



Cisco IOS リリース 15.2(7)Ex (Catalyst 1000 スイッチ) VLAN コ ンフィギュレーションガイド

初版：2019年12月25日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

VTP の設定 1

VTP の前提条件	1
VTP の制約事項	2
VTP の概要	2
VTP	2
VTP ドメイン	2
VTP モード	3
VTP アドバタイズ	5
VTP バージョン 2	5
VTP バージョン 3	6
VTP プルーニング	7
VTP 設定時の注意事項	7
VTP の設定要件	7
VTP の設定	7
VTP 設定のためのドメイン名	8
VTP ドメインのパスワード	8
VTP バージョン	9
VTP のデフォルト設定	10
VTP の設定方法	11
VTP モードの設定	11
VTP バージョン 3 のパスワードの設定	13
VTP バージョン 3 のプライマリ サーバの設定	14
VTP バージョンのイネーブル化	15
VTP プルーニングのイネーブル化	17

ポート単位の VTP の設定	18
VTP ドメインへの VTP クライアント スイッチの追加	19
VTP のモニタ	21
VTP の設定例	22
例：スイッチをプライマリ サーバとして設定する	22
例：VTP サーバとしてのスイッチの設定	22
例：インターフェイスでの VTP のイネーブル化	23
例：VTP パスワードの作成	23
VTP の機能履歴と情報	23

第 2 章

VLAN の設定	25
VLAN の前提条件	25
VLAN の制約事項	25
VLAN について	26
論理ネットワーク	26
サポートされる VLAN	26
VLAN ポート メンバシップ モード	27
VLAN コンフィギュレーション ファイル	28
標準範囲 VLAN 設定時の注意事項	29
拡張範囲 VLAN 設定時の注意事項	30
VLAN のデフォルト設定	30
イーサネット VLAN のデフォルト設定	30
VLAN の設定方法	31
標準範囲 VLAN の設定方法	31
イーサネット VLAN の作成または変更	32
VLAN の削除	33
VLAN へのスタティック アクセス ポートの割り当て	34
拡張範囲 VLAN の設定方法	36
拡張範囲 VLAN の作成	36
VLAN のモニタリング	37
設定例	39

例：VLAN 名の作成	39
例：アクセス ポートとしてのポートの設定	40
例：拡張範囲 VLAN の作成	40
VLAN の設定の機能履歴と情報	40

第 3 章

VLAN トランクの設定	41
VLAN トランクの前提条件	41
VLAN トランクについて	42
トランキングの概要	42
トランキング モード	42
レイヤ 2 インターフェイス モード	42
トランクでの許可 VLAN	43
トランク ポートでの負荷分散	44
STP プライオリティによるネットワーク負荷分散	44
STP パス コストによるネットワーク負荷分散	44
機能の相互作用	44
レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定	45
VLAN トランクの設定方法	45
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	46
トランク ポートの設定	46
トランクでの許可 VLAN の定義	48
ブルーニング適格リストの変更	49
タグなしトラフィック用ネイティブ VLAN の設定	50
トランク ポートの負荷分散の設定	52
STP ポート プライオリティによる負荷分散の設定	52
STP パス コストによる負荷分散の設定	55
VLAN トランキングの設定例	58
例：トランク ポートの設定	58
例：ポートからの VLAN の削除	58
VLAN トランクの機能履歴と情報	58

第 4 章

音声 VLAN の設定 59

音声 VLAN の前提条件 59

音声 VLAN の制約事項 60

音声 VLAN に関する情報 60

音声 VLAN 60

Cisco IP Phone の音声トラフィック 60

Cisco IP Phone のデータトラフィック 60

音声 VLAN 設定時の注意事項 61

音声 VLAN のデフォルト設定 62

音声 VLAN の設定方法 63

Cisco IP Phone の音声トラフィックの設定 63

音声 VLAN のモニタリング 65

設定例 65

例：Cisco IP Phone の音声トラフィックの設定 65

音声 VLAN の機能履歴と情報 66



第 1 章

VTP の設定

- [VTP の前提条件 \(1 ページ\)](#)
- [VTP の制約事項 \(2 ページ\)](#)
- [VTP の概要 \(2 ページ\)](#)
- [VTP の設定方法 \(11 ページ\)](#)
- [VTP のモニタ \(21 ページ\)](#)
- [VTP の設定例 \(22 ページ\)](#)
- [VTP の機能履歴と情報 \(23 ページ\)](#)

VTP の前提条件

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

VTP は、1 台のスイッチで行われた更新が VTP を介してドメイン内の他のスイッチ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スイッチ上で同時に発生する環境の場合、VTP は適していません。VLAN データベースの不整合が生じます。

スイッチは、合計 256 の VLAN をサポートします。VTP が新しい VLAN をスイッチに通知し、スイッチ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、スイッチはハードウェアリソース不足を伝えるメッセージを送信して、VLAN をシャットダウンします。

show vlan EXEC コマンドの出力に、中断状態の VLAN が示されます。

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 の制約事項



(注) VTP クライアントスイッチを 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 ドメイン内の他のスイッチ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 ドメイン内のスイッチは常に、VTP コンフィギュレーションリビジョン番号が最大のスイッチの 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スイッチを追加すると、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。

次に、VTP を設定する際の制約事項を示します。

- 約 10 のアクセスインターフェイスまたは 5 つのトランク インターフェイスを同時にフラップさせるのは、一般的なことです。これによる CPU 使用率への影響はごくわずかです。同時にフラップするインターフェイスが多い場合は、CPU 使用率が非常に高くなる可能性があります。

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 バージョン 1 およびバージョン 2 は、標準範囲の VLAN (VLAN ID 1 ~ 1005) だけをサポートします。VTP バージョン 3 は、VLAN 範囲全体 (VLAN 1 ~ 4094) をサポートします。拡張範囲 VLAN (VLAN 1006 ~ 4094) は、VTP バージョン 3 でだけサポートされます。

拡張 VLAN がドメインに設定されている場合は、VTP バージョン 3 から VTP バージョン 2 に変換できません。

VTP ドメイン

VTP ドメイン (別名 VLAN 管理ドメイン) は、1 つのスイッチ、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スイッチで構成されます。スイッチは、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、スイッチは 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。

