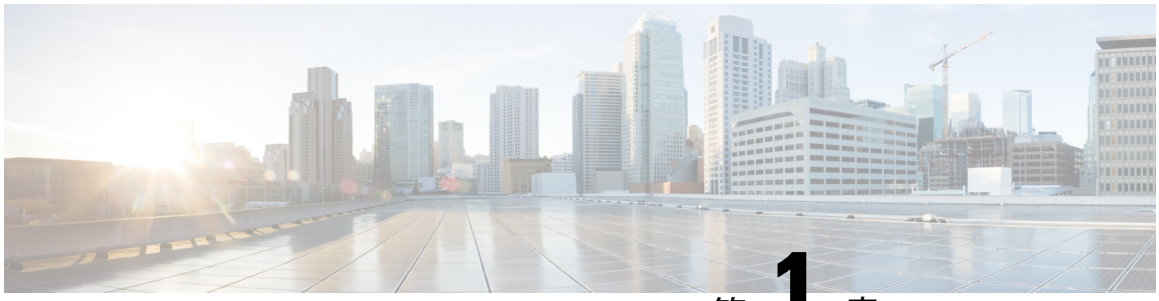
Cisco IOS XE Everest 16.6.x（Catalyst 3650 スイッチ）VLAN コンフィギュレーション ガイド

初版：2017 年 7 月 31 日

最終更新：2017 年 11 月 3 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

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

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 つまたは複数のdevices上で中央集約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devicesに伝達できます。VTP を使用しない場合、VLAN 情報を他のdevicesに送信することはできません。

VTP は、1 つのdeviceで行われた更新が VTP を介してドメイン内の他のdevices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devices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。

deviceは合計 4094 の VLAN をサポートします。ただし、設定済み機能の個数によって、device ハードウェアの使用状況は左右されます。VTP が新しい VLAN をdeviceに通知し、deviceが使用可能な最大限のハードウェア リソースをすでに使用している場合、コントローラはハードウェア リソース不足を伝えるメッセージを送信して、VLAN をシャットダウンします。**show vlan** EXEC コマンドの出力に、中断状態の VLAN が示されます。

[**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、deviceを VTP サーバ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、deviceまたはdevice 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device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、deviceはVTP アドバタイズを受信できません。

関連トピック

VTP アドバタイズ （7 ページ）
VTP ドメインへの VTP クライアント の追加 （23 ページ）
VTP ドメイン （3 ページ）
VTP モード （4 ページ）

VTP の制約事項

次に、VTP に関する制約事項を示します。

- device スタックに スイッチと スイッチを混在させることはできません。

注意 VTP クライアント device 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 devices 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 ドメインの Devices は、VTP 設定リビジョン番号が最も高い device の VLAN 設定をいつも使用します。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deviceを追加すると、VTP サーバおよび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

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devicesが、アクティブdevice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。device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devicesに伝達されます。

device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devicesはアクティブ device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 device、または複数の相互接続された devices 、または同じ VTP ドメイン名を共有して同一管理下にある device スタックで構成されます。deviceは、1 つの VTP ドメインにだけ所属できます。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、またはユーザがドメイン名を設定しない限り、deviceはVTP非管理ドメイン ステートです。管理ドメイン名を指定するか学習するまでは、VTP サーバ上で VLAN を作成または変更できません。また、VLAN 情報はネットワークを介して伝播されません。

device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device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devices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device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devicesには送信されません。また、変更が作用するのは、個々のdeviceに限られます。ただし、deviceがこのモードのときに設定を変更すると、変更内容がdevice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device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。

関連トピック

VTP ドメインへの VTP クライアント の追加 （23 ページ）
VTP の前提条件 （1 ページ）
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 （104 ページ）
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 （109ページ）

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 ドメイン全体に対して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。VTP サーバは、同一 VTP ドメイン内の他のdevicesに自身の VLAN 設定をアドバタイズし、トランク リンクを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devicesと同期させます。 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。deviceがコンフィギュレーションを 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 モードからクライアント 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、deviceを VTP サーバ モードに戻すことはできません。

VTP モード	説明
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 アップデートを送受信しますが、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。VLAN は、ドメインに含まれる、他のサーバ モードのdevice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 に保存されません。VTP バージョン 3 では、VLAN 設定はクライアント モードで NVRAM に保存されます。

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 devicesは、VTP に参加しません。VTP トランスペアレント device は自身の 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 設定を同期さ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、トランスペアレント devicesは、トランクインターフェイスを介して他のdevicesから受信した VTP アドバタイズを転送します。VTP トランスペアレント モードでは、device上の VLAN を作成、変更、削除できます。 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、device は VTP トランスペアレント 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 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 モードに変更しないでください。VTP バージョン 3 では、クライアント モードとサーバ モードでもプライベート VLAN をサポートします。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クライアント モードやサーバ モードに変更しないでください。 device 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 NVRAM に保存されますが、他のdevicesにはアドバタイズされません。このモードでは、VTP モードおよびドメイン名は device 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 device の実行コンフィギュレーションに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。 device 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ションは、スタック内のすべてのdevicesについて同じです。
VTP オフ	VTP オフ モードでのdeviceの機能は、トランクを介して VTP アドバタイズを転送しないことを除くと VTP トランスペアレント device としての機能と同じです。

関連トピック

VTP の前提条件 （1 ページ）
VTP モードの設定 （15 ページ）

VTP アドバタイズ

VTP ドメイン内の各device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 devices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。

関連トピック

VTP の前提条件 （1 ページ）

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、device が VTP サーバ 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 device 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 device 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。

関連トピック

VTP バージョンのイネーブル化 （19 ページ）

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 サーバのステータスは、device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。

関連トピック

VTP バージョンのイネーブル化 （19 ページ）

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、deviceは受信側のdevices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、deviceのトランク ポート上でVLAN 2 ～ 1001 がプルーニング適格です。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 Devices C、E、F も含めて、ネットワーク内のすべてのdeviceがこのブロードキャストを受信します。

