Cisco IOS XE Everest 16.6.x（Catalyst 9300 スイッチ）VLAN コンフィギュレーション ガイド

初版：2017 年 07 月 31 日

最終更新：2017 年 11 月 03 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

VTP の設定 1

機能情報の確認 1

VTP の前提条件 2

VTP の制約事項 2

VTP の概要 3

[VTP] 3

VTP ドメイン 3

VTP モード 4

VTP アドバタイズ 5

VTP バージョン 2 6

VTP バージョン 3 7

VTP プルーニング 8

VTP とデバイス スタック 10

VTP 設定時の注意事項 10

VTP の設定要件 10

VTP の設定 11

VTP 設定のためのドメイン名 11

VTP ドメインのパスワード 12

VTP バージョン（VTP Version） 12

VTP の設定方法 14

VTP モードの設定（CLI） 14

VTP バージョン 3 のパスワードの設定（CLI） 16

VTP バージョン 3 のプライマリ サーバの設定（CLI） 17

VTP バージョンのイネーブル化（CLI） 18

VTP プルーニングのイネーブル化（CLI） 20

ポート単位の VTP の設定（CLI） 21

VTP ドメインへの VTP クライアント の追加（CLI） 22

VTP のモニタ 25
VTP の設定例 25
例：スイッチをプライマリ サーバとして設定する 25
次の作業 26
その他の参考資料 26
VTP の機能履歴と情報 28
VLAN の設定 29
機能情報の確認 29
VLAN の前提条件 29
VLAN の制約事項 30
VLAN について 30
[論理ネットワーク（Logical Networks）] 30
サポートされる VLAN 31
VLAN ポート メンバーシップ モード 31
VLAN コンフィギュレーション ファイル 33
標準範囲 VLAN 設定時の注意事項 33
拡張範囲 VLAN 設定時の注意事項 34
VLAN の設定方法 35
標準範囲 VLAN の設定方法 35
イーサネット VLAN の作成または変更（CLI） 36
VLAN の削除（CLI） 39
VLAN へのスタティック アクセス ポートの割り当て（CLI） 40
拡張範囲 VLAN の設定方法 42
拡張範囲 VLAN の作成（CLI） 42
VLAN のモニタリング 44
次の作業 45
その他の参考資料 45
VLAN の機能履歴と情報 47
VLAN トランクの設定 49
機能情報の確認 49
VLAN トランクの前提条件 49
VLAN トランクの制約事項 50

VLAN トランクについて 51
トランキングの概要 51
トランキング モード 51
レイヤ 2 インターフェイス モード 52
トランクでの許可 VLAN 53
トランク ポートでの負荷分散 53
STP プライオリティによるネットワーク負荷分散 54
STP パス コストによるネットワーク負荷分散 54
機能の相互作用 54
VLAN トランクの設定方法 55
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 55
トランク ポートの設定（CLI） 55
トランクでの許可 VLAN の定義（CLI） 58
プルーニング適格リストの変更（CLI） 59
タグなしトラフィック用ネイティブ VLAN の設定（CLI） 61
トランク ポートの負荷分散の設定 62
STP ポート プライオリティによる負荷分散の設定（CLI） 62
STP パス コストによる負荷分散の設定（CLI） 66
次の作業 68
その他の参考資料 69
VLAN トランクの機能履歴と情報 70
音声 VLAN の設定 71
機能情報の確認 71
音声 VLAN の前提条件 71
音声 VLAN の制約事項 72
音声 VLAN に関する情報 72
音声 VLAN 72
Cisco IP Phone の音声トラフィック 72
Cisco IP Phone のデータ トラフィック 73
音声 VLAN 設定時の注意事項 74
音声 VLAN の設定方法 75
Cisco IP Phone の音声トラフィックの設定（CLI） 75

着信データ フレームのプライオリティ設定（CLI） 77
音声 VLAN のモニタリング 79
次の作業 79
その他の参考資料 80
音声 VLAN の機能履歴と情報 81
プライベート VLAN の設定 83
機能情報の確認 83
プライベート VLAN の前提条件 83
プライベート VLAN の制約事項 84
プライベート VLAN について 85
プライベート VLAN ドメイン 85
セカンダリ VLAN 86
プライベート VLAN ポート 86
ネットワーク内のプライベート VLAN 88
プライベート VLAN での IP アドレッシング方式 88
複数のデバイスにまたがるプライベート VLAN 89
プライベート VLAN の他機能との相互作用 89
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 89
プライベート VLAN と SVI 90
プライベート VLAN とデバイススタック 91
ダイナミック MAC アドレスを備えたプライベート VLAN 91
スタティック MAC アドレスを備えたプライベート VLAN 91
プライベート VLAN と VACL/QOS との相互作用 92
プライベート VLAN および HA サポート 93
プライベート VLAN 設定時の注意事項 93
プライベート VLAN のデフォルト設定 93
セカンダリ VLAN およびプライマリ VLAN の設定 93
プライベート VLAN ポートの設定 96
プライベート VLAN の設定方法 96
プライベート VLAN の設定 96
プライベート VLAN 内の VLAN の設定および対応付け 97

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
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
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
プライベート VLAN のモニタ 106
プライベート VLAN の設定例 107
例：プライベート VLAN 内の VLAN の設定および関連付け 107
例：ホスト ポートとしてのインターフェイスの設定 107
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
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
例：プライベート VLAN のモニタリング 109
次の作業 109
その他の参考資料 110
通告 113
Trademarks 113

第 1 章

VTP の設定

- 機能情報の確認，1 ページ
- VTP の前提条件，2 ページ
- VTP の制約事項，2 ページ
- VTP の概要，3 ページ
- VTP の設定方法，14 ページ
- VTP のモニタ，25 ページ
- VTP の設定例，25 ページ
- 次の作業，26 ページ
- その他の参考資料，26 ページ
- VTP の機能履歴と情報，28 ページ

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 Cisco 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 つまたは複数のデバイス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デバイスに伝達できます。VTP を使用しない場合、VLAN 情報を他のデバイスに送信することはできません。

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

デバイスは合計 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、デバイス ハードウェアの使用状況は左右されます。VTP が新しい VLAN をデバイスに通知し、デバイス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** ユーザ EXEC コマンドの出力に、サスペンド ステートの VLAN が示されます。

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

関連トピック

VTP アドバタイズ, （5 ページ）
VTP ドメインへの VTP クライアント の追加（CLI）, （22 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

注意 VTP クライアント デバイスを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のデバイスのコンフィギュレーション リビジョン番号より小さいことを確認してください。VTP ドメイン内のデバイスは常に、VTP コンフィギュレーション リビジョン番号が最大のデバイスの VLAN コンフィギュレーションを使用します。VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つデバイスを追加すると、VTP サーバおよび 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デバイスが、アクティブ デバイスから継承した同一のVLANおよびVTPコンフィギュレーションを保持します。デバイスが VTP メッセージを通じて新しい VLAN について学習したり、ユーザが新しい VLAN を設定したりすると、新しい VLAN 情報がスタック内のすべてのデバイスに伝達されます。

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

VTP ドメイン

VTP ドメイン（別名 VLAN 管理ドメイン）は、1 つのデバイス、または同じ VTP ドメイン名を共有して同一管理下にある相互接続された複数のデバイスまたはデバイススタックで構成されます。デバイスは、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、デバイスは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。

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

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

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

関連トピック

VTP ドメインへの VTP クライアント の追加（CLI），（22 ページ）

VTP の前提条件，（2 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（VTP Mode）	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 ドメイン内の他のデバイスに自身の 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 設定を他のデバイスと同期させます。 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。デバイス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、デバイスを VTP サーバモードに戻すことはできません。
VTP クライアント	VTP クライアントは VTP サーバと同様に機能し、そのトランクで VTP アップデー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 モードのデバイスで設定します。 VTP バージョン 1 および 2 の VTP クライアント モードでは、VLAN 設定は NVRAM 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（VTP Mode）	説明
VTP トランスペアレント	VTP トランスペアレント デバイスは、VTP に参加しません。VTP トランスペアレントデバイスは自身の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デバイスは、トランク インターフェイスを介して他のデバイスから受信したVTPアドバタイズを転送します。VTP トランスペアレント モードでは、デバイス上の VLAN を作成、変更、削除できます。 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、デバイスは 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。 デバイスが VTP トランスペアレント モードの場合、VTP および VLAN の設定はNVRAMに保存されますが、他のデバイスにはアドバタイズされません。このモードでは、VTP モードおよびドメイン名はデバイスの実行コンフィギュレーションに保存されます。この情報をデバイスのスタートアップ 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 コマンドを使用します。 デバイス スタックでは、実行コンフィギュレーションと保存されているコンフィギュレーションは、スタック内のすべてのデバイスについて同じです。
VTP オフ	VTP オフ モードでのデバイスの機能は、トランクを介して VTP アドバタイズを転送しないことを除くと VTP トランスペアレント デバイスとしての機能と同じです。

