Cisco Nexus 3600 NX-OS レイヤ 2 スイッチング コンフィギュレーション ガイド、リリース 10.2(x)

初版：2021 年 8 月 23 日

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

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角かっこで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y | z}]	角かっこまたは波かっこ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。角かっこ内の波かっこと縦棒は、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。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
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ないでください。引用符を使用すると、その引用符も含めて string と見なされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	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。

Cisco Nexus 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ スイッチ全体のマニュアル セットは、次の URL にあります。

http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

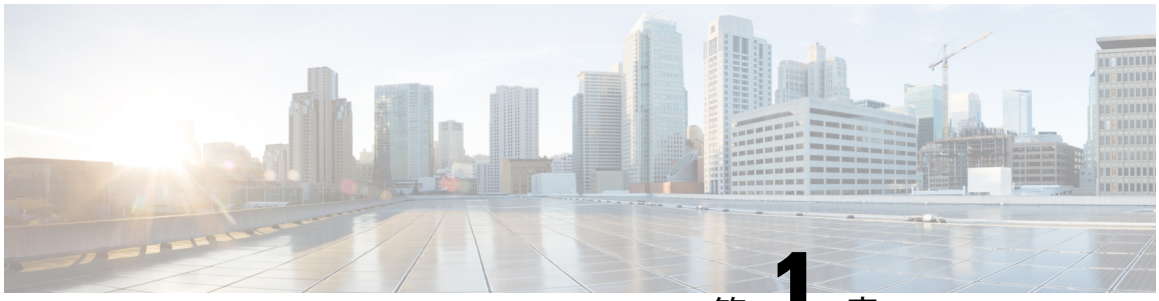
通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコサービスにアクセスしてください。
- サービス リクエストを送信するには、シスコサポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

通信、サービス、およびその他の情報



第 1 章

新規および変更情報

この章では、「*Cisco Nexus 9000* シリーズ *NX-OS* レイヤー *2* コンフィギュレーション ガイド」に記載されている新機能および変更された機能に関するリリース固有の情報について説明します。

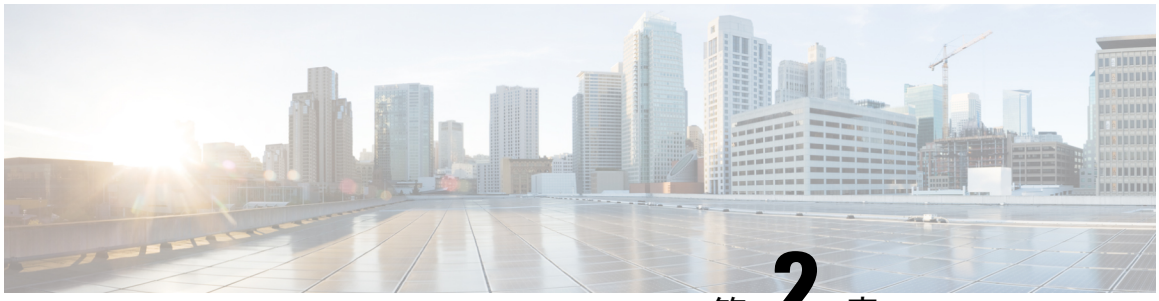
新規および変更情報

次の表は、『*Cisco Nexus 3600* シリーズ *NX-OS* レイヤ *2* スイッチング コンフィギュレーション ガイド リリース *10.2(x)*』に記載されている新機能および変更機能をまとめたものです。それぞれの説明が記載されている箇所も併記されています。

表 *1*：新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
機能の更新なし		10.2(1)F	

新規および変更情報



第 2 章

概要

ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。

レイヤ 2 イーサネット スイッチングの概要

このデバイスは、レイヤ2イーサネットセグメント間の同時パラレル接続をサポートします。イーサネット セグメント間のスイッチド コネクションは、パケットが伝送されている間だけ維持されます。次のパケットには、別のセグメント間に新しい接続が確立されます。

デバイスは、高帯域幅デバイスや多数のユーザによって引き起こされるトラフィックの輻輳を解決するため、各デバイスにドメイン（サーバなど）を割り当てます。

イーサネットネットワークではコリジョンによって深刻な輻輳が発生するため、全二重通信を使用することが有効な対処法の 1 つとなります。一般的に、10/100 Mbps イーサネットは半二重モードで動作するので、各ステーションは送信または受信のどちらかしか実行できません。これらのインターフェイスを全二重モードに設定すると、2 つのステーション間で同時に送受信を実行できます。パケットを双方向へ同時に送ることができるので、有効なイーサネット帯域幅は 2 倍になります。1/10 ギガビット イーサネットは、全二重モードだけで動作します。

VLANs

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 に属する端末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であると見なされます。VLAN に属していないステーション宛てのパケットは、ブリッジまたはルータを経由して転送する必要があります。

デバイスの初回の起動時にすべてのポートがデフォルトの VLAN（VLAN1）に割り当てられます。

このデバイスは、IEEE 802.1Q 規格に基づき、4094 の VLAN をサポートします。これらの VLAN はいくつかの範囲に分かれています。各範囲の使用法は少しずつ異なります。一部の VLAN はデバイスの内部使用のために予約されているため、設定には使用できません。

Note スイッチ間リンク（ISL）トランキングはサポートされません。

スパニングツリー

ここでは、スパニングツリー プロトコル（STP）の実装について説明します。

STP の概要

STP は、レイヤ 2 レベルで、ループのないネットワークを実現します。レイヤ 2 LAN ポートは STP フレーム（ブリッジ プロトコル データ ユニット（BPDU））を一定の時間間隔で送受信します。ネットワーク デバイスは、これらのフレームを転送せずに、フレームを使用してループフリー パスを構築します。

802.1D は、オリジナルの STP 規格です。基本的なループフリー STP から、多数の改善を経て拡張されました。Per VLAN Spanning Tree（PVST+）では、各 VLAN に個別にループフリー パスを作成できます。また、機器の高速化に対応して、ループフリーコンバージェンス処理も高速化するために、規格全体が再構築されました。802.1w規格は、高速コンバージェンスが統合された STP で、Rapid Spanning Tree（RSTP）と呼ばれています。

さらに、802.1s 規格のマルチ スパニングツリー（MST）では、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できます。各インスタンスは、独立したスパニングツリー トポロジで実行されます。

ソフトウェアは、従来の 802.1D システムで相互運用できますが、デバイスでは Rapid PVST+ および MST が実行されます。特定の VDC に、Rapid PVST+ または MST のどちらかを使用できます。1 つの VDC では両方は使用できません。Rapid PVST+ はデフォルトの STP プロトコルです。

Note Cisco NX-OS では、拡張システム ID と MAC アドレス リダクションが使用されます。これらの機能はディセーブルにできません。

また、シスコはスパニングツリーの動作を拡張するための独自の機能をいくつか作成しました。

Rapid PVST+

Rapid PVST+は、ソフトウェアのデフォルトのスパニングツリーモードで、デフォルトVLANおよび新規作成のすべての VLAN 上で、デフォルトでイネーブルになります。

設定された各 VLAN 上で RSTP の単一インスタンスまたはトポロジが実行され、VLAN 上の各 Rapid PVST+ インスタンスに 1 つのルート デバイスが設定されます。Rapid PVST+ の実行中には、VLAN ベースで STP をイネーブルまたはディセーブルにできます。

MST

このソフトウェアは、MST もサポートしています。MST を使用した複数の独立したスパニングツリー トポロジにより、データ トラフィック用に複数の転送パスを提供し、ロード バランシングを有効にして、多数の VLAN をサポートするために必要な STP インスタンスの数を削減できます。

MST には RSTP が統合されているので、高速コンバージェンスもサポートされます。MST では、1 つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）に影響しないため、ネットワークのフォールト トレランスが向上します。

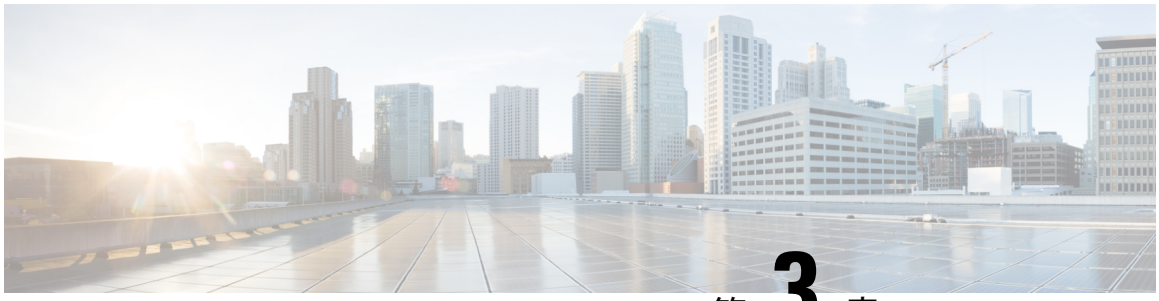
Note スパニングツリー モードを変更すると、すべてのスパニングツリー インスタンスが前のモードで停止して新規モードで開始されるため、トラフィックが中断されます。

STP 拡張機能

このソフトウェアは、次に示すシスコ独自の機能をサポートしています。

- スパニングツリー ポート タイプ：デフォルトのスパニングツリー ポート タイプは、標準（normal）です。レイヤ2ホストに接続するインターフェイスをエッジ ポートとして、また、レイヤ2スイッチまたはブリッジに接続するインターフェイスをネットワーク ポートとして設定できます。
- ブリッジ保証：ポートをネットワーク ポートとして設定すると、ブリッジ保証によりすべてのポート上に BPDU が送信され、BPDU を受信しないポートはブロッキング ステートに移行します。この拡張機能を使用できるのは、Rapid PVST+ または MST を実行する場合だけです。

- BPDU ガード：BPDU ガードは、BPDU を受信したポートをシャットダウンします。
- BPDU フィルタ：BPDU フィルタは、ポート上での BPDU の送受信を抑制します。
- ループ ガード：ループ ガードは、ポイントツーポイント リンク上の単方向リンク障害が原因で発生するブリッジング ループを防止します。
- ルート ガード：ルート ガードは、ポートがルート ポートまたはブロッキングされたポートになることを防ぎます。ルート ガードに設定されたポートが上位 BPDU を受信すると、このポートはただちにルートとして一貫性のない（ブロッキングされた）状態になります。



第 3 章

レイヤ 2 スイッチングの設定

レイヤ 2 スイッチングについて

Note インターフェイスの作成の詳細については、『Cisco Nexus 3600 Series NX-OS Interfaces Configuration Guide』を参照してください。

レイヤ2スイッチング ポートは、アクセス ポートまたはトランク ポートとして設定できます。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することができます。レイヤ 2 スイッチング ポートはすべて、MAC アドレス テーブルを維持します。

レイヤ 2 イーサネット スイッチングの概要

このデバイスは、レイヤ2イーサネット セグメント間の同時パラレル接続をサポートします。イーサネット セグメント間のスイッチド コネクションは、パケットが伝送されている間だけ維持されます。次のパケットには、別のセグメント間に新しい接続が確立されます。

また、このデバイスでは、各デバイス（サーバなど）を独自のコリジョン ドメインに割り当てることによって、広帯域デバイスおよび多数のユーザによって発生する輻輳の問題を解決できます。各 LAN ポートが個別のイーサネット コリジョン ドメインに接続されるので、スイッチド環境のサーバは全帯域幅にアクセスできます。

イーサネット ネットワークではコリジョンによって深刻な輻輳が発生するため、全二重通信を使用することが有効な対処法の 1 つとなります。一般的に、10/100 Mbps イーサネットは半二重モードで動作するので、各ステーションは送信または受信のどちらかしか実行できません。これらのインターフェイスを全二重モードに設定すると、2 つのステーション間で同時に送受信を実行できます。パケットを双方向へ同時に送ることができるので、有効なイーサネット帯域幅は 2 倍になります。

セグメント間のフレーム スイッチング

デバイス上の各LANポートは、単一のワークステーション、サーバ、またはワークステーションやサーバがネットワークへの接続時に経由する他のデバイスに接続できます。

信号の劣化を防ぐために、デバイスは各 LAN ポートを個々のセグメントとして処理します。異なる LAN ポートに接続しているステーションが相互に通信する必要がある場合、デバイスは、一方のLANポートから他方のLANポートにワイヤ速度でフレームを転送し、各セッションが全帯域幅を利用できるようにします。

デバイスは、LAN ポート間で効率的にフレームをスイッチングするために、アドレス テーブルを管理しています。デバイスは、フレームを受信すると、受信した LAN ポートに、送信側ネットワーク デバイスのメディア アクセス コントロール（MAC）アドレスを関連付けます。

アドレス テーブルの構築およびアドレス テーブルの変更

デバイスは、受信したフレームの送信元MACアドレスを使用して、アドレス テーブルをダイナミックに構築します。自分のアドレス テーブルに登録されていない宛先MACアドレスを持つフレームを受信すると、デバイスは、そのフレームを同じ VLAN のすべての LAN ポート（受信したポートは除く）に送出します。宛先端末が応答を返してきたら、デバイスは、その応答パケットの送信元 MAC アドレスとポート ID をアドレス テーブルに追加します。以降、その宛先へのフレームを、すべてのLANポートに送出せず、単一のLANポートだけに転送します。

スタティック MAC アドレスと呼ばれる、デバイス上の特定のインターフェイスだけをスタティックに示すMACアドレスを設定できます。スタティックMACアドレスは、インターフェイス上でダイナミックに学習された MAC アドレスをすべて書き換えます。ブロードキャストのアドレスは、スタティック MAC アドレスとして設定できません。スタティック MAC エントリは、デバイスのリブート後も保持されます。

仮想ポート チャネル（vPC）ピア リンクにより接続されている両方のデバイスに、同一のスタティック MAC アドレスを手動で設定する必要があります。MAC アドレス テーブルの表示が拡張されて、vPCを使用しているMACアドレスに関する情報が表示されるようになりました。

vPC の詳細については、Cisco Nexus 3600 Series NX-OS Interfaces Configuration Guide を参照してください。

アドレス テーブルは、ハードウェアのI/Oモジュールに応じて多数のMACアドレス エントリを格納できます。デバイスは、設定可能なエージング タイマーによって定義されるエージング メカニズムを使用しているため、アドレスが非アクティブな状態のまま指定時間（秒）が経過すると、そのアドレスはアドレス テーブルから削除されます。

スーパーバイザおよびモジュール上で一貫した MAC アドレス テーブル

各モジュールのすべての MAC アドレス テーブルが、スーパーバイザ上の MAC アドレスと正確に一致するのが理想的です。**show forwarding consistency l2** コマンドまたは **show consistency-checker l2** コマンドを入力すると、不一致、欠落、および余分の MAC アドレス エントリが表示されます。

レイヤ 3 スタティック MAC アドレス

スタティック MAC アドレスは、次のレイヤ 3 インターフェイスに設定できます。

- レイヤ 3 インターフェイス
- レイヤ 3 サブインターフェイス
- レイヤ 3 ポート チャネル
- VLAN ネットワーク インターフェイス

（注） トンネル インターフェイスにはスタティック MAC アドレスを設定できません。

レイヤ 3 インターフェイスの設定の詳細については、『Cisco Nexus 3600 Series NX-OS Interfaces Configuration Guide』を参照してください。

スイッチングのハイ アベイラビリティ

従来のイーサネット スイッチングごとに、ソフトウェアのアップグレードまたはダウングレードをシームレスに実行できます。レイヤ 3 インターフェイス上にスタティック MAC アドレスを設定している場合、ソフトウェアをダウングレードするために、これらのポートの設定を解除する必要があります。

MAC アドレス設定の前提条件

MAC アドレスには次の前提条件があります。

- デバイスにログインしていること。
- 必要に応じて、アドバンスド サービスのライセンスをインストールします。

レイヤ 2 スイッチングのデフォルト設定

次の表に、レイヤ 2 スイッチングのパラメータのデフォルト設定を示します。

Table 2: **レイヤ *2* スイッチング パラメータのデフォルト値**

パラメータ	デフォルト
エージング タイム	1800 秒

レイヤ 2 スイッチングの設定手順

Note Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

スタティック MAC アドレスの設定

スタティック MAC アドレスと呼ばれる、デバイス上の特定のインターフェイスだけをスタティックに示すMACアドレスを設定できます。スタティックMACアドレスは、インターフェイス上でダイナミックに学習された MAC アドレスをすべて書き換えます。ブロードキャストまたはマルチキャストのアドレスは、スタティック MAC アドレスとして設定できません。

SUMMARY STEPS

1. **config t**
2. **mac address-table static** *mac-address* **vlan** *vlan-id* {[**drop** | **interface** {*type slot/port*} | **port-channel** *number*]}
3. **exit**
4. (Optional) **show mac address-table static**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	Command or Action	Purpose
ステップ 2	**mac address-table static** *mac-address* **vlan** *vlan-id* {[**drop** | **interface** {*type slot/port*} | **port-channel** *number*]} **Example:** `switch(config)# mac address-table static 1.1.1 vlan 2 interface ethernet 1/2`	レイヤ 2 MAC アドレス テーブルに追加するスタティック MAC アドレスを指定します。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	(Optional) **show mac address-table static** **Example:** `switch# show mac address-table static`	スタティック MAC アドレスを表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、レイヤ 2 MAC アドレス テーブルにスタティック エントリを入力する例を示します。

```
switch# config t
switch(config)# mac address-table static 1.1.1 vlan 2 interface ethernet 1/2
switch(config)#
```

レイヤ 3 インターフェイス上のスタティック MAC アドレスの設定

レイヤ 3 インターフェイスのスタティック MAC アドレスを設定できます。ブロードキャストまたはマルチキャストのアドレスは、スタティック MAC アドレスとして設定できません。

Note トンネル インターフェイス上には、スタティック MAC アドレスを設定できません。

Note この設定は、16 の VLAN インターフェイスに制限されます。追加の VLAN インターフェイスに設定を適用すると、ハードウェアプログラムが失敗したインターフェイスがダウン状態になります。ステータス。

レイヤ 3 インターフェイスの設定の詳細については、『Cisco Nexus 3600 Series NX-OS Interfaces Configuration Guide』を参照してください。

SUMMARY STEPS

1. **config t**
2. **interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*]
3. **mac-address** *mac-address*
4. **exit**
5. (Optional) **show interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** [**ethernet** *slot/port*	**ethernet** *slot/port.number*	**port-channel** *number*	**vlan** *vlan-id*] **Example:** `switch(config)# interface ethernet 7/3`	レイヤ 3 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。 **Note** スタティック MAC アドレスを割り当てる前に、レイヤ 3 インターフェイスを作成する必要があります。

ステップ 3	**mac-address** *mac-address*
	Example:
	`switch(config-if)# mac-address 22ab.47dd.ff89`
	`switch(config-if)#`
		レイヤ 3 インターフェイスに追加するスタティック MAC アドレスを指定します。

ステップ 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	(Optional) **show interface** [**ethernet** *slot/port*	**ethernet** *slot/port.number*	**port-channel** *number*	**vlan** *vlan-id*] **Example:** `switch# show interface ethernet 7/3`	レイヤ 3 インターフェイスに関する情報を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、スロット 7、ポート 3 上のレイヤ 3 インターフェイスにスタティック MAC アドレスを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 7/3
switch(config-if)# mac-address 22ab.47dd.ff89
switch(config-if)#
```

MAC テーブルのエージング タイムの設定

MAC アドレス エントリ（パケットの送信元 MAC アドレスおよびパケットを学習したポート）を、レイヤ 2 情報を含む MAC テーブルに格納しておく時間を設定できます。

Note MAC アドレスのエージング タイムアウトの最大時間は、設定された MAC アドレス テーブルのエージング タイムアウトの 2 倍です。

Note インターフェイス コンフィギュレーション モードまたは VLAN コンフィギュレーション モードで MAC エージング タイムを設定することもできます。

SUMMARY STEPS

1. **config t**
2. **mac address-table aging-time** *seconds*
3. **exit**
4. (Optional) **show mac address-table aging-time**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**mac address-table aging-time** *seconds* **Example:** `switch(config)# mac address-table aging-time 600`	エントリが期限切れになり、レイヤ 2 MAC アドレス テーブルから廃棄される前にエージング タイムを指定します。指定できる範囲は 120 ～ 918000 秒です。デフォルトは 1800 秒です。0 を入力すると、MAC エージングがディセーブルになります。

	Command or Action	Purpose

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	(Optional) **show mac address-table aging-time** **Example:** `switch# show mac address-table aging-time`	MAC アドレスを保持するエージング タイム設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、レイヤ 2 MAC アドレス テーブルのエントリのエージング タイムを 600 秒（10 分）に設定する例を示します。

```
switch# config t
switch(config)# mac address-table aging-time 600
switch(config)#
```

MAC アドレス テーブルの整合性検査

スーパーバイザ上の MAC アドレス テーブルとすべてのモジュールの一致を確認できるようになりました。

Note または、 **show consistency-checker l2** {*module_number*} を使用することもできます。 MACアドレステーブルの整合性を確認します。

例：

```
switch# show consistency-checker l2 module 1
switch#
```

SUMMARY STEPS

1. **show forwarding consistency l2** {*module_number*}

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	**show forwarding consistency l2** {*module_number*} **Example:**	スーパーバイザと指定のモジュールの間の、矛盾、不足、余分な MAC アドレスを表示します。

	Command or Action	Purpose
	`switch# show forwarding consistency l2 7` `switch#`	

Example

次に、スーパーバイザと指定のモジュールの間の、MACアドレステーブル内の矛盾、不足、余分なエントリを表示する例を示します。

```
switch# show forwarding consistency l2 7
switch#
```

MAC テーブルからのダイナミック アドレスのクリア

MAC アドレス テーブルにある、すべてのダイナミック レイヤ 2 エントリをクリアできます。（指定したインターフェイスまたは VLAN によりエントリをクリアすることもできます。）

SUMMARY STEPS

1. **clear mac address-table dynamic** {**address** *mac_addr*} {**interface** [**ethernet** *slot/port* | **port-channel** *channel-number*]} {**vlan** *vlan_id*}
2. (Optional) **show mac address-table**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	**clear mac address-table dynamic** {**address** *mac_addr*} {**interface** [**ethernet** *slot/port* | **port-channel** *channel-number*]} {**vlan** *vlan_id*} **Example:** `switch# clear mac address-table dynamic`	レイヤ 2 の MAC アドレス テーブルから、ダイナミック アドレス エントリをクリアします。
ステップ 2	(Optional) **show mac address-table** **Example:** `switch# show mac address-table`	MAC Address Table を表示します。

Example

次に、レイヤ 2 MAC アドレス テーブルからダイナミック エントリをクリアする例を示します。

```
switch# clear mac address-table dynamic
switch#
```

MAC アドレス制限の設定

SUMMARY STEPS

1. **config t**
2. **mac address-table limit vlan** *vlan-id limit -value*
3. **exit**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**mac address-table limit vlan** *vlan-id limit -value* **Example:** `switch(config)# mac address-table limit vlan 40 108`	MAC アドレスの制限を適用する VLAN を指定します。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

レイヤ 2 スイッチング設定の確認

レイヤ 2 スイッチングの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show mac address-table	MACアドレステーブルに関する情報を表示します。
show mac address-table limit	MACアドレステーブルの制限設定に関する情報を表示します。

コマンド	目的
show mac address-table aging-time	MACアドレステーブルに設定されているエージング タイムの情報を表示します。
show mac address-table static	MACアドレステーブルのスタティック エントリの情報を表示します。
show interface [*interface*] **mac-address**	インターフェイスのMACアドレスとバーンドインMACアドレスを表示します。
show forwarding consistency l2 {*module*}	モジュールとスーパーバイザのテーブル間の不一致、不明、および追加のMACアドレスを表示します。

レイヤ 2 スイッチングの設定例

次に、スタティック MAC アドレスを追加し、MAC アドレスのデフォルトのグローバル エージング タイムを変更する例を示します。

```
switch# configure terminal
switch(config)# mac address-table static 0000.0000.1234 vlan 10 interface ethernet 2/15
switch(config)# mac address-table aging-time 120
```

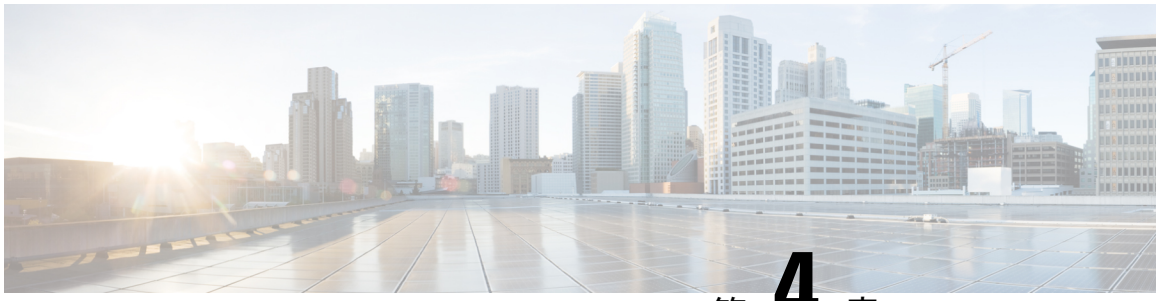
レイヤ 2 スイッチングの追加情報（CLI バージョン）

関連資料

関連項目	マニュアル タイトル
スタティックMACアドレス	『*Cisco Nexus 3600 Series NX-OS Security Configuration Guide*』
インターフェイス	『*Cisco Nexus 3600 Series NX-OS Interfaces Configuration Guide*』
システム管理	『*Cisco Nexus 3600 Series NX-OS System Management Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—



第 4 章

VLAN の設定

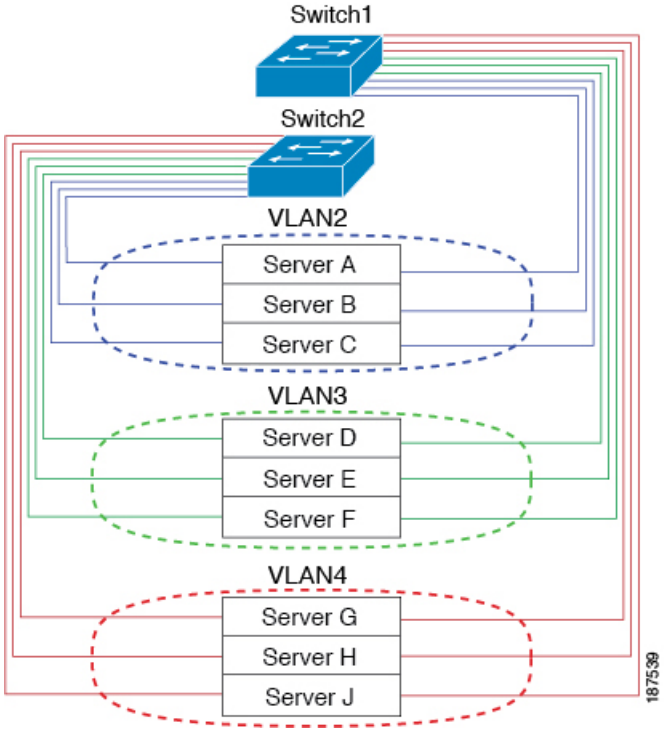
VLAN について

VLAN の概要

VLANは、ユーザの物理的な場所に関係なく、機能またはアプリケーションによって論理的にセグメント化されるスイッチド ネットワーク内の端末のグループです。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 に属する端末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であると見なされます。VLAN に属していないステーション宛てのパケットは、ルータを経由して転送する必要があります。次の図は、論理ネットワークとしての VLAN を図示したものです。エンジニアリング部門のステーション、マーケティング部門のステーション、および会計部門のステーションはそれぞれ別の VLAN に割り当てられています。

Figure 1: 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関連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。VLAN 間で通信するには、トラフィックをルーティングする必要があります。

デフォルトでは、新規に作成された VLAN は動作可能です。つまり、新規に作成された VLAN は、非シャットダウンの状態になります。また、トラフィックを通過させるアクティブ ステート、またはパケットを通過させない一時停止ステートに、VLAN を設定することもできます。デフォルトでは、VLAN はアクティブ ステートでトラフィックを通過させます。

VLAN 範囲

Note Cisco NX-OS デバイスでは、拡張システム ID が常に自動的にイネーブルになります。

このデバイスは、IEEE 802.1Q 規格に従って、最大 4094 の VLAN をサポートします。これらの VLAN は、ソフトウェアによっていくつかの範囲に分割され、範囲によって用途が少しずつ異なります。

設定制限に関する詳細については、Cisco Nexus 3600 プラットフォーム スイッチのマニュアルで設定制限についての説明を参照してください。

この表では、VLAN 範囲について説明します。

***Table 3: VLAN* 範囲**

VLAN の番号	数の範囲	使用法
1	標準	シスコのデフォルトです。このVLANは使用できますが、変更と削除はできません。
2 ～ 1005	標準	これらの VLAN は作成、使用、変更、および削除ができます。
1006 ～ 3967 と 4048 ～ 4093	拡張	これらの VLAN は作成、命名、使用ができます。以下のパラメータは変更できません。 • ステートは必ず、アクティブです。 • VLAN は常にイネーブルです。これらの VLAN はシャット ダウンできません。
3968 ～ 4047 と 4094	内部割り当て	これらの 80 の VLAN と VLAN 4094 は、内部デバイス用に割り当てられています。内部使用のために予約されたブロック内にある VLAN は、作成、削除、および変更はできません。

このソフトウェアは、内部VLANの使用を必要とするマルチキャストや診断などの機能用に、VLAN 番号のグループを割り当てます。予約グループの VLAN の使用、変更、削除はできません。内部的に割り当てられている VLAN、およびそれに関連した用途は表示できます。

VLAN の作成、削除、変更

VLAN には 1 ～ 4094 の番号が付けられます。スイッチを初めて起動したとき、すべての設定済みポートはデフォルト VLAN に属します。デフォルト VLAN（VLAN1）では、デフォルト値のみ使用されます。デフォルト VLAN では、アクティビティの作成、削除、および一時停止は行えません。

VLAN を作成する際は、その VLAN に番号を割り当てます。VLAN は削除することもできますが、アクティブ動作ステートから一時停止動作ステートに移行することもできます。既存の VLAN ID で VLAN を作成しようとすると、スイッチは VLAN サブモードになりますが、同一の VLAN は再作成しません。

新しく作成した VLAN は、その VLAN にポートが割り当てられるまで使用されません。すべてのポートはデフォルトで VLAN1 に割り当てられます。

VLAN の範囲により、次のパラメータを VLAN 用に設定できます（デフォルト VLAN を除く）。

- VLAN 名
- シャットダウンまたは非シャットダウン

特定の VLAN を削除すると、その VLAN に関連するポートはシャットダウンされ、トラフィックは流れなくなります。ただし、システムではその VLAN の VLAN/ポート マッピングがすべて維持されるため、その VLAN の再イネーブル化 や再作成を行うと、その VLAN の元のポートはすべて自動的に回復します。

VLAN の設定

VLAN の作成および削除

デフォルト VLAN およびスイッチによる使用のために内部的に割り当てられている VLAN を除き、すべての VLAN は、作成または削除が可能です。VLAN を作成すると、その VLAN は自動的にアクティブ ステートになります。

Note VLAN を削除すると、その VLAN にアソシエートされたポートはシャットダウンします。トラフィックは流れなくなり、パケットはドロップされます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan** {*vlan-id* | *vlan-range*}
3. switch(config-vlan)# **no vlan** {*vlan-id* | *vlan-range*}

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **vlan** {*vlan-id* | *vlan-range*}	単独の VLAN またはある範囲に属する複数の VLAN を作成します。 VLAN にすでに割り当てられている番号を入力すると、その VLAN の VLAN コンフィギュレーション サブモードがスイッチによって開始されます。内部的に割り当てられている VLAN に割り当てられている番号を入力すると、エラー メッセージが返されます。VLAN の範囲を入力し、指定 VLAN の 1 つ以上が、内部的に割り当てられた VLAN の範囲外である場合、コマンドは範囲外の VLAN だけで有効になります。指定できる範囲は 2 ～ 4094 です。VLAN1 はデフォルト VLAN であり、作成や削除はできませ

	Command or Action	Purpose
		ん。内部使用のために予約されている VLAN の作成や削除はできません。
ステップ 3	switch(config-vlan)# **no vlan** {*vlan-id* | *vlan-range*}	指定した VLAN または VLAN の範囲を削除し、VLAN コンフィギュレーション サブモードを終了します。VLAN1 または内部的に割り当てられている VLAN は削除できません。

Example

次の例は、15 ～ 20 の範囲で VLAN を作成する方法を示しています。