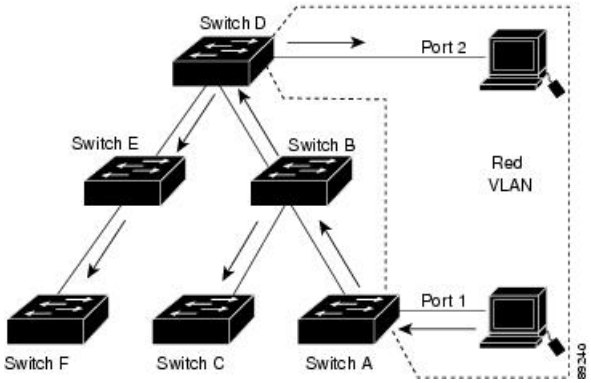
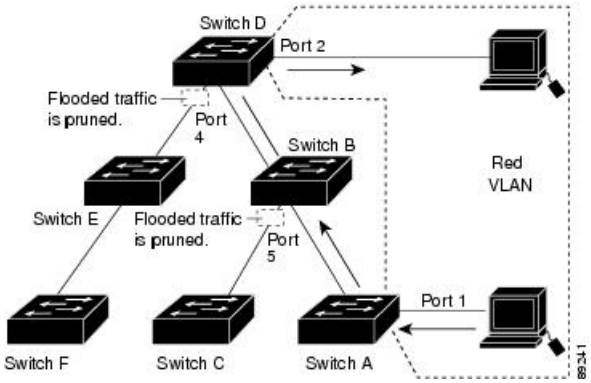


図 *2: VTP* プルーニングによるフラッディング トラフィックの最適化

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、Devices 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device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devices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。

関連トピック

VTP プルーニングのイネーブル化 （21 ページ）

VTP とデバイス スタック

VTP 設定は、device スタックのすべてのメンバで同一です。deviceスタックが VTP サーバ、クライアント、またはトランスペアレントモードになっている場合、スタック内のすべてのdevices の VTP 設定が同一になります。

- スタックに参加したdeviceは、VTP および VLAN のプロパティをアクティブなスイッチから継承します。
- 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deviceの VTP モードが変更されると、そのスタック内のその他のdevicesも VTP モードを変更し、device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 deviceでもスタックでも同じように機能しますが、device スタックが VTP データベースのプライマリ サーバである場合だけは例外です。この場合は、アクティブなスイッチの MAC アドレスがプライマリ サーバ ID として使用されます。アクティブなdeviceがリロードされるか電源オフになると、新たにアクティブなスイッチが選択されます。

- 固定 MAC アドレス機能を設定しない場合、新たにアクティブなdeviceが選択されると、現在のスタック MAC アドレスを使用してテイクオーバーメッセージを送信します。

（注） デフォルトでは、永続的 MAC アドレスがオンになっています。

VTP 設定時の注意事項

VTP の設定要件

VTP を設定する場合は、deviceがドメイン内の他のdevices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、device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device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 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 device 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 device 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。device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。

device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、deviceを再起動すると、device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。

関連トピック

ポート単位の VTP の設定 （22 ページ）
VTP バージョン 3 のプライマリ サーバの設定 （18 ページ）

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devicesを、同じドメイン名で設定する必要があります。VTP トランスペアレントモードのDevicesは、他のdevices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devicesを VTP サーバ モードにする必要があります。

注意 すべてのdevices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deviceを VTP サーバ モードに設定してください。

関連トピック

VTP ドメインへの VTP クライアント の追加 （23 ページ）

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 devices で同じパスワードを共有し、管理ドメイン内の device 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、または間違ったパスワードの Devices は、VTP アドバタイズが拒否されます。

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device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、device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deviceを追加した場合、その新しいdevice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device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。

関連トピック

VTP バージョン 3 のパスワードの設定 （17 ページ）
例：スイッチをプライマリ サーバとして設定する （26 ページ）

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devices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device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deviceは、VTP バージョン 1 を実行しているdevice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device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deviceが VTP バージョン 1 を実行しているdeviceに接続すると、VTP バージョン 1 のdeviceは VTP バージョン 2 に移行し、VTP バージョン 3 の

device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 device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device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deviceがバージョン 2 に対応可能な場合を除いて、devices 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device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devices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device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devices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 devices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。

関連トピック

VTP バージョンのイネーブル化 （19 ページ）

VTP の設定方法

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 モード：VTP サーバ 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 deviceは、VTP ドメイン内の VTP サーバから 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、deviceで VTP がディセーブルになります。deviceは VTP アップデートを送信せず、他のdevice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device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device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：** `デバイス> 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：** `デバイス# 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 domain** *domain-name* **例：** `デバイス(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 モードまたはクライアント モードのdevicesは、すべて

	コマンドまたはアクション	目的
		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。deviceがVTP ドメインにトランク接続されている場合、deviceはドメイン内のVTPサーバ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： `デバイス(config)# vtp mode server`	VTP モード（クライアント、サーバ、トランスペアレント、またはオフ）のdevice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： `デバイス(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device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： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show vtp status** 例： `デバイス# 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。

	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： `デバイス# 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。 device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。

関連トピック

VTP モード （4 ページ）

VTP バージョン 3 のパスワードの設定

device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： `デバイス> 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： `デバイス# 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： `デバイス(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： `デバイス(config)# vtp password mypassword hidden`	（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。 • （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

	コマンドまたはアクション	目的
		ます。VTP プライマリ サーバ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： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show vtp password** 例： `デバイス# show vtp password`	入力を確認します。次のような出力が表示されます。 VTP password: 89914640C8D90868B6A0D8103847A733
ステップ 7	**copy running-config startup-config** 例： `デバイス# 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。

関連トピック

VTP ドメインのパスワード （13 ページ）
例：スイッチをプライマリ サーバとして設定する （26 ページ）

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： `デバイス(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 2	**vtp primary** [**vlan** | **mst**] [**force**] 例： `デバイス# vtp primary vlan force`	deviceの動作ステートをセカンダリ サーバ（デフォルト）からプライマリ サーバに変更し、その設定をドメインにアドバタイズします。device 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。