関連トピック

VTP の前提条件, （2 ページ）
VTP モードの設定（CLI）, （14 ページ）

VTP アドバタイズ

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

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

VTP アドバタイズにより、次のグローバル ドメイン情報が配信されます。

- VTP ドメイン名
- VTP 設定のリビジョン番号
- アップデート ID およびアップデート タイムスタンプ
- 各 VLAN の最大伝送単位（MTU）サイズを含む MD5 ダイジェスト VLAN コンフィギュレーション
- フレーム形式

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

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

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

関連トピック

VTP の前提条件, （2 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、デバイスが 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 デバイスが VTP メッセージ中のドメイン名およびバージョンを調べ、バージョンおよびドメイン名が一致する場合に限りメッセージを転送します。VTP バージョン 2 がサポートするドメインは 1 つだけですが、VTP バージョン 2 トランスペアレント デバイスは、ドメイン名が一致した場合のみメッセージを転送します。
- 整合性検査：VTP バージョン 2 では、CLI または SNMP を介して新しい情報が入力された場合に限り、VLAN 整合性検査（VLAN 名、値など）を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージの MD5 ダイジェストが有効であれば、情報を受け入れます。

関連トピック

VTP バージョンのイネーブル化（CLI），（18 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** にしている場合、パスワード文字列からの秘密キーは 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ときは、パスワードを再入力する必要があります。キーワード **secret** を入力する場合、パスワードに秘密キー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、デバイスにパスワードが設定されている場合でも、装置がリロードしたり、ドメインのパラメータが変更したりすると失われます。

- VTP をトランク単位（ポート単位）でオンまたオフにするオプション：ポート単位で VTP をイネーブルまたはディセーブルにするには、[**no**] **vtp** インターフェイス コンフィギュレーション コマンドを入力します。トランク ポート上でVTPをディセーブルにすると、そのポートのすべてのVTPインスタンスがディセーブルになります。VTPの設定を、MSTデータベースには *off* にする一方で、同じポートの VLAN データベースには *on* にすることはできません。

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

関連トピック

VTP バージョンのイネーブル化（CLI），（18 ページ）

VTP プルーニング

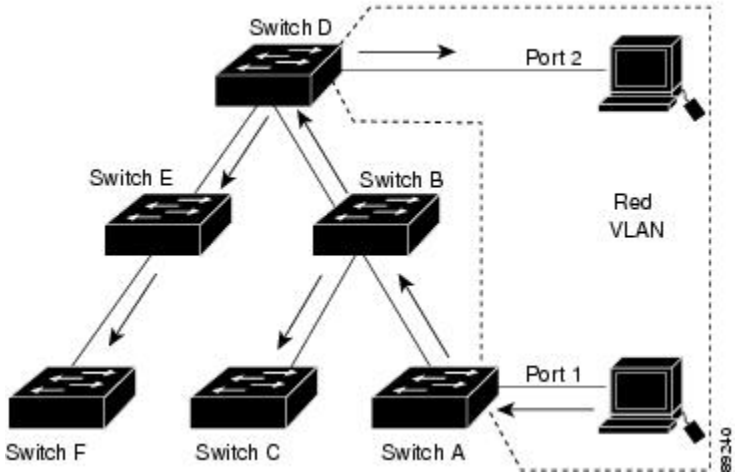
VTP プルーニングを使用すると、トラフィックが宛先デバイスに到達するために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されるので、使用可能なネットワーク帯域幅が増えます。VTP プルーニングを使用しない場合、デバイスは受信側のデバイスで廃棄される可能性があっても、VTP ドメイン内のすべてのトランク リンクに、ブロードキャスト、マルチキャスト、および不明のユニキャスト トラフィックをフラッディングします。VTP プルーニングはデフォルトでディセーブルです。

VTPプルーニングは、プルーニング適格リストに指定されたVLANトランク ポートへの不要なフラッディング トラフィックを阻止します。プルーニング適格リストに指定されたVLANだけが、プルーニングの対象になります。デフォルトでは、デバイスのトランク 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。

VTPプルーニングは、スイッチドネットワークでは無効です。デバイス A のポート 1 およびデバイス D のポート 2 は、Red という VLAN に割り当てられています。デバイス A に接続されたホストからブロードキャストが送信された場合、デバイス A は、このブロードキャストをフラッディ

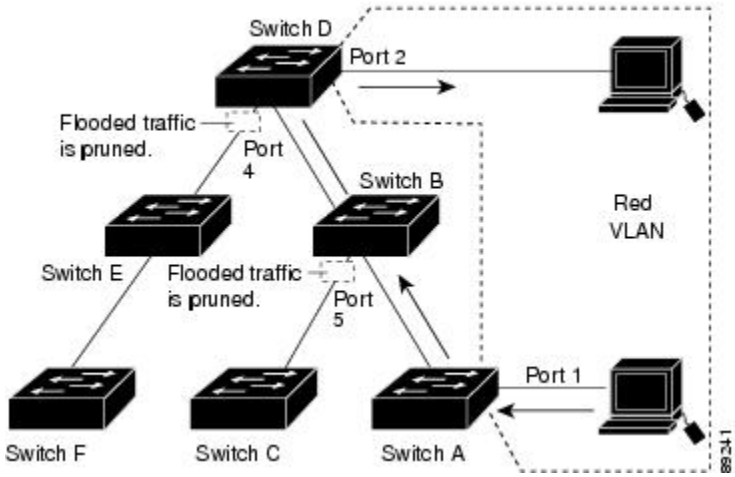
ングします。Red VLAN にポートを持たないデバイス C、E、F も含めて、ネットワーク内のすべてのデバイスがこのブロードキャストを受信します。

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

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 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、ドメイン内の各デバイス上で手動によってプルーニングを有効にする必要があります。VLAN をプルーニング適格または不適格として設定する場合、影響を受けるのは、そのトランク上の VLAN のプルーニングだけです（VTP ドメイン内のすべてのデバイスに影響するわけではありません）。

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

関連トピック

VTP プルーニングのイネーブル化（CLI），（20 ページ）

VTP とデバイス スタック

VTP 設定は、デバイス スタックのすべてのメンバで同一です。デバイス スタックが VTP サーバ、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デバイスの VTP 設定が同一になります。

- スタックに参加したデバイスは、VTP および VLAN のプロパティをアクティブ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。
- スタック内のデバイスの VTP モードが変更されると、そのスタック内のその他のデバイスも VTP モードを変更し、デバイスの VLAN データベースの一貫性が保たれます。

VTP バージョン 3 は、スタンドアロン デバイスでもスタックでも同じように機能しますが、デバイス 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。アクティブなデバイス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デバイスが選択されると、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、デバイスがドメイン内の他のデバイスと VTP アドバタイズを送受信できるように、トランク ポートを設定する必要があります。

VTP バージョン 1 および 2 ではプライベート VLAN をサポートしません。VTP バージョン 3 ではプライベート VLAN をサポートします。プライベート VLAN を設定した場合、デバイスは VTP トランスペアレント モードでなければなりません。プライベート VLAN がデバイスに設定されて

いる場合、VTP モードをトランスペアレント モードからクライアント モードやサーバ 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 モードがトランスペアレントである場合、VTP ドメイン名およびモードはデバイスの実行コンフィギュレーション ファイルにも保存されます。この情報をデバイスのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを入力します。デバイスをリセットした場合にも、VTP モードをトランスペアレントとして保存するには、このコマンドを使用する必要があります。

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

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

関連トピック

ポート単位の VTP の設定（CLI），（21 ページ）
VTP バージョン 3 のプライマリ サーバの設定（CLI），（17 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デバイスを、同じドメイン名で設定しなければなりません。VTP トランスペアレント モードのデバイスは、他のデバイスと VTP メッセージを交換しません。これらのコントローラについては VTP ドメイン名を設定する必要はありません。

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

注意 すべてのデバイスが VTP クライアント モードで動作している場合は、VTP ドメインを設定しないでください。ドメインを設定すると、そのドメインの VLAN 設定を変更できなくなります。VTP ドメイン内の少なくとも 1 台のデバイスを VTP サーバ 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（CLI），（22 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 デバイスで同じパスワードを共有し、管理ドメイン内のデバイスごとにパスワードを設定する必要があります。パスワードのないデバイス、またはパスワードが不正なコントローラは、VTP アドバタイズを拒否します。