```
switch# configure terminal
switch(config)# vlan 15-20
```

Note VLAN コンフィギュレーション サブモードで VLAN の作成と削除を行うこともできます。

VLAN の設定

VLAN の次のパラメータの設定または変更を行うには、VLAN コンフィギュレーション サブモードを開始する必要があります。

- 名前
- シャットダウン

Note デフォルト VLAN または内部的に割り当てられた VLAN の作成、削除、変更はできません。また、一部の VLAN では変更できないパラメータがあります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan** {*vlan-id* | *vlan-range*}
3. switch(config-vlan)# **name** *vlan-name*
4. switch(config-vlan)# **state** {**active** | **suspend**}
5. (Optional) switch(config-vlan)# **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **vlan** {*vlan-id* | *vlan-range*}	VLAN コンフィギュレーション サブモードを開始します。VLAN が存在しない場合は、先に指定 VLAN が作成されます。
ステップ 3	switch(config-vlan)# **name** *vlan-name*	VLAN に名前を付けます。32 文字までの英数字を入力して VLAN に名前を付けることができます。VLAN1 または内部的に割り当てられている VLAN の名前は変更できません。デフォルト値はVLANxxxx であり、xxxx は、VLAN ID 番号と等しい 4 桁の数字（先行ゼロも含む）を表します。
ステップ 4	switch(config-vlan)# **state** {**active** | **suspend**}	VLAN のステート（アクティブまたは一時停止）を設定します。VLAN ステートを一時停止（suspended）にすると、その VLAN に関連付けられたポートがシャットダウンし、VLAN のトラフィック転送が停止します。デフォルト ステートは active です。デフォルト VLAN および VLAN 1006 ～ 4094 のステートを一時停止にすることはできません。
ステップ 5	(Optional) switch(config-vlan)# **no shutdown**	VLAN をイネーブルにします。デフォルト値は **no shutdown**（つまりイネーブル）です。デフォルト VLAN の VLAN1、または VLAN 1006 ～ 4094 はシャットダウンできません。

Example

次の例は、VLAN 5 のオプション パラメータを設定する方法を示しています。

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# name accounting
switch(config-vlan)# state active
switch(config-vlan)# no shutdown
```

VLAN へのポートの追加

VLAN の設定が完了したら、ポートを割り当てます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
3. switch(config-if)# **switchport access vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** {**ethernet** *slot*/*port* | **port-channel** *number*}	設定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。インターフェイスは、物理イーサネット ポートでも EtherChannel でもかまいません。
ステップ 3	switch(config-if)# **switchport access vlan** *vlan-id*	インターフェイスのアクセス モードを指定 VLAN に設定します。

Example

次の例は、VLAN 5 に参加するようにイーサネット インターフェイスを設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/13
switch(config-if)# switchport access vlan 5
```

VLAN メンバシップ整合性チェッカーのトリガー

VLAN メンバシップ整合性チェッカーを手動でトリガーして、VLAN 上のすべてのポートのハードウェア設定とソフトウェア設定を比較し、結果を表示することができます。VLAN メンバシップ整合性チェッカーを手動でトリガーして結果を表示するには、次のコマンドを特定のモードで使用します。

手順の概要

1. switch# **show consistency-checker membership vlan** *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	switch# **show consistency-checker membership vlan** *vlan-id*	*vlan-id* のメンバー ポートに対する VLAN メンバーシップ整合性検査を開始して結果を表示します。

例

次に、VLANメンバーシップ整合性検査をトリガーして結果を表示する例を示します。

```
switch# show consistency-checker membership vlan 2
Checks: Port membership of Vlan
Vlan  2 :
Consistency Check: PASSED
 Vlan:2, Hardware state consistent for:
   Ethernet1/18
   Ethernet1/20
   Ethernet1/29
   Ethernet1/30
   Ethernet1/31
   Ethernet1/32
   Ethernet1/33
   Ethernet1/34
   Ethernet1/35
   Ethernet1/36
   Ethernet1/37
   Ethernet1/38
   Ethernet1/39
   Ethernet1/4
   Ethernet1/40
   Ethernet1/41
   Ethernet1/42
   Ethernet1/43
   Ethernet1/44
   Ethernet1/45
   Ethernet1/46
   Ethernet1/47
   Ethernet1/48
   Ethernet1/5
   Ethernet1/6
```

ルーテッド SVI としての VLAN の設定

ルーテッド スイッチ仮想インターフェイス（SVI）となるように VLAN を設定できます。

始める前に

- レイヤ 3 ライセンスをインストールします。詳細については、*Cisco NX-OS* ソフトウェアのライセンスおよび版権情報 は、次の URL から入手できます。http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html を参照してください。
- この機能の注意事項および制限事項を必ず理解するようにしてください。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature interface-vlan**
3. switch(config)# **interface-vlan** *vlan-id*
4. switch(config-if)# **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	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	switch(config)# **feature interface-vlan**	SVI の作成をイネーブルにします。
ステップ 3	switch(config)# **interface-vlan** *vlan-id*	VLANインターフェイス（SVI）を作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	switch(config-if)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

次に、VLAN をルーテッド SVI として設定する例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# interface vlan 5
switch(config-if)# copy running-config startup-config
switch(config-if)#
```

次に、VLAN からルーテッド SVI 機能を削除する例を示します。

```
switch# configure terminal
switch(config)# no interface vlan 5
switch(config-if)# copy running-config startup-config
switch(config-if)#
```

次のタスク

このインターフェイスでルーティング プロトコルを設定できます。

管理 SVI としての VLAN の設定

管理スイッチ仮想インターフェイス（SVI）となるように VLAN を設定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature interface-vlan**
3. switch(config)# **interface-vlan** *vlan-id* **management**
4. switch(config-if)# **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	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	switch(config)# **feature interface-vlan**	SVI の作成をイネーブルにします。
ステップ 3	switch(config)# **interface-vlan** *vlan-id* **management**	VLAN インターフェイス（SVI）を作成し、SVI をインバンド管理に使用するように設定します。
ステップ 4	switch(config-if)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

次に、VLAN を管理 SVI として設定する例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# interface vlan 5
switch(config-if)# management
switch(config-if)# copy running-config startup-config
switch(config-if)#
```

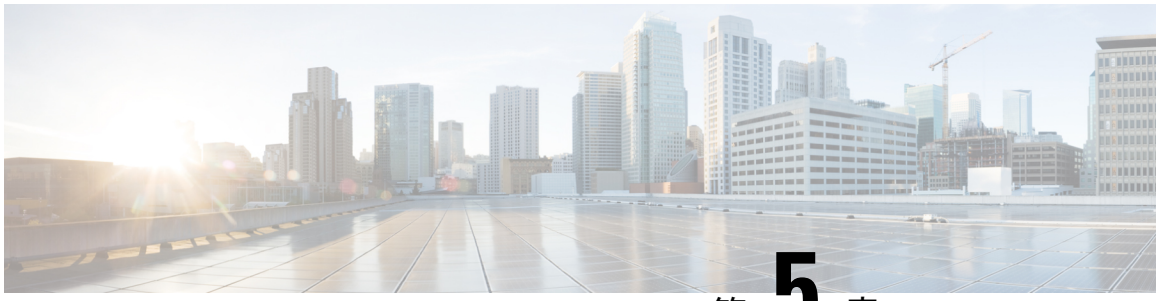
次に、SVI から管理機能を削除する例を示します。

```
switch# configure terminal
switch(config)# interface vlan 5
switch(config-if)# no management
switch(config-if)# copy running-config startup-config
switch(config-if)#
```

VLAN の設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
switch# **show running-config vlan** [*vlan_id* | *vlan_range*]	VLAN 情報を表示します。
switch# **show vlan** [**brief** | **id** [*vlan_id* | *vlan_range*] | **name** *name* | **summary**]	定義済み VLAN の選択した設定情報を表示します。



第 5 章

アクセス インターフェイスとトランク インターフェイスの設定

アクセスインターフェイスとトランクインターフェイスについて

アクセス インターフェイスとトランク インターフェイスの概要

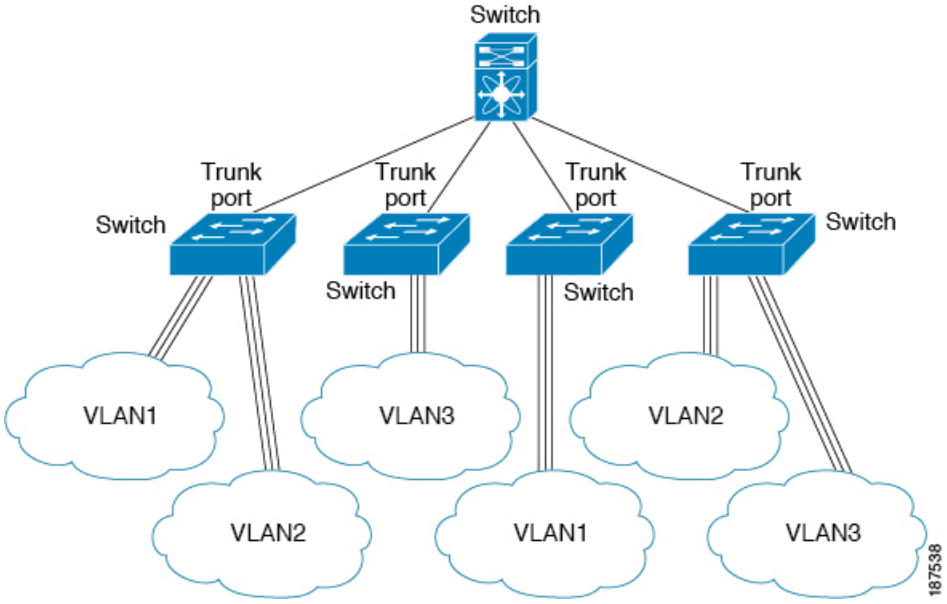
イーサネット インターフェイスは、次のように、アクセス ポートまたはトランク ポートとして設定できます。

- アクセス ポートはインターフェイス上に設定された 1 つの VLAN だけに対応し、1 つの VLAN のトラフィックだけを伝送します。
- トランク ポートはインターフェイス上に設定された 2 つ以上の VLAN に対応しているため、複数の VLAN のトラフィックを同時に伝送できます。

Note Cisco NX-OS では、IEEE 802.1Q タイプの VLAN トランク カプセル化だけをサポートしています。

次の図は、ネットワークにおけるトランク ポートの使い方を示したものです。トランク ポートは、2 つ以上の VLAN のトラフィックを伝送します。

Figure 2: トランキング環境におけるデバイス



複数の VLAN に対応するトランク ポートでトラフィックが正しく送信されるようにするため、デバイスでは IEEE 802.1Q カプセル化（タギング）方式が使用されます。

アクセス ポートでのパフォーマンスを最適化するには、そのポートをホスト ポートとして設定します。ホスト ポートとして設定されたポートは、自動的にアクセス ポートとして設定され、チャネル グループ化はディセーブルになります。ホスト ポートを使用すると、指定ポートがパケットの転送を開始するための所要時間を短縮できます。

Note ホスト ポートとして設定できるのは端末だけです。端末以外のポートをホストとして設定しようとするとエラーになります。

アクセス ポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。

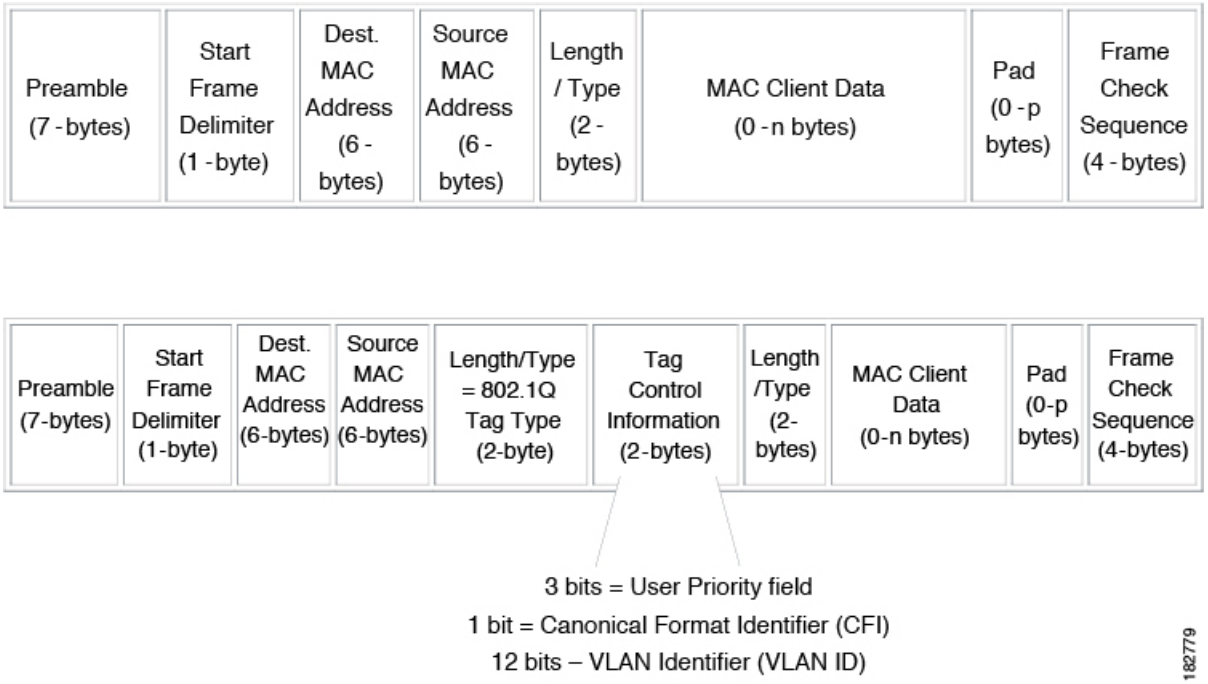
Note イーサネット インターフェイスはアクセス ポートまたはトランク ポートとして動作できますが、両方のポート タイプとして同時に動作することはできません。

IEEE 802.1Q カプセル化の概要

トランクは、デバイスと他のネットワーク デバイス間のポイントツーポイント リンクです。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することができます。

複数の VLAN に対応するトランク ポートでトラフィックが正しく送信されるようにするため、デバイスでは IEEE 802.1Q カプセル化（タギング）方式が使用されます。このタグには、そのフレームおよびパケットが属する特定の VLAN に関する情報が含まれます。タグ方式を使用すると、複数の異なる VLAN 用にカプセル化されたパケットが、同じポートを通過しても、各 VLAN のトラフィックを区別することができます。

***Figure 3: 802.1Q* タグが含まれているヘッダーと含まれていないヘッダー**



アクセス VLAN の概要

アクセス モードでポートを設定すると、そのインターフェイスのトラフィックを伝送する VLAN を指定できます。アクセス モードのポート（アクセス ポート）用に VLAN を設定しないと、そのインターフェイスはデフォルトの VLAN（VLAN1）のトラフィックだけを伝送します。

VLAN のアクセス ポート メンバーシップを変更するには、新しい VLAN を指定します。VLAN をアクセス ポートのアクセス VLAN として割り当てるには、まず、VLAN を作成する必要があります。アクセス ポート上のアクセス VLAN を、まだ作成されていない VLAN に変更すると、システムはそのアクセス ポートをシャット ダウンします。

Note アクセス ポートまたはトランク ポートで VLAN を変更すると、インターフェイスがフラップします。ただし、ポートが vPC の一部である場合は、最初にセカンダリ vPC のネイティブ VLAN を変更してから、プライマリ vPC に変更します。

アクセス ポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。

トランク ポートのネイティブ VLAN ID の概要

トランク ポートは、タグなしのパケットと 802.1Q タグ付きのパケットを同時に伝送できます。デフォルトのポート VLAN ID をトランク ポートに割り当てると、すべてのタグなしトラフィックが、そのトランク ポートのデフォルトのポート VLAN ID で伝送され、タグなしトラフィックはすべてこの VLAN に属するものと見なされます。この VLAN のことを、トランク ポートのネイティブ VLAN ID といいます。ネイティブ VLAN ID とは、トランク ポート上でタグなしトラフィックを伝送する VLAN のことです。

トランク ポートは、デフォルトのポート VLAN ID と同じ VLAN が設定された出力パケットをタグなしで送信します。他のすべての出力パケットは、トランク ポートによってタグ付けされます。ネイティブ VLAN ID を設定しないと、トランク ポートはデフォルト VLAN を使用します。

Note ネイティブ VLAN ID 番号は、トランクの両端で一致していなければなりません。

許可 VLAN の概要

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。各トランク上では、すべての VLAN ID が許可されます。この包括的なリストから VLAN を削除することによって、特定の VLAN からのトラフィックが、そのトランクを通過するのを禁止できます。トランク経由でトラフィックを伝送したい VLAN を後でリストに戻すこともできます。

デフォルト VLAN のスパニングツリープロトコル（STP）トポロジを区切るには、許容 VLAN のリストから VLAN1 を削除します。この分割を行わないと、VLAN1（デフォルトでは、すべてのポートでイネーブル）が非常に大きな STP トポロジを形成し、STP の収束時に問題が発生する可能性があります。VLAN1 を削除すると、そのポート上で VLAN1 のデータ トラフィックはすべてブロックされますが、制御トラフィックは通過し続けます。

ネイティブ 802.1Q VLAN の概要

802.1Q トランク ポートを通過するトラフィックのセキュリティを高めるため、**vlan dot1q tag native** コマンドが導入されました。この機能により、802.1Q トランク ポートから送信されるすべてのパケットが必ずタグ付けされるとともに、タグなしのパケットが 802.1Q トランク ポートで受信されないようにすることができるようになりました。

この機能がない場合、802.1Q トランク ポートで受信されたタグ付き入力フレームは、許可 VALN のリストに含まれる限り受信が許可され、それらのタグは維持されます。タグなしフレームについては、トランク ポートのネイティブ VLAN ID でタグ付けされたうえで、それ以降の処理が行われます。出力フレームは、その VLAN タグが 802.1Q トランク ポートで許可さ

アクセス インターフェイスとトランク インターフェイスの設定

れる範囲内に属する場合に限って受信されます。フレームの VLAN タグが、トランク ポートのネイティブ VLAN のタグと一致した場合、その VLAN タグは取り除かれ、フレームはタグなしで送信されます。

この動作は、ハッカーがフレームを別の VLAN へジャンプさせる「VLAN ホッピング」に利用される可能性があります。また、タグなしパケットを 802.1Q トランク ポートへ送信することにより、トラフィックをネイティブ VLAN の一部にすることもできます。

こうした問題を解決するため、**vlan dot1q tag native** コマンドでは次のような機能を実行できるようになっています。

- 入力側では、タグなしのデータ トラフィックをすべてドロップする。
- 出力側では、すべてのトラフィックをタグ付けする。ネイティブ VLAN に属するトラフィックは、ネイティブ VLAN ID でタグ付けされます。

この機能は、すべての直接接続されたイーサネット インターフェイスおよびポート チャネル インターフェイスでサポートされます。

（注） コマンドをイネーブルにするには、グローバル コンフィギュレーション モードで **vlan dot1q tag native** コマンドを入力します。

アクセスインターフェイスとトランクインターフェイスの設定

LANインターフェイスをイーサネットアクセスポートとして設定する

イーサネット インターフェイスはアクセス ポートとして設定できます。アクセス ポートは、パケットを、1 つのタグなし VLAN 上だけで送信します。管理者は、そのインターフェイスで伝送する VLAN トラフィックを指定します。アクセス ポートの VLAN を指定しないと、そのインターフェイスは、デフォルト VLAN だけのトラフィックを伝送します。デフォルトの VLAN は VLAN 1 です。

VLAN をアクセス VLAN として指定するには、その VLAN が存在しなければなりません。システムは、存在しないアクセス VLAN に割り当てられたアクセス ポートをシャット ダウンします。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {{*type slot*/*port*} | {**port-channel** *number*}}
3. switch(config-if)# **switchport mode** {**access** | **trunk**}
4. switch(config-if)# **switchport access vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** {{*type slot*/*port*} | {**port-channel** *number*}}	設定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	switch(config-if)# **switchport mode** {**access** | **trunk**}	トランキングなし、タグなしの単一 VLAN イーサネット インターフェイスとして、インターフェイスを設定します。アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。デフォルトでは、アクセス ポートは VLAN1 のトラフィックを伝送します。異なる VLAN のトラフィックを伝送するようにアクセス ポートを設定するには、**switchport access vlan** を使用します
ステップ 4	switch(config-if)# **switchport access vlan** *vlan-id*	このアクセス ポートでトラフィックを伝送する VLAN を指定します。このコマンドを入力しないと、アクセス ポートは VLAN1 だけのトラフィックを伝送します。このコマンドを使用して、アクセス ポートがトラフィックを伝送する VLAN を変更できます。

Example

次に、指定された VLAN のみのトラフィックを送受信するイーサネット アクセス ポートとしてインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/10
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
```

アクセス ホスト ポートの設定

スイッチポート ホストを使用することにより、アクセス ポートをスパンニングツリー エッジ ポートにすることが可能であり、BPDU フィルタリングおよび BPDU ガードを同時にイネーブルにすることができます。

Before you begin

設定を行うインターフェイスが適切であることを確認します。対象となるインターフェイスは、エンド ステーションに接続されていることが必要です。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **switchport host**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** *type slot*/*port*	設定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	switch(config-if)# **switchport host**	Sets the interface to spanning-tree port type edge, turns on BPDU Filtering and BPDU Guard. **Note** このコマンドは、ホストに接続されたスイッチポートに対してのみ使用してください。

Example

次に、EtherChannel がディセーブルにされたイーサネット アクセス ホスト ポートとしてインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/10
switch(config-if)# switchport host
```

トランク ポートの設定

イーサネット ポートをトランク ポートとして設定できます。トランク ポートは、ネイティブ VLAN のタグなしパケット、および複数の VLAN のカプセル化されたタグ付きパケットを伝送します

Note Cisco NX-OS は、IEEE 802.1Q カプセル化だけをサポートしています。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {*type slot*/*port* | **port-channel** *number*}
3. switch(config-if)# **switchport mode** {**access** | **trunk**}

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** {*type slot*/*port* | **port-channel** *number*}	設定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	switch(config-if)# **switchport mode** {**access** | **trunk**}	インターフェイスをイーサネット トランク ポートとして設定します。トランク ポートは、同じ物理リンクで 1 つ以上の VLAN 内のトラフィックを伝送できます（各 VLAN はトランキングが許可された VLAN リストに基づいています）。デフォルトでは、トランク インターフェイスはすべての VLAN のトラフィックを伝送できます。特定のトランク上で特定の VLAN だけを許可するように指定するには、**switchport trunk allowed vlan** コマンドを使用します。

Example

次の例は、インターフェイスをイーサネット トランク ポートとして設定する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport mode trunk
```

802.1Q トランク ポートのネイティブ VLAN の設定

このパラメータを設定しないと、トランク ポートは、デフォルト VLAN をネイティブ VLAN ID として使用します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {*type slot*/*port* | **port-channel** *number*}
3. switch(config-if)# **switchport trunk native vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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。

	Command or Action	Purpose
ステップ 2	switch(config)# **interface** {*type slot*/*port* | **port-channel** *number*}	設定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	switch(config-if)# **switchport trunk native vlan** *vlan-id*	802.1Q トランクのネイティブ VLAN を設定します。指定できる範囲は 1 ～ 4094 です（ただし、内部使用に予約されている VLAN は除きます）。デフォルト値は VLAN 1 です。

Example

次の例は、イーサネット トランク ポートに対してネイティブ VALN を設定する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport trunk native vlan 5
```

トランキング ポートの許可 VLAN の設定

特定のトランク ポートで許可されている VLAN の ID を指定できます。

指定トランク ポートの許可 VLAN を設定する前に、正しいインターフェイスを設定していること、およびそのインターフェイスがトランクであることを確認してください。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {*type slot*/*port* | **port-channel** *number*}
3. switch(config-if)# **switchport trunk allowed vlan** {*vlan-list* **all** | **none** [**add** |except | none | **remove** {*vlan-list*}]}

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** {*type slot*/*port* | **port-channel** *number*}	設定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	switch(config-if)# **switchport trunk allowed vlan** {*vlan-list* **all** | **none** [**add** |except | none | **remove** {*vlan-list*}]}	トランク インターフェイスの許可 VLAN を設定します。デフォルトでは、トランク インターフェイス上のすべての VLAN（1 ～ 3967 および 4048 ～ 4094）が許可されます。VLAN 3968 ～ 4047 は、内部利用

	Command or Action	Purpose
		のためにデフォルトで予約されているVLANです。このVLANグループは設定できません。デフォルトでは、すべてのトランク インターフェイスですべての VLAN が許可されます。 **Note** 内部で割り当て済みの VLAN を、トランク ポート上の許可 VLAN として追加することはできません。内部で割り当て済みの VLAN を、トランク ポートの許可 VLAN として登録しようとすると、メッセージが返されます。

Example

次の例は、イーサネット トランク ポートの許可 VLAN のリストにいくつかの VLAN を追加する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport trunk allow vlan 15-20
```

ネイティブ 802.1Q VLAN の設定

通常は、ネイティブ VLAN ID で 802.1Q トランクを設定します。これによって、その VLAN 上のすべてのパケットからタギングが取り除かれます。この設定は、すべてのタグなしトラフィックと制御トラフィックが Cisco Nexus デバイスを通過できるようにします。ネイティブ VLAN ID の値と一致する 802.1Q タグを持つ、スイッチに着信するパケットも、同様にタギングが取り除かれます。