スイッチがトランク リンクを介して VTP アドバタイズを受信すると、スイッチは管理ドメイン名および VTP コンフィギュレーション リビジョン番号を継承します。その後スイッチは、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スイッチに伝播されます。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 モードでスイッチを設定した場合、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スイッチには送信されません。また、変更が作用するのは、個々のスイッチに限られます。ただし、スイッチがこのモードの際に設定を変更すると、変更内容がスイッチの実行コンフィギュレーションに保存されます。この変更はスイッチのスタートアップ コンフィギュレーション ファイルに保存することもできます。

VTP モード

表 1: VTP モード

VTP モード	説明
VTP サーバ	<p>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 ドメイン内の他のスイッチに自身の 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 設定を他のスイッチと同期させます。</p> <p>VTP サーバがデフォルトのモードです。</p> <p>VTP サーバモードでは、VLAN 設定は NVRAM に保存されます。スイッチ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、スイッチは NVRAM が動作するまで VTP サーバモードに戻ることができません。</p>

VTP モード	説明
VTP クライアント	<p>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スイッチで設定します。</p> <p>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。</p>
VTP トランスペアレント	<p>VTP トランスペアレントスイッチは、VTP に参加しません。VTP トランスペアレントスイッチは自身の 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スイッチは、トランク インターフェイスを介して他のスイッチから受信した 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、スイッチ上の VLAN を作成、変更、削除できます。</p> <p>スイッチが 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、他のスイッチ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スイッチの実行コンフィギュレーションに保存されます。この情報をスイッチの実行コンフィギュレーションに保存するには、copy running-config startup-config 特権 EXEC コマンドを使用します。</p>
VTP オフ	<p>VTP オフモードでのスイッチの機能は、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スイッチとしての機能と同じです。</p>

VTP アドバタイズ

VTP ドメイン内の各スイッチは、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送信します。このようなアドバタイズを受信したネイバースイッチは、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。

VTP アドバタイズにより、次のグローバルドメイン情報が配信されます。

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

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

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

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

VTP バージョン 2

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

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

- トークンリングサポート : VTP バージョン 2 は、トークンリングブリッジリレー機能 (TrBRF) およびトークンリングコンセンタリレー機能 (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、スイッチが 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スイッチが 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スイッチは、ドメイン名が一致した場合のみメッセージを転送します。
- 整合性検査：VTP バージョン 2 では、CLI または SNMP を介して新しい情報が入力された場合に限り、VLAN 整合性検査（VLAN 名、値など）を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージの MD5 ダイジェストが有効であれば、情報を受け入れます。

VTP バージョン 3

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

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



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

- 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、スイッチにパ

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 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 リンクへのフラッドイング 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、スイッチは受信側のスイッチ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ドイングします。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ドイング 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、スイッチのトランク 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、引き続きフラッドイングが行われます。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 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、ドメイン内の各スイッチ上で手動によってプルーニングをイネーブル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スイッチに影響するわけではありません)。

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

VTP 設定時の注意事項

VTP の設定要件

VTP を設定する場合は、スイッチがドメイン内の他のスイッチと 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 の設定

VTP 情報は VTP VLAN データベースに保存されます。VTP モードが透過的である場合、VTP ドメイン名およびモードはスイッチ実行コンフィギュレーションファイルに保存されます。この情報をスイッチ 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。スイッチ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。

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

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

VTP 設定のためのドメイン名

VTP を初めて設定するときは、必ずドメイン名を割り当てる必要があります。また、VTP ドメイン内のすべてのスイッチを、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スイッチは、他のスイッチと VTP メッセージを交換しません。これらのスイッチについては 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スイッチを VTP サーバモードにする必要があります。



注意 すべてのスイッチが 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 台のスイッチを VTP サーバモードに設定してください。

VTP ドメインのパスワード

VTP ドメインのパスワードは設定できますが、必須ではありません。ドメインパスワードを設定する場合は、すべてのドメインスイッチで同じパスワードを共有し、管理ドメイン内のスイッチごとにパスワードを設定する必要があります。パスワードのない、または間違っったパスワードのスイッチは、VTP アドバタイズが拒否されます。

ドメインに VTP パスワードを設定する場合、VTP 設定なしで起動したスイッチは、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、スイッチは同じパスワードおよびドメイン名を使用した 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スイッチを追加した場合、その新しいスイッチに適切なパスワードを設定して初めて、スイッチ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、ドメイン内の各スイッチに管理ドメインパスワードを割り当てなかった場合には、管理ドメインが正常に動作しません。

VTP バージョン

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

- VTP ドメイン内のすべてのスイッチ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 対応のスイッチ上で 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 対応スイッチは、VTP バージョン 1 を実行しているスイッチと同じ 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 に対応可能なスイッチが VTP バージョン 3 アドバタイズを受信すると、このスイッチは VTP バージョン 2 に自動的に移行します。
- VTP バージョン 3 を実行しているスイッチが VTP バージョン 1 を実行しているスイッチに接続すると、VTP バージョン 1 のスイッチは VTP バージョン 2 に移行し、VTP バージョン 3 のスイッチは、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 スイッチ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 を実行するスイッチは、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スイッチがバージョン 2 に対応可能な場合を除いて、スイッチ上で VTP バージョン 2 をイネーブルにしないでください。あるスイッチでバージョン 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 対応スイッチでバージョン 2 がイネーブルになります。バージョン 1 専用のスイッチがドメインに含まれている場合、そのスイッチはバージョン 2 対応スイッチとの間で VTP 情報を交換できません。
- VTP バージョン 1 および 2 スイッチは、VTP バージョン 3 アドバタイズメントを転送できないため、ネットワークのエッジに配置することをお勧めします。
- 使用環境に TrBRF および TrCRF トークンリング ネットワークが含まれている場合に、トークンリング VLAN スイッチング機能を正しく動作させるには、VTP バージョン 2 またはバージョン 3 をイネーブルにする必要があります。トークンリングおよびトークンリング Net を実行する場合は、VTP バージョン 2 をディセーブルにします。
- VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN (VLAN 1006 ~ 4094) の設定情報を伝播しません。これらの VLAN は各装置で手動によって設定する必要があります。VTP バージョン 3 は拡張範囲 VLAN と、拡張範囲 VLAN データベースの伝播をサポートします。
- VTP バージョン 3 装置のトランク ポートが VTP バージョン 2 装置からのメッセージを受信した場合、この装置は、VLAN データベースをスケールダウンし、その特定のトランク

