VLAN コンフィギュレーション ガイド、Cisco IOS XE リリース 3SE（Catalyst 3850 スイッチ）

初版：2013 年 01 月 29 日

最終更新：2013 年 10 月 07 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/

Text Part Number: OL-26762-02

【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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

CiscoおよびCisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、http://www.cisco.com/go/trademarks でご確認いただけます。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

© 2013 Cisco Systems, Inc. All rights reserved.

目 次

はじめに ix

表記法 ix

関連資料 xi

マニュアルの入手方法およびテクニカル サポート xi

コマンドライン インターフェイスの使用 1

コマンドライン インターフェイスの使用に関する情報 1

コマンド モード 1

ヘルプ システムの使用 5

コマンドの省略形 6

コマンドの no 形式および default 形式 6

CLI のエラー メッセージ 6

コンフィギュレーション ロギング 7

CLI を使用して機能を設定する方法 8

コマンド履歴の設定 8

コマンド履歴バッファ サイズの変更 8

コマンドの呼び出し 8

コマンド履歴機能の無効化 9

編集機能の有効化および無効化 9

キー入力によるコマンドの編集 10

画面幅よりも長いコマンドラインの編集 12

show および more コマンド出力の検索およびフィルタリング 13

スイッチ スタックでの CLI へのアクセス 13

コンソール接続または Telnet 経由で CLI にアクセスする 14

Web グラフィカル ユーザ インターフェイスの使用 15

Web GUI の使用に関する前提条件 15

Web GUI の使用に関する情報 15

Web GUI の機能 16
スイッチのコンソール ポートの接続 17
Web GUI へのログイン 17
Web モードおよびセキュア Web モードの有効化 17
スイッチ Web GUI の設定 18
VTP の設定 23
機能情報の確認 23
VTP の前提条件 24
VTP の制約事項 24
VTP の概要 25
VTP 25
VTP ドメイン（VTP domain） 25
VTP モード 26
VTP アドバタイズ 27
VTP バージョン 2 28
VTP バージョン 3 29
VTP プルーニング 30
VTP とスイッチ スタック 31
VTP 設定時の注意事項 32
VTP の設定要件 32
VTP の設定 32
VTP 設定のためのドメイン名 33
VTP ドメインのパスワード 33
VTP Version 34
VTP の設定方法 35
VTP モードの設定（CLI） 35
VTP バージョン 3 のパスワードの設定（CLI） 37
VTP バージョン 3 のプライマリ サーバの設定（CLI） 39
VTP バージョンのイネーブル化（CLI） 39
VTP プルーニングのイネーブル化（CLI） 41
ポート単位の VTP の設定（CLI） 43
VTP ドメインへの VTP クライアント スイッチの追加（CLI） 44
VTP のモニタ 47

VTP の設定例 48
例：スイッチをプライマリ サーバとして設定する 48
次の作業 48
その他の参考資料 48
VTP の機能履歴と情報 50
VLAN の設定 51
機能情報の確認 51
VLAN の前提条件 51
VLAN の制約事項 52
VLAN について 52
論理ネットワーク 52
サポートされる VLAN 53
VLAN ポート メンバーシップ モード 54
VLAN コンフィギュレーション ファイル 55
標準範囲 VLAN 設定時の注意事項 56
拡張範囲 VLAN 設定時の注意事項 57
VLAN の設定方法 58
標準範囲 VLAN の設定方法 58
イーサネット VLAN の作成または変更（CLI） 58
VLAN の削除（CLI） 61
VLAN へのスタティック アクセス ポートの割り当て（CLI） 63
拡張範囲 VLAN の設定方法 64
拡張範囲 VLAN の作成（CLI） 65
VLAN の設定方法（GUI） 67
レイヤ 2 VLAN の作成（GUI） 67
レイヤ 3 インターフェイスの作成（GUI） 67
レイヤ 2 VLAN の表示（GUI） 68
レイヤ 3 インターフェイスの表示（GUI） 69
レイヤ 2 VLAN の削除（GUI） 69
レイヤ 3 インターフェイスの削除（GUI） 70
VLAN のモニタリング 71
次の作業 72

その他の参考資料 72
VLAN の機能履歴と情報 74
VLAN グループの設定 77
機能情報の確認 77
VLAN グループの前提条件 77
VLAN グループの制約事項 78
VLAN グループについて 78
VLAN グループの設定方法 79
VLAN グループの作成（CLI） 79
VLAN グループの削除（CLI） 79
VLAN グループの作成（GUI） 80
WLAN への VLAN グループの追加（CLI） 81
WLAN への VLAN グループの追加（GUI） 82
VLAN グループの削除（GUI） 82
VLAN グループの VLAN の表示（CLI） 83
VLAN グループの表示（GUI） 83
次の作業 83
その他の参考資料 84
VLAN グループの機能履歴と情報 86
VLAN トランクの設定 87
機能情報の確認 87
VLAN トランクの前提条件 87
VLAN トランクの制約事項 88
VLAN トランクについて 88
トランキングの概要 88
トランキング モード 89
レイヤ 2 インターフェイス モード 89
トランクでの許可 VLAN 90
トランク ポートでの負荷分散 91
STP プライオリティによるネットワーク負荷分散 91
STP パス コストによるネットワーク負荷分散 92
機能の相互作用 93

VLAN トランクの設定方法 94
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 94
トランク ポートの設定（CLI） 94
トランクでの許可 VLAN の定義（CLI） 97
プルーニング適格リストの変更（CLI） 98
タグなしトラフィック用ネイティブ VLAN の設定（CLI） 100
トランク ポートの負荷分散の設定 101
STP ポート プライオリティによる負荷分散の設定（CLI） 101
STP パス コストによる負荷分散の設定（CLI） 106
次の作業 108
その他の参考資料 109
VLAN トランクの機能履歴と情報 110
音声 VLAN の設定 111
機能情報の確認 111
音声 VLAN の前提条件 111
音声 VLAN の制約事項 112
音声 VLAN に関する情報 112
音声 VLAN 112
Cisco IP Phone の音声トラフィック 113
Cisco IP Phone のデータ トラフィック 114
音声 VLAN 設定時の注意事項 114
音声 VLAN の設定方法 116
Cisco IP Phone の音声トラフィックの設定（CLI） 116
着信データ フレームのプライオリティ設定（CLI） 118
音声 VLAN のモニタリング 120
次の作業 120
その他の参考資料 120
音声 VLAN の機能履歴と情報 122

はじめに

- 表記法，ix ページ
- 関連資料，xi ページ
- マニュアルの入手方法およびテクニカル サポート，xi ページ

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します（ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
Italic フォント	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、イタリック体で示しています。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
`太字の courier` フォント	ユーザが入力したテキストは、太字の courier フォントで示しています。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3 つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。

表記法	説明
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	どれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス　時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告　安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。Statement 1071

これらの注意事項を保管しておいてください。

関連資料

（注）　スイッチをインストールまたはアップグレードする前に、スイッチのリリース ノートを参照してください。

- 次の URL にある Cisco Catalyst 3850 スイッチ のマニュアル：

  Http://www.cisco.com/go/cat3850_docs

- 次の URL にある Cisco SFP、SFP+、および QSFP+ モジュールのマニュアル（互換性マトリクスを含む）：

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html

- 次の URL にある Cisco Validated Design（CVD）のマニュアル：

  http://www.cisco.com/go/designzone

- 次の URL にあるエラー メッセージ デコーダ：

  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定するこ

ともできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

コマンドライン インターフェイスの使用

- コマンドライン インターフェイスの使用に関する情報，1 ページ
- CLI を使用して機能を設定する方法，8 ページ

コマンドライン インターフェイスの使用に関する情報

コマンド モード

Cisco IOS ユーザ インターフェイスは、いくつかのモードに分かれています。使用可能なコマンドは、現在のモードによって異なります。各コマンド モードで使用できるコマンドのリストを取得するには、システム プロンプトで疑問符（?）を入力します。

CLI セッションはコンソール接続、Telnet、SSH、またはブラウザを使用することによって開始できます。

セッションを開始するときは、ユーザ モード（別名ユーザ EXEC モード）が有効です。ユーザ EXEC モードでは、限られた一部のコマンドしか使用できません。たとえばユーザ EXEC コマンドの大部分は、**show** コマンド（現在のコンフィギュレーション ステータスを表示する）、**clear** コマンド（カウンタまたはインターフェイスをクリアする）などのように、1 回限りのコマンドです。ユーザ EXEC コマンドは、スイッチをリブートするときには保存されません。

すべてのコマンドにアクセスするには、特権 EXEC モードを開始する必要があります。特権 EXEC モードを開始するには、通常、パスワードが必要です。このモードでは、任意の特権 EXEC コマンドを入力でき、また、グローバル コンフィギュレーション モードを開始することもできます。

コンフィギュレーション モード（グローバル、インターフェイス、およびライン）を使用して、実行コンフィギュレーションを変更できます。設定を保存した場合はこれらのコマンドが保存され、スイッチをリブートするときに使用されます。各種のコンフィギュレーション モードにアクセスするには、まずグローバル コンフィギュレーション モードを開始する必要があります。グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コンフィギュレーション モードを開始できます。

次の表に、主要なコマンド モード、各モードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法を示します。

表 *1*：コマンド モードの概要

モード	Access Method	プロンプト	終了方法	モードの用途
ユーザ EXEC	Telnet、SSH、またはコンソールを使用してセッションを開始します。	`Switch>`	**logout** または **quit** を入力します。	このモードを使用して次の作業を行います。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで、**enable** コマンドを入力します。	`Switch#`	**disable** を入力して終了します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure** コマンドを入力します。	`Switch(config)#`	終了して特権 EXEC モードに戻るには、**exit** または **end** コマンドを入力するか、Ctrl+Z を押します。	このモードは、スイッチ全体に適用するパラメータを設定する場合に使用します。
VLAN コンフィギュレーション	グローバル コンフィギュレーション モードで、**vlan** *vlan-id* コマンドを入力します。	`Switch(config-vlan)#`	グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	

モード	Access Method	プロンプト	終了方法	モードの用途
				このモードを使用して、VLAN（仮想LAN）パラメータを設定します。VTPモードがトランスペアレントであるときは、拡張範囲 VLAN（VLAN ID が 1006以上）を作成して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設定を保存できます。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、**interface** コマンドを入力し、インターフェイスを指定します。	`Switch(config-if)#`	終了してグローバル コンフィギュレーションモードに戻るには、**exit** を入力します。 特権EXECモードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、イーサネット ポートのパラメータを設定します。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードで、**line vty** または **line console** コマンドを使用して回線を指定します。	`Switch(config-line)#`	終了してグローバル コンフィギュレーションモードに戻るには、**exit** を入力します。 特権EXECモードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、端末回線のパラメータを設定します。

ヘルプ システムの使用

システム プロンプトに疑問符（?）を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。また、任意のコマンドについて、関連するキーワードおよび引数の一覧を表示することもできます。

手順の概要

1. **help**
2. *abbreviated-command-entry***?**
3. コマンドの先頭部分 <Tab>
4. **?**
5. *command* **?**
6. *command keyword* **?**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**help** 例： `Switch# help`	コマンド モードのヘルプ システムの簡単な説明を表示します。

ステップ 2	*abbreviated-command-entry***?**
	
	例：
	`Switch# di?`
	`dir disable disconnect`
		特定のストリングで始まるコマンドのリストを表示します。

ステップ 3	コマンドの先頭部分 <Tab>
	
	例：
	`Switch# sh conf<tab>`
	`Switch# show configuration`
		特定のコマンド名を補完します。

ステップ 4	**?** 例： `Switch> ?`	特定のコマンド モードで使用可能なすべてのコマンドをリストします。
ステップ 5	*command* **?** 例： `Switch> show ?`	コマンドに関連するキーワードを一覧表示します。

	コマンドまたはアクション	目的

ステップ 6	*command keyword* **?**
	
	例：
	`Switch(config)# cdp holdtime ?`
	`  <10-255> Length of time (in sec) that receiver must keep this packet`
		キーワードに関連する引数を一覧表示します。

コマンドの省略形

スイッチでコマンドが一意に認識される長さまでコマンドを入力します。

show configuration 特権 EXEC コマンドを省略形で入力する方法を次に示します。

```
Switch# show conf
```

コマンドの no 形式および default 形式

大部分のコンフィギュレーション コマンドに、**no** 形式があります。**no** 形式は一般に、特定の機能または動作をディセーブルにする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスのシャットダウンが取り消されます。**no** キーワードなしでコマンドを使用すると、ディセーブルにされた機能を再度イネーブルにしたり、デフォルトでディセーブルになっている機能をイネーブルにすることができます。