ネイティブ VLAN でのタギングを維持し、タグなしトラフィックをドロップするには、**vlan dot1q tag native** コマンドを入力します。スイッチによって、ネイティブ VLAN で受信したトラフィックがタグ付けされ、802.1Q タグが付けられたフレームのみが許可され、ネイティブ VLAN のタグなしトラフィックを含むすべてのタグなしトラフィックはドロップされます。

ネイティブ VLAN でのタギングを維持し、タグ付きトラフィックとタグなしトラフィックの両方を許可するには、**vlan dot1q tag native** コマンドを使用します。

vlan dot1q tag native コマンドがイネーブルになっていても、トランク ポートのネイティブ VLAN のタグなし制御トラフィックは引き続き許可されます。

（注） **vlan dot1q tag native** コマンドはグローバル ベースでイネーブルになります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vlan dot1q tag native**
3. （任意） switch(config)# **no vlan dot1q tag native**
4. （任意） switch# **show vlan dot1q tag native**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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	switch(config)# **vlan dot1q tag native**	Cisco Nexus デバイス 上のすべてのトランク ポートのすべてのネイティブ VLAN の dot1q（IEEE 802.1Q）タギングをイネーブルにします。デフォルトでは、この機能は無効になっています。
ステップ 3	（任意） switch(config)# **no vlan dot1q tag native**	スイッチ上の全トランキング ポートを対象に、そのネイティブ VLAN すべてに対して dot1q（IEEE 802.1Q）タギングをイネーブルにします。
ステップ 4	（任意） switch# **show vlan dot1q tag native**	ネイティブ VLAN のタギングのステータスを表示します。

例

次に、スイッチ上の 802.1Q タギングをイネーブルにする例を示します。

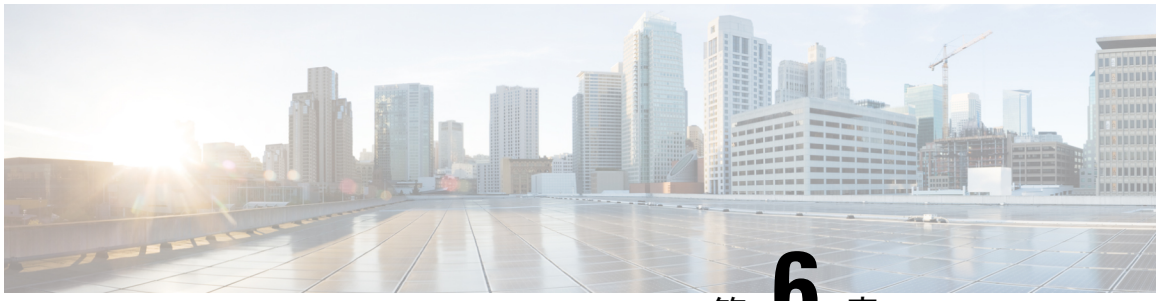
```
switch# configure terminal
switch(config)# vlan dot1q tag native
switch(config)# exit
switch# show vlan dot1q tag native
vlan dot1q native tag is enabled
```

インターフェイスの設定の確認

アクセスおよびトランク インターフェイス設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
switch# **show interface**	インターフェイス設定を表示します。

コマンド	目的
switch# **show interface switchport**	すべてのイーサネット インターフェイス（アクセス インターフェイスとトランク インターフェイスを含む）の情報を表示します。
switch# **show interface brief**	インターフェイス設定情報を表示します。



第 6 章

Rapid PVST+ の設定

Rapid PVST+ について

Rapid PVST+ プロトコルは、VLAN 単位で実装される IEEE 802.1w 標準（高速スパニングツリープロトコル（RSTP））です。Rapid PVST+ は、個別の VLAN でなく、すべての VLAN に対応する単一の STP インスタンスが規定された IEEE 802.1D 標準と相互運用されます。

Rapid PVST+ は、デフォルト VLAN（VLAN1）と、ソフトウェアで新たに作成された新しい VLAN でデフォルトでイネーブルになります。Rapid PVST+ はレガシー IEEE 802.1D STP が稼働するデバイスと相互運用されます。

RSTP は、元の STP 規格 802.1D の拡張版で、より高速な収束が可能です。

Note このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。IEEE 802.1D STP について説明している箇所では、802.1D と明記します。

STP についての概要

STP の概要

イーサネット ネットワークが適切に動作するには、任意の 2 つのステーション間のアクティブパスは 1 つだけでなければなりません。

フォールトトレラントなインターネットワークを作成する場合、ネットワーク上のすべてのノード間にループフリーパスを構築する必要があります。STP アルゴリズムでは、スイッチドネットワーク中で、ループのない最適のパスが計算されます。LAN ポートでは、定期的な間隔で、ブリッジ プロトコル データ ユニット（BPDU）と呼ばれる STP フレームの送受信が実

行されます。スイッチはこのフレームを転送しませんが、このフレームを使って、ループの発生しないパスを実現します。

エンド ステーション間に複数のアクティブ パスがあると、ネットワーク内でループが発生する原因になります。ネットワークにループがあると、エンドステーションがメッセージを重複して受信したり、複数の LAN ポートでエンド ステーションの MAC アドレスをスイッチが認識してしまうことがあります。このような状態になるとブロードキャスト ストームが発生し、ネットワークが不安定になります。

STP では、ルートブリッジでツリーを定義し、ルートからネットワーク内のすべてのスイッチへ、ループのないパスを定義します。STP は冗長データパスを強制的にブロック状態にします。スパニングツリーのネットワーク セグメントに障害が発生した場合、冗長パスがあると、STP アルゴリズムにより、スパニングツリー トポロジが再計算され、ブロックされたパスがアクティブになります。

スイッチの 2 つの LAN ポートで同じ MAC アドレスを認識することでループが発生している場合は、STP ポートのプライオリティとポート パス コストの設定により、フォワーディング ステートになるポートと、ブロッキング ステートになるポートが決定されます。

トポロジ形成の概要

スパニングツリーを構成している、拡張 LAN のスイッチはすべて、BPDU を交換することによって、ネットワーク内の他のスイッチについての情報を収集します。この BPDU の交換により、次のアクションが発生します。

- そのスパニングツリー ネットワーク トポロジでルート スイッチが 1 台選択されます。
- LAN セグメントごとに指定スイッチが 1 台選定されます。
- 冗長なインターフェイスをバックアップ ステートにする（スイッチド ネットワークの任意の箇所からルート スイッチに到達するために必要としないパスをすべて STP ブロック ステートにする）ことにより、スイッチド ネットワークのループをすべて解除します。

アクティブなスイッチド ネットワーク上のトポロジは、次の情報によって決定されます。

- 各スイッチにアソシエートされている、スイッチの一意なスイッチ識別情報である MAC アドレス
- 各インターフェイスにアソシエートされているルートのパス コスト
- 各インターフェイスにアソシエートされているポートの識別情報

スイッチド ネットワークでは、ルート スイッチが論理的にスパニングツリー トポロジの中心になります。STP では、BPDU を使用して、スイッチド ネットワークのルート スイッチやルート ポート、および、各スイッチド セグメントのルート ポートや指定ポートが選定されます。

ブリッジ ID の概要

それぞれのスイッチの各 VLAN には固有の 64 ビット ブリッジ ID があります。この ID は、ブリッジ プライオリティ値、拡張システム ID（IEEE 802.1t）、STP MAC アドレス割り当てから構成されます。

ブリッジ プライオリティ値

拡張システム ID がイネーブルの場合、ブリッジ プライオリティは 4 ビット値です。

Note Cisco NX-OS では、拡張システム ID は常にイネーブルです。拡張システム ID はディセーブルにできません。

拡張システム ID を伴わない

12 ビットの拡張システム ID フィールドは、ブリッジ IDの一部です。

Figure 4: 拡張システム *ID* 付きのブリッジ *ID*

スイッチは 12 ビットの拡張システム ID を常に使用します。

システム ID の拡張は、ブリッジ ID と組み合わされ、VLAN の一意の識別情報として機能します。

Table 4: 拡張システム *ID* をイネーブルにしたブリッジ プライオリティ値および拡張システム *ID*

ブリッジ プライオリティ値				拡張システム ID（VLAN ID と同設定）											
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4,096	2,048	1024	512	256	128	64	32	16	8	4	2	1

STP MAC アドレス割り当て

Note 拡張システム ID と MAC アドレス削減は、ソフトウェア上で常にイネーブルです。

任意のスイッチの MAC アドレス削減がイネーブルの場合、不要なルート ブリッジの選定とスパニングツリー トポロジの問題を避けるため、他のすべての接続スイッチでも、MAC アドレス削減をイネーブルにする必要があります。

MAC アドレス リダクションをイネーブルにすると、ルート ブリッジ プライオリティは、4096 + VLAN ID の倍数となります。スイッチのブリッジ ID（最小の優先ルート ブリッジを特定するために、スパニングツリー アルゴリズムによって使用される）は、4096 の倍数を指定します。指定できるのは次の値だけです。

- 0
- 4096
- 8192
- 12288
- 16384
- 20480
- 24576
- 28672
- 32768
- 36864
- 40960
- 45056
- 49152
- 53248
- 57344
- 61440

STP は、拡張システム ID および MAC アドレスを使用して、VLAN ごとにブリッジ ID を一意にします。

Note 同じスパニングツリードメインにある別のブリッジで MAC アドレス削減機能が実行されていない場合、そのブリッジのブリッジ ID と、MAC アドレス削減機能で指定されている値のいずれかが一致する可能性があり、その場合はそのブリッジがルートブリッジとして機能することになります。

BPDU の概要

スイッチは STP インスタンス全体にブリッジ プロトコル データ ユニット（BPDU）を送信します。各スイッチにより、コンフィギュレーション BPDU が送信され、スパニングツリー トポロジの通信が行われ、計算されます。各コンフィギュレーション BPDU に含まれる最小限の情報は、次のとおりです。

- 送信するスイッチによりルート ブリッジが特定される、スイッチの一意なブリッジ ID
- ルートまでの STP パス コスト
- 送信側ブリッジのブリッジ ID
- メッセージ エージ

- 送信側ポートの ID
- Hello タイマー、転送遅延タイマー、最大エージング タイム プロトコル タイマー
- STP 拡張プロトコルの追加情報

スイッチにより Rapid PVST+ BPDU フレームが送信されるときには、フレームの送信先の VLAN に接続されているすべてのスイッチで、BPDU を受信します。スイッチで BPDU を受信するときに、スイッチによりフレームは送信されませんが、フレームにある情報を使用して BPDU が計算されます。トポロジが変更される場合は、BPDU の送信が開始されます。

BPDU 交換によって次の処理が行われます。

- 1 つのスイッチがルート ブリッジとして選択されます。
- ルート ブリッジへの最短距離は、パス コストに基づいてスイッチごとに計算されます。
- LAN セグメントごとに指定ブリッジが選択されます。これは、ルート ブリッジに最も近いスイッチで、そのスイッチを介してフレームがルートに転送されます。
- ルート ポートが選択されます。これはブリッジからルート ブリッジまでの最適パスを提供するポートです。
- スパニングツリーに含まれるポートが選択されます。

ルート ブリッジの選定

各 VLAN では、ブリッジ ID の数値が最も小さいスイッチが、ルート ブリッジとして選択されます。すべてのスイッチがデフォルトのプライオリティ（32768）で設定されている場合、その VLAN で最小の MAC アドレスを持つスイッチが、ルート ブリッジになります。ブリッジ プライオリティ値はブリッジ ID の最上位ビットを占めます。

ブリッジのプライオリティの値を変更すると、スイッチがルートブリッジとして選定される可能性を変更することになります。小さい値を設定するほどその可能性が大きくなり、大きい値を設定するほどその可能性は小さくなります。

STP ルート ブリッジは論理的に、ネットワークで各スパニングツリー トポロジの中心です。ネットワークの任意の箇所からルート ブリッジに到達するために必要ではないすべてのパスは、STP ブロッキング モードになります。

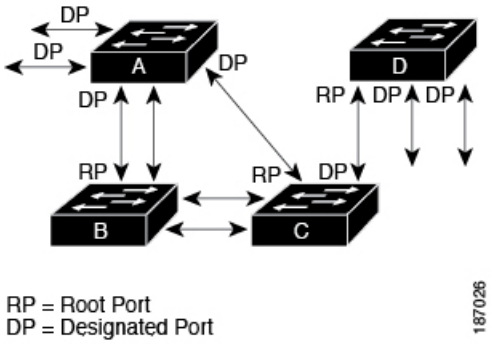
BPDU には、送信側ブリッジおよびそのポートについて、ブリッジおよび MAC アドレス、ブリッジ プライオリティ、ポート プライオリティ、パス コストなどの情報が含まれます。STP では、この情報を使用して、STP インスタンス用のルート ブリッジを選定し、ルート ブリッジに導くルート ポートを選択し、各セグメントの指定ポートを特定します。

スパニングツリー トポロジの作成

次の図では、スイッチ A がルート ブリッジに選定されます。これは、すべてのスイッチでブリッジ プライオリティがデフォルト（32768）に設定されており、スイッチ A の MAC アドレスが最小であるためです。しかし、トラフィック パターン、フォワーディング ポートの数、リンク タイプによっては、スイッチ A が最適なルート ブリッジでないことがあります。任意

のスイッチのプライオリティを高くする（数値を小さくする）ことでそのスイッチがルートブリッジになるようにします。これによりSTPが強制的に再計算され、そのスイッチをルートとする新しいスパニングツリー トポロジが形成されます。

Figure 5: スパニングツリー トポロジ



スパニングツリートポロジがデフォルトのパラメータに基づいて算出された場合、スイッチドネットワークの送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない場合があります。たとえば、現在のルートポートよりも数値の大きいポートに高速リンクを接続すると、ルートポートが変更される場合があります。最高速のリンクをルートポートにすることが重要です。

たとえば、スイッチ B の 1 つのポートが光ファイバ リンクであり、同じスイッチの別のポート（シールドなしツイストペア（UTP）リンク）がルートポートになっていると仮定します。ネットワーク トラフィックを高速の光ファイバ リンクに流した方が効率的です。光ファイバ ポートの STP ポート プライオリティをルート ポートよりも高いプライオリティに変更すると（数値を下げる）、光ファイバ ポートが新しいルート ポートになります。

Rapid PVST+ の概要

Rapid PVST+ の概要

Rapid PVST+ は、VLAN ごとに実装されている IEEE 802.1w（RSTP）規格です。（手作業で STP をディセーブルにしていない場合、）STP の 1 つのインスタンスは、設定されている各 VLAN で実行されます。VLAN 上の各 Rapid PVST+ インスタンスには、1 つのルート スイッチがあります。Rapid PVST+ の実行中には、VLAN ベースで STP をイネーブルまたはディセーブルにできます。

Note Rapid PVST+ は、スイッチでのデフォルト STP モードです。

Rapid PVST+ では、ポイントツーポイントの配線を使用して、スパニングツリーの高速収束が行われます。Rapid PVST+ によりスパニングツリーの再設定を 1 秒未満に発生させることができます（802.1D STP のデフォルト設定では 50 秒）。

Note Rapid PVST+ では、VLAN ごとに 1 つの STP インスタンスがサポートされます。

Rapid PVST+ を使用すると、STP コンバージェンスが急速に発生します。STP にある各指定ポートまたは各ルート ポートにより、デフォルトで、2 秒ごとに BPDU が送信されます。トポロジの指定ポートまたはルート ポートで、hello メッセージが 3 回連続失われた場合、または、最大経過時間の期限が切れた場合、ポートでは、すべてのプロトコル情報がテーブルにただちにフラッシュされます。ポートでは、3 つの BPDU が失われるか、最大経過時間の期限が切れた場合、直接のネイバー ルートまたは指定ポートへの接続が失われたと見なされます。プロトコル情報の急速な経過により、障害検出を迅速に行うことができます。スイッチは PVID を自動的に確認します。

Rapid PVST+ により、ネットワーク デバイス、スイッチ ポート、または LAN の障害の直後に、接続が迅速に回復されます。エッジ ポート、新しいルート ポート、ポイントツーポイント リンクで接続したポートに、高速コンバージェンスが次のように提供されます。

- エッジポート：RSTP スイッチにあるエッジ ポートとしてポートを設定する場合、エッジ ポートでは、フォワーディング ステートにただちに移行します（この急速な移行は、PortFast と呼ばれていたシスコ特有の機能でした）。エッジ ポートとして 1 つのエンド ステーションに接続されているポートにのみ、設定する必要があります。エッジ ポートでは、リンクの変更時にはトポロジの変更は生成されません。

  STP エッジ ポートとしてポートを設定するには、**spanning-tree port type** 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。

  Note ホストに接続されているすべてのポートを、エッジ ポートとして設定することを推奨します。

- ルート ポート：Rapid PVST+ により新しいルート ポートが選択された場合、古いポートがブロックされ、新しいルート ポートがただちにフォワーディング ステートに移行します。

- ポイントツーポイント リンク：ポイントツーポイント リンクによってあるポートと別のポートを接続することでローカル ポートが指定ポートになると、提案合意ハンドシェイクを使用して他のポートと急速な移行がネゴシエートされ、トポロジにループがなくなります。

Rapid PVST+ では、エッジ ポートとポイントツーポイント リンクでのみ、フォワーディング ステートへの急速な移行が達成されます。リンク タイプは設定が可能ですが、システムでは、ポートのデュプレックス設定からリンク タイプ情報が自動的に引き継がれます。全二重ポートはポイントツーポイント ポートであると見なされ、半二重ポートは共有ポートであると見なされます。

エッジ ポートでは、トポロジの変更は生成されませんが、直接接続されているネイバーから 3 回連続 BPDU の受信に失敗するか、最大経過時間のタイム アウトが発生すると、他のすべて

の指定ポートとルート ポートにより、トポロジ変更（TC）BPDU が生成されます。この時点で、指定ポートまたはルート ポートにより、TC フラグがオンに設定された状態で BPDU が送信されます。BPDU では、ポート上で TC While タイマーが実行されている限り、TC フラグが設定され続けます。TC While タイマーの値は、hello タイムに 1 秒を加えて設定された値です。トポロジ変更の初期ディテクタにより、トポロジ全体で、この情報がフラッディングされます。

Rapid PVST+ により、トポロジの変更が検出される場合、プロトコルでは次の処理が発生します。

- すべての非エッジ ルート ポートと指定ポートで、必要に応じ、hello タイムの 2 倍の値で TC While タイマーが開始されます。
- これらのすべてのポートにアソシエートされている MAC アドレスがフラッシュされます。

トポロジ変更通知は、トポロジ全体で迅速にフラッディングされます。システムでトポロジの変更が受信されると、システムにより、ポート ベースでダイナミック エントリがただちにフラッシュされます。

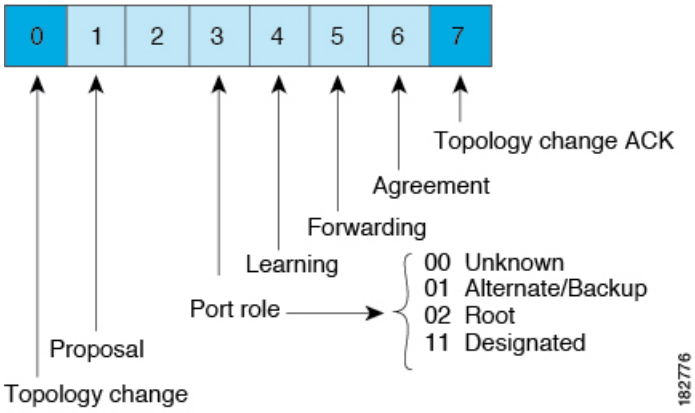
Note スイッチが、レガシー 802.1D STP を実行しているスイッチと相互に動作しているときにのみ、TCA フラグが使用されます。

トポロジの変更後、提案と合意のシーケンスがネットワークのエッジ方向に迅速に伝播され、接続がただちに回復します。

Rapid PVST+ BPDU

Rapid PVST+ と 802.1w では、フラグ バイトの 6 ビットすべてを使用して、BPDU の送信元のポートのロールおよびステートと、提案や合意のハンドシェイクが追加されます。次の図に、Rapid PVST+ の BPDU フラグの使用法を示します。

Figure 6: BPDU の Rapid PVST+ フラグ バイト

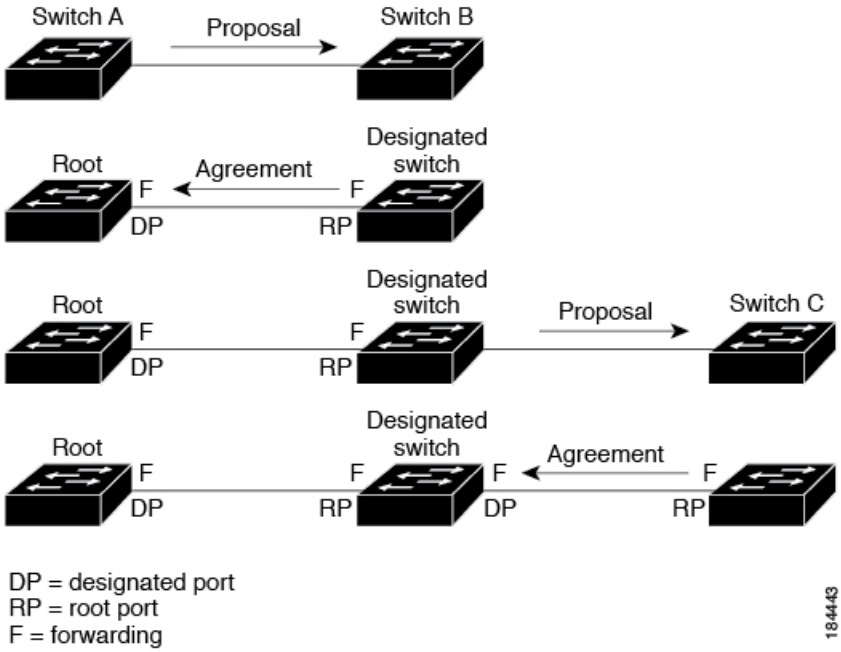


もう一つの重要な変更点は、Rapid PVST+ BPDU がタイプ 2、バージョン 2 であることで、これにより、スイッチでは、接続されているレガシー（802.1D）ブリッジを検出できるようになります。802.1D の BPDU は、バージョン 0 です。

提案と合意のハンドシェイク

次の図のように、スイッチ A は、ポイントツーポイント リンクを介してスイッチ B に接続され、すべてのポートがブロッキング ステートになります。スイッチ A のプライオリティ値がスイッチ B のプライオリティ値より小さい数値である場合、

Figure 7: 高速コンバージェンスの提案と合意のハンドシェイク



スイッチ A はスイッチ B に提案メッセージ（提案フラグが設定されたコンフィギュレーション BPDU）を送信し、スイッチ A 自身が指定スイッチになることを提案します。

スイッチ B は、提案メッセージを受信すると、提案メッセージを受信したポートを新しいルートポートとして選択し、すべての非エッジポートをブロッキング ステートにします。さらに、新しいルート ポート経由で合意メッセージ（合意フラグが設定された BPDU）を送信します。

スイッチ B から合意 メッセージの受信後、スイッチ A でも、その指定ポートがただちにフォワーディング ステートに移行されます。スイッチ B ですべての非エッジ ポートがブロックされ、スイッチ A とスイッチ B の間にポイントツーポイント リンクがあるため、ネットワークではループが形成されることはあり得ません。

スイッチ C がスイッチ B に接続されると、類似したハンドシェイク メッセージのセットがやり取りされます。スイッチ C は、そのルート ポートとしてスイッチ B に接続されたポートを選択し、リンクの両端がただちにフォワーディング ステートになります。このハンドシェイク処理の繰り返しごとに、さらに 1 つのネットワーク デバイスがアクティブなトポロジに参加し

ます。ネットワークの収束のたびに、この提案と合意のハンドシェイクが、ルートからスパニングツリーの末端に向かって進みます。

スイッチは、ポート デュプレックス モードからリンク タイプを認識します。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。**spanning-tree link-type** 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、デュプレックス設定によって制御されるデフォルト設定を無効にすることができます。

この提案合意ハンドシェイクが開始されるのは、非エッジ ポートがブロッキング ステートからフォワーディング ステートに移行するときだけです。次に、ハンドシェイク処理は、トポロジ全体に段階的に広がります。

プロトコル タイマー

次の表に、Rapid PVST+ のパフォーマンスに影響するプロトコル タイマーを示します。

***Table 5: Rapid PVST+* プロトコル タイマー**

変数	説明
ハロー タイマー	各スイッチから他のスイッチにBPDUをブロードキャストする頻度を決定します。デフォルトは 2 秒で、範囲は 1 ～ 10 です。
転送遅延タイマー	ポートが転送を開始するまでの、リスニング ステートおよびラーニング ステートが継続する時間を決定します。このタイマーは通常、プロトコルによっては使用されませんが、バックアップとして使用されます。デフォルトは 15 秒で、範囲は 4 ～ 30 秒です。
最大エージング タイマー	ポートで受信したプロトコル情報がスイッチで保存される時間を決めます。このタイマーは通常、プロトコルによっては使用されませんが、802.1D スパニングツリーと相互に動作するときに使用されます。デフォルトは 20 秒で、範囲は 6 ～ 40 秒です

ポート ロール

Rapid PVST+ では、ポート ロールを割り当て、アクティビティ トポロジを認識することによって、高速収束が行われます。Rapid PVST+ は、802.1D STP を利用して、最も高いプライオリティ（最小プライオリティ値）を持つスイッチをルート ブリッジとして選択します。Rapid PVST+ により、次のポートのロールの 1 つが個々のポートに割り当てられます。

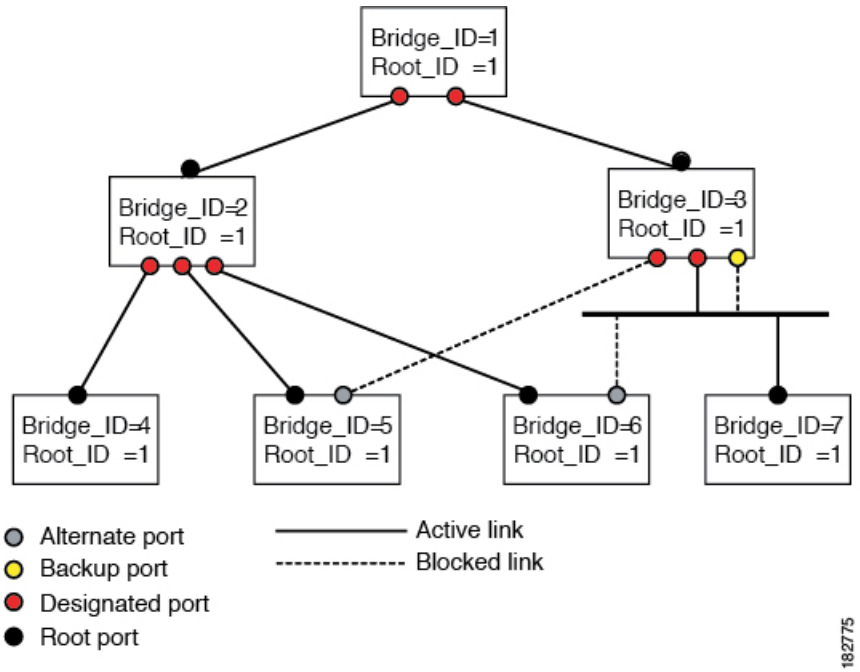
- ルート ポート：スイッチによりパケットがルート ブリッジに転送されるときに、最適のパス（最小コスト）を用意します。
- 指定ポート：指定スイッチに接続します。指定スイッチでは、LAN からルート ブリッジにパケットが転送されるときに、発生するパス コストが最小になります。指定スイッチが LAN に接続するポートのことを指定ポートと呼びます。

- 代替ポート：現在のルート ポートによって用意されているパスに、ルート ブリッジへの代替パスを用意します。代替ポートにより、トポロジにある別のスイッチへのパスが確保されます。
- バックアップ ポート：指定ポートが提供した、スパニング ツリーのリーフに向かうパスのバックアップとして機能します。バックアップ ポートが存在できるのは、2 つのポートがポイントツーポイント リンクよってループバックで接続されている場合、または 1 つのスイッチに共有 LAN セグメントへの接続が 2 つ以上ある場合です。バックアップ ポートにより、スイッチに対する別のパスがトポロジ内で確保されます。
- ディセーブル ポート：スパニング ツリーの動作において何もロールが与えられていません。

ネットワーク全体でポートのロールに一貫性のある安定したトポロジでは、Rapid PVST+ により、ルート ポートと指定ポートがすべてただちにフォワーディング ステートになり、代替ポートとバックアップ ポートはすべて、必ずブロッキング ステートになります。指定ポートはブロッキング ステートで開始されます。ポートのステートにより、転送処理および学習処理の動作が制御されます。

ルート ポートまたは指定ポートのロールを持つポートは、アクティブなトポロジに含まれます。代替ポートまたはバックアップ ポートのロールを持つポートは、アクティブなトポロジから除外されます（次の図を参照）。