上で VTP バージョン 2 フォーマットを使用して送信します。VTP バージョン 3 装置は、最初にそのトランク ポートで VTP バージョン 2 パケットを受信しない限り、VTP バージョン 2 フォーマットのパケットを送信しません。

- VTP バージョン 3 装置が、あるトランク ポートで VTP バージョン 2 装置を検出した場合、両方のネイバーが同一トランク上で共存できるように、VTP バージョン 2 パケットだけでなく VTP バージョン 3 パケットの送信も継続します。
- VTP バージョン 3 装置は、VTP バージョン 2 またはバージョン 1 の装置からの設定情報は受け入れません。
- 2 つの VTP バージョン 3 リージョンは、VTP バージョン 1 リージョンまたはバージョン 2 リージョンでは、トランスペアレントモードでだけ通信できます。
- VTP バージョン 1 にだけ対応する装置は、VTP バージョン 3 装置との相互運用はできません。
- VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN (VLAN 1006 ~ 4094) の設定情報を伝播しません。これらの VLAN を各装置上に手動で設定する必要があります。

VTP のデフォルト設定

次の表に、VTP のデフォルト設定を記載します。

表 2: VTP のデフォルト設定

機能	デフォルト設定
VTP ドメイン名	ヌル
VTP モード (VTP バージョン 1 およびバージョン 2)	サーバ
VTP モード (VTP バージョン 3)	このモードは、VTP バージョン 3 に変換する前のバージョン 1 または 2 のモードと同じです。
VTP バージョン	バージョン 1
MST データベース モード	トランスペアレント
VTP バージョン 3 のサーバタイプ	セカンダリ
VTP パスワード	なし
VTP プルーニング	ディセーブル

VTP の設定方法

VTP モードの設定

次のいずれかに VTP モードを設定できます。

- VTP サーバモード : VTP サーバモードでは、VLAN の設定を変更し、ネットワーク全体に伝播させることができます。
- VTP クライアントモード : VTP クライアントモードでは、VLAN の設定を変更できません。クライアントスイッチは、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、スイッチで VTP がディセーブルになります。スイッチは VTP アップデートを送信せず、他のスイッチから受信した 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スイッチは、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。別のドメインにスイッチを再び割り当てるしかありません。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	vtp 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スイッチは、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
		<p>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。スイッチが VTP ドメインにトランク接続されている場合、スイッチはドメイン内の VTP サーバからドメイン名を取得します。</p> <p>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。</p>
ステップ 4	<p>vtp mode {client server transparent off} {vlan mst unknown}</p> <p>例 :</p> <pre>Device(config)# vtp mode server</pre>	<p>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) のスイッチの設定。</p> <ul style="list-style-type: none"> • 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	<p>vtp password password</p> <p>例 :</p> <pre>Device(config)# vtp password mypassword</pre>	<p>(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、ドメイン内の各スイッチ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。</p>
ステップ 6	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 7	<p>show vtp status</p> <p>例 :</p> <pre>Device# show vtp status</pre>	<p>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。</p>

	コマンドまたはアクション	目的
ステップ 8	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) 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。 スイッチの実行コンフィギュレーションに保存され、スタートアップ コンフィギュレーション ファイルにコピーできるのは、VTP モードおよびドメイン名だけです。

VTP バージョン 3 のパスワードの設定

スイッチで VTP バージョン 3 のパスワードを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	vtp version 3 例 : Device(config)# vtp version 3	デバイスで VTP バージョン 3 を有効にします。デフォルトは VTP バージョン 1 です。
ステップ 4	vtp password password [hidden secret] 例 : Device(config)# vtp password mypassword 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。 <ul style="list-style-type: none"> (任意) hidden : パスワード文字列から生成される秘密キーが、<code>nvrām:vlan.dat</code> 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

	コマンドまたはアクション	目的
		<p>とすると、パスワードの再入力を要求されます。</p> <ul style="list-style-type: none"> （任意） secret : パスワードを直接設定します。シークレットパスワードには 16 進数文字を 32 個含める必要があります。
ステップ 5	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show vtp password 例 : Device# show vtp password	<p>入力を確認します。次のような出力が表示されます。</p> <p>VTP password: 89914640C8D90868B6A0D8103847A733</p>
ステップ 7	copy running-config startup-config 例 : Device# copy running-config startup-config	（任意） コンフィギュレーション ファイルに設定を保存します。

VTP バージョン 3 のプライマリ サーバの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	vtp version 3 例 : Device(config)# vtp version 3	デバイスで VTP バージョン 3 を有効にします。デフォルトは VTP バージョン 1 です。
ステップ 2	vtp primary [vlan mst] [force] 例 : Device# vtp primary vlan force	スイッチ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。スイッチのパス

	コマンドまたはアクション	目的
		<p>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。</p> <ul style="list-style-type: none"> • (任意) vlan : テイクオーバー機能として VLAN データベースを選択します。これはデフォルトです。 • (任意) mst : テイクオーバー機能としてマルチスパンニングツリー (MST) データベースを選択します • (任意) force : 競合するサーバの設定が上書きされます。 force を入力しない場合、テイクオーバーの実行前に確認を求められます。

VTP バージョンのイネーブル化


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

- あるスイッチ上で 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スイッチでバージョン 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、各スイッチ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、VTP サーバモードまたはトランスペアレントモードのスイッチでだけバージョンを設定できます。スイッチが VTP バージョン 3 を実行し、かつスイッチがクライアントモードの場合、既存の拡張 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 ドメイン内のスイッチ上で、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スイッチが VTP バージョン 2 をサポートしている場合を除き、VTP バージョン 2 をイネーブルにはしないでください。

- TrCRF および TrBRF トークンリング環境では、トークンリング VLAN スイッチング機能を正しく動作させるために、VTP バージョン 2 または VTP バージョン 3 をイネーブルにする必要があります。トークンリングおよびトークンリング Net メディアの場合は、VTP バージョン 2 をディセーブルにします。

- 

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	vtp version {1 2 3} 例 : Device(config)# vtp version 2	スイッチで 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。

VTP プルーニングのイネーブル化

始める前に

VTP プルーニングは VTP トランスペアレント モードでは機能しないように設計されています。ネットワーク内に VTP トランスペアレントモードのスイッチが 1 台または複数存在する場合は、次のいずれかのアクション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スイッチのアップストリーム側にあるスイッチのトランク上で、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ッ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ッキングを実行しているかどうかにかかわらず、設定できます。

