Cisco IOS XE Everest 16.6.x （Catalyst 3650 スイッチ） レイヤ 2 およびレイヤ 3 コンフィギュレーション ガイド

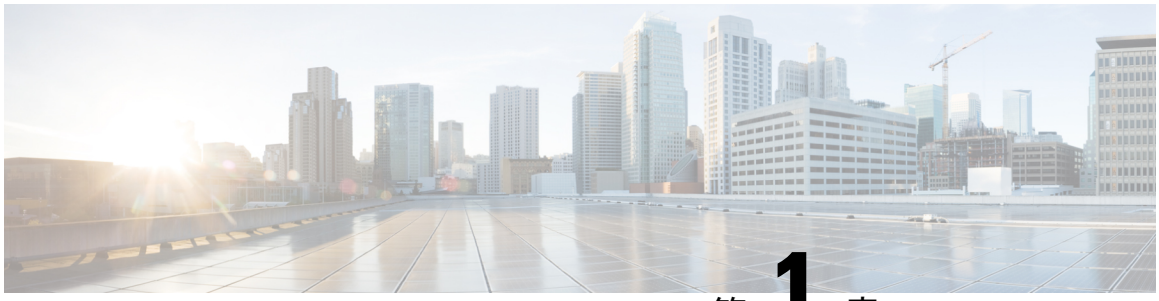
初版：2017 年 7 月 31 日

最終更新：2017 年 11 月 3 日

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

© 2017 Cisco Systems, Inc. All rights reserved.

目 次



第 1 章

スパニングツリー プロトコルの設定

機能情報の確認

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

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

STP の制約事項

- ルート deviceとしてdeviceを設定しようとする場合、ルート deviceにするために必要な値が 1 未満だと、失敗します。
- ネットワークが、拡張システム ID をサポートするdevicesとサポートしないものの両方で構成されている場合、拡張システム ID をサポートするdeviceがルート deviceになる可能性は低くなります。古いソフトウェアを実行している接続devicesの優先度より VLAN 番号が大きい場合は常に、拡張システム ID によってdevice 優先度の値が増加します。

- 各スパニングツリーインスタンスのルートdeviceは、バックボーンまたはディストリビューション deviceでなければなりません。アクセス deviceをスパニングツリープライマリ ルートとして設定しないでください。
- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

関連トピック

ルート デバイスの設定 （18 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID
スパニングツリー トポロジと BPDU （3 ページ）
接続を維持するためのエージング タイムの短縮 （11 ページ）

スパニング ツリー プロトコルに関する情報

スパニングツリー プロトコル

スパニングツリープロトコル（STP）は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ2リンク管理プロトコルです。レイヤ2イーサネット ネットワークが正常に動作するには、任意の2つのステーション間で存在できるアクティブ パスは1つだけです。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、ネットワークにループが生じます。ネットワークにループが存在すると、エンドステーションがメッセージを重複して受信する可能性があります。また、Devices が複数のレイヤ 2 インターフェイス上のエンドステーション MAC アドレスを学習する可能性もあります。このような状況によって、ネットワークが不安定になります。スパニングツリーの動作は透過的であり、エンドステーション側で、単一LAN セグメントに接続されているのか、複数セグメントからなるスイッチド LAN に接続されているのかを検出することはできません。

STPは、スパニングツリーアルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のdeviceを 1 つ選択します。アルゴリズムは、次に基づき、各ポートに役割を割り当て、スイッチドレイヤ2ネットワークを介して最良のループフリーパスを算出します。アクティブ トポロジでのポートの役割：

- ルート：スパニングツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニングツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートに役割が指定されているdevice、またはバックアップの役割が指定されているスイッチはルート deviceです。 少なくとも *1* つのポートに役割が指定されているdeviceは、指定deviceを意味します。

冗長データ パスはスパニングツリーによって、強制的にスタンバイ（ブロックされた）ステートにされます。スパニングツリーのネットワークセグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリー アルゴリズムがスパニングツリートポロジを再計算し、スタンバイパスをアクティブにします。Devices は次のように呼ばれるスパニングツリー フレームを送受信します。 （ブリッジ プロトコル データ ユニット（BPDU）と呼ばれる）を定期間隔で送受信します。devicesはこのフレームを転送しませんが、このフレームを使用してループフリー パスを構築します。 BPDU には、deviceおよび MAC アドレス、deviceの優先順位、ポートの優先順位、およびパス コストを含む、送信側deviceとそのポートに関する情報が含まれます。スパニングツリーはこの情報を使用して、スイッチド ネットワーク用のルート deviceおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび指定ポートを選定します。

deviceの 2 つのポートがループの一部である場合、 spanning-tree および、パス コスト設定は、どのポートがフォワーディング ステートになるか、およびどのポートがブロッキング ステートになるかを制御します。スパニングツリー ポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ適切であるかを表します。The コスト値は、メディア速度を表します。

（注） ショートパスコスト方式は、デフォルトの STP パスコスト方式です。

（注） デフォルトではdeviceは、Small Form-Factor Pluggable（SFP）モジュールを備えていないインターフェイスにだけ、（接続が稼働していることを確認するために）キープアライブ メッセージを送信します。[**no**] **keepalive**インターフェイス コンフィギュレーション コマンドをキーワードなしで入力すると、インターフェイスのデフォルトを変更できます。

スパニングツリー トポロジと BPDU

スイッチド ネットワーク内の安定したアクティブ スパニングツリー トポロジは、次の要素によって制御されます。

- device上の各 VLAN に関連付けられた一意のブリッジ ID（device優先度および MAC アドレス）。device スタックでは、ある特定のスパニングツリーインスタンスに対して、すべての devices が同一のブリッジ ID を使用します。
- ルート deviceに対するスパニングツリー パス コスト。
- 各レイヤ 2 インターフェイスに対応付けられたポート ID（ポート プライオリティおよび MAC アドレス）。

ネットワーク内のdevicesに電源が入ると、各機能はルート deviceとして機能します。各deviceは、そのすべてのポートからコンフィギュレーションBPDUを送信します。BPDUによって通信が行われ、スパニングツリー トポロジが計算されます。各設定 BPDU には、次の情報が含まれています。

- 送信deviceがルート deviceとして識別するdeviceの一意のブリッジ ID。
- ルートまでのスパニングツリー パス コスト
- 送信deviceのブリッジ ID。
- メッセージ エージ
- 送信側インターフェイス ID
- hello タイマー、転送遅延タイマー、および max-age プロトコル タイマーの値

deviceは、優位な情報（より小さいブリッジID、より低いパス コストなど）が含まれているコンフィギュレーションBPDUを受信すると、そのポートに対する情報を保存します。このBPDUをdeviceのルート ポート上で受信した場合、そのdeviceが指定deviceとなっているすべての接続 LAN に、更新したメッセージを付けて BPDU を転送します。

deviceは、そのポートに現在保存されている情報よりも下位の情報を含むコンフィギュレーション BPDU を受信した場合は、その BPDU を廃棄します。deviceが下位 BPDU を受信した LAN の指定deviceである場合、そのポートに保存されている最新情報を含む BPDU をその LAN に送信します。このようにして下位情報は廃棄され、優位情報がネットワークで伝播されます。

BPDU の交換によって、次の処理が行われます。

- ネットワーク内の 1 つのdeviceがとして選択されます。 ルート device（スイッチド ネットワークのスパニングツリー トポロジーの論理的な中心）。箇条書きの項目の下の図を参照してください。

  VLAN ごとに、device優先度が最も高い（最も小さい数字の優先順位の値）deviceがルート deviceとして選択されます。すべてのdevicesがデフォルトの優先度（32768）で設定されている場合、VLAN 内で MAC アドレスの最も小さいdeviceがルート deviceになります。device の優先順位の値は、次の図のようにブリッジ ID の最上位ビットを占めます。

- deviceごとに（ルート deviceを除く）、ルート ポートが 1 つ選択されます。このポートは、deviceからルート deviceにパケットを転送するときに最適パス（最小コスト）を提供します。

  device スタックのルート ポートを選択する場合には、スパニング ツリーは次の順序に従います。

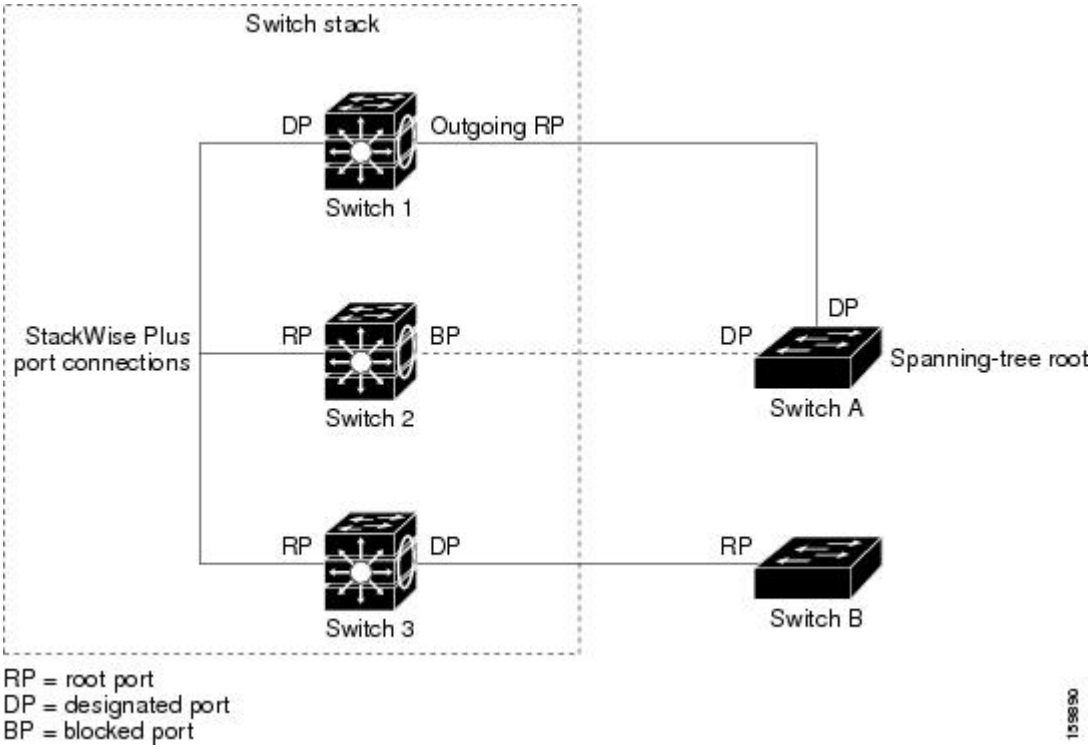
  - 最も低いルート ブリッジ ID を選択
  - ルート deviceへの最も低いパス コストを選択
  - 最も低い代表ブリッジ ID を選択
  - 最も低い代表パス コストを選択
  - 最も低いポート ID を選択

- スタック ルート device上の 1 つの発信ポートだけが、ルート ポートとして選択されます。スタック内の残りのdevicesは、次の図に示すように指定devicesになります（デバイス 2 およびデバイス 3）。

- ルート deviceへの最短距離は、パス コストに基づいてdeviceごとに計算されます。
- LAN セグメントごとに指定deviceが選択されます。指定deviceは、その LAN からルート deviceにパケットを転送するときの最小パス コストを提供します。DP は、指定deviceが LAN に接続されているポートです。

図 *1*: デバイス スタックのスパニング ツリー ポート ステート

1 つのスタック メンバーがスタック ルート deviceとして選択されます。スタック ルート device には出力ルート ポート（デバイス1）が含まれます。



スイッチド ネットワーク上のいずれの地点からもルート deviceに到達する場合に必要のないパスはすべて、スパニングツリー ブロッキング モードになります。

関連トピック

ルート デバイスの設定 （18 ページ）
STP の制約事項 （1 ページ）

ブリッジ ID、デバイス プライオリティ、および拡張システム ID

IEEE 802.1D 標準では、それぞれのdeviceに固有のルートdeviceの選択を制御するブリッジ識別子（ブリッジ ID）が必要です。各 VLAN は PVST+ と Rapid PVST+ によって異なる論理ブリッジと見なされるので、同一のdeviceは設定された各 VLAN とは異なるブリッジ ID を保有している必要があります。device上の各 VLAN には一意の 8 バイト ブリッジ ID が設定されます。上位の 2 バイトはdevice プライオリティに使用され、残りの 6 バイトがdeviceの MAC アドレスから取得されます。

従来はdevice プライオリティに使用されていた 2 バイトが、4 ビットのプライオリティ値と 12 ビットの拡張システム ID 値（VLAN ID と同じ）に割り当てられています。

表 *1:* デバイス プライオリティ値および拡張システム *ID*

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	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

スパニングツリーは、ブリッジ ID を VLAN ごとに一意にするために、拡張システム ID、device プライオリティ、および割り当てられたスパニングツリー MAC アドレスを使用します。device スタックは他のネットワークからは単一のdeviceとして認識されるため、スタック内のすべてのdevicesは、指定のスパニングツリーに対して同一のブリッジ ID を使用します。スタック マスターに障害が発生した場合、スタック メンバは新しいスタック マスターの新しい MAC アドレスに基づいて、実行中のすべてのスパニングツリーのブリッジ ID を再計算します。

拡張システム ID のサポートにより、ルート device、セカンダリ ルート device、および VLAN のdevice プライオリティの手動での設定方法に影響が生じます。たとえば、deviceのプライオリティ値を変更すると、deviceがルート deviceとして選定される可能性も変更されることになります。大きい値を設定すると可能性が低下し、値が小さいと可能性が増大します。

指定された VLAN のルート deviceに 24576 に満たないdevice プライオリティが設定されている場合は、deviceはその VLAN について、自身のプライオリティを最小のdevice プライオリティより 4096 だけ小さい値に設定します4096 は、表に示すように 4 ビット device スイッチ プライオリティ値の最下位ビットの値です。

ポート プライオリティとパス コスト

ループが発生した場合、スパニングツリーはポート プライオリティを使用して、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。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）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に同じプライオリティ値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

スパニングツリー 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に基づきます。ループが発生した場合、スパニングツリー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。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択される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。すべてのインターフェイスに同じコスト値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

deviceがdevice スタックのメンバーの場合は、最初に選択させたいインターフェイスには小さいコスト値を与え、最後に選択させたいインターフェイスには（ポートプライオリティを調整せずに）大きいコスト値を与えます。詳細については、関連項目を参照してください。

関連トピック

ポート プライオリティの設定 （21 ページ）
パス コストの設定 （23 ページ）

スパニングツリー インターフェイス ステート

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。インターフェイスがスパニングツリートポロジに含まれていない状態からフォワーディング ステートに直接移行すると、一時的にデータ ループが形成されることがあります。インターフェイスは新しいトポロジ情報がスイッチド LAN 上で伝播されるまで待機し、フレーム転送を開始する必要があります。インターフェイスはさらに、古いトポロジで使用されていた転送フレームのフレーム存続時間を満了させることも必要です。

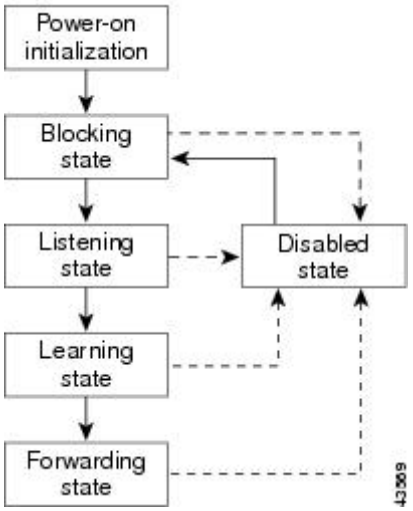
スパニングツリーを使用しているdeviceの各レイヤ 2 インターフェイスは、次のいずれかのステートになります。

- ブロッキング：インターフェイスはフレーム転送に関与しません。
- リスニング：インターフェイスをフレーム転送に関与させることをスパニングツリーが決定した場合、ブロッキング ステートから最初に移行するステートです。
- ラーニング：インターフェイスはフレーム転送に関与する準備をしている状態です。
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：インターフェイスはスパニングツリーに含まれません。シャットダウンポートであるか、ポート上にリンクがないか、またはポート上でスパニングツリーインスタンスが稼働していないためです。

インターフェイスは次のように、ステートを移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 *2:* スパニングツリー インターフェイス ステート



インターフェイスはこれらのステート間を移動します。

デフォルト設定では、deviceを起動するとスパニングツリーがイネーブルになります。その後、deviceの各インターフェイス、VLAN、ネットワークがブロッキング ステートからリスニングおよびラーニングという移行ステートを通過します。スパニングツリーは、フォワーディング ステートまたはブロッキング ステートで各インターフェイスを安定させます。

スパニングツリー アルゴリズムがレイヤ 2 インターフェイスをフォワーディング ステートにする場合、次のプロセスが発生します。

1. スパニングツリーがインターフェイスをブロッキング ステートに移行させるプロトコル情報を待つ間、インターフェイスはリスニング ステートになります。
2. スパニングツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニング ステートに移行させ、転送遅延タイマーをリセットします。
3. ラーニング ステートの間、deviceが転送データベースのエンド ステーションの位置情報を学習しているとき、インターフェイスはフレーム転送をブロックし続けます。
4. 転送遅延タイマーが満了すると、スパニングツリーはインターフェイスをフォワーディング ステートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

ブロッキング ステート

ブロッキング ステートのレイヤ2インターフェイスはフレームの転送に関与しません。初期化後、deviceの各インターフェイスにBPDUが送信されます。deviceは最初、他のdevicesとBPDUを交換するまで、ルートとして動作します。この交換により、ネットワーク内でどのdeviceがルートまたはルート deviceになるかが確立されます。ネットワーク内にdeviceが 1 つしかない場合は交換は行われず、転送遅延タイマーが満了し、インターフェイスがリスニング ステートになります。インターフェイスはdeviceの初期化後、必ずブロッキング ステートになります。

ブロッキング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。

- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

リスニング ステート

リスニング ステートは、ブロッキング ステートを経て、レイヤ 2 インターフェイスが最初に移行するステートです。インターフェイスがリスニング ステートになるのは、スパニングツリーによってそのインターフェイスのフレーム転送への関与が決定された場合です。

リスニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのレイヤ2インターフェイスは、フレームの転送に関与できるように準備します。インターフェイスはリスニング ステートからラーニング ステートに移行します。

ラーニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

フォワーディング ステート

フォワーディング ステートのレイヤ2インターフェイスは、フレームを転送します。インターフェイスはラーニング ステートからフォワーディング ステートに移行します。

フォワーディング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上でフレームを受信して転送します。
- 他のインターフェイスからスイッチングされたフレームを転送します。
- アドレスを学習します。
- BPDU を受信します。

