco IOS XE Amsterdam 17.3.1	トランクポートおよびポートチャネルのプライベート VLAN	プライベート VLAN は独立トランクポート、無差別トランクポートおよびポートチャネルに導入されました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/ に進みます。



第 6 章

レイヤ 3 サブインターフェイスの設定

このモジュールでは、スタティックまたはダイナミック ルーティング プロトコルを使用して IPv4 および IPv6 パケットを別のデバイスに転送する、レイヤ 3 インターフェイスでの dot1q VLAN サブインターフェイスの設定方法について説明します。レイヤ 2 トラフィックの IP ルーティングおよび内部 Virtual Local Area Network（VLAN）ルーティングにはレイヤ 3 インターフェイスが使用できます。

レイヤ 3 サブインターフェイスの設定に関する制約事項

- StackWise 仮想リンクでは、サブインターフェイスはサポートされていません。
- Software-Defined Access（SD-Access）を使用するサブインターフェイスはサポートされません。
- ルーテッド物理インターフェイス、SVI インターフェイス、およびサブインターフェイスを含む 4,000 を超えるレイヤ 3 インターフェイスを設定しないでください。
- 最大 1000 の SVI インターフェイスがサポートされます。
- **native** キーワードを使用せずに、IEEE 802.1Q トランクのネイティブ VLAN でカプセル化を設定しないでください。VLAN ID が IEEE 802.1Q ネイティブ VLAN の ID の場合、**dot1q vlan** コマンドの **native** キーワードを必ず使用してください。
- サブインターフェイス上で標準範囲 VLAN を設定する場合、VLAN トランキングプロトコル（VTP）モードをトランスペアレントから変更できません。
- レイヤ 3 ポートにネイティブ VLAN として dot1q が設定されたサブインターフェイスがある場合、ネイティブ VLAN サブインターフェイスの機能を妨げるため、レイヤ 3 ポートにルーティング関連の設定を行わないことを推奨します。

レイヤ 3 サブインターフェイスに関する情報

dot1q VLAN サブインターフェイスは、ルーテッド物理インターフェイス上の VLAN ID に関連付けられた仮想 Cisco IOS インターフェイスです。親インターフェイスは物理ポートです。サブインターフェイスは、レイヤ 3 物理インターフェイスでもレイヤ 3 ポートチャネルでも作成できます。サブインターフェイスは、IP アドレッシング、転送ポリシー、Quality of Service（QoS）ポリシー、セキュリティポリシーなどのさまざまな機能に関連付けることができます。

親インターフェイスはサブインターフェイスによって複数の仮想インターフェイスに分割されます。これらの仮想インターフェイスに IP アドレスやダイナミック ルーティング プロトコルなど固有のレイヤ 3 パラメータを割り当てることができます。各サブインターフェイスの IP アドレスは、親インターフェイスの他のサブインターフェイスのサブネットとは異なります。

サブインターフェイスの名前は、親インターフェイスの名前（たとえば HundredGigabitEthernet 1/0/33）+ ピリオド（.）+ そのインターフェイス独自の番号です。たとえば、HundredGigabitEthernet 1/0/33.1 という名前の HundredGigabitEthernet インターフェイス 1/0/33 のサブインターフェイスを作成できます。ここで、.1 はサブインターフェイスを示します。

サブインターフェイスを使用すると、親インターフェイスがサポートする各 VLAN に独自のレイヤ 3 インターフェイスを実現できます。この場合、親インターフェイスは別のデバイスのレイヤ 2 トランキング ポートに接続します。サブインターフェイスを設定したら 802.1Q トランキングを使って VLAN ID に関連付けることができます。

VTP トランキングプロトコル（VTP）トランスペアレントモードでは、任意の標準範囲または拡張範囲の VLAN ID を使用して、サブインターフェイスを設定できます。VLAN ID 1 ～ 1005 は、VTP ドメインでグローバルであり、VTP ドメイン内の他のネットワーク デバイス上で定義することができるため、VTP クライアント/サーバー モードでは、拡張範囲 VLAN だけをサブインターフェイスとともに使用することができます。VTP クライアント/サーバーモードでは、標準範囲 VLAN がサブインターフェイスから除外されます。

ルーティングされないプロトコルのブリッジングを行うには、VLAN インターフェイス上でブリッジグループを使用します。これはフォールバックブリッジングとも呼ばれます。VLAN インターフェイスのブリッジグループは、ルートプロセッサ（RP）ソフトウェアでサポートされます。