関連トピック

VTP の設定 （12 ページ）

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device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device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device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 モードまたはトランスペアレント モードのdevicesだけです。deviceが VTP バージョン 3 を実行し、かつdevice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devices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device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： `デバイス> 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： `デバイス# 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： `デバイス(config)# vtp version 2`	deviceでVTP バージョンをイネーブルにします。デフォルトは VTP バージョン 1 です。
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status** 例：	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。

	コマンドまたはアクション	目的
	デバイス# **show vtp status**	
ステップ 6	**copy running-config startup-config** 例： デバイス# **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。

関連トピック

VTP バージョン （13 ページ）
VTP バージョン 2 （8 ページ）
VTP バージョン 3 （8 ページ）

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devices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 deviceのアップストリーム側にあるdevice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： デバイス> **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： デバイス# **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： デバイス(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 モードの 1 台のdevice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： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status** 例： デバイス# **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。

関連トピック

VTP プルーニング （9 ページ）

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： デバイス> **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： `デバイス# 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： `デバイス(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： `デバイス(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： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id* 例： `デバイス# 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： `デバイス# show vtp status`	設定を確認します。

関連トピック

VTP の設定 （12 ページ）

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device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 devices 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 ドメインの Devices は、VTP 設定リビジョン番号が最も高い device の VLAN 設定をいつも使用します。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deviceを追加すると、VTP サーバおよび 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。

device 上で VTP をディセーブルにし、VTP ドメイン内の他の devices 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： デバイス> **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	**show vtp status** 例： デバイス# **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、device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、device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： デバイス# **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 4	**vtp domain** *domain-name* 例： `デバイス(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： `デバイス(config)# end`	特権 EXEC モードに戻ります。device 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： `デバイス# 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： `デバイス# 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 8	**vtp domain** *domain-name* 例： `デバイス(config)# vtp domain domain012`	deviceの元のドメイン名を開始します。
ステップ 9	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。device の VLAN 情報が更新されます。
ステップ 10	**show vtp status** 例： `デバイス# 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。

関連トピック

VTP ドメイン （3 ページ）

VTP の前提条件 （1 ページ）
VTP 設定のためのドメイン名 （12 ページ）

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。device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 メッセージに関するカウンタを表示します。
show vtp devices [**conflict**]	ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。プライマリ サーバと競合する VTP バージョン 3 の装置が表示されます。**show vtp devices** コマンドは、deviceがトランスペアレントモードまたはオフモードのと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指定されたインターフェイスに対する VTP のステータスおよび設定を表示します。
show vtp password	VTP パスワードを表示します。表示されるパスワードの形式は、**hidden** キーワードが入力されているか、または、暗号化がdeviceでイネーブル化されているかどうかによって異なります。
show vtp status	VTP device設定情報を表示します。

VTP の設定例

例：スイッチをプライマリ サーバとして設定する

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（デフォルト）としてdeviceを設定する方法の例を示します。

```
デバイス# 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
```

関連トピック

VTP バージョン 3 のパスワードの設定 （17 ページ）
VTP ドメインのパスワード （13 ページ）

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。	『*VLAN Command Reference (Catalyst 3650 Switches)*』 『*Layer 2/3 Command Reference (Catalyst 3650 Switches)*』
追加の設定コマンドおよび手順。	『*LAN Switching* コンフィギュレーション ガイド, *Cisco IOS XE Release 3SE (Catalyst 3650* スイッチ*)*』 『*Layer 2/3 Configuration Guide (Catalyst 3650 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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

MIB

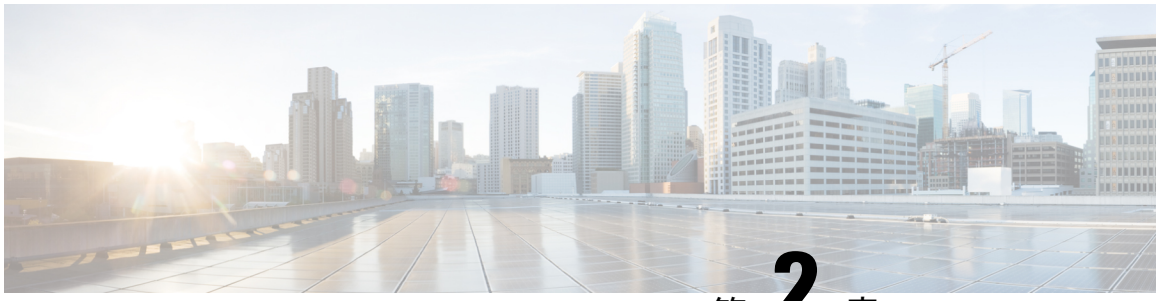
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

VTP の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。



第 2 章

VLAN の設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

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。

- Web UI を使用して VLAN を設定するには、仮想端末（VTY）回線を 50 に変更する必要があります。Web UI は、HTTP リクエストの処理に VTY 回線を使用します。複数の接続が開いていると、デバイスによって設定されたデフォルトの VTY 回線 15 が使い果たされた状態になることがあります。したがって、Web UI を使用する前に VTY 回線を 50 に変更する必要があります。

（注） デバイスのVTY回線を増やすには、コンフィギュレーションモードで次のコマンドを実行します。

```
Device#configure terminal
 Device(config)#service tcp-keepalives in
 Device(config)#service tcp-keepalives out

 Device#configure terminal
 Device(config)#line vty 16-50
```

- 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。
- deviceで多数のVLANを設定し、ルーティングをイネーブルにしない予定の場合は、Switch Database Management（SDM）機能を VLAN 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。
- LANベース フィーチャ セットが稼働しているDevicesは、SVIのスタティック ルーティングのみをサポートします。
- VLAN グループに VLAN を追加できるようにするため、VLAN がdevice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。