ディセーブル ステート

ブロッキング ステートのレイヤ2インターフェイスは、フレームの転送やスパニングツリーに関与しません。ディセーブル ステートのインターフェイスは動作不能です。

ディセーブル インターフェイスは、次の機能を実行します。

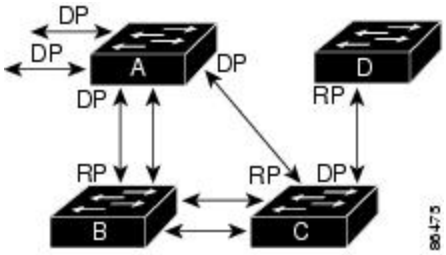
- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信しません。

デバイス またはポートがルート デバイスまたはルート ポートになる仕組み

ネットワーク上のすべてのdevicesがデフォルトのスパニングツリー設定で有効になっている場合、最小の MAC アドレスを持つdeviceがルート deviceになります。

図 *3:* スパニングツリー トポロジ

デバイス A はルート deviceとして選択されます。すべてのdevicesのdeviceの優先度がデフォルト（32768）に設定されており、デバイス A の MAC アドレスが最も小さいためです。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、デバイス A が最適なルート deviceとは限りません。ルート deviceになるように、最適なdeviceのプライオリティを引き上げる（数値を引き下げる）と、スパニングツリーの再計算が強制的に行われ、最適なdeviceをルートとした新しいトポロジが形成されます。



RP = Root Port
DP = Designated Port

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、ルート ポートよりプライオリティの高いインターフェイスに高速リンクを接続すると、ルート ポートが変更される可能性があります。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、デバイス B のあるポートがギガビット イーサネット リンクで、デバイス上の別のポート（10/100 リンク）がルート ポートであると仮定します。ネットワーク トラフィックはギガビット イーサネット リンクに流す方が効率的です。ギガビット イーサネット ポートのスパニングツリーポートプライオリティをルートポートより高くする（数値を小さくする）と、ギガビット イーサネット ポートが新しいルート ポートになります。

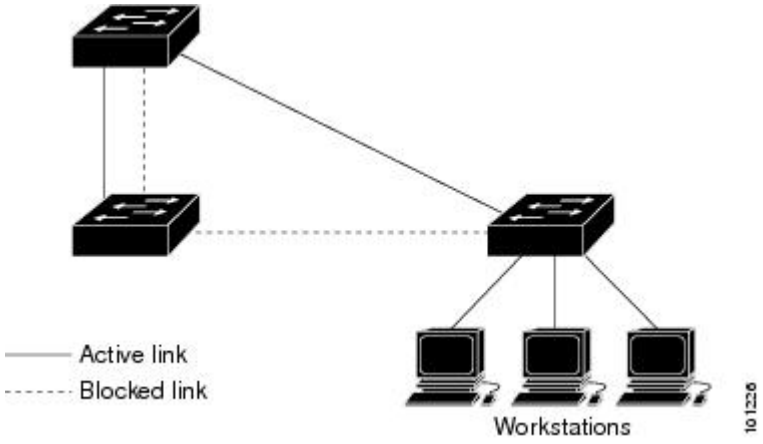
関連トピック

ポート プライオリティの設定 （21 ページ）

スパニングツリーおよび冗長接続

図 *4:* スパニングツリーおよび冗長接続

2 つのdevice インターフェイスを別の 1 台のデバイス、または 2 台の異なるデバイスに接続することにより、スパニングツリーを使用して冗長バックボーンを作成できます。スパニングツリーは一方のインターフェイスを自動的にディセーブルにし、他方でエラーが発生した場合にはそのディセーブルにしていた方をイネーブルにします。一方のリンクが高速で、他方が低速の場合、必ず、低速の方のリンクがディセーブルになります。速度が同じ場合、ポート優先度とポート ID が加算され、最大値を持つリンクがスパニングツリーによって無効にされます。



EtherChannel グループを使用して、devices間に冗長リンクを設定することもできます。

スパニングツリー アドレスの管理

IEEE 802.1D では、各種ブリッジ プロトコルに使用させるために、0x00180C2000000 ～ 0x0180C2000010 の範囲で 17 のマルチキャスト アドレスが規定されています。これらのアドレスは削除できないスタティック アドレスです。

スパニングツリー ステートに関係なく、スタック内の各deviceは 0x0180C2000000 ～ 0x0180C2000000 のアドレス宛てのパケットを受信しますが、転送は行いません。

スパニングツリーがイネーブルの場合、deviceまたはスタック内の各deviceの CPU は 0x0180C2000000 および 0x0180C2000010 宛てのパケットを受信します。スパニングツリーがディセーブルの場合は、deviceまたはスタック内の各deviceは、それらのパケットを不明のマルチキャスト アドレスとして転送します。

接続を維持するためのエージング タイムの短縮

ダイナミックアドレスのエージングタイムはデフォルトで 5 分です。これは、**mac address-table aging-time** グローバル コンフィギュレーション コマンドのデフォルトの設定です。ただし、スパニングツリーの再構成により、多数のステーションの位置が変更されることがあります。このようなステーションは、再構成中、5 分以上にわたって到達できないことがあるので、ア

ドレステーブルからステーションアドレスを削除し、改めて学習できるように、アドレスエージングタイムが短縮されます。スパニングツリー再構成時に短縮されるエージングタイムは、転送遅延パラメータ値（**spanning-tree vlan** *vlan-id* **forward-time** *seconds* グローバル コンフィギュレーション コマンド）と同じです。

各 VLAN はそれぞれ独立したスパニングツリー インスタンスであるため、deviceは VLAN 単位でエージングタイムを短縮します。ある VLAN でスパニングツリーの再構成が行われると、その VLAN で学習されたダイナミック アドレスがエージング タイム短縮の対象になります。他の VLAN のダイナミック アドレスは影響を受けず、deviceで設定されたエージング間隔がそのまま保持されます。

関連トピック

ルート デバイスの設定 （18 ページ）
STP の制約事項 （1 ページ）

スパニングツリー モードおよびプロトコル

このdeviceでサポートされるモードおよびプロトコルは、次のとおりです。

- PVST+：このスパニングツリー モードは、IEEE 802.1D 標準およびシスコ独自の拡張機能に準拠します。PVST+ はdevice上の各 VLAN でサポートされる最大数まで動作し、各 VLAN にネットワーク上でのループフリーパスを提供します。

  PVST+ は、対象となる VLAN にレイヤ 2 ロード バランシングを提供します。ネットワーク上の VLAN を使用してさまざまな論理トポロジを作成し、特定のリンクに偏らないようにすべてのリンクを使用できるようにします。VLAN 上の PVST+インスタンスごとに、それぞれ 1 つのルート deviceがあります。このルート deviceは、その VLAN に対応するスパニングツリー情報を、ネットワーク上の他のすべてのdevicesに伝送します。このプロセスにより、各deviceがネットワークに関する共通の情報を持つため、ネットワーク トポロジが確実に維持されます。

- Rapid PVST+：デバイスのデフォルト STP モードは Rapid PVST+ です。このスパニングツリーモードは、IEEE 802.1w 標準に準拠した高速コンバージェンスを使用する以外は PVST+ と同じです。。高速コンバージェンスを行うため、Rapid PVST+ はトポロジ変更を受信すると、ポート単位でダイナミックに学習した MAC アドレス エントリをただちに削除します。このような場合、PVST+ では、ダイナミックに学習した MAC アドレス エントリには短いエージング タイムが使用されます。

  Rapid PVST+ は PVST+ と同じ設定を使用しているので（特に明記する場合を除く）、device で必要なことは最小限の追加設定のみです。Rapid PVST+ の利点は、大規模な PVST+ のインストール ベースを Rapid PVST+ に移行する際に、複雑なマルチ スパニングツリー プロトコル（MSTP）設定の学習やネットワーク再設定の必要がないことです。Rapid PVST+ モードでは、各 VLAN は独自のスパニングツリー インスタンスを最大数実行します。

- MSTP：このスパニングツリー モードは IEEE 802.1s 標準に準拠しています。複数の VLAN を同一のスパニングツリー インスタンスにマッピングし、多数の VLAN をサポートする場合に必要となるスパニングツリーインスタンスの数を減らすことができます。MSTP は Rapid Spanning-Tree Protocol（RSTP）（IEEE 802.1w 準拠）上で実行され、転送遅延を解消し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行するこ

とにより、スパニングツリーの高速コンバージェンスを可能にします。deviceスタックでは、クロススタック高速移行（CSRT）機能が RSTP と同じ機能を実行します。RSTP または CSRT を使用しなければ、MSTP は稼働できません。

関連トピック

スパニングツリー モードの変更 （16 ページ）

サポートされるスパニングツリー インスタンス

PVST+ または Rapid PVST+ モードでは、deviceまたはdevice スタックは最大 128 のスパニングツリー インスタンスをサポートします。

MSTP モードでは、deviceまたはdevice スタックは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。

関連トピック

スパニング ツリーのディセーブル化 （17 ページ）
スパニングツリー機能のデフォルト設定 （15 ページ）
MSTP のデフォルト設定 （52 ページ）

スパニングツリーの相互運用性と下位互換性

MSTP および PVST+ が混在したネットワークでは、Common Spanning-Tree（CST）のルートは MST バックボーンの内側に配置する必要があり、PVST+ deviceを複数の MST リージョンに接続することはできません。

ネットワーク内に Rapid PVST+ を実行しているdevicesと PVST+ を実行しているdevicesが存在する場合、Rapid PVST+ devicesと PVST+ devicesを別のスパニングツリー インスタンスに設定することを推奨します。Rapid PVST+ スパニングツリー インスタンスでは、ルート deviceは Rapid PVST+ deviceでなければなりません。PVST+ インスタンスでは、ルート deviceは PVST+ deviceでなければなりません。PVST+ devicesはネットワークのエッジに配置する必要があります。

すべてのスタック メンバーが、同じバージョンのスパニングツリーを実行します（すべて PVST+、すべて Rapid PVST+、またはすべて MSTP）。

表 *2 : PVST+、MSTP、Rapid PVST+* の相互運用性と互換性

	PVST+	MSTP	Rapid PVST+
PVST+	あり	あり （制限あり）	あり （PVST+に戻る）
MSTP	あり （制限あり）	あり	あり （PVST+に戻る）
Rapid PVST+	あり （PVST+に戻る）	あり （PVST+に戻る）	対応

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）
MSTP 設定時の注意事項 （36 ページ）

MST リージョン （37 ページ）

STP および IEEE 802.1Q トランク

VLAN トランクに関する IEEE 802.1Q 規格は、ネットワークのスパニングツリー ストラテジに一定の制限を設けています。この規格では、トランク上で使用できるすべての VLAN に対して、1 つのスパニングツリー インスタンスしか認められません。ただし、IEEE 802.1Q トランクを介して接続される Cisco devicesのネットワークにおいて、devicesはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持します。

IEEE 802.1Q トランクを介して Cisco deviceを他社製のデバイスに接続する場合、Cisco deviceは PVST+を使用してスパニングツリーの相互運用性を実現します。Rapid PVST+がイネーブルの場合、deviceは PVST+ ではなく Rapid PVST+ を使用します。deviceは、トランクの IEEE 802.1Q VLAN のスパニングツリー インスタンスと他社の IEEE 802.1Q deviceのスパニングツリー インスタンスを結合します。

ただし、PVST+ または Rapid PVST+ の情報はすべて、他社製の IEEE 802.1Q devicesからなるクラウドにより分離された Cisco devicesによって維持されます。Cisco devicesを分離する他社製の IEEE 802.1Q クラウドは、devices間の単一トランク リンクとして扱われます。

PVST+ は IEEE 802.1Q トランクで自動的に有効になるので、ユーザ側で設定する必要はありません。アクセス ポートおよびISL（スイッチ間リンク）トランク ポートでの外部スパニングツリーの動作は、PVST+ の影響を受けません。

スパニング ツリーとデバイス スタック

device スタックが PVST+ または Rapid PVST+ モードで動作している場合：

- device スタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが与えられたスパニングツリーに同一のブリッジ ID を使用します。ブリッジ ID は、active switchの MAC アドレスから取得されます。
- 新しいdeviceがスタックに加わると、そのスイッチは、active switchのブリッジ ID を自分のブリッジ ID として設定します。新しく追加されたdeviceの ID が最も小さく、ルート パス コストがすべてのスタック メンバー間で同じ場合は、新しく追加されたdeviceがスタック ルートになります。
- スタック メンバがスタックから除外されると、スタック内でスパニングツリーの再コンバージェンスが発生します（スタック外で発生する場合もあります）。残っているスタック メンバのうち最も低いスタック ポート ID を持つスタック メンバが、スタック ルートになります。
- device スタック外にあるネイバー deviceに障害が発生したか、またはその電源が停止した場合、通常のスパニングツリー処理が発生します。スパニングツリーの再コンバージェンスは、アクティブなトポロジ内のdeviceが失われたことにより発生する場合もあります。
- device スタック外にある新しい deviceがネットワークに追加された場合、通常のスパニングツリー処理が発生します。スパニングツリーの再コンバージェンスは、ネットワークにdeviceが追加されたことにより発生する場合もあります。

スパニングツリー機能のデフォルト設定

表 *3:* スパニングツリー機能のデフォルト設定

機能	デフォルト設定
イネーブル ステート	VLAN 1 上でイネーブル
スパニングツリー モード	Rapid PVST+（PVST+ と MSTP はディセーブル）
デバイス priority	32768
スパニングツリー ポート プライオリティ（インターフェイス単位で設定可能）	128
スパニングツリー ポート コスト（インターフェイス単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリー VLAN ポート プライオリティ（VLAN 単位で設定可能）	128
スパニングツリー VLAN ポート コスト（VLAN 単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリー タイマー	hello タイム：2 秒 転送遅延時間：15 秒 最大エージング タイム：20 秒 転送保留カウント：6 BPDU

（注） Cisco IOS Release 15.2(4)E 以降では、デフォルトの STP モードは Rapid PVST+ です。

関連トピック

スパニング ツリーのディセーブル化 （17 ページ）
サポートされるスパニングツリー インスタンス （13 ページ）

スパニングツリー機能の設定方法

スパニングツリー モードの変更

スイッチは次の 3 つのスパニングツリー モードをサポートします。Per-VLAN Spanning-Tree Plus（PVST+）、Rapid PVST+、またはマルチ スパニングツリープロトコル（MSTP）。デフォルトでは、device Rapid PVST+ プロトコルを実行します。

デフォルト モード以外のモードをイネーブルにする場合、この手順は必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**} 例： `デバイス(config)# spanning-tree mode pvst`	スパニングツリーモードを設定します。 すべてのスタック メンバーは、同じバージョンのスパニング ツリーを実行します。 • PVST+ をイネーブルにするには、**pvst** を選択します。 • MSTP をイネーブルにするには、**mst** を選択します。 • rapid PVST+ をイネーブルにするには、**rapid-pvst** を選択します。
ステップ 4	**interface** *interface-id* 例： `デバイス(config)# interface GigabitEthernet1/0/1`	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。有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。VLAN ID の範囲は 1 ～ 4094 です。

	コマンドまたはアクション	目的
		指定できるポートチャネルの範囲は1～48 です。
ステップ 5	**spanning-tree link-type point-to-point** 例： `デバイス(config-if)# spanning-tree link-type point-to-point`	このポートのリンク タイプがポイントツーポイントであることを指定します。 このポート（ローカル ポート）をポイントツーポイント リンクでリモート ポートと接続し、ローカル ポートが指定ポートになると、deviceはリモート ポートとネゴシエーションし、ローカル ポートをフォワーディング ステートにすばやく変更します。
ステップ 6	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**clear spanning-tree detected-protocols** 例： `デバイス# clear spanning-tree detected-protocols`	device 上のいずれかのポートがレガシー IEEE 802.1D device 上のポートに接続されている場合は、このコマンドにより device 全体のプロトコル移行プロセスを再開します。 このステップは、このdeviceで Rapid PVST+ が稼働していることを指定deviceが検出する場合のオプションです。

関連トピック

スパニングツリー モードおよびプロトコル （12 ページ）

スパニング ツリーのディセーブル化

スパニングツリーはデフォルトで、VLAN 1 およびスパニングツリー限度を上限として新しく作成されたすべての VLAN 上でイネーブルです。スパニングツリーをディセーブルにするのは、ネットワーク トポロジにループがないことが確実な場合だけにしてください。

注意 スパニングツリーがディセーブルでありながら、トポロジにループが存在していると、余分なトラフィックが発生し、パケットの重複が無限に繰り返されることによって、ネットワークのパフォーマンスが大幅に低下します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no spanning-tree vlan** *vlan-id* 例： `デバイス(config)# no spanning-tree vlan 300`	*vlan-id* に指定できる範囲は 1 ～ 4094 です。
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

関連トピック

サポートされるスパニングツリー インスタンス （13 ページ）
スパニングツリー機能のデフォルト設定 （15 ページ）

ルート デバイスの設定

特定の VLAN で device をルートとして設定するには、**spanning-tree vlan** *vlan-id* **root** 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、deviceのプライオリティをデフォルト値（32768）から、それより大幅に小さい値に変更します。 このコマンドを入力すると、ソフトウェアが各 VLAN について、ルート devicesのdevice プライオリティを確認します。拡張システム ID をサポートするため、deviceは指定された VLAN の自身のプライオリティを 24576 に設定します。この値によって、このdeviceを指定された VLAN のルートに設定できます。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンドステーション間deviceの最大ホップカウント）を指定するには、**diameter** キーワードを指定します。ネットワーク直径を指定すると、device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 タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きできます。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **root primary** [**diameter** *net-diameter* 例： `デバイス(config)# spanning-tree vlan 20-24 root primary diameter 4`	指定された VLAN のルートになるように、deviceを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一のVLAN、ハイフンで区切られた範囲のVLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は1～4094 です。 •（任意）**diameter** *net-diameter* には、任意の2つのエンドステーション間devicesの最大数を指定します。範囲は 2 ～ 7 です。
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

次のタスク

ルートdeviceとしてdeviceを設定した後で、**spanning-tree vlan** *vlan-id* **hello-time**、**spanning-tree vlan** *vlan-id* **forward-time**、および **spanning-tree vlan** *vlan-id* **max-age** 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、および最大エージングタイムを手動で設定することは推奨できません。