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

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

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

関連トピック

VTP バージョン 3 のパスワードの設定（CLI），（16 ページ）

例：スイッチをプライマリ サーバとして設定する，（25 ページ）

VTP バージョン（VTP Version）

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

- VTP ドメイン内のすべてのデバイスは同じドメイン名を使用する必要がありますが、すべてが同じ VTP バージョンを実行する必要はありません。
- VTP バージョン 2 対応のデバイス上で VTP バージョン 2 がディセーブルに設定されている場合、VTP バージョン 2 対応デバイスは、VTP バージョン 1 を実行しているデバイスと同じ VTP ドメインで動作できます（デフォルトでは VTP バージョン 2 はディセーブルになっています）。
- VTP バージョン 1 を実行しているものの、VTP バージョン 2 に対応可能なデバイスが VTP バージョン 3 アドバタイズを受信すると、このコントローラは VTP バージョン 2 に自動的に移行します。
- VTP バージョン 3 を実行しているデバイスが VTP バージョン 1 を実行しているデバイスに接続すると、VTP バージョン 1 のデバイスは VTP バージョン 2 に移行し、VTP バージョン 3 のデバイスは、スケールダウンしたバージョンの VTP パケットを送信するため、VTP バージョン 2 デバイスは自身のデータベースをアップデートできます。

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

関連トピック

VTP バージョンのイネーブル化（CLI），（18 ページ）

VTP の設定方法

VTP モードの設定（CLI）

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 デバイスは、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、デバイスで VTP がディセーブルになります。デバイスは VTP アップデートを送信せず、他のデバイスから受信した VTP アップデートにも反応しません。ただし、VTP バージョン 2 を実行する VTP トランスペアレント モードのデバイスは、対応するトランク リンクで、受信した VTP アドバタイズを転送します。
- VTP オフ モード：VTP オフ モードは、VTP アドバタイズが転送されない以外は、VTP トランスペアレント モードと同じです。

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp domain** *domain-name* 例： `Device(config)# vtp domain eng_group`	VTP 管理ドメイン名を設定します。1 ～ 32 文字の名前を使用できます。同一管理下にある VTP サーバ モードまたはクライアント モードのデバイスは、すべて同じドメイン名に設定する必要があります。

	コマンドまたはアクション	目的
		サーバ モード以外にはこのコマンドは任意です。VTP サーバ モードではドメイン名が必要です。デバイスが VTP ドメインにトランク接続されている場合、デバイスはドメイン内の VTP サーバ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。 （注）
ステップ 4	**vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**} 例： `Device(config)# vtp mode server`	VTP モード（クライアント、サーバ、トランスペアレント、またはオフ）のデバイスの設定。 • **vlan**：何も設定されていない場合は VLAN データベースがデフォルトです。 • **mst**：マルチスパニング ツリー（MST）データベース。 • **unknown**：データベース タイプは不明です。
ステップ 5	**vtp password** *password* 例： `Device(config)# vtp password mypassword`	（任意）VTP ドメイン用のパスワードを設定します。パスワードに使用できる文字数は 8 ～ 64 文字です。VTP パスワードを設定したにもかかわらず、ドメイン内の各デバイスに同じパスワードを割り当てなかった場合には、VTP ドメインが正常に動作しません。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show vtp status** 例： `Device# show vtp status`	表示された *[VTP Operating Mode]* および *[VTP Domain Name]* フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）スタートアップ コンフィギュレーション ファイルに設定を保存します。 デバイスの実行コンフィギュレーションに保存され、スタートアップ コンフィギュレーション ファイルにコピーできるのは、VTP モードおよびドメイン名だけです。

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（CLI）

デバイスで VTP バージョン 3 のパスワードを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp version 3** 例： `Device(config)# vtp version 3`	デバイスで VTP バージョン 3 を有効にします。デフォルトは VTP バージョン 1 です。
ステップ 4	**vtp password** *password* [**hidden** | **secret**] 例： `Device(config)# vtp password mypassword 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。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show vtp password** 例： `Device# show vtp password`	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： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VTP ドメインのパスワード, （12 ページ）
例：スイッチをプライマリ サーバとして設定する, （25 ページ）

VTP バージョン 3 のプライマリ サーバの設定（CLI）

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

手順

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

	コマンドまたはアクション	目的
ステップ 2	**vtp primary** [**vlan** | **mst**] [**force**] 例： `Device# vtp primary vlan force`	デバイスの動作ステートをセカンダリ サーバ（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。デバイスのパスワードが **hidden** に設定されている場合は、パスワードの再入力を要求されます。 • （任意）**vlan**：テイクオーバー機能として VLAN データベースを選択します。これがデフォルトです。 • （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, （11 ページ）

VTP バージョンのイネーブル化（CLI）

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

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

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

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

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

- ⚠

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

手順

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

関連トピック

VTP バージョン（VTP Version），（12 ページ）
VTP バージョン 2，（6 ページ）
VTP バージョン 3，（7 ページ）

VTP プルーニングのイネーブル化（CLI）

はじめる前に

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

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp pruning** 例： `Device(config)# vtp pruning`	VTP 管理ドメインでプルーニングをイネーブルにします。 プルーニングは、デフォルトではディセーブルに設定されています。VTP サーバ モードの 1 台の

	コマンドまたはアクション	目的
		デバイス上に限ってプルーニングをイネーブルにする必要があります。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status** 例： `Device# show vtp status`	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，（8 ページ）

ポート単位の VTP の設定（CLI）

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**vtp** 例： `Device(config-if)# vtp`	指定したポートの VTP をイネーブルにします。
ステップ 5	**end** 例： `Device(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： `Device# show running-config interface gigabitethernet1/0/1`	ポートの変更を確認します。
ステップ 7	**show vtp status** 例： `Device# show vtp status`	設定を確認します。

関連トピック

VTP の設定, （11 ページ）

VTP ドメインへの VTP クライアント の追加（CLI）

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

はじめる前に

VTP クライアントを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のデバイスのコンフィギュレーション リビジョン番号より小さいこ

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show vtp status** 例： `Device# show vtp status`	VTP コンフィギュレーション リビジョン番号をチェックします。 番号が 0 の場合は、デバイスを VTP ドメインに追加します。 番号が 0 より大きい場合は、次の手順に従います。 • ドメイン名を書き留めます。 • コンフィギュレーション リビジョン番号を書き留めます。 • 次のステップに進んで、デバイスのコンフィギュレーション リビジョン番号をリセットします。
ステップ 3	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**vtp domain** *domain-name* 例： `Device(config)# vtp domain domain123`	ドメイン名を、ステップ 1 で表示された元の名前から新しい名前に変更します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。デバイスの VLAN 情報が更新され、コンフィギュレーション リビジョン番号が 0 にリセットされます。
ステップ 6	**show vtp status** 例： `Device# show vtp status`	コンフィギュレーション リビジョン番号が 0 にリセットされていることを確認します。
ステップ 7	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 8	**vtp domain** *domain-name* 例： `Device(config)# vtp domain domain012`	デバイスの元のドメイン名を開始します。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。デバイスの VLAN 情報が更新されます。
ステップ 10	**show vtp status** 例： `Device# show vtp status`	（任意）ドメイン名がステップ 1 のものと同じであり、コンフィギュレーション リビジョン番号が 0 であることを確認します。

関連トピック

VTP ドメイン，（3 ページ）
VTP の前提条件，（2 ページ）
VTP 設定のためのドメイン名，（11 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。デバイスで送受信されたアドバタイズに関する統計情報を表示することもできます。