手順

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

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

ポート単位の VTP の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface interface-id 例 : Device (config) # interface gigabitethernet 1/0/1	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 :	特権 EXEC モードに戻ります。

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

VTP ドメインへの VTP クライアント スイッチの追加

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

始める前に

VTP クライアントを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のスイッチ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 ドメイン内のスイッチは常に、VTP コンフィギュレーション リビジョン番号が最大のスイッチの 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スイッチを追加すると、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。

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	show vtp status 例 : Device# show vtp status	VTP コンフィギュレーションリビジョン番号をチェックします。 番号が 0 の場合は、スイッチを 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。 <ul style="list-style-type: none"> • 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、スイッチのコンフィギュレーションリビジョン番号をリセットします。
ステップ 3	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 4	vtp domain domain-name 例 : Device(config)# vtp domain domain123	ドメイン名を、ステップ 1 で表示された元の名前から新しい名前に変更します。
ステップ 5	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show vtp status 例 : Device# show vtp status	コンフィギュレーションリビジョン番号が 0 にリセットされていることを確認します。
ステップ 7	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーションモードを開始します。

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

VTP のモニタ

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

VTP の設定情報 (ドメイン名、現在の VTP バージョン、VLAN 数) を表示することによって、VTP をモニタします。スイッチ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 3: VTP モニタ コマンド

コマンド	目的
show vtp counters	送受信された VTP メッセージに関するカウンタを表示します。
show vtp devices [conflict]	ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。プライマリサーバと競合する VTP バージョン 3 の装置が表示されます。 show vtp devices コマンドは、スイッチ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。

コマンド	目的
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、暗号化がスイッチ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 スイッチの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）としてスイッチを設定する方法の例を示します。

```
Device# vtp primary vlan
VTP Feature Conf Revision Primary Server Device ID Device Description
-----
VLAN Yes 25 bcf1.f2e4.9700 0c75.bd07.4a00 P3A_NEW
VLAN Yes 547 0c75.bd07.4a00 40a6.e8db.9780 Switch_A
MST Yes 10 006c.bc4e.2500 40a6.e8db.9780 Switch_A
VLAN Yes 25 bcf1.f2e4.9700 e8b7.489c.cc00 Switch_B-11

Do you want to continue? [confirm]
Switch#
Jun 17 01:08:50.758 PST: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: 006c.bc4e.2500 has become
the primary server for the VLAN VTP feature
```

例：VTP サーバとしてのスイッチの設定

次に、ドメイン名が *eng_group*、パスワードが *mypassword* という VTP サーバとしてスイッチを設定する例を示します。

```
Switch(config)# vtp domain eng_group
Setting VTP domain name to eng_group.

Switch(config)# vtp mode server
Setting device to VTP Server mode for VLANs.

Switch(config)# vtp password mypassword
Setting device VLAN database password to mypassword.
Switch(config)# end
```

例：インターフェイスでの VTP のイネーブル化

インターフェイス上で VTP をイネーブルにするには、**vtp** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイス上で VTP を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 コマンドを使用します。

```
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# vtp
Device(config-if)# end
```

例：VTP パスワードの作成

次に、VTP パスワードを作成する例を示します。

```
Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Switch(config)# end
Switch# show vtp password
VTP password: 89914640C8D90868B6A0D8103847A733
```

VTP の機能履歴と情報

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

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

表 4: VTP の機能履歴と情報

機能	リリース	機能情報
VTP の設定	Cisco IOS リリース 15.2(7)E1	この機能が導入されました。



第 2 章

VLAN の設定

- [VLAN の前提条件 \(25 ページ\)](#)
- [VLAN の制約事項 \(25 ページ\)](#)
- [VLAN について \(26 ページ\)](#)
- [VLAN の設定方法 \(31 ページ\)](#)
- [VLAN のモニタリング \(37 ページ\)](#)
- [設定例 \(39 ページ\)](#)
- [VLAN の設定の機能履歴と情報 \(40 ページ\)](#)

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 トランッキングプロトコル (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。
- スイッチは、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 256 の VLAN をサポートしています。

VLAN の制約事項

次に、VLAN を設定する際の制約事項を示します。

- 標準範囲の VLAN 設定の CPU 使用率が高いことを示す警告メッセージを回避するには、使用する VLAN を 256 までにすることを推奨します。多数のアクセス インターフェイスまたはトランク インターフェイスが同時にフラップすると、CPU 使用率が過度に高くなる可能性があります。

VLAN について

論理ネットワーク

VLANは、ユーザの物理的な位置に関係なく、機能、プロジェクトチーム、またはアプリケーションなどで論理的に分割されたスイッチドネットワークです。VLANは、物理LANと同じ属性をすべて備えていますが、同じLANセグメントに物理的に配置されていないエンドステーションもグループ化できます。どのスイッチポートもVLANに割り当てることができます。ユニキャスト、ブロードキャスト、およびマルチキャストパケットは、VLAN内のエンドステーションだけに転送およびフラッディングが行われます。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をサポートするスイッチを経由して伝送しなければなりません。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、スパン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。スイッチ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。この方法でスイッチ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。

スイッチは、スイッチ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する必要があります。

サポートされる VLAN

スイッチは、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 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。

VTPバージョン1およびバージョン2は、標準範囲のVLAN (VLAN ID 1～1005) だけをサポートします。これらのバージョンで1006～4094のVLAN IDを作成する場合は、スイッチをVTPトランスペアレントモードにする必要があります。Cisco IOS Release 12.2(52)SE以降ではVTPバージョン3をサポートします。VTPバージョン3は、VLAN範囲全体 (VLAN 1～4094) をサポートします。拡張範囲VLAN (VLAN 1006～4094) は、VTPバージョン3でのみサポートされます。拡張VLANがドメインに設定されている場合は、VTPバージョン3からVTPバージョン2に変換できません。

スイッチは、最大64のスパン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つずつスパンニングツリーインスタンスを使用できます。スイッチは、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 トランッキングのみをサポートします。