関連トピック

ブリッジ ID、デバイス プライオリティ、および拡張システム ID

スパニングツリー トポロジと BPDU （3 ページ）
接続を維持するためのエージング タイムの短縮 （11 ページ）
STP の制約事項 （1 ページ）

セカンダリ ルート デバイスの設定

deviceをセカンダリ ルートとして設定すると、deviceプライオリティがデフォルト値（32768）から 28672 に変更されます。このプライオリティでは、deviceがプライマリ ルート deviceが失敗した場合の、指定された VLAN のルートdeviceになる可能性があります。ここでは、その他のネットワーク devicesが、デフォルトのdevice プライオリティの 32768 を使用しているためにルート deviceになる可能性が低いことが前提となっています。

このコマンドを複数のdeviceに対して実行すると、複数のバックアップ ルート devicesを設定できます。**spanning-tree vlan** *vlan-id* **root primary** グローバル コンフィギュレーション コマンドでプライマリルート device を設定したときと同じネットワーク直径および hello タイム値を使用してください。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例：** `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **root secondary** [**diameter** *net-diameter* **例：** `デバイス(config)# spanning-tree vlan 20-24 root secondary diameter 4`	指定された VLAN のセカンダリ ルートになるように、deviceを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （任意）**diameter** *net-diameter* には、任意の 2 つのエンドステーショ

	コマンドまたはアクション	目的
		ン間devicesの最大数を指定します。指定できる範囲は 2 ～ 7 です。 プライマリ ルート deviceを設定したときと同じネットワーク直径を使用してください。
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。

ポート プライオリティの設定

（注） device が device スタックのメンバーである場合、**spanning-tree** [**vlan** *vlan-id*] **port-priority** *priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree** [**vlan** *vlan-id*] **cost** *cost* インターフェイス コンフィギュレーション コマンドを使用して、フォワーディング ステートにするインターフェイスを選択する必要があります。最初に選択させるインターフェイスには、低いコスト値を割り当て、最後に選択させるインターフェイスには高いコスト値を割り当てます。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： `デバイス(config)# interface gigabitethernet1/0/2`	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。 有効なインターフェイスは、物理ポートおよびポートチャネル論理インターフェイス（**port-channel** *port-channel-number*）です。
ステップ 4	**spanning-tree port-priority** *priority* 例： `デバイス(config-if)# spanning-tree port-priority 0`	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* に指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 5	**spanning-tree vlan** *vlan-id* **port-priority** *priority* 例： `デバイス(config-if)# spanning-tree vlan 20-25 port-priority 0`	VLAN のポート プライオリティを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *priority* に指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 6	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

ポート プライオリティとパス コスト （6 ページ）
デバイス またはポートがルート デバイスまたはルート ポートになる仕組み （10 ページ）

パス コストの設定

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `デバイス(config)# interface gigabitethernet1/0/1`	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。有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）です。
ステップ 4	**spanning-tree cost** *cost* 例： `デバイス(config-if)# spanning-tree cost 250`	インターフェイスのコストを設定します。 ループが発生した場合、スパニングツリーはパス 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。低いパス コストは高速送信を表します。 *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 5	**spanning-tree vlan** *vlan-id* **cost** *cost* 例：	VLAN のコストを設定します。

	コマンドまたはアクション	目的
	デバイス(config-if)# **spanning-tree vlan 10,12-15,20 cost 300**	ループが発生した場合、スパニングツリー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。低いパス コストは高速送信を表します。 • *vlan-id* には、VLAN ID 番号で識別された単一のVLAN、ハイフンで区切られた範囲のVLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は1～4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 6	**end** 例： デバイス(config-if)# **end**	特権 EXEC モードに戻ります。

show spanning-tree interface *interface-id* 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

ポート プライオリティとパス コスト （6 ページ）

VLAN のデバイス プライオリティの設定

device プライオリティを設定して、スタンドアロン deviceまたはスタックにあるdeviceがルート deviceとして選択される可能性を高めることができます。

（注） このコマンドの使用には注意してください。deviceのプライオリティを変更する場合は通常、**spanning-tree vlan** *vlan-id* **root primary** および **spanning-tree vlan** *vlan-id* **root secondary** 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ことを推奨します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **priority** *priority* 例： `デバイス(config)# spanning-tree vlan 20 priority 8192`	VLAN のdevice プライオリティの設定 • *vlan-id* には、VLAN ID 番号で識別された単一のVLAN、ハイフンで区切られた範囲のVLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は1～4094 です。 • *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。この値が低いほど、deviceがルート deviceとして選択される可能性が高くなります。 有効なプライオリティ値は 4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。その他の値はすべて拒否されます。
ステップ 4	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

hello タイムの設定

hello タイムはルート deviceによって設定メッセージが生成されて送信される時間の間隔です。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**spanning-tree vlan** *vlan-id* **hello-time** *seconds* 例： デバイス(config)# **spanning-tree vlan 20-24 hello-time 3**	VLAN の hello タイムを設定します。hello タイムはルート deviceによって設定メッセージが生成されて送信される時間の間隔です。このメッセージは、deviceが活動中であることを表します。 • *vlan-id* には、VLAN ID 番号で識別された単一のVLAN、ハイフンで区切られた範囲のVLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は1～4094 です。 • *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 3	**end** 例： デバイス(config-if)# **end**	特権 EXEC モードに戻ります。

VLAN の転送遅延時間の設定

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	デバイス# **configure terminal**	
ステップ 3	**spanning-tree vlan** *vlan-id* **forward-time** *seconds* 例： デバイス(config)# **spanning-tree vlan 20,25 forward-time 18**	VLANの転送時間を設定します。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、インターフェイスが待機する秒数です。 • *vlan-id* には、VLAN ID 番号で識別された単一のVLAN、ハイフンで区切られた範囲のVLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は1～4094 です。 • *seconds* に指定できる範囲は 4 ～ 30 です。デフォルトは 15 です。
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。

VLAN の最大エージング タイムの設定

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**spanning-tree vlan** *vlan-id* **max-age** *seconds* 例： `デバイス(config)# spanning-tree vlan 20 max-age 30`	VLAN の最大エージング タイムを設定します。最大エージング タイムは、deviceが再設定を試す前にスパニングツリー設定メッセージを受信せずに待機する秒数です。 • *vlan-id* には、VLAN ID 番号で識別された単一のVLAN、ハイフンで区切られた範囲のVLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は1～4094 です。 • *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 4	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

転送保留カウントの設定

転送保留カウント値を変更することで、BPDU のバースト サイズを設定できます。

（注） このパラメータをより高い値に変更すると、（特に Rapid PVST+ モードで）CPU の使用率に大きく影響します。逆に、この値を低く設定すると、セッションによってはコンバージェンスを抑えることができます。この値は、デフォルト設定で使用することを推奨します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	デバイス# **configure terminal**	
ステップ 3	**spanning-tree transmit hold-count** *value* 例： デバイス(config)# **spanning-tree transmit hold-count 6**	1 秒間停止する前に送信できる BPDU 数を設定します。 *value* に指定できる範囲は 1 ～ 20 です。デフォルト値は 6 です。
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。

スパニングツリー ステータスのモニタリング

表 *4:* スパニングツリー ステータス表示用のコマンド

show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree vlan *vlan-id*	指定した VLAN のスパニング ツリー情報を表示します。
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree interface *interface-id* **portfast**	指定したインターフェイスのスパニングツリー portfast 情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示します。または STP ステート セクションのすべての行を表示します。

スパニングツリーカウンタをクリアするには、**clear spanning-tree** [**interface** *interface-id*] 特権 EXEC コマンドを使用します。

スパニング ツリー プロトコルに関する追加情報

関連資料

関連項目	マニュアル タイトル
スパニング ツリー プロトコル コマンド	*LAN Switching Command Reference, Cisco IOS XE Release 3SE（Catalyst 3650 Switches）*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

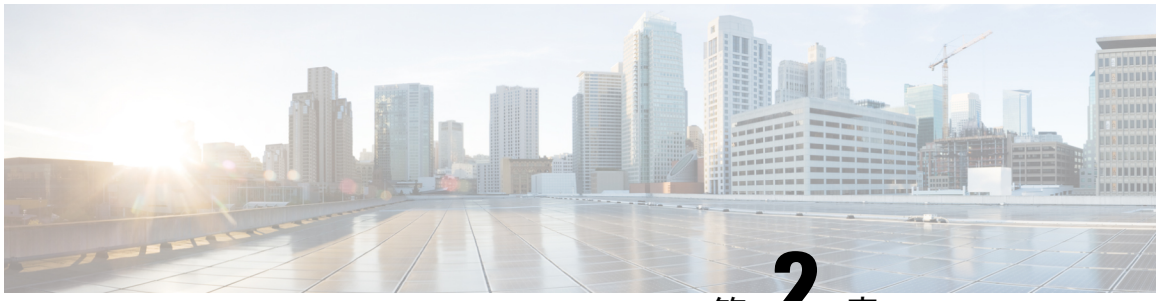
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

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

STP の機能情報

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



第 2 章

複数のスパニング ツリー プロトコルの設定

機能情報の確認

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

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

MSTP の前提条件

- 2つ以上のdevicesを同じマルチスパニングツリー（MST）リージョンに設定するには、その 2 つに同じ 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。
- 2 つ以上のスタックされたスイッチを同じ 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。

- ネットワーク内の冗長パスでロード バランシングを機能させるには、すべての VLAN/インスタンスマッピングの割り当てが一致している必要があります。一致していないと、すべてのトラフィックが 1 つのリンク上で伝送されます。パスコストを手動で設定することで、device スタック全体にわたりロードバランシングを実現できます。
- Per-VLAN Spanning-Tree Plus（PVST+）と MST クラウドの間、または Rapid- PVST+ と MST クラウドの間でロードバランシングが機能するためには、すべての MST 境界ポートがフォワーディングでなければなりません。MST クラウドの内部スパニングツリー（IST）マスターが共通スパニング ツリー（CST）のルートである場合、MST 境界ポートはフォワーディングです。MST クラウドが複数の MST リージョンから構成されている場合、いずれかの MST リージョンに CST ルートを含める必要があり、その他すべての MST リージョンに、PVST+ クラウドまたは高速 PVST+ クラウドを通るパスよりも、MST クラウド内に含まれるルートへのパスが良くする必要があります。クラウド内のdevicesを手動で設定しなければならない場合もあります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）
MSTP 設定時の注意事項 （36 ページ）
MST リージョン （37 ページ）

MSTP の制約事項

- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。
- device スタックは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。
- PVST+、Rapid PVST+、および MSTP はサポートされますが、アクティブにできるのは 1 つのバージョンだけです（たとえば、すべての VLAN で PVST+ を実行する、すべての VLAN で Rapid PVST+ を実行する、またはすべての VLAN で MSTP を実行します）。
- MST コンフィギュレーションの VLAN トランキング プロトコル（VTP）伝搬はサポートされません。ただし、コマンドライン インターフェイス（CLI）または簡易ネットワーク管理プロトコル（SNMP）サポートを通じて、MST リージョン内の各deviceで MST コンフィギュレーション（リージョン名、リビジョン番号、および VLAN とインスタンスのマッピング）を手動で設定することは可能です。
- ネットワークを多数のリージョンに分割することは推奨できません。ただし、どうしても分割せざるを得ない場合は、スイッチド LAN をルータまたは非レイヤ 2 デバイスで相互接続された小規模な LAN に分割することを推奨します。
- リージョンは、同じ MST コンフィギュレーションを持つ 1 つまたは複数のメンバーで構成されます。リージョンの各メンバーは高速スパニングツリープロトコル（RSTP）ブリッジ プロトコル データ ユニット（BPDU）を処理する機能を備えている必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポー

トできるスパニングツリー インスタンスの数は 65 までです。VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

- ルートdeviceとしてdeviceを設定した後で、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** 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、および最大エージングタイムを手動で設定することは推奨できません。

表 *5 : PVST+*、*MSTP*、*Rapid PVST+* の相互運用性と互換性

	PVST+	MSTP	Rapid PVST+
PVST+	あり	あり（制限あり）	あり（PVST+に戻る）
MSTP	あり（制限あり）	あり	あり（PVST+に戻る）
Rapid PVST+	あり（PVST+に戻る）	あり（PVST+に戻る）	対応

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）
MSTP 設定時の注意事項 （36 ページ）
MST リージョン （37 ページ）
ルート デバイスの設定 （55 ページ）
ルート スイッチ （37 ページ）

MSTP について

MSTP の設定

高速コンバージェンスのために RSTP を使用する MSTP では、複数の VLAN をグループ化して同じスパニングツリーインスタンスにマッピングすることが可能で、多くの VLAN をサポートするのに必要なスパニングツリー インスタンスの数を軽減できます。MSTP は、データ トラフィックに複数の転送パスを提供し、ロード バランシングを実現して、多数の VLAN をサポートするのに必要なスパニングツリーインスタンスの数を減らすことができます。MSTP を使用すると、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）は影響を受けないので、ネットワークのフォールトトレランスが向上します。

（注） マルチ スパニングツリー（MST）実装は IEEE 802.1s 標準に準拠しています。

MSTP を導入する場合、最も一般的なのは、レイヤ 2 スイッチド ネットワークのバックボーンおよびディストリビューション レイヤへの導入です。MSTP の導入により、サービス プロバイダー環境に求められる高可用性ネットワークを実現できます。

deviceが MST モードの場合、IEEE 802.1w 準拠の RSTP が自動的にイネーブルになります。RSTP は、IEEE 802.1D の転送遅延を軽減し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行する明示的なハンドシェイクによって、スパニングツリーの高速コンバージェンスを実現します。

MSTP と RSTP は、既存のシスコ独自の Multiple Instance STP（MISTP）、および既存の Cisco PVST+ と Rapid Per-VLAN Spanning-Tree plux（Rapid PVST+）を使用して、スパニングツリーの動作を改善し、（オリジナルの）IEEE 802.1D スパニング ツリーに準拠した機器との下位互換性を保持しています。

device スタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが同一のdevice ID を使用します。

MSTP 設定時の注意事項

- **spanning-tree mode mst** 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、MST をイネーブルにすると、RSTP が自動的にイネーブルになります。
- UplinkFast、BackboneFast、クロススタック UplinkFast の設定のガイドラインについては、関連項目のセクションの該当するセクションを参照してください。
- deviceが MST モードの場合は、パス コスト値の計算に、ロング パス コスト計算方式（32 ビット）が使用されます。ロング パス コスト計算方式では、次のパス コスト値がサポートされます。

速度	パス コスト値
10 Mb/s	2,000,000
100 Mb/s	200,000
1 Gb/s	20,000
10 Gb/s	2,000
100 Gb/s	200

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）
MSTP の前提条件 （33 ページ）
MSTP の制約事項 （34 ページ）
スパニングツリーの相互運用性と下位互換性 （13 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast （80 ページ）
UplinkFast （75 ページ）

ルート スイッチ

deviceは、マッピングされているVLANグループのスパニングツリーインスタンスを保持しています。device ID は、deviceのプライオリティおよびdeviceの MAC アドレスで構成されており、各インスタンスに関連付けられます。VLANのグループでは、最小のdevice IDをもつdeviceがルート deviceになります。

deviceをルートとして設定する場合は、deviceプライオリティをデフォルト値（32768）からそれより大幅に低い値に変更し、deviceが、指定したスパニング ツリー インスタンスのルート deviceになるようにします。このコマンドを入力すると、deviceはルート devicesのdevice プライオリティをチェックします。拡張システム ID をサポートしているため、24576 という値でdevicesが指定したスパニングツリーインスタンスのルートとなる場合、そのdeviceは指定したインスタンスに対する自身のプライオリティを 24576 に設定します。

指定されたインスタンスのルート deviceに 24576 に満たないdevice プライオリティが設定されている場合は、deviceは自身のプライオリティを最小のdeviceプライオリティより 4096 だけ小さい値に設定します（4096 は 4 ビット device プライオリティの最下位ビットの値です）。詳細については、関連項目の「ブリッジ ID、スイッチ プライオリティ、および拡張システム ID デバイス」リンクを参照してください。

ネットワークが、拡張システム ID をサポートするdevicesとサポートしないものの両方で構成されている場合、拡張システム ID をサポートするdeviceがルート deviceになる可能性は低くなります。古いソフトウェアを実行している接続deviceのプライオリティより VLAN 番号が大きい場合は常に、拡張システム ID によってスイッチ プライオリティ値が増加します。

各スパニングツリー インスタンスのルート deviceは、バックボーンまたはディストリビューション deviceでなければなりません。アクセス deviceをスパニングツリープライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンドステーション間の最大 device ホップカウント）を指定するには、**diameter** キーワード（MST インスタンスが 0 の場合のみ使用できる）を指定します。ネットワーク直径を指定すると、device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 タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きできます。

関連トピック

ルート デバイスの設定 （55 ページ）
MSTP の制約事項 （34 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID

MST リージョン

スイッチをMSTインスタンスに加入させるには、同じMSTコンフィギュレーション情報を使用して矛盾のないようにスイッチを設定する必要があります。同じMST設定の相互接続スイッチの集まりによって MST リージョンが構成されます。

MST 設定では、それぞれのdeviceが属する MST リージョンが制御されます。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。その中で MST リージョンの設定を指定することにより、リージョンのdeviceを設定します。MST インスタンスに VLAN をマッピングし、リージョン名を指定して、リビジョン番号を設定できます。手順と例については、関連項目の「MST リージョン設定の指定と MSTP のイネーブル化」リンクをクリックします。

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。さらに、各メンバは、RSTP ブリッジプロトコルデータユニット（BPDU）を処理できる必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリーインスタンスの数は 65 までです。インスタンスは、0 ～ 4094 の範囲の任意の番号で識別できます。VLAN には、一度に 1 つのスパニングツリーインスタンスのみ割り当てることができます。

関連トピック

MST リージョンの図 （41 ページ）
MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）
MSTP の前提条件 （33 ページ）
MSTP の制約事項 （34 ページ）
スパニングツリーの相互運用性と下位互換性 （13 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast （80 ページ）
UplinkFast （75 ページ）

IST、CIST、CST

すべてのスパニングツリー インスタンスが独立している PVST+ および Rapid PVST+ とは異なり、MSTP は次の 2 つのタイプのスパニングツリーを確立して保持しています。

- Internal Spanning-Tree（IST）は、1 つの MST リージョン内で稼働するスパニングツリーです。

  各 MST リージョン内の MSTP は複数のスパニングツリー インスタンスを維持しています。インスタンス 0 は、リージョンの特殊なインスタンスで、IST と呼ばれています。その他すべての MSTI には、1 ～ 4094 の番号が付きます。