コンフィギュレーション コマンドには、**default** 形式もあります。コマンドの **default** 形式は、コマンドの設定値をデフォルトに戻します。大部分のコマンドはデフォルトでディセーブルに設定されているので、**default** 形式は **no** 形式と同じになります。ただし、デフォルトでイネーブルに設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。これらのコマンドについては、**default** コマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

CLI のエラー メッセージ

次の表に、CLI を使用してスイッチを設定するときに表示される可能性のあるエラー メッセージの一部を紹介します。

表 *2*：*CLI* の代表的なエラー メッセージ

エラー メッセージ	意味	ヘルプの表示方法
`% Ambiguous command: "show con"`	スイッチがコマンドとして認識できるだけの文字数が入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを入れません。 コマンドとともに使用できるキーワードが表示されます。
`% Incomplete command.`	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。
`% Invalid input detected at '^' marker.`	コマンドの入力ミスです。間違っている箇所をキャレット（^）記号で示しています。	疑問符（?）を入力すると、そのコマンド モードで利用できるすべてのコマンドが表示されます。 コマンドとともに使用できるキーワードが表示されます。

コンフィギュレーション ロギング

スイッチの設定変更を記録して表示させることができます。Configuration Change Logging and Notification 機能を使用することで、セッションまたはユーザ ベースごとに変更内容をトラッキングできます。ログに記録されるのは、適用された各コンフィギュレーション コマンド、コマンドを入力したユーザ、コマンドの入力時間、コマンドに対するパーサからのリターン コードです。この機能には、登録しているアプリケーションの設定が変更されるときに通知される非同期通知方式もあります。Syslog へこの通知を送信することも選択できます。

（注） CLI または HTTP の変更のみがログとして記録されます。

CLI を使用して機能を設定する方法

コマンド履歴の設定

入力したコマンドは、ソフトウェア側にコマンド履歴として残されます。コマンド履歴機能は、アクセスコントロールリストの設定時など、長い複雑なコマンドまたはエントリを何度も入力しなければならない場合、特に便利です。必要に応じて、この機能をカスタマイズできます。

コマンド履歴バッファ サイズの変更

デフォルトでは、スイッチは履歴バッファにコマンドライン10行を記録します。現在の端末セッションまたは特定回線のすべてのセッションで、この数を変更できます。この手順は任意です。

手順の概要

1. **terminal history** [**size** *number-of-lines*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal history** [**size** *number-of-lines*] 例： `Switch# terminal history size 200`	特権 EXEC モードで現在のターミナル セッション中にスイッチが記録するコマンドラインの数を変更します。サイズは 0 から 256 までの間で設定できます。

コマンドの呼び出し

履歴バッファにあるコマンドを呼び出すには、次の表に示すいずれかの操作を行います。これらの操作は任意です。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

手順の概要

1. **Ctrl-P** または **up arrow** キーを使用します。
2. **Ctrl-N** または **down arrow** キーを使用します。
3. **show history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**Ctrl-P** または **up arrow** キーを使用します。	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。
ステップ 2	**Ctrl-N** または **down arrow** キーを使用します。	Ctrl+P または↑キーでコマンドを呼び出した後で、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。
ステップ 3	**show history** 例： `Switch# show history`	特権 EXEC モードで、直前に入力したコマンドをいくつか表示します。表示されるコマンドの数は、**terminal history** グローバル コンフィギュレーション コマンドおよび **history** ライン コンフィギュレーション コマンドの設定値によって制御されます。

コマンド履歴機能の無効化

コマンド履歴機能は、自動的にイネーブルになっています。現在の端末セッションまたはコマンドラインでディセーブルにできます。この手順は任意です。

手順の概要

1. **terminal no history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal no history** 例： `Switch# terminal no history`	特権 EXEC モードで現在のターミナルセッション中のこの機能を無効にします。

編集機能の有効化および無効化

拡張編集モードは自動的にイネーブルに設定されますが、ディセーブルにしたり、再びイネーブルにしたりできます。

手順の概要

1. **terminal editing**
2. **terminal no editing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal editing** 例： `Switch# terminal editing`	特権 EXEC モードで現在のターミナルセッションにおける拡張編集モードを再び有効にします。
ステップ 2	**terminal no editing** 例： `Switch# terminal no editing`	特権 EXEC モードで現在のターミナルセッションにおける拡張編集モードを無効にします。

キー入力によるコマンドの編集

キーストロークは、コマンドラインの編集に役立ちます。これらのキーストロークは任意です。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

表 *3*：編集コマンド

編集コマンド	説明
Ctrl-B または**left arrow** キーを使用します。	カーソルを 1 文字後退させます。
Ctrl-F または**right arrow** キーを使用します。	カーソルを 1 文字前進させます。
Ctrl-A	コマンドラインの先頭にカーソルを移動します。
Ctrl-E	カーソルをコマンド ラインの末尾に移動します。
Esc B	カーソルを 1 単語後退させます。
Esc F	カーソルを 1 単語前進させます。

Ctrl-T	カーソルの左にある文字を、カーソル位置の文字と置き換えます。
Delete または **Backspace** キー	カーソルの左にある文字を消去します。
Ctrl-D	カーソル位置にある文字を削除します。
Ctrl-K	カーソル位置からコマンドラインの末尾までのすべての文字を削除します。
Ctrl-U または **Ctrl-X**	カーソル位置からコマンドラインの先頭までのすべての文字を削除します。
Ctrl-W	カーソルの左にある単語を削除します。
Esc D	カーソルの位置から単語の末尾までを削除します。
Esc C	カーソル位置のワードを大文字にします。
Esc L	カーソルの場所にある単語を小文字にします。
Esc U	カーソルの位置から単語の末尾までを大文字にします。
Ctrl-V または **Esc Q**	特定のキーストロークを実行可能なコマンド（通常はショートカット）として指定します。
Return キー	1 行または 1 画面下へスクロールして、端末画面に収まりきらない表示内容を表示させます。 （注） **show** コマンドの出力など、端末画面に一度に表示できない長い出力では、More プロンプトが使用されます。More プロンプトが表示された場合は、Return キーおよび Space キーを使用してスクロールできます。
Space bar	1 画面分下にスクロールします。
Ctrl-L または **Ctrl-R**	スイッチから画面に突然メッセージが出力された場合に、現在のコマンドラインを再表示します。

画面幅よりも長いコマンドラインの編集

画面上で 1 行分を超える長いコマンドラインについては、コマンドのラップアラウンド機能を使用できます。カーソルが右マージンに達すると、そのコマンドラインは10文字分だけ左へシフトされます。コマンドラインの先頭から10文字までは見えなくなりますが、左へスクロールして、コマンドの先頭部分の構文をチェックできます。これらのキー操作は任意です。

コマンドの先頭にスクロールして入力内容をチェックするには、**Ctrl-B**キーまたは←キーを繰り返し押します。コマンドラインの先頭に直接移動するには、**Ctrl-A**を押します。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

次に、画面上で 1 行を超える長いコマンドラインを折り返す例を示します。

手順の概要

1. **access-list**
2. **Ctrl-A**
3. **Return** キー

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**access-list**
	
	例：
	`Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35`
	`Switch(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25`
	`Switch(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq`
	`Switch(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45`
		1 行分を超えるグローバル コンフィギュレーション コマンド入力を表示します。
		最初にカーソルが行末に達すると、その行は 10 文字分だけ左へシフトされ、再表示されます。ドル記号（$）は、その行が左へスクロールされたことを表します。カーソルが行末に達するたびに、その行は再び 10 文字分だけ左へシフトされます。

ステップ 2	**Ctrl-A** 例： `Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$`	完全な構文をチェックします。 行末に表示されるドル記号（$）は、その行が右へスクロールされたことを表します。
ステップ 3	**Return** キー	コマンドを実行します。

	コマンドまたはアクション	目的
		ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。画面の幅が異なる場合は、**terminal width** 特権 EXEC コマンドを使用して端末の幅を設定します。 ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンドエントリを呼び出して変更できます。

show および more コマンド出力の検索およびフィルタリング

show および **more** コマンドの出力を検索およびフィルタリングできます。この機能は、大量の出力をソートする場合や、出力から不要な情報を除外する場合に役立ちます。これらのコマンドの使用は任意です。

手順の概要

1. {**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	{**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*
	
	例：
	`Switch# show interfaces | include protocol`
	`Vlan1 is up, line protocol is up`
	`Vlan10 is up, line protocol is down`
	`GigabitEthernet1/0/1 is up, line protocol is down`
	`GigabitEthernet1/0/2 is up, line protocol is up`
		出力を検索およびフィルタリングします。
		文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、**output** を含む行は表示されませんが、**output** を含む行は表示されます。

スイッチ スタックでの CLI へのアクセス

CLI にはコンソール接続、Telnet、SSH、またはブラウザを使用することによってアクセスできます。

スイッチ スタックおよびスタック メンバ インターフェイスは、アクティブ スイッチを経由して管理します。スイッチごとにスタック メンバを管理することはできません。1 つまたは複数のスタック メンバーのコンソール ポートまたはイーサネット管理ポートを経由してアクティブ スイッチへ接続できます。アクティブ スイッチで複数の CLI セッションを使用する場合は注意してくだ

さい。1 つのセッションで入力したコマンドは、別のセッションには表示されません。したがって、コマンドを入力したセッションを追跡できない場合があります。

（注） スイッチ スタックを管理する場合は、1 つの CLI セッションを使用することを推奨します。

特定のスタック メンバ ポートを設定する場合は、CLI コマンドインターフェイス表記にスタック メンバ番号を含めてください。

スタンバイ スイッチをデバッグするには、アクティブなスイッチから **session standby ios** 特権 EXEC コマンドを使用してスタンバイ スイッチの IOS コンソールにアクセスします。特定のスタック メンバをデバッグするには、アクティブなスイッチから **session switch** *stack-member-number* 特権 EXEC コマンドを使用して、スタック メンバの診断シェルにアクセスします。これらのコマンドの詳細情報については、スイッチ コマンド リファレンスを参照してください。

コンソール接続または Telnet 経由で CLI にアクセスする

CLI にアクセスするには、スイッチのハードウェア インストレーション ガイドに記載されている手順で、スイッチのコンソール ポートに端末または PC を接続するか、または PC をイーサネット管理ポートに接続して、スイッチの電源をオンにする必要があります。

スイッチがすでに設定されている場合は、ローカル コンソール接続またはリモート Telnet セッションによって CLI にアクセスできますが、このタイプのアクセスに対応できるように、先にスイッチを設定しておく必要があります。

次のいずれかの方法で、スイッチとの接続を確立できます。

- スイッチ コンソール ポートに管理ステーションまたはダイヤルアップ モデムを接続するか、またはイーサネット管理ポートに PC を接続します。コンソール ポートまたはイーサネット管理ポートへの接続については、スイッチのハードウェア インストレーション ガイドを参照してください。
- リモート管理ステーションから任意の Telnet TCP/IP または暗号化セキュア シェル（SSH）パッケージを使用します。スイッチは Telnet または SSH クライアントとのネットワーク接続が可能でなければなりません。また、スイッチにイネーブル シークレット パスワードを設定しておくことも必要です。
  - スイッチは同時に最大 16 の Telnet セッションをサポートします。1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。
  - スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

コンソール ポート、イーサネット管理ポート、Telnet セッション、または SSH セッションを通じて接続すると、管理ステーション上にユーザ EXEC プロンプトが表示されます。

第 2 章

Web グラフィカル ユーザ インターフェイスの使用

- Web GUI の使用に関する前提条件，15 ページ
- Web GUI の使用に関する情報，15 ページ
- スイッチのコンソール ポートの接続，17 ページ
- Web GUI へのログイン，17 ページ
- Web モードおよびセキュア Web モードの有効化，17 ページ
- スイッチ Web GUI の設定，18 ページ

Web GUI の使用に関する前提条件

- GUI を使用する PC では、Windows 7、Windows XP SP1 以降のリリースまたは Windows 2000 SP4 以降のリリースが稼働している必要があります。
- スイッチGUI は、Microsoft Internet Explorer バージョン 10.x、Mozilla Firefox 20.x、または Google Chrome 26.x. と互換性があります。