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 5: 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、あるデバイスのトランクポートに接続した別のデバイス上に1つまたは複数のトランクポートがなければなりません。
トランク (IEEE 802.1Q) • IEEE 802.1Q : 業界標準のトランッ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 のメンバーです。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。
ダイナミックアクセス	ダイナミックアクセスポートは1つの VLAN (VLAN ID が 1 ~ 4094) にのみ所属し、VLAN Member Policy Server (VMPS) によって動的に割り当てられます。 同一のデバイス上でダイナミックアクセスポートとトランクポートを使用できますが、ダイナミックアクセスポートは別のデバイスではなく、エンドステーションまたはハブに接続する必要があります。	VTP は必須です。 VMPS およびクライアントを同じ VTP ドメイン名で設定してください。 VTP に加入するには、別のデバイスのトランクポートに、デバイス上の少なくとも1つのトランクポートが接続されている必要があります。

メンバーシップモード	VLAN メンバーシップの特性	VTP の特性
音声 VLAN	音声 VLAN ポートは、Cisco IP Phone に接続し、電話に接続されたデバイスからの音声トラフィックに 1 つの VLAN を、データトラフィックに別の VLAN を使用するように設定されたアクセスポートです。	VTP は不要です。VTP は音声 VLAN に対して無効です。

VLAN コンフィギュレーションファイル

VLAN ID 1 ~ 1005 の設定は `vlan.dat` ファイル (VLAN データベース) に書き込まれます。この設定を表示するには、`show vlan` 特権 EXEC コマンドを入力します。`vlan.dat` ファイルはフラッシュメモリに格納されます。VTP モードがトランスペアレントモードの場合、こ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。

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

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

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



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

標準範囲 VLAN 設定時の注意事項

標準範囲 VLAN は、ID が 1 ～ 1005 の VLAN です。

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

- 標準範囲 VLAN は、1 ～ 1001 の番号で識別します。VLAN 番号 1002 ～ 1005 は、トークンリングおよび FDDI VLAN 専用です。
- VLAN 1 ～ 1005 の VLAN 設定は、常に VLAN データベースに格納されます。VTP モードがトランスペアレントモードの場合、VTP と VLAN の設定もスイッチ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。
- スイッチが 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、スイッチを VTP サーバモードまたは VTP トランスペアレントモードにしておく必要があります。スイッチが 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。
- スイッチは、トークンリングまたは FDDI メディアをサポートしません。スイッチは FDDI、FDDI-Net、TrCRF、または TrBRF トラフィックを伝送しませんが、VTP を介して VLAN 設定を伝播します。
- スイッチは 64 のスパニングツリーインスタンスをサポートします。スイッチのアクティブな VLAN 数が、サポートされているスパニングツリーインスタンス数より多い場合でも、スパニングツリーはサポートされている数の VLAN でのみ有効になり、残りの VLAN ではスパニングツリーは無効になります。

スイッチ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、そのスイッチ上にスパニングツリーが稼働しない VLAN が生成されます。そのスイッチのトランク 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、複数の隣接スイッチ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スイッチのトランク ポートに許可リストを設定することにより、このような可能性を防ぐことができます。

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

拡張範囲 VLAN 設定時の注意事項

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

拡張範囲 VLAN を作成するときは次の注意事項に従ってください。

- 拡張範囲の VLAN ID は、スイッチが 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。

VLAN のデフォルト設定

イーサネット VLAN のデフォルト設定

次の表に、イーサネット VLAN のデフォルト設定を記載します。



- (注) スイッチがサポートするのは、イーサネット インターフェイスだけです。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ため、FDDI およびトークンリング メディア固有の特性は、他のスイッチに対する VTP グローバル アドバタイズにのみ設定します。

表 6: イーサネット VLAN のデフォルトおよび範囲

パラメータ	デフォルト	範囲
VLAN ID	1	1 ～ 4094 (注) 拡張範囲 VLAN (VLAN ID 1006 ～ 4094) は、VTP バージョン 3 の VLAN データベースにのみ保存されます。
VLAN 名	VLANxxxx。xxxx は VLAN ID 番号に等しい 4 桁の数字 (先行ゼロを含む) です。	範囲なし

パラメータ	デフォルト	範囲
IEEE 802.10 SAID	100001 (100000 と VLAN ID の和)	1 ~ 4294967294
IEEE 802.10 SAID	1500	576 ~ 18190

VLAN のデフォルト設定

拡張範囲 VLAN については MTU サイズおよびリモート 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す。

VLAN の設定方法

標準範囲 VLAN の設定方法

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

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

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

イーサネット VLAN の作成または変更

VLAN データベース内の各イーサネット VLAN の ID は 4 桁の一意の数字で、1 ~ 1001 を指定できます。VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN 用に予約されています。標準範囲 VLAN を作成して VLAN データベースに追加するには、VLAN に番号および名前を割り当てます。



- (注) 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。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	vlan vlan-id 例： Device(config)# vlan 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 4	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 <i>vlan-id</i> 値が付加されます。たとえば、VLAN 4 のデフォルト

	コマンドまたはアクション	目的
		トの VLAN 名は VLAN0004 になります。
ステップ 5	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show vlan { name vlan-name id vlan-id} 例： Device# show vlan name test20 id 20	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

VLAN の削除

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

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



注意

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。

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

VLAN へのスタティック アクセス ポートの割り当て

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例 : Device(config)# interface gigabitethernet 1/0/1	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)# 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 gigabitethernet 1/0/1	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 gigabitethernet 1/0/1 switchport	表示された [Administrative Mode] フィールドおよび [Access Mode VLAN] フィールドの設定を確認します。

拡張範囲 VLAN の設定方法

VTP バージョン 1 およびバージョン 2 でスイッチが VTP トランスペアレント モード (VTP がディセーブル) の場合、拡張範囲 VLAN (1006~4094) を作成できます。VTP バージョンは、拡張範囲 VLAN をサーバモードおよびトランスペアレントモードでサポートします。サービスプロバイダーは拡張範囲 VLAN を使用することにより、インフラストラクチャを拡張して、多数の顧客に対応できます。拡張範囲 VLAN ID は、VLAN ID が許可されている **switchport** コマンドで使用できます。

VTP バージョン 1 または 2 での拡張範囲 VLAN の設定は VLAN データベースに格納されません。ただし、VTP モードがトランスペアレントであるため、スイッチの実行コンフィギュレーションファイルにストアされます。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するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。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 の作成