  IST は、BPDU を送受信する唯一のスパニングツリー インスタンスです。他のスパニングツリーの情報はすべて、MSTP BPDU 内にカプセル化されている M レコードに格納されています。MSTP BPDU はすべてのインスタンスの情報を伝送するので、複数のスパニングツリー インスタンスをサポートする処理が必要な BPDU の数を大幅に減少できます。

  同一リージョン内のすべての MST インスタンスは同じプロトコル タイマーを共有しますが、各 MST インスタンスは独自のトポロジ パラメータ（ルート device ID、ルート パス コストなど）を持っています。デフォルトでは、すべての VLAN が IST に割り当てられます。

MSTI はリージョンにローカルです。たとえばリージョン A およびリージョン B が相互接続されていても、リージョン A の MSTI 1 は、リージョン B の MSTI 1 に依存しません。

- Common and Internal Spanning-Tree（CIST）は、各 MST リージョン内の IST と、MST リージョンおよびシングル スパニングツリーを相互接続する Common Spanning-Tree（CST）の集合です。

  1 つのリージョン内で計算されたスパニングツリーは、スイッチド ドメイン全体を網羅する CST のサブツリーと見なされます。CIST は、IEEE 802.1w、IEEE 802.1s、および IEEE 802.1D 標準をサポートするスイッチ間で実行されるスパニングツリーアルゴリズムによって形成されます。MST リージョン内の CIST は、リージョン外の CST と同じです。

MST リージョン内の動作

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（IEEE 802.1s 標準が実装される以前は *IST* マスターと呼ばれた）になります。これは、リージョン内で最も小さいdevice ID、および CIST ルートに対するパス コストをもつdeviceです。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 ルートがリージョンの外部にある場合、リージョンの境界に位置する MSTP 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。

MSTP deviceは初期化時に、自身が CIST のルートおよび CIST リージョナル ルートであることを主張するために CIST ルートと CIST リージョナル ルートへのパス コストがいずれもゼロに設定された BPDU を送信します。deviceはすべての MSTI を初期化し、そのすべてのルートであることを主張します。deviceは、ポート用に現在保存されているものより上位の MST ルート情報（低いdevice ID、低いパス コストなど）を受信した場合、CIST リージョナル ルートとしての主張を放棄します。

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、優位の IST 情報を受信すると、古いサブリージョンを脱退して、真の CIST リージョナル ルートが含まれている新しいサブリージョンに加入します。真の CIST リージョナル ルートが含まれている以外のサブリージョンは、すべて縮小します。

正常な動作のためには、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。共通の CIST リージョナル ルートに収束する場合、そのリージョン内にある 2 つのスイッチは、1 つの MST インスタンスに対するポートの役割のみを同期させます。

関連トピック

MST リージョンの図 （41 ページ）

MST リージョン間の動作

ネットワーク内に複数のリージョンまたはレガシー IEEE 802.1D devicesが混在している場合、MSTP は、ネットワーク内のすべての MST リージョンとすべてのレガシー STP devicesから構

成される CST を構築して保持します。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 devicesを接続し、スイッチド ドメイン全体を囲む CIST のサブツリーとして認識されます。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 deviceおよび MST リージョンへの仮想devicesとして認識されます。

CST インスタンスのみが BPDU を送受信し、MST インスタンスはスパニングツリー情報を BPDU に追加して隣接するdevicesと相互作用し、最終的なスパニングツリー トポロジーを算出します。したがって、BPDU 伝送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 インスタンスだけで設定されますが、その影響はすべての MST インスタンスに及びます。スパニングツリー トポロジに関連するパラメータ（device 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 MST インスタンスの両方で設定できます。

MSTP devicesは、バージョン 3 RSTP BPDU または IEEE 802.1D STP BPDU を使用して、レガシー IEEE 802.1D devicesと通信します。MSTP devicesは、MSTP BPDU を使用して MSTP devices と通信します。

関連トピック

MST リージョンの図 （41 ページ）

IEEE 802.1s の用語

シスコの先行標準実装で使用される一部のMST命名規則は、一部の内部パラメータまたはリージョンパラメータを識別するように変更されました。これらのパラメータは、ネットワーク全体に関連している外部パラメータと違い、MST リージョン内でのみ影響があります。CIST はネットワーク全体を網羅するスパニングツリー インスタンスのため、CIST パラメータのみ、内部修飾子やリージョナル修飾子ではなく外部修飾子が必要です。

- CISTルートは、ネットワーク全体を網羅する一意のインスタンスのためのルート device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 への単一deviceと見なすことに注意してください。CIST 外部ルート パス コストは、これらの仮想devices、およびどのリージョンにも属さないdevicesの間で算出されるルート パス コストです。
- CIST リージョナル ルートは、準規格の実装で IST マスターと呼ばれていました。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。CIST ルートがリージョン内にない場合、CIST リージョナル ルートは、リージョン内の CIST ルートに最も近いdeviceです。CIST リージョナル ルートは、IST のルート device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。

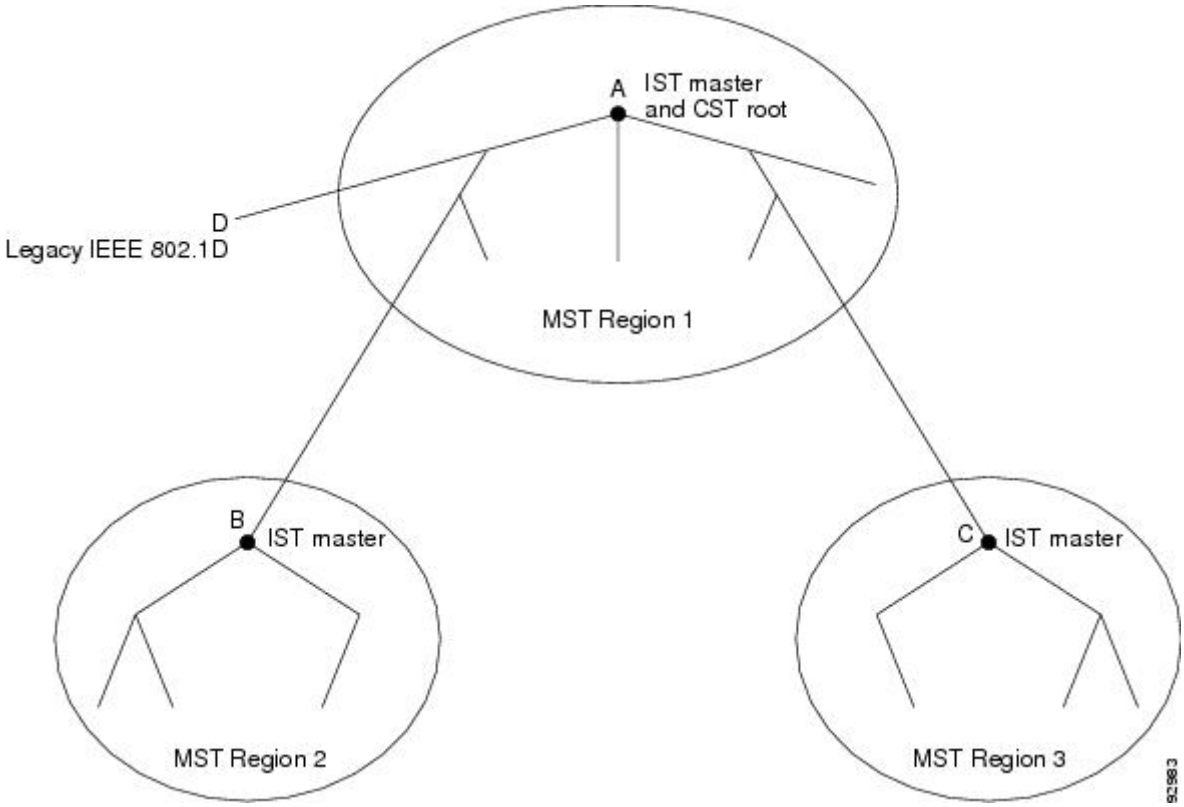
表 *6 :* 準規格と規格の用語

IEEE 標準	シスコ先行標準	シスコ標準
CIST リージョナル ルート	IST マスター	CIST リージョナル ルート
CIST 内部ルート パス コスト	IST マスター パス コスト	CIST 内部パス コスト
CIST 外部ルート パス コスト	ルート パス コスト	ルート パス コスト
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

MST リージョンの図

この図は、3 個の MST リージョンとレガシー IEEE 802.1D device（D）を示しています。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。RSTP はすべてのリージョンで稼働しています。

図 *5 : MST* リージョン、*CIST* マスター、および *CST* ルート



関連トピック

MST リージョン （37 ページ）
MST リージョン内の動作 （39 ページ）
MST リージョン間の動作 （39 ページ）

ホップ カウント

IST および MST インスタンスは、スパニングツリー トポロジの計算に、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 タイムの情報を使用しません。その代わりに、IP Time To Live（TTL）メカニズムに似た、ルートまでのパス コストおよびホップ 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、領域内で最大ホップ カウントを設定し、その領域の 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 カウントを設定すると、メッセージ エージ情報を設定するのと同様の結果が得られます（再構成の開始時期を決定します）。インスタンスのルート device は、コストが 0 でホップ カウントが最大値に設定されている BPDU（M レコード）を常に送信します。device は、この BPDU を受信すると、受信した残りのホップ カウントから 1 を引き、生成する BPDU で残りのホップ カウントとしてこの値を伝播します。カウントがゼロに達すると、device は BPDU を廃棄し、ポート用に維持されている情報を期限切れにします。

BPDU の RSTP 部分に格納されているメッセージ有効期間と最大エージング タイムの情報は、リージョン全体で同じままであり、そのリージョンの境界に位置する指定ポートによって同じ値が伝播されます。

境界ポート

シスコ先行標準の実装では、境界ポートは、RSTP が稼働する単一のスパニングツリー リージョン、PVST+ または Rapid PVST+ が稼働する単一のスパニングツリー リージョン、または異なる MST コンフィギュレーションを持つ別の MST リージョンに MST リージョンを接続します。境界ポートは、LAN、単一のスパニングツリー device または MST 設定が異なる device の指定 device にも接続します。

IEEE 802.1s 標準では、境界ポートの定義はなくなりました。IEEE 802.1Q-2002 標準では、ポートが受信できる 2 種類のメッセージを識別します。

- 内部（同一リージョンから）
- 外部（別のリージョンから）

メッセージが内部の場合、CIST の部分は CIST によって受信されるので、各 MST インスタンスは個々の M レコードだけを受信します。

メッセージが外部である場合、CIST だけが受信します。CIST の役割がルートや代替ルートの場合、または外部 BPDU のトポロジが変更された場合は、MST インスタンスに影響する可能性があります。

MST リージョンには、devicesおよびLANの両方が含まれます。セグメントは、DPのリージョンに属します。そのため、セグメントの指定ポートではなく異なるリージョンにあるポートは境界ポートになります。この定義では、リージョン内部の2つのポートが、別のリージョンに属するポートとセグメントを共有し、内部メッセージおよび外部メッセージの両方を 1 つのポートで受信できるようになります。

シスコ先行標準の実装との主な違いは、STP互換モードを使用している場合、指定ポートが境界ポートとして定義されない点です。

（注） レガシー STP deviceがセグメントに存在する場合、メッセージは常に外部と見なされます。

シスコ先行標準の実装から他に変更された点は、送信device ID を持つ RSTP またはレガシー IEEE 802.1Q deviceの部分に、CIST リージョナル ルート device ID フィールドが加えられたことです。リージョン全体は、一貫した送信者device ID をネイバー devicesに送信し、単一仮想deviceのように動作します。この例では、A または B がセグメントに指定されているかどうかに関係なく、ルートの一貫した送信者device ID が同じである BPDU をdevice C が受信します。

IEEE 802.1s の実装

シスコの IEEE MST 標準の実装には、標準の要件を満たす機能だけでなく、すでに公開されている標準には含まれていない一部の（要望されている）先行標準の機能が含まれています。

ポートの役割名の変更

境界の役割は最終的に MST 標準に含まれませんでしたが、境界の概念自体はシスコの実装に投影されています。ただし、リージョン境界にある MST インスタンスのポートは、対応するCISTポートのステートに必ずしも従うわけではありません。現在、2つの境界の役割が存在しています。

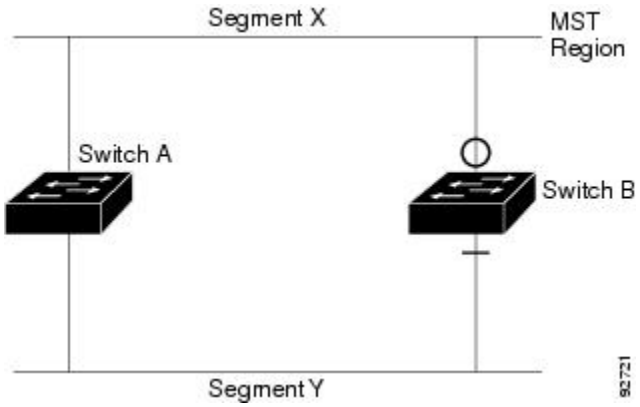
- 境界ポートが CIST リージョナル ルートのルート ポートである場合：CIST インスタンス ポートを提案されて同期中の場合、対応するすべての MSTI ポートの同期を取り終わった後であれば（その後フォワーディングします）、その場合のみ合意を返信してフォワーディング ステートに移行できます。MSTI ポートには、特別なマスターの役割があります。
- 境界ポートが CIST リージョナル ルートのルート ポートでない：MSTI ポートは、CIST ポートのステートおよび役割に従います。標準では提供される情報が少ないため、MSTI ポートが BPDU（M レコード）を受信しない場合、MSTI ポートが BPDU を代わりにブロックできる理由がわかりにくい場合があります。この場合、境界の役割自体は存在していませんが、**show** コマンドで見ると、出力される *type* カラムで、ポートが境界ポートとして認識されていることがわかります。

レガシーおよび規格Devicesの相互運用

準規格devicesの自動検出はエラーになることがあるので、インターフェイス コンフィギュレーション コマンドを使用して準規格ポートを識別できます。deviceの規格と準規格の間にリージョンを形成することはできませんが、CIST を使用して相互運用することができます。このような特別な方法を採用しても、失われる機能は、異なるインスタンス上のロードバランシングだけです。ポートが先行標準の BPDU を受信すると、CLI（コマンドライン インターフェイス）にはポートの設定に応じて異なるフラグが表示されます。deviceが準規格 BPDU 送信用に設定されていないポートで準規格 BPDU を初めて受信したときは、Syslog メッセージも表示されます。

図 *6:* 規格および準規格のデバイスの相互運用

A が規格のdeviceで、B が準規格のdeviceとして、両方とも同じリージョンに設定されているとします。A は CIST のルート device です。B のセグメント X にはルートポート（BX）、セグメント Y には代替ポート（BY）があります。セグメント Y がフラップして BY のポートが代替になってから準規格 BPDU を 1 つ送信すると、AY は準規格 device が Y に接続されていることを検出できず、規格 BPDU の送信を続けます。ポート BY は境界に固定され、A と B との間でのロード ランシングは不可能になります。セグメント X にも同じ問題がありますが、B はトポロジの変更であれば送信する場合があります。



（注） 規格 MST 実装と準規格 MST 実装間の相互作用を最低限に抑えることを推奨します。

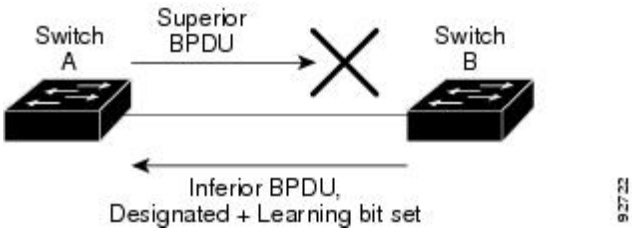
単一方向リンク障害の検出

IEEE MST 標準にはこの機能が存在していませんが、Cisco IOS Release には加えられています。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、その役割を維持しますが、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。

図 7: 単一方向リンク障害の検出

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。デバイス A はルートdeviceであり、device B へのリンクで BPDU は失われます。RSTP および MST BPDU には、送信側ポートの役割と状態が含まれます。device A はこの情報を使用し、ルータ A が送信する上位 BPDU にdevice B が反応しないこと、およびdevice B がルート deviceではなく指定ブリッジであることを検出できます。この結果、device 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。



MSTP およびデバイス スタック

device スタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが与えられたスパニングツリーに同一のブリッジ ID を使用します。ブリッジ ID は、active switchの MAC アドレスから取得されます。

MSTP をサポートしていないdeviceが、MSTP またはリバースをサポートしているdevice スタックに追加されると、deviceはバージョンが不一致の状態になります。可能な場合、deviceは、device スタックで実行中のソフトウェアと同じバージョンに自動的にアップグレードまたはダウングレードされます。

IEEE 802.1D STP との相互運用性

MSTP が稼働しているdeviceは、IEEE 802.1D 準拠のレガシー devicesとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このdeviceは、レガシー IEEE 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）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MSTP device は、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信することによって、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、deviceが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシー deviceが指定deviceでない限り、レガシー deviceがリンクから削除されたかどうか検出できないためです。このdeviceが接続するdeviceがリージョンに加入していると、deviceはポートに境界の役割を割り当て続ける場合があります。プロトコル移行プロセスを再開するには（強制的にネイバー devices と再びネゴシエーションするには）、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンク上のすべてのレガシー devicesが RSTP devicesであれば、これらのスイッチは、RSTP BPDU 同様に MSTP BPDU を処理できます。したがって、MSTP devicesは、バージョン 0 コンフィギュレーションと TCN BPDU またはバージョン 3 MSTP BPDU のいずれかを境界ポートで

送信します。境界ポートは、LAN、単一スパニングツリー deviceまたは MST 設定が異なる deviceのいずれかの指定のdeviceに接続します。

RSTP 概要

RSTP は、ポイントツーポイントの配線を利用して、スパニングツリーの高速コンバージェンスを実現します。また、1 秒未満の間に、スパニングツリーを再構成できます（IEEE 802.1D スパニングツリーのデフォルトに設定されている 50 秒とは異なります）。

ポートの役割およびアクティブ トポロジ

RSTP は、ポートに役割を割り当てて、アクティブ トポロジを学習することによって高速コンバージェンスを実現します。RSTP は device をルート deviceとして最も高いdevice プライオリティ（プライオリティの数値が一番小さい）に選択するために、IEEE 802.1D STP 上に構築されます。RSTP は、次のうちいずれかのポートの役割をそれぞれのポートに割り当てます。