Web GUI の使用に関する情報

Web ブラウザ、つまり、グラフィカル ユーザ インターフェイス（GUI）は、各スイッチに組み込まれています。

サービス ポート インターフェイスまたは管理インターフェイスを使用して GUI にアクセスできますが、サービスポートインターフェイスの使用をお勧めします。GUI のページ上部にある [Help] をクリックすると、オンラインヘルプが表示されます。オンラインヘルプを表示するには、ブラウザのポップアップ ブロッカを無効にする必要があります。

Web GUI の機能

スイッチWeb GUI は次の機能をサポートします。

構成ウィザード : IP アドレスおよびローカルユーザ名/パスワードの初期設定、または認証サーバでの認証（必須特権 15）の後、ウィザードは最初の無線設定を完了するための手順を提供します。[Configuration] > [Wizard] を起動し、次のことを設定するために、9 ステップの手順に従います。

- 管理ユーザ
- SNMP システムの概要
- Management Port
- ワイヤレス管理
- RF Mobility と国番号
- モビリティ設定
- WLAN
- 802.11 設定
- 設定時間

[Monitor] タブ:

- 概要のスイッチ、クライアント、アクセス ポイントの詳細を表示します。
- すべての無線および AP 接続統計情報を表示します。
- アクセス ポイントの電波品質を表示します。
- すべてのインターフェイスおよび CDP トラフィック情報の Cisco Discovery Protocol (CDP) のすべてのネイバーの一覧を表示します。
- 分類 Friendly、Malicious、Ad hoc、Classified、および Unclassified に基づいて、すべての不正アクセス ポイントを表示します。

[Configuration] タブ:

- Web 設定ウィザードを使用して、すべての初期操作のためにスイッチを設定できます。ウィザードでは、ユーザの詳細、管理インターフェイスなどを設定できます。
- システム、内部 DHCP サーバ、管理、およびモビリティ管理パラメータを設定できます。
- スイッチ、WLAN、無線を設定できます。
- スイッチで、セキュリティ ポリシーを設定できます。
- オペレーティング システム ソフトウェアの管理コマンドスイッチにアクセスできます。

[Administration] タブで、システム ログを設定できます。

スイッチのコンソール ポートの接続

はじめる前に

基本的な動作ができるようにスイッチを設定するには、VT-100 ターミナル エミュレーション プログラム（HyperTerminal、ProComm、Minicom、Tip など）を実行する PC にコントローラを接続する必要があります。

ステップ 1 ヌルモデム シリアル ケーブルの一端をスイッチの RJ-45 コンソール ポートに接続し、もう一端を PC のシリアル ポートに接続します。

ステップ 2 AC 電源コードをスイッチに接続し、アース付き 100 ～ 240 VAC、50/60 Hz の電源コンセントに差し込みます。電源を入れます。起動スクリプトによって、オペレーティング システム ソフトウェアの初期化（コードのダウンロードおよび電源投入時自己診断テスト）および基本設定が表示されます。スイッチの電源投入時自己診断テストに合格した場合は、起動スクリプトによって設定ウィザードが実行されます。画面の指示に従って、基本設定を入力してください。

ステップ 3 **yes** と入力します。CLI セットアップ ウィザードの基本的な初期設定パラメータに進みます。gigabitethernet 0/0 インターフェイスであるサービス ポートの IP アドレスを指定します。
構成ウィザードの設定パラメータを入力すると、Web GUI にアクセスできます。これで、スイッチがサービス ポートの IP アドレスにより設定されます。

Web GUI へのログイン

ブラウザのアドレス バーに IP アドレススイッチを入力します。接続をセキュリティで保護するには、https://**ip-address** と入力します。接続をセキュリティで保護しない場合は、http://**ip-address** と入力します。

Web モードおよびセキュア Web モードの有効化

ステップ 1 [Configuration] > [Management] > [Protocol Management] > [HTTP-HTTPS]を選択します。

[HTTP-HTTPS Configuration] ページが表示されます。

ステップ 2 Web モード（ユーザが「http://ip-address」を使用してスイッチ GUI にアクセスできます）を有効にするには、[HTTP Access] ドロップダウン リストから [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。Web モード（HTTP）の接続は、セキュリティで保護されません。

ステップ 3 セキュア Web モード（ユーザが「https://ip-address」を使用してスイッチ GUI にアクセスできます）を有効にするには、[HTTPS Access] ドロップダウン リストから [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。セキュア Web モード（HTTPS）の接続は、セキュリティで保護されています。

ステップ 4 [IP Device Tracking] チェックボックスで、デバイスを追跡することを選択します。

ステップ 5 [Enable] チェックボックスでトラスト ポイントをイネーブルにすることを選択します。

ステップ 6 [Trustpoints] ドロップダウン リストからトラストポイントを選択します。

ステップ 7 [HTTP Timeout-policy (1 to 600 sec)] テキスト ボックスに、非アクティブ化により Web セッションがタイムアウトするまでの時間を秒単位で入力します。
有効な範囲は 1 ～ 600 秒です。

ステップ 8 [Server Life Time (1 to 86400 sec)] テキスト ボックスにサーバのライフタイムを入力します。
有効な範囲は 1 ～ 86400 秒です。

ステップ 9 [Maximum number of Requests (1 to 86400)] テキスト ボックスに、サーバが受け入れる最大接続要求数を入力します。
指定できる接続数の範囲は、1 ～ 86400 です。

ステップ 10 [Apply] をクリックします。

ステップ 11 [Save Configuration] をクリックします。

スイッチ Web GUI の設定

設定ウィザードでは、スイッチ上での基本的な設定を行うことができます。このウィザードは、スイッチを購入した直後やスイッチを工場出荷時のデフォルトにリセットした後に実行します。設定ウィザードは、GUI と CLI の両方の形式で使用できます。

ステップ 1 PC をサービス ポートに接続し、スイッチと同じサブネットを使用するように IPv4 アドレスを設定します。スイッチが IOS XE イメージとともにロードされ、サービス ポート インターフェイスが gigabitethernet 0/0 として設定されます。

ステップ 2 PC で Internet Explorer 10 以降、Firefox 2.0.0.11 以降、または Google Chrome を開始し、ブラウザ ウィンドウに管理インターフェイスの IP アドレスを入力します。管理インターフェイスの IP アドレスは、gigabitethernet 0/0（別名、サービス ポート インターフェイス）と同じです。初めてログインするときに、HTTP のユーザ名およびパスワードを入力する必要があります。デフォルトでは、ユーザ名は **admin**、パスワードは **cisco** です。

サービス ポート インターフェイスを使用するときは、HTTP と HTTPS の両方を使用できます。HTTPS はデフォルトでイネーブルであり、HTTP をイネーブルにすることもできます。

初めてログインすると、 <Model Number> <Hostname>] ページが表示されます。

ステップ 3 ページで、スイッチ Web GUI の [Home] ページにアクセスするために、[Wireless Web GUI] リンクをクリックします。

ステップ 4 最初にスイッチの設定に必要なすべての手順を実行するために、[Configuration] > [Wizard]を選択します。[Admin Users] ページが表示されます。

ステップ 5 [Admin Users] ページで、このスイッチに割り当てる管理者のユーザ名を [User Name] テキスト ボックスに入力し、このスイッチに割り当てる管理パスワードを [Password] テキスト ボックスおよび [Confirm Password] テキスト ボックスに入力します。[Next] をクリックします。
デフォルトのユーザ名は **admin** で、デフォルトのパスワードは **cisco** です。またはスイッチの新しい管理者ユーザを作成できます。ユーザ名とパスワードには、最大 24 文字の ASCII 文字を入力できます。

[SNMP System Summary] ページが表示されます。

ステップ 6 [SNMP System Summary] ページで、スイッチの次の SNMP システム パラメータを入力し、[Next] をクリックします。

- [Location] テキスト ボックスでユーザ定義可能なスイッチの場所。
- [Contact] テキスト ボックスで名前や電話番号などのユーザ定義可能な連絡先の詳細。
- SNMP 通知をさまざまな SNMP トラップで送信するには、[SNMP Global Trap] ドロップダウン リストで [Enabled] を選択し、さまざまな SNMP トラップに対して SNMP 通知を送信しないようにするには [Disabled] を選択します。
- システム ログ メッセージを送信するには [SNMP Logging] ドロップダウン リストから [Enabled] を選択し、システム ログ メッセージを送信しない場合は [Disabled] を選択します。

（注） SNMP トラップ サーバは、ディストリビューション ポートから到達可能であることが必要です（gigabitethernet0/0 サービスまたは管理インターフェイスは経由しません）。

[Management Port] ページが表示されます。

ステップ 7 [Management Port] ページで、管理ポートのインターフェイス（gigabitethernet 0/0）の次のパラメータを入力し、[Next] をクリックします。

- [IP Address] テキスト ボックスでサービス ポートに割り当てたインターフェイスの IP アドレス。
- [Netmask] テキスト ボックスで、管理ポートのインターフェイスのネットワーク マスクのアドレス。
- [IPv4 DHCP Server] テキスト ボックスで選択されたポートの IPv4 Dynamic Host Configuration Protocol (DHCP) のアドレス。

[Wireless Management] ページが表示されます。

ステップ 8 [Wireless Management] ページでは、次のワイヤレス インターフェイス管理の詳細を入力し、[Next] をクリックします。

- [Select Interface] ドロップダウン リストから、インターフェイスとして VLAN または 10 ギガビット イーサネットを選択します。
- [VLAN ID] テキスト ボックスで VLAN タグの ID。VLAN タグがない場合は 0。
- [IP Address] テキスト ボックスで、アクセス ポイントが接続されたワイヤレス管理インターフェイスの IP アドレス。
- [Netmask] テキスト ボックスで、ワイヤレス管理インターフェイスのネットワーク マスクのアドレス。
- [IPv4 DHCP Server] テキスト ボックスで DHCP IPv4 IP アドレス。

インターフェイスとして VLAN を選択すると、[Switch Port Configuration] テキスト ボックスで指定されたリストから、ポートとしてトランク ポートまたはアクセス ポートを指定できます。

[RF Mobility and Country Code] ページが表示されます。

ステップ 9 [RF Mobility and Country Code] ページで、RF モビリティ ドメイン名を [RF Mobility] テキスト ボックスに入力し、[Country Code] ドロップダウン リストから現在の国コードを選択して、[Next] をクリックします。GUI からは、1 つの国番号のみを選択できます。

（注） RF グループ化パラメータとモビリティ設定を設定する前に、必ず関連する概念のコンテンツを参照してから、設定に進むようにしてください。

[Mobility Configuration] ページが開き、モビリティのグローバル コンフィギュレーション設定が表示されます。

ステップ 10 [Mobility Configuration] ページで、次のモビリティのグローバル コンフィギュレーション設定を参照および入力し、[Next] をクリックします。

- [Mobility Role] ドロップダウン リストから、[Mobility Controller] または [Mobility Agent] を選択します。
  - [Mobility Agent] を選択した場合は、[Mobility Controller IP Address] テキスト ボックスにモビリティ コントローラの IP アドレス、[Mobility Controller Public IP Address] テキスト ボックスにモビリティ コントローラの IP アドレスを入力します。
  - [Mobility Controller] を選択すると、モビリティ コントローラの IP アドレスとモビリティ コントローラのパブリック IP アドレスがそれぞれのテキスト ボックスに表示されます。
- [Mobility Protocol Port] テキスト ボックスにモビリティ プロトコルのポート番号が表示されます。
- [Mobility Switch Peer Group Name] テキスト ボックスにモビリティ スイッチのピア グループ名が表示されます。
- [DTLS Mode] テキスト ボックスで、DTLS がイネーブルであるかどうかが示されます。

  DTLS は、標準化過程にある TLS に基づくインターネット技術特別調査委員会（IETF）プロトコルです。
- [Mobility Domain ID for 802.11 radios] テキスト ボックスに、802.11 無線のモビリティ ドメイン ID が表示されます。

- [Mobility Keepalive Interval (1-30)sec] テキスト ボックスで、ピアスイッチに送信する各 ping 要求の間隔（秒単位）。

  有効範囲は 1 ～ 30 秒で、デフォルト値は 10 秒です。

- [Mobility Keep Alive Count（3-20）] テキスト ボックスで、ピア スイッチが到達不能と判断するまでに ping 要求を送信する回数。