レイヤ 2 VLAN またはレイヤ 3 VLAN インターフェイスとレイヤ 3 サブ インターフェイスで同じ VLAN ID を設定できます。

レイヤ 3 サブインターフェイスでは、次の機能とプロトコルがサポートされています。

- アドレッシングとルーティング：IPv4 と IPv6。
- ユニキャストルーティング：Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Routing Information Protocol（RIP）、ボーダー ゲートウェイ プロトコル（BGP）、およびスタティックルーティング。

- マルチキャストルーティング：Internet Group Management Protocol（IGMP）、Protocol-Independent Multicast Sparse Mode（PIM-SM）、Source Specific Multicast（SSM）、および Multiprotocol Label Switching（MPLS）。
- ファーストホップ冗長プロトコル（FHRP）：ホットスタンバイ ルータ プロトコル（HSRP）、仮想ルータ冗長プロトコル（VRRP）およびゲートウェイ ロード バランシング プロトコル（GLBP）。
- 双方向フォワーディング検出（BFD）、ユニキャストリバースパス転送（uRPF）、および等コストマルチパス（ECMP）。
- 最大伝送単位（MTU）および IPv4 フラグメント化。
- Virtual Routing and Forwarding（VRF）Lite。
- ルータ アクセス コントロール リストおよびポリシーベースルーティング（PBR）。
- Quality of Service（QoS）：マーキングおよびポリシング。
- サービス：ネットワークアドレス変換（NAT）IPv4、セキュリティ グループ アクセス コントロール リスト（SGACL）の適用、DHCP サーバー/リレー、SGT 交換プロトコル（SXP）、および NetFlow。
- レイヤ 3 EtherChannel。

レイヤ 3 サブインターフェイスの設定方法

ルーテッドインターフェイスに 1 つまたは複数のサブインターフェイスを設定できます。**no switchport** コマンドを使用して、親インターフェイスをルーテッドインターフェイスとして設定します。親インターフェイスには、独自の IP アドレス、ポリシー、および設定を添付できます。ポートに着信するタグなしトラフィックおよびタグ付きトラフィックまたはVLAN（サブインターフェイスでは処理されない）は、親インターフェイスで処理されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例**： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** **例**： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** {*type switch* / *slot* / *port.subinterface*} **例**：	インターフェイスまたはインターフェイス範囲を選択して、サブインターフェイス コンフィギュレーション モードを開

	コマンドまたはアクション	目的

	`Device(config)# interface HundredGigabitEthernet 1/0/33.201`
	または
	`Device(config)# interface range HundredGigabitEthernet1/0/33.201-HundredGigabitEthernet1/0/33.204`
		始します。（インターフェイスを削除するには、このコマンドの **no** 形式を使用します。）
		• この例に示すように、関連付けられた dot1q VLAN ID とともにインターフェイスの範囲を指定することもできます。

ステップ 4	**encapsulation dot1q** *vlan-id* [**native**] 例： `Device(config-subif)# encapsulation dot1q 201 native`	サブインターフェイスの 802.1Q カプセル化を設定します。指定できる範囲は 1 ～ 4000 です。（サブインターフェイスの 802.1Q カプセル化を削除するには、このコマンドの **no** 形式を使用します。） • **native** ：サブインターフェイスをポートに着信するタグなしパケットのデフォルトハンドラにするには、このキーワードを使用します。このキーワードをサブインターフェイスで設定し、IP およびその他の設定が親インターフェイスでも設定されている場合、このキーワードは親インターフェイスの設定を上書きします。このキーワードは、サブインターフェイスで設定するか、親インターフェイスで同時に設定します。 （注） **shutdown** および **no shutdown** コマンドを使用して、親インターフェイスまたは他のサブインターフェイスを通過するトラフィックに影響を与えずに、特定のサブインターフェイスでシャットダウンまたはシャットダウンの反転を実行できます。
ステップ 5	**end** 例： `Device(config-subif)# end`	サブインターフェイスモードを終了して、特権 EXEC モードに戻ります。

例：レイヤ 3 サブインターフェイスの設定

次に、レイヤ 3 インターフェイスのサブインターフェイスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface HundredGigabitEthernet 1/0/33
Device(config-if)# no switchport
Device(config-if)# no ip address
Device(config-if)# exit
Device(config)# interface HundredGigabitEthernet 1/0/33.201
Device(config-subif)# encapsulation dot1q 201 native
Device(config-subif)# end
```

次に、レイヤ 3 ポートチャネルのサブインターフェイスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# no switchport
Device(config-if)# no ip address
Device(config-if)# exit
Device(config)# interface port-channel 2.10
Device(config-subif)# encapsulation dot1q 10
Decvice(config-subif)# ip address 10.10.10.11 255.255.255.0
Device(config-subif)# end
```