- ルート ポート：device がルートdevice にパケットを転送するとき、最適なパス（最低コスト）を提供します。
- 指定ポート：指定deviceに接続し、その LAN からルート deviceにパケットを転送するとき、パス コストを最低にします。DP は、指定deviceが LAN に接続されているポートです。
- 代替ポート：現在のルート ポートが提供したパスに代わるルート deviceへの代替パスを提供します。
- 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 ポートは、2 つのポートがループバック内でポイントツーポイント リンクによって接続されるか、共有 LAN セグメントとの複数の接続がdeviceにある場合に限って存在できます。
- 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役割が与えられていません。

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 ポートのロールがあるポートは、アクティブ トポロジから除外されます。

ネットワーク全体のポートの役割に矛盾のない安定したトポロジでは、RSTPは、すべてのルート ポートおよび指定ポートがただちにフォワーディング ステートに移行し、代替ポートとバックアップ ポートが必ず廃棄ステート（IEEE 802.1D のブロッキング ステートと同じ）になるように保証します。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。

表 7: ポート ステートの比較

運用ステータス	STP ポート ステート（IEEE 802.1D）	RSTP ポート ステート	ポートがアクティブ トポロジに含まれているか
イネーブル	ブロッキング	廃棄	いいえ

運用ステータス	STP ポート ステート（IEEE 802.1D）	RSTP ポート ステート	ポートがアクティブトポロジに含まれているか
イネーブル	リスニング	廃棄	いいえ
イネーブル	ラーニング	ラーニング	はい
イネーブル	転送	転送	はい
ディセーブル	ディセーブル	廃棄	いいえ

Cisco STP の実装との一貫性を保つため、このマニュアルでは、ポート ステートを廃棄ではなくブロッキングとして定義します。DP はリスニング ステートから開始します。

高速コンバージェンス

RSTP は、device、device ポート、LAN のうちいずれかの障害のあと、接続の高速回復を提供します。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：**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して RSTP deviceでエッジポートとしてポートを設定した場合、エッジポートはフォワーディング ステートにすぐに移行します。エッジ ポートは Port Fast 対応ポートと同じであり、単一エンドステーションに接続しているポートだけでイネーブルにする必要があります。
- ルート ポート：RSTP は、新しいルート ポートを選択した場合、古いルート ポートをブロックし、新しいルート ポートをフォワーディング ステートにすぐに移行します。
- 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。

図 *8*：高速コンバージェンスの提案と合意のハンドシェイク

デバイス A がデバイス B にポイントツーポイント リンクで接続され、すべてのポートはブロッキング ステートになっています。デバイス A の優先度がデバイス B の優先度よりも数値的に小さいとします。デバイス A は提案メッセージ（提案フラグを設定した設定 BPDU）をデバイス B に送信し、指定deviceとしてそれ自体を提案します。

デバイス B は、提案メッセージの受信後、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、エッジ以外のすべてのポートを強制的にブロッキング ステートにして、新しいルート ポートを介して合意メッセージ（合意フラグを設定した BPDU）を送信します。

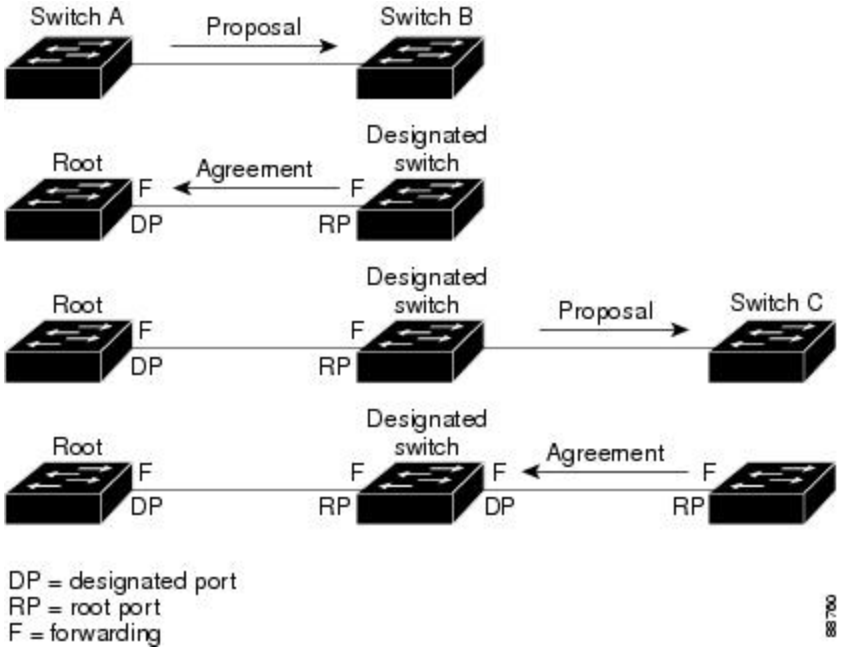
デバイス A も、デバイス B の合意メッセージの受信後、指定ポートをフォワーディング ステートにすぐに移行します。デバイス B はすべてのエッジ以外のポートをブロックし、

Devices A およびルータ B の間にポイントツーポイント リンクがあるので、ネットワークにループは形成されません。

デバイス C がデバイス B に接続すると、同様のセットのハンドシェーク メッセージが交換されます。デバイス C はデバイス B に接続されているポートをルート ポートとして選択し、両端がフォワーディング ステートにすぐに移行します。このハンドシェーク処理を繰り返して、もう 1 つのdeviceがアクティブ トポロジーに加わります。ネットワークが収束すると、この提案/合意ハンドシェイクがルートからスパニングツリーのリーフへと進みます。

device スタックでは、Cross-Stack Rapid Transition（CSRT）機能を使用すると、ポートがフォワーディング ステートに移行する前に、スタック メンバで、提案/合意ハンドシェイク中にすべてのスタック メンバーから確認メッセージを受信できます。deviceが MST モードの場合、CSRT は自動的に有効にされます。

deviceはポートのデュプレックス モードによってリンク タイプを学習します。全二重ポートはポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。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には、**spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを入力します。



ポート ロールの同期

deviceがそのルータのポートの 1 つ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、RSTP によってその他すべてのポートが新しいルートの情報と強制的に同期化します。

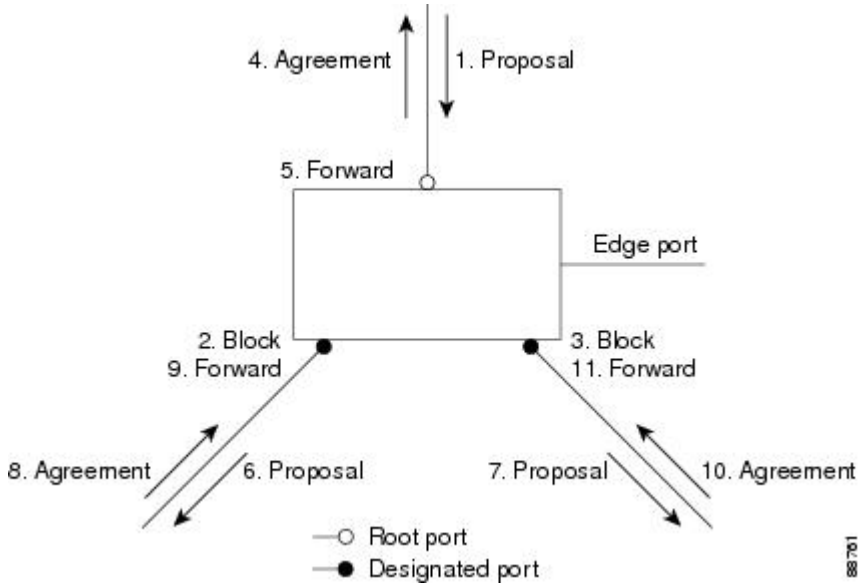
その他すべてのポートが同期化されている場合、deviceはルート ポートで受信した上位ルート情報で同期化されます。deviceのそれぞれのポートは、次のような場合に同期化します。

- 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）。

指定ポートがフォワーディング ステートでエッジ ポートとして設定されていない場合、RSTP によって新しいルート情報と強制的に同期されると、その指定ポートはブロッキング ステートに移行します。一般的に RSTP がルート情報でポートを強制的に同期化し、ポートが上の条件を満たしていない場合、そのポート ステートはブロッキングに設定されます。

図 *9*：高速コンバージェンス中のイベントのシーケンス

deviceは、すべてのポートが同期化されたことを確認した後で、ルート ポートに対応する指定deviceに合意メッセージを送信します。ポイントツーポイント リンクで接続されたdevicesがポートの役割で合意すると、RSTP はポート ステートをフォワーディングにすぐに移行します。



ブリッジ プロトコル データ ユニットの形式および処理

RSTP BPDU のフォーマットは、プロトコル バージョンが 2 に設定されている点を除き、IEEE 802.1D BPDU のフォーマットと同じです。新しい 1 バイトのバージョン 1 の Length フィールドは 0 に設定されます。これはバージョン 1 のプロトコルの情報がないことを示しています。

表 *8*：*RSTP BPDU* フラグ

ビット	機能
0	トポロジーの変化（TC）
1	提案

ビット	機能
2 ～ 3: 00 01 10 11	ポートの役割： 不明（Unknown） 代替ポート ルートポート 指定ポート
4	ラーニング
5	転送
6	合意
7	トポロジー変更確認応答（TCA）

送信側deviceは RSTP BPDU の提案フラグを設定し、そのLAN の指定deviceとして自分自身を提案します。提案メッセージのポートの役割は、常に DP に設定されます。

送信側deviceは、RSTP BPDU の合意フラグを設定して以前の提案を受け入れます。合意メッセージ内のポート ロールは、常にルート ポートに設定されます。

RSTP には個別のトポロジ変更通知（TCN）BPDU はありません。TC フラグが使用されて、TC が示されます。ただし、IEEE 802.1D devicesとの相互運用性を保つために、RSTP deviceは TCN BPDU の処理と生成を行います。

ラーニング フラグおよびフォワーディング フラグは、送信側ポートのステートに従って設定されます。

優位 BPDU 情報の処理

ポートに現在保存されているルート情報よりも優位のルート情報（小さいdevice ID、低いパスコストなど）をポートが受け取ると、RSTP は再構成を開始します。ポートが新しいルート ポートとして提案されて選択されると、RSTP は強制的にその他すべてのポートを同期化します。

受信した BPDU が、提案フラグが設定されている RSTP BPDU である場合、deviceはその他すべてのポートが同期化されてから合意メッセージを送信します。BPDU が IEEE 802.1D BPDU の場合、deviceは提案フラグを設定せずに、そのポートの転送遅延タイマーを起動します。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。

ポートで優位の情報が受信されたために、その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、RSTP はそのポートをブロッキング ステートに設定し、合意メッセージは送信しません。DP は、転送遅延タイマーが失効するまで、提案フラグを設定して BPDU を送信し続け、転送遅延タイマーの失効時に、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

指定ポートの役割を持つ下位 BPDU（そのポートに現在保存されている値より大きいdevice ID、高いパスコストなど）を指定ポートが受信した場合、その指定ポートはただちに現在の自身の情報で応答します。

トポロジの変更

ここでは、スパニングツリー トポロジの変更処理について、RSTP と IEEE 802.1D の相違を説明します。

- 検出：IEEE 802.1D では、どのようなブロッキング ステートとフォワーディング ステートとの間の移行でもトポロジの変更が発生しますが、RSTP でトポロジの変更が発生するのは、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場合だけです（トポロジの変更と見なされるのは、接続数が増加する場合だけです）。エッジポートにおけるステート変更は、TC の原因になりません。RSTP deviceは、TC を検出すると、TCN を受信したポートを除く、エッジ以外のすべてのポートで学習した情報を削除します。
- 通知：IEEE 802.1D は TCN BPDU を使用しますが、RSTP は使用しません。ただし、IEEE 802.1D との相互運用性を保つために、RSTP deviceは TCN BPDU の処理と生成を行います。
- 確認：RSTP deviceは、指定ポートで IEEE 802.1D deviceから TCN メッセージを受信した場合、TCA ビットが設定された IEEE 802.1D コンフィギュレーション BPDU で応答します。ただし、IEEE 802.1D deviceに接続されたルート ポートで TC 時間タイマー（IEEE 802.1D のトポロジ変更タイマーと同じ）がアクティブであり、TCA ビットが設定されたコンフィギュレーション BPDU が受信された場合、TC 時間タイマーはリセットされます。

  この処理は、IEEE 802.1D devicesをサポートする目的でのみ必要とされます。RSTP BPDU は TCA ビットが設定されていません。
- 伝播：RSTP deviceは、DP またはルート ポートを介して別のdeviceから TC メッセージを受信すると、エッジ以外のすべての DP、およびルート ポート（TC メッセージを受信したポートを除く）に変更を伝播します。deviceはこのようなすべてのポートで TC-while タイマーを開始し、そのポートで学習した情報を消去します。
- プロトコルの移行：IEEE 802.1D devicesとの下位互換性を保つため、RSTP は IEEE 802.1D コンフィギュレーション BPDU および TCN BPDU をポート単位で必要に応じて送信します。

  ポートが初期化されると、移行遅延タイマーが開始され（RSTP BPDU が送信される最低時間を指定）、RSTP BPDU が送信されます。このタイマーがアクティブである間、device 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。

  deviceはポートの移行遅延タイマーが満了した後に IEEE 802.1D BPDU を受信した場合、IEEE 802.1D deviceに接続されていると想定し、IEEE 802.1D BPDU のみの使用を開始します。ただし、RSTP deviceが 1 つのポートで IEEE 802.1D BPDU を使用していて、タイマーが満了した後に RSTP BPDU を受信した場合、タイマーが再起動し、そのポートで RSTP BPDU の使用が開始されます。

プロトコル移行プロセス

MSTP が稼働しているdeviceは、IEEE 802.1D 準拠のレガシー devicesとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このdeviceは、レガシー IEEE 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）を受信すると、そのポート上ではIEEE 802.1D BPDUのみを送信します。また、MST deviceは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RST BPDU（バージョン 2）を受信することによって、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、deviceが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシー deviceが指定deviceでない限り、レガシー deviceがリンクから削除されたかどうか検出できないためです。また、接続するdeviceがリージョンに加入していると、deviceはポートに境界の役割を割り当て続ける場合があります。

関連トピック

プロトコルの移行プロセスの再開 （69 ページ）

MSTP のデフォルト設定

表 *9 : MSTP* のデフォルト設定

機能	デフォルト設定
スパニングツリー モード	MSTP
デバイス プライオリティ（CIST ポートごとに設定可能）	32768
スパニングツリー ポート プライオリティ（CIST ポート単位で設定可能）	128
スパニングツリー ポート コスト（CIST ポート単位で設定可能）	1000 Mb/s：20000 100 Mb/s：20000 10 Mb/s：20000 1000 Mb/s：20000 100 Mb/s：20000 10 Mb/s：20000
hello タイム	3 秒
転送遅延時間	20 秒
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

関連トピック

サポートされるスパニングツリー インスタンス （13 ページ）
MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）

MSTP 機能の設定方法

MST リージョン設定の指定と MSTP のイネーブル化

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。

リージョンには、MST設定が同一である、1 つ以上のメンバーを含めることができます。各メンバーでは、RSTP BPDU を処理できる必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリーインスタンスの数は 65 までです。VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst configuration** 例： `デバイス(config)# spanning-tree mst configuration`	MST 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	**instance** *instance-id* **vlan** *vlan-range* 例： `デバイス(config-mst)# instance 1 vlan 10-20`	VLAN を MSTI にマップします。 • *instance-id* に指定できる範囲は、0 ～ 4094 です。

	コマンドまたはアクション	目的
		• **vlan** *vlan-range* に指定できる範囲は、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、ハイフンを使用します。たとえば **instance 1 vlan 1-63** では、VLAN 1 ～ 63 が MSTI 1 にマップされます。 VLAN を列挙して指定する場合は、カンマを使用します。たとえば **instance 1 vlan 10, 20, 30** と指定すると、VLAN 10、20、30 が MST インスタンス 1 にマッピングされます。
ステップ 5	**name** *name* 例： `デバイス(config-mst)# name region1`	コンフィギュレーション名を指定します。*name* 文字列の最大の長さは 32 文字であり、大文字と小文字が区別されます。
ステップ 6	**revision** *version* 例： `デバイス(config-mst)# revision 1`	設定リビジョン番号を指定します。指定できる範囲は 0 ～ 65535 です。
ステップ 7	**show pending** 例： `デバイス(config-mst)# show pending`	保留中の設定を表示し、設定を確認します。
ステップ 8	**exit** 例： `デバイス(config-mst)# exit`	すべての変更を適用し、グローバルコンフィギュレーションモードに戻ります。
ステップ 9	**spanning-tree mode mst** 例： `デバイス(config)# spanning-tree mode mst`	MSTP をイネーブルにします。RSTP もイネーブルになります。 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は以前のモードであるため停止

	コマンドまたはアクション	目的
		し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。 MSTP と PVST+ または MSTP と Rapid PVST+ を同時に実行することはできません。
ステップ 10	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

関連トピック

- MSTP 設定時の注意事項 （36 ページ）
- MST リージョン （37 ページ）
- MSTP の前提条件 （33 ページ）
- MSTP の制約事項 （34 ページ）
- スパニングツリーの相互運用性と下位互換性 （13 ページ）
- オプションのスパニングツリー設定時の注意事項
- BackboneFast （80 ページ）
- UplinkFast （75 ページ）
- MSTP のデフォルト設定 （52 ページ）
- ルート デバイスの設定 （55 ページ）
- ブリッジ ID、デバイス プライオリティ、および拡張システム ID
- セカンダリ ルートの設定デバイス （57 ページ）
- ポート プライオリティの設定 （58 ページ）
- パス コストの設定 （60 ページ）
- デバイス プライオリティの設定 （61 ページ）
- hello タイムの設定 （63 ページ）
- 転送遅延時間の設定 （64 ページ）
- 最大エージング タイムの設定 （65 ページ）
- 最大ホップ カウントの設定 （66 ページ）
- 高速移行を確実にするためのリンク タイプの指定 （67 ページ）
- ネイバー タイプの設定 （68 ページ）
- プロトコルの移行プロセスの再開 （69 ページ）

ルート デバイスの設定

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、deviceで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定されたMSTインスタンスIDも把握する必要があります。この例のステップ2では、インスタンスIDとして0を使用します。これは「関連項目」で示されている手順によって設定されたインスタンスIDが0であるためです。

手順

	コマンドまたはアクション	目的
ステップ1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ3	**spanning-tree mst** *instance-id* **root primary** 例： `デバイス(config)# spanning-tree mst 0 root primary`	ルート deviceとしてdeviceを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
ステップ4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ルート スイッチ （37 ページ）
MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）
MSTP の制約事項 （34 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID
セカンダリ ルートの設定デバイス （57 ページ）