グローバルコンフィギュレーションモードで拡張範囲 VLAN を作成するには、**vlan** グローバルコンフィギュレーションコマンドを入力し、1006~4094 の VLAN ID を指定します。拡張範囲 VLAN には、デフォルトのイーサネット VLAN の特性と MTU サイズがあります。すべてのパラメータのデフォルト設定については、コマンドリファレンスに記載された **vlan** グローバルコンフィギュレーションコマンドの説明を参照してください。VTP バージョン 1 または 2 で、スイッチが VTP トランスペアレントモードでない場合に拡張範囲 VLAN ID を入力すると、VLAN コンフィギュレーションモードの終了時にエラーメッセージが生成され、拡張範囲 VLAN が作成されません。

VTP バージョン 1 および 2 では、拡張範囲 VLAN は VLAN データベースに保存されず、スイッチ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。拡張範囲 VLAN 設定をスイッチ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。VTP バージョン 3 は、拡張範囲 VLAN を VLAN データベースに保存します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバルコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	vtp mode transparent 例 : Device(config)# vtp mode transparent	デバイスを VTP トランスペアレントモードで設定し、VTP をディセーブルにします。 (注) この手順は、VTP バージョン 3 では不要です。
ステップ 4	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。
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 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 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。

VLAN のモニタリング

表 7: 特権 EXEC 表示コマンド

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

コマンド	目的
<pre>show vlan [brief group [group-name name] id vlan-id ifindex internal mtu name name summary]]</pre>	<p>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。</p> <ul style="list-style-type: none"> • brief : VTP VLAN のステータス概要を表示します。 • 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。 • summary : VLAN 情報の要約を表示します。

コマンド	目的
<pre>show vlan [access-log { config flow statistics } access-map name brief dot1q { tag native } filter [access-map vlan] group [group-name name] id vlan-id ifindex internal usage mtu name name summary]</pre>	<p>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。</p> <ul style="list-style-type: none"> • access-log : VACL ログギングを表示します。 • 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。 • summary : VLAN 情報の要約を表示します。

設定例

例 : VLAN 名の作成

次に、イーサネット VLAN 20 を作成し、test20 という名前を付け、VLAN データベースに追加する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

例：アクセスポートとしてのポートの設定

次に、VLAN 2 のアクセスポートとしてポートを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

例：拡張範囲 VLAN の作成

次に、すべてデフォルトの特性で拡張範囲 VLAN を新規作成し、VLAN コンフィギュレーションモードを開始して、新規 VLAN をスイッチのスタートアップ コンフィギュレーションファイルに保存する例を示します。

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

VLAN の設定の機能履歴と情報

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

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

表 8: VLAN の設定の機能履歴と情報

機能	リリース	機能情報
VLAN の設定	Cisco IOS リリース 15.2(7)E1	この機能が導入されました。



第 3 章

VLAN トランクの設定

- [VLAN トランクの前提条件](#) (41 ページ)
- [VLAN トランクについて](#) (42 ページ)
- [VLAN トランクの設定方法](#) (45 ページ)
- [VLAN トランキングの設定例](#) (58 ページ)
- [VLAN トランクの機能履歴と情報](#) (58 ページ)

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nk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。

一般的な制約事項

- ネイティブ VLAN タギングはサポートされておらず、`vlan dot1q tag native` コマンドは使用できません。

VLAN トランクについて

トランキングの概要

トランクは1つまたは複数のイーサネットスイッチインターフェイスと、ルータまたはスイッチなど別のネットワーク デバイス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。



(注) トランクを設定できるのは、1つのイーサネット インターフェイスまたは EtherChannel バンドルに対してです。

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。

レイヤ2 インターフェイス モード

表 9: レイヤ2 インターフェイス モード

モード	機能
switchport mode access	インターフェイス (アクセス ポート) を永続的な非トランキング モードにして、リンクの非トランク リンクへの変換をネゴシエートします。インターフェイスは、ネイバー インターフェイスがトランク インターフェイスかどうかに関係なく、非トランク インターフェイスになります。

モード	機能
switchport mode dynamic auto	インターフェイスがリンクをトランク リンクに変換できるようにします。インターフェイスは、ネイバーインターフェイスが trunk または desirable モードに設定されている場合、トランクインターフェイスになります。すべてのイーサネット インターフェイスのデフォルトのスイッチポートモードは dynamic auto です。
switchport mode dynamic desirable	インターフェイスがリンクのトランク リンクへの変換をアクティブに実行するようにします。インターフェイスは、ネイバーインターフェイスが trunk 、 desirable または auto モードに設定されている場合、トランクインターフェイスになります。
switchport mode trunk	インターフェイスを永続的なトランキングモードにして、ネイバーリンクのトランク リンクへの変換をネゴシエートします。インターフェイスは、ネイバーインターフェイスがトランク インターフェイスでない場合でも、トランク インターフェイスになります。
switchport nonegotiate	インターフェイスが DTP フレームを生成しないようにします。このコマンドは、インターフェイス スwitch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。

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 VLANID (1~4094) が許可されます。ただし、許可リストから VLAN を削除することにより、それらの VLAN からのトラフィックがトランク上を流れないようにすることができます。

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

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

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

VTP が新しい VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されていない場合には、トランク ポートはその VLAN のメンバにはなりません。

トランク ポートでの負荷分散

負荷分散により、スイッチ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ず。STP は通常、ループを防止するために、スイッチ間で 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スイッチ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スイッチにも、2 台の異なるスイッチにも接続できます。

STP プライオリティによるネットワーク負荷分散

同一スイッチ上の 2 つのポートがループを形成すると、スイッチは STP ポートプライオリティを使用して、どのポートをイネーブルとし、どのポートをブロッキングステートとするかを判断します。パラレル トランク ポートにプライオリティを設定することにより、そのポートに、特定の VLAN のすべてのトラフィックを伝送させることができます。VLAN に対するプライオリティの高い（値の小さい）トランク ポートがその VLAN のトラフィックを転送します。同じ VLAN に対してプライオリティの低い（値の大きい）トランク ポートは、その VLAN に対してブロッキングステートのままです。1 つのトランク ポートが特定の VLAN に関するすべてのトラフィックを送受信することになります。

STP パス コストによるネットワーク負荷分散

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

機能の相互作用

トランッ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、スイッチは、入力された設定をグループ内のすべてのポートに伝播します。
 - 許可 VLAN リスト。

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

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

- トランク ポートで IEEE 802.1X をイネーブルにしようとする、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、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。