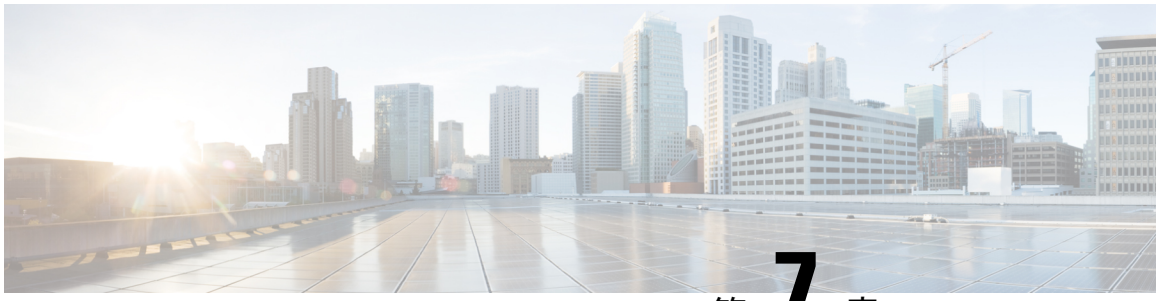
レイヤ 3 サブインターフェイスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *7:* レイヤ *3* サブインターフェイスの機能情報

機能名	リリース	機能情報
レイヤ 3 サブインターフェイス	Cisco IOS XE Gibraltar 16.12.1	レイヤ 3 インターフェイスは、IPv4 および IPv6 パケットをスタティックまたはダイナミック ルーティング プロトコルを使って別のデバイスに転送します。レイヤ 2 トラフィックの IP ルーティングおよび内部 Virtual Local Area Network（VLAN）ルーティングにはレイヤ 3 インターフェイスが使用できます。