セカンダリ ルートの設定デバイス

拡張システム ID をサポートするdeviceをセカンダリ ルートとして設定する場合、device プライオリティはデフォルト値（32768）から 28672 に修正されます。プライマリ ルート deviceで障害が発生した場合は、このdeviceが指定インスタンスのルート deviceになる可能性があります。ここでは、その他のネットワーク devicesが、デフォルトのdevice プライオリティの 32768 を使用しているためにルート deviceになる可能性が低いことが前提となっています。

このコマンドを複数のdeviceに対して実行すると、複数のバックアップ ルート devicesを設定できます。**spanning-tree mst** *instance-id* **root primary** グローバル コンフィギュレーション コマンドでプライマリルート device を設定したときと同じネットワーク直径および hello タイム値を使用してください。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、deviceで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID も把握する必要があります。この例では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst** *instance-id* **root secondary** 例： `デバイス(config)# spanning-tree mst 0 root secondary`	セカンダリ ルート deviceとしてdeviceを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）
ルート デバイスの設定 （55 ページ）

ポート プライオリティの設定

ループが発生した場合、MSTP はポート プライオリティを使用して、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。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）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に同じプライオリティ値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

（注） device が device スタックのメンバーの場合、**spanning-tree mst** [*instance-id*] **port-priority** *priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree mst** [*instance-id*] **cost** *cost* インターフェイス コンフィギュレーション コマンドを使用し、フォワーディング ステートにするインターフェイスを選択する必要があります。最初に選択させたいポートには、より小さいコスト値を割り当て、最後に選択させたいポートには、より大きいコスト値を割り当てることができます。詳細については、関連項目の下に表示されるパス コストのトピックを参照してください。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、deviceで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連トピック」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： デバイス(config)# **interface GigabitEthernet1/0/1**	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	**spanning-tree mst** *instance-id* **port-priority** *priority* 例： デバイス(config-if)# **spanning-tree mst 0 port-priority 64**	ポート プライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *priority* 値の範囲は 0 ～ 240 で、16 ずつ増加します。デフォルト値は 128 です。値が小さいほど、プライオリティが高くなります。 使用可能な値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 だけです。その他の値はすべて拒否されます。
ステップ 5	**end** 例： デバイス(config-if)# **end**	特権 EXEC モードに戻ります。

show spanning-tree mst interface *interface-id* 特権 EXEC コマンドで情報が表示されるのは、ポートがリンクアップ動作可能の状態にある場合に限られます。そうでない場合は、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）
パス コストの設定 （60 ページ）

パス コストの設定

MSTP 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に基づきます。ループが発生した場合、MSTP 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。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択される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。すべてのインターフェイスに同じコスト値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、deviceで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連項目」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順

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

	コマンドまたはアクション	目的
	デバイス(config)# **interface gigabitethernet1/0/1**	ンモードを開始します。有効なインターフェイスには、物理ポートとポートチャネル論理インターフェイスがあります。指定できるポートチャネルの範囲は1～48です。
ステップ4	**spanning-tree mst** *instance-id* **cost** *cost* 例： デバイス(config-if)# **spanning-tree mst 0 cost 17031970**	コストを設定します。 ループが発生した場合、MSTP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。低いパス コストは高速送信を表します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ5	**end** 例： デバイス(config-if)# **end**	特権 EXEC モードに戻ります。

show spanning-tree mst interface *interface-id* 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

ポート プライオリティの設定 （58 ページ）
MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）

デバイス プライオリティの設定

deviceのプライオリティを変更すると、スタンドアロンdeviceまたはスタック内のdeviceであるかに関係なく、ルートdeviceとして選択される可能性が高くなります。

（注） このコマンドの使用には注意してください。通常のネットワーク設定では、**spanning-tree mst** *instance-id* **root primary** および **spanning-tree mst** *instance-id* **root secondary** 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、deviceをルートまたはセカンダリルートdeviceとして指定することをお勧めします。これらのコマンドが動作しない場合にのみdeviceプライオリティを変更する必要があります。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、deviceで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

使用する指定されたMSTインスタンスIDも把握する必要があります。この例では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst** *instance-id* **priority** *priority* 例： `デバイス(config)# spanning-tree mst 0 priority 40960`	deviceのプライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。 • *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。この値が低いほど、deviceがルート deviceとして選択される可能性が高くなります。

	コマンドまたはアクション	目的
		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。これらは唯一の許容値です。
ステップ 4	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）

hello タイムの設定

hello タイムはルート deviceによって設定メッセージが生成されて送信される時間の間隔です。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、deviceで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst hello-time** *seconds* 例：	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 deviceによって設定メッセージ

	コマンドまたはアクション	目的
	デバイス(config)# **spanning-tree mst hello-time 4**	が生成されて送信される時間の間隔です。このメッセージは、deviceが活動中であることを表します。 *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 3 です。
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）

転送遅延時間の設定

始める前に

マルチ スパニングツリー（MST）が、deviceで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst forward-time** *seconds* 例： デバイス(config)# **spanning-tree mst forward-time 25**	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。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、ポートが待機する秒数です。

	コマンドまたはアクション	目的
		seconds に指定できる範囲は 4 ～ 30 です。デフォルトは 20 です。
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）

最大エージング タイムの設定

始める前に

マルチ スパニングツリー（MST）が、deviceで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst max-age** *seconds* 例： `デバイス(config)# spanning-tree mst max-age 40`	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。最大エージング タイムは、deviceが再設定を試す前にスパニングツリー設定メッセージを受信せずに待機する秒数です。 *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）

最大ホップ カウントの設定

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、deviceで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst max-hops** *hop-count* 例： `デバイス(config)# spanning-tree mst max-hops 25`	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* に指定できる範囲は 1 ～ 255 です。デフォルト値は 20 です。
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）

高速移行を確実にするためのリンク タイプの指定

ポイントツーポイント リンクでポート間を接続し、ローカル ポートが DP になると、RSTP は提案と合意のハンドシェークを使用して別のポートと高速移行をネゴシエーションし、ループがないトポロジを保証します。

デフォルトの場合、リンク タイプ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、半二重ポートは共有接続と見なされます。MSTP を実行しているリモート deviceの単一ポートに、半二重リンクを物理的にポイントツーポイントで接続した場合は、リンク タイプのデフォルト設定を無効にして、フォワーディング ステートへの高速移行をイネーブルにすることができます。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、deviceで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連項目」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `デバイス(config)# interface GigabitEthernet1/0/1`	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。有効なインターフェイスには、物理ポート、VLAN、およびポート チャネル論理インターフェ

	コマンドまたはアクション	目的
		イスがあります。VLAN ID の範囲は 1 ～ 4094 です。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 4	**spanning-tree link-type point-to-point** 例： `デバイス(config-if)# spanning-tree link-type point-to-point`	ポートのリンク タイプがポイントツーポイントであることを指定します。
ステップ 5	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）

ネイバー タイプの設定

トポロジには、先行標準に準拠したデバイスと IEEE 802.1s 標準準拠のデバイスの両方を加えることができます。デフォルトの場合、ポートは準規格デバイスを自動的に検出できますが、規格 BPDU および準規格 BPDU の両方を受信できます。デバイスとそのネイバーの間に不一致がある場合は、CIST だけがインターフェイスで動作します。

準規格 BPDU だけを送信するようにポートを設定できます。先行標準のフラグは、ポートが STP 互換モードにある場合でも、すべての **show** コマンドで表示されます。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、deviceで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `デバイス(config)# interface GigabitEthernet1/0/1`	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。有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	**spanning-tree mst pre-standard** 例： `デバイス(config-if)# spanning-tree mst pre-standard`	ポートが準規格 BPDU だけを送信できることを指定します。
ステップ 5	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）

プロトコルの移行プロセスの再開

この手順では、プロトコル移行プロセスを再開し、ネイバーdevicesとの再ネゴシエーションを強制します。また、deviceを MST モードに戻します。これは、IEEE 802.1D BPDU の受信後にdeviceがそれらを受信しない場合に必要です。

deviceでプロトコルの移行プロセスを再開する（隣接するdevicesで再ネゴシエーションを強制的に行う）手順については、これらの手順に従ってください。

始める前に

マルチ スパニングツリー（MST）が、deviceで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

コマンドのインターフェイス バージョンを使用する場合は、使用する MST インターフェイスが分かっている必要があります。この例では、インターフェイスとして GigabitEthernet1/0/1 を使用します。それが「関連項目」で示されている手順によって設定されたインターフェイスであるからです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	次のいずれかのコマンドを入力します。 • **clear spanning-tree detected-protocols** • **clear spanning-tree detected-protocols interface** *interface-id* 例： デバイス# **clear spanning-tree detected-protocols** または デバイス# **clear spanning-tree detected-protocols interface GigabitEthernet1/0/1**	deviceが MSTP モードに戻り、プロトコルの移行プロセスが再開されます。

次のタスク

この手順は、deviceでさらにレガシー IEEE 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 に設定された BPDU）を受信する場合に、繰り返しが必要なことがあります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）
プロトコル移行プロセス （52 ページ）

MSTP に関する追加情報

関連資料

関連項目	マニュアル タイトル
スパニング ツリー プロトコル コマンド	*LAN Switching Command Reference, Cisco IOS XE Release 3SE（Catalyst 3650 Switches）*

標準および RFC

標準/RFC	タイトル
なし	—

MIB

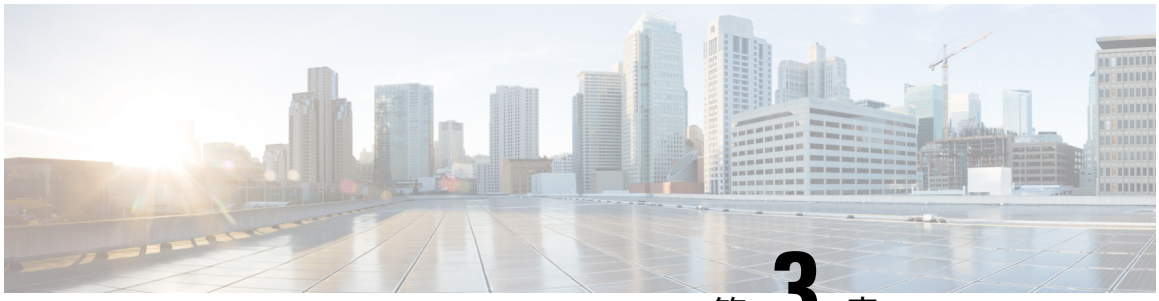
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

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

MSTP の機能情報

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



第 3 章

オプションのスパニングツリー機能の設定

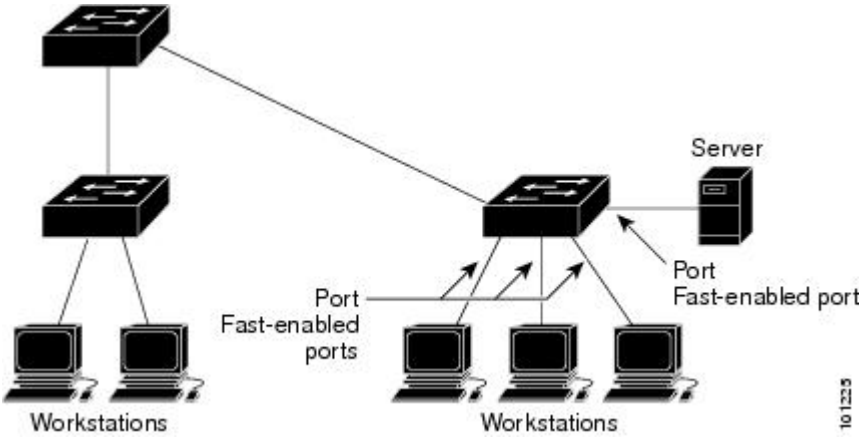
オプションのスパニングツリー機能について

PortFast

PortFast機能を使用すると、アクセス ポートまたはトランク ポートとして設定されているインターフェイスが、リスニング ステートおよびラーニング ステートを経由せずに、ブロッキング ステートから直接フォワーディング ステートに移行します。

図 *10 : PortFast* が有効なインターフェイス

1 台のワークステーションまたはサーバに接続されているインターフェイス上で PortFast を使用すると、スパニングツリーが収束するのを待たずにデバイスをすぐにネットワークに接続できます。



1 台のワークステーションまたはサーバに接続されたインターフェイスがブリッジプロトコル データ ユニット（BPDU）を受信しないようにする必要があります。スイッチを再起動すると、PortFast が有効に設定されているインターフェイスは通常のスパニングツリー ステータスの遷移をたどります。

インターフェイスまたはすべての非トランク ポートで有効にして、この機能を有効にできます。

関連トピック

PortFast のイネーブル化 （84 ページ）
オプションのスパニング ツリー機能の制約事項

BPDU ガード

ブリッジプロトコルデータユニット（BPDU）ガード機能はスイッチ上でグローバルにイネーブルにすることも、ポート単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

PortFast エッジ対応ポート上でグローバル レベルで BPDU ガードをイネーブルにすると、スパニング ツリーは、BPDU が受信されると、PortFast エッジ動作ステートのポートをシャット ダウンします。有効な設定では、PortFast エッジ対応ポートは BPDU を受信しません。PortFast エッジ対応ポートが BPDU を受信した場合は、許可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってポートは error-disabled ステートになります。この状態になると、スイッチは違反が発生したポート全体をシャットダウンします。

PortFast エッジ機能をイネーブルにせずにインターフェイス レベルでポート上の BPDU ガードをイネーブルにした場合、ポートが BPDU を受信すると、error-disabled ステートになります。

インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でアクセス ポートがスパニングツリーに参加しないようにするには、BPDU ガード機能を使用します。

関連トピック

BPDU ガードのイネーブル化 （86 ページ）

BPDU フィルタリング

BPDU フィルタリング機能はスイッチ上でグローバルにイネーブルにすることも、インターフェイス単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルでは、PortFast エッジ対応インターフェイスで BPDU フィルタリングをイネーブルにすると、PortFast エッジ動作ステートにあるインターフェイスでの BPDU の送受信が防止されます。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。PortFast エッジ対応インター

フェイスでは、BPDU を受信すると、PortFast エッジ動作ステートが解除され、BPDU フィルタリングがディセーブルになります。

PortFastエッジ機能をイネーブルにせずに、インターフェイスでBPDUフィルタリングをイネーブルにすると、インターフェイスでの BPDU の送受信が防止されます。

注意 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ことは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリーループが発生することがあります。

スイッチ全体または1つのインターフェイスでBPDUフィルタリング機能をイネーブルにできます。

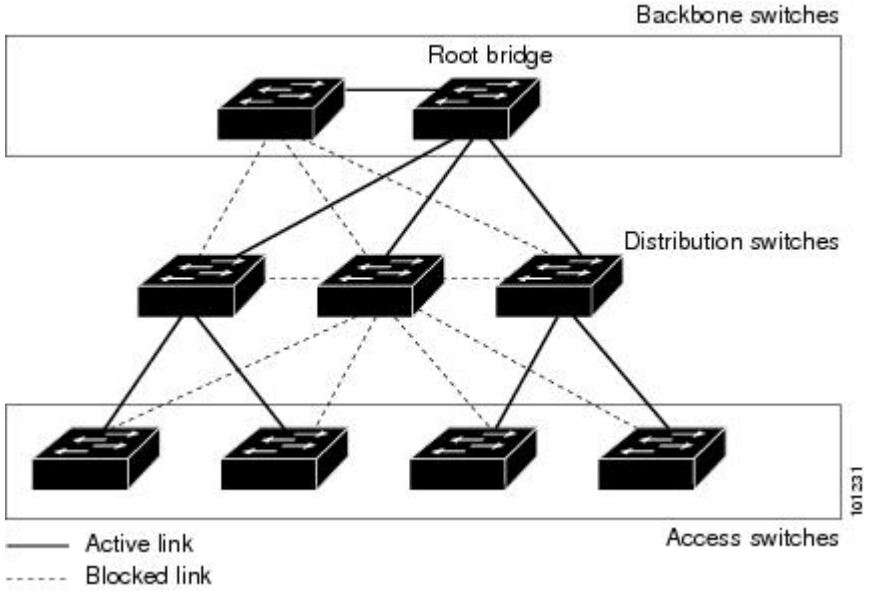
関連トピック

BPDU フィルタリングのイネーブル化 （88 ページ）

UplinkFast

図 *11* : 階層型ネットワークのスイッチ

階層型ネットワークに配置されたスイッチは、バックボーン スイッチ、ディストリビューション スイッチ、およびアクセス スイッチに分類できます。この複雑なネットワークには、ディストリビューション スイッチとアクセス スイッチがあり、ループを防止するために、スパニング ツリーがブロックする冗長リンクが少なくとも 1 つあります。



スイッチの接続が切断されると、スイッチはスパニングツリーが新しいルートポートを選択すると同時に代替パスの使用を開始します。リンクやスイッチに障害が発生した場合、またはスパニングツリーが UplinkFast の有効化によって自動的に再設定された場合に、新しいルートポートを短時間で選択できます。ルートポートは、通常のスパニングツリー手順とは異なり、

リスニング ステートおよびラーニング ステートを経由せず、ただちにフォワーディング ステートに移行します。

スパニングツリーが新規ルート ポートを再設定すると、他のインターフェイスはネットワークにマルチキャスト パケットをフラッディングし、インターフェイス上で学習した各アドレスにパケットを送信します。max-update-rate パラメータの値を小さくすることで、これらのマルチキャスト トラフィックのバーストを制限できます（このパラメータはデフォルトで毎秒 150 パケットです）。ただし、0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。

（注） UplinkFast は、ネットワークのアクセスまたはエッジに位置する、ワイヤリング クローゼットのスイッチで非常に有効です。バックボーン デバイスには適していません。他のアプリケーションにこの機能を使用しても、有効とは限りません。

UplinkFast は、直接リンク障害発生後に高速コンバージェンスを行い、アップリンク グループを使用して、冗長レイヤ 2 リンク間でロードバランシングを実行します。アップリンク グループは、（VLAN ごとの）レイヤ 2 インターフェイスの集合であり、いかなるときも、その中の 1 つのインターフェイスだけが転送を行います。つまり、アップリンク グループは、（転送を行う）ルート ポートと、（セルフループを行うポートを除く）ブロックされたポートの集合で構成されます。アップリンク グループは、転送中のリンクで障害が起きた場合に代替パスを提供します。