  有効な範囲は 3 ～ 20 で、デフォルト値は 3 です。

- [Mobility Control Message DSCP Value (0-63)] テキスト ボックスで、モビリティ スイッチに設定される DSCP 値。

  有効な範囲は 0 ～ 63 で、デフォルト値は 0 です。

- [Switch Peer Group Members Configured] テキスト ボックスで設定したモビリティ スイッチ ピア グループ メンバーの数を表示します。

[WLANs] ページが表示されます。

ステップ 11 [WLANs] ページで、次の WLAN 設定パラメータを入力し、[Next] をクリックします。

- [WLAN ID] テキスト ボックスで WLAN 識別子。
- [SSID] テキスト ボックスで、クライアントに関連付けられている WLAN の SSID。
- [Profile Name] テキスト ボックスで、クライアントが使用する WLAN の名前。

[802.11 Configuration] ページが表示されます。

ステップ 12 [802.11 Configuration] ページで、[802.11a/n/ac] チェックボックスと [802.11b/g/n] チェックボックスのいずれかまたは両方をオンにして 802.11 無線をイネーブルにし、[Next] をクリックします。
[Set Time] ページが表示されます。

ステップ 13 [Set Time] ページで、次のパラメータに基づいてスイッチの日時を設定し、[Next] をクリックします。

- [Current Time] テキスト ボックスで、スイッチの現在のタイムスタンプが表示されます。
- [Mode] ドロップダウン リストから [Manual] または [NTP] を選択します。

  NTP サーバの使用時に、スイッチに接続されているすべてのアクセス ポイントが、使用可能な NTP サーバ設定に基づいて時間を同期します。

- [Year, Month, and Day] ドロップダウン リストからスイッチの日付を選択します。
- [Hours, Minutes, and Seconds] ドロップダウン リストから時間を選択します。
- 時間帯を [Zone] テキスト ボックスに入力し、スイッチで設定された現在の時刻と比較した場合に必要なオフセットを [Offset] ドロップダウン リストから選択します。

[Save Wizard] ページが表示されます。

ステップ 14 [Save Wizard] ページで、この手順を使用してスイッチで行った設定を確認できます。設定値を変更する場合は、[Previous] をクリックし、該当ページに移動します。

すべてのウィザードについて成功メッセージが表示された場合にのみ、ウィザードを使用して作成したスイッチ設定を保存できます。[Save Wizard] ウィザードページでエラーが表示された場合、スイッチの初期設定のためにウィザードを再実行する必要があります。

第 3 章

VTP の設定

- 機能情報の確認，23 ページ
- VTP の前提条件，24 ページ
- VTP の制約事項，24 ページ
- VTP の概要，25 ページ
- VTP の設定方法，35 ページ
- VTP のモニタ，47 ページ
- VTP の設定例，48 ページ
- 次の作業，48 ページ
- その他の参考資料，48 ページ
- VTP の機能履歴と情報，50 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シスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

VTP の前提条件

VLAN を作成する前に、ネットワークで VLAN Trunking Protocol（VTP）を使用するかどうかを決定する必要があります。VTP を使用すると、1 つまたは複数のスイッチ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スイッチに伝達できます。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 つ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 は適切に機能せず、VLAN データベースの不整合が生じます。

スイッチは合計 4094 の VLAN をサポートします。ただし、ルーテッド ポート、SVI、およびその他の設定済み機能の個数によって、スイッチ 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、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、スイッチまたはスイッチ 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。

関連トピック

VTP アドバタイズ, （27 ページ）

VTP ドメインへの VTP クライアント スイッチの追加（CLI）, （44 ページ）

VTP ドメイン（VTP domain）, （25 ページ）

VTP モード, （26 ページ）

VTP の制約事項

次に、VTP に関する制約事項を示します。

- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

注意 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。

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スイッチが、アクティブ スイッチ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。スイッチが 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スイッチに伝達されます。

スイッチ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、新しいスイッチはアクティブ スイッチから VTP 情報を取得します。

VTP ドメイン（VTP domain）

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またはスイッチ スタックで構成されます。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とき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。

関連トピック

VTP ドメインへの VTP クライアント スイッチの追加（CLI），（44 ページ）
VTP の前提条件，（24 ページ）

VTP モード

表 *4*：*VTP* モード

VTP モード	説明
VTP サーバ	VTP サーバ モードでは、VLAN の作成、変更、削除ができます。また、VTP ドメイン全体に対して他のコンフィギュレーション パラメータ（VTP バージョンなど）を指定できます。VTP サーバは、同一 VTP ドメイン内の他のスイッチに自身の 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。 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。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、NVRAM が正常に動作するまで、スイッチを 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 モードのスイッチで設定します。 VTP バージョン 1 および 2 の VTP クライアント モードでは、VLAN 設定は NVRAM に保存されません。VTP バージョン 3 では、VLAN 設定はクライアント モードで NVRAM に保存されます。

VTP モード	説明
VTP トランスペアレント	VTP トランスペアレント 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。 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。 スイッチ 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スイッチについて同じです。
VTP オフ	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。

関連トピック

VTP の前提条件, （24 ページ）
VTP モードの設定（CLI）, （35 ページ）

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に送信します。ネイバー スイッチは、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。

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, （24 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、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。

関連トピック

VTP バージョンのイネーブル化（CLI）, （39 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。

- 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 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、スイッチを 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），（39 ページ）

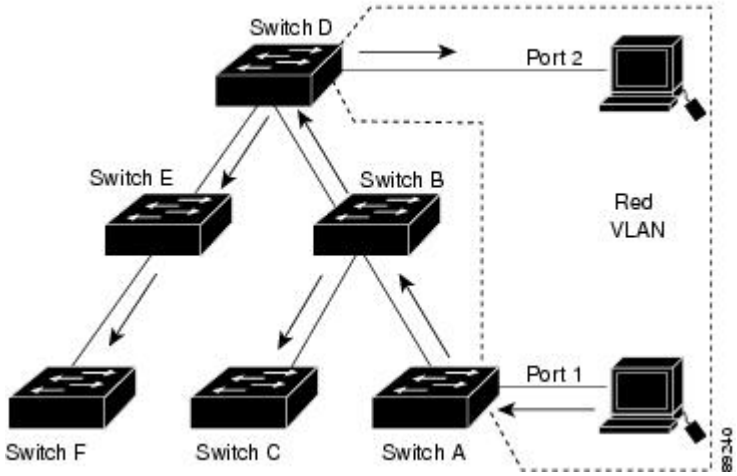
VTP プルーニング

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、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、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 ネットワークではディセーブルです。スイッチ A のポート 1 およびスイッチ D のポート 2 は、Red という VLAN に割り当てられています。スイッチ 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、スイッチ 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スイッチ C、E、F も含めて、ネットワーク内のすべてのスイッチがこのブロードキャストを受信します。

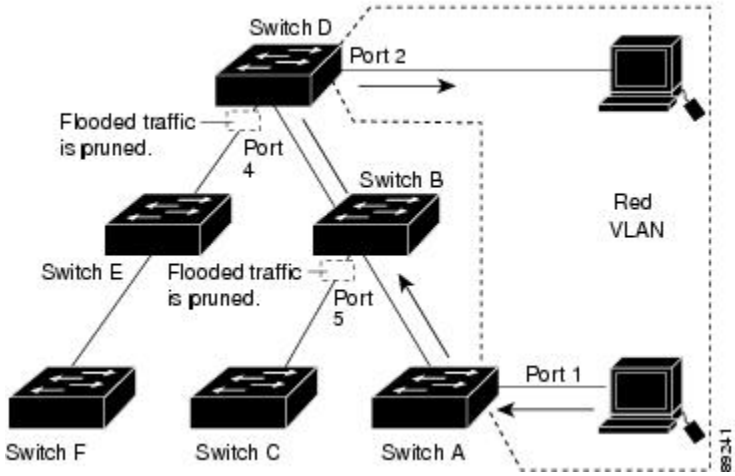
図 *1*：*VTP* プルーニングを使用しない場合のフラッディング トラフィック



VTP プルーニングは、スイッチド ネットワークではイネーブルです。スイッチ A からのブロードキャスト トラフィックは、スイッチ 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（スイッチ B のポート 5、およびスイッチ 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 サーバで VTP プルーニングをイネーブルにすると、管理ドメイン全体でプルーニングがイネーブルになります。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。

関連トピック

VTP プルーニングのイネーブル化（CLI），（41 ページ）

VTP とスイッチ スタック

VTP 設定は、スイッチ スタックのすべてのメンバで同一です。スイッチ 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スイッチの VTP 設定が同一になります。

- スタックに参加したスイッチは、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。
- スタック内のスイッチの VTP モードが変更されると、そのスタック内のその他のスイッチも VTP モードを変更し、スイッチの 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 スイッチでもスタックでも同じように機能しますが、スイッチ スタックが VTP データベースのプライマリ サーバ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。アクティブなスイッチ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スイッチが選択されると、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、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スイッチ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。

関連トピック

ポート単位の VTP の設定（CLI），（43 ページ）

VTP バージョン 3 のプライマリ サーバの設定（CLI），（39 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。

関連トピック

VTP ドメインへの VTP クライアント スイッチの追加（CLI），（44 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 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。パスワードのないスイッチ、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、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。

関連トピック

VTP バージョン 3 のパスワードの設定（CLI），（37 ページ）
例：スイッチをプライマリ サーバとして設定する，（48 ページ）

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。1 つの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、そのコントローラはバージョン 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。
- スイッチを VTP クライアント モードに設定した場合、スイッチでは VLAN データベース ファイル（vlan.dat）は作成されません。そのままスイッチの電源をオフにすると、VTP 設定はデフォルトにリセットされます。スイッチが再起動された後も VTP 設定を VTP クライアント モードに維持するには、VTP モードを設定する前に、VTP ドメイン名を設定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 ドメイン名を設定しないでください。ドメイン名を設定すると、そのドメインの VLAN 設定を変更できなくなります。したがって、少なくとも 1 つのスイッチを VTP サーバとして設定してください。

関連トピック

VTP バージョンのイネーブル化（CLI），（39 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 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。

手順の概要

1. **configureterminal**
2. **vtp domain** *domain-name*
3. **vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**}
4. **vtp password** *password*
5. **end**
6. **show vtp status**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# 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	**vtp domain** *domain-name* 例： `Switch(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。 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。 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 3	**vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**}	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。

	コマンドまたはアクション	目的
	例： `Switch(config)# vtp mode server`	• **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 4	**vtp password** *password* 例： `Switch(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。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show vtp status** 例： `Switch# 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 7	**copy running-config startup-config** 例： `Switch# 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。

関連トピック

VTP モード，（26 ページ）

VTP バージョン 3 のパスワードの設定（CLI）

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。

手順の概要

1. **configureterminal**
2. **vtp password** *password* [**hidden** | **secret**]
3. **end**
4. **show vtp password**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# 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	**vtp password** *password* [**hidden** | **secret**] 例： `Switch(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。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show vtp password** 例： `Switch# 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 5	**copy running-config startup-config** 例： `Switch# 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。

関連トピック

VTP ドメインのパスワード，（33 ページ）
例：スイッチをプライマリ サーバとして設定する，（48 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。

手順の概要

1. **vtp primary** [**vlan** | **mst**] [**force**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**vtp primary** [**vlan** | **mst**] [**force**] 例： `Switch# 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。スイッチのパスワードが **hidden** に設定されている場合は、パスワードの再入力を要求されます。 • （任意）**vlan**：テイクオーバー機能として VLAN データベースを選択します。これはデフォルトです。 • （任意）**mst**：テイクオーバー機能としてマルチ スパニング ツリー（MST）データベースを選択します。 • （任意）**force**：競合するサーバの設定が上書きされます。**force** を入力しない場合、テイクオーバーの実行前に確認を求められます。

関連トピック

VTP の設定，（32 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、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 モードのスイッチだけです。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。

手順の概要

1. **configureterminal**
2. **vtp version {1 | 2 | 3}**
3. **end**
4. **show vtp status**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# 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	**vtp version** {**1** | **2** | **3**} 例： `Switch(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 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show vtp status** 例： `Switch# 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 5	**copy running-config startup-config** 例： `Switch# 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。

関連トピック

VTP Version,　（34 ページ）
VTP バージョン 2,　（28 ページ）
VTP バージョン 3,　（29 ページ）

VTP プルーニングのイネーブル化（CLI）

プルーニングは、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 リンクだけにフラッディング トラフィックを制限することによって、使用可能な帯域幅を増やします。VTP プルーニングをイネーブルにできるのは、スイッチ が VTP サーバ モードの場合だけです。