Figure 8: ポートのロールをデモンストレーションするトポロジのサンプル



ポート ステート

Rapid PVST+ ポート ステートの概要

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジーの変化が発生します。スパニングツリートポロジで LAN ポートが非伝搬ステートからフォワーディング ステートに直接移行する際、一時的にデータがループすることがあります。ポートは新しいトポロジー情報がスイッチド LAN 経由で伝播されるまで待機し、それからフレーム転送を開始する必要があります。

Rapid PVST+ または MST を使用しているソフトウェア上の各 LAN ポートは、次の 4 つのステートの 1 つで終了します。

- ブロッキング：LAN ポートはフレーム転送に参加しません。
- ラーニング：LAN ポートは、フレーム転送への参加を準備します。
- フォワーディング：LAN ポートはフレームを転送します。
- ディセーブル：LAN ポートは STP に参加せず、フレームを転送しません。

Rapid PVST+ をイネーブルにすると、ソフトウェアのすべてのポート、VLAN、ネットワークは、電源投入時にブロッキング ステートからラーニングの移行ステートに進みます。各 LAN ポートは、適切に設定されていれば、フォワーディング ステートまたはブロッキング ステートで安定します。

STP アルゴリズムにより LAN ポートがフォワーディング ステートになると、次の処理が発生します。

- ラーニング ステートに進む必要があることを示すプロトコル情報を待つ間、LAN ポートはブロッキング ステートになります。
- LAN ポートは転送遅延タイマーの期限が切れるのを待ち、ラーニング ステートに移行し、転送遅延タイマーを再開します。
- ラーニング ステートでは、LAN ポートはフォワーディング データベースのエンド ステーション位置情報をラーニングする間、フレームの転送をブロックし続けます。
- LAN ポートは転送遅延タイマーの期限が切れるのを待って、フォワーディング ステートに移行します。このフォワーディング ステートでは、ラーニングとフレーム転送がイネーブルになります。

ブロッキング ステート

ブロッキング ステートにある LAN ポートはフレームを転送しません。

ブロッキング ステートの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。

- エンド ステーションの場所は、そのアドレス データベースには取り入れません（ブロッキング LAN ポートではラーニングがないため、アドレス データベースは更新されません）。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから送られた BPDU を受信し、処理して送信します。
- ネットワーク管理メッセージを受信して応答します。

ラーニング ステート

ラーニング ステートにある LAN ポートは、フレームの MAC アドレスをラーニングすることによって、フレーム転送の準備をします。LAN ポートは、ブロッキング ステートからラーニング ステートになります。

ラーニング ステートの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- エンド ステーションの場所を、そのアドレス データベースに取り入れます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから送られた BPDU を受信し、処理して送信します。
- ネットワーク管理メッセージを受信して応答します。

フォワーディング ステート

フォワーディング ステートにある LAN ポートでは、フレームを転送します。LAN ポートは、ラーニング ステートからフォワーディング ステートになります。

フォワーディング ステートの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを転送します。
- 転送用に他のポートからスイッチングされたフレームを転送します。
- エンド ステーションの場所情報を、そのアドレス データベースに取り入れます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を処理します。
- ネットワーク管理メッセージを受信して応答します。

ディセーブル ステート

ディセーブル ステートにある LAN ポートは、フレーム転送または STP は行いません。ディセーブル ステートの LAN ポートは、実質的に動作が停止しています。

ディセーブルの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- エンド ステーションの場所は、そのアドレス データベースには取り入れません（ラーニングは行われないため、アドレス データベースは更新されません）。
- ネイバーから BPDU を受信しません。
- システム モジュールから送信用の BPDU を受信しません。

ポート ステートの概要

次の表に、ポートおよびそれに対応してアクティブ トポロジに含められる、可能性のある動作と Rapid PVST+ のステートのリストを示します。

Table 6: アクティブなトポロジのポート ステート

動作ステータス（Operational Status）	ポート状態	ポートがアクティブ トポロジに含まれているか
有効	ブロッキング	いいえ
有効	ラーニング	はい
有効	転送	はい
無効	無効	不可

ポート ロールの同期

スイッチがいずれかのポートで提案メッセージを受信し、そのポートが新しいルート ポートとして選択されると、Rapid PVST+ は、強制的に、すべての他のポートと新しいルート情報との同期をとります。

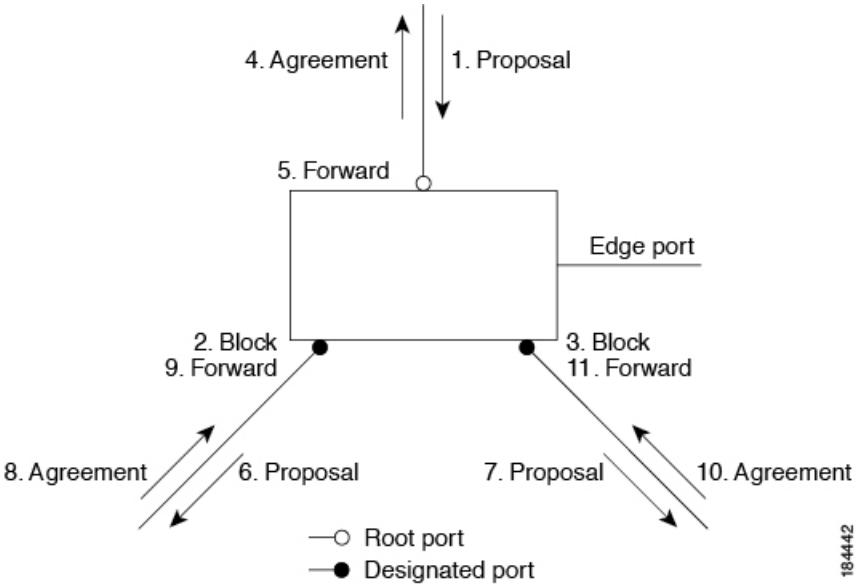
他のすべてのポートが同期化されると、スイッチはルート ポートで受信した優位のルート情報に同期化されます。次のいずれかが当てはまる場合、スイッチ上の個々のポートで同期がとられます。

- ポートがブロッキング ステートである。
- エッジ ポートである（ネットワークのエッジに存在するように設定されたポート）。

指定されたポートは、フォワーディング ステートになっていてエッジ ポートとして設定されていない場合、Rapid PVST+ によって強制的に新しいルート情報で同期化されると、ブロッキング ステートに移行します。一般的に、Rapid PVST+ により、強制的にルート情報との同期がとられる場合で、ポートで前述の条件のいずれかが満たされない場合、ポート ステートはブロッキングに設定されます。

すべてのポートで同期がとられた後で、スイッチから、ルートポートに対応する指定スイッチへ、合意メッセージが送信されます。ポイントツーポイントリンクで接続されているスイッチが、そのポートのロールについての合意に存在する場合、Rapid PVST+により、ポートステートがただちにフォワーディング ステートに移行します。この一連のイベントを次の図に示します。

Figure 9: 高速コンバージェンス中のイベントのシーケンス



優位 BPDU 情報の処理

上位 BPDU とは、自身のために現在保存されているものより上位であるルート情報（より小さいスイッチ ID、より小さいパス コストなど）を持つ BPDU のことです。

上位 BPDU がポートで受信されると、Rapid PVST+ は再設定を起動します。そのポートが新しいルートポートとして提案、選択されている場合、Rapid PVST+ は残りすべてのポートを同期させます。

受信した BPDU が提案フラグの設定された Rapid PVST+ BPDU の場合、スイッチは残りすべてのポートを同期させたあと、合意メッセージを送信します。前のポートがブロッキング ステートになるとすぐに、新しいルート ポートがフォワーディング ステートに移行します。

ポートで受信した上位情報によりポートがバックアップポートまたは代替ポートになる場合、Rapid PVST+ はポートをブロッキング ステートに設定し、合意メッセージを送信します。指定ポートは、転送遅延タイマーが期限切れになるまで、提案フラグが設定された BPDU を送信し続けます。期限切れになると、ポートはフォワーディング ステートに移行します。

下位 BPDU 情報の処理

下位 BPDU とは、自身のために現在保存されているものより下位であるルート情報（より大きいスイッチ ID、より大きいパス コストなど）を持つ BPDU のことです。

DP は、下位 BPDU を受信すると、独自の情報で直ちに応答します。

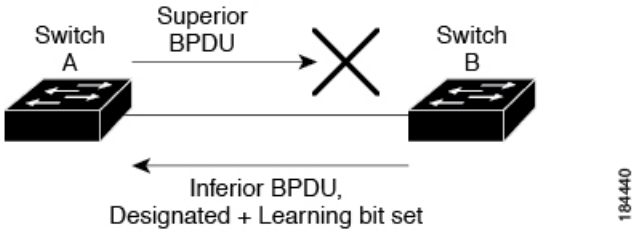
スパニングツリーの異議メカニズム

ソフトウェアは、受信したBPDUでポートのロールおよびステートの一貫性をチェックし、ブリッジング ループの原因となることがある単方向リンク障害を検出します。

指定ポートは、矛盾を検出すると、そのロールを維持しますが、廃棄ステートに戻ります。一貫性がない場合は、接続を中断した方がブリッジング ループを解決できるからです。

次の図に、ブリッジングループの一般的な原因となる単方向リンク障害を示します。スイッチ A はルート ブリッジであり、スイッチ B へのリンクで BPDU は失われます。802.1w 規格の BPDUには、送信側ポートのロールと状態が含まれます。この情報により、送信する上位BPDU に対してスイッチ B が反応しないこと、スイッチ B はルート ポートではなく指定ポートであることが、スイッチAによって検出できます。この結果、スイッチAは、そのポートをブロックし（またはブロックし続け）、ブリッジングループが防止されます。ブロックは、STPの矛盾として示されます。

Figure 10: 単一方向リンク障害の検出



ポートコスト

Note Rapid PVST+はデフォルトで、ショート（16ビット）パスコスト方式を使用してコストを計算します。ショートパスコスト方式では、1～65,535の範囲で任意の値を割り当てることができます。ただし、ロング型（32ビット）のパスコスト方式を使用するようにスイッチを設定することもできます。この場合、1～200,000,000の範囲の値を割り当てることができます。パスコスト計算方式はグローバルに設定します。

STP ポートのパスコストのデフォルト値は、メディア速度と LAN インターフェイスのパスコストの計算方式によって決まります。ループが発生した場合、STP では、LAN インターフェイスの選択時に、フォワーディング ステートにするためのポート コストを考慮します。

Table 7: デフォルト ポート コスト

帯域幅	ポートコストのショートパスコスト方式	ポート コストのロング パスコスト方式
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 ギガビット イーサネット	4	20,000

帯域幅	ポートコストのショートパスコスト方式	ポート コストのロング パスコスト方式
10 ギガビットイーサネット	2	2,000

STP に最初に選択させたい LAN インターフェイスには低いコスト値を、最後に選択させたい LAN インターフェイスには高いコスト値を割り当てることができます。すべての LAN インターフェイスが同じコスト値を使用している場合には、STP は LAN インターフェイス番号が最も小さい LAN インターフェイスをフォワーディング ステートにして、残りの LAN インターフェイスをブロックします。

アクセス ポートでは、ポート コストをポートごとに割り当てます。トランク ポートでは VLAN ごとにポート コストを割り当てるため、トランク ポート上のすべての VLAN に同じポート コストを設定できます。

ポートプライオリティ

ループが発生し、複数のポートに同じパス コストが割り当てられている場合、Rapid PVST+ では、フォワーディング ステートにする LAN ポートの選択時に、ポートのプライオリティを考慮します。Rapid PVST+ に最初に選択させる LAN ポートには小さいプライオリティ値を割り当て、Rapid PVST+ に最後に選択させる LAN ポートには大きいプライオリティ値を割り当てます。

すべての LAN ポートに同じプライオリティ値が割り当てられている場合、Rapid PVST+ は、LAN ポート番号が最小の LAN ポートをフォワーディング ステートにし、他の LAN ポートをブロックします。プライオリティの範囲は 0 ～ 224（デフォルトは 128）で、32 ずつ増加させて設定できます。LAN ポートがアクセス ポートとして設定されているときはポートのプライオリティ値が使用され、LAN ポートがトランク ポートとして設定されているときは VLAN ポートのプライオリティ値が使用されます。

Rapid PVST+ と IEEE 802.1Q トランク

Cisco スイッチを 802.1Q トランクで接続しているネットワークでは、スイッチは、トランクの VLAN ごとに STP のインスタンスを 1 つ維持します。ただし、非 Cisco 802.1Q スイッチでは、トランクのすべての VLAN に対して維持する STP のインスタンスは 1 つだけです。

802.1Q トランクで Cisco スイッチを非 Cisco スイッチに接続している場合は、Cisco スイッチにより、トランクの 802.1Q VLAN の STP インスタンスが、非 Cisco 802.1Q スイッチの STP インスタンスと組み合わされます。ただし、Cisco スイッチで維持されている VLAN ごとの STP 情報はすべて、非シスコ 802.1Q スイッチのクラウドによって分けられます。Cisco スイッチを分ける非 Cisco 802.1Q クラウドは、スイッチ間の単一のトランク リンクとして扱われます。

Rapid PVST+ のレガシー 802.1D STP との相互運用

Rapid PVST+ は、レガシー 802.1D プロトコルを実行中のスイッチと相互に動作させることができます。スイッチが BPDU バージョン 0 を受信すると、802.1D を実行中の機器と相互に動作していることを認識します。Rapid PVST+ の BPDU はバージョン 2 です。受信した BPDU

が、提案フラグがオンに設定された 802.1w BPDU バージョン 2 の場合、スイッチは残りすべてのポートを同期させたあと、合意メッセージを送信します。受信した BPDU が 802.1D BPDU バージョン 0 の場合は、スイッチは提案フラグを設定せずに、ポートの転送遅延タイマーを開始します。新しいルートポートでは、フォワーディング ステートに移行するために、2 倍の転送遅延時間が必要となります。

スイッチは、次のように、レガシー 802.1D スイッチと相互動作します。

- 通知：802.1D BPDU とは異なり 802.1w は、TCN BPDU を使用しません。ただし、802.1D スイッチとの相互運用のため、Cisco NX-OS では、TCN BPDU を処理し、生成します。
- 受信応答：802.1w スイッチでは、802.1D スイッチから指定ポート上に TCN メッセージを受信すると、TCA ビットを設定し、802.1D コンフィギュレーション BPDU で応答します。ただし、802.1D スイッチに接続されているルート ポートで TC While タイマー（802.1D の TC タイマーと同じ）がアクティブの場合、TCA がセットされたコンフィギュレーション BPDU を受信すると、TC While タイマーはリセットされます。

動作のこの方式は、802.1D スイッチでのみ必要です。802.1w BPDU では、TCA ビットは設定されません。

- プロトコル移行：802.1D スイッチとの下位互換性のために、802.1w は、802.1D コンフィギュレーション BPDU と TCN BPDU をポートごとに選択的に送信します。

ポートが初期化されると、移行遅延タイマー（802.1w BPDU が送信される最小時間を指定）が開始され、802.1w BPDU が送信されます。このタイマーがアクティブな間、スイッチはそのポートで受信したすべての BPDU を処理し、プロトコル タイプを無視します。

ポート移行遅延タイマーの期限切れ後にスイッチで 802.1D BPDU を受信した場合は、802.1D スイッチに接続していると見なして、802.1D BPDU のみを使用して開始します。ただし、802.1w スイッチが、ポート上で 802.1D BPDU を使用中で、タイマーの期限切れ後に 802.1w BPDU を受信すると、タイマーが再起動され、ポート上の 802.1w BPDU を使用して開始されます。

Note すべてのスイッチでプロトコルを再ネゴシエーションするには、Rapid PVST+ を再起動する必要があります。

Rapid PVST+ の 802.1s MST との相互運用

Rapid PVST+ は、IEEE 802.1s マルチ スパニングツリー（MST）規格とシームレスに相互運用されます。ユーザによる設定は不要です。

Rapid PVST+ の設定

Rapid PVST+ プロトコルには 802.1w 規格が適用されていますが、Rapid PVST+ は、ソフトウェアのデフォルト STP 設定です。

Rapid PVST+ は VLAN ごとにイネーブルにします。STP のインスタンスが VLAN ごとに維持されます（STP をディセーブルにした VLAN を除く）。デフォルトで Rapid PVST+ は、デフォルト VLAN と、作成した各 VLAN でイネーブルになります。

Rapid PVST+ に関する注意事項および制約事項

Rapid PVST+ 設定時の注意事 項と制限事項は次のとおりです。

- Rapid PVST+ モードでは 250 の VLAN のみがサポートされます。

Rapid PVST+ のイネーブル化

スイッチ上で Rapid PVST+ をイネーブルにすると、指定されている VLAN で Rapid PVST+ をイネーブルにする必要があります。

Rapid PVST+ はデフォルトの STP モードです。MST と Rapid PVST+ は同時には実行できません。

Note スパニングツリー モードを変更すると、変更前のモードのスパニングツリー インスタンスがすべて停止されて新しいモードで起動されるため、トラフィックが中断する場合があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mode rapid-pvst**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree mode rapid-pvst**	スイッチで Rapid PVST+ をイネーブルにします。Rapid PVST+ はデフォルトのスパニングツリー モードです。 **Note** スパニングツリー モードを変更すると、変更前のモードのスパニングツリー インスタンスがすべて停止されて新しいモードで起動されるため、トラフィックが中断する場合があります。

Example

次の例は、スイッチで Rapid PVST+ をイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mode rapid-pvst
```

Note STP はデフォルトでイネーブルのため、設定結果を参照するために **show running-config** コマンドを入力しても、Rapid PVST+ をイネーブルするために入力したコマンドは表示されません。

Rapid PVST+ の VLAN ベースのイネーブル化

Rapid PVST+ は、VLAN ごとにイネーブルまたはディセーブルにできます。

Note Rapid PVST+ は、デフォルト VLAN と、作成したすべての VLAN でデフォルトでイネーブルになります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree** *vlan-range*
3. (Optional) switch(config)# **no spanning-tree** *vlan-range*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree** *vlan-range*	VLAN ごとに Rapid PVST+（デフォルト STP）をイネーブルにします。 *vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。
ステップ 3	(Optional) switch(config)# **no spanning-tree** *vlan-range*	指定 VLAN で Rapid PVST+ をディセーブルにします。

	Command or Action	Purpose
		Caution VLANのすべてのスイッチおよびブリッジでスパニングツリーがディセーブルになっていない場合は、VLAN でスパニングツリーをディセーブルにしないでください。VLANの一部のスイッチおよびブリッジでスパニングツリーをディセーブルにして、その他のスイッチおよびブリッジでイネーブルにしておくことはできません。スパニングツリーをイネーブルにしたスイッチとブリッジに、ネットワークの物理トポロジに関する不完全な情報が含まれることになるので、この処理によって予想外の結果となることがあります。 VLANに物理ループが存在しないことを確認せずに、VLAN でスパニング ツリーをディセーブルにしないでください。スパニングツリーは、設定の誤りおよび配線の誤りに対する保護手段として動作します。

Example

次に、VLAN で STP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5
```

ルート ブリッジ ID の設定

Rapid PVST+ では、STP のインスタンスはアクティブな VLAN ごとに管理されます。VLAN ごとに、最小のブリッジ ID を持つスイッチが、その VLAN のルート ブリッジとして選定されます。

特定の VLAN インスタンスがルート ブリッジになるように設定するには、そのブリッジのプライオリティをデフォルト値（32768）よりかなり小さい値に変更します。

spanning-tree vlan *vlan_ID* **root** コマンドを入力すると、各 VLAN で現在ルートになっているブリッジのブリッジ プライオリティがスイッチによって確認されます。スイッチは指定した VLAN のブリッジ プライオリティを 24576 に設定します（このスイッチがその VLAN のルートになる値）。指定した VLAN のいずれかのルート ブリッジに 24576 より小さいブリッジ プライオリティが設定されている場合は、スイッチはそのVLANのブリッジプライオリティを、最小のブリッジ プライオリティより 4096 だけ小さい値に設定します。

Note ルート ブリッジになるために必要な値が 1 より小さい場合は、 **spanning-tree vlan** *vlan_ID* **root** このコマンドは機能しません。

Caution STP の各インスタンスのルート ブリッジは、バックボーン スイッチまたはディストリビューション スイッチでなければなりません。アクセス スイッチは、STP のプライマリ ルートとして設定しないでください。

キーワード **diameter** を入力し、ネットワーク直径（ネットワーク内の任意の 2 つのエンド ステーション間での最大ブリッジホップ数）を指定します。ネットワーク直径を指定すると、ソフトウェアはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に選びます。その結果、STP のコンバージェンスに要する時間が大幅に短縮されます。自動的に算出された hello タイムを無効にするには、 **hello-time** キーワードを入力します。

Note ルート ブリッジとして設定されているスイッチでは、hello タイム、転送遅延時間、最大エージング タイムを、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** の各コンフィギュレーション コマンドを使用して手動で設定しないでください。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree vlan** *vlan-range* **root primary** [**diameter** *dia* [**hello-time** *hello-time*]]

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree vlan** *vlan-range* **root primary** [**diameter** *dia* [**hello-time** *hello-time*]]	ソフトウェア スイッチをプライマリ ルート ブリッジとして設定します。 *vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。 *dia* のデフォルトは 7 です。 *hello-time* は 1 ～ 10 秒で、デフォルト値は 2 秒です。

Example

次の例は、VLAN のルート スイッチとしてスイッチを設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 root primary diameter 4
```

セカンダリ ルート ブリッジの設定

ソフトウェア スイッチをセカンダリ ルートとして設定しているときに、STP ブリッジのプライオリティをデフォルト値（32768）から変更しておくと、プライマリ ルート ブリッジに障害が発生した場合に、そのスイッチが、指定した VLAN のルート ブリッジになります（ネットワークの他のスイッチで、デフォルトのブリッジプライオリティ 32768 が使用されているとします）。STP により、ブリッジ プライオリティが 28672 に設定されます。

キーワード **diameter** を入力し、ネットワーク直径（ネットワーク内の任意の 2 つのエンド ステーション間での最大ブリッジホップ数）を指定します。ネットワーク直径を指定すると、ソフトウェアはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に選びます。その結果、STP のコンバージェンスに要する時間が大幅に短縮されます。自動的に算出された hello タイムを無効にするには、 **hello-time** キーワードを入力します。

複数のスイッチに対して同様に設定すれば、複数のバックアップ ルート ブリッジを設定できます。プライマリ ルート ブリッジの設定時に使用した値と同じネットワーク直径と hello タイムの値を入力します。

Note ルート ブリッジとして設定されているスイッチでは、hello タイム、転送遅延時間、最大エージング タイムを、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** の各グローバル コンフィギュレーション コマンドを使用して手動で設定しないでください。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree vlan** *vlan-range* **root secondary** [**diameter** *dia* [**hello-time** *hello-time*]]

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree vlan** *vlan-range* **root secondary** [**diameter** *dia* [**hello-time** *hello-time*]]	ソフトウェア スイッチをセカンダリ ルート ブリッジとして設定します。 *vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。 *dia* のデフォルトは 7 です。 *hello-time* は 1 ～ 10 秒で、デフォルト値は 2 秒です。

Example

次の例は、VLANのセカンダリ ルート スイッチとしてスイッチを設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 root secondary diameter 4
```

Rapid PVST+ のポート プライオリティの設定

Rapid PVST+ に最初に選択させる LAN ポートには小さいプライオリティ値を割り当て、Rapid PVST+ に最後に選択させる LAN ポートには大きいプライオリティ値を割り当てます。すべてのLANポートに同じプライオリティ値が割り当てられている場合、RapidPVST+は、LANポート番号が最小の LAN ポートをフォワーディング ステートにし、他の LAN ポートをブロックします。

LAN ポートがアクセス ポートとして設定されているときはポートのプライオリティ値が使用され、LAN ポートがトランク ポートとして設定されているときは VLAN ポートのプライオリティ値が使用されます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **spanning-tree** [**vlan** *vlan-list*] **port-priority** *priority*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** *type slot*/*port*	設定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	switch(config-if)# **spanning-tree** [**vlan** *vlan-list*] **port-priority** *priority*	LAN インターフェイスのポート プライオリティを設定します。 *priority* の値は 0 ～ 224 の範囲です。値が小さいほどプライオリティが高いことを示します。プライオリティ値は、0、32、64、96、128、160、192、224 です。その他の値はすべて拒否されます。デフォルト値は 128 です。

Example

次の例は、イーサネット インタフェースのアクセス ポートのプライオリティを設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree port-priority 160
```

このコマンドを使用できるのは、物理イーサネット インターフェイスに対してだけです。

Rapid PVST+ パスコスト方式およびポート コストの設定

アクセス ポートでは、ポートごとにポート コストを割り当てます。トランク ポートではVLANごとにポート コストを割り当てるため、トランク上のすべての VLAN に同じポート コストを設定できます。

Note Rapid PVST+ モードでは、ショート型またはロング型のいずれかのパス コスト方式を使用できます。この方式は、インターフェイスまたはコンフィギュレーション サブモードのいずれかで設定できます。デフォルトのパス コスト方式は、ショート型です。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree pathcost method** {**long** | **short**}
3. switch(config)# **interface** *type slot*/*port*
4. switch(config-if)# **spanning-tree** [**vlan** *vlan-id*] **cost** [*value* | **auto**]

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree pathcost method** {**long** | **short**}	Rapid PVST+ パスコスト計算に使用される方式を選択します。デフォルト方式は short 型です。
ステップ 3	switch(config)# **interface** *type slot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	switch(config-if)# **spanning-tree** [**vlan** *vlan-id*] **cost** [*value* | **auto**]	LAN インターフェイスのポート コストを設定します。ポート コスト値には、パスコスト計算方式に応じて、次の値を指定できます。 • ショート型：1 ～ 65535 • ロング型：1 ～ 200000000

	Command or Action	Purpose
		Note このパラメータは、アクセス ポートのインターフェイス別、およびトランク ポートの VLAN 別に設定します。 デフォルトの **auto** では、パスコスト計算方式およびメディア速度に基づいてポートコストが設定されます。

Example

この例は、イーサネット インターフェイスのアクセス ポート コストを設定する方法を示しています。

```
switch# configure terminal
switch (config)# spanning-tree pathcost method long
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree cost 1000
```

このコマンドを使用できるのは、物理イーサネットインターフェイスに対してだけです。

VLAN の Rapid PVST+ のブリッジ プライオリティの設定

VLAN の Rapid PVST+ のブリッジ プライオリティを設定できます。

Note この設定を使用するときは注意が必要です。ほとんどの場合、プライマリ ルートとセカンダリ ルートを設定して、ブリッジ プライオリティを変更することを推奨します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree vlan** *vlan-range* **priority** *value*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree vlan** *vlan-range* **priority** *value*	VLAN のブリッジ プライオリティを設定します。有効な値は 0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、

	Command or Action	Purpose
		49152、53248、57344、61440 です。その他の値はすべて拒否されます。デフォルト値は 32768 です。

Example

次の例は、VLAN のブリッジ プライオリティを設定する方法を示します。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 priority 8192
```

VLAN の Rapid PVST+ の hello タイムの設定

VLAN では、Rapid PVST+ の hello タイムを設定できます。

Note この設定を使用するときは注意が必要です。ほとんどの場合、プライマリ ルートとセカンダリ ルートを設定して、hello タイムを変更することを推奨します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree vlan** *vlan-range* **hello-time** *hello-time*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree vlan** *vlan-range* **hello-time** *hello-time*	VLAN の hello タイムを設定します。hello タイムの値には 1 ～ 10 秒を指定できます。デフォルト値は 2 秒です。

Example

次の例は、VLAN の hello タイムの値を設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 hello-time 7
```

VLAN の Rapid PVST+ の転送遅延時間の設定

Rapid PVST+ の使用時は、VLAN ごとに転送遅延時間を設定できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree vlan** *vlan-range* **forward-time** *forward-time*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree vlan** *vlan-range* **forward-time** *forward-time*	VLAN の転送遅延時間を設定します。転送遅延時間の値の範囲は 4 ～ 30 秒で、デフォルトは 15 秒です。

Example

次の例は、VLAN の転送遅延時間を設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 forward-time 21
```

VLAN の Rapid PVST+ の最大経過時間の設定

Rapid PVST+ の使用時は、VLAN ごとに最大経過時間を設定できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree vlan** *vlan-range* **max-age** *max-age*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **spanning-tree vlan** *vlan-range* **max-age** *max-age*	VLAN の最大エージング タイムを設定します。最大経過時間の値の範囲は 6 ～ 40 秒で、デフォルトは 20 秒です。