表 *2*：*VTP* モニタ コマンド

コマンド（**Command**）	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、デバイス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、暗号化がデバイス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 デバイス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）としてデバイスを設定する方法の例を示します。

```
Device# vtp primary vlan
Enter VTP password: mypassword
```

```
This switch is becoming Primary server for vlan feature in the VTP  domain

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

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

関連トピック

VTP バージョン 3 のパスワードの設定（CLI）, （16 ページ）
VTP ドメインのパスワード, （12 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	参照先
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9300 Series Switches)*
追加の設定コマンドおよび手順。	*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	役職（Title）
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 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

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、Product Alert Tool（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	変更箇所
Cisco IOS XE Everest 16.5.1a	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，29 ページ
- VLAN の前提条件，29 ページ
- VLAN の制約事項，30 ページ
- VLAN について，30 ページ
- VLAN の設定方法，35 ページ
- VLAN のモニタリング，44 ページ
- 次の作業，45 ページ
- その他の参考資料，45 ページ
- VLAN の機能履歴と情報，47 ページ

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 Cisco 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。

- VLAN を作成する前に、VLAN トランキング プロトコル（VTP）を使用してネットワークのグローバルな VLAN 設定を維持するかどうかを決定する必要があります。
- デバイスで多数の VLAN を設定し、ルーティングを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。
- VLAN グループに VLAN を追加できるようにするため、VLAN がデバイスに存在している必要があります。

VLAN の制約事項

次に、VLAN の制約事項を示します。

- デバイスは、最大 128 のスパニングツリー インスタンスを持つ Per-VLAN Spanning-Tree Plus（PVST+）または Rapid PVST+ をサポートします。VLAN ごとに 1 つずつスパニングツリー インスタンスを使用できます。
- デバイスは、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。

VLAN について

[論理ネットワーク（Logical Networks）]

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

VLAN は通常、IP サブネットワークに対応付けられます。たとえば、特定の IP サブネットに含まれるエンドステーションはすべて同じ VLAN に属します。デバイス上のインターフェイスの VLAN メンバーシップは、インターフェイスごとに手動で割り当てます。この方法でデバイス インター

フェイスを VLAN に割り当てた場合、これをインターフェイス ベース（またはスタティック）VLAN メンバーシップと呼びます。

VLAN 間のトラフィックは、ルーティングする必要があります。

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

サポートされる VLAN

デバイスは、VTP クライアント、サーバ、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 デバイス 伝播拡張範囲 VLAN 設定情報を実行します。拡張範囲 VLAN が VTP バージョン 1 および 2 で作成された場合、設定情報は伝播されません。デバイス上のローカル VTP データベース エントリも更新されませんが、拡張範囲VLAN設定情報が作成され、実行コンフィギュレーション ファイルに保存されます。

最大 4094 の VLAN をデバイスに設定できます。

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、デバイスはVLAN単位で、ポートに対応するアドレスを学習して管理します。

表 *3*：ポートのメンバーシップ モードとその特性

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
スタティック アクセス	スタティック アクセス ポートは、手動で割り当てられ、1 つの VLAN だけに所属します。	VTP は必須ではありません。VTP にグローバルに情報を伝播させないようにする場合は、VTP モードをトランスペアレント モードに設定します。VTP に加入するには、別のデバイスまたはデバイス スタックのトランク ポートに接続されているデバイスまたはデバイス スタック上に少なくとも 1 つのトランク ポートが必要です。
トランク（IEEE 802.1Q） • IEEE 802.1Q：業界標準のトランキング カプセル化方式です。	デフォルトで、トランク ポートは拡張範囲 VLAN を含むすべての VLAN のメンバです。ただし、メンバーシップは許可 VLAN リストを設定して制限できます。また、プルーニング適格リストを変更して、リストに指定したトランク ポート上の VLAN へのフラッディング トラフィックを阻止することもできます。	VTP を推奨しますが、必須ではありません。VTP は、ネットワーク全体にわたって VLAN の追加、削除、名前変更を管理することにより、VLAN 設定の整合性を維持します。VTP はトランク リンクを通じて他のデバイスと VLAN コンフィギュレーション メッセージを交換します。
ボイス 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（CLI），（40 ページ）
VLAN のモニタリング，（44 ページ）

VLAN へのスタティック アクセス ポートの割り当て（CLI），（40 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（VLAN データベース）ファイルに書き込まれます。この設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。vlan.dat ファイルはフラッシュ メモリに格納されます。VTP モードがトランスペアレント モードの場合、それらの設定もデバイスの実行コンフィギュレーション ファイルに保存されます。

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

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

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

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントで、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。
- VTP バージョン 1 および 2 では、VTP モードがサーバである場合、VLAN ID 1 ～ 1005 のドメイン名と VLAN 設定で VLAN データベース情報が使用されます。VTP バージョン 3 は、VLAN 1006 ～ 4094 もサポートします。

標準範囲 VLAN 設定時の注意事項

標準範囲 VLAN は、ID が 1 ～ 1005 の VLAN です。

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

- 標準範囲 VLAN は、1 ～ 1001 の番号で識別します。VLAN 番号 1002 ～ 1005 は、トークンリングおよび FDDI VLAN 専用です。
- VLAN 1 ～ 1005 の VLAN 設定は、常に VLAN データベースに格納されます。VTP モードがトランスペアレント モードの場合、VTP と VLAN の設定もデバイスの実行コンフィギュレーション ファイルに保存されます。

- デバイスが VTP サーバ モードまたは VTP トランスペアレント モードにある場合は、VLAN データベース内の VLAN 2 ～ 1001 について設定を追加、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、デバイスを 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。デバイスが 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。
- デバイスは、トークンリングまたはFDDIメディアをサポートしません。デバイスはFDDI、FDDI-Net、TrCRF、またはTrBRFトラフィックを転送するのではなく、VTPを介してVLAN設定を伝播します。
- デバイス は 128 スパニングツリー インスタンスをサポートします。デバイスのアクティブな VLAN 数が、サポートされているスパニングツリー インスタンス数よりも多い場合、スパニングツリーは 128 の VLAN で有効にできます。残りの VLAN で、スパニングツリーは無効になります。デバイス上の使用可能なスパニングツリーインスタンスをすべて使い切ってしまった後に、VTP ドメインの中にさらに別のVLANを追加すると、そのデバイス上にスパニングツリーが稼働しない VLAN が生成されます。そのデバイスのトランク ポート上でデフォルトの許可リスト（すべてのVLANを許可するリスト）が設定されていると、すべてのトランク ポート上に新しい VLAN が割り当てられます。ネットワーク トポロジによっては、新しいVLAN上で、切断されないループが生成されることがあります。特に、複数の隣接デバイスでスパニングツリーインスタンスをすべて使用してしまっている場合には注意が必要です。スパニングツリー インスタンスの割り当てを使い果たしたデバイスのトランク ポートに許可リストを設定することにより、このような可能性を防ぐことができます。

  デバイス上の VLAN の数がサポートされているスパニングツリー インスタンスの最大数を超える場合、デバイス上に IEEE 802.1s Multiple STP（MSTP）を設定して、複数の VLAN を単一のスパニングツリー インスタンスにマッピングすることを推奨します。
- スタック内のデバイスが新しい 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。
- デバイス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は、新しいデバイス上の VTP 情報（vlan.dat ファイル）とアクティブなデバイス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（CLI），（36 ページ）
VLAN のモニタリング，（44 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、デバイスが VTP バージョン 3 を実行していない場合は VLAN データベースに保存されず、VTP で認識されません。
- プルーニング適格範囲に拡張範囲 VLAN を含めることはできません。
- VTP バージョン 1 または 2 では、グローバル コンフィギュレーション モードで、VTP モードをトランスペアレントに設定できます。VTP トランスペアレント モードでデバイスが始動するように、この設定をスタートアップ コンフィギュレーションに保存する必要があります。このようにしないと、デバイスをリセットした場合に、拡張範囲VLAN設定が失われます。VTP バージョン 3 で拡張範囲 VLAN を作成する場合は、VTP バージョン 1 または 2 に変更できません。
- デバイススタックでは、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（CLI），（42 ページ）
VLAN のモニタリング，（44 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（Admin. VLAN ID）
- VLAN 名
- VLAN タイプ
  - Ethernet
  - 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）

- VLAN の最大伝送単位（MTU）
- 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（CLI）

はじめる前に

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

デバイスは、イーサネット インターフェイスだけをサポートしています。FDDI およびトークンリング VLAN は、ローカルではサポートされないので、FDDI およびトークンリング メディア固有の特性は、他のデバイスに対する VTP グローバル アドバタイズにのみ設定します。

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

- トークンリング TrBRF VLAN
- トークンリング TrCRF VLAN

手順

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

	コマンドまたはアクション	目的
ステップ 2	**vlan** *vlan-id* 例： `Device(config)# vlan 20`	VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。新規の VLAN ID を入力して VLAN を作成するか、または既存の VLAN ID を入力してその VLAN を変更します。 （注） このコマンドで指定できる VLAN ID 範囲は 1 ～ 4094 です。
ステップ 3	**name** *vlan-name* 例： `Device(config-vlan)# name test20`	（任意）VLAN の名前を入力します。VLAN 名を指定しなかった場合には、デフォルトとして、VLAN という語の後ろに先行ゼロを含めた *vlan-id* 値が付加されます。たとえば、VLAN 4 のデフォルトの VLAN 名は VLAN0004 になります。 次の追加 VLAN コンフィギュレーション コマンド オプションが使用可能です。 • **are**：この VLAN の All-Route Explorer（ARE）ホップの最大数を設定します。 • **backupcrf**：VLAN のバックアップ コンセントレータ リレー機能（CRF）モードをイネーブルまたはディセーブルにします。 • **bridge**：FDDI-Net またはトークン リング ネット タイプの VLAN にブリッジ番号の値を設定します。 • **exit**：変更を適用し、リビジョン番号を増分して、終了します。 • **media**：VLAN のメディア タイプを設定します。 • **no**：コマンドまたはデフォルトを拒否します。 • **parent**：FDDI の親 VLAN やトークン リング タイプの VLAN に ID の値を設定します。 • **remote-span**：リモート SPAN VLAN を設定します。 • **ring**：FDDI またはトークン リング タイプの VLAN にリング番号値を設定します。 • **said**：IEEE 802.10 SAID の値を設定します。 • **shutdown**：VLAN スイッチングをシャットダウンします。 • **state**：運用上の VLAN ステートを実行中または停止中に設定します。