第 7 章

有線ダイナミック PVLAN の設定

次のセクションでは、有線動的 PVLAN の設定について説明します。

有線ダイナミック PVLAN の制約事項

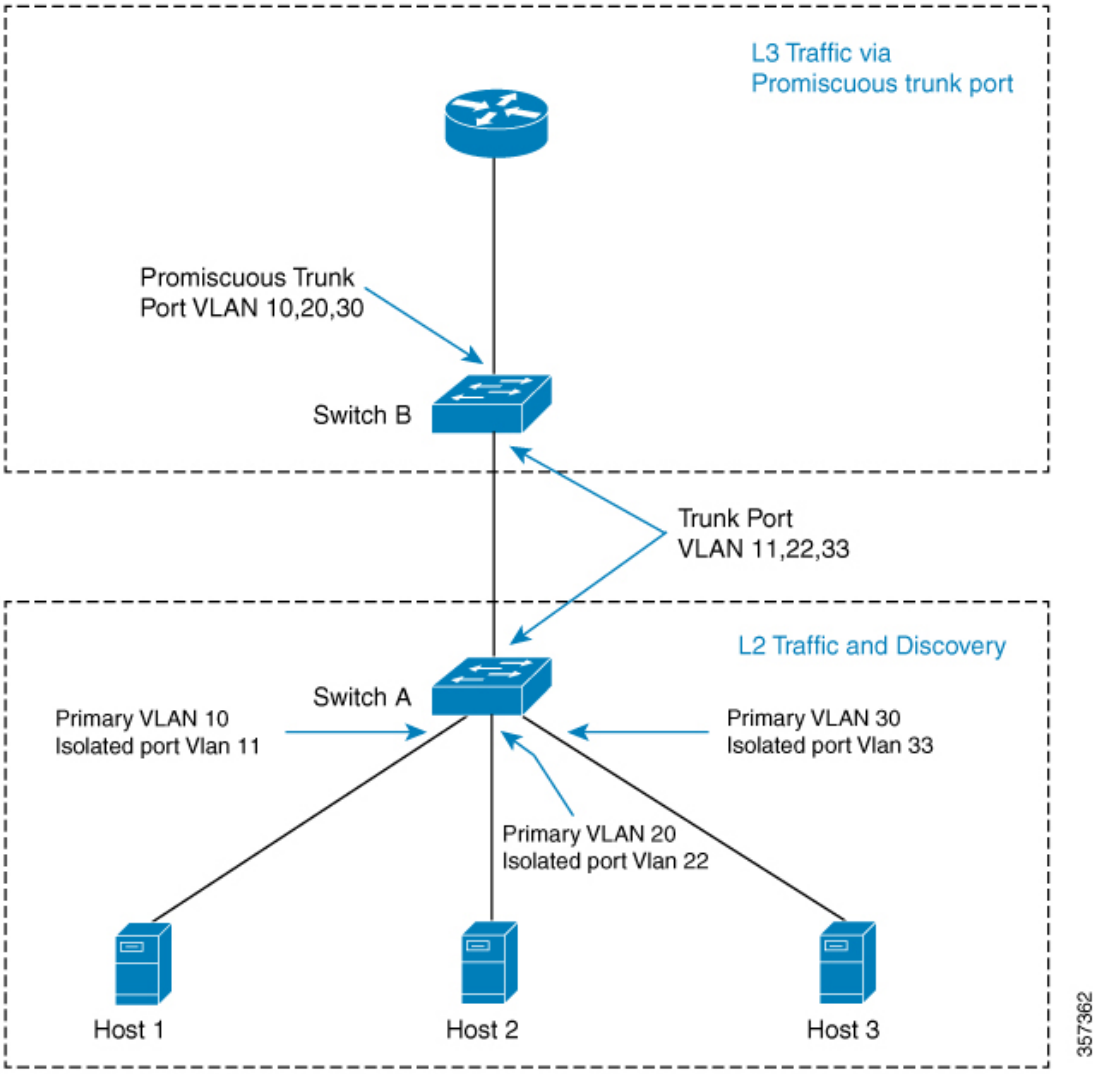
- 有線ダイナミック PVLAN では、ハイアベイラビリティはサポートされません。
- 音声 VLAN 設定は、この機能と共存できません。
- ローカル We b認証（LWA）および中央 Web 認証（CWA）は、この機能では使用できません。
- ダイナミック PVLANインターフェイステンプレートを使用するすべての有線クライアントは、データクライアントとしてプログラムされます。
- PVLAN テンプレートをサポートするのは、既存のアクセスまたは PVLAN ホストスイッチポートモードのインターフェイスのみです。
- ダイナミックテンプレートのサポートには、Identity Based Networking Services 2.0（IBNS 2.0）を使用する必要があります。

有線ダイナミック PVLAN に関する情報

有線ダイナミック PVLAN は、AAA 許可のあるプライベート VLAN を使用してクライアントを分離し、ゼロトラストを提供する機能です。これは、サブネット/VLAN 内のピアツーピア通信をブロックする方法です。ここで、クライアントは PVLAN に割り当てられ、1 つのポートに接続された有線クライアントをレイヤ 2 の他のすべてのポートから分離し、レイヤ 3 通信は無差別ポートを介して行われます。この機能では、ポイントツーポイントブロッキングを保

証するために、ポートインターフェイスごとに単一の有線データクライアントがサポートされます。

（注） 同じインターフェイス上の複数のクライアントからのトラフィックはブロックされません。



このトポロジでは、ホストはスイッチAに接続されており、スイッチの無差別トランクポートとのみ通信できます。PVLANは、中間スイッチを追加することで、複数のスイッチにまたがって拡張できます。上記のトポロジでスイッチ A とスイッチ B の間にスイッチ（スイッチ C）がある場合は、中間リンクにレイヤ 2 トランクポートを設定する必要があります。コミュニティ VLAN の場合、同じコミュニティ VLAN 内の他のホストでパケットを確認できます。

ホストがケーブルでスイッチポートに接続されている場合、そのホストは他のホストを検出できない独立 PVLAN に配置されます。その後、ホストは RADIUS サーバーによって認証されま

す。もう 1 つのシナリオは、ポートがクローズモードになり、ポートが認証されていない場合、Extensible Authentication Protocol over LAN（EAPoL）パケットのみが許可される場合です。ポートが認証されると、そのポートは独立 VLAN に動的に配置されます。ホストは最初に RADIUS サーバで認証されるため、ホストのポートに適用されるダイナミック インターフェイス テンプレートの名前を送信します。このインターフェイステンプレートには、ポートで PVLAN プライマリ VLAN とセカンダリ VLAN を有効にするための設定が含まれています。テンプレートがホストに適用されると、スイッチポートモードが変更され、ポートがアクセスモードから PVLAN モードにフラップします。