Example

次の例は、VLAN の最大経過時間を設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 max-age 36
```

リンク タイプの設定

Rapid の接続性（802.1w 規格）は、ポイントツーポイントのリンク上でのみ確立されます。リンク タイプは、デフォルトでは、インターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。

リモート スイッチの 1 つのポートに、ポイントツーポイントで物理的に接続されている半二重リンクがある場合、リンク タイプのデフォルト設定を上書きし、高速移行をイネーブルにできます。

リンクを共有に設定すると、STP は 802.1D に戻ります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **spanning-tree link-type** {**auto** | **point-to-point** | **shared**}

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** *type slot*/*port*	設定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	switch(config-if)# **spanning-tree link-type** {**auto** | **point-to-point** | **shared**}	リンク タイプを、ポイントツーポイント インクまたは共有リンクに設定します。デフォルト値はスイッチ接続から読み取られ、半二重リンクは共有、全二重リンクはポイントツーポイントです。リンク タイプが共有の場合、STP は 802.1D に戻ります。デフォルトは auto で、インターフェイスのデュプレックス設定に基づいてリンク タイプが設定されます。

Example

次の例は、リンクタイプをポイントツーポイントリンクとして設定する方法を示しています。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree link-type point-to-point
```

このコマンドを使用できるのは、物理イーサネットインターフェイスに対してだけです。

プロトコルの再開

レガシーブリッジに接続されている場合、Rapid PVST+ を実行しているブリッジは、そのポートの 1 つに 802.1D BPDU を送信できます。ただし、STP プロトコルの移行では、レガシー スイッチが指定スイッチではない場合、レガシー スイッチがリンクから削除されたかどうかを認識できません。スイッチ全体または指定したインターフェイスでプロトコル ネゴシエーションを再開する（強制的に隣接スイッチと再ネゴシエーションさせる）ことができます。

コマンド	目的
switch# **clear spanning-tree detected-protocol** [**interface** *interface* [*interface-num* | *port-channel*]]	スイッチのすべてのインターフェイスまたは指定インターフェイスで Rapid PVST+ を再起動します。

次の例は、イーサネットインターフェイスで Rapid PVST+ を再起動する方法を示しています。

```
switch# clear spanning-tree detected-protocol interface ethernet 1/8
```

Rapid PVST+ 設定の確認

Rapid PVST+ の設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
show running-config spanning-tree [**all**]	現在のスパニングツリー設定を表示します。
show spanning-tree [*options*]	最新のスパニングツリー設定について、指定した詳細情報を表示します。

次の例は、スパニングツリーのステータスの表示方法を示しています。

```
switch# show spanning-tree brief

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32768
             Address     001c.b05a.5447
```

```
            Cost        2
            Port        131 (Ethernet1/3)
            Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
            Address     000d.ec6d.7841
            Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Eth1/3           Root FWD 2         128.131  P2p Peer(STP)
```

VLAN STP ステート整合性チェッカーのトリガー

VLAN STP ステート整合性チェッカーを手動でトリガーして、VLAN のスパニング ツリー ステートのハードウェア設定とソフトウェア設定を比較し、結果を表示することができます。VLAN STP ステート整合性チェッカーを手動でトリガーして結果を表示するには、次のコマンドを特定のモードで使用します。

手順の概要

1. **show consistency-checker stp-state vlan** *vlan-id*

手順の詳細

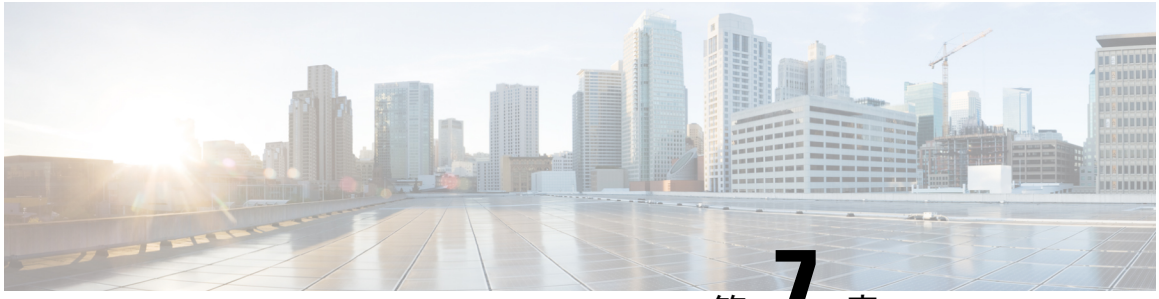
	コマンドまたはアクション	目的
ステップ 1	**show consistency-checker stp-state vlan** *vlan-id*	指定された VLAN に対する VLAN STP ステート整合性検査を開始して結果を表示します。

例

次に、VLAN STP ステート整合性検査をトリガーして結果を表示する例を示します。

```
switch# show consistency-checker stp-state vlan 250
Checks: Spanning tree state
Consistency Check: PASSED
 Vlan:250, Hardware state consistent for:
   Ethernet1/4
   Ethernet1/5
   Ethernet1/6
   Ethernet1/18
   Ethernet1/20
   Ethernet1/29
   Ethernet1/30
   Ethernet1/31
   Ethernet1/32
   Ethernet1/33
   Ethernet1/34
   Ethernet1/35
   Ethernet1/36
   Ethernet1/37
   Ethernet1/38
   Ethernet1/39
   Ethernet1/40
   Ethernet1/41
   Ethernet1/42
```

```
Ethernet1/43
Ethernet1/44
Ethernet1/45
Ethernet1/46
Ethernet1/47
Ethernet1/48
```



第 7 章

マルチ スパニングツリーの設定

MST について

MST の概要

Note このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。IEEE 802.1D STP について説明している箇所では、802.1D と明記します。

MST は、複数の VLAN を 1 つのスパニング ツリー インスタンスにマップします。各インスタンスのスパニング ツリー トポロジは、他のスパニング ツリー インスタンスの影響を受けません。このアーキテクチャでは、データ トラフィックに対して複数のフォワーディング パスがあり、ロード バランシングが可能です。これによって、非常に多数の VLAN をサポートする際に必要な STP インスタンスの数を削減できます。

MST では、各 MST インスタンスで IEEE 802.1w 規格を採用することによって、明示的なハンドシェイクによる高速収束が可能なため、802.1D 転送遅延がなくなり、ルート ブリッジ ポートと指定ポートが迅速にフォワーディング ステートに変わります

MST の使用中は、MAC アドレスの削減が常にイネーブルに設定されますこの機能はディセーブルにはできません。

MST ではスパニング ツリーの動作が改善され、次の STP バージョンとの下位互換性を維持しています。

- 元の 802.1D スパニング ツリー
- Rapid per-VLAN スパニングツリー（Rapid PVST+）

  IEEE 802.1 は、Rapid Spanning Tree Protocol（RSTP）で定義されて、IEEE 802.1D に組み込まれました。
- IEEE 802.1s では MST が定義されて、IEEE 802.1Q に組み込まれました。

Note MST をイネーブルにする必要があります。Rapid PVST+ は、デフォルトのスパニングツリーモードです。

MST 領域

スイッチが MSTI に参加できるようにするには、同一の MST 設定情報でスイッチの設定に整合性を持たせる必要があります。

同じ MST 設定の相互接続スイッチの集まりが MST リージョンです。MST リージョンは、同じ MST 設定で MST ブリッジのグループとリンクされます。

各スイッチがどの MST リージョンに属するかは、MST コンフィギュレーションによって制御されます。この設定には、領域の名前、バージョン番号、MST VLAN とインスタンスの割り当てマップが含まれます。

リージョンには、同一の MST コンフィギュレーションを持った 1 つまたは複数のメンバが必要です。各メンバーでは、802.1w ブリッジ プロトコル データ ユニット（BPDU）を処理できる機能が必要です。ネットワーク内の MST リージョンには、数の制限はありません。

各リージョンは、最大 65 の MST インスタンス（MSTI）までサポートします。インスタンスは、1 ～ 4094 の範囲の任意の番号によって識別されます。インスタンス 0 は、特別なインスタンスである IST 用に予約されています。VLAN は、一度に 1 つの MST インスタンスに対してのみ割り当てることができます。

MST 領域は、隣接の MST 領域、他の Rapid PVST+ 領域、802.1D スパニングツリー プロトコルへの単一のブリッジとして表示されます。

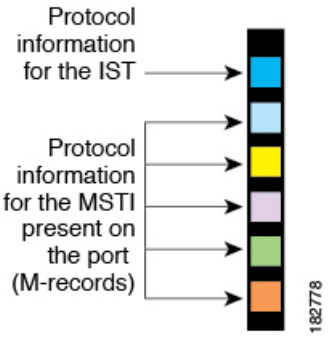
Note ネットワークを、非常に多数の領域に分けることは推奨しません。

MST BPDU

1 つの領域に含まれる MST BPDU は 1 つだけで、その BPDU により、領域内の各 MSTI について M レコードが保持されます（次の図を参照）。IST だけが MST リージョンの BPDU を送

信します。すべてのM レコードは、IST が送信する 1 つの BPDU でカプセル化されています。MST BPDU にはすべてのインスタンスに関する情報が保持されるため、MSTI をサポートするために処理する必要がある BPDU の数は、非常に少なくなります。

Figure 11: MSTI の M レコードが含まれる MST BPDU



MST設定について

単一の MST 領域内にあるすべてのスイッチで MST 設定を同一にする必要がある場合は、ユーザ側で設定します。

MST 設定の次の 3 つのパラメータを設定できます。

- 名前：MST リージョンを特定する 32 文字のストリング（ヌルでパディングし、ヌルで終了）
- リビジョン番号：現在の MST 設定のリビジョンを指定する 16 ビットの符号なし数字。

Note MST 設定の一部として必要な場合、リビジョン番号を設定する必要があります。MST 設定をコミットするたびにリビジョン番号が自動的に増加することはありません。

- MST 設定テーブル：要素が 4096 あるテーブルで、サポート対象の、存在する可能性のある 4094 の各 VLAN を該当のインスタンスにアソシエートします。最初（0）と最後（4095）の要素は 0 に設定されています。要素番号 X の値は、VLAN X がマッピングされるインスタンスを表します。

Caution VLAN/MSTI マッピングを変更すると、MST は再起動されます。

MST BPDU には、これらの 3 つの設定パラメータが含まれています。MST ブリッジは、これら 3 つの設定パラメータが厳密に一致する場合、MST BPDU をそのリージョンに受け入れます。設定属性が 1 つでも異なっていると、MST ブリッジでは、BPDU が別の MST リージョンのものであると見なされます。

IST、CIST、CST

IST、CIST、CST の概要

すべての STP インスタンスが独立している Rapid PVST+ と異なり、MST は IST、CIST、および CST スパニングツリーを次のように確立して、維持します。

- IST は、MST 領域で実行されるスパニングツリーです。

MST は、それぞれの MST 領域内で追加のスパニングツリーを確立して維持します。このスパニングツリーは、Multiple Spanning Tree Instance（MSTI）と呼ばれます。

インスタンス 0 は、IST という、領域の特殊インスタンスです。IST は、すべてのポートに必ず存在します。IST（インスタンス 0）は削除できません。デフォルトでは、すべての VLAN が IST に割り当てられます。その他すべての MSTI には、1 ～ 4094 の番号が付きます。

IST は、BPDU の送受信を行う唯一の STP インスタンスです。他の MSTI 情報はすべて MST レコード（M レコード）に含まれ、MST BPDU 内でカプセル化されます。

同じリージョン内のすべての MSTI は同じプロトコル タイマーを共有しますが、各 MSTI には、ルート ブリッジ ID やルート パス コストなど、それぞれ独自のトポロジ パラメータがあります。

MSTI は、リージョンに対してローカルです。たとえば、リージョン A とリージョン B が相互接続されている場合でも、リージョン A にある MSTI 9 は、リージョン B にある MSTI 9 とは独立しています。

- CST は、MST リージョンと、ネットワーク上で実行されている可能性がある 802.1D および 802.1w STP のインスタンスを相互接続します。CST は、ブリッジ型ネットワーク全体で 1 つだけ存在する STP インスタンスで、すべての MST リージョン、802.1w インスタンスおよび 802.1D インスタンスを含みます。
- CIST は、各 MST リージョンの IST の集合です。CIST は、MST リージョンの内部では IST と同じであり、MST リージョンの外部では CST と同じです。

MST 領域で計算されるスパニングツリーは、スイッチ ドメイン全体を含んだ CST 内のサブツリーとして認識されます。CIST は、802.1w、802.1s、802.1D の各規格をサポートするスイッチで実行されているスパニングツリー アルゴリズムによって形成されています。MST リージョン内の CIST は、リージョン外の CST と同じです。

MST 領域内でのスパニングツリーの動作

IST は 1 つのリージョン内のすべての MSTP スイッチを接続します。IST が収束すると、IST のルートは CIST リージョナル ルートになります。ネットワークに領域が 1 つしかない場合、CIST リージョナル ルートは CIST ルートにもなります。CIST ルートが領域外にある場合、領域の境界にある MST スイッチの 1 つが CIST リージョナル ルートとして選択されます。

MST スイッチが初期化されると、スイッチ自体を識別する BPDU が、CIST のルートおよび CIST リージョナル ルートとして送信されます。このとき、CIST ルートと CIST リージョナル ルートへのパス コストは両方ゼロに設定されます。また、スイッチはすべての MSTI を初期化し、これらすべての MSTI のルートであることを示します。現在ポートに格納されている情報よりも上位の MST ルート情報（より小さいスイッチ ID、より小さいパス コストなど）をスイッチが受信すると、CIST リージョナル ルートとしての主張を撤回します。

MST リージョンには、初期化中に多くのサブリージョンが含まれて、それぞれに独自の CIST リージョナル ルートが含まれることがあります。スイッチは、同一リージョンのネイバーから優位 IST 情報を受信すると、古いサブリージョンを離れ、本来の CIST リージョナル ルートを含む新しいサブリージョンに加わります。このようにして、真の CIST リージョナル ルートが含まれているサブ リージョン以外のサブ領域はすべて縮小します。

MST リージョン内のすべてのスイッチが同じ CIST リージョナル ルートを承認する必要があります。領域内の任意の 2 つのデバイスは、共通 CIST リージョナル ルートに収束する場合、MSTI のポート ロールのみを同期化します。

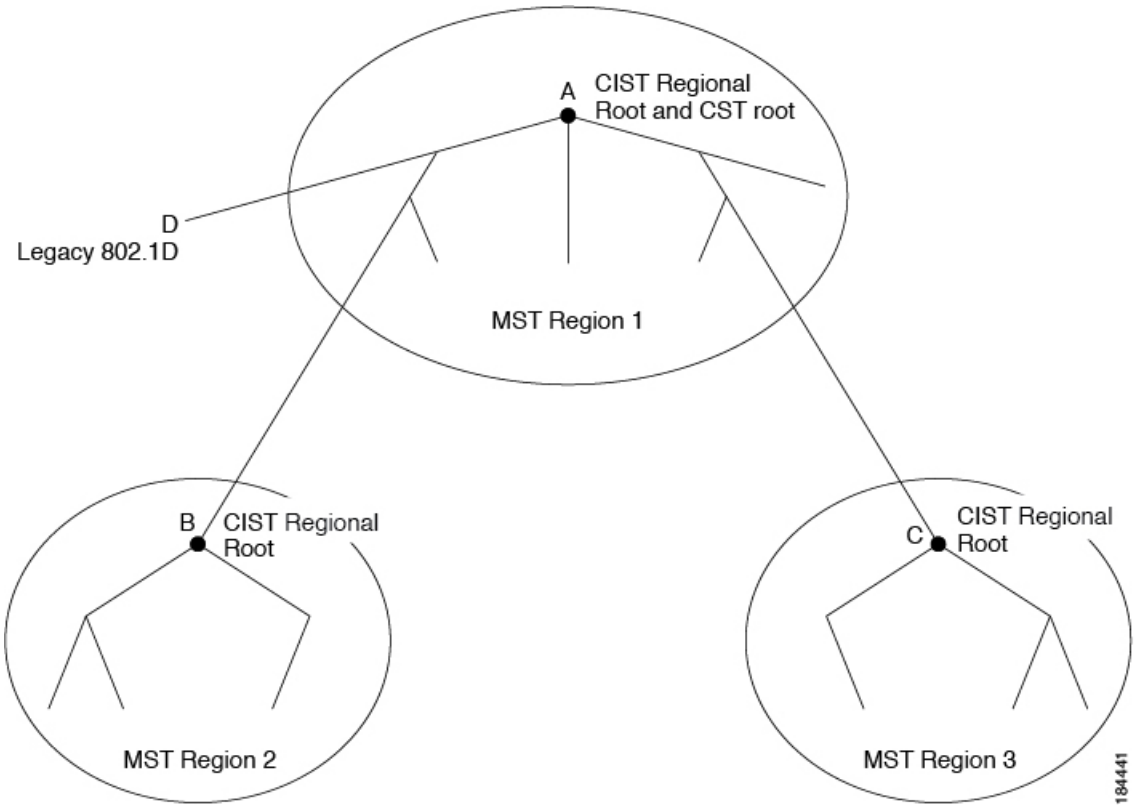
MST 領域間のスパニングツリー動作

ネットワーク内に複数の領域、または 802.1 w や 802.1D STP インスタンスがある場合、MST はネットワーク内のすべての MST 領域、すべての 802.1w と 802.1D STP スイッチを含む CST を確立して、維持します。MSTI は、リージョンの境界にある IST と組み合わさり、CST になります。

IST は、リージョン内のすべての MSTP スイッチに接続し、スイッチド ドメイン全体を網羅する CIST のサブツリーとして見なされます。サブツリーのルートは CIST リージョナル ルートです。MST リージョンは、隣接する STP スイッチや MST リージョンからは仮想スイッチとして認識されます。

次の図に、3 つの MST 領域と 802.1D（D）があるネットワークを示します。リージョン 1 の CIST リージョナル ルート（A）は、CIST ルートでもあります。リージョン 2 の CIST リージョナル ルート（B）、およびリージョン 3 の CIST リージョナル ルート（C）は、CIST 内のそれぞれのサブツリーのルートです。

Figure 12: MST リージョン、*CIST* リージョナル ルート、*CST* ルート



BPDU を送受信するのは CST インスタンスのみです。MSTI は、そのスパニングツリー情報を BPDUに（M レコードとして）追加し、隣接スイッチと相互作用して、最終的なスパニングツリートポロジを計算します。このプロセスのため、BPDUの送信に関連するスパニングツリーパラメータ（helloタイム、転送時間、最大エージングタイム、最大ホップカウントなど）は、CSTインスタンスにのみ設定されますが、すべてのMSTIに影響します。スパニングツリートポロジに関連するパラメータ（スイッチプライオリティ、ポートVLANコスト、ポートVLANプライオリティなど）は、CST インスタンスと MSTI の両方に設定できます。

MST スイッチは、802.1D 専用スイッチと通信する場合、バージョン 3 BPDU または 802.1D STP BPDU を使用します。MST スイッチは、MST スイッチと通信する場合、MST BPDU を使用します。

MST 用語

MST の命名規則には、内部パラメータまたはリージョナル パラメータの識別情報が含まれます。これらのパラメータは MST 領域内だけで使用され、ネットワーク全体で使用される外部パラメータと比較されます。CIST だけがネットワーク全体に広がるスパニングツリー インスタンスなので、CIST パラメータだけに外部修飾子が必要になり、修飾子またはリージョン修飾子は不要です。MST 用語を次に示します。

- CIST ルートは CIST のルート ブリッジで、ネットワーク全体にまたがる一意のインスタンスです。

- CIST 外部ルート パス コストは、CIST ルートまでのコストです。このコストは MST 領域内で変化しません。MST リージョンは、CIST に対する唯一のスイッチのように見えます。CIST 外部ルート パス コストは、これらの仮想スイッチとリージョンに属していないスイッチ間を計算して出したルート パス コストです。
- CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。または、CIST リージョナル ルートがそのリージョンで CIST ルートに最も近いスイッチになります。CIST リージョナル ルートは、IST のルート ブリッジとして動作します。
- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートまでのコストです。このコストは、IST つまりインスタンス 0 だけに関連します。

ホップ カウント

MST リージョン内の STP トポロジを計算する場合、MST はコンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報は使用しません。代わりに、ルートへのパス コストと、IP の存続可能時間（TTL）メカニズムに類似したホップ カウント メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用すると、領域内の最大ホップ数を設定し、IST およびその領域のすべての MSTI に適用できます。

ホップ カウントは、メッセージ エージ情報と同じ結果になります（再設定を開始）。インスタンスのルート ブリッジは、コストが 0 でホップ カウントが最大値に設定された BPDU（M レコード）を常に送信します。スイッチがこの BPDU を受信すると、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウントとする BPDU を生成し、これを伝播します。このホップ カウントが 0 になると、スイッチはその BPDU を廃棄し、ポート用に維持されていた情報を期限切れにします。

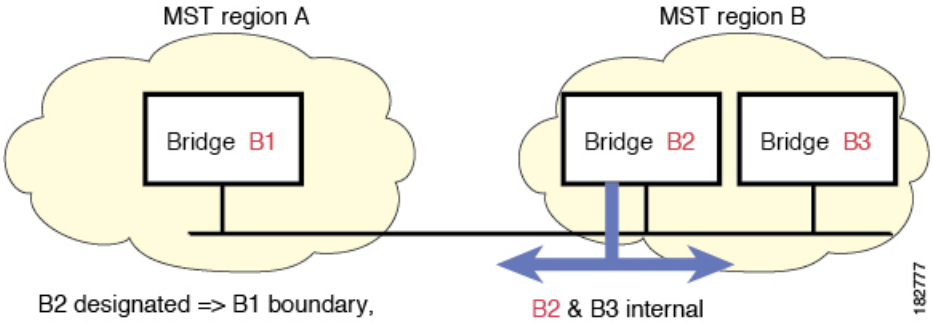
BPDU の 802.1w 部分に格納されているメッセージ有効期間および最大エージング タイムの情報は、領域全体で同じです（IST の場合のみ）。同じ値が、境界にある領域の指定ポートによって伝播されます。

スイッチがスパニングツリー設定メッセージを受信せずに再設定を試行するまで待機する秒数として最大エージング タイムを設定します。

境界ポート

境界ポートは、ある領域を別の領域に接続するポートです。指定ポートは、STP ブリッジを検出するか、設定が異なる MST ブリッジまたは Rapid PVST+ ブリッジから合意提案を受信すると、境界にあることを認識します。この定義により、領域の内部にある 2 つのポートが、異なる領域に属すポートとセグメントを共有できるため、ポートで内部メッセージと外部メッセージの両方を受信できる可能性があります（次の図を参照）。

Figure 13: MST 境界ポート



境界では、MST ポートのロールは問題ではなく、そのステートは強制的に IST ポート ステートと同じに設定されます。境界フラグがポートに対してオンに設定されている場合、MST ポートのロールの選択処理では、ポートのロールが境界に割り当てられ、同じステートが IST ポートのステートとして割り当てられます。境界にある IST ポートでは、バックアップ ポートのロール以外のすべてのポートのロールを引き継ぐことができます。

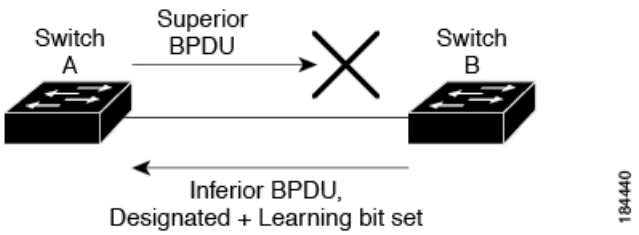
スパニングツリーの異議メカニズム

現在、この機能は、IEEE MST 規格にはありませんが、規格準拠の実装に含まれています。ソフトウェアは、受信した BPDU でポートのロールおよびステートの一貫性をチェックし、ブリッジング ループの原因となることがある単方向リンク障害を検出します。

指定ポートは、矛盾を検出すると、そのロールを維持しますが、廃棄ステートに戻ります。一貫性がない場合は、接続を中断した方がブリッジング ループを解決できるからです。

次の図に、ブリッジング ループの一般的な原因となる単一方向リンク障害を示します。スイッチ A はルート ブリッジであり、スイッチ B へのリンクで BPDU は失われます。Rapid PVST+ (802.1w) には、送信側ポートのロールと状態が含まれます。この情報により、スイッチ B は送信される上位 BPDU に対して反応せず、スイッチ B はルート ポートではなく指定ポートであることが、スイッチ A によって検出できます。この結果、スイッチ A は、そのポートをブロックし（またはブロックし続け）、ブリッジング ループが防止されます。ブロックは、STP の矛盾として示されます。

Figure 14: 単一方向リンク障害の検出



ポート コストとポート プライオリティ

スパニングツリーはポートコストを使用して、指定ポートを決定します。値が低いほど、ポート コストは小さくなります。スパニングツリーでは、最小のコスト パスが選択されます。デフォルト ポート コストは、次のように、インターフェイス帯域幅から取得されます。

- 10 Mbps：2,000,000
- 100 Mbps：200,000
- 1 ギガビット イーサネット：20,000
- 10 ギガビット イーサネット：2,000

ポート コストを設定すると、選択されるポートが影響を受けます。

Note MST では常にロング パスコスト計算方式が使用されるため、有効値は 1 ～ 200,000,000 です。

コストが同じポートを差別化するために、ポートプライオリティが使用されます。値が小さいほど、プライオリティが高いことを示します。デフォルトのポートのプライオリティは128です。プライオリティは、0 ～ 224 の間の値に、32 ずつ増やして設定できます。

IEEE 802.1D との相互運用性

MST が実行されるスイッチでは、802.1D STP スイッチとの相互運用を可能にする、内蔵プロトコル移行機能がサポートされます。このスイッチで、802.1D コンフィギュレーション BPDU（プロトコル バージョンが 0 に設定されている BPDU）を受信する場合、そのポート上の 802.1D BPDU のみが送信されます。また、MST スイッチは、802.1D BPDU、別の領域に関連する MST BPDU（バージョン 3）、802.1w BPDU（バージョン 2）のうちいずれかを受信すると、ポートが領域の境界にあることを検出できます。

ただし、スイッチは、802.1D BPDU を受信しなくなった場合でも、自動的には MSTP モードには戻りません。これは、802.1D スイッチが指定スイッチではない場合、802.1D スイッチがリンクから削除されたかどうかを検出できないためです。さらにスイッチは、接続先スイッチがリージョンに加入した場合であっても、引き続きポートに境界の役割を指定する可能性があります。

プロトコル移行プロセスを再開する（強制的に隣接デバイスと再ネゴシエーションさせる）には、**clear spanning-tree detected-protocols** コマンドを入力します。

リンク上にあるすべての Rapid PVST+ スイッチ（およびすべての 8021.D STP スイッチ）では、MST BPDU を 802.1w BPDU の場合と同様に処理できます。MST スイッチは、バージョン 0 設定とトポロジ変更通知（TCN）BPDU、またはバージョン 3 MST BPDU のどちらかを境界ポートで送信できます。境界ポートは LAN に接続され、その指定スイッチは、単一スパニングツリー スイッチか、MST 設定が異なるスイッチのいずれかです。

Note MST は、MST ポート上で先行標準 MSTP を受信するたびに、シスコの先行標準マルチ スパニングツリー プロトコル（MSTP）と相互に動作します。明示的な設定は必要ありません。

Rapid PVST+ の相互運用性と PVST シミュレーションについて

MST は、ユーザが設定しなくても、Rapid PVST+ と相互運用できます。PVST シミュレーション機能により、このシームレスな相互運用が可能になっています。

Note PVST シミュレーションは、デフォルトでイネーブルになっています。つまり、スイッチ上のすべてのインターフェイスは、デフォルトで、MST と Rapid PVST+ との間で相互動作します。

ただし、MST と Rapid PVST+ との接続を制御し、MST 対応ポートを Rapid PVST+ 対応ポートに誤って接続するのを防止することが必要な場合もあります。Rapid PVST+ はデフォルト STP モードのため、Rapid PVST+ がイネーブルな多数の接続が検出されることがあります。

Rapid PVST+ シミュレーションを、ポート単位でディセーブルにするか、スイッチ全体でグローバルにディセーブルにすると、MST イネーブル ポートは、Rapid PVST+ イネーブル ポートに接続したことが検出された時点で、ブロッキング ステートに移行します。このポートは、Rapid PVST+/SSTP BPDU を受信しなくなるまで不整合ステートのままですが、そのあとは標準 STP のステート移行を再開します。

MST コンフィギュレーション

MST 設定時の注意事項

- MST 設定モードの場合、次の注意事項が適用されます。
  - 各コマンド参照行により、保留中のリージョン設定が作成されます。
  - 保留中のリージョン設定により、現在のリージョン設定が開始されます。
  - 変更をコミットすることなく MST コンフィギュレーション モードを終了するには、**abort** コマンドを入力します。
  - 行った変更内容をすべてコミットして MST コンフィギュレーション モードを終了するには、**exit** コマンドを入力します。