	コマンドまたはアクション	目的
		• **ste**：VLANのスパニングツリーエクスプローラ（STE）のホップの最大数を設定します。 • **stp**：VLAN のスパニングツリー特性を設定します。
ステップ 4	**media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** } 例： `Device(config-vlan)# media ethernet`	VLAN のメディア タイプを設定します。コマンド オプションは次のとおりです。 • **ethernet**：VLANのメディア タイプをイーサネットに設定します。 • **fd-net**：VLAN のメディア タイプを FDDI-net に設定します。 • **fddi**：VLANのメディア タイプをFDDIに設定します。 • **tokenring**：VLANメディア タイプをトークン リングに設定します。 • **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： `Device(config-vlan)# remote-span`	
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show vlan** {**name** *vlan-name* | **id** *vlan-id*} 例： `Device# show vlan name test20 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, （33 ページ）

VLAN のモニタリング，（44 ページ）

VLAN の削除（CLI）

VTP サーバ モードのデバイスから VLAN を削除すると、VTP ドメイン内のすべてのデバイスの VLAN データベースから、その VLAN が削除されます。VTP トランスペアレント モードのデバイスから VLAN を削除した場合、その特定のデバイススイッチまたはデバイススタック上に限り 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： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no vlan** *vlan-id* 例： `Device(config)# no vlan 4`	VLAN ID を入力して、VLAN を削除します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show vlan brief** 例： `Device# show vlan brief`	VLAN が削除されたことを確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

VLAN のモニタリング，（44 ページ）

VLAN へのスタティック アクセス ポートの割り当て（CLI）

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。

クラスタ メンバ デバイス上のポートを VLAN に割り当てる場合、最初に **rcommand** 特権 EXEC コマンドを使用して、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： `Device> enable`	特権EXECモードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	VLAN に追加するインターフェイスを入力します。
ステップ 4	**switchport mode access** 例： `Device(config-if)# switchport mode access`	ポート（レイヤ 2 アクセス ポート）の VLAN メンバーシップ モードを定義します。
ステップ 5	**switchport access vlan** *vlan-id* 例： `Device(config-if)# switchport access vlan 2`	VLAN にポートを割り当てます。指定できる VLAN ID の範囲は 1 ～ 4094 です。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config interface** *interface-id* 例： `Device# show running-config interface gigabitethernet2/0/1`	インターフェイスの VLAN メンバーシップ モードを確認します。
ステップ 8	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces gigabitethernet2/0/1 switchport`	表示された *Administrative Mode* および *Access Mode VLAN* フィールドの設定を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（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, （31 ページ）
VLAN のモニタリング, （44 ページ）
VLAN ポート メンバーシップ モード, （31 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 を許可するどの **switchport** コマンドでも許可されます。

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

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

拡張範囲 VLAN の作成（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**vlan** *vlan-id*
	
	例：
	
	`Device(config)# vlan 2000`
	`Device(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。

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

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

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

関連トピック

拡張範囲 VLAN 設定時の注意事項，（34 ページ）
VLAN のモニタリング，（44 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（**Command**）	目的
show interfaces [**vlan** *vlan-id*]	デバイス上に設定されたすべてのインターフェイスまたは特定の VLAN の特性を表示します。
show vlan [**access-map** *name* | **brief** | **dot1q** { **tag native** } | **filter** [**access-map** | **vlan**] | **group** [**group-name** *name*] | **id** *vlan-id* | **ifindex** | **mtu** | **name** *name* | **private-vlan remote-span** | **summary**]	デバイス上のすべての VLAN または特定の VLAN のパラメータを表示します。次のコマンド オプションが使用可能です。 • **access-map**：VLAN アクセスマップを表示します。 • **brief**：VTP VLAN のステータス概要を表示します。 • **dot1q**：dot1q パラメータを表示します。 • **filter**：VLAN フィルタ情報を表示します。 • **group**：VLAN グループをグループ名と使用可能な接続済みの VLAN と一緒に表示します。 • **id**：識別番号別に VTP VLAN ステータスを表示します。 • **ifindex**：SNMP ifIndex を表示します。 • **mtu**：VLAN MTU 情報を表示します。 • **name**：指定された名前の VTP VLAN 情報を表示します。 • **private-vlan**：プライベート VLAN 情報を表示します。 • **remote-span**：リモート SPAN VLAN を表示します。 • **summary**：VLAN 情報の要約を表示します。 （注） デバイス CLI に表示される **private-vlan** コマンド オプションはサポートされません。

関連トピック

イーサネット VLAN の作成または変更（CLI），（36 ページ）
標準範囲 VLAN 設定時の注意事項，（33 ページ）
VLAN の削除（CLI），（39 ページ）
VLAN へのスタティック アクセス ポートの割り当て（CLI），（40 ページ）
VLAN ポート メンバーシップ モード，（31 ページ）
拡張範囲 VLAN の作成（CLI），（42 ページ）
拡張範囲 VLAN 設定時の注意事項，（34 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	参照先
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 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	役職（Title）
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 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

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、Product Alert Tool（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	変更箇所
Cisco IOS XE Everest 16.5.1a	この機能が導入されました。

第 3 章

VLAN トランクの設定

- 機能情報の確認，49 ページ
- VLAN トランクの前提条件，49 ページ
- VLAN トランクの制約事項，50 ページ
- VLAN トランクについて，51 ページ
- VLAN トランクの設定方法，55 ページ
- 次の作業，68 ページ
- その他の参考資料，69 ページ
- VLAN トランクの機能履歴と情報，70 ページ

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 Cisco 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 デバイスのネットワークでは、デバイスはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持しま

す。他社製のデバイスは、すべての VLAN でスパニングツリー インスタンスを 1 つサポートする場合があります。

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

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

VLAN トランクの制約事項

次に、VLAN トランクに関する制約事項を示します。

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

    ポート グループ内の 1 つのポートがトランクでなくなると、すべてのポートがトランクでなくなります。
- Per VLAN Spanning Tree（PVST）モードでは最大 24 までのトランク ポート、マルチ スパニング ツリー（MST）モードでは最大 40 までのトランク ポートを設定することを推奨します。

- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミックに変更しようとしても、ポート モードは変更されません。
- ダイナミック トランキング プロトコル（DTP）はトンネル ポートではサポートされていません。
- デバイスはレイヤ 3 トランクをサポートしません。したがって、サブインターフェイスを設定する、またはレイヤ 3 インターフェイスで **encapsulation** キーワードを使用することはできません。ただし、デバイスは、同等の機能を備えたレイヤ 2 トランクおよびレイヤ 3 VLAN インターフェイスをサポートします。

VLAN トランクについて

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 デバイス 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、デバイスなど）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（CLI），（55 ページ）

レイヤ 2 インターフェイス モード

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（Mode）]	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。

[モード（Mode）]	機能
switchport nonegotiate	インターフェイスが DTP フレームを生成しないようにします。このコマンドは、インターフェイス スイッチポート モードが **access** または **trunk** の場合だけ使用できます。トランク リンクを確立するには、手動でネイバーインターフェイスをトランク インターフェイスとして設定する必要があります。
switchport mode private-vlan	プライベート VLAN モードを設定します。

トランクでの許可 VLAN

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランクですべての VLAN ID（1 ～ 4094）が許可されます。ただし、許可リストから VLAN を削除することにより、それらの VLAN からのトラフィックがトランク上を流れないようにすることができます。

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

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

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

関連トピック

トランクでの許可 VLAN の定義（CLI），（58 ページ）

トランク ポートでの負荷分散

負荷分散により、デバイスに接続しているパラレル トランクの提供する帯域幅が分割されます。STP は通常、ループを防止するために、デバイス間で 1 つのパラレル リンク以外のすべてのリン

クをブロックします。負荷分散を行うと、トラフィックの所属する VLAN に基づいて、リンク間でトラフィックが分散されます。

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

STP プライオリティによるネットワーク負荷分散

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

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（CLI），（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（CLI），（66 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、デバイスは、入力された設定をグループ内のすべてのポートに伝播します。
  - 許可 VLAN リスト。

- 各 VLAN の STP ポート プライオリティ。
- STP PortFast の設定値。
- トランク ステータス：

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

- Per VLAN Spanning Tree（PVST）モードでは最大 24 までのトランク ポート、マルチ スパニング ツリー（MST）モードでは最大 40 までのトランク ポートを設定することを推奨します。
- 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（CLI）