（注） AAA 許可によって参照されるインターフェイステンプレートと同じ名前のものをスイッチで設定する必要があります。

インターフェイステンプレートが適用されると、スティッキータイマーで設定された時間だけポートは物理的にダウンし、再びアップします。RADIUS サーバーがインターフェイステンプレートを 2 回送信すると、変換が完了したため無視されます。その後、ポートは隔離されたままの PVLAN に割り当てられます。ホストは許可を完了し、準備完了状態になります。

access-session interface-template sticky timer*time* コマンドを使用して、インターフェイス テンプレート情報をポートから削除する前に保持するキープタイムを設定します。

有線ダイナミック PVLAN の設定

有線ダイナミック PVLAN を設定するには、ユーザーデバイス（上記のトポロジのスイッチ A）で次の手順を実行します。

始める前に

ユーザーデバイスで dot1x aaa が設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**vlan** *vlan-id* 例： `Device(config)# vlan 200`	（任意）VLAN コンフィギュレーション モードを開始して、独立 VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 4	**private-vlan isolated** 例： `Device(config-vlan)# private-vlan isolated`	VLAN を独立 VLAN として指定します。
ステップ 5	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**vlan** *vlan-id* 例： `Device(config)# vlan 100`	VLAN コンフィギュレーション モードを開始して、プライマリ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 7	**private-vlan primary** 例： `Device(config-vlan)# private-vlan primary`	VLAN をプライマリ VLAN として指定します。
ステップ 8	**private-vlan association** [**add** | **remove**] *secondary_vlan_list* 例： `Device(config-vlan)# private-vlan association 200`	セカンダリ VLAN をプライマリ VLAN に関連付けます。単一のプライベート VLAN ID でも、またはハイフンで連結したプライベート VLAN ID でもかまいません。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。

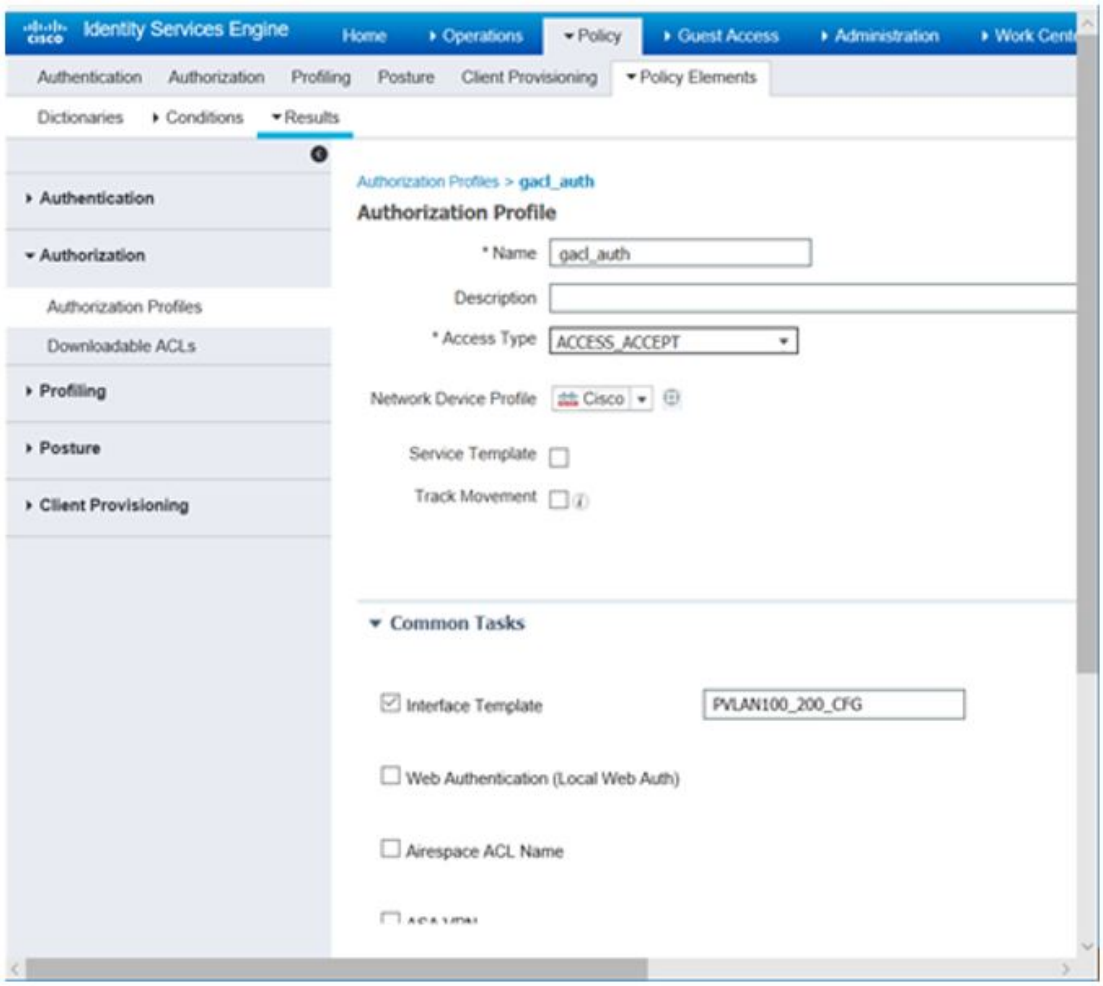
	コマンドまたはアクション	目的
		• *secondary_vlan_list* パラメータには複数のコミュニティ VLAN ID を含められますが、独立 VLAN ID は 1 つだけです。 • *secondary_vlan_list* を入力するか、または *secondary_vlan_list* で **add** キーワードを指定し、セカンダリ VLAN とプライマリ VLAN を関連付けます。 • セカンダリ VLAN とプライマリ VLAN 間の関連付けをクリアするには、*secondary_vlan_list* に **remove** キーワードを使用します。 • このコマンドは、VLAN コンフィギュレーション モードを終了するまで機能しません。
ステップ 9	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**template** *template-name* 例： `Device(config)# template PVLAN100_200_CFG`	ユーザーテンプレートを作成し、テンプレート コンフィギュレーション モードを開始します。
ステップ 11	**switchport mode private-vlan host** 例： `Device(config-template)# switchport mode private-vlan host`	レイヤ 2 ポートを PVLAN ホストポートとしてテンプレートに設定します。
ステップ 12	**switchport private-vlan host-association** *primary_vlan_id secondary_vlan_id* 例： `Device(config-template)# switchport private-vlan host-association 100 200`	テンプレートの PVLAN とレイヤ 2 ポートの関連付けを設定します。