VTP バージョン 1 および 2 では、VTP サーバでプルーニングをイネーブルにすると、その VTP ドメイン全体でプルーニングがイネーブルになります。VTP バージョン 3 では、ドメイン内の各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。

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、トランク ポート上で VLAN 2 ～ 1001 がプルーニング適格です。専用の VLAN および拡張範囲 VLAN をプルーニングすることはできません。

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 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。

手順の概要

1. **configureterminal**
2. **vtp pruning**
3. **end**
4. **show vtp status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# 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	**vtp pruning** 例： `Switch(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。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show vtp status** 例： `Switch# 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，（30 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。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **vtp**
4. **end**
5. **show running-config interface** *interface-id*
6. **show vtp status**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Switch(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 3	**vtp** 例： `Switch(config)# vtp`	指定したポートのVTPをイネーブルにします。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config interface** *interface-id* 例： `Switch# show running-config interface gigabitethernet1/0/1`	ポートの変更を確認します。
ステップ 6	**show vtp status** 例： `Switch# show vtp status`	設定を確認します。

関連トピック

VTP の設定，（32 ページ）

VTP ドメインへの VTP クライアント スイッチの追加（CLI）

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。

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。

手順の概要

1. **show vtp status**
2. **configureterminal**
3. **vtp domain** *domain-name*
4. **end**
5. **show vtp status**
6. **configure terminal**
7. **vtp domain** *domain-name*
8. **end**
9. **show vtp status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show vtp status** 例： `Switch# 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。 • 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 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**vtp domain** *domain-name* 例： `Switch(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 4	**end** 例： `Switch(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、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 5	**show vtp status** 例： `Switch# 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 6	**configure terminal** 例： `Switch# 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 7	**vtp domain** *domain-name* 例： `Switch(config)# vtp domain domain012`	スイッチの元のドメイン名を開始します。
ステップ 8	**end** 例： `Switch(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 9	**show vtp status** 例： `Switch# 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（VTP domain），（25 ページ）