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

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	トランクに設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**} 例： `Device(config-if)# switchport mode dynamic desirable`	インターフェイスをレイヤ 2 トランクとして設定します（インターフェイスがレイヤ 2 アクセス ポートまたはトンネル ポートであり、トランキング モードを設定する場合に限り必要となります）。 • **dynamic auto**：ネイバー インターフェイスが trunk または desirable モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。これがデフォルトです。 • **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

	コマンドまたはアクション	目的
		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： `Device(config-if)# switchport access vlan 200`	（任意）インターフェイスがトランキングを停止した場合に使用するデフォルト VLAN を指定します。
ステップ 6	**switchport trunk native vlan** *vlan-id* 例： `Device(config-if)# switchport trunk native vlan 200`	IEEE 802.1Q トランク用のネイティブ VLAN を指定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces gigabitethernet1/0/2 switchport`	インターフェイスのスイッチポート設定を表示します。[Administrative Mode] および [Administrative Trunking Encapsulation] フィールドに表示されます。
ステップ 9	**show interfaces** *interface-id***trunk** 例： `Device# show interfaces gigabitethernet1/0/2 trunk`	インターフェイスのトランクの設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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

トランクでの許可 VLAN の定義（CLI）

VLAN 1 は、すべての Cisco デバイスのすべてのトランク ポートのデフォルト VLAN です。以前は、すべてのトランク リンクで VLAN 1 を必ずイネーブルにする必要がありました。VLAN 1 の最小化機能を使用して、個々の VLAN トランク リンクで VLAN 1 をディセーブルに設定できます。これにより、ユーザ トラフィック（スパニングツリー アドバタイズなど）は VLAN 1 で送受信されなくなります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 5	**switchport trunk allowed vlan** { *word* | **add** | **all** | **except** | **none** | **remove**} *vlan-list*	（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

	コマンドまたはアクション	目的
	例： `Device(config-if)# switchport trunk allowed vlan remove 2`	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： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** *interface-id* **switchport** 例： `Device# show interfaces gigabitethernet1/0/1 switchport`	表示された [Trunking VLANs Enabled] フィールドの設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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（CLI）

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	VLAN 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。
ステップ 4	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan* [,*vlan* [,,,]]	トランクからのプルーニングを許可する VLAN のリストを設定します。 **add**、**except**、**none**、および **remove** キーワードの使用方法については、このリリースに対応するコマンド リファレンスを参照してください。 連続していない VLAN ID は、カンマ（スペースなし）で区切ります。ID の範囲はハイフンで指定します。有効な ID 範囲は 2 ～ 1001 です。拡張範囲 VLAN（VLAN ID 1006 ～ 4094）はプルーニングできません。 プルーニング不適格の VLAN は、フラッディング トラフィックを受信します。 デフォルトでは、プルーニングが許可される VLAN のリストには、VLAN 2 ～ 1001 が含まれます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show interfaces** *interface-id* **switchport** 例： `Device# show interfaces gigabitethernet2/0/1 switchport`	表示された [Pruning VLANs Enabled] フィールドの設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

タグなしトラフィック用ネイティブ VLAN の設定（CLI）

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

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	IEEE 802.1Q トランクとして設定するインターフェイスを定義して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport trunk native vlan** *vlan-id* 例： `Device(config-if)# switchport trunk native vlan 12`	トランク ポート上でタグなしトラフィックを送受信する VLAN を設定します。 *vlan-id* に指定できる範囲は 1 ～ 4094 です。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces gigabitethernet1/0/2 switchport`	[Trunking Native Mode VLAN] フィールドの設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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（CLI）

デバイスがデバイス スタックのメンバである場合、**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： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	デバイス A で、グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp domain** *domain-name* 例： `Device(config)# vtp domain workdomain`	VTP 管理ドメインを設定します。 1 ～ 32 文字のドメイン名を使用できます。
ステップ 4	**vtp mode server** 例： `Device(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： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show vtp status** 例： `Device# show vtp status`	デバイス A 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： `Device# show vlan`	デバイス A のデータベースに VLAN が存在していることを確認します。

	コマンドまたはアクション	目的
ステップ 8	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 9	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	ポートをトランク ポートとして設定します。
ステップ 11	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 12	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces gigabitethernet1/0/1 switchport`	VLAN の設定を確認します。
ステップ 13	デバイス A で、デバイス またはデバイス 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： `Device# show vlan`	トランク リンクがアクティブになると、VTP がデバイス B に VTP および VLAN 情報を渡します。このコマンドは、デバイス B が VLAN 設定を学習したことを確認します。

	コマンドまたはアクション	目的
ステップ 16	**configure terminal** 例： `Device# configure terminal`	デバイス A で、グローバル コンフィギュレーション モードを開始します。
ステップ 17	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 18	**spanning-tree vlan** *vlan-range***port-priority** *priority-value* 例： `Device(config-if)# spanning-tree vlan 8-10 port-priority 16`	指定された VLAN 範囲にポート プライオリティを割り当てます。0 ～ 240 のポート プライオリティ値を入力します。ポート プライオリティ値は 16 ずつ増分します。
ステップ 19	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 20	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 21	**spanning-tree vlan** *vlan-range***port-priority** *priority-value* 例： `Device(config-if)# spanning-tree vlan 3-6 port-priority 16`	指定された VLAN 範囲にポート プライオリティを割り当てます。0 ～ 240 のポート プライオリティ値を入力します。ポート プライオリティ値は 16 ずつ増分します。
ステップ 22	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 23	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 24	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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, （54 ページ）

STP パス コストによる負荷分散の設定（CLI）

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： `Device> enable`	特権EXECモードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	デバイス A で、グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface 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。

	コマンドまたはアクション	目的
ステップ 4	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	ポートをトランク ポートとして設定します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	デバイス A またはデバイス A スタック内の別のインターフェイスでステップ 2 ～ 4 を繰り返します。	
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。画面で、インターフェイスがトランク ポートとして設定されていることを確認してください。
ステップ 9	**show vlan** 例： `Device# show vlan`	トランク リンクがアクティブになると、デバイス A がもう一方のデバイスから 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 11	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	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。

	コマンドまたはアクション	目的
ステップ 12	**spanning-tree vlan** *vlan-range***cost** *cost-value* 例： `Device(config-if)# spanning-tree vlan 2-4 cost 30`	VLAN 2 ～ 4 のスパニングツリー パス コストを 30 に設定します。
ステップ 13	**end** 例： `Device(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	デバイス A に設定したもう一方のトランク インターフェイスでステップ 9 ～ 13 を繰り返し、VLAN 8、9、および 10 のスパニングツリー パス コストを 30 に設定します。	
ステップ 15	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 16	**show running-config** 例： `Device# show running-config`	入力を確認します。両方のトランク インターフェイスに対してパス コストが正しく設定されていることを表示で確認します。
ステップ 17	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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
- 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	参照先
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* コマンド リファレンス *(Catalyst 3850* スイッチ*)* 『*Layer 2/3* コマンド リファレンス *(Catalyst 3850* スイッチ*)*』 *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	役職（Title）
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 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

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、Product Alert Tool（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	変更箇所