	コマンドまたはアクション	目的
ステップ 13	**exit** 例： `Device(config-template)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**access-session interface-template sticky timer** *time* 例： `Device(config)# access-session interface-template sticky timer 60`	テンプレートの保持時間をグローバルに設定します。最後のクライアントが離れると、設定された保持時間の後にテンプレートがポートから削除されます。 （注） スティッキータイマーを60秒に設定することをお勧めします。
ステップ 15	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet1/0/1`	インターフェイス設定モードに入り、インターフェイスを指定します。
ステップ 16	**access-session interface-template sticky timer** *time* 例： `Device(config-if)# access-session interface-template sticky timer 60`	インターフェイス上のテンプレートの保持時間を設定します。最後のクライアントが離れると、設定された保持時間の後にテンプレートがポートから削除されます。 （注） スティッキータイマーを60秒に設定することをお勧めします。
ステップ 17	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

次のタスク

上記の手順の後、Identity Services Engine（ISE）またはその他の RADIUS サーバーを設定して、クライアントが正常に認証された後にクライアントのポートインターフェイスにテンプレートを割り当てます。

図 *8 :* インターフェイステンプレートを割り当てるための *ISE* の設定



ISE を使用している場合、[Policy] > [Policy Elements] > [Authorization] > [Authorization Profile] ページの順にアクセスします。[Interface Template] チェックボックスをオンにして、クライアント インターフェイスに割り当てるテンプレートの名前を入力します。

別の RADIUS サーバーを使用している場合は、最初のクライアント認証が完了した後に、属性 **Cisco-AVpair="interface:template=name"** をスイッチにプッシュする必要があります。

有線ダイナミック PVLAN の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Bengaluru 17.5.1	有線ダイナミック PVLAN （ホワイトリスト P2P ブロッキング）	有線ダイナミック PVLAN 機能は、プライベート VLAN を使用してクライアントを分離し、ゼロトラストを提供します。これは、サブネット/VLAN 内のピアツーピア通信をブロックする方法です。クライアントは、ポートに接続された単一の有線クライアントを他のポートから分離する PVLAN に割り当てられます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/ に進みます。

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。