VTP の前提条件, （24 ページ）
VTP 設定のためのドメイン名, （33 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。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 5：***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。
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。

```
Switch# 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），（37 ページ）
VTP ドメインのパスワード，（33 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。

- VLANs
- VLAN グループ
- VLAN トランキング
- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
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)*』

関連項目	マニュアル タイトル
追加の設定コマンドおよび手順。	『*LAN Switching* コンフィギュレーション ガイド, *Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』 『*Layer 2/3* コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)*』

エラー メッセージ デコーダ

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

シスコのテクニカル サポート

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

VTP の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 4 章

VLAN の設定

- 機能情報の確認，51 ページ
- VLAN の前提条件，51 ページ
- VLAN の制約事項，52 ページ
- VLAN について，52 ページ
- VLAN の設定方法，58 ページ
- VLAN のモニタリング，71 ページ
- 次の作業，72 ページ
- その他の参考資料，72 ページ
- VLAN の機能履歴と情報，74 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シスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

VLAN の前提条件

VLAN 設定時の前提条件と考慮事項を次に示します。

- 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。
- スイッチで多数の VLAN を設定し、ルーティングをイネーブルにしない予定の場合は、Switch Database Management（SDM）機能を VLAN テンプレートに設定します。これにより、最大数のユニキャスト MAC アドレスをサポートするようにシステム リソースが設定されます。
- LAN ベース フィーチャ セットが稼働しているスイッチでは、SVI のスタティック ルーティングだけがサポートされます。
- VLAN グループに VLAN を追加できるようにするため、VLAN がスイッチ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。

- スイッチは、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。
- 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。
- プライベート VLAN はスイッチではサポートされません。
- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

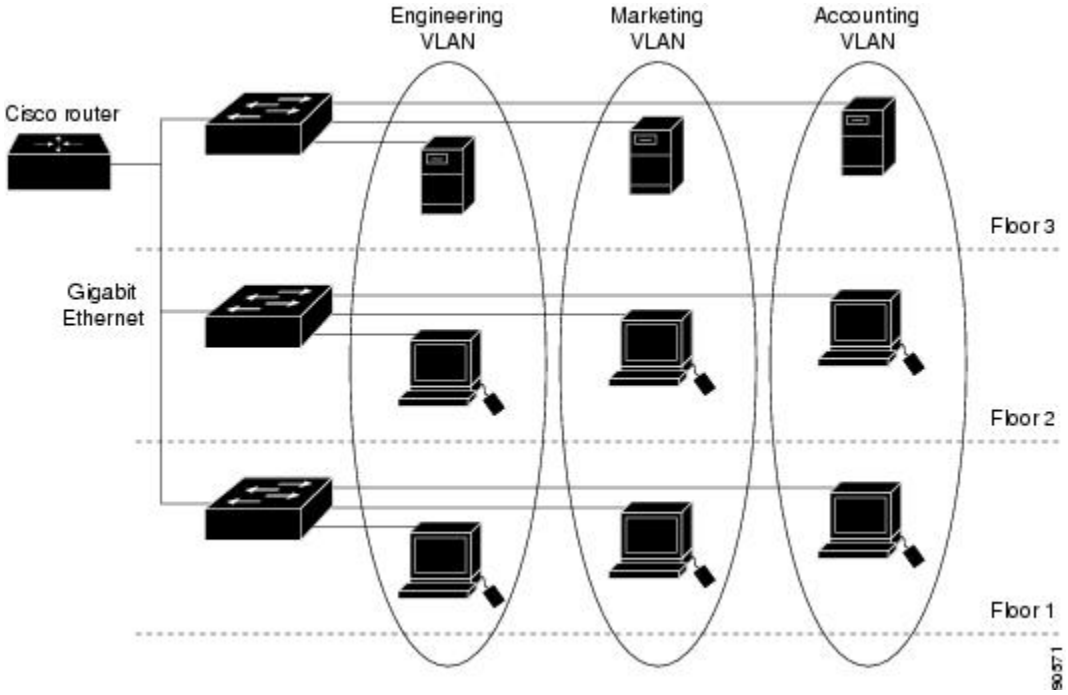
VLAN について

論理ネットワーク

VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。どのようなスイッチ 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スイッチを経由して伝送しなければなりません。スイッチ スタックでは、VLAN はスタック全体にまたがる複数のポートに設定できます。VLAN はそれぞれが独立した論理ネットワークと

見なされるので、VLAN ごとに独自のブリッジ管理情報ベース（MIB）情報があり、スパニングツリーの独自の実装をサポートできます。

図 *3*：論理的に定義されたネットワークとしての *VLAN*



VLAN は通常、IP サブネットワークに対応付けられます。たとえば、特定の IP サブネットに含まれるエンドステーションはすべて同じ VLAN に属します。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 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 スイッチ 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。スイッチ上のローカル 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、実行設定ファイルに保存されます。

最大 4094 の VLAN をスイッチに設定できます。

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、スイッチは 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 *6*：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、別のスイッチまたはスイッチ スタックのトランク ポートに接続されているスイッチまたはスイッチ 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スイッチと VLAN コンフィギュレーション メッセージを交換します。

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。

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），（63 ページ）
VLAN のモニタリング，（71 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），（63 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 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。一部のスイッチでは、vlan.dat ファイルがアクティブ スイッチのフラッシュ 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、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、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 モードにする必要があります。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 トラフィックを転送するのではなく、VTP を介して VLAN 設定を伝播します。
- スイッチは 128 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も多い場合、スパニングツリーは 128 の VLAN でイネーブルにできます。残りの VLAN で、スパニングツリーはディセーブルになります。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。

スイッチ上の 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、スイッチ上に 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。

- スタック内のスイッチが新しい 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。
- スイッチ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、新しいスイッチの VTP 情報（vlan.dat ファイル）のスタック スイッチの一貫性が保たれます。

関連トピック

イーサネット VLAN の作成または変更（CLI），（58 ページ）
VLAN のモニタリング，（71 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、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 モードでスイッチが始動するように、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、スイッチをリセットした場合に、拡張範囲 VLAN 設定が失われます。VTP バージョン 3 で拡張範囲 VLAN を作成する場合は、VTP バージョン 1 または 2 に変更できません。
- 。スイッチ上に最大数のスパニングツリーインスタンスが存在している場合に、VLAN を新規作成すると、この VLAN 上でスパニングツリーはディセーブルになります。スイッチ上の VLAN の数がスパニングツリー インスタンスの最大数を超える場合、スイッチ上に IEEE 802.1s 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。
- スイッチスタックでは、スタック全体が同一の実行コンフィギュレーションと保存されているコンフィギュレーションを使用しており、拡張範囲 VLAN 情報はスタック全体で共有されます。

関連トピック

拡張範囲 VLAN の作成（CLI），（65 ページ）
VLAN のモニタリング，（71 ページ）

VLAN の設定方法

標準範囲 VLAN の設定方法

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

- VLAN ID
- VLAN 名
- VLAN タイプ
  - イーサネット
  - Fiber Distributed Data Interface [FDDI]
  - FDDI ネットワーク エンティティ タイトル [NET]
  - TrBRF または TrCRF
  - Token Ring
  - 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 でスイッチが 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。

スイッチは、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。

このスイッチ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、サポート対象スイッチのうちの 1 台から管理できます。VTP バージョン 2 が稼働しているスイッチは、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

手順の概要

1. **configureterminal**
2. **vlan** *vlan-id*
3. **name** *vlan-name*
4. **media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** }
5. **remote-span**
6. **end**
7. **show vlan** {**name** *vlan-name* | **id** *vlan-id*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id* 例： `Switch(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。 追加の **vlan** コマンド オプションは次のとおりです。 • **access-map**：VLAN アクセスマップを作成したり、VLAN アクセスマップ コマンド モードを開始します。 • **configuration**：VLAN 機能コンフィギュレーション モードになります。 • **dot1q**：VLAN dot1q tag native パラメータを設定します。

	コマンドまたはアクション	目的
		• **filter**：VLAN フィルタ マップを VLAN リストに適用します。 • **group**：VLAN グループを作成します。
ステップ 3	**name** *vlan-name* 例： `Switch(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。 • **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。

	コマンドまたはアクション	目的
ステップ 4	**media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** } 例： `Switch(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： `Switch(config-vlan)# remote-span`	（任意）リモート スイッチド ポート アナライザ（SPAN）セッションに対する RSPAN VLAN として、VLAN を設定します。リモート SPAN の詳細については、『*Catalyst 3850* ネットワーク管理コンフィギュレーション ガイド』を参照してください。
ステップ 6	**end** 例： `Switch(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： `Switch# 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，（56 ページ）
VLAN のモニタリング，（71 ページ）

VLAN の削除（CLI）

VTP サーバ モードのスイッチから VLAN を削除すると、VTP ドメイン内のすべてのスイッチの 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 モードのスイッ

チから VLAN を削除した場合、その特定のスイッチスイッチまたはスイッチスタック上に限り 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。

手順の概要

1. **configureterminal**
2. **no vlan** *vlan-id*
3. **end**
4. **show vlan brief**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# 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	**no vlan** *vlan-id* 例： `Switch(config)# no vlan 4`	VLAN ID を入力して、VLAN を削除します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show vlan brief** 例： `Switch# show vlan brief`	VLAN が削除されたことを確認します。

関連トピック

VLAN のモニタリング，（71 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。

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

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **switchport access vlan** *vlan-id*
5. **end**
6. **show running-config interface** *interface-id*
7. **show interfaces** *interface-id***switchport**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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： `Switch(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 3	**switchport mode access** 例： `Switch(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。

	コマンドまたはアクション	目的
ステップ 4	**switchport access vlan** *vlan-id* 例： `Switch(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 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id* 例： `Switch# 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 7	**show interfaces** *interface-id***switchport** 例： `Switch# 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。

関連トピック

VLAN ポート メンバーシップ モード，（54 ページ）
VLAN のモニタリング，（71 ページ）
VLAN ポート メンバーシップ モード，（54 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、スイッチ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）

手順の概要

1. **configureterminal**
2. **vlan** *vlan-id*
3. **remote-span**
4. **exit**
5. **interface vlan**
6. **ip mtu** *mtu-size*
7. **end**
8. **show vlan id** *vlan-id*
9. **copy running-config startup config**

手順の詳細

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

ステップ 2	**vlan** *vlan-id*
	
	例：
	
	`Switch(config)# vlan 2000`
	`Switch(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 3	**remote-span** 例： `Switch(config-vlan)# remote-span`	（任意）RSPAN VLAN として VLAN を設定します。

ステップ 4	**exit**
	
	例：
	
	`Switch(config-vlan)# exit`
	`Switch(config)#`
		コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的

ステップ 5	**interface vlan**
	
	例：
	
	`Switch(config)# interface vlan 200`
	`Switch(config-if)#`
		選択した VLAN につい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 6	**ip mtu** *mtu-size*
	
	例：
	
	`Switch(config-if)# ip mtu 1024`
	`Switch(config-if)#`
		（任意）MTU サイズを変更して、VLAN を変更します。68 ～ 1500 バイトの MTU サイズを設定できます。
		
		（注） CLI ヘルプにすべての VLAN コマンドが表示されますが、拡張範囲 VLAN でサポートされているのは、**ip mtu** *mtu-size* コマンド、 コマンド、**remote-span** コマンドだけです。

ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show vlan id** *vlan-id* 例： `Switch# show vlan id 2000`	VLAN が作成されたことを確認します。
ステップ 9	**copy running-config startup config** 例： `Switch# copy running-config startup-config`	（任意）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設定を保存します。拡張範囲 VLAN 設定を保存するには、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 VTP トランスペアレント モード設定と拡張範囲 VLAN 設定を保存する必要があります。これらを保存しないと、スイッチをリセットした場合に、スイッチがデフォルトで VTP サーバ モードになり、拡張範囲 VLAN ID は保存されません。 （注） VTP バージョン 3 では、VLAN が VLAN データベースに保存されるため、この手順は必要ありません。

関連トピック

拡張範囲 VLAN 設定時の注意事項，（57 ページ）
VLAN のモニタリング，（71 ページ）

VLAN の設定方法（GUI）

レイヤ 2 VLAN の作成（GUI）

スイッチ Web UI を使用してレイヤ 2 VLAN を作成するには、次の手順に従う必要があります。

ステップ 1 レイヤ 2 VLAN を作成するには、[設定（Configuration）] > [コントローラ（Controller）] > [システム（System）] > [VLAN] > [レイヤ 2 VLAN（Layer2 VLAN）] の順に選択します。
[VLAN レイヤ 2（VLAN Layer2）] ページが表示されます。[レイヤ 2（Layer2）] ページに表示されているすべてのパラメータの値を入力する必要があります。

パラメータ	説明
VLAN ID	VLAN タグの ID、VLAN タグがない場合は、0。
名前	VLAN 名。
状態	VLAN ステート。値は次のとおりです。 • Active • Suspended

ステップ 2 [Apply] をクリックします。

レイヤ 3 インターフェイスの作成（GUI）

スイッチ Web UI を使用してレイヤ 3 インターフェイスを作成するには、次の手順に従う必要があります。

ステップ 1 レイヤ 3 インターフェイスを作成するには、[設定（Configuration）] > [コントローラ（Controller）] > [システム（System）] > [VLAN] > [レイヤ 3 インターフェイス（Layer3 Interface）] の順に選択します。
[レイヤ 3 インターフェイス（Layer3 Interface）] ページが表示されます。その画面に表示されているすべてのパラメータの値を入力する必要があります。

パラメータ	説明
説明	レイヤ 3 インターフェイスの説明。
DHCP リレー情報	コントローラ内蔵の DHCP リレー エージェント情報。

パラメータ	説明
IP Address	VLAN SVI（スイッチ仮想インターフェイス）の IP アドレス/サブネット マスク。
アドレスをマスク	DHCP サーバのアドレスをマスク。
IPv6 Address	DHCP サーバの IPv6 アドレス。
IPv4 DHCP サーバ	DHCP サーバの IPv4 アドレス
IPv6 DHCP サーバ	DHCP サーバの IPv6 アドレス。

ステップ 2 [Apply] をクリックします。

レイヤ 2 VLAN の表示（GUI）

Web UI を使用して、スイッチインターフェイスに設定されているレイヤ 2 VLAN の詳細を表示できます。

はじめる前に

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	[Configuration] > [Controller] > [System] > [VLAN] > [Layer2 VLAN] .を選択します。	レイヤ 2 VLAN のページが表示され、スイッチとともにレイヤ 2 VLAN の詳細が以下のように表示されます。 パラメータ：説明 VLAN ID：VLAN タグの ID を表示します。 名前：VLAN 名。 状態：VLAN ステート。表示される値は次のとおりです。 • Active • Suspended MTU：最大伝送単位。

レイヤ 3 インターフェイスの表示（GUI）

Web UI を使用して、スイッチに設定されているレイヤ 3 インターフェイスの詳細を表示できます。

[Configuration] > [Controller] > [System] > [VLAN] > [Layer3 Interface] .を選択します。
レイヤ 2 VLAN のページが表示され、スイッチとともにレイヤ 3 インターフェイスの詳細が以下のように表示されます。

パラメータ	説明
Interface Name	レイヤ 3 インターフェイス名。
Status（ステータス）	レイヤ 3 インターフェイスのステータス。値は次のとおりです。 • Up • Down
プロトコル	レイヤ 3 インターフェイスに使用されるプロトコル。
IP Address	レイヤ 3 セキュリティおよびモビリティ マネージャに使用される IP アドレス。

レイヤ 2 VLAN の削除（GUI）

スイッチウェブ UI を使用してレイヤ 2 VLAN を削除するには、以下を行う必要があります。

ステップ 1 [Configuration] > [Controller] > [System] > [VLAN] > [Layer2 VLAN] .を選択します。
レイヤ 2 VLAN のページが表示され、スイッチとともにレイヤ 2 VLAN の詳細が以下のように表示されます。

パラメータ	説明
VLAN ID	VLAN タグの ID を表示します。
名前	VLAN 名。
状態	VLAN ステート。表示される値は次のとおりです。 • Active • Suspended

パラメータ	説明
MTU	最大伝送単位。

ステップ 2 一覧から、削除する必要のあるレイヤ 2 VLAN のチェックボックスに印をつけます。
選択したレイヤ 2 VLAN の削除に関する確認メッセージが表示されます。

ステップ 3 [OK] をクリックします。

レイヤ 3 インターフェイスの削除（GUI）

スイッチウェブ UI を使用してレイヤ 3 インターフェイスを削除するには、以下を行う必要があります。

ステップ 1 [Configuration] > [Controller] > [System] > [VLAN] > [Layer3 Interface] .を選択します。
レイヤ 3 インターフェイスのページが表示され、スイッチとともにレイヤ 3 インターフェイスの詳細が以下のように表示されます。

パラメータ	説明
Interface Name	レイヤ 3 インターフェイス名。
Status（ステータス）	レイヤ 3 インターフェイスのステータス。値は次のとおりです。 • Up • Down
プロトコル	レイヤ 3 インターフェイスに使用されるプロトコル。
IP Address	レイヤ 3 セキュリティおよびモビリティ マネージャに使用される IP アドレス。

ステップ 2 一覧から、削除する必要のあるレイヤ 3 インターフェイスのチェックボックスに印をつけます。
選択したレイヤ 3 インターフェイスの削除に関する確認メッセージが表示されます。

ステップ 3 [OK] をクリックします。

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*]	スイッチ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* | **remote-span** | **summary**]	スイッチ上のすべての 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。 • **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。

関連トピック

イーサネット VLAN の作成または変更（CLI），（58 ページ）
標準範囲 VLAN 設定時の注意事項，（56 ページ）

VLAN の削除（CLI），（61 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），（63 ページ）