Cisco IOS XE Everest 16.5.1a	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，71 ページ
- 音声 VLAN の前提条件，71 ページ
- 音声 VLAN の制約事項，72 ページ
- 音声 VLAN に関する情報，72 ページ
- 音声 VLAN の設定方法，75 ページ
- 音声 VLAN のモニタリング，79 ページ
- 次の作業，79 ページ
- その他の参考資料，80 ページ
- 音声 VLAN の機能履歴と情報，81 ページ

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

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

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

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

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

Cisco IP Phone の音声トラフィック

Cisco IP Phone と接続するアクセス ポートを、1 つの VLAN は音声トラフィック用に、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータ トラフィック用に使用するように設定できます。Cisco Discovery Protocol（CDP）パケットを送信するよう、デバイス上のアクセス

ポートを設定できます。CDP パケットは、接続する IP Phone に対して、次のいずれかの方法で音声トラフィックをデバイスに送信するよう指示します。

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

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

関連トピック

Cisco IP Phone の音声トラフィックの設定（CLI），（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

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

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

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

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（CLI），（77 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、デバイスを Cisco IP Phone に接続するポートは、さまざまな種類のトラフィックを伝送できます。ポートを設定することによって、Cisco IP Phone による音声トラフィックおよびデータ トラフィックの伝送方法を決定できます。
- IP Phone で音声 VLAN 通信が適切に行われるには、デバイス上に音声 VLAN が存在し、アクティブになっている必要があります。VLAN が存在しているかどうかを確認するには、**show vlan** 特権 EXEC コマンドを使用します（リストで表示されます）。VLAN がリストされていない場合は、音声 VLAN を作成します。
- Power Over Ethernet（PoE）デバイスは、シスコ先行標準の受電デバイスまたは IEEE 802.3af 準拠の受電デバイスが AC 電源から電力を供給されてない場合に、それらの受電デバイスに自動的に電力を供給できます。
- 音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。
- Cisco IP Phone とその IP Phone に接続されたデバイスが同じ VLAN 上にある場合、両方とも同じ IP サブネットに属していなければなりません。次の条件が満たされている場合は、同じ VLAN 上にあります。
  - 両方とも IEEE 802.1p またはタグなしフレームを使用する。
  - Cisco IP Phone が IEEE 802.1p フレームを使用し、デバイスがタグなしフレームを使用する。
  - Cisco IP Phone がタグなしフレームを使用し、デバイスが IEEE 802.1p フレームを使用する。
  - Cisco IP Phone が IEEE 802.1Q フレームを使用し、音声 VLAN がアクセス VLAN と同じである。
- Cisco IP Phone と IP Phone に接続されたデバイスは、同一 VLAN、同一サブネット上にあっても、使用するフレーム タイプが異なる場合は通信できません。トラフィックは同一サブネット上でルーティングされないからです（ルーティングによってフレーム タイプの相違が排除されます）。
- 音声 VLAN ポートには次のポート タイプがあります。
  - ダイナミック アクセス ポート。
  - IEEE 802.1x 認証ポート。

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

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

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

音声 VLAN の設定方法

Cisco IP Phone の音声トラフィックの設定（CLI）

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	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**trust device cisco-phone** 例： `Device(config-if)# trust device cisco-phone`	Cisco IP Phone の着信トラフィック パケットを信頼するようにインターフェイスを設定します。
ステップ 4	**switchport voice vlan** {*vlan-id* | **dot1p** | **none** | **untagged**} 例： `Device(config-if)# switchport voice vlan dot1p`	音声 VLAN を設定します。 • *vlan-id*：すべての音声トラフィックが特定の VLAN を経由して転送されるように IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。指定できる VLAN ID の範囲は 1 ～ 4094 です。 • **dot1p**：VLAN ID 0（ネイティブ VLAN）のタグが付けられた音声およびデータ IEEE 802.1p プライオリティ フレームを受け入れるよう、デバイスを設定します。デフォルトでは、デバイスは VLAN 0 のタグが付いたすべての音声およびデータ トラフィックをドロップします。802.1p に対応するよう設定されると、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用してトラフィックを転送します。 • **none**：IP Phone で独自の設定を使ってタグなし音声トラフィックを送信できるようにします。 • **untagged**：タグなしの音声トラフィックを送信するように電話を設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	次のいずれかを使用します。 • **show interfaces** *interface-id***switchport** • **show running-config interface** *interface-id*	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。

	コマンドまたはアクション	目的

	例：
	`Device# show interfaces gigabitethernet1/0/1 switchport`
	または
	`Device# show running-config interface gigabitethernet1/0/1`	

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

関連トピック

Cisco IP Phone の音声トラフィック，（72 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（CLI）

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	Cisco IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport priority extend** {**cos** *value* | **trust**} 例： `Device(config-if)# switchport priority extend trust`	Cisco IP Phone のアクセス ポートから受信したデータ トラフィックのプライオリティを次のように設定します。 • **cos** *value*：PC または接続しているデバイスから受信したプライオリティを、指定のCoS値にオーバーライドするよう、IP Phone を設定します。値は0～7です。7が最高のプライオリティです。デフォルトのプライオリティは **cos** 0 です。 • **trust**：PCまたは接続しているデバイスから受信したプライオリティを信頼するよう IP Phone アクセス ポートを設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id***switchport** 例： `Device# show interfaces`	入力を確認します。

	コマンドまたはアクション	目的
	gigabitethernet1/0/1 switchport	
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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（CLI），（75 ページ）
Cisco IP Phone の音声トラフィック，（72 ページ）
着信データ フレームのプライオリティ設定（CLI），（77 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 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	参照先
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 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	役職（Title）
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 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

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、Product Alert Tool（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	変更箇所
Cisco IOS XE Everest 16.5.1a	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，83 ページ
- プライベート VLAN の前提条件，83 ページ
- プライベート VLAN の制約事項，84 ページ
- プライベート VLAN について，85 ページ
- プライベート VLAN の設定方法，96 ページ
- プライベート VLAN のモニタ，106 ページ
- プライベート VLAN の設定例，107 ページ
- 次の作業，109 ページ
- その他の参考資料，110 ページ

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 Cisco 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 の制約事項

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

- プライベート VLAN が設定されているデバイスでは、フォールバック ブリッジングを設定しないでください。
- リモート SPAN（RSPAN）をプライベート VLAN のプライマリまたはセカンダリ VLAN として設定しないでください。
- 次のような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）
  - Link Aggregation Control Protocol（LACP）
  - マルチキャスト VLAN レジストレーション（MVR）
  - ボイス 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

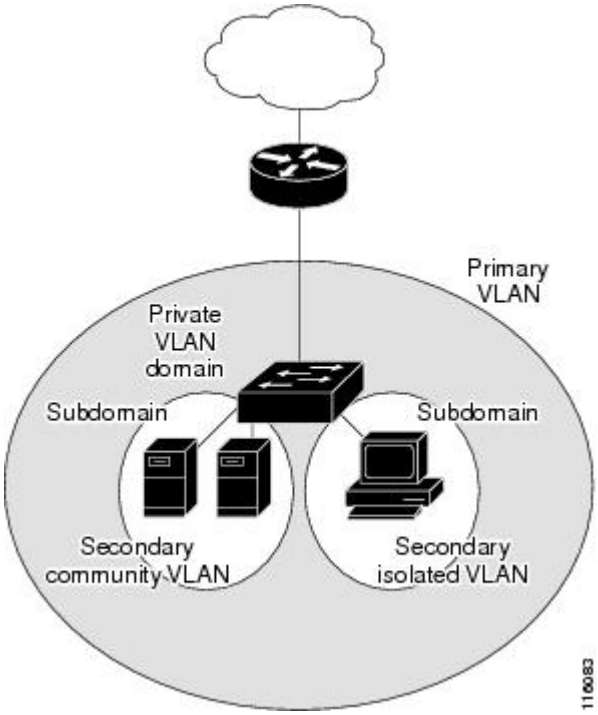
PVLAN 機能を使用すると、サービス プロバイダーが VLAN を使用したときに直面する 2 つの問題に対処できます。

- Network Essentials または Network Advantage を実行している場合、最大で 4094 個のアクティブ VLAN がデバイスでサポートされます。サービス プロバイダーが 1 カスタマーあたり 1 つの VLAN を割り当てる場合、サービス プロバイダーがサポートできるカスタマー数はこれに制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネット アドレス空間またはアドレス ブロックを割り当てますが、これにより、未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が起きます。

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VLANIDは、各サブドメインの区別に使用されます。

図 *3*：プライベート *VLAN* ドメイン



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デバイスに接続されます。無差別ポートでは、広範囲なデバイスをプライベート VLAN のアクセス ポイントとして接続できます。たとえば、すべてのプライベート VLAN サーバ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。

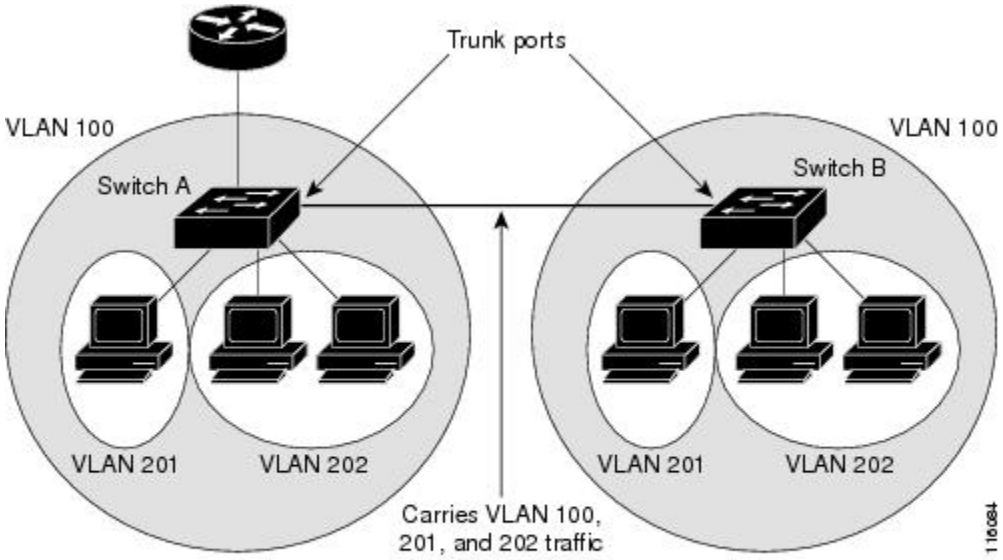
- カスタマー VLAN にアドレスのブロックを割り当てると、未使用 IP アドレスが発生することがあります。
- VLAN 内のデバイス数が増加した場合、それに対応するだけのアドレスを割り当てられない場合があります。

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。

複数のデバイスにまたがるプライベート VLAN

通常の VLAN と同様に、プライベート VLAN を複数のデバイスにまたがるように設定できます。トランク ポートはプライマリ VLAN およびセカンダリ VLAN をネイバーデバイスに伝送します。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。複数のデバイスにまたがるプライベート VLAN の機能の特徴として、デバイス A にある独立ポートからのトラフィックはデバイス B に到達しません。

図 *4*：複数のスイッチにまたがるプライベート *VLAN*



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 スイッチデバイスでは、デバイス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 はデバイス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 メンバー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された場合、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、デバイスを再起動したときに、権利を獲得しなかったデバイスのプライベート 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
```