レイヤ2イーサネットインターフェイス VLAN のデフォルト設定

次の表に、レイヤ2イーサネットインターフェイス VLAN のデフォルト設定を記載します。

表 10: レイヤ2イーサネットインターフェイス VLAN のデフォルト設定

機能	デフォルト設定
インターフェイス モード	switchport mode dynamic auto
VLAN 許容範囲	VLAN 1 ~ 4094
プルーニングに適格な VLAN 範囲	VLAN 2 ~ 1001
デフォルト VLAN (アクセス ポート用)	VLAN 1
ネイティブ VLAN (IEEE 802.1Q トランク用)	VLAN 1

VLAN トランクの設定方法

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

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

ンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

トランク ポートとしてのイーサネット インターフェイスの設定

トランク ポートの設定

トランク ポートは VTP アドバタイズを送受信するので、VTP を使用する場合は、スイッチ上で少なくとも 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。

手順

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

	コマンドまたはアクション	目的
		<p>クとして設定します。これはデフォルトです。</p> <ul style="list-style-type: none"> • dynamic desirable : ネイバー インターフェイスが trunk、desirable、または auto モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。 • trunk : ネイバー インターフェイスがトランク インターフェイスでない場合でも、インターフェイスを永続的なトランキング モードに設定して、リンクをトランク リンクに変換するようにネゴシエートします。
ステップ 5	switchport access vlan <i>vlan-id</i> 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 <i>vlan-id</i> 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 <i>interface-id</i> switchport 例 : Device # show interfaces gigabitethernet 1/0/1 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 <i>interface-id</i> trunk 例 :	インターフェイスのトランクの設定を表示します。

	コマンドまたはアクション	目的
	Device# show interfaces gigabitethernet 1/0/2 trunk	
ステップ 10	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

トランクでの許可 VLAN の定義

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	設定するポートを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	switchport mode trunk 例： Device(config-if)# switchport mode trunk	インターフェイスを VLAN トランクポートとして設定します。

	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 interfaces interface-id switchport 例 : Device# show interfaces gigabitethernet 1/0/2 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 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。

プルーニング適格リストの変更

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例 : Device(config)# interface fastethernet0/1-48	VLAN プルーニングを適用するトランク ポートを選択し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	switchport trunk pruning vlan {add except none remove} vlan-list [,vlan [,vlan [,...]]]	<p>トランクからのプルーンングを許可する VLAN のリストを設定します。</p> <p>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。</p> <p>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）はプルーンングできません。</p> <p>プルーンング不適格の VLAN は、フラッディングトラフィックを受信します。</p> <p>デフォルトでは、プルーンングが許可される VLAN のリストには、VLAN 2 ~ 1001 が含まれます。</p>
ステップ 5	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show interfaces interface-id switchport 例： Device# show interfaces gigabitethernet 0/2 switchport	表示された [Pruning VLANs Enabled] フィールドの設定を確認します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	（任意）コンフィギュレーションファイルに設定を保存します。

タグなしトラフィック用ネイティブ VLAN の設定

IEEE 802.1Q タギングが設定されたトランクポートは、タグ付きトラフィックおよびタグなしトラフィックの両方を受信できます。デフォルトでは、タグなしトラフィックは、ポートに設定されたネイティブ VLAN に転送されます。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、スイッチはそのパケットをタグ付きで送信します。

手順

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

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

トランク ポートの負荷分散の設定

STP ポート プライオリティによる負荷分散の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	vtp 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	スイッチ A を VTP サーバとして設定します。
ステップ 5	end 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device (config) # end	
ステップ 6	show vtp status 例 : Device# show vtp status	スイッチ A および B の両方で、VTP 設定を確認します。 表示された <i>VTP Operating Mode</i> および <i>VTP Domain Name</i> フィールドをチェックします。
ステップ 7	show vlan 例 : Device# show vlan	スイッチ A のデータベースに VLAN が存在していることを確認します。
ステップ 8	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 9	interface interface-id 例 : Device (config) # interface gigabitethernet 1/0/2	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) # 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 gigabitethernet 1/0/2 switchport	VLAN の設定を確認します。

	コマンドまたはアクション	目的
ステップ 13	スイッチの 2 番目のポートについて、スイッチ A 上で上記のステップを繰り返します。	
ステップ 14	スイッチ B で前述の手順を繰り返し、スイッチ 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 がスイッチ B に VTP および VLAN 情報を渡します。このコマンドは、スイッチ B が VLAN 設定を学習したことを確認します。
ステップ 16	configure terminal 例： Device# configure terminal	スイッチ A で、グローバル コンフィギュレーションモードを開始します。
ステップ 17	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	STP のポートプライオリティを設定するインターフェイスを定義し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 18	spanning-tree vlan vlan-range port-priority priority-value 例： Device(config-if)# spanning-tree vlan 8-10 port-priority 16	指定された VLAN 範囲にポートプライオリティを割り当てます。0 ~ 240 のポートプライオリティ値を入力します。ポートプライオリティ値は 16 ずつ増分します。
ステップ 19	exit 例： 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 gigabitethernet 1/0/2	STP のポートプライオリティを設定するインターフェイスを定義し、インターフェイスコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 21	spanning-tree vlan <i>vlan-range</i> port-priority <i>priority-value</i> 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) # end	特権 EXEC モードに戻ります。
ステップ 23	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 24	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

STP パス コストによる負荷分散の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	interface interface-id 例 : Device(config)# interface gigabitethernet 1/0/1	トランクとして設定するインターフェイスを定義し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 4	switchport mode trunk 例 : Device(config-if)# switchport mode trunk	ポートをトランクポートとして設定します。
ステップ 5	exit 例 : Device(config-if)# exit	グローバル コンフィギュレーションモードに戻ります。
ステップ 6	スイッチ A の 2 番目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、スイッチ A がもう一方のスイッチから VTP 情報を受信します。このコマンドは、スイッチ 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。

	コマンドまたはアクション	目的
ステップ 11	interface interface-id 例 : Device (config) # interface gigabitethernet 1/0/1	STP コストを設定するインターフェイスを定義し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 12	spanning-tree vlan vlan-range cost cost-value 例 : Device (config-if) # spanning-tree vlan 2-4 cost 30	VLAN 2 ~ 4 のスパニングツリー パス コストを 30 に設定します。
ステップ 13	end 例 : Device (config-if) # end	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	スイッチ 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。