VLAN ポート メンバーシップ モード，（54 ページ）
拡張範囲 VLAN の作成（CLI），（65 ページ）
拡張範囲 VLAN 設定時の注意事項，（57 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 グループ
- VLAN トランキング プロトコル（VTP）
- VLAN トランク
- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*VLAN 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)*』
VLAN アクセス マップ	*Security コンフィギュレーション ガイド (Catalyst 3850 スイッチ)* *Security コマンド リファレンス (Catalyst 3850 スイッチ)*
VLAN およびモビリティ エージェント	『*Mobility コンフィギュレーション ガイド, Cisco IOS XE Release 3SE (Catalyst 3850 スイッチ)*』

関連項目	マニュアル タイトル
Cisco Flexible NetFlow	『*Cisco Flexible NetFlow コンフィギュレーション ガイド, Cisco IOS XE Release 3SE (Catalyst 3850 スイッチ)*』 『*Flexible Netflow コンフィギュレーション ガイド, Cisco IOS XE Release 3SE (Catalyst 3850 スイッチ)*』
IGMP スヌーピング	*IP Multicast Routing コマンド リファレンス (Catalyst 3850 スイッチ)* *IP Multicast Routing コンフィギュレーション ガイド (Catalyst 3850 スイッチ)*
IPv6	*IPv6 コンフィギュレーション ガイド (Catalyst 3850 スイッチ)* *IPv6 コマンド リファレンス (Catalyst 3850 スイッチ)*
SPAN	ネットワーク管理コマンド リファレンス *(Catalyst 3850 スイッチ)* ネットワーク管理コンフィギュレーションガイド *(Catalyst 3850 スイッチ)*
プラットフォームに依存しない設定情報	『*Identity Based Networking Services コンフィギュレーション ガイド, Cisco IOS XE Release 3SE (Catalyst 3850 スイッチ)*』

エラー メッセージ デコーダ

説明	Link
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	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management

標準/RFC	Title
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIB

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

シスコのテクニカル サポート

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

VLAN の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。
Cisco IOS XE 3.3SE	VLAN（GUI）サポート。

第 5 章

VLAN グループの設定

- 機能情報の確認，77 ページ
- VLAN グループの前提条件，77 ページ
- VLAN グループの制約事項，78 ページ
- VLAN グループについて，78 ページ
- VLAN グループの設定方法，79 ページ
- 次の作業，83 ページ
- その他の参考資料，84 ページ
- VLAN グループの機能履歴と情報，86 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シスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

VLAN グループの前提条件

VLAN グループに VLAN を追加できるようにするため、VLAN がスイッチに存在している必要があります。

VLAN グループの制約事項

1 つの VLAN グループにマッピングされる VLAN の数は、Cisco IOS Software Release による制限を受けません。ただし、VLAN グループの VLAN の数が推奨値である 32 を超えた場合、予期されないモビリティの動作が発生し、VLAN グループ内の一部の VLAN で L2 マルチキャストが中断します。したがって、VLAN グループ内で適切な数の VLAN を設定する責任は管理者にあります。すでに 32 個の VLAN が含まれている WLAN にマップされている VLAN グループに VLAN を追加すると、警告が生成されます。ただし、32 を超える VLAN が含まれている WLAN に新しい VLAN グループがマッピングされると、エラーが生成されます。

VLAN グループが予期通り動作するためには、グループでマッピングされた VLAN がスイッチに存在している必要があります。スタティック IP クライアント動作はサポートされません。

VLAN グループについて

無線クライアントが無線ネットワーク（WLAN）に接続すると、クライアントは、WLAN に関連付けられている VLAN に配置されます。講堂、競技場、会議場などといった大規模な会場では、大量のワイヤレス クラインアントが使用されており、単一の WLAN だけで多数のクライアントに対応することは困難な場合があります。

VLAN グループ機能は、複数の VLAN に対応可能な単一 WLAN を使用します。クライアントは、設定されている VLAN の 1 つに割り当てることができます。この機能は、VLAN グループを使用して WLAN を 1 つまたは複数の VLAN にマップします。ワイヤレス クライアントが WLAN に関連付けられると、ワイヤレス クライアントの MAC アドレスに基づいてアルゴリズムにより VLAN が生成されます。VLAN がクライアントに割り当てられ、クライアントが割り当てられた VLAN から IP アドレスを取得します。またこの機能は、現行の AP グループ アーキテクチャおよび AAA オーバーライド アーキテクチャを拡張します。これらのアーキテクチャでは AP グループと AAA オーバーライドが、WLAN がマップされている 1 つの VLAN または VLAN グループをオーバーライドできます。

関連トピック

VLAN グループの作成（CLI），（79 ページ）

VLAN グループの設定方法

VLAN グループの作成（CLI）

手順の概要

1. **configure terminal**
2. **vlan group** *WORD* **vlan-list** *vlan-ID*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**vlan group** *WORD* **vlan-list** *vlan-ID* 例： `Switch(config)#vlan group vlangrp1 vlan-list 91-95`	所定のグループ名（vlangrp1）で VLAN グループを作成し、コマンドに一覧表示されているすべての VLAN を追加します。VLAN リストの範囲は 1 ～ 4096 で、1 つのグループの VLAN の数として推奨される数は 32 です。
ステップ 3	**end** 例： `Switch(config)#end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。また、**CTRL-Z** を押して、グローバル コンフィギュレーション モードを終了します。

関連トピック

VLAN グループについて，（78 ページ）

VLAN グループの削除（CLI）

手順の概要

1. **configure terminal**
2. **vlan group** *WORD* **vlan-list** *vlan-ID*
3. **no vlan group** *WORD* **vlan-list** *vlan-ID*
4. **end**

手順の詳細

ステップ 1 **configure terminal**

例：
```
Switch# configure terminal
```
グローバル コマンド モードを開始します。

ステップ 2 **vlan group** *WORD* **vlan-list** *vlan-ID*

例：
```
Switch(config)#vlan group vlangrp1 vlan-list 91-95
```
所定のグループ名（vlangrp1）でVLANグループを作成し、コマンドに一覧表示されているすべてのVLANを追加します。VLAN リストの範囲は 1 ～ 4096 で、1 つのグループの VLAN の数として推奨される数は 32 です。

ステップ 3 **no vlan group** *WORD* **vlan-list** *vlan-ID*

例：
```
Switch(config)#no vlan group vlangrp1 vlan-list 91-95
```
所定のグループ名（vlangrp1）の VLAN グループが削除されます。

ステップ 4 **end**

例：
```
Switch(config)#end
```
グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。また、**CTRL-Z** を押して、グローバル コンフィギュレーション モードを終了します。

VLAN グループの作成（GUI）

スイッチ Web UI を使用して VLAN グループを作成するには、次の操作を実行する必要があります。

ステップ 1 [Configuration] > [Controller] > [System] > [VLAN] > [VLAN Group] を選択します。
[VLAN Group] ページが表示されます。[VLAN グループ] ウィンドウに表示されているすべてのパラメータの値を入力します。

パラメータ	説明
VLAN Group Name	VLAN のグループ名。

パラメータ	説明
VLAN List	メッシュ アクセス ポイントの（MAP）アクセス ポートを設定するための VLAN リスト。

ステップ 2 [Apply] をクリックします。

WLAN への VLAN グループの追加（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *WORD number*
3. **client vlan** *WORD*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**wlan** *WORD number* 例： `Switch(config)#wlan wlanname 512`	WLAN が ID を使用して VLAN グループをマッピングできるようにします。WLAN ID 値の範囲は 1 ～ 512 です。
ステップ 3	**client vlan** *WORD* 例： `Switch(config-wlan)#client vlan vlangrp1`	VLAN ID、VLAN グループ、または VLAN 名を入力して、VLAN グループを WLAN にマッピングします。
ステップ 4	**end** 例： `Switch(config-wlan)#end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。また、**CTRL-Z** を押して、グローバル コンフィギュレーション モードを終了します。

WLAN への VLAN グループの追加（GUI）

スイッチ Web UI を使用して VLAN グループを WLAN に追加するには、この手順で説明するステップに従う必要があります。

ステップ 1 VLAN グループを WLAN に追加するには、[Configuration] > [Wireless] > [WLANs] > [WLAN Profile] > [General] の順に選択します。
WLAN グループの一般パラメータのページが表示されます。

ステップ 2 選択した WLAN プロファイルを VLAN グループに関連付けるため、[Interface/Interface Group] ドロップダウン リストから VLAN グループ値を選択します。

ステップ 3 [Apply] をクリックします。

VLAN グループの削除（GUI）

スイッチ Web UI を使用して VLAN グループを削除するには、次の操作を実行する必要があります。

ステップ 1 [Configuration] > [Controller] > [System] > [VLAN] > [VLAN Group] を選択します。
[VLAN Group] ページが出力され、スイッチに関連付けられている VLAN グループの次の詳細が表示されます。

パラメータ	説明
VLAN Group Name	VLAN のグループ名。
VLAN List	メッシュ アクセス ポイントの（MAP）アクセス ポートを設定するための VLAN リスト。

ステップ 2 VLAN グループ リストに表示される VLAN グループ名から削除する VLAN グループのチェックボックスにチェックを付けます。
選択された VLAN グループの削除を確認する確認メッセージが表示されます。

ステップ 3 [OK] をクリックします。

VLAN グループの VLAN の表示（CLI）

コマンド	説明
`show vlan group`	VLAN グループの名前と使用可能な VLAN のリストを表示します。
`show vlan group group-name` **`<group_name>`**	指定された VLAN グループの詳細を表示します。
`show wireless vlan group` **`<group_name>`**	指定されたワイヤレス VLAN グループの詳細を表示します。

VLAN グループの表示（GUI）

スイッチ Web UI を使用して VLAN グループを表示するには、次の操作を実行する必要があります。

ステップ 1 [Configuration] > [Controller] > [System] > [VLAN] > [VLAN Group] を選択します。
[VLAN Group] ページが出力され、スイッチに関連付けられている VLAN グループの次の詳細が表示されます。

パラメータ	説明
VLAN Group Name	VLAN のグループ名。
VLAN List	メッシュ アクセス ポイントの（MAP）アクセス ポートを設定するための VLAN リスト。

ステップ 2 [Apply] をクリックします。

次の作業

VLAN グループを設定したら、次の項目を設定できます。

- VLANs
- VLAN トランキング プロトコル（VTP）
- VLAN トランク

- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*VLAN* 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*)*』
VLAN アクセス マップ	*Security* コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)* *Security* コマンド リファレンス *(Catalyst 3850* スイッチ*)*
VLAN およびモビリティ エージェント	『*Mobility* コンフィギュレーション ガイド*, Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』
Cisco Flexible NetFlow	『*Cisco Flexible NetFlow* コンフィギュレーション ガイド*, Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』 『*Flexible Netflow* コンフィギュレーション ガイド*, Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』
IGMP スヌーピング	*IP Multicast Routing* コマンド リファレンス *(Catalyst 3850* スイッチ*)* *IP Multicast Routing* コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)*
IPv6	*IPv6* コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)* *IPv6* コマンド リファレンス *(Catalyst 3850* スイッチ*)*
SPAN	ネットワーク管理コマンド リファレンス *(Catalyst 3850* スイッチ*)* ネットワーク管理コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)*

関連項目	マニュアル タイトル
プラットフォームに依存しない設定情報	『*Identity Based Networking Services* コンフィギュレーション ガイド, *Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』

エラー メッセージ デコーダ

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

シスコのテクニカル サポート

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

VLAN グループの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。
Cisco IOS XE 3.3SE	VLAN（GUI）サポート。

第 6 章

VLAN トランクの設定

- 機能情報の確認，87 ページ
- VLAN トランクの前提条件，87 ページ
- VLAN トランクの制約事項，88 ページ
- VLAN トランクについて，88 ページ
- VLAN トランクの設定方法，94 ページ
- 次の作業，108 ページ
- その他の参考資料，109 ページ
- VLAN トランクの機能履歴と情報，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シスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

VLAN トランクの前提条件

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

- IEEE 802.1Q トランクを使用して接続している Cisco スイッチのネットワークでは、スイッチ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 スイッチを他社製のデバイスに接続する場合、Cisco スイッチは、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 スイッチ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 スイッチからなるクラウドにより分離された Cisco スイッチによって維持されます。Cisco スイッチと分離された他社製の IEEE 802.1Q クラウドは、スイッチ間の単一トランク 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。

- 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。
- スイッチはレイヤ 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、スイッチは、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。
- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

VLAN トランクについて

トランキングの概要

トランクとは、1 つまたは複数のイーサネット スイッチ 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、スイッチなど）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），（94 ページ）
レイヤ 2 インターフェイス モード，（89 ページ）

レイヤ 2 インターフェイス モード

表 *8*：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。

関連トピック

トランク ポートの設定（CLI）, （94 ページ）
トランキング モード, （89 ページ）

トランクでの許可 VLAN

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

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

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

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

関連トピック

トランクでの許可 VLAN の定義（CLI），（97 ページ）

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ます。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接続することも、2 台の異なるスイッチに接続することもできます。

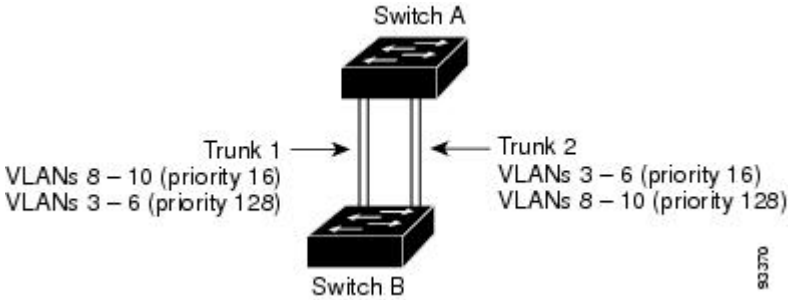
STP プライオリティによるネットワーク負荷分散

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。

次の図は、サポートされているスイッチを接続する 2 つのトランクを示します。

- VLAN 8 ～ 10 は、トランク 1 で 16 というポート プライオリティが割り当てられています。
- VLAN 3 ～ 6 は、トランク 1 でデフォルトのポート プライオリティである 128 のままです。
- VLAN 3 ～ 6 は、トランク 2 で 16 というポート プライオリティが割り当てられています。
- VLAN 8 ～ 10 は、トランク 2 でデフォルトのポート プライオリティである 128 のままです。

図 *4*：*STP* ポート プライオリティによる負荷分散



トランク 1 が VLAN 8 ～ 10 のトラフィックを伝送し、トランク 2 が VLAN 3 ～ 6 のトラフィックを伝送します。アクティブ トランクで障害が起きた場合には、プライオリティの低いトランクが引き継ぎ、それらすべての VLAN のトラフィックを伝送します。いずれのトランク ポート上でも、トラフィックの重複は発生しません。

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），（101 ページ）

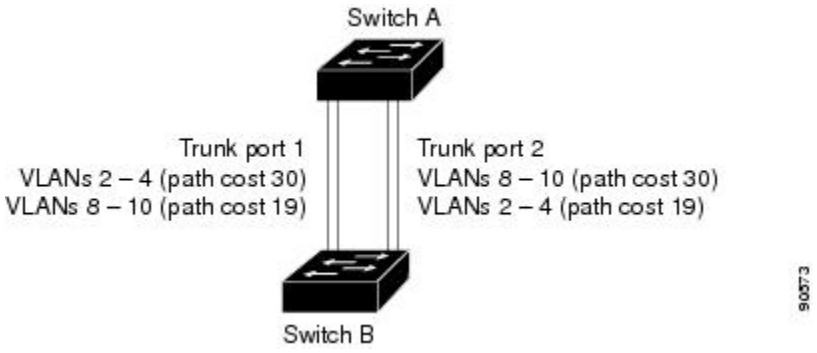
STP パス コストによるネットワーク負荷分散

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。

トランク ポート 1 および 2 は 100BASE-T ポートとして設定されています。次の VLAN パス コストが割り当てられています。

- VLAN 2 ～ 4 は、トランク ポート 1 で 30 というパス コストが割り当てられています。
- VLAN 8 ～ 10 は、トランク ポート 1 で 100BASE-T のデフォルトのパス コストである 19 のままです。
- VLAN 8 ～ 10 は、トランク ポート 2 で 30 というパス コストが割り当てられています。
- VLAN 2 ～ 4 は、トランク ポート 2 で 100BASE-T のデフォルトのパス コストである 19 のままです。

図 *5*：パス コストによってトラフィックが分散される負荷分散トランク



関連トピック

STP パス コストによる負荷分散の設定（CLI），（106 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、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。
- 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、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。

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。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**}
4. **switchport access vlan** *vlan-id*
5. **switchport trunk native vlan** *vlan-id*
6. **end**
7. **show interfaces** *interface-id***switchport**
8. **show interfaces** *interface-id***trunk**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# 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： `Switch(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 3	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**} 例： `Switch(config-if)# switchport mode dynamic desirable`	インターフェイスをレイヤ 2 トランクとして設定します（インターフェイスがレイヤ 2 アクセス ポートまたはトンネル ポートであり、トランキング モードを設定する場合に限り必要となります）。 • **dynamic auto**：ネイバー インターフェイスが trunk または desirable モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。これはデフォルトです。 • **dynamic desirable**：ネイバー インターフェイスが trunk、desirable、または auto モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。 • **trunk**：ネイバー インターフェイスがトランク インターフェイスでない場合でも、インターフェイスを永続的なトランキング モードに設定して、リンクをトランク リンクに変換するようにネゴシエートします。

	コマンドまたはアクション	目的
ステップ 4	**switchport access vlan** *vlan-id* 例： `Switch(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 5	**switchport trunk native vlan** *vlan-id* 例： `Switch(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 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** *interface-id***switchport** 例： `Switch# 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 8	**show interfaces** *interface-id***trunk** 例： `Switch# 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 9	**copy running-config startup-config** 例： `Switch# 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，（89 ページ）
レイヤ 2 インターフェイス モード，（89 ページ）

トランクでの許可 VLAN の定義（CLI）

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。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchport mode trunk**
4. **switchport trunk allowed vlan** { *word* | **add** | **all** | **except** | **none** | **remove**} *vlan-list*
5. **end**