- deviceは、イーサネット ポート経由のVLANトラフィックの送信方式として、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ルータのMACアドレスの設定はサポートされていません。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。
- スイッチ スタックに Catalyst 3850 スイッチと Catalyst 3650 スイッチを組み合わせて含めることはできません。

VLAN について

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device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deviceを経由して伝送しなければなりません。device スタックでは、スタック全体にまたがる複数のポートで VLAN を形成できます。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。

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。device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device 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。

deviceは、device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

deviceは、VTP クライアント、サーバ、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。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 device 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。device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。

deviceで最大 4049 の VLAN を設定できます。

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、device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deviceまたはdevice スタックのトランク ポートに接続されているdeviceまたはdevice 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。
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devices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。

関連トピック

VLAN へのスタティック アクセス ポートの割り当て （41 ページ）
VLAN のモニタリング （45 ページ）

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device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。

device 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devicesでは、vlan.dat ファイルがアクティブ device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、deviceを再起動すると、device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device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。

- deviceが VTP サーバ 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）。
- VTP トランスペアレント モードで作成された拡張範囲 VLAN は、VLAN データベースに保存されず、伝播されません。VTP バージョン 3 では、VTP サーバ モードでの拡張範囲 VLAN（VLAN 1006～4094）データベース伝播をサポートします。
- VLAN を作成する前に、deviceを VTP サーバ 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。deviceが VTP サーバである場合には、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。
- device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。device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。
- deviceでは、一定数のスパニングツリー インスタンスがサポートされています（最新情報についてはデータシートを参照してください）。device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。

  device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device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device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devices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devices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。

  device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、device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。
- スタック内のdeviceが新しい VLAN を学習するか、または既存の VLA を削除または変更すると（ネットワーク ポートを介した VTP を通じてか、または CLI を通じて）、その VLAN 情報はすべてのスタック メンバに伝達されます。
- deviceがスタックに参加した場合、またはスタックの結合が発生した場合には、新しいdevices上の VTP 情報（vlan.dat ファイル）とアクティブなdeviceとの間の一貫性が維持されます。

関連トピック

イーサネット VLAN の作成または変更 （38 ページ）
VLAN のモニタリング （45 ページ）

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、device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device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、device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。
- device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。

関連トピック

拡張範囲 VLAN の作成 （43 ページ）
VLAN のモニタリング （45 ページ）

VLAN の設定方法

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 データベースの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device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。

device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devices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deviceはトークン リング接続をサポートしませんが、トークン リング接続を行っているリモート デバイスを、いずれかのサポート対象devicesから管理できます。VTP バージョン 2 を実行しているDevices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： `デバイス# 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：	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

	コマンドまたはアクション	目的
	デバイス(config)# **vlan 20**	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： デバイス(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、VLAN 4 のデフォルトの VLAN 名は VLAN0004 になります。
ステップ 4	**media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** } 例： デバイス(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。 • **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	**remote-span** 例： デバイス(config-vlan)# **remote-span**	（任意）リモート スイッチド ポート アナライザ（SPAN）セッションに対する RSPAN VLAN として、VLAN を設定します。リモート SPAN の詳細については、『*Catalyst 3650* ネットワーク管理コンフィギュレーション ガイド』を参照してください。
ステップ 6	**end** 例： デバイス(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 vlan** { **name** *vlan-name* | **id** *vlan-id*} 例： デバイス# **show vlan name test20 id 20**	入力を確認します。

関連トピック

標準範囲 VLAN 設定時の注意事項 （35 ページ）
VLAN のモニタリング （45 ページ）

VLAN の削除

VTP サーバ モードのdeviceから VLAN を削除すると、VTP ドメイン内のすべてのdevices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 deviceから VLAN を削除した場合、その特定のdeviceスイッチまたはdeviceスタック上に限り 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： デバイス> **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： デバイス# **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：	VLAN ID を入力して、VLAN を削除します。

	コマンドまたはアクション	目的
	デバイス(config)# **no vlan 4**	
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show vlan brief** 例： デバイス# **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： デバイス# **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。

関連トピック

VLAN のモニタリング （45 ページ）

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。

Cisco Catalyst 9500 シリーズ スイッチで、クラスタ メンバ deviceのポートを VLAN に割り当てる場合は、最初に **rcommand** 特権 EXEC コマンドを使用してそのクラスタ メンバ スイッチにログインします。

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： デバイス> **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： `デバイス# 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： `デバイス(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： `デバイス(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： `デバイス(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： `デバイス(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： `デバイス# 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： `デバイス# 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： デバイス# **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。

関連トピック

VLAN ポート メンバーシップ モード （33 ページ）
VLAN のモニタリング （45 ページ）

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、device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： デバイス> **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： デバイス# **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：
	`デバイス(config)# vlan 2000`
	`デバイス(config-vlan)#`
		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。

ステップ 4	**remote-span** 例： `デバイス(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：
	`デバイス(config-vlan)# exit`
	`デバイス(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： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show vlan id** *vlan-id* 例： `デバイス# 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： `デバイス# 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。

関連トピック

拡張範囲 VLAN 設定時の注意事項 （37 ページ）
VLAN のモニタリング （45 ページ）

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*]	device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。
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**]	device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） deviceCLI 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。

関連トピック

イーサネット VLAN の作成または変更 （38 ページ）
標準範囲 VLAN 設定時の注意事項 （35 ページ）
VLAN の削除 （40 ページ）
VLAN へのスタティック アクセス ポートの割り当て （41 ページ）
VLAN ポート メンバーシップ モード （33 ページ）
拡張範囲 VLAN の作成 （43 ページ）
拡張範囲 VLAN 設定時の注意事項 （37 ページ）