VLAN トランキングの設定例

例：トランク ポートの設定

次に、IEEE 802.1Q トランクとしてポートを設定する例を示します。この例では、ネイバーインターフェイスが IEEE 802.1Q トランキングをサポートするように設定されていることを前提としています。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/0/2
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# end
```

例：ポートからの VLAN の削除

次に、ポートの許可 VLAN リストから VLAN 2 を削除する例を示します。

```
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

VLAN トランクの機能履歴と情報

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

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

表 11: VLAN トランクの機能履歴と情報

機能	リリース	機能情報
VLAN トランクの設定	Cisco IOS リリース 15.2(7)E1	この機能が導入されました。



第 4 章

音声 VLAN の設定

- 音声 VLAN の前提条件 (59 ページ)
- 音声 VLAN の制約事項 (60 ページ)
- 音声 VLAN に関する情報 (60 ページ)
- 音声 VLAN の設定方法 (63 ページ)
- 音声 VLAN のモニタリング (65 ページ)
- 設定例 (65 ページ)
- 音声 VLAN の機能履歴と情報 (66 ページ)

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 設定はスイッチ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 をイネーブルにする前に、**mls qos** グローバル コンフィギュレーション コマンドを入力してスイッチ上で QoS をイネーブルに設定し、さらに **mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力してポートの信頼状態を **trust** に設定しておくことを推奨します。Auto-QoS 機能を使用すると、これらは自動的に設定されます。
- Cisco IP 電話に接続しているスイッチポート上の Cisco Discovery Protocol をイネーブルにし、Cisco IP 電話に設定を送信する必要があります (Cisco Discovery Protocol は、デフォルトではすべてのスイッチ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。スイッチを Cisco IP Phone に接続すると、IP Phone はレイヤ 3 IP precedence 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、このスイッチでは、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、スイッチ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 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プライオリティを信頼するように、または上書きするようにスイッチを設定できます。

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。スイッチ上のアクセスポートを設定して、Cisco Discovery Protocol パケットを送信させることができます。Cisco Discovery Protocol には、接続する IP Phone に対して、次のいずれかの方法でスイッチに音声トラフィックを送信するように指定します。

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



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

Cisco IP Phone のデータトラフィック

スイッチは、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た、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。Cisco Discovery Protocol パケットを送信するよう、スイッチ上のレイヤ 2 アクセスポートを設定できます。Cisco Discovery Protocol パケットは、接続する IP Phone に対して、次のいずれかのモードで IP Phone アクセスポートを設定するよう指示します。

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



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

音声 VLAN 設定時の注意事項

- Cisco IP Phone は、PC または他のデバイスとの接続もサポートしているので、スイッチを 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 での通信が適切に行えるように、音声 VLAN はスイッチ上で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) スイッチは、シスコ先行標準の受電デバイスまたは IEEE 802.3af 準拠の受電デバイスが AC 電源から電力を供給されていない場合に、それらの受電デバイスに自動的に電力を供給できます。
- 音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。
- Cisco IP Phone とその IP Phone に接続されたデバイスが同じ VLAN 上にある場合、両方とも同じ IP サブネットに属していなければなりません。次の条件が満たされている場合は、同じ VLAN 上にあります。
 - 両方とも IEEE 802.1p またはタグなしフレームを使用する。
 - Cisco IP Phone が IEEE 802.1p フレームを使用し、デバイスがタグなしフレームを使用する。
 - Cisco IP Phone がタグなしフレームを使用し、デバイスが IEEE 802.1p フレームを使用する。

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



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

- 保護ポート。
- SPAN 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リングする場合、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 のデフォルト設定

音声 VLAN 機能は、デフォルトではディセーブルに設定されています。

音声 VLAN 機能がイネーブルの場合、すべてのタグなしトラフィックはポートのデフォルトの CoS プライオリティに従って送信されます。

IEEE 802.1p または IEEE 802.1Q のタグ付きトラフィックでは、CoS 値が信頼されません。

音声 VLAN の設定方法

Cisco IP Phone の音声トラフィックの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	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	mls qos trust cos 例： Device(config-if)# mls qos trust cos	パケットの CoS 値を使用して着信トラフィック パケットを分類するよう、インターフェイスを設定します。タグなしパケットの場合、ポートのデフォルト CoS 値が使用されます。

	コマンドまたはアクション	目的
		(注) ポートの信頼状態を設定する前に、最初に mls qos グローバルコンフィギュレーションコマンドを使用して、QoS をグローバルでイネーブルに設定しておく必要があります。
ステップ 5	switchport voice {vlan {vlan-id dot1p none untagged}} 例 : <pre>Device(config-if)# switchport voice vlan dot1p</pre>	音声 VLAN を設定します。 <ul style="list-style-type: none"> • 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 フレームを受け付けるよう、スイッチを設定します。デフォルトでは、スイッチは VLAN 0 のタグが付いたすべての音声およびデータトラフィックをドロップします。802.1p に対応するよう設定されると、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用してトラフィックを転送します。 • none : IP Phone が独自の設定を使用してタグなしの音声トラフィックを送信するようにします。 • untagged : タグなしの音声トラフィックを送信するように電話を設定します。
ステップ 6	end 例 : <pre>Device(config-if)# end</pre>	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	<p>次のいずれかを使用します。</p> <ul style="list-style-type: none"> • show interfaces <i>interface-id</i> switchport • show running-config interface <i>interface-id</i> <p>例 :</p> <pre>Device# show interfaces gigabitethernet 1/0/1 switchport</pre> <p>または</p> <pre>Device# show running-config interface gigabitethernet 1/0/1</pre>	音声 VLAN の設定、または QoS および音声 VLAN の設定を確認します。
ステップ 8	<p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

音声 VLAN のモニタリング

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

設定例

例 : Cisco IP Phone の音声トラフィックの設定

次の例では、CoS 値を使用して着信トラフィックを分類し、VLAN ID 0 のタグが付いた音声およびデータプライオリティトラフィックを受け付けるよう、Cisco IP Phone に接続しているポートを設定する方法について示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# switchport voice vlan dot1p
Switch(config-if)# end
```

ポートをデフォルトの設定に戻す場合は、**no switchport voice 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。

音声 VLAN の機能履歴と情報

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

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

表 12: 音声 VLAN の機能履歴と情報

機能	リリース	機能情報
音声 VLAN の設定	Cisco IOS リリース 15.2(7)E1	この機能が導入されました。