6. **show interfaces** *interface-id***switchport**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# 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： `Switch(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 3	**switchport mode trunk** 例： `Switch(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 4	**switchport trunk allowed vlan** { *word* | **add** | **all** | **except** | **none** | **remove**} *vlan-list* 例： `Switch(config-if)# switchport trunk`	（任意）トランク上で許容される VLAN のリストを設定します。 *vlan-list* パラメータは、1 ～ 4094 の単一の VLAN 番号、または 2 つの VLAN 番号（小さい方が先、ハイフンで区切る）で指定された VLAN 範囲です。カンマで区切っ

	コマンドまたはアクション	目的
	allowed vlan remove 2	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 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id***switchport** 例： `Switch# 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 7	**copy running-config startup-config** 例： `Switch# 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, （90 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。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan* [,*vlan* [,,,]]
4. **end**
5. **show interfaces** *interface-id***switchport**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# 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： `Switch(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 3	**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 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id***switchport** 例： `Switch# 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。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `Switch# 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、スイッチ 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、スイッチはそのパケットをタグ付きで送信します。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchport trunk native vlan** *vlan-id*
4. **end**
5. **show interfaces** *interface-id***switchport**
6. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Switch(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 3	**switchport trunk native vlan** *vlan-id* 例： `Switch(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 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id***switchport** 例： `Switch# 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 6	**copy running-config startup-config** 例： `Switch# 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）

スイッチがスイッチ スタックのメンバの場合、**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。

手順の概要

1. **configure terminal**
2. **vtp domain** *domain-name*
3. **vtp mode server**
4. **end**
5. **show vtp status**
6. **show vlan**
7. **configure terminal**
8. **interface** *interface-id*
9. **switchport mode trunk**
10. **end**
11. **show interfaces** *interface-id***switchport**
12. スイッチ A で、スイッチ またはスイッチ 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。
13. 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。
14. **show vlan**
15. **configure terminal**
16. **interface** *interface-id*
17. **spanning-tree vlan** *vlan-range***port-priority** *priority-value*
18. **exit**
19. **interface** *interface-id*
20. **spanning-tree vlan** *vlan-range***port-priority** *priority-value*
21. **end**
22. **show running-config**
23. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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。

	コマンドまたはアクション	目的
ステップ 2	**vtp domain** *domain-name* 例： `Switch(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 3	**vtp mode server** 例： `Switch(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 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status** 例： `Switch# show vtp status`	スイッチ A およびスイッチ 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 6	**show vlan** 例： `Switch# 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 7	**configure terminal** 例： `Switch# 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	**interface** *interface-id* 例： `Switch(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 9	**switchport mode trunk** 例： `Switch(config-if)# switchport mode trunk`	ポートをトランク 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 10	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show interfaces** *interface-id***switchport** 例： `Switch# show interfaces gigabitethernet1/0/1 switchport`	VLAN の設定を確認します。
ステップ 12	スイッチ A で、スイッチ またはスイッチ 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 13	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 14	**show vlan** 例： `Switch# 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 15	**configure terminal** 例： `Switch# 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 16	**interface** *interface-id* 例： `Switch(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 17	**spanning-tree vlan** *vlan-range***port-priority** *priority-value* 例： `Switch(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。

	コマンドまたはアクション	目的
ステップ 18	**exit** 例： `Switch(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 19	**interface** *interface-id* 例： `Switch(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 20	**spanning-tree vlan** *vlan-range***port-priority** *priority-value* 例： `Switch(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 21	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 22	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 23	**copy running-config startup-config** 例： `Switch# 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，（91 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。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport mode trunk**
4. **exit**
5. スイッチ A またはスイッチ 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。
6. **end**
7. **show running-config**
8. **show vlan**
9. **configure terminal**
10. **interface** *interface-id*
11. **spanning-tree vlan** *vlan-range***cost** *cost-value*
12. **end**
13. 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。
14. **exit**
15. **show running-config**
16. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**interface** *interface-id* 例： `Switch(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 3	**switchport mode trunk** 例： `Switch(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 4	**exit** 例： `Switch(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 5	スイッチ A またはスイッチ 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 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# 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 8	**show vlan** 例： `Switch# 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 9	**configure terminal** 例： `Switch# 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 10	**interface** *interface-id* 例： `Switch(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 11	**spanning-tree vlan** *vlan-range* **cost** *cost-value* 例： `Switch(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 12	**end** 例： `Switch(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 13	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 14	**exit** 例： `Switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 15	**show running-config** 例： `Switch# 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 16	**copy running-config startup-config** 例： `Switch# 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, （92 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。

- VLANs
- VLAN グループ
- 音声 VLAN

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*VLAN 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)*』
スパニング ツリー プロトコル（STP）	ネットワーク管理コマンド リファレンス *(Catalyst 3850 スイッチ)* ネットワーク管理コンフィギュレーション ガイド *(Catalyst 3850 スイッチ)*

エラー メッセージ デコーダ

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

シスコのテクニカル サポート

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

VLAN トランクの機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

第 7 章

音声 VLAN の設定

- 機能情報の確認，111 ページ
- 音声 VLAN の前提条件，111 ページ
- 音声 VLAN の制約事項，112 ページ
- 音声 VLAN に関する情報，112 ページ
- 音声 VLAN の設定方法，116 ページ
- 音声 VLAN のモニタリング，120 ページ
- 次の作業，120 ページ
- その他の参考資料，120 ページ
- 音声 VLAN の機能履歴と情報，122 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シスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

音声 VLAN の前提条件

音声 VLAN の前提条件は、次のとおりです。

- 音声 VLAN 設定は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、スイッチ上の 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 に接続するスイッチ 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 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、このスイッチは 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。

Cisco7960 IP Phone は設定可能なデバイスであり、IEEE 802.1p プライオリティ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したり、オーバーライドしたりするようにスイッチを設定できます。

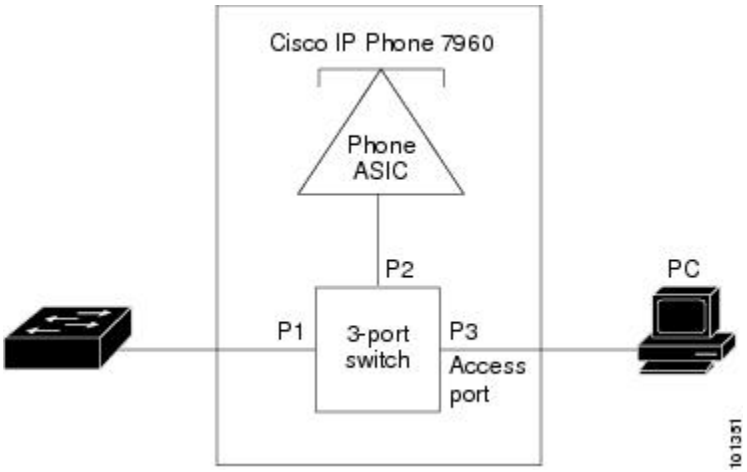
このネットワーク設定は、Cisco 7960 IP Phone を接続する 1 つの方法です。

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

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

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

図 *6*：スイッチに接続された *Cisco7960 IP Phone*



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、スイッチ上のアクセス 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スイッチ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），（116 ページ）
音声 VLAN のモニタリング，（120 ページ）

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、スイッチ上のレイヤ 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），（118 ページ）
音声 VLAN のモニタリング，（120 ページ）

音声 VLAN 設定時の注意事項

- Cisco7960 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、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 で音声 VLAN 通信が適切に行われるには、スイッチ上に音声 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）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 をイネーブルにした場合、その IP Phone からスイッチへの接続が最大 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。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **trust device cisco-phone**
4. **switchport voice vlan** {*vlan-id* | **dot1p** | **none** | **untagged**}
5. **end**
6. 次のいずれかを使用します。
   - **show interfaces** *interface-id***switchport**
   - **show running-config interface** *interface-id*
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# 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： `Switch(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： `Switch(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： `Switch(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、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 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： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	次のいずれかを使用します。 • **show interfaces** *interface-id***switchport** • **show running-config interface** *interface-id* 例： `Switch# show interfaces gigabitethernet1/0/1 switchport`	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
	または `Switch# show running-config interface gigabitethernet1/0/1`	
ステップ 7	**copy running-config startup-config** 例： `Switch# 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，（113 ページ）
音声 VLAN のモニタリング，（120 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スイッチを設定できます。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。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchport priority extend** {**cos** *value* | **trust**}
4. **end**
5. **show interfaces** *interface-id***switchport**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# 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： `Switch(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 3	**switchport priority extend** {**cos** *value* | **trust**} 例： `Switch(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 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id***switchport** 例： `Switch# show interfaces gigabitethernet1/0/1 switchport`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# 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，（114 ページ）
音声 VLAN のモニタリング，（120 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），（116 ページ）
Cisco IP Phone の音声トラフィック，（113 ページ）
着信データ フレームのプライオリティ設定（CLI），（118 ページ）
Cisco IP Phone のデータ トラフィック，（114 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。

- VLANs
- VLAN グループ
- VLAN トランキング
- VTP

その他の参考資料

関連資料

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

関連項目	マニュアル タイトル
追加の設定コマンドおよび手順。	『*LAN Switching* コンフィギュレーション ガイド, *Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』 『*Layer 2/3* コンフィギュレーション ガイド *(Catalyst 3850* スイッチ*)*』
プラットフォームに依存しない設定情報	『*Identity Based Networking Services* コンフィギュレーション ガイド, *Cisco IOS XE Release 3SE (Catalyst 3850* スイッチ*)*』

エラー メッセージ デコーダ

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

シスコのテクニカル サポート

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

音声 VLAN の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

索 引

C

Cisco 7960 IP フォン 112
Cisco IP Phone のデータ トラフィック 114
Cisco IP Phone の音声トラフィック 113
CoS 118
　プライオリティのオーバーライド 118

I

IEEE 802.1Q タギング 100

M

MST モード 93

P

password 33
priority 118
　CoS の無効化 118
PVST モード 93

S

STP パス コスト 106
STP ポート プライオリティ 101

V

VLAN 52
　定義 52
VLAN のモニタリング コマンド 71
VLAN ポート メンバーシップ モード 54
VTP 25, 32, 34
　version 34
　設定の要件 32
VTP アドバタイズ 27
VTP ドメイン（VTP domain） 25, 44
VTP の設定 32
VTP バージョン 39, 53
VTP バージョン 2 28
VTP バージョン 3 29
VTP パスワード 37
VTP プライマリ 39
VTP プルーニング 30, 41
VTP モード 26, 35

い

イーサネット VLAN 58

こ

コンフィギュレーション ファイル 55

す

スイッチ スタック 31

そ

その他の参考資料 48, 72, 84, 109, 120
　VLAN トランク 109
　VLANs 72, 84
　VTP 48
　音声 VLAN 120

と

トークン リング 39
ドメイン名 33
トランキング 88
トランキング モード 89
トランク 90, 94, 97
　許可 VLAN 90
　設定 94
トランク ポート 94

ね

ネイティブ VLAN 100
ネットワーク負荷分散 91, 92
　STP パス コスト 92
　STP プライオリティ 91

ふ

プルーニング適格リスト 98

も

モニタリング 47, 120
　VTP 47
　音声 VLAN 120

れ

レイヤ 2 インターフェイス モード 89