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。	『*VLAN Command Reference (Catalyst 3650 Switches)*』 『*Layer 2/3 Command Reference (Catalyst 3650 Switches)*』
VLAN アクセス マップ	『*Security Configuration Guide (Catalyst 3650 Switches)*』 『*Security Command Reference (Catalyst 3650 Switches)*』
VLAN およびモビリティ エージェント	『*Mobility コンフィギュレーション ガイド, Cisco IOS XE Release 3SE (Catalyst 3650 スイッチ)*』
Cisco Flexible NetFlow	『*Cisco Flexible NetFlow コンフィギュレーション ガイド, Cisco IOS XE Release 3SE (Catalyst 3650 スイッチ)*』 『*Flexible Netflow コンフィギュレーション ガイド, Cisco IOS XE Release 3SE (Catalyst 3650 スイッチ)*』
IGMP スヌーピング	『*IP Multicast Routing Command Reference (Catalyst 3650 Switches)*』 『*IP Multicast Routing Configuration Guide (Catalyst 3650 Switches)*』
IPv6	『*IPv6 Configuration Guide (Catalyst 3650 Switches)*』 『*IPv6 Command Reference (Catalyst 3650 Switches)*』

関連項目	マニュアル タイトル
SPAN	『*Network Management Command Reference (Catalyst 3650 Switches)*』 『*Network Management Configuration Guide (Catalyst 3650 Switches)*』
プラットフォームに依存しない設定情報	『*Identity Based Networking Services* コンフィギュレーション ガイド, *Cisco IOS XE Release 3SE (Catalyst 3650* スイッチ*)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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

MIB

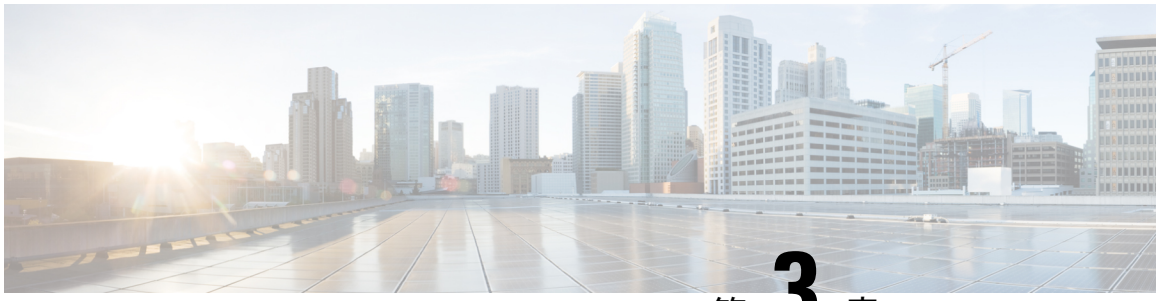
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

VLAN の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	VLAN（GUI）サポート。



第 3 章

VLAN トランクの設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

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 devicesのネットワークでは、devices 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 deviceを他社製のデバイスに接続する場合、Cisco device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 device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 devicesからなるクラウドにより分離されたCisco devicesによって維持されます。Cisco devicesを分離する他社製のIEEE 802.1Qクラウドは、devices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、device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。
- device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、device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。
- スイッチ スタックに Catalyst 3850 スイッチと Catalyst 3650 スイッチを組み合わせて含めることはできません。

VLAN トランクについて

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 device 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、device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。

すべてのイーサネット インターフェイス上で、次のトランキング カプセル化方式を使用できます。

- IEEE 802.1Q：業界標準のトランキング カプセル化方式です。

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。

関連トピック

トランク ポートの設定 （55 ページ）
レイヤ 2 インターフェイス モード （52 ページ）

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。 （注） **switchport mode private-vlan** コマンドオプションはサポートされていません。

関連トピック

トランク ポートの設定 （55 ページ）
トランキング モード （51 ページ）

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。

関連トピック

トランクでの許可 VLAN の定義 （57 ページ）

トランク ポートでの負荷分散

負荷分散により、devices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、devices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device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deviceに接続することも、2 台の異なるdevices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device上の 2 つのポートがループを形成すると、device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。

関連トピック

STP ポート プライオリティによる負荷分散の設定 （62 ページ）

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。

関連トピック

STP パス コストによる負荷分散の設定 （65 ページ）

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、device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

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、device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device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、device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： `デバイス> 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：	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
	デバイス# **configure terminal**	
ステップ 3	**interface** *interface-id* 例： デバイス(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： デバイス(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： デバイス(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。

	コマンドまたはアクション	目的
ステップ 6	**switchport trunk native vlan** *vlan-id* 例： `デバイス(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： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** *interface-id* **switchport** 例： `デバイス# 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： `デバイス# 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： `デバイス# 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。

関連トピック

トランキング モード （51 ページ）
レイヤ 2 インターフェイス モード （52 ページ）

トランクでの許可 VLAN の定義

VLAN 1 は、すべての Cisco devices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： デバイス> **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： デバイス# **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： デバイス(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： デバイス(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： デバイス(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： デバイス(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 interfaces** *interface-id* **switchport** 例： `デバイス# 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： `デバイス# 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。

関連トピック

トランクでの許可 VLAN （53 ページ）

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： `デバイス> 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： `デバイス# 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： `デバイス(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： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id* **switchport** 例： `デバイス# 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： `デバイス# 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、device 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、device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： `デバイス> 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： `デバイス# 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： `デバイス(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： `デバイス(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： `デバイス(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： `デバイス# show interfaces`	[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
	gigabitethernet 1/0/2 switchport	
ステップ 7	**copy running-config startup-config** 例： デバイス# **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

STP ポート プライオリティによる負荷分散の設定

device が device スタックのメンバーである場合、**spanning-tree** [**vlan** *vlan-id*] **port-priority** *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*] **cost** *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： デバイス> **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： デバイス# **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： デバイス(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： `デバイス(config)# vtp mode server`	デバイス A を VTP サーバとして設定します。
ステップ 5	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show vtp status** 例： `デバイス# show vtp status`	デバイス A およびデバイス 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： `デバイス# 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： `デバイス# 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： `デバイス(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： `デバイス(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
	デバイス(config-if)# **end**	
ステップ 12	**show interfaces** *interface-id* **switchport** 例： デバイス# **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 A で、device またはdevice スタック の 2 番目のポートに対して前述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： デバイス# **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： デバイス# **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： デバイス(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： デバイス(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
	デバイス(config-if)# **exit**	
ステップ 20	**interface** *interface-id* 例： デバイス(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： デバイス(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： デバイス(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 23	**show running-config** 例： デバイス# **show running-config**	入力を確認します。
ステップ 24	**copy running-config startup-config** 例： デバイス# **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。