- このデバイスでは、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、このデバイスの場合、他のプラットフォームの「単方向」と比べ、双方向です。

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

レイヤ 2 のフレームがプライベート VLAN 内で転送されると、入力側と出力側とで VLAN マップが適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが入力側に適用されます。同様に、フレームが外部ポートからプライベート VLAN にルーティングされると、プライベート VLAN は出力側に適用されます。これは、ブリッジされたトラフィックとルーティングされたトラフィックの両方に適用されます。

ブリッジング：

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

ルーティング

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

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

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

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

プライベート VLAN および HA サポート

PVLANは、高可用性（HA）機能とシームレスに連携します。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。デバイスで VTP バージョン 1 または 2 が稼働している場合は、VTP をトランスペアレント モードに設定する必要があります。プライベート VLAN を設定した後で、VTP モードをクライアントまたはサーバに変更できません。VTP バージョン 3 は、すべてのモードでプライベート VLAN をサポートします。
- VTP バージョン 1 または 2 でプライベート VLAN を設定した後、**copy running-config startup config** 特権 EXEC コマンドを使用して、VTP トランスペアレント モード設定とプライベート VLAN 設定を デバイス スタートアップ コンフィギュレーション ファイルに保存します。保存しないと、デバイスをリセットした場合にデフォルトの 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。

  また、**copy flash:config_file running-config** の代わりに **configure replace flash:config_file force** も使用できます。
- 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 コマンドおよび **ip sticky-arpinterface** 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。

参照 プライベート VLAN 内の VLAN の設定および対応付け，（97 ページ）

（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。

参照 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）

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。

参照 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）

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。

参照 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）

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

private-vlan 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。

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vtp mode transparent** 例： `Device(config)# vtp mode transparent`	VTP モードをトランスペアレントに設定します（VTP をディセーブルにします）。 （注） VTP3 の場合、サーバまたはトランスペアレント モードのいずれにもモードを設定できます。
ステップ 4	**vlan** *vlan-id* 例： `Device(config)# vlan 20`	VLANコンフィギュレーションモードを開始して、プライマリ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 5	**private-vlan primary** 例： `Device(config-vlan)# private-vlan primary`	VLAN をプライマリ VLAN として指定します。
ステップ 6	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**vlan** *vlan-id* 例： `Device(config)# vlan 501`	（任意）VLAN コンフィギュレーション モードを開始して、独立 VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 8	**private-vlan isolated** 例： `Device(config-vlan)# private-vlan isolated`	VLAN を独立 VLAN として指定します。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**vlan** *vlan-id* 例： `Device(config)# vlan 502`	（任意）VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 11	**private-vlan community** 例： `Device(config-vlan)# private-vlan community`	VLAN をコミュニティ VLAN として指定します。
ステップ 12	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**vlan** *vlan-id* 例： `Device(config)# vlan 503`	（任意）VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 14	**private-vlan community** 例： `Device(config-vlan)# private-vlan community`	VLAN をコミュニティ VLAN として指定します。
ステップ 15	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**vlan** *vlan-id* 例： `Device(config)# vlan 20`	ステップ 4 で指定したプライマリ VLAN に関して VLAN コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 17	**private-vlan association** [**add** | **remove**] *secondary_vlan_list* 例： `Device(config-vlan)# private-vlan association 501-503`	セカンダリ VLAN をプライマリ VLAN に関連付けます。単一のプライベート VLAN ID でも、またはハイフンで連結したプライベート VLAN ID でもかまいません。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。 • *secondary_vlan_list* パラメータには複数のコミュニティ VLAN ID を含められますが、独立 VLAN ID は 1 つだけです。 • *secondary_vlan_list* を入力するか、または **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 とプライマリ VLAN を関連付けます。 • セカンダリ VLAN とプライマリ VLAN 間の関連付けをクリアするには、*secondary_vlan_list* に **remove** キーワードを使用します。 • このコマンドは、VLAN コンフィギュレーション モードを終了するまで機能しません。
ステップ 18	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 19	**show vlan private-vlan** [**type**] または **show interfaces status** 例： `Device# show vlan private-vlan`	設定を確認します。
ステップ 20	**copy running-config startup config** 例： `Device# copy running-config`	デバイス スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

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

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/22`	設定するレイヤ 2 インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode private-vlan host** 例： `Device(config-if)# switchport mode private-vlan host`	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。

	コマンドまたはアクション	目的
ステップ 5	**switchport private-vlan host-association** *primary_vlan_id secondary_vlan_id* 例： `Device(config-if)# switchport private-vlan host-association 20 501`	レイヤ 2 ポートをプライベート VLAN と関連付けます。 （注） これは、レイヤ 2 インターフェイスに PVLAN を関連付けるために必要な手順です。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： `Device# show interfaces gigabitethernet1/0/22 switchport`	設定を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	設定するレイヤ 2 インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode private-vlan promiscuous** 例： `Device(config-if)# switchport mode private-vlan promiscuous`	レイヤ 2 ポートをプライベート VLAN 無差別ポートとして設定します。
ステップ 5	**switchport private-vlan mapping** *primary_vlan_id* {**add** | **remove**} *secondary_vlan_list* 例： `Device(config-if)# switchport private-vlan mapping 20 add 501-503`	プライベート VLAN 無差別ポートをプライマリ VLAN、および選択したセカンダリ VLAN にマッピングします。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。 • セカンダリ VLAN とプライマリ VLAN をプライベート VLAN 無差別ポートにマッピングするには、*secondary_vlan_list* 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、

	コマンドまたはアクション	目的
		remove キーワードを指定した *secondary_vlan_list* を使用します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** [*interface-id*] **switchport** 例： `Device# show interfaces gigabitethernet1/0/2 switchport`	設定を確認します。
ステップ 8	**copy running-config startup config** 例： `Device# copy running-config startup-config`	デバイス スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

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： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface vlan** *primary_vlan_id* 例： `Device(config)# interface vlan 20`	プライマリ VLAN でインターフェイス コンフィギュレーション モードを開始して、VLAN を SVI として設定します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 4	**private-vlan mapping** [**add** | **remove**] *secondary_vlan_list* 例： `Device(config-if)# private-vlan mapping 501-503`	セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングして、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にします。 （注） **private-vlan mapping** インターフェイス コンフィギュレーション コマンドは、レイヤ 3 スイッチングされているプライベート VLAN トラフィックにだけ影響を与えます。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。 • *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN をプライマリ VLAN にマッピングします。 • **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： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interface private-vlan mapping** 例： `Device# show interfaces private-vlan mapping`	設定を確認します。
ステップ 7	**copy running-config startup config** 例： `Device# copy running-config startup-config`	デバイス スタートアップ コンフィギュレーション ファイルに設定項目を保存します。

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（Command）	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]	Deviceまたは Device スタックのプライベート VLAN 情報を表示します。

コマンド（Command）	目的
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。

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

例：ホスト ポートとしてのインターフェイスの設定

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

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/22
Device(config-if)# switchport mode private-vlan host
Device(config-if)# switchport private-vlan host-association 20 501
Device(config-if)# end
Device# show interfaces gigabitethernet1/0/22 switchport
```

```
Name: Gi1/0/22
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 20 501
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 501

<output truncated>
```

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。

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

show vlan private-vlan または **show interface status** 特権 EXEC コマンドを使用してプライマリおよびセカンダリ VLAN と Device 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。

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

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。

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

次の作業

次の設定を行えます。

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

その他の参考資料

関連資料

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

標準および RFC

標準/RFC	役職（Title）
RFC 1573	
RFC 1757	
RFC 2021	

MIB

MIB	MIB 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

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、Product Alert Tool（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

通告

Trademarks

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)