MST の有効化

MST はイネーブルにする必要があります。デフォルトは Rapid PVST+ です。

Caution スパニングツリー モードを変更すると、変更前のモードのスパニングツリー インスタンスがすべて停止されて新しいモードで起動されるため、トラフィックが中断する場合があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch# **configure terminal**
3. switch(config)# **spanning-tree mode mst**
4. (Optional) switch(config)# **no spanning-tree mode mst**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 3	switch(config)# **spanning-tree mode mst**	スイッチ上で MST をイネーブルにします。
ステップ 4	(Optional) switch(config)# **no spanning-tree mode mst**	スイッチ上の MST がディセーブルにされ、Rapid PVST+ に戻ります。

Example

次の例は、スイッチで MST をイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mode mst
```

Note STP はデフォルトでイネーブルのため、設定結果を参照するために **show running-config** コマンドを入力しても、STP をイネーブルするために入力したコマンドは表示されません。

MST コンフィギュレーション モードの開始

スイッチ上で、MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定するには、MST コンフィギュレーション モードを開始します。

同じ MST リージョンにある複数のスイッチには、同じ MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定しておく必要があります。

Note 各コマンド参照行により、MST コンフィギュレーション モードで保留中の領域設定が作成されます。加えて、保留中のリージョン設定により、現在のリージョン設定が開始されます。

MST コンフィギュレーション モードで作業している場合、**exit** コマンドと **abort** コマンドとの違いに注意してください。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst configuration**
3. switch(config-mst)# **exit** or switch(config-mst)# **abort**
4. (Optional) switch(config)# **no spanning-tree mst configuration**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree mst configuration**	システム上で、MST コンフィギュレーション モードを開始します。次の MST コンフィギュレーション パラメータを割り当てるには、MST コンフィギュレーション モードを開始しておく必要があります。 • MST 名 • インスタンスから VLAN へのマッピング • MST リビジョン番号
ステップ 3	switch(config-mst)# **exit** or switch(config-mst)# **abort**	終了または中断します。 • **exit** コマンドは、すべての変更をコミットして MST コンフィギュレーション モードを終了します。 • **abort** コマンドは、変更をコミットすることなく MST コンフィギュレーション モードを終了します。

	Command or Action	Purpose
ステップ 4	(Optional) switch(config)# **no spanning-tree mst configuration**	MST リージョン設定を次のデフォルト値に戻します。 • 領域名は空の文字列になります。 • VLAN は MSTI にマッピングされません（すべての VLAN は CIST インスタンスにマッピングされます）。 • リビジョン番号は 0 です。

MST の名前の指定

ブリッジに領域名を設定できます。同じ MST リージョンにある複数のブリッジには、同じ MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定しておく必要があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst configuration**
3. switch(config-mst)# **name** *name*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree mst configuration**	MST コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-mst)# **name** *name*	MST 領域の名前を指定します。*name* ストリングには 32 文字まで使用でき、大文字と小文字が区別されます。デフォルトは空の文字列です。

Example

次の例は、MST リージョンの名前の設定方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst configuration
switch(config-mst)# name accounting
```

MST 設定のリビジョン番号の指定

リビジョン番号は、ブリッジ上に設定します。同じ MST リージョンにある複数のブリッジには、同じ MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定しておく必要があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst configuration**
3. switch(config-mst)# **revision** *name*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree mst configuration**	MST コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-mst)# **revision** *name*	MST リージョンのリビジョン番号を指定します。範囲は 0 ～ 65535 で、デフォルト値は 0 です。

Example

次に、MSTI 領域のリビジョン番号を 5 に設定する例を示します。

```
switch# configure terminal
switch(config)# spanning-tree mst configuration
switch(config-mst)# revision 5
```

MST リージョンでの設定の指定

2つ以上のスイッチを同じMSTリージョンに設定するには、その2つのスイッチに同じVLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。

領域には、同じ MST 設定の 1 つのメンバまたは複数のメンバを存在させることができます。各メンバでは、IEEE 802.1w RSTP BPDU を処理できる必要があります。ネットワーク内の MST リージョンには数の制限はありませんが、各リージョンでは最大 65 までのインスタンスをサポートできます。VLAN は、一度に 1 つの MST インスタンスに対してのみ割り当てることができます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst configuration**
3. switch(config-mst)# **instance** *instance-id* **vlan** *vlan-range*
4. switch(config-mst)# **name** *name*
5. switch(config-mst)# **revision** *name*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree mst configuration**	MST コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-mst)# **instance** *instance-id* **vlan** *vlan-range*	VLAN を MST インスタンスにマッピングする手順は、次のとおりです。 • *instance-id* の範囲は 1 ～ 4094 です。 • **vlan** *vlan-range* の範囲は 1 ～ 4094 です。 VLAN を MSTI にマップする場合、マッピングは増加され、コマンドに指定した VLAN は、以前マッピングした VLAN に追加されるか、そこから削除されます。 VLAN の範囲を指定するにはハイフンを入力します。たとえば VLAN 1 ～ 63 を MST インスタンス 1 にマッピングするには、 **instance 1 vlan 1-63** コマンドを入力します。 一連の VLAN を指定するにはカンマを入力します。たとえば VLAN 10、20、30 を MST インスタンス 1 にマッピングするには、 **instance 1 vlan 10, 20, 30** コマンドを入力します。
ステップ 4	switch(config-mst)# **name** *name*	インスタンス名を指定します。 *name* ストリングには 32 文字まで使用でき、大文字と小文字が区別されます。
ステップ 5	switch(config-mst)# **revision** *name*	設定リビジョン番号を指定します。範囲は 0 ～ 65535 です。

Example

デフォルトに戻すには、次のように操作します。

- デフォルトの MST リージョン設定に戻すには、 **no spanning-tree mst configuration** コンフィギュレーション コマンドを入力します。
- VLAN インスタンス マッピングをデフォルトの設定に戻すには、 **no instance** *instance-id* **vlan** *vlan-range* MST コンフィギュレーション コマンドを使用します。
- デフォルトの名前に戻すには、 **no name** MST コンフィギュレーション コマンドを入力します。
- デフォルトのリビジョン番号に戻すには、 **no revision** MST コンフィギュレーション コマンドを入力します。
- Rapid PVST +を再度イネーブルにするには、 **no spanning-tree mode** または **spanning-tree mode rapid-pvst** グローバルコンフィギュレーションコマンドを入力します。

次の例は、MST コンフィギュレーション モードを開始し、VLAN 10 ～ 20 を MSTI 1 にマッピングし、領域に region1 という名前を付けて、設定リビジョンを 1 に設定し、保留中の設定を表示し、変更を適用してグローバル コンフィギュレーション モードに戻る方法を示しています。

```
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 1 vlan 10-20
switch(config-mst)# name region1
switch(config-mst)# revision 1
switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instances configured 2
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------
```

VLAN から MST インスタンスへのマッピングとマッピング解除

Caution VLAN/MSTI マッピングを変更すると、MST は再起動されます。

Note MSTI はディセーブルにできません。

同じ MST リージョンにある複数のブリッジには、同じ MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定しておく必要があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst configuration**
3. switch(config-mst)# **instance** *instance-id* **vlan** *vlan-range*
4. switch(config-mst)# **no instance** *instance-id* **vlan** *vlan-range*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree mst configuration**	MST コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-mst)# **instance** *instance-id* **vlan** *vlan-range*	VLAN を MST インスタンスにマッピングする手順は、次のとおりです。 • *instance-id* の範囲は 1 ～ 4094 です。 インスタンス 0 は、各 MST リージョンでの IST 用に予約されています。 • *vlan-range* の範囲は 1 ～ 4094 です。 VLAN を MSTI にマッピングすると、マッピングは差分で実行され、コマンドで指定された VLAN が、以前マッピングされた VLAN に追加または VLAN から削除されます。
ステップ 4	switch(config-mst)# **no instance** *instance-id* **vlan** *vlan-range*	指定したインスタンスを削除し、VLAN を、デフォルト MSTI である CIST に戻します。

Example

次の例は、VLAN 200 を MSTI 3 にマッピングする方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 3 vlan 200
```

ルート ブリッジの設定

スイッチは、ルート ブリッジになるよう設定できます。

Note 各 MSTI のルート ブリッジは、バックボーン スイッチまたはディストリビューション スイッチである必要があります。アクセス スイッチは、スパニングツリーのプライマリ ルートブリッジとして設定しないでください。

MSTI 0（または IST）でのみ使用可能な **diameter** キーワードを入力し、ネットワーク直径（ネットワーク内の任意の 2 つのエンド ステーション間での最大ホップ数）を指定します。ネットワークの直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムをスイッチが自動的に設定するので、コンバージェンスの所要時間を大幅に短縮できます。自動的に算出された hello タイムを無効にするには、**hello** キーワードを入力します。

Note ルート ブリッジとして設定されたデバイスでは、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、**spanning-tree mst max-age** のグローバル コンフィギュレーション コマンドを使用して hello タイム、転送遅延時間、最大エージング タイムを手動で設定しないでください。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]]
3. (Optional) switch(config)# **no spanning-tree mst** *instance-id* **root**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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。

	Command or Action	Purpose
ステップ 2	switch(config)# **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]]	次のように、ルートブリッジとしてスイッチを設定します。 • *instance-id* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。値の範囲は 1 ～ 4094 です。 • diameter *net-diameter* には、2 つのエンド ステーション間にホップの最大数を設定します。デフォルトは 7 です。このキーワードは、MSTI インスタンス 0 の場合にのみ使用できます。 • hello-time *seconds* には、ルート ブリッジが設定メッセージを生成する時間を秒単位で指定します。有効範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。
ステップ 3	(Optional) switch(config)# **no spanning-tree mst** *instance-id* **root**	スイッチのプライオリティ、範囲、hello タイムをデフォルト値に戻します。

Example

次の例は、MSTI 5 のルート スイッチとしてスイッチを設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst 5 root primary
```

セカンダリ ルート ブリッジの設定

このコマンドは、複数のスイッチに対して実行し、複数のバックアップ ルート ブリッジを設定できます。**spanning-tree mst root primary** コンフィギュレーション コマンドでプライマリ ルート ブリッジを設定したときに使用したのと同じネットワーク直径と hello タイムの値を入力します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]]
3. (Optional) switch(config)# **no spanning-tree mst** *instance-id* **root**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]]	次のように、セカンダリ ルート ブリッジとしてスイッチを設定します。 • *instance-id* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。値の範囲は 1 ～ 4094 です。 • diameter *net-diameter* には、2 つのエンド ステーション間にホップの最大数を設定します。デフォルトは 7 です。このキーワードは、MSTI インスタンス 0 の場合にのみ使用できます。 • hello-time *seconds* には、ルート ブリッジが設定メッセージを生成する時間を秒単位で指定します。有効範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。
ステップ 3	(Optional) switch(config)# **no spanning-tree mst** *instance-id* **root**	スイッチのプライオリティ、範囲、hello タイムをデフォルト値に戻します。

Example

次の例は、MSTI 5 のセカンダリ ルート スイッチとしてスイッチを設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst 5 root secondary
```

ポートのプライオリティの設定

ループが発生する場合、MST は、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とき、ポートプライオリティを使用します。最初に選択させるインターフェイスには低いプライオリティの値を割り当て、最後に選択させるインターフェイスには高いプライオリティの値を割り当てることができます。すべてのインターフェイスのプライオリティ値が同一である場合、MST はインターフェイス番号が最も低いインターフェイスをフォワーディング ステートにして、その他のインターフェイスをブロックします。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {{*type slot*/*port*} | {**port-channel** *number*}}
3. switch(config-if)# **spanning-tree mst** *instance-id* **port-priority** *priority*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** {{*type slot*/*port*} | {**port-channel** *number*}}	設定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	switch(config-if)# **spanning-tree mst** *instance-id* **port-priority** *priority*	次のように、ポートのプライオリティを設定します。 • *instance-id* には、単一 MSTI、ハイフンで区切った MSTI の範囲、カンマで区切った一連の MSTI を指定できます。値の範囲は 1 ～ 4094 です。 • *priority* の範囲は 0 ～ 224 で、32 ずつ増加します。デフォルトは 128 です。値が小さいほど、プライオリティが高いことを示します。 プライオリティ値は、0、32、64、96、128、160、192、224 です。システムでは、他のすべての値が拒否されます。

Example

次の例は、イーサネット ポート 3/1 で MSTI 3 の MST インターフェイス ポート プライオリティを 64 に設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# spanning-tree mst 3 port-priority 64
```

このコマンドを使用できるのは、物理イーサネット インターフェイスに対してだけです。

ポート コストの設定

MST パス コストのデフォルト値は、インターフェイスのメディア速度から算出されます。ループが発生した場合、MST は、コストを使用して、フォワーディング ステートにするインター

フェイスを選択します。最初に選択させるインターフェイスには小さいコストの値を割り当て、最後に選択させるインターフェイスの値には大きいコストを割り当てることができます。すべてのインターフェイスのコスト値が同一である場合、MST はインターフェイス番号が最も低いインターフェイスをフォワーディング ステートにして、その他のインターフェイスをブロックします。

Note MST はロング パスコスト計算方式を使用します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {{*type slot*/*port*} | {**port-channel** *number*}}
3. switch(config-if)# **spanning-tree mst** *instance-id* **cost** [*cost* | **auto**]

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** {{*type slot*/*port*} | {**port-channel** *number*}}	設定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	switch(config-if)# **spanning-tree mst** *instance-id* **cost** [*cost* | **auto**]	コストを設定します。 ループが発生した場合、MST はパス コストを使用して、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します。パス コストが小さいほど、送信速度が速いことを示します。 • *instance-id* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。値の範囲は 1 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値は auto で、インターフェイスのメディア速度から派生されます。

Example

次の例は、イーサネット ポート 3/1 で MSTI 4 の MST インターフェイス ポート コストを設定する方法を示しています。

```
switch# configure terminal
```

```
switch(config)# interface ethernet 3/1
switch(config-if)# spanning-tree mst 4 cost 17031970
```

スイッチ プライオリティの設定

MST インスタンスのスイッチのプライオリティは、指定されたポートがルート ブリッジとして選択されるように設定できます。

Note このコマンドの使用には注意してください。ほとんどの場合、スイッチのプライオリティを変更するには、**spanning-tree mst root primary** および **spanning-tree mst root secondary** のグローバル コンフィギュレーション コマンドの使用を推奨します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst** *instance-id* **priority** *priority-value*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree mst** *instance-id* **priority** *priority-value*	次のように、スイッチのプライオリティを設定します。 • *instance-id* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。値の範囲は 1 ～ 4094 です。 • priority には、4096 単位で 0 ～ 61440 の値を指定します。デフォルトは 32768 です。小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高くなります。 使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。システムでは、他のすべての値が拒否されます。

Example

次の例は、MSTI 5 のブリッジのプライオリティを 4096 に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst 5 priority 4096
```

hello タイムの設定

hello タイムを変更することによって、スイッチ上のすべてのインスタンスについて、ルートブリッジにより設定メッセージを生成する間隔を設定できます。

Note このコマンドの使用には注意してください。多くの状況では、 **spanning-tree mst** *instance-id* **root primary** および **spanning-tree mst** *instance-id* **root secondary** コンフィギュレーション コマンドを入力して hello タイムを変更することを推奨します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst hello-time** *seconds*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree mst hello-time** *seconds*	すべての MST インスタンスについて、hello タイムを設定します。hello タイムは、ルート ブリッジが設定メッセージを生成する時間です。これらのメッセージは、スイッチがアクティブであることを意味します。*seconds* の範囲は 1 ～ 10 で、デフォルトは 2 秒です。

Example

次の例は、スイッチの hello タイムを 1 秒に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst hello-time 1
```

転送遅延時間の設定

スイッチ上のすべての MST インスタンスには、1 つのコマンドで転送遅延タイマーを設定できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst forward-time** *seconds*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree mst forward-time** *seconds*	すべての MST インスタンスについて、転送時間を設定します。転送遅延は、スパニングツリーブロッキング ステートとラーニング ステートからフォワーディング ステートに変更する前に、ポートが待つ秒数です。秒数は 4 ～ 30 秒で、デフォルトは 15 秒です。

Example

次の例は、スイッチの転送遅延時間を 10 秒に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst forward-time 10
```

最大エージング タイムの設定

最大経過時間タイマーは、スイッチが、再設定を試行する前に、スパニングツリー設定メッセージの受信を待つ秒数です。

スイッチ上のすべての MST インスタンスには、1 つのコマンドで最大経過時間タイマーを設定できます（最大経過時間は IST にのみ適用されます）。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst max-age** *seconds*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree mst max-age** *seconds*	すべての MST インスタンスについて、最大経過時間を設定します。最大経過時間は、スイッチが、再設定を試行する前に、スパニングツリー設定メッセージの受信を待つ秒数です。*seconds* の範囲は 6 ～ 40 で、デフォルトは 20 秒です。

Example

次の例は、スイッチの最大エージング タイマーを 40 秒に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst max-age 40
```

最大ホップ カウントの設定

MST では、IST リージョナル ルートへのパス コストと、IP の存続可能時間（TTL）メカニズムに類似したホップ カウント メカニズムが、使用されます。領域内の最大ホップを設定し、それをその領域内にある IST およびすべての MST インスタンスに適用できます。ホップ カウントは、メッセージ エージ情報と同じ結果になります（再設定を開始）。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst max-hops** *hop-count*

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree mst max-hops** *hop-count*	BPDU を廃棄してポート用に保持していた情報を期限切れにするまでの、リージョンでのホップ数を設定します。*hop-count* の有効範囲は 1 ～ 255 で、デフォルト値は 20 ホップです。

Example

次の例は、最大ホップ カウントを 40 に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst max-hops 40
```

PVST シミュレーションのグローバル設定

この自動機能は、グローバルまたはポートごとにブロックできます。グローバル コマンドを入力すると、インターフェイス コマンド モードの実行中に、スイッチ全体の PVST シミュレーション設定を変更できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no spanning-tree mst simulate pvst global**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **no spanning-tree mst simulate pvst global**	Rapid PVST+ モードで実行中の接続スイッチと自動的に相互動作する状態から、スイッチ上のすべてのインターフェイスをディセーブルにできます。スイッチ上のすべてのインターフェイスは、デフォルトで、Rapid PVST+ と MST との間でシームレスに動作します。

Example

次の例は、Rapid PVST+ を実行している接続スイッチと自動的に相互運用することを防止するようにスイッチを設定する方法を示しています。

```
switch# configure terminal
switch(config)# no spanning-tree mst simulate pvst global
```

ポートごとの PVST シミュレーションの設定

MST は、Rapid PVST+ とシームレスに相互動作します。ただし、デフォルト STP モードとして MST が実行されていないスイッチへの誤った接続を防ぐため、この自動機能をディセーブ

ルにする必要が生じる場合があります。Rapid PVST+ シミュレーションをディセーブルにした場合、MST がイネーブルなポートが Rapid PVST+ がイネーブルなポートに接続されていることが検出されると、MST がイネーブルなポートは、ブロッキング ステートに移行します。このポートは、BPDU の受信が停止されるまで、一貫性のないステートのままになり、それから、ポートは、通常の STP 送信プロセスに戻ります。

この自動機能は、グローバルまたはポートごとにブロックできます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {{*type slot*/*port*} | {**port-channel** *number*}}
3. switch(config-if)# **spanning-tree mst simulate pvst disable**
4. switch(config-if)# **spanning-tree mst simulate pvst**
5. switch(config-if)# **no spanning-tree mst simulate pvst**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** {{*type slot*/*port*} | {**port-channel** *number*}}	設定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	switch(config-if)# **spanning-tree mst simulate pvst disable**	Rapid PVST+ モードで実行中の接続スイッチと自動的に相互動作する状態から、指定したインターフェイスをディセーブルにします。 スイッチ上のすべてのインターフェイスは、デフォルトで、Rapid PVST+ と MST との間でシームレスに動作します。
ステップ 4	switch(config-if)# **spanning-tree mst simulate pvst**	指定したインターフェイスで、MST と Rapid PVST+ との間のシームレスな動作を再度イネーブルにします。
ステップ 5	switch(config-if)# **no spanning-tree mst simulate pvst**	インターフェイスを、**spanning-tree mst simulate pvst global** コマンドを使用して、設定したスイッチ全体で MST と Rapid PVST+ との間で相互動作するよう設定します。

Example

次の例は、MSTを実行していない接続スイッチと自動的に相互運用することを防止するように指定インターフェイスを設定する方法を示しています。

```
switch# configure terminal
```

```
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree mst simulate pvst disable
```

リンク タイプの設定

Rapid の接続性（802.1w 規格）は、ポイントツーポイントのリンク上でのみ確立されます。リンク タイプは、デフォルトでは、インターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。

リモート スイッチの 1 つのポートに、ポイントツーポイントで物理的に接続されている半二重リンクがある場合、リンク タイプのデフォルト設定を上書きし、高速移行をイネーブルにできます。

リンクを共有に設定すると、STP は 802.1D に戻されます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# **spanning-tree link-type** {**auto** | **point-to-point** | **shared**}

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** *type slot/port*	設定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	switch(config-if)# **spanning-tree link-type** {**auto** | **point-to-point** | **shared**}	リンク タイプを、ポイントツーポイントまたは共有に設定します。システムでは、スイッチ接続からデフォルト値を読み込みます。半二重リンクは共有で、全二重リンクはポイントツーポイントです。リンク タイプが共有の場合、STP は 802.1D に戻ります。デフォルトは auto で、インターフェイスのデュプレックス設定に基づいてリンク タイプが設定されます。

Example

次の例は、リンク タイプをポイントツーポイントとして設定する方法を示しています。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
```

```
switch(config-if)# spanning-tree link-type point-to-point
```

プロトコルの再開

MST ブリッジは、レガシー BPDU または別のリージョンと関連付けられた MST BPDU を受信すると、ポートがリージョンの境界に位置していることを検出できます。ただし、STP プロトコルの移行では、レガシー スイッチが指定スイッチではない場合、IEEE 802.1D のみが実行されているレガシー スイッチが、リンクから削除されたかどうかを認識できません。スイッチ全体または指定したインターフェイスでプロトコル ネゴシエーションを再開する（強制的に隣接スイッチと再ネゴシエーションさせる）には、このコマンドを入力します。

SUMMARY STEPS

1. switch# **clear spanning-tree detected-protocol** [**interface** *interface* [*interface-num* | *port-channel*]]

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **clear spanning-tree detected-protocol** [**interface** *interface* [*interface-num*	*port-channel*]]	スイッチ全体または指定したインターフェイスで、MST を再開します。

Example

次の例は、スロット 2、ポート 8 のイーサネット インターフェイスで MST を再起動する方法を示しています。

```
switch# clear spanning-tree detected-protocol interface ethernet 2/8
```

MST 設定の確認

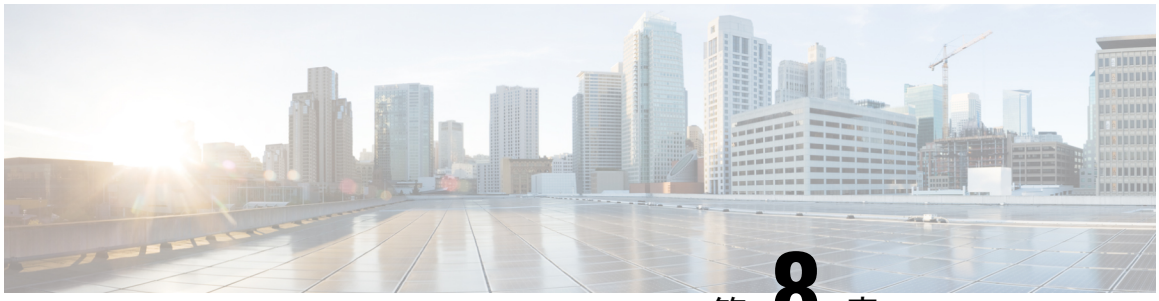
MST の設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
show running-config spanning-tree [**all**]	現在のスパニングツリー設定を表示します。
show spanning-tree mst [*options*]	現在の MST 設定の詳細情報を表示します。

次に、現在の MST 設定を表示する例を示します。

```
switch# show spanning-tree mst configuration
% Switch is not in mst mode
Name      [mist-attempt]
Revision  1     Instances configured 2
```

```
Instance  Vlans mapped
--------  ------------------------------------------------------------------------
0         1-12,14-41,43-4094
1         13,42
```



第 8 章

STP 拡張機能の設定

STP 拡張機能について

STP 拡張機能について

シスコでは、スパニングツリープロトコル（STP）に、収束をより効率的に行うための拡張機能を追加しました。場合によっては、同様の機能が IEEE 802.1w 高速スパニングツリープロトコル（RSTP）標準にも組み込まれている可能性がありますが、シスコの拡張機能を使用することを推奨します。これらの拡張機能はすべて、RPVST+ およびマルチ スパニングツリー プロトコル（MST）と組み合わせて使用できます。

使用可能な拡張機能には、スパニングツリー ポート タイプ、Bridge Assurance、ブリッジ プロトコルデータ ユニット（BPDU）ガード、BPDU フィルタリング、ループ ガード、ルート ガードがあります。これらの機能の大部分は、グローバルに、または指定インターフェイスに適用できます。

Note このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。IEEE 802.1D STP について説明している箇所では、802.1D と明記します。

STP ポート タイプの概要

スパニングツリー ポートは、エッジ ポート、ネットワーク ポート、または標準ポートとして構成できます。ポートは、ある一時点において、これらのうちいずれか 1 つの状態をとります。デフォルトのスパニング ツリー ポート タイプは「標準」です。インターフェイスが接続

されているデバイスのタイプによって、スパニングツリー ポートを上記いずれかのポート タイプに設定できます。

スパニングツリー エッジ ポート

エッジ ポートは、ホストに接続されるポートであり、アクセス ポートとトランク ポートのどちらにもなります。エッジ ポート インターフェイスは、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します（この直接移行動作は、以前は、シスコ独自の機能 PortFast として設定していました）。

ホストに接続されているインターフェイスは、STP ブリッジ プロトコル データ ユニット（BPDU）を受信してはなりません。

Note 別のスイッチに接続されているポートをエッジ ポートとして設定すると、ブリッジング ループが発生する可能性があります。

スパニングツリー ネットワーク ポート

ネットワーク ポートは、スイッチまたはブリッジにだけ接続されます。Bridge Assurance がグローバルにイネーブルになっている間にポートをネットワーク ポートとして設定すると、そのポートで Bridge Assurance がイネーブルになります。

Note ホストまたは他のエッジ デバイスに接続されているポートを誤ってスパニングツリー ネットワーク ポートとして設定すると、それらのポートは自動的にブロッキング ステートに移行します。

スパニングツリー標準ポート

標準ポートは、ホスト、スイッチ、またはブリッジに接続できます。これらのポートは、標準スパニングツリー ポートとして機能します。

デフォルトのスパニングツリー インターフェイスは標準ポートです。

Bridge Assurance の概要

Bridge Assurance を使用すると、ネットワーク内でブリッジング ループの原因となる問題の発生を防ぐことができます。具体的には、単方向リンク障害や、スパニングツリー アルゴリズムを実行しなくなってもデータ トラフィックの転送を続けているデバイスなどからネットワークを保護できます。

Note Bridge Assurance は、Rapid PVST+ および MST だけでサポートされています。従来の 802.1D スパニングツリーではサポートされていません。

Bridge Assurance はデフォルトでイネーブルになっており、グローバル単位でだけディセーブルにできます。また、Bridge Assurance をイネーブルにできるのは、ポイントツーポイント リンクに接続されたスパニングツリー ネットワーク ポートだけです。Bridge Assurance は必ず、リンクの両端でイネーブルにする必要があります。

Bridge Assurance をイネーブルにすると、BPDU が hello タイムごとに、動作中のすべてのネットワーク ポート（代替ポートとバックアップ ポートを含む）に送出されます。所定の期間 BPDU を受信しないポートは、ブロッキング ステートに移行し、ルート ポートの決定に使用されなくなります。BPDU を再度受信するようになると、そのポートで通常のスパニングツリー状態遷移が再開されます。

BPDU ガードの概要

BPDU ガードをイネーブルにすると、BPDU を受信したときにそのインターフェイスがシャットダウンされます。

BPDU ガードはインターフェイス レベルで設定できます。BPDU ガードをインターフェイス レベルで設定すると、そのポートはポート タイプ設定にかかわらず BPDU を受信するとすぐにシャットダウンされます。

BPDU ガードをグローバル単位で設定すると、動作中のスパニングツリー エッジ ポート上だけで有効となります。正しい設定では、LAN エッジ インターフェイスは BPDU を受信しません。エッジ インターフェイスが BPDU を受信すると、無効な設定（未認証のホストまたはスイッチへの接続など）を知らせるシグナルが送信されます。BPDUガードをグローバル単位でイネーブルにすると、BPDU を受信したすべてのスパニングツリー エッジ ポートがシャットダウンされます。