関連トピック

STP プライオリティによるネットワーク負荷分散 （53 ページ）

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： `デバイス> 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： `デバイス# 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： `デバイス(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： `デバイス(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： `デバイス(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： `デバイス(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 8	**show running-config** 例： `デバイス# 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： `デバイス# show vlan`	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devicesからVTP情報を受信します。このコマンドは、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： `デバイス# 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： `デバイス(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： `デバイス(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： `デバイス(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。	

	コマンドまたはアクション	目的
ステップ 15	**exit** 例： `デバイス(config)# exit`	特権 EXEC モードに戻ります。
ステップ 16	**show running-config** 例： `デバイス# 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。
ステップ 17	**copy running-config startup-config** 例： `デバイス# 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。

関連トピック

STP パス コストによるネットワーク負荷分散 （54 ページ）

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
- VLAN グループ
- 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。	『*VLAN Command Reference (Catalyst 3650 Switches)*』 『*Layer 2/3 Command Reference (Catalyst 3650 Switches)*』 *Command Reference (Catalyst 9300 Series Switches)* *Command Reference (Catalyst 9500 Series Switches)*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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

MIB

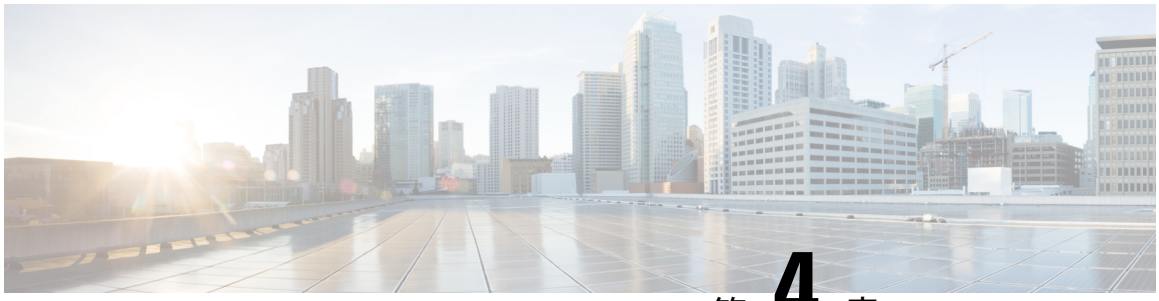
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートWebサイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

VLAN トランクの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。



第 4 章

音声 VLAN の設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

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device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、device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device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device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

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。device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device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、device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deviceを設定できます。

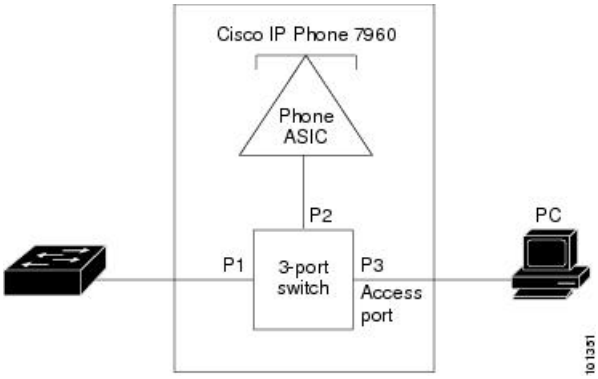
図 *3:* デバイスに接続された *Cisco7960 IP Phone*

このネットワーク設定は、Cisco 7960 IP Phone を接続する 1 つの方法です。

Cisco IP Phone には、統合型 3 ポート 10/100 deviceが搭載されています。これらのポートは、次のデバイスへの接続専用です。

- ポート 1 は、deviceまたは他の Voice over IP（VoIP）デバイスに接続します。
- ポート 2 は、IP Phone のトラフィックを伝送する内部 10/100 インターフェイスです。

• ポート 3（アクセス ポート）は、PC または他のデバイスに接続します。



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、device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device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。

関連トピック

Cisco IP Phone の音声トラフィックの設定 （75 ページ）
音声 VLAN のモニタリング （79 ページ）

Cisco IP Phone のデータ トラフィック

device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、device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。

関連トピック

着信データ フレームのプライオリティ設定 （78 ページ）
音声 VLAN のモニタリング （79 ページ）

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、device 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、device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）devices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device 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

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： `デバイス# 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： `デバイス(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： `デバイス(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： `デバイス(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、device を設定します。デフォルトでは、device 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

	コマンドまたはアクション	目的
		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： `デバイス(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：
	`デバイス# show interfaces gigabitethernet1/0/1 switchport`
	または
	`デバイス# 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： `デバイス# 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。

関連トピック

Cisco IP Phone の音声トラフィック （73 ページ）
音声 VLAN のモニタリング （79 ページ）

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device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：** `デバイス> 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：** `デバイス# 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：** `デバイス(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：** `デバイス(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： `デバイス(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： `デバイス# 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： `デバイス# 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。

関連トピック

Cisco IP Phone のデータ トラフィック （73 ページ）
音声 VLAN のモニタリング （79 ページ）

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。

関連トピック

Cisco IP Phone の音声トラフィックの設定 （75 ページ）
Cisco IP Phone の音声トラフィック （73 ページ）
着信データ フレームのプライオリティ設定 （78 ページ）
Cisco IP Phone のデータ トラフィック （73 ページ）

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 グループ
- VLAN トランキング
- VTP
- 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。	『*VLAN Command Reference (Catalyst 3650 Switches)*』 『*Layer 2/3 Command Reference (Catalyst 3650 Switches)*』 *Command Reference (Catalyst 9500 Series Switches)* *Command Reference (Catalyst 9300 Series Switches)*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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