図 *12* : 直接リンク障害が発生する前の *UplinkFast* の例

このトポロジにはリンク障害がありません。ルート スイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

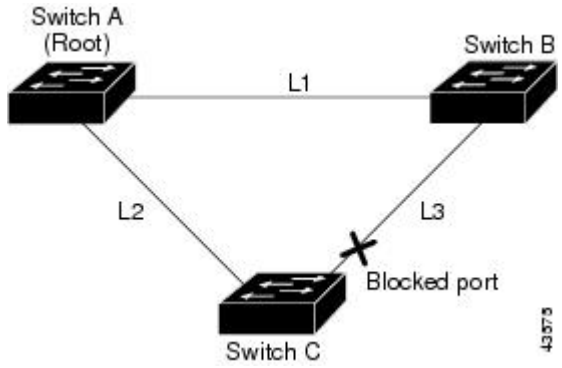
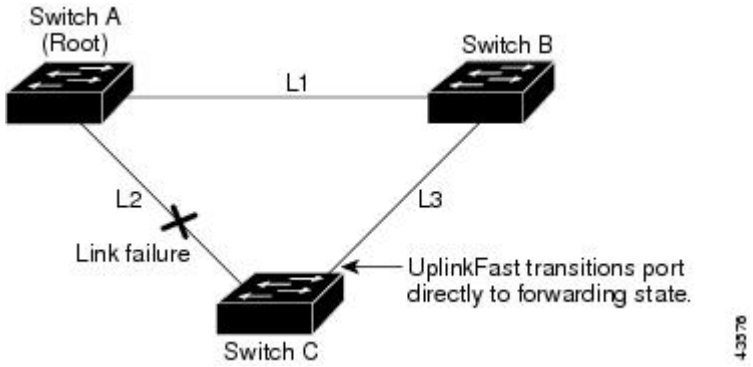


図 *13* : 直接リンク障害が発生したあとの *UplinkFast* の例

スイッチ C が、ルート ポートの現在のアクティブ リンクである L2 でリンク障害（直接リンク障害）を検出すると、UplinkFast がスイッチ C でブロックされていたインターフェイスのブロックを解除し、リスニング ステートおよびラーニング ステートを経由せずに、直接フォワー

ディング ステートに移行させます。この切り替えに必要な時間は、約 1 ～ 5 秒です。



関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）
MSTP 設定時の注意事項 （36 ページ）
MST リージョン （37 ページ）
冗長リンクで使用するための UplinkFast のイネーブル化 （89 ページ）
高速コンバージェンスを発生させるイベント （79 ページ）

クロススタック UplinkFast

クロススタック UplinkFast（CSUF）は、スイッチ スタック全体にスパニングツリー高速移行（通常のネットワーク状態の下では1秒未満の高速コンバージェンス）を提供します。高速移行の間は、スタック上の代替冗長リンクがフォワーディング ステートになり、一時的なスパニングツリーループもバックボーンへの接続の損失も発生させません。一部の設定では、この機能により、冗長性と復元力を備えたネットワークが得られます。CSUF は UplinkFast 機能をイネーブルにすると、自動的にイネーブルになります。

CSUF で高速移行が得られない場合もあります。この場合は、通常のスパニングツリー移行が発生し、30 ～ 40 秒以内に完了します。詳細については、「関連項目」を参照してください。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化 （89 ページ）
高速コンバージェンスを発生させるイベント （79 ページ）

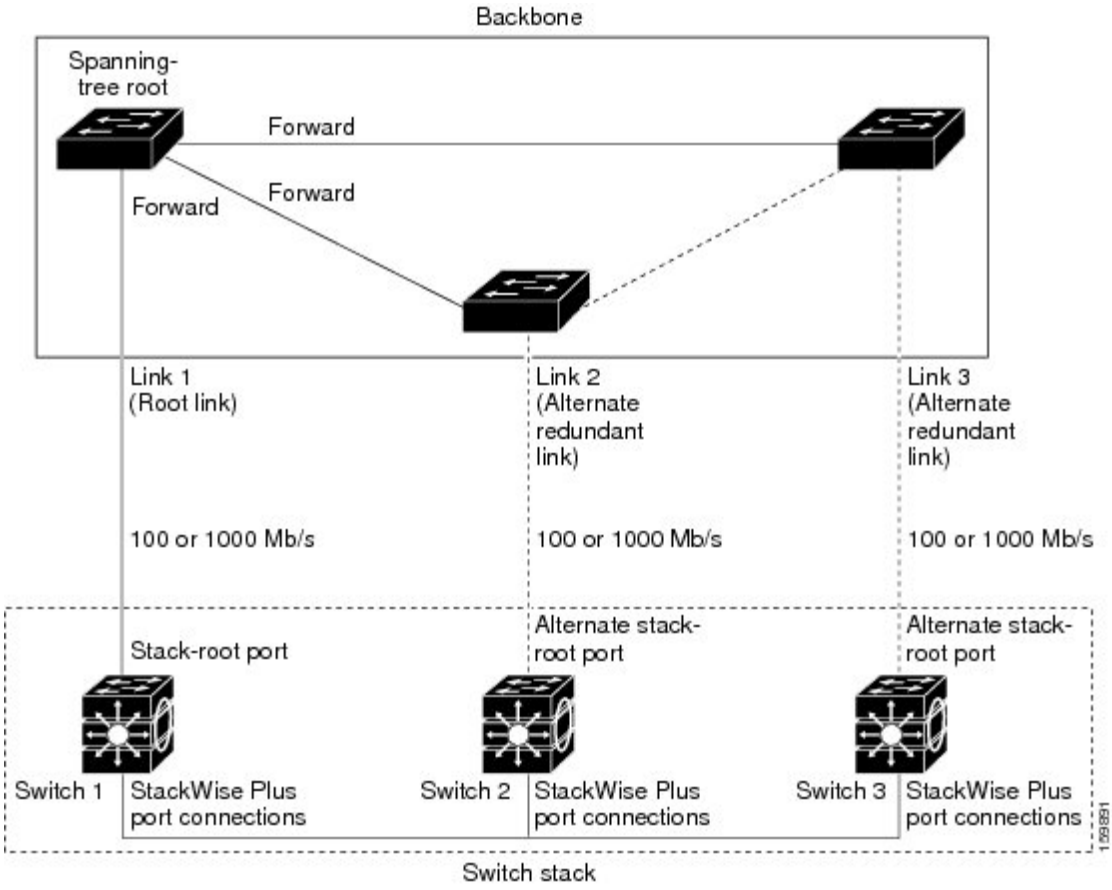
クロススタック UplinkFast の動作

クロススタック UplinkFast（CSUF）によって、ルートへのパスとしてスタック内で1つのリンクが確実に選択されます。

図 *14*：クロススタック *UplinkFast* トポロジ

スイッチ1のスタックルート ポートは、スパニングツリーのルートへパスを提供しています。スイッチ 2 およびスイッチ 3 の代替スタックルート ポートは、現在のスタックルート スイッチに障害が発生したか、またはそのスパニングツリールートへのリンクに障害が発生した場合に、スパニングツリー ルートへの代替パスを提供できます。

ルート リンクである Link 1 は、スパニングツリー フォワーディング ステートになっています。Link 2 と Link 3 は、スパニングツリー ブロッキング ステートになっている代替冗長リンクです。スイッチ 1 に障害が発生したか、そのスタック ルート ポートに障害が発生したか、または Link 1 に障害が発生した場合には、CSUF が、1 秒未満でスイッチ 2 またはスイッチ 3 のいずれかにある代替スタックルート ポートを選択して、それをフォワーディング ステートにします。



特定のリンク損失またはスパニングツリーイベントが発生した場合（次のトピックを参照）、Fast Uplink Transition Protocol は、ネイバー リストを使用して、高速移行要求をスタック メンバーに送信します。

高速移行要求を送信するスイッチは、ルート ポートとして選択されたポートをフォワーディング ステートへ高速移行する必要があります。また、高速移行を実行するには、事前に各スタックから確認応答を取得しておく必要があります。

スタック内の各スイッチが、ルート、コスト、およびブリッジ ID を比較することにより、このスパニングツリー インスタンスのスタック ルートとなるよりも送信スイッチの方がよりよい選択肢であるかどうかを判断します。スタック ルートとして送信スイッチが最も良い選択である場合は、スタック内の各スイッチが確認応答を返します。それ以外の場合は、高速移行要求を送信します。この時点では、送信スイッチは、すべてのスタック スイッチから確認応答を受け取っていません。

すべてのスタック スイッチから確認応答を受け取ると、送信スイッチの Fast Uplink Transition Protocol は代替スタックルート ポートをすぐにフォワーディング ステートに移行させます。送信スイッチがすべてのスタック スイッチからの確認応答を取得しなかった場合、通常のスパニングツリー移行（ブロッキング、リスニング、ラーニング、およびフォワーディング）が行われ、スパニングツリー トポロジが通常のレート（2 × 転送遅延時間 + 最大エージング タイム）で収束します。

Fast Uplink Transition Protocol は、VLAN ごとに実装されており、一度に 1 つのスパニングツリー インスタンスにしか影響しません。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化 （89 ページ）
高速コンバージェンスを発生させるイベント （79 ページ）

高速コンバージェンスを発生させるイベント

CSUF 高速コンバージェンスは、ネットワーク イベントまたはネットワーク障害に応じて、発生する場合もあれば発生しない場合もあります。

高速コンバージェンス（通常のネットワーク状態で 1 秒未満）は、次のような状況で発生します。

- スタック ルート ポート リンクに障害が発生した。

  スタック内の 2 つのスイッチがルートへの代替パスを持つ場合、それらのスイッチの片方だけが高速移行を行います。

- スタック ルートをスパニングツリー ルートに接続するリンクに障害が発生し、回復した。
- ネットワークの再設定により、新しいスタックルート スイッチが選択された。
- ネットワークの再設定により、現在のスタックルート スイッチ上で新しいポートがスタック ルート ポートとして選択された。

（注） 複数のイベントが同時に発生すると、高速移行が行われなくなる場合もあります。たとえば、スタック メンバの電源がオフになり、それと同時にスタック ルートをスパニングツリー ルートに接続しているリンクが回復した場合、通常のスパニングツリー コンバージェンスが発生します。

通常のスパニングツリー コンバージェンス（30 ～ 40 秒）は、次のような状況で発生します。

- スタック ルート スイッチの電源がオフになったか、またはソフトウェアに障害が発生した。
- 電源がオフになっていたか、または障害が発生していたスタック ルート スイッチの電源が入った。
- スタック ルートになる可能性のある新しいスイッチがスタックに追加された。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化 （89 ページ）
UplinkFast （75 ページ）
クロススタック UplinkFast （77 ページ）
クロススタック UplinkFast の動作 （77 ページ）

BackboneFast

BackboneFast は、バックボーンのコアにおける間接障害を検出します。BackboneFast は、UplinkFast 機能を補完するテクノロジーです。UplinkFast は、アクセス スイッチに直接接続されたリンクの障害に対応します。BackboneFast は、最大エージング タイマーを最適化します。最大エージング タイマーによって、スイッチがインターフェイスで受信したプロトコル情報を保存しておく時間の長さが制御されます。スイッチが別のスイッチの指定ポートから下位BPDUを受信した場合、BPDUは他のスイッチでルートまでのパスが失われた可能性を示すシグナルとなり、BackboneFast はルートまでの別のパスを見つけようとします。

スイッチのルート ポートまたはブロックされたインターフェイスが、指定スイッチから下位 BPDU を受け取ると、BackboneFast が開始します。下位 BPDU は、ルート ブリッジと指定スイッチの両方を宣言しているスイッチを識別します。スイッチが下位BPDUを受信した場合、そのスイッチが直接接続されていないリンク（間接リンク）で障害が発生したことを意味します（指定スイッチとルート スイッチ間の接続が切断されています）。スパニングツリーのルールに従い、スイッチは最大エージング タイム（デフォルトは 20 秒）の間、下位 BPDU を無視します。

スイッチは、ルート スイッチへの代替パスの有無を判別します。下位 BPDU がブロック インターフェイスに到達した場合、スイッチ上のルート ポートおよび他のブロック インターフェイスがルート スイッチへの代替パスになります（セルフループ ポートはルート スイッチの代替パスとは見なされません）。下位 BPDU がルート ポートに到達した場合には、すべてのブロック インターフェイスがルート スイッチへの代替パスになります。下位 BPDU がルート ポートに到達し、しかもブロック インターフェイスがない場合、スイッチはルート スイッチへの接続が切断されたものと見なし、ルート ポートの最大エージング タイムが経過するまで待ち、通常のスパニングツリー ルールに従ってルート スイッチになります。

スイッチが代替パスでルート スイッチに到達できる場合、スイッチはその代替パスを使用して、Root Link Query（RLQ）要求を送信します。スイッチは、スタック メンバーがルート スイッチへの代替ルートを持つかどうかを学習するために、すべての代替パスに RLQ 要求を送信し、ネットワーク内およびスタック内の他のスイッチからのRLQ応答を待機します。スイッチは、すべての代替パスに RLQ 要求を送信し、ネットワーク内の他のスイッチからの RLQ 応答を待機します。

スタック メンバが、ブロック インターフェイス上の非スタック メンバから RLQ 応答を受信し、その応答が他の非スタック スイッチ宛てのものであった場合、そのスタック メンバは、スパニングツリー インターフェイス ステートに関係なく、その応答パケットを転送します。

スタック メンバが非スタック メンバから RLQ 応答を受信し、その応答がスタック宛てのものであった場合、そのスタック メンバは、他のすべてのスタック メンバがその応答を受信するようにその応答を転送します。

ルートへの代替パスがまだ存在していると判断したスイッチは、下位 BPDU を受信したインターフェイスの最大エージング タイムが経過するまで待ちます。ルート スイッチへのすべての代替パスが、スイッチとルート スイッチ間の接続が切断されていることを示している場合、スイッチは RLQ 応答を受信したインターフェイスの最大エージング タイムを満了させます。1 つまたは複数の代替パスからルート スイッチへ引き続き接続できる場合、スイッチは下位 BPDU を受信したすべてのインターフェイスを指定ポートにして、（ブロッキング ステートになっていた場合）ブロッキング ステートを解除し、リスニング ステート、ラーニング ステートを経てフォワーディング ステートに移行させます。

図 *15* : 間接リンク障害が発生する前の *BackboneFast* の例

これは、リンク障害が発生していないトポロジ例です。ルート スイッチであるスイッチ A はリンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

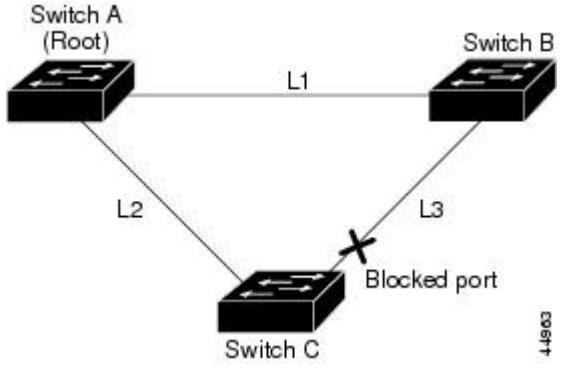


図 *16* : 間接リンク障害が発生したあとの *BackboneFast* の例

リンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、この障害を検出できません。一方スイッチ B は、L1 によってルート スイッチに直接接続されているため障害を検出し、スイッチ B 自身をルートとして選定して、自らをルートとして特定した状態で BPDU をスイッチ C へ送信し始めます。スイッチ B から下位 BPDU を受信したスイッチ C は、間接障害が発生していると見なします。この時点で、BackboneFast は、スイッチ C のブロック インターフェイスを、インターフェイスの最大エージング タイムが満了するまで待たずに、ただちにリスニング ステートに移行させます。BackboneFast は、次に、スイッチ C のレイヤ 2 インターフェイスをフォワーディング ステートに移行させ、スイッチ B からスイッチ A へのパスを提供します。ルート スイッチの選択には約 30 秒必要です。これは転送遅延時間がデフォルトの 15 秒に設定されていればその倍の時間です。BackboneFast がリンク L1 で発

生した障害に応じてトポロジを再設定します。

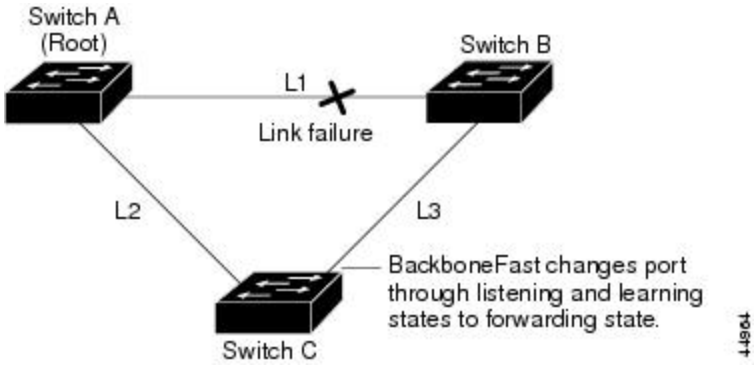
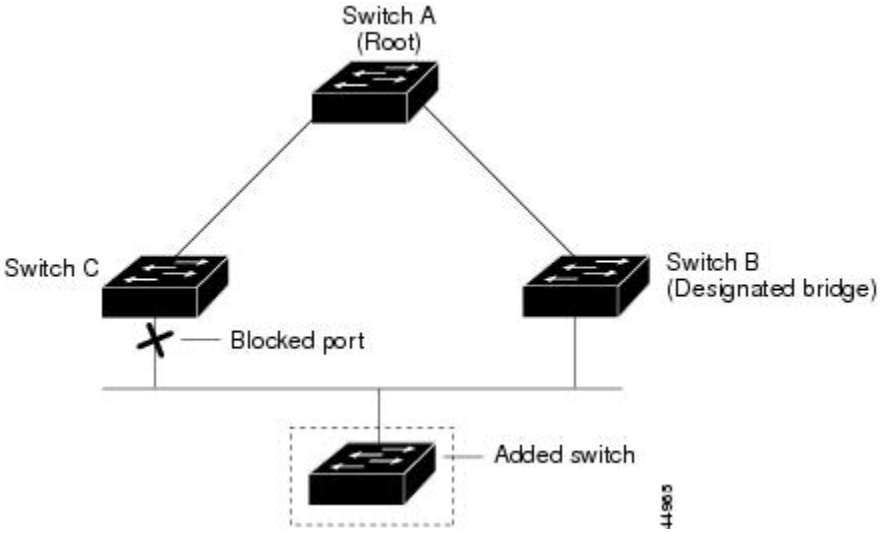