Note エッジ トランク インターフェイスレベルでは、無効な VLAN のリモート側がアクセス ポートとして設定されている場合、BPDU は無視されます。

BPDUガードは、無効な設定があると確実に応答を返します。無効な設定をした場合は、当該 LAN インターフェイスを手動でサービス状態に戻す必要があるからです。

Note BPDU ガードをグローバル単位でイネーブルにすると、動作中のすべてのスパニングツリー エッジ インターフェイスに適用されます。

BPDU フィルタリングの概要

BPDUフィルタリングを使用すると、スイッチが特定のポートでBPDUを送信または受信するのを禁止できます。

グローバルに設定された BPDU フィルタリングは、動作中のすべてのスパニングツリー エッジポートに適用されます。エッジポートはホストだけに接続してください。ホストでは通常、BPDU は破棄されます。動作中のスパニングツリー エッジ ポートが BPDU を受信すると、ただちに標準のスパニングツリー ポート タイプに戻り、通常のポート状態遷移が行われます。その場合、当該ポートで BPDU フィルタリングはディセーブルとなり、スパニングツリーによって、同ポートでの BPDU の送信が再開されます。

BPDU フィルタリングは、インターフェイスごとに設定することもできます。BPDU フィルタリングを特定のポートに明示的に設定すると、そのポートはBPDUを送出しなくなり、受信したBPDUをすべてドロップします。特定のインターフェイスを設定することによって、個々のポート上のグローバルなBPDUフィルタリングの設定を実質的に上書きできます。このようにインターフェイスに対して実行されたBPDUフィルタリングは、そのインターフェイスがトランキングであるか否かに関係なく、インターフェイス全体に適用されます。

Caution BPDUフィルタリングをインターフェイスごとに設定するときは注意が必要です。ホストに接続されていないポートに BPDU フィルタリングを明示的に設定すると、ブリッジング ループに陥る可能性があります。というのは、そうしたポートは受信したBPDUをすべて無視して、フォワーディング ステートに移行するからです。

ポートがデフォルトで BPDU フィルタリングに設定されていなければ、エッジ設定によってBPDUフィルタリングが影響を受けることはありません。次の表に、すべてのBPDUフィルタリングの組み合わせを示します。

***Table 8: BPDU* フィルタリングの設定**

ポート単位の **BPDU** フィルタリングの設定	グローバルな **BPDU** フィルタリングの設定	**STP** エッジ ポート設定	**BPDU** フィルタリングの状態
デフォルト	有効	有効	イネーブルポートは10以上の BPDU を送信します。このポートは、BPDU を受信すると、スパニングツリー標準ポート状態に戻り、BPDU フィルタリングはディセーブルになります。
デフォルト	有効	無効	無効

ポート単位の BPDU フィルタリングの設定	グローバルな BPDU フィルタリングの設定	STP エッジ ポート設定	BPDU フィルタリングの状態
デフォルト	無効	Enabled/Disabled	無効
無効	Enabled/Disabled	Enabled/Disabled	無効
有効	Enabled/Disabled	Enabled/Disabled	有効 **Caution** BPDU は送信されませんが、受信した場合には、通常の STP の動作が開始されません。BPDU の使用に当たっては、十分注意してください。

ループ ガードの概要

ループ ガードは、次のような原因によってネットワークでループが発生するのを防ぎます。

- ネットワーク インターフェイスの誤動作
- CPU の過負荷
- BPDU の通常転送を妨害する要因

STP ループは、冗長なトポロジにおいてブロッキング ポートが誤ってフォワーディング ステートに移行すると発生します。こうした移行は通常、物理的に冗長なトポロジ内のポートの 1 つ（ブロッキング ポートとは限らない）が BPDU の受信を停止すると起こります。

ループ ガードは、デバイスがポイントツーポイント リンクによって接続されているスイッチド ネットワークでだけ役立ちます。ポイントツーポイント リンクでは、下位 BPDU を送信するか、リンクをダウンしない限り、代表ブリッジは消えることはありません。

Note ループ ガードは、ネットワークおよび標準のスパニングツリー ポート タイプ上だけでイネーブルにできます。

ループ ガードを使用して、ルート ポートまたは代替/バックアップ ループ ポートが BPDU を受信するかどうかを確認できます。BPDU を受信しないポートを検出すると、ループ ガードは、そのポートを不整合状態（ブロッキング ステート）に移行します。このポートは、再度

BPDUの受信を開始するまで、ブロッキング ステートのままです。不整合状態のポートはBPDUを送信しません。このようなポートが BPDU を再度受信すると、ループ ガードはそのループ不整合状態を解除し、STPによってそのポート状態が確定されます。こうしたリカバリは自動的に行われます。

ループ ガードは障害を分離し、STPは障害のあるリンクやブリッジを含まない安定したトポロジに収束できます。ループ ガードをディセーブルにすると、すべてのループ不整合ポートはリスニング ステートに移行します

ループ ガードはポート単位でイネーブルにできます。ループ ガードを特定のポートでイネーブルにすると、そのポートが属するすべてのアクティブ インスタンスまたは VLAN にループ ガードが自動的に適用されます。ループ ガードをディセーブルにすると、指定ポートでディセーブルになります。

ルート ガードの概要

特定のポートでルート ガードをイネーブルにすると、そのポートはルート ポートになることが禁じられます。受信した BPDU によって STP コンバージェンスが実行され、指定ポートがルート ポートになると、そのポートはルート不整合（ブロッキング）状態になります。このポートが優位 BPDU の送信を停止すると、ブロッキングが再度解除されます。次に、STP によって、フォワーディング ステートに移行します。リカバリは自動的に行われます。

特定のインターフェイスでルートガードをイネーブルにすると、そのインターフェイスが属するすべての VLAN にルート ガード機能が適用されます。

ルートガードを使用すると、ネットワーク内にルートブリッジを強制的に配置できます。ルート ガードは、ルート ガードがイネーブルにされたポートを指定ポートに選出します。通常、ルート ブリッジのポートはすべて指定ポートとなります（ただし、ルート ブリッジの 2 つ以上のポートが接続されている場合はその限りではありません）。ルート ブリッジは、ルートガードがイネーブルにされたポートで上位 BPDU を受信すると、そのポートをルート不整合 STP 状態に移行します。このように、ルートガードはルートブリッジの配置を適用します。

ルート ガードをグローバルには設定できません。

Note ルート ガードはすべてのスパニングツリー ポート タイプ（標準、エッジ、ネットワーク）でイネーブルにできます。

STP 拡張機能の設定

STP 拡張機能の設定における 注意事項

STP 拡張機能を設定する場合は、次の注意事項に従ってください。

- ホストに接続されたすべてのアクセス ポートとトランク ポートをエッジ ポートとして設定します。
- Bridge Assurance は、ポイントツーポイントのスパニングツリー ネットワーク ポート上だけで実行されます。この機能は、リンクの両端で設定する必要があります。
- ループ ガードは、スパニングツリー エッジ ポートでは動作しません。
- ポイントツーポイント リンクに接続していないポートでループ ガードをイネーブルにはできません。
- ルート ガードがイネーブルになっている場合、ループ ガードをイネーブルにはできません。
- 最大 MAC 学習制限を超えると、すべての着信パケットは MAC テーブルで学習されず、宛先 MAC に基づいて転送されます。

スパニングツリー ポート タイプのグローバルな設定

スパニングツリー ポート タイプの割り当ては、そのポートが接続されているデバイスのタイプによって次のように決まります。

- エッジ：エッジ ポートは、ホストに接続されるポートであり、アクセス ポートとトランク ポートのどちらかです。
- ネットワーク：ネットワーク ポートは、スイッチまたはブリッジだけに接続されます。
- 標準：標準ポートはエッジ ポートでもネットワーク ポートでもない、標準のスパニングツリー ポートです。標準ポートは、任意のタイプのデバイスに接続できます。

ポート タイプは、グローバル単位でもインターフェイス単位でも設定できます。デフォルトのスパニングツリー ポート タイプは「標準」です。

Before you begin

STP が設定されていること。

インターフェイスに接続されているデバイスのタイプに合わせてポートが正しく設定されていること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree port type edge default**
3. switch(config)# **spanning-tree port type network default**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree port type edge default**	すべてのインターフェイスをエッジポートとして設定します。このコマンドの使用は、すべてのポートがホスト/サーバに接続されていることが前提になります。エッジ ポートは、リンク アップすると、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。デフォルトのスパニングツリー ポート タイプは「標準」です。
ステップ 3	switch(config)# **spanning-tree port type network default**	すべてのインターフェイスをスパニングツリー ネットワーク ポートとして設定します。このコマンドの使用は、すべてのポートがスイッチまたはブリッジに接続されていることが前提になります。Bridge Assurance をイネーブルにすると、各ネットワーク ポート上で Bridge Assurance が自動的に実行されます。デフォルトのスパニングツリー ポート タイプは「標準」です。 **Note** ホストに接続されているインターフェイスをネットワーク ポートとして設定すると、それらのポートは自動的にブロッキング ステートに移行します。

Example

次に、ホストに接続されたアクセス ポートおよびトランク ポートをすべて、スパニングツリー エッジ ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type edge default
```

次に、スイッチまたはブリッジに接続されたポートをすべて、スパニングツリー ネットワーク ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type network default
```

指定インターフェイスでのスパニングツリー エッジ ポートの設定

指定インターフェイスにスパニングツリー エッジ ポートを設定できます。スパニングツリー エッジポートとして設定されたインターフェイスは、リンク アップ時に、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。

このコマンドには次の 4 つの状態があります。

- **spanning-tree port type edge**：このコマンドを実行すると、アクセス ポート上のエッジ動作が明示的にイネーブルにされます。
- **spanning-tree port type edge trunk**：このコマンドを実行すると、トランク ポート上のエッジ動作が明示的にイネーブルにされます。

Note **spanning-tree port type edge trunk** コマンドを入力すると、そのポートは、アクセス モードであってもエッジ ポートとして設定されます。

- **spanning-tree port type normal**：このコマンドを実行すると、ポートは標準スパニングツリー ポートとして明示的に設定されますが、フォワーディング ステートへの直接移行はイネーブルにされません。
- **no spanning-tree port type**：このコマンドを実行すると、**spanning-tree port type edge default** コマンドをグローバル コンフィギュレーション モードで定義した場合に、エッジ動作が暗黙にイネーブルにされます。エッジ ポートをグローバルに設定していない場合、 **no spanning-tree port type** コマンドは **spanning-tree port type disable** コマンドと同じです。

Before you begin

STP が設定されていること。

インターフェイスがホストに接続されていること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **spanning-tree port type edge**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** *type slot*/*port*	設定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。

	Command or Action	Purpose
ステップ 3	switch(config-if)# **spanning-tree port type edge**	指定したアクセス インターフェイスをスパニング エッジ ポートに設定します。エッジ ポートは、リンク アップすると、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。デフォルトのスパニングツリー ポート タイプは「標準」です。

Example

次に、アクセス インターフェイス Ethernet 1/4 をスパニングツリー エッジ ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree port type edge
```

BPDU ガードのグローバルなイネーブル化

BPDU ガードをデフォルトでグローバルにイネーブルにできます。BPDU ガードがグローバルにイネーブルにされると、システムは、BPDU を受信したエッジ ポートをシャット ダウンします。

Note すべてのエッジ ポートで BPDU ガードをイネーブルにすることを推奨します。

Before you begin

STP が設定されていること。

少なくとも一部のスパニングツリー エッジ ポートが設定済みであること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree port type edge bpduguard default**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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。

	Command or Action	Purpose
ステップ 2	switch(config)# **spanning-tree port type edge bpduguard default**	すべてのスパニングツリーエッジポートで、BPDU ガードを、デフォルトでイネーブルにします。デフォルトでは、グローバルな BPDU ガードはディセーブルです。

Example

次に、すべてのスパニングツリー エッジ ポートで BPDU ガードをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type edge bpduguard default
```

指定インターフェイスでの BPDU ガードのイネーブル化

指定インターフェイスで、BPDU ガードをイネーブルにできます。BPDU ガードがイネーブルにされたポートは、BPDU を受信すると、シャットダウンされます。

BPDU ガードは、指定インターフェイスで次のように設定にできます。

- **spanning-tree bpduguard enable**：インターフェイスで BPDU ガードを無条件でイネーブルにします。
- **spanning-tree bpduguard disable**：インターフェイスで BPDU ガードを無条件でディセーブルにします。
- **no spanning-tree bpduguard**：動作中のエッジ ポート インターフェイスに **spanning-tree port type edge bpduguard default** コマンドが設定されている場合、そのインターフェイスで BPDU ガードをイネーブルにします。

Before you begin

STP が設定されていること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **spanning-tree bpduguard** {**enable** | **disable**}
4. (Optional) switch(config-if)# **no spanning-tree bpduguard**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** *type slot/port*	設定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	switch(config-if)# **spanning-tree bpduguard** {**enable** | **disable**}	指定したスパニングツリー エッジ インターフェイスの BPDU ガードをイネーブルまたはディセーブルにします。デフォルトでは、BPDU ガードは、物理イーサネット インターフェイスではディセーブルです。
ステップ 4	(Optional) switch(config-if)# **no spanning-tree bpduguard**	インターフェイス上で BPDU ガードをディセーブルにします。 **Note** 動作中のエッジ ポート インターフェイスで、**spanning-tree port type edge bpduguard default** コマンドを入力した場合、そのインターフェイスで BPDU ガードをイネーブルにします。

Example

次に、エッジ ポート Ethernet 1/4 で BPDU ガードを明示的にイネーブルにする例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpduguard enable
switch(config-if)# no spanning-tree bpduguard
```

BPDU フィルタリングのグローバルなイネーブル化

スパニングツリーエッジポートで、BPDUフィルタリングをデフォルトでグローバルにイネーブルにできます。

BPDU フィルタリングがイネーブルにされたエッジ ポートは、BPDU を受信すると、エッジ ポートとしての動作ステータスを失い、通常の STP 状態遷移を再開します。ただし、このポートは、エッジ ポートとしての設定は保持したままです。

Caution このコマンドを使用するときには注意してください。誤って使用すると、ブリッジングループが発生するおそれがあります。

Note グローバルにイネーブルにされた BPDU フィルタリングは、動作中のエッジ ポートにだけ適用されます。ポートは数個の BPDU をリンクアップ時に送出してから、実際に、発信 BPDU のフィルタリングを開始します。エッジポートは、BPDUを受信すると、動作中のエッジポート ステータスを失い、BPDU フィルタリングはディセーブルになります。

Before you begin

STP が設定されていること。

少なくとも一部のスパニングツリー エッジ ポートが設定済みであること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree port type edge bpdufilter default**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree port type edge bpdufilter default**	すべてのスパニングツリーエッジポートで、BPDU フィルタリングを、デフォルトでイネーブルにします。デフォルトでは、グローバルな BPDU フィルタリングはディセーブルです。

Example

次に、すべての動作中のスパニングツリー エッジ ポートで BPDU フィルタリングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type edge bpdufilter default
```

指定インターフェイスでの BPDU フィルタリングのイネーブル化

指定インターフェイスにBPDUフィルタリングを適用できます。BPDUフィルタリングを特定のインターフェイス上でイネーブルにすると、そのインターフェイスはBPDUを送信しなくなり、受信した BPDU をすべてドロップするようになります。この BPDU フィルタリング機能は、トランキングインターフェイスであるかどうかに関係なく、すべてのインターフェイスに適用されます。

Caution 指定インターフェイスで **spanning-tree bpdufilter enable** コマンドを入力する場合は注意してください。ホストに接続されていないポートにBPDUフィルタリングを明示的に設定すると、ブリッジング ループに陥る可能性があります。というのは、そうしたポートは受信した BPDU をすべて無視して、フォワーディング ステートに移行するからです。

このコマンドを入力すると、指定インターフェイスのポート設定が上書きされます。

このコマンドには次の 3 つの状態があります。

- **spanning-tree bpdufilter enable**：インターフェイス上の BPDU フィルタリングを無条件にイネーブルにします。
- **spanning-tree bpdufilter disable**：インターフェイス上の BPDU フィルタリングを無条件にディセーブルにします。
- **no spanning-tree bpdufilter**：動作中のエッジ ポート インターフェイスに **spanning-tree port type edge bpdufilter default** コマンドが設定されている場合、そのインターフェイスでBPDUフィルタリングをイネーブルにします。

Note 特定のポートだけで BPDU フィルタリングをイネーブルにすると、そのポートでの BPDU の送受信が禁止されます。

Before you begin

STP が設定されていること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **spanning-tree bpdufilter** {**enable** | **disable**}
4. (Optional) switch(config-if)# **no spanning-tree bpdufilter**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** *type slot/port*	設定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	switch(config-if)# **spanning-tree bpdufilter** {**enable** | **disable**}	指定したスパニング ツリー エッジ インターフェイスの BPDU フィルタリングをイネーブルまたはディセーブルにします。デフォルトでは、BPDU フィルタリングはディセーブルです。
ステップ 4	(Optional) switch(config-if)# **no spanning-tree bpdufilter**	インターフェイス上で BPDU フィルタリングをディセーブルにします。 **Note** 動作中のエッジ ポート インターフェイスに **spanning-tree port type edge bpdufilter default** コマンドが設定されている場合、そのインターフェイスで BPDU フィルタリングをイネーブルにします。

Example

次に、スパニング ツリー エッジ ポート Ethernet 1/4 で BPDU フィルタリングを明示的にイネーブルにする例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpdufilter enable
```

ループ ガードのグローバルなイネーブル化

ループ ガードは、デフォルトの設定により、すべてのポイントツーポイント スパニング ツリーの標準およびネットワーク ポートで、グローバルにイネーブルにできます。ループ ガードは、エッジ ポートでは動作しません。

ループ ガードを使用すると、ブリッジ ネットワークのセキュリティを高めることができます。ループ ガードは、単方向リンクを引き起こす可能性のある障害が原因で、代替ポートまたはルート ポートが指定ポートになるのを防ぎます。

Note 指定インターフェイスでループ ガード コマンドを入力すると、グローバルなループ ガード コマンドが上書きされます。

Before you begin

STP が設定されていること。

スパニングツリー標準ポートが存在し、少なくとも一部のネットワーク ポートが設定済みであること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree loopguard default**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **spanning-tree loopguard default**	スパニングツリーのすべての標準およびネットワーク ポートで、ループ ガードを、デフォルトでイネーブルにします。デフォルトでは、グローバルなループ ガードはディセーブルです。

Example

次に、スパニングツリーのすべての標準およびネットワーク ポートでループ ガードをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# spanning-tree loopguard default
```

指定インターフェイスでのループガードまたはルートガードのイネーブル化

ループ ガードまたはルート ガードは、指定インターフェイスでイネーブルにできます。

特定のポートでルート ガードをイネーブルにすると、そのポートはルート ポートになることを禁止されます。ループ ガードは、単方向リンクを発生させる可能性のある障害が原因で代替ポートまたはルート ポートが指定ポートになるのを防ぎます。

特定のインターフェイスでループ ガードおよびルート ガードの両機能をイネーブルにすると、そのインターフェイスが属するすべての VLAN に両機能が適用されます。

Note 指定インターフェイスでループ ガード コマンドを入力すると、グローバルなループ ガード コマンドが上書きされます。

Before you begin

STP が設定されていること。

ループ ガードが、スパニングツリーの標準またはネットワーク ポート上で設定されていること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# **spanning-tree guard** {**loop** | **root** | **none**}

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** *type slot/port*	設定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	switch(config-if)# **spanning-tree guard** {**loop** | **root** | **none**}	ループ ガードまたはルート ガードを、指定インターフェイスでイネーブルまたはディセーブルにします。ルート ガードはデフォルトでディセーブル、ループ ガードも指定ポートでディセーブルになります。 **Note** ループ ガードは、スパニングツリーの標準およびネットワーク インターフェイスだけで動作します。

Example

次に、Ethernet ポート 1/4 で、ルート ガードをイネーブルにする例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree guard root
```

STP 拡張機能の設定の確認

STP 拡張機能の設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
show running-config spanning-tree [**all**]	スイッチ上でスパニングツリーの最新ステータスを表示します。
show spanning-tree [*options*]	最新のスパニングツリー設定について、指定した詳細情報を表示します。

ループ検出エラーメッセージのトラブルシューティング

このセクションでは、Cisco Nexus 3600 プラットフォーム スイッチのログに FWM-2-STM_LOOP_DETECT のエラー メッセージがあった場合の解決方法について説明します。

Cisco Nexus 3600 プラットフォーム スイッチが次のメッセージを表示した場合、スイッチがこれら 2 つのインターフェイスで同じ送信元の MAC アドレスを持つフレームを受信し、これらのインターフェイスで同じ MAC アドレスを高速で認識することを示しています。スイッチはこの条件をループとして検出します。スイッチは、コントロール プレーンを保護するために MAC アドレス ラーニングを無効にします。これは、ループが 1 つの VLAN だけに発生した場合でも、すべての VLAN で実行されます。

```
2016 Apr 11 18:00:18 N3k-4-3229 %FWM-2-STM_LOOP_DETECT: Loops detected in the network
for mac 0000.0602.0602 among ports Eth1/48
and Eth1/50/3 on vlan 4 - Disabling dynamic learning notifications for a period between
 120 and 240 seconds on vlan 4
```

エラー メッセージの考えられる原因は次のとおりです。

- 不正なスパニング ツリー プロトコル（STP）ポート ステート コンバージェンスのため、MAC アドレスが移動する。
- STP ステートがコンバージされて正しい状態にあるときに、データの送信元がすべてのスイッチを物理的に横断していることが原因で、MAC アドレスが移動します。

ループの検出

フォワーディング マネージャ（FWM）には、移動した MAC アドレスをカウントし、MAC アドレスの移動回数に基づいてその重み付けをする機能があります。これにより、移動した MAC アドレスの合計（すべての VLAN、MAC、インターフェイスでのスイッチ全体）が算出され、%FWM-2-STM_LOOP_DETECT 条件が宣言され、ループ状態の FWM を保護するためにラーニングが無効になります。

（注） MAC ラーニングは、システムごとではなく、VLAN ごとにディセーブルになります。

MAC 移動通知のロジックに注意する必要があります。MAC 移動の MAC アドレス テーブルの通知が有効の場合、MAC 移動が通知される可能性があります。これによりコンソールの通知ログが追加されますが、アクションは実行されません。移動が宣言されるのは、10秒間の時系列スキャン期間内に VLAN の任意の 2 つのポート間で特定の MAC アドレスが 3 回行き来（移動）した場合です。

（注） MAC アドレスは、2 つのポートのそれぞれで 50 回検出される必要があります。

スイッチの MAC アドレス通知を有効にすると、どの MAC アドレスが移動するかを見つけることができます。

手順の概要

1. switch# **conf t**
2. switch# **mac address-table notification mac-move**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **conf t**	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	switch# **mac address-table notification mac-move**	MAC 移動通知をイネーブルにします。

syslog エラーメッセージの生成

MAC 移動通知に関する syslog メッセージを生成するために、MAC 移動通知を有効にするだけでは、必ずしも十分ではありません。syslog メッセージが確実に生成されるようにするには、前のコマンドと一緒に **mac address-table notification mac-move** というコマンドを入力します。

手順の概要

1. **conf t**
2. **logging level spanning-tree 6**
3. **logging level fwm 6**
4. **logging monitor 6**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**conf t**	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	**logging level spanning-tree 6**	レベル 6 から最も重大度の高いイベントまでのすべてのスパニング ツリー イベントのロギングをイネーブルにします。
ステップ 3	**logging level fwm 6**	レベル 6 から最も重大度の高いイベントまでのすべての FWM イベントのロギングをイネーブルにします。
ステップ 4	**logging monitor 6**	デバイスが重大度 6 以上のメッセージをモニタに記録できるようにします。

これらのコマンドを追加すると、MAC アドレス移動がある場合に FWM 検出が syslog に必ず表示されます。VLAN 全体でスイッチの STP ポート ステートを検証するには、次のコマンドを入力します。

```
switch# show spanning-tree
switch# show spanning-tree vlan <id>
switch# show spanning-tree internal interaction
```

例

MAC アドレスが移動したかどうかを確認するには、次のコマンドを入力します。

```
# show mac address-table notification mac-move
 MAC Move Notify Triggers: 1206
 Number of MAC Addresses added: 944088
 Number of MAC Addresses moved: 265
 Number of MAC Addresses removed: 943920
```

どの MAC アドレスが移動したかを表示するには、MAC アドレスの移動も記録される最小ロギング レベルであるレベル 6 が必要です。

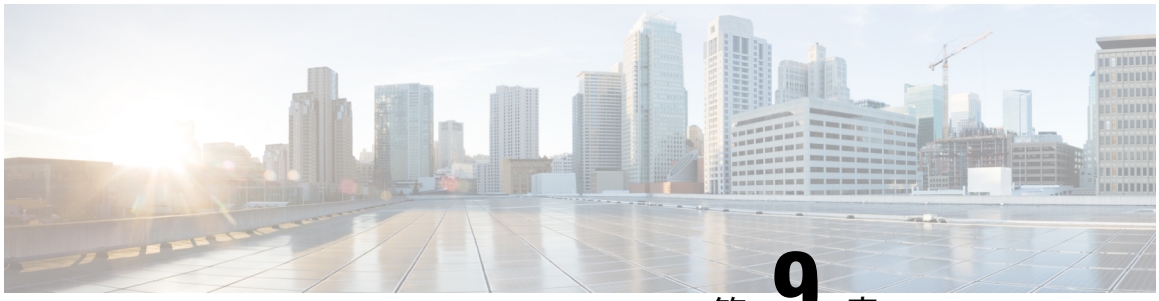
```
2016 Jun 12 16:05:31.564 switch %FWM-6-MAC_MOVE_NOTIFICATION:
Host 0000.0000.fe00 in vlan 85 is flapping between
port Eth104/1/8 and port Eth104/1/9
```

次のタスク

正しい STP コンバージェンスを確認し、関係図内のすべてのスイッチで STP ポートステートをチェックします。競合がないこと、および不適切なポート ステートがないことを確認します。

物理的に移動しているデータ フレームの送信元を特定したら、高速での連続的な移動を停止するために送信元を制御します。

デフォルトでは、動的なラーニングは180秒後に再度有効になります。その時点で、すべてのSTP競合または不整合は解決されている必要があります。そうでない場合、動的なラーニングは再度、無効になります。



第 9 章

LLDP の設定

グローバル LLDP コマンドの設定

グローバルな LLDP 設定値を設定できます。これらの設定値には、ピアから受信した LLDP 情報を廃棄するまでの時間、任意のインターフェイスで LLDP 初期化を実行するまで待機する時間、LLDP パケットを送信するレート、ポート記述、システム機能、システム記述、およびシステム名が含まれます。

LLDP は一連の属性をサポートし、これらを使用してネイバーデバイスを検出します。属性には、Type、Length、および Value の説明が含まれていて、これらを TLV と呼びます。LLDP をサポートするデバイスは、ネイバーとの情報の送受信に TLV を使用できます。設定情報、デバイスの機能、デバイス ID などの詳細情報は、このプロトコルを使用してアドバタイズできます。

スイッチは、次の必要な管理 LLDP TLV をサポートします。

- Data Center Ethernet Parameter Exchange（DCBXP）TLV
- 管理アドレス TLV
- ポート記述 TLV
- ポート VLAN ID TLV（IEEE 802.1 に固有の TLV）
- システム機能 TLV

- システム記述 TLV
- システム名 TLV

Data Center Bridging Exchange Protocol（DCBXP）は、LLDP を拡張したプロトコルです。このプロトコルは、ピア間のノードパラメータのアナウンス、交換、およびネゴシエートに使用されます。DCBXP パラメータは、特定の DCBXP TLV にパッケージ化されます。この TLV は、受信した LLDP パケットに応答するように設計されています。

LLDP をイネーブルにすると、DCBXP がデフォルトでイネーブルになります。LLDP が有効な場合、DCBXP は **[no] lldp tlv-select dcbxp** コマンドを使用して有効または無効にできます。LLDP の送信または受信がディセーブルになっているポートでは、DCBXP はディセーブルです。

LLDP の設定

Before you begin

スイッチでリンク層検出プロトコル（LLDP）機能がイネーブルになっていることを確認します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **lldp** {**holdtime** *seconds* | **reinit** *seconds* | **timer** *seconds* | **tlv-select** {**dcbxp** | **management-address** [**v4** | **v6**] | **port-description** | **port-vlan** | **system-capabilities** | **system-description** | **system-name**}}
3. switch(config)# **no lldp** {**holdtime** | **reinit** | **timer**}
4. （任意）switch# **show lldp**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **lldp** {**holdtime** *seconds* | **reinit** *seconds* | **timer** *seconds* | **tlv-select** {**dcbxp** | **management-address** [**v4** | **v6**] | **port-description** | **port-vlan** | **system-capabilities** | **system-description** | **system-name**}}	LLDP オプションを設定します。 **holdtime** オプションを使用して、デバイスが受信した LLDP 情報を廃棄するまでの保存時間を設定します（10 ～ 255 秒）。デフォルト値は 120 秒です。 **reinit** オプションを使用して、任意のインターフェイスで LLDP 初期化を実行するまでの待機時間を設定します（1 ～ 10 秒）。デフォルト値は 2 秒です。

	Command or Action	Purpose
		timer オプションを使用して、LLDP パケットを送信するレートを設定します（5 ～ 254 秒）。デフォルト値は 30 秒です。 **tlv-select** オプションを使用して、Type Length Value（TLV）を指定します。デフォルトでは、すべての TLV の送受信がイネーブルです。 **dcbxp** オプションを使用して、Data Center Ethernet Parameter Exchange（DCBXP）TLV メッセージを指定します。 **management-address** オプションを使用して、管理アドレス TLV メッセージを指定します。 **management-address v4** オプションを使用して、IPv4 管理アドレス TLV メッセージを指定します。 **management-address v6** オプションを使用して、IPv6 管理アドレス TLV メッセージを指定します。 **port-description** オプションを使用して、ポート記述 TLV メッセージを指定します。 **port-vlan** オプションを使用して、ポート VLAN ID TLV メッセージを指定します。 **system-capabilities** オプションを使用して、システム機能 TLV メッセージを指定します。 **system-description** オプションを使用して、システム記述 TLV メッセージを指定します。 **system-name** オプションを使用して、システム名 TLV メッセージを指定します。
ステップ 3	switch(config)# **no lldp** {**holdtime** | **reinit** | **timer**}	LLDP 値をデフォルトにリセットします。
ステップ 4	（任意）switch# **show lldp**	LLDP の設定を表示します。

Example

次に、グローバルな LLDP ホールドタイムを 200 秒に設定する例を示します。