MIB

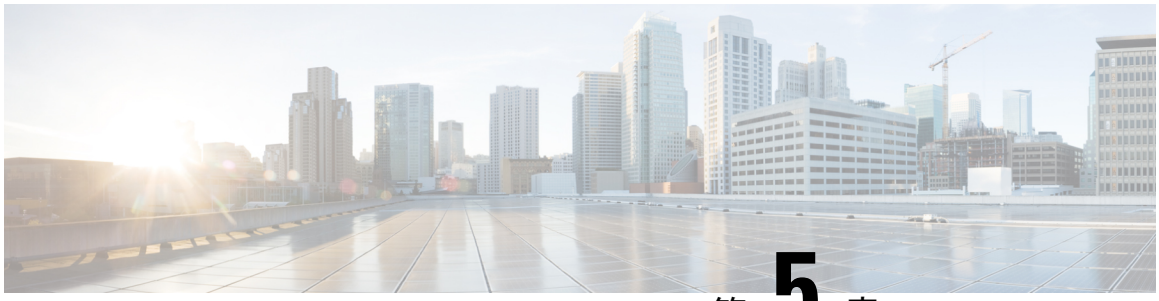
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

音声 VLAN の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。



第 5 章

プライベート VLAN の設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

プライベート VLAN の前提条件

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 モードでもサポートされます。

プライベート VLAN をdevice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。

プライベート VLAN の制約事項

- プライベート VLAN が設定されているdevices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。
- 次のような機能が設定されているインターフェイスにプライベート VLAN ポートを設定しないでください。
  - 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）
  - IPv6 Security Group（SG）
  - ポート集約プロトコル（PAgP）
  - リンク集約制御プロトコル（LACP）
  - 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）
- 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 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（SVI）はプライマリ VLAN にだけ設定してください。

プライベート VLAN について

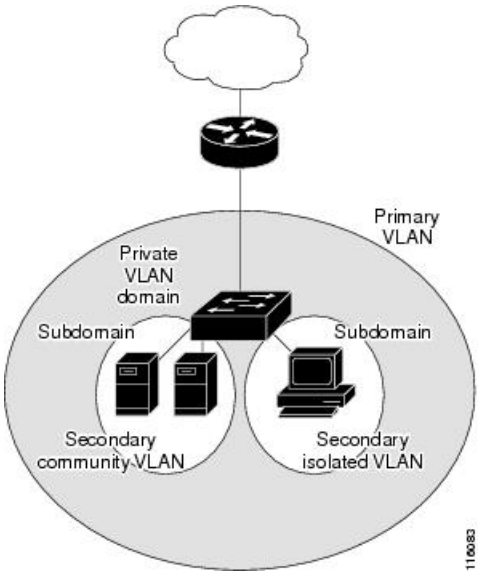
プライベート VLAN ドメイン

PVLAN 機能を使用すると、サービス プロバイダーが 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。

- IP Base イメージまたは IP Services イメージを実行している場合、最大で 4094 個のアクティブ VLAN がdevice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 プロバイダーにとっては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。

関連トピック

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（104 ページ）
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（109 ページ）

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deviceに接続されます。無差別ポートでは、広範囲なデバイスをプライベート VLAN のアクセス ポイントとして接続できます。たとえば、すべてのプライベート VLAN サーバを管理ワークステーションから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。

関連トピック

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 （101 ページ）
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 （102 ページ）
例：ホスト ポートとしてのインターフェイスの設定 （107 ページ）
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 （108 ページ）

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の場合、この設定によりサーバ間のレイヤ 2 通信ができなくなります。
- デフォルト ゲートウェイおよび選択したエンドステーション（バックアップ サーバなど）に接続されているインターフェイスを無差別ポートとして設定し、すべてのエンドステーションがデフォルト ゲートウェイにアクセスできるようにします。

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

プライベート VLAN 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。

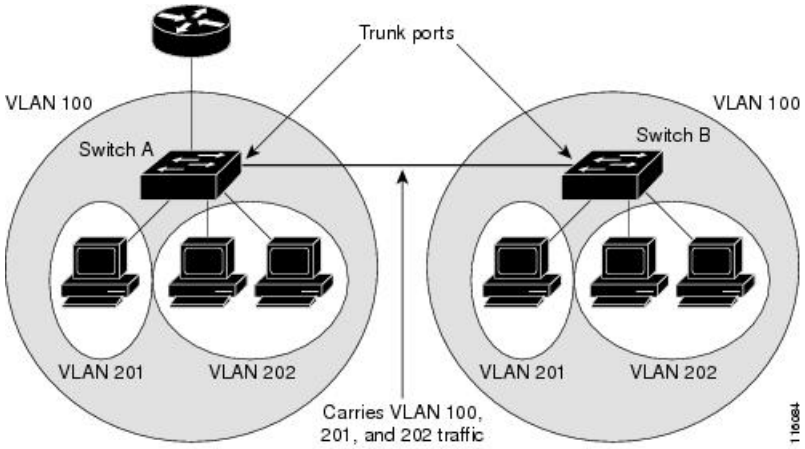
この問題は、プライベート VLAN を使用すると軽減します。プライベート VLAN では、プライベート VLAN のすべてのメンバーが、プライマリ VLAN に割り当てられている共通アドレス空間を共有するためです。ホストはセカンダリ VLAN に接続され、プライマリ VLAN に割り当てられているアドレスのブロックから IP アドレスが DHCP サーバによってホストに割り当てられますが、同一プライマリ VLAN 内のセカンダリ VLAN には割り当てられません。さまざまなセカンダリ VLAN のカスタマー デバイスには後続 IP アドレスが割り当てられます。新しいデバイスを追加すると、サブネ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

複数にまたがるプライベート VLAN Devices

図 *5:* 複数のスイッチにまたがるプライベート *VLAN*

通常の VLAN と同じように、プライベート VLAN は複数の devices に広げることができます。トランク ポートはプライマリ VLANおよびセカンダリ VLANをネイバーdevice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devicesに及ぶプ