図 17: メディア共有型トポロジにおけるスイッチの追加

新しいスイッチがメディア共有型トポロジに組み込まれた場合、認識された指定スイッチ（スイッチ B）から下位 BPDU が届いていないので、BackboneFast はアクティブになりません。新しいスイッチは、自身がルート スイッチであることを伝える下位 BPDU の送信を開始します。ただし、他のスイッチはこれらの下位 BPDU を無視し、新しいスイッチはスイッチ B がルート スイッチであるスイッチ A への指定スイッチであることを学習します。



関連トピック

MST リージョン設定の指定と MSTP のイネーブル化 （53 ページ）
MSTP 設定時の注意事項 （36 ページ）
MST リージョン （37 ページ）
BackboneFast をイネーブル化 （92 ページ）

EtherChannel ガード

EtherChannel ガードを使用すると、スイッチと接続したデバイス間での EtherChannel の設定の矛盾を検出できます。スイッチ インターフェイスは EtherChannel として設定されているものの、もう一方のデバイスのインターフェイスではその設定が行われていない場合、設定の矛盾

が発生します。また、EtherChannel の両端でチャネルのパラメータが異なる場合にも、設定の矛盾が発生します。

スイッチが、他のデバイス上で設定の矛盾を検出した場合、EtherChannel ガードは、スイッチのインターフェイスを errdisable ステートにし、エラー メッセージを表示します。

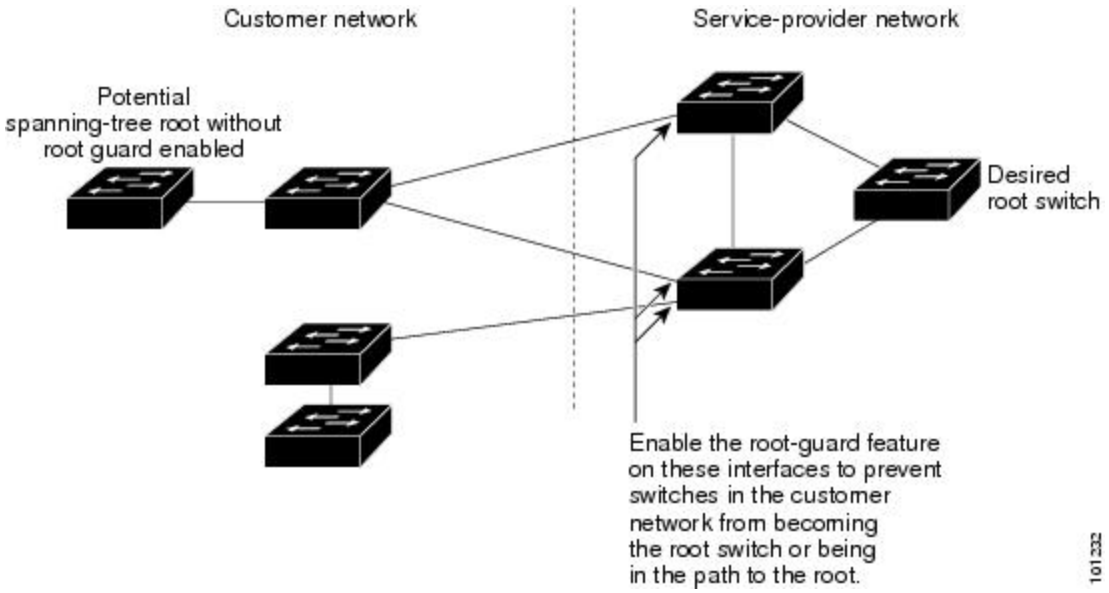
関連トピック

EtherChannel ガードのイネーブル化 （93 ページ）

ルート ガード

図 *18*：サービス プロバイダー ネットワークのルート ガード

サービス プロバイダー（SP）のレイヤ 2 ネットワークには、SP 以外が所有するスイッチへの接続が多く含まれている場合があります。このようなトポロジでは、スパニングツリーが再構成され、カスタマー スイッチをルート スイッチとして選択する可能性があります。この状況を防ぐには、カスタマー ネットワーク内のスイッチに接続する SP スイッチ インターフェイス上でルート ガード機能を有効に設定します。スパニングツリーの計算によってカスタマーネットワーク内のインターフェイスがルート ポートとして選択されると、ルート ガードがそのインターフェイスを root-inconsistent（ブロッキング）ステートにして、カスタマーのスイッチがルート スイッチにならないようにするか、ルートへのパスに組み込まれないようにします。



SP ネットワーク外のスイッチがルート スイッチになると、インターフェイスがブロックされ（root-inconsistent ステートになり）、スパニングツリーが新しいルート スイッチを選択します。カスタマーのスイッチがルート スイッチになることはありません。ルートへのパスに組み込まれることもありません。

スイッチが MST モードで動作している場合、ルート ガードが強制的にそのインターフェイスを指定ポートにします。また、境界ポートがルート ガードによって Internal Spanning-Tree（IST）インスタンスでブロックされている場合にも、このインターフェイスはすべての MST インス

タンスでもブロックされます。境界ポートは、指定スイッチが IEEE 802.1D スイッチまたは異なる MST リージョン設定を持つスイッチのいずれかである LAN に接続されるインターフェイスです。

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。VLAN は、MST インスタンスに対してグループ化された後、マッピングされます。

⚠

注意 ルート ガード機能を誤って使用すると、接続が切断されることがあります。

関連トピック

ルート ガードのイネーブル化 （94 ページ）

ループ ガード

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチドネットワーク全体でイネーブルにした場合に最も効果があります。ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

スイッチが PVST+ または Rapid PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

スイッチが MST モードで動作しているとき、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされている場合でのみ、非境界ポートで BPDU を送信しません。境界ポートでは、ループ ガードがすべての MST インスタンスでインターフェイスをブロックします。

関連トピック

ループ ガードのイネーブル化 （95 ページ）

オプションのスパニングツリー機能の設定方法

PortFast のイネーブル化

PortFast 機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、すぐにスパニングツリー フォワーディング ステートに移行されます。

音声 VLAN 機能をイネーブルにすると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

⚠

注意 PortFast を使用するのは、1 つのエンド ステーションがアクセス ポートまたはトランク ポートに接続されている場合に限定されます。スイッチまたはハブに接続するインターフェイス上でこの機能をイネーブルにすると、スパニングツリーがネットワーク ループを検出または阻止できなくなり、その結果、ブロードキャスト ストームおよびアドレス ラーニングの障害が起きる可能性があります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `デバイス(config)# interface gigabitethernet1/0/2`	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	**spanning-tree portfast** [**trunk**] 例： `デバイス(config-if)# spanning-tree portfast trunk`	単一ワーク ステーションまたはサーバに接続されたアクセス ポート上で PortFast をイネーブルにします。 **trunk** キーワードを指定すると、トランク ポート上で PortFast をイネーブルにできます。

	コマンドまたはアクション	目的
		（注） トランク ポートで PortFast をイネーブルにするには、**spanning-tree portfast trunk** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**spanning-tree portfast** コマンドは、トランクポート上では機能しません。 トランク ポート上で PortFast をイネーブルにする場合は、事前に、トランク ポートとワークステーションまたはサーバの間にループがないことを確認してください。 デフォルトでは、PortFast はすべてのインターフェイスでディセーブルです。
ステップ 5	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

次のタスク

spanning-tree portfast default 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、すべての非トランクポート上で PortFast 機能をグローバルにイネーブルにできます。

関連トピック

PortFast （73 ページ）
オプションのスパニング ツリー機能の制約事項

BPDU ガードのイネーブル化

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU ガード機能をイネーブルにできます。

⚠

注意 PortFast エッジは、エンド ステーションに接続するインターフェイスのみに設定します。それ以外に設定すると、予期しないトポロジ ループが原因でデータのパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree portfast edge bpduguard default** 例： `デバイス(config)# spanning-tree portfast edge bpduguard default`	BPDU ガードをグローバルにイネーブルにします。 BPDU ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	**interface** *interface-id* 例： `デバイス(config)# interface gigabitethernet1/0/2`	エンドステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**spanning-tree portfast edge** 例： `デバイス(config-if)# spanning-tree portfast edge`	PortFast エッジ機能をイネーブルにします。
ステップ 6	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

次のタスク

ポートをシャットダウンしないようにするには、**errdisable detect cause bpduguard shutdown vlan** 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、違反が発生したポート上の原因となっている VLAN だけをシャットダウンします。

PortFast 機能をイネーブルにしなくても、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のポートで BPDU ガードをイネーブルにすることもできます。BPDU を受信したポートは、errdisable ステートになります。

関連トピック

BPDU ガード （74 ページ）

BPDU フィルタリングのイネーブル化

PortFast エッジ機能をイネーブルにしなくても、**spanning-tree bpdufilter enable** インターフェイス コンフィギュレーション コマンドを使用して、任意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することもできます。このコマンドを実行すると、インターフェイスは BPDU を送受信できなくなります。

⚠

注意 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ことは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリーループが発生することがあります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU フィルタリング機能をイネーブルにできます。

⚠

注意 PortFast エッジは、エンド ステーションに接続するインターフェイスのみに設定します。それ以外に設定すると、予期しないトポロジ ループが原因でデータのパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例：** `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**spanning-tree portfast edge bpdufilter default** 例： `デバイス(config)# spanning-tree portfast edge bpdufilter default`	BPDU フィルタリングをグローバルにイネーブルにします。 BPDU フィルタリングは、デフォルトではディセーブルに設定されています。
ステップ 4	**interface** *interface-id* 例： `デバイス(config)# interface gigabitethernet1/0/2`	エンドステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**spanning-tree portfast edge** 例： `デバイス(config-if)# spanning-tree portfast edge`	指定したインターフェイスで PortFast エッジ機能をイネーブルにします。
ステップ 6	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

BPDU フィルタリング （74 ページ）

冗長リンクで使用するための UplinkFast のイネーブル化

（注） UplinkFast をイネーブルにすると、スイッチまたはスイッチ スタックのすべての VLAN に影響します。個々の VLAN について UplinkFast を設定することはできません。

Rapid PVST+ または MSTP に対して UplinkFast または Cross-Stack UplinkFast（CSUF）機能を設定できますが、この機能は、スパニングツリーのモードを PVST+ に変更するまではディセーブル（非アクティブ）になったままです。

この手順は任意です。UplinkFast および CSUF をイネーブルにするには、次の手順に従います。

始める前に

スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにすることはできません。スイッチプライオリティが設定されている VLAN 上で UplinkFast をイネーブルにする場合は、最初に **no spanning-tree vlan** *vlan-id* **priority** 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ことによって、VLANのスイッチプライオリティをデフォルト値に戻す必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree uplinkfast** [**max-update-rate** *pkts-per-second*] 例： デバイス(config)# **spanning-tree uplinkfast max-update-rate 200**	UplinkFast をイネーブルにします。 （任意）*pkts-per-second* に指定できる範囲は毎秒 0 ～ 32000 パケットです。デフォルト値は 150 です。 0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。 このコマンドを入力すると、すべての非スタック ポート インターフェイス上で CSUF もイネーブルになります。
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティは 49152 に設定されます。UplinkFast をイネーブルにする場合、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満の値に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します（パス コストを 3000 以上の値に変更した場合、パス コストは変更されません）。スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低くなります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をイネーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにイネーブルになります。

関連トピック

UplinkFast （75 ページ）
クロススタック UplinkFast （77 ページ）
クロススタック UplinkFast の動作 （77 ページ）
高速コンバージェンスを発生させるイベント （79 ページ）

UplinkFast のディセーブル化

この手順は任意です。

UplinkFast および Cross-Stack UplinkFast（SUF）をディセーブルにするには、次の手順に従います。

始める前に

UplinkFast を有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no spanning-tree uplinkfast** 例： `デバイス(config)# no spanning-tree uplinkfast`	スイッチおよびそのスイッチのすべての VLAN で UplinkFast および CSUF をディセーブルにします。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	デバイス(config)# **end**	

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をディセーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにディセーブルになります。

BackboneFast をイネーブル化

BackboneFast をイネーブルにすると、間接リンク障害を検出し、スパニングツリーの再構成をより早く開始できます。

Rapid PVST+ または MSTP に対して BackboneFast 機能を設定できます。ただし、スパニングツリーモードを PVST+に変更するまで、この機能はディセーブル（非アクティブ）のままです。

この手順は任意です。スイッチ上で BackboneFast をイネーブルにするには、次の手順に従います。

始める前に

BackboneFast を使用する場合は、ネットワーク上のすべてのスイッチでイネーブルする必要があります。BackboneFast は、トークンリング VLAN ではサポートされません。この機能は他社製スイッチでの使用にサポートされています。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree backbonefast** 例：	BackboneFast をイネーブルにします。

	コマンドまたはアクション	目的
	デバイス(config)# **spanning-tree backbonefast**	
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

BackboneFast （80 ページ）

EtherChannel ガードのイネーブル化

deviceで PVST+、Rapid PVST+、または MSTP が稼働している場合、EtherChannel の設定の矛盾を検出する EtherChannel ガード機能をイネーブルにできます。

この手順は任意です。

deviceで EtherChannel ガードをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree etherchannel guard misconfig** 例： デバイス(config)# **spanning-tree etherchannel guard misconfig**	EtherChannel ガードをイネーブルにします。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	デバイス(config)# **end**	

次のタスク

show interfaces status err-disabled 特権 EXEC コマンドを使用することで、EtherChannel の設定矛盾が原因でディセーブルになっている device ポートを表示できます。リモートデバイス上では、**show etherchannel summary** 特権 EXEC コマンドを使用して、EtherChannel の設定を確認できます。

設定を修正した後、誤って設定していたポート チャネル インターフェイス上で、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してください。

関連トピック

EtherChannel ガード （82 ページ）

ルート ガードのイネーブル化

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロック ステートの）バックアップ インターフェイスがルート ポートになります。ただし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）ステートになり、フォワーディング ステートに移行できなくなります。

（注） ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

この手順は任意です。

スイッチ上でルート ガードをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `デバイス(config)# interface gigabitethernet1/0/2`	設定する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	**spanning-tree guard root** 例： `デバイス(config-if)# spanning-tree guard root`	インターフェイス上でルート ガードをイネーブルにします。 デフォルトでは、ルート ガードはすべてのインターフェイスでディセーブルです。
ステップ 5	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

ルート ガード （83 ページ）

ループ ガードのイネーブル化

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチドネットワーク全体に設定した場合に最も効果があります。ループ ガードは、スパニングツリーがポイントツーポイントと見なすインターフェイス上でのみ動作します。

（注） ループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。

deviceで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

この手順は任意です。deviceでループ ガードをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的

ステップ 1	次のいずれかのコマンドを入力します。
	• **show spanning-tree active**
	• **show spanning-tree mst**
	例：
	`デバイス# show spanning-tree active`
	または
	`デバイス# show spanning-tree mst`
		どのインターフェイスが代替ポートまたはルートポートであるかを確認します。

ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree loopguard default** 例： `デバイス(config)# spanning-tree loopguard default`	ループ ガードをイネーブルにします。 ループ ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ループ ガード （84 ページ）

スパニングツリー ステータスのモニタリング

表 *10 :* スパニングツリー ステータスをモニタリングするコマンド

コマンド	目的
show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。

コマンド	目的
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree mst interface *interface-id*	指定インターフェイスのMST情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示します。またはスパニングツリー ステート セクションのすべての行を表示します。
show spanning-tree mst interface *interface-id* **portfast edge**	指定したインターフェイスのスパニングツリーportfast 情報を表示します。

オプションのスパニング ツリー機能に関する追加情報

関連資料

関連項目	マニュアル タイトル
スパニング ツリー プロトコル コマンド	LAN Switching Command Reference, Cisco IOS XE Release 3SE（Catalyst 3650 Switches）

標準および RFC

標準/RFC	タイトル
なし	—

MIB

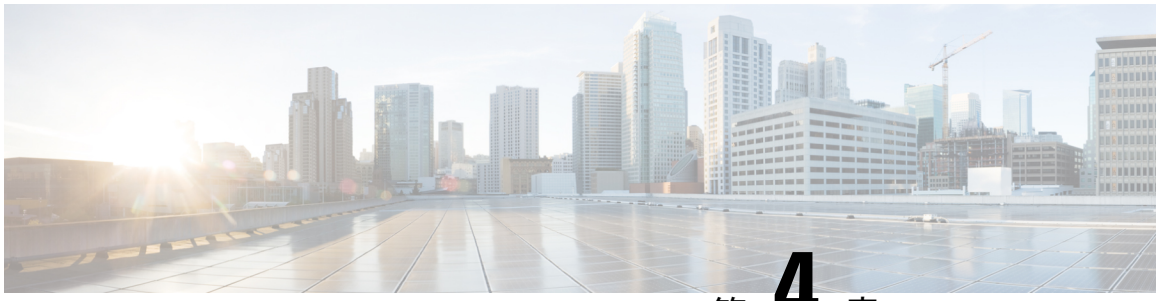
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

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

オプションのスパニングツリー機能の機能情報

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



第 4 章

EtherChannel の設定

機能情報の確認

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

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

EtherChannel の制約事項

次に、EtherChannels の制約事項を示します。

- EtherChannel のすべてのポートは同じ VLAN に割り当てるか、またはトランク ポートとして設定する必要があります。

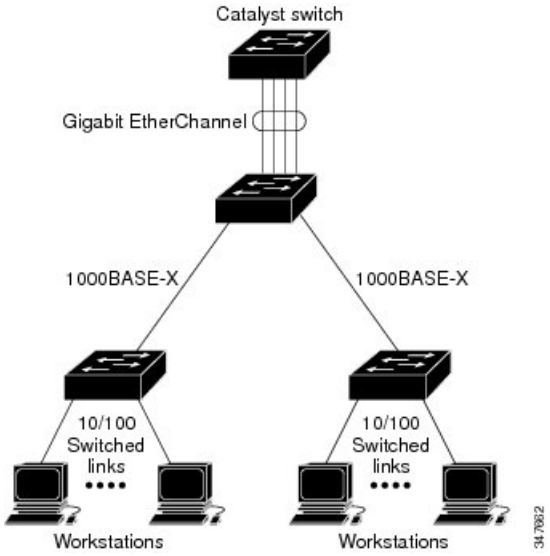
EtherChannel について

EtherChannel の概要

EtherChannel は、スイッチ、ルータ、およびサーバ間にフォールトトレラントな高速リンクを提供します。EtherChannel を使用して、ワイヤリング クローゼットとデータセンター間の帯域幅を増やすことができます。さらに、ボトルネックが発生しやすいネットワーク上のあらゆる場所に EtherChannel を配置できます。EtherChannel は、他のリンクに負荷を再分散させることによって、リンク切断から自動的に回復します。リンク障害が発生した場合、EtherChannel は自動的に障害リンクからチャネル内の他のリンクにトラフィックをリダイレクトします