```
switch# configure terminal
switch(config)# lldp holdtime 200
switch(config)#
```

次に、LLDP をイネーブルにして管理アドレス TLV を送受信する例を示します。

```
switch# configure terminal
switch(config)# lldp tlv-select management-address
switch(config)#
```

次に、LLDP をイネーブルにして IPv4 管理アドレス TLV を送受信する例を示します。

```
switch# configure terminal
switch(config)# lldp tlv-select management-address v4
switch(config)#
```

次に、LLDP をイネーブルにして IPv6 管理アドレス TLV を送受信する例を示します。

```
switch# configure terminal
switch(config)# lldp tlv-select management-address v6
switch(config)#
```

LLDP 管理 TLV IP アドレスについて

LLDP 管理 TLV を使用して、ネットワーク デバイスのシステム情報をネイバーに伝達することができます。LLDP 管理 TLV には、リモート マネージャがローカル デバイスに関する情報を取得するために使用できる管理アドレスが含まれています。現在は、デフォルトで、管理ポート mgmt0 の IPv4 および IPv6 アドレスが管理 TLV で送信されます。

Cisco NX-OS Release 7.0(3)F3(1) で、IPv4 と IPv6 の 2 つの TLV のサポートが導入されました。

LLDP 管理 TLV で送信する管理 IPv4 または IPv6 アドレスは明示的に指定できます。この IP アドレスは次のいずれかにすることができます。

- ポートの IPv4 または IPv6 アドレス
- VLAN（SVI）の IPv4 または IPv6 アドレス

IPv4 の場合、LLDP 管理 TLV で送信する管理アドレスを選択するときに次のルールが適用されます。

- LLDP 管理 v4 TLV が送信用に設定され、ポートの LLDP 管理 IPv4 アドレスが設定されている場合は、そのポート上で設定された LLDP 管理 IPv4 アドレスが、送信する LLDP プロトコル データ ユニット（PDU）の管理 TLV で使用されます。
- LLDP 管理 v4 TLV が送信用に設定され、LLDP VLAN が設定されている場合:
  - VLAN ID が指定され、その SVI が操作可能な場合は、VLAN ID の SVI IPv4 アドレスが、送信する LLDP PDU の管理 v4 TLV で使用されます。
  - ネイティブ VLAN が利用可能で、その SVI が操作可能な場合は、ネイティブ VLAN の SVI IPv4 アドレスが、送信する LLDP PDU の管理 v4 TLV で使用されます。
- LLDP 管理 v4 TLV が送信用に設定され、LLDP 管理 IPv4 アドレスと LLDP VLAN の両方が設定されていない場合は、管理ポート mgmt0 の IPv4 アドレスが、送信する LLDP PDU の管理 v4 TLV で使用されます。

- LLDP 管理 v4 TLV に IPv4 アドレスが設定されていない場合、インターフェイス ポートの MAC アドレスは 1 つの TLV で送信されます。
- LLDP 管理 v4 TLV が送信用に設定されていない場合は、管理 TLV IPv4 アドレスは送信されません。

IPv6 の場合、LLDP 管理 TLV で送信する管理アドレスを選択するときに次のルールが適用されます。

- LLDP 管理 v6 TLV が送信用に設定され、ポートの LLDP 管理 IPv6 アドレスが設定されている場合は、そのポート上で設定された LLDP 管理 IPv6 が、送信する LLDP プロトコル データ ユニット（PDU）の管理 TLV で使用されます。
- LLDP 管理 v6 TLV が送信用に設定され、LLDP VLAN が設定されている場合:
  - VLAN ID が指定され、その SVI が操作可能な場合は、VLAN ID の SVI IPv6 アドレスが、送信する LLDP PDU の管理 v6 TLV で使用されます。
  - ネイティブ VLAN が利用可能で、その SVI が操作可能な場合は、ネイティブ VLAN の SVI IPv6 アドレスが、送信する LLDP PDU の管理 v6 TLV で使用されます。
- LLDP 管理 v6 TLV が送信用に設定され、LLDP 管理 IPv6 アドレスと LLDP VLAN の両方が設定されていない場合は、管理ポート mgmt0 の IPv6 アドレスが、送信する LLDP PDU の管理 v6 TLV で使用されます。
- LLDP 管理 v6 TLVに IPv6 アドレスが設定されていない場合、インターフェイス ポートの MAC アドレスは 1 つの TLV で送信されます。
- LLDP 管理 v6 TLV が送信用に設定されていない場合は、管理 TLV IPv6 アドレスは送信されません。

次に、設定された IPv4 または IPv6 アドレスに基づいて実行される TLV 選択プロセスを示します。

- IP アドレス未設定：インターフェイス ポートの MAC アドレスは 1 つの TLV で送信されます。
- IPv4 アドレスのみ設定：2 つの TLV が送信されます。1 つは IPv4 アドレスで、もう 1 つはインターフェイスポートの MAC アドレスです。このプロセスは、IPv4 の LLDP 管理 TLV で送信する管理アドレスを選択するときに適用される次のルールに従います。
- IPv6 アドレスのみ設定：IPv6 アドレスは 1 つの TLV で送信されます。このプロセスは、IPv6 の LLDP 管理 TLV で送信する管理アドレスを選択するときに適用される次のルールに従います。
- IPv4 と IPv6 の両方のアドレスが設定されている：2 つの TLV が送信されます。1 つは IPv4 アドレス、もう 1 つは IPv6 アドレスを持ちます。このプロセスは、IPv4 および IPv6 の LLDP 管理 TLV で送信する管理アドレスを選択するときに適用される次のルールに従います。

(注) 両方の TLV が設定され、IPv4 アドレスが設定されていない場合、v4 TLV ではインターフェイス ポートの MAC アドレスは送信されません。1 つの TLV のみが送信されます。

インターフェイス ポートの MAC アドレスを持つ TLV が 1 つだけ送信される場合、このアドレスはピアの IPv4 アドレスと IPv6 アドレスの両方の列に表示されます。

インターフェイスでの LLDP 管理 TLV IP アドレスの設定

始める前に

LLDP 管理 TLV オプションが設定されていることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *slot/port*
3. switch(config-if)# [**no**] **lldp tlv-set** { **management-address** *ip-address* [**ipv6**] | **vlan** [*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	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	switch(config)# **interface ethernet** *slot/port*	設定するインターフェイスを指定します。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	switch(config-if)# [**no**] **lldp tlv-set** { **management-address** *ip-address* [**ipv6**] | **vlan** [*vlan-id*] }	管理 IPv4 アドレス、IPv6 アドレス、または VLAN ID を指定します。 **lldp tlv-set vlan** コマンドは、レイヤ 2 ポートでのみ実行する必要があります。レイヤ 3 ポートでこのコマンドを実行すると、その設定は LLDP 管理 TLV の管理 IPv4 または IPv6 アドレスの特定中に無視されます。ただし、設定は削除されません。ポート レイヤ モードが再度レイヤ 2 に変更されると、その設定は再度考慮されるようになります。

例

次に、管理 TLV で管理 IPv4 アドレスを指定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/8
switch(config-if)# lldp tlv-set management-address 1.1.1.20
```

次に、管理 TLV で管理 IPv6 アドレスを指定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/8
switch(config-if)# lldp tlv-set management-address 0dc3:0dc3:0000:0000:0218:baff:fed8:239d
 ipv6
```

次に、管理 TLV で VLAN ID を指定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/8
switch(config-if)# lldp tlv-set vlan 10
```

インターフェイス LLDP の設定

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# [**no**] **lldp** {**receive** | **transmit**}
4. (Optional) switch# **show lldp** {**interface** | **neighbors** [**detail** | **interface** | **system-detail**] | **timers** | **traffic**}

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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	switch(config)# **interface** *type slot/port*	変更するインターフェイスを選択します。
ステップ 3	switch(config-if)# [**no**] **lldp** {**receive**	**transmit**}	選択したインターフェイスを受信または送信に設定します。 このコマンドの **no** 形式を使用すると、LLDP の送信または受信をディセーブルにします。
ステップ 4	(Optional) switch# **show lldp** {**interface**	**neighbors** [**detail**	**interface**	**system-detail**]	**timers**	**traffic**}	LLDP の設定を表示します。

Example

次に、LLDP パケットを送信するようインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# lldp transmit
```

次に、LLDP をディセーブルにするようインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
```

次に、LLDP インターフェイス情報を表示する例を示します。

```
switch# show lldp interface ethernet 1/2
tx_enabled: TRUE
rx_enabled: TRUE
dcbx_enabled: TRUE
Port MAC address:    00:0d:ec:a3:5f:48
Remote Peers Information
No remote peers exist
```

次に、LLDP ネイバーの情報を表示する例を示します。

```
switch# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID             Local Intf      Hold-time  Capability  Port ID
BLR-VPC2-QS8          Eth1/25         120        BR          Ethernet1/25
BLR-VPC2-QS8          Eth1/26         120        BR          Ethernet1/26
BLR-VPC2-QS8          Eth1/27         120        BR          Ethernet1/27
BLR-VPC2-QS8          Eth1/28         120        BR          Ethernet1/28
Total entries displayed: 4
switch#
```

次に、LLDP ネイバーに関するインターフェイスの詳細を表示する例を示します。

```
switch(config-if)# show lldp neighbor interface ethernet 1/4 detail
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID            Local Intf      Hold-time  Capability  Port ID

Chassis id: 0022.bddf.548b
Port id: Ethernet1/4
Local Port id: Eth1/4
Port Description: Ethernet1/4
System Name: abc.mycompany.com
System Description: Cisco Nexus Operating System (NX-OS) Software 7.0(3)F3(1)
TAC support: http://www.cisco.com/tac
```

```
Copyright (c) 2002-2014, Cisco Systems, Inc. All rights reserved.
Time remaining: 108 seconds
System Capabilities: B, R
Enabled Capabilities: B, R
Management Address: 10.105.215.235
Management Address IPV6: 0022.bddf.548b
Vlan ID: 1

Total entries displayed: 1
switch(config-if)#
```

次に、LLDP ネイバーに関するシステムの詳細を表示する例を示します。

```
switch# sh lldp neighbors system-detail
Capability codes:
 (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
 (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID Local Intf Chassis ID PortID Hold-time Capability

switch-2  Eth1/7  0005.73b7.37ce Eth1/7  120 B
switch-3  Eth/9   0005.73b7.37d0 Eth1/9  120 B
switch-4  Eth1/10 0005.73b7.37d1 Eth1/10 120 B
Total entries displayed: 3
```

次に、LLDP タイマー情報を表示する例を示します。

```
switch# show lldp timers

LLDP Timers

holdtime 120 seconds

reinit 2 seconds

msg_tx_interval 30 seconds
```

次に、LLDP カウンタに関する情報を表示する例を示します。

```
switch# show lldp traffic

LLDP traffic statistics:

    Total frames out: 8464

    Total Entries aged: 6

    Total frames in: 6342

    Total frames received in error: 2

    Total frames discarded: 2

    Total TLVs unrecognized: 0
```

LLDP マルチネイバー サポート

多くの場合、ネットワーク デバイスは複数の LLDP パケットを送信しますが、そのうちの 1 つは実際のホストからのものです。Cisco Nexus スイッチがデバイスと通信しているが、インターフェイスごとに 1 つの LLDP ネイバーしか管理できない場合は、実際に必要なホストとのネイバーになることが失敗する可能性があります。これを最小限に抑えるために、Cisco Nexus ス

イッチ インターフェイスは複数の LLDP ネイバーをサポートできるため、正しいデバイスで LLDP ネイバーになる可能性が高くなります。

同じインターフェイスで複数の LLDP ネイバーをサポートするには、LLDP マルチネイバー サポートをグローバルに設定する必要があります。

（注） LLDP マルチネイバー サポートを設定する前に、DCBX をグローバルに無効にする必要があります。これを行わないと、エラー メッセージが表示されます。

インターフェイスでの LLDP マルチネイバー サポートのイネーブル化またはディセーブル化

始める前に

インターフェイスで LLDP マルチネイバー サポートを有効にする前に、次の点を考慮してください。

- デバイスで LLDP をグローバルにイネーブルにしていることを確認します（グローバル設定コマンド **feature lldp**）。

  （注） LLDP をグローバルに有効にすると、LLDP は、デフォルトで、サポートされているすべてのインターフェイスで有効になります。

- 1 つのインターフェイスで最大 3 つのネイバーがサポートされます。
- LLDP マルチネイバーは、FEX インターフェイスではサポートされません。

手順の概要

1. **configure terminal**
2. **no lldp tlv-select dcbxp**
3. [**no**] **lldp multi-neighbor**
4. **interface** *port* / *slot*
5. （任意） [**no**] **lldp transmit**
6. （任意） [**no**] **lldp receive**
7. （任意） **show lldp interface** *port* / *slot*
8. （任意） **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`
	`switch(config)#`
		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	必須: **no lldp tlv-select dcbxp**
	例：
	`switch(config)# no lldp tlv-select dcbxp`
	`switch(config)#`
		DCBXP TLV をグローバルに無効にします。
		（注） LLDP マルチネイバー サポートが設定された後にエラーメッセージが表示されないようにするには、このコマンドを入力する必要があります。

ステップ 3	必須: [**no**] **lldp multi-neighbor**
	例：
	`switch(config)# lldp multi-neighbor`
	`switch(config)#`
		すべてのインターフェイスのLLDPマルチネイバー サポートをグローバルに有効または無効にします。

ステップ 4	**interface** *port* / *slot*
	例：
	`switch(config)# interface 1/1`
	`switch(config-if)#`
		LLDP をイネーブルに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 5	（任意） [**no**] **lldp transmit** 例： `switch(config-if)# lldp transmit`	インターフェイスでの LLDP パケットの送信をディセーブル（またはイネーブル）にします。 （注） このインターフェイスでの LLDP パケットの送信は、グローバル **feature lldp** コマンドを使用してイネーブルにされました。このオプションは、この特定のインターフェイスの機能を無効にします。
ステップ 6	（任意） [**no**] **lldp receive** 例： `switch(config-if)# lldp receive`	インターフェイスでの LLDP パケットの受信をディセーブル（またはイネーブル）にします。 （注） このインターフェイスでの LLDP パケットの受信は、グローバル **feature lldp** コマンドを使用してイネーブルになりました。このオプションは、この特定のインターフェイスの機能を無効にします。
ステップ 7	（任意） **show lldp interface** *port* / *slot* 例： `switch(config-if)# show lldp interface 1/1`	インターフェイス上で LLDP の設定を表示します。

	コマンドまたはアクション	目的
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

ポート チャネル インターフェイスでの LLDP サポートの有効化または無効化

始める前に

ポート チャネルで LLDP サポートを有効にする前に、次の点を考慮してください。

- デバイスでLLDPをグローバルにイネーブルにしていることを確認します（グローバル設定コマンド **feature lldp**）。

> **注** LLDPをグローバルに有効にすると、LLDPは、デフォルトで、サポートされているすべてのインターフェイスで有効になります。

- ポート チャネルに **lldp transmit** および **lldp receive** コンフィギュレーション コマンドを適用しても、ポート チャネルのメンバーの設定には影響しません。
- LLDP ネイバーは、LLDP 送受信がポート チャネルの両側で設定されている場合にのみ、ポート チャネル間で形成されます。
- LLDP の送受信コマンドは、MCT、VPC、FEX ファブリック、FEX ポート チャネル、およびポート チャネル サブ インターフェイスでは機能しません。

> **注** LLDP ポート チャネル機能をグローバルに有効にすると、LLDP 設定はこれらのポート タイプのいずれにも適用されません。ポート チャネルから設定が削除された場合、またはポート タイプ機能がグローバルに無効になった場合は、**lldp port-channel** コマンドを使用して新しくサポートされたポート チャネルで有効にすることはできません。コマンドはすでに発行されています。問題のポート チャネルでLLDP ポート チャネルを有効にするには、**lldp transmit** および **lldp receive** を各ポート チャネルに対して設定します（次の手順のステップ 4、5、および 6 を参照）。

手順の概要

1. **configure terminal**
2. **no lldp tlv-select dcbxp**
3. [**no**] **lldp port-channel**
4. **interface port-channel** [*port-channel-number* | *port-channel-range*]
5. （任意） [**no**] **lldp transmit**
6. （任意） [**no**] **lldp receive**
7. （任意） **show lldp interface port-channel***port-channel-number*
8. （任意） **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`
	`switch(config)#`
		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	必須: **no lldp tlv-select dcbxp**
	例：
	`switch(config)# no lldp tlv-select dcbxp`
	`switch(config)#`
		DCBXP TLV をグローバルに無効にします。ポート チャネルで LLDP を設定する前に、このコマンドを入力する必要があります。

ステップ 3	必須: [**no**] **lldp port-channel**
	例：
	`switch(config)# lldp port-channel`
	`switch(config)#`
		すべてのポート チャネルの LLDP 送受信をグローバルに有効または無効にします。

ステップ 4	**interface port-channel** [*port-channel-number*	*port-channel-range*]
		例：
		`switch(config)# interface port-channel 3`
		`switch(config-if)#`
		例：
		複数のポート チャネルで LLDP を設定する場合は、ポート チャネル番号の範囲を入力します。
		`switch(config)# interface port-channel 1-3`
		`switch(config-if-range)#`
			LLDP を有効にするインターフェイス ポート チャネルを指定し、インターフェイス設定モードを開始します。
			LLDP を有効にするインターフェイス ポートチャネル範囲を指定し、インターフェイス範囲設定モードを開始します。

ステップ 5	（任意） [**no**] **lldp transmit** 例： `switch(config-if)# lldp transmit`	ポート チャネルまたはポート チャネルの範囲で LLDP パケットの送信を無効（または有効）にします。

	コマンドまたはアクション	目的
		（注） このポート チャネルでの LLDP パケットの送信は、ステップ 3 の **lldp port-channel** コマンドを使用して有効になりました。このオプションは、この特定のポート チャネルの機能を無効にします。
ステップ 6	（任意） **[no] lldp receive** 例： `switch(config-if)# lldp receive`	ポート チャネルまたはポート チャネルの範囲での LLDP パケットの受信を無効（または有効）にします。 （注） このポート チャネルでの LLDP パケットの受信は、ステップ 3 の **lldp port-channel** コマンドを使用して有効になりました。このオプションは、この特定のポート チャネルの機能を無効にします。
ステップ 7	（任意） **show lldp interface port-channel***port-channel-number* 例： `switch(config-if)# show lldp interface port-channel 3`	ポートチャネル上の LLDP 設定を表示します。
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

LLDP の MIB

MIB	リンク
LLDP-MIB	ftp://ftp.cisco.com/pub/mibs/supportlists/nexus3000/Nexus3000MIBSupportList.html

第 10 章

トラフィック ストーム制御の設定

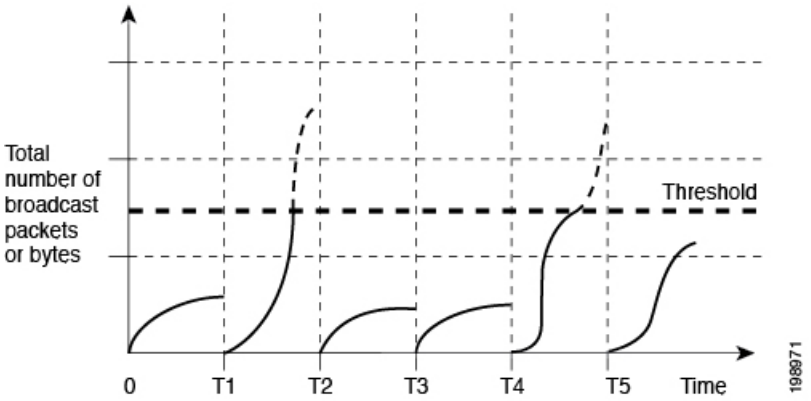
トラフィック ストーム制御について

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御機能を使用すると、物理インターフェイス上におけるブロードキャスト、マルチキャスト、または未知のトラフィック ストームによって、イーサネット インターフェイス経由の通信が妨害されるのを防ぐことができます。

トラフィック ストーム制御（トラフィック抑制ともいう）では、ブロードキャスト、マルチキャスト、ユニキャストの着信トラフィックのレベルを 10 ミリ秒間隔で監視します。この間、トラフィック レベル（ポートの使用可能合計帯域幅に対するパーセンテージ）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

次の図に、指定したタイム インターバル期間中におけるイーサネット インターフェイス上のブロードキャスト トラフィック パターンを示します。この例では、トラフィック ストーム制御が T1 と T2 時間の間、および T4 と T5 時間の間で発生します。これらの間隔中に、ブロードキャスト トラフィックの量が設定済みのしきい値を超過したためです。

Figure 15: ブロードキャストの抑制



トラフィック ストーム制御のしきい値とタイム インターバルを使用することで、トラフィック ストーム制御アルゴリズムは、さまざまなレベルのパケット粒度で機能します。たとえば、しきい値が高いほど、より多くのパケットを通過させることができます。

トラフィック ストーム制御は、ハードウェアに実装されています。トラフィック ストーム制御回路は、イーサネットインターフェイスから来て通過するパケットを監視します。また、パケットの宛先アドレスに設定されている Individual/Group ビットを使用して、パケットがユニキャストかブロードキャストかを判断し、10 マイクロ秒以内の間隔でパケット数を追跡します。パケット数がしきい値に到達したら、後続のパケットをすべて破棄します。

トラフィック ストーム制御では、トラフィック量の計測に帯域幅方式を使用します。制御対象のトラフィックが使用できる、利用可能な合計帯域幅に対するパーセンテージを設定します。パケットは一定の間隔で到着するわけではないので、10マイクロ秒の間隔によって、トラフィック ストーム制御の動作が影響を受けることがあります。

次に、トラフィック ストーム制御の動作がどのような影響を受けるかを示します。

- ブロードキャスト トラフィック ストーム制御をイネーブルにした場合、ブロードキャスト トラフィックが 10 マイクロ秒のインターバル以内にしきい値レベルを超えると、トラフィック ストーム制御により、そのインターバルが終了するまですべての超過ブロードキャスト トラフィックがドロップされます。
- マルチキャスト トラフィック ストーム制御をイネーブルにした場合、マルチキャスト トラフィックが10マイクロ秒のインターバル以内にしきい値レベルを超えると、トラフィック ストーム制御により、そのインターバルが終了するまですべての超過マルチキャスト トラフィックがドロップされます。
- ブロードキャストおよびマルチキャスト トラフィック ストーム制御をイネーブルにした場合、ブロードキャスト トラフィックが 10 マイクロ秒のインターバル以内にしきい値レベルを超えると、トラフィック ストーム制御により、そのインターバルが終了するまですべての超過ブロードキャスト トラフィックがドロップされます。
- ブロードキャストおよびマルチキャスト トラフィック ストーム制御をイネーブルにした場合、マルチキャスト トラフィックが 10 マイクロ秒のインターバル以内にしきい値レベ

ルを超えると、トラフィック ストーム制御により、そのインターバルが終了するまですべての超過マルチキャスト トラフィックがドロップされます。

デフォルトでは、Cisco NX-OS は、トラフィックが設定済みレベルを超えても是正のための処理を行いません。

トラフィック ストーム制御の注意事項と制約事項

トラフィック ストーム制御レベルを設定する場合は、次の注意事項と制限事項に留意してください。

- ポート チャネル インターフェイス上にトラフィック ストーム制御を設定できます。
- レベルをインターフェイスの帯域幅全体に対する割合として指定します。
  - レベルの指定範囲は 0 ～ 100 です。
  - 任意で、レベルの小数部を 0 ～ 99 の範囲で指定できます。
  - 100% は、トラフィック ストーム制御がないことを意味します。
  - 0.0% は、すべてのトラフィックを抑制します。
- ストーム制御ドロップが個別にカウントされることを防ぐ、ローカル リンクおよびハードウェアの制約事項があります。代わりに、ストーム制御ドロップは discards カウンタの他のドロップとカウントされます。
- ハードウェアの制限およびサイズの異なるパケットがカウントされる方式のため、レベルの割合は概数になります。着信トラフィックを構成するフレームのサイズに応じて、実際に適用されるパーセンテージ レベルと設定したパーセンテージ レベルの間には、数パーセントの誤差がある可能性があります。
- ストーム制御は、未知のユニキャスト、未知のマルチキャスト、ブロードキャスト トラフィックなどの入力トラフィック専用です。
- リンクレベル制御プロトコル（LACP、LLDPなど）は、トラフィックストームの場合には影響を受けません。ストーム制御は、データプレーントラフィックにのみ適用されます。
- バーストサイズの値は次のとおりです。
  - 10G ポートの場合、48.68 M バイト/ 390 M ビット
  - 1G ポートの場合、25 Mバイト/ 200 Mビット
- トラフィック ストーム制御機能は、Cisco Nexusリリース9.2(1) を実行する、N3K-C36180YC-R および N3K-C3636C-R ラインカードを搭載した Cisco Nexus 3600 プラットフォーム スイッチではサポートされません。
- Cisco Nexusリリース9.2(4) 以降、トラフィック ストーム制御機能は、N3K-C36180YC-R および N9K-X9636C-RX ライン カードを搭載した Cisco Nexus 3600 プラットフォーム スイッ

チでサポートされます。インターフェイスがブロードキャスト トラフィックでフラッディングされた場合、トラフィック ストーム制御カウンタは増加しません。

- Cisco Nexus リリース 9.3(2) 以降、トラフィック ストーム制御機能は、N3K-C36180YC-R および N9K-X9636C-RX ライン カードを搭載した Cisco Nexus 3600 プラットフォーム スイッチでサポートされます。インターフェイスがブロードキャスト トラフィックでフラッディングされた場合、トラフィック ストーム制御カウンタは増加しません。

トラフィック ストーム制御のデフォルト設定

次の表に、トラフィック ストーム制御パラメータのデフォルト設定値を示します。

Table 9: **デフォルトのトラフィック ストーム制御パラメータ**

パラメータ	デフォルト
トラフィック ストーム制御	無効
しきい値パーセンテージ	100

トラフィック ストーム制御の設定

制御対象のトラフィックが使用できる、利用可能な合計帯域幅に対するパーセンテージを設定できます。

Note トラフィック ストーム制御では 10 マイクロ秒のインターバルを使用しており、このインターバルがトラフィック ストーム制御の動作に影響を及ぼす可能性があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
3. switch(config-if)# **[no] storm-control** [**broadcast** | **multicast** | **unicast**] **level** *percentage*[*fraction*]}
   ]

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	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。

	Command or Action	Purpose
ステップ 2	switch(config)# **interface** {**ethernet** *slot*/*port* | **port-channel** *number*}	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	switch(config-if)# **[no] storm-control** [**broadcast** | **multicast** | **unicast**] **level** *percentage*[*fraction*]}]	インターフェイスを通過するトラフィックのトラフィック ストーム制御を設定します。デフォルトのステートはディセーブルです。

トラフィック ストーム制御の設定の確認

トラフィック ストーム制御の設定情報を表示するには、次のコマンドを使用します。.

コマンド	目的
show interface [**ethernet** *slot*/*port* | **port-channel** *number*]	トラフィック ストーム制御の設定を表示します。
show running-config interface	トラフィック ストーム制御の設定を表示します。

Note ストームイベントが発生してシャットダウンまたはトラップがトリガーされると、syslog メッセージが生成されます。

トラフィック ストーム制御の設定例

次に、トラフィック ストーム制御を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# storm-control broadcast level 40
switch(config-if)# storm-control multicast level 40
switch(config-if)# storm-control unicast level 40
```

次に、ポートチャネル 122 および 123 のトラフィック ストーム制御を設定する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 122, port-channel 123
switch(config-if-range)# storm-control unicast level 66.75
switch(config-if-range)# storm-control multicast level 66.75
switch(config-if-range)# storm-control broadcast level 66.75
switch(config-if-range)#
```