ライベート VLAN には、デバイス A の独立ポートからのトラフィックが、デバイス B の独立ポートに達しないという特徴があります



VLAN 100 = Primary VLAN
VLAN 201 = Secondary isolated VLAN
VLAN 202 = Secondary community 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 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 クライアントがある場合、サーバ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。

プライベート VLAN の他機能との相互作用

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

通常の VLAN 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 のメンバーはレイヤ 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

レイヤ 3 device では、device 仮想インターフェイス（SVI）が 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 デバイス スタック

プライベート VLAN は device スタック内で動作することができ、プライベート VLAN ポートはさまざまなスタックメンバ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スタック メンバー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 無差別ポートが 1 つだけあるスタック マスターに障害が発生した場合、またはスタックを残し、新しいスタック マスターが選択された場合、古いスタック マスター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、device を再起動したときに、権利を獲得しなかった device 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deviceでは、ユーザは関連 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device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 [英語]

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device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。スイッチオーバーの前に、マスターにあるプライベート VLAN は、スイッチオーバー後と同じである必要があります（新しいマスターはIOS側および、FED側両方で以前のマスターと同様のPVLAN設定が必要です）。

プライベート VLAN 設定時の注意事項

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。device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device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、deviceをリセットした場合、デフォルトの VTP サーバモードになり、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

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 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**transparent**に設定します。

（注） 注：VTP3 の場合、サーバ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 （97 ページ）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（101 ページ）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（102 ページ）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（104 ページ）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： `デバイス> 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： `デバイス# 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： `デバイス(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。

	コマンドまたはアクション	目的
ステップ 4	**vlan** *vlan-id* 例： `デバイス(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： `デバイス(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 6	**exit** 例： `デバイス(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： `デバイス(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： `デバイス(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： `デバイス(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： `デバイス(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：	VLAN をコミュニティ VLAN として指定します。

	コマンドまたはアクション	目的
	デバイス(config-vlan)# **private-vlan community**	
ステップ 12	**exit** 例： デバイス(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 13	**vlan** *vlan-id* 例： デバイス(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： デバイス(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： デバイス(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： デバイス(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： デバイス(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

	コマンドまたはアクション	目的
		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** 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： `デバイス(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： `デバイス# show vlan private-vlan`	設定を確認します。
ステップ 20	**copy running-config startup config** 例： `デバイス# copy running-config startup-config`	device 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： `デバイス> 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： `デバイス# 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： `デバイス(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： `デバイス(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： `デバイス(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。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： デバイス# **show interfaces gigabitethernet1/0/22 switchport**	設定を確認します。
ステップ 8	**copy running-config startup-config** 例： デバイス# **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。

関連トピック

プライベート VLAN ポート （86 ページ）
例：ホスト ポートとしてのインターフェイスの設定 （107 ページ）
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 （108 ページ）

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： デバイス> **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： `デバイス# 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： `デバイス(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： `デバイス(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。
ステップ 5	**switchport private-vlan mapping** *primary_vlan_id* {**add** | **remove**} *secondary_vlan_list* 例： `デバイス(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。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： デバイス# **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： デバイス# **copy running-config startup-config**	device 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。

関連トピック

プライベート VLAN ポート （86 ページ）
例：ホスト ポートとしてのインターフェイスの設定 （107 ページ）
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 （108 ページ）

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：	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
	デバイス> **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： デバイス# **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： デバイス(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： デバイス(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。 • **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。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interface private-vlan mapping** 例： `デバイス# show interfaces private-vlan mapping`	設定を確認します。
ステップ 7	**copy running-config startup config** 例： `デバイス# copy running-config startup-config`	device 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。

関連トピック

VTP ドメイン （3 ページ）
セカンダリ VLAN （86 ページ）
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 （109 ページ）

プライベート VLAN のモニタ

次の表に、プライベート VLAN をモニタ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、インターフェイスのステータスを表示します。
show vlan private-vlan [type]	デバイス または デバイス スタックのプライベート VLAN 情報を表示します。
show interface switchport	インターフェイス上のプライベート VLAN 設定を表示します。
show interface private-vlan mapping	VLAN SVI のプライベート VLAN マッピングに関する情報を表示します。

プライベート VLAN の設定例

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。

```
デバイス# configure terminal
デバイス(config)# vlan 20
デバイス(config-vlan)# private-vlan primary
デバイス(config-vlan)# exit
デバイス(config)# vlan 501
デバイス(config-vlan)# private-vlan isolated
デバイス(config-vlan)# exit
デバイス(config)# vlan 502
デバイス(config-vlan)# private-vlan community
デバイス(config-vlan)# exit
デバイス(config)# vlan 503
デバイス(config-vlan)# private-vlan community
デバイス(config-vlan)# exit
デバイス(config)# vlan 20
デバイス(config-vlan)# private-vlan association 501-503
デバイス(config-vlan)# end
デバイス# 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。

```
デバイス# configure terminal
デバイス(config)# interface gigabitethernet1/0/22
デバイス(config-if)# switchport mode private-vlan host
デバイス(config-if)# switchport private-vlan host-association 20 501
デバイス(config-if)# end
デバイス# 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>
```

関連トピック

プライベート VLAN ポート （86 ページ）
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 （101 ページ）
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 （102 ページ）

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。

```
デバイス# configure terminal
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# switchport mode private-vlan promiscous
デバイス(config-if)# switchport private-vlan mapping 20 add 501-503
デバイス(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。

関連トピック

プライベート VLAN ポート （86 ページ）
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 （101 ページ）
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 （102 ページ）

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。

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

関連トピック

VTP ドメイン （3 ページ）
セカンダリ VLAN （86 ページ）
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（104 ページ）

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。

```
デバイス# 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
- 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
CLI コマンド	LAN Switching コマンド リファレンス, Cisco IOS リリース

標準および RFC

標準/RFC	タイトル
RFC 1573	
RFC 1757	
RFC 2021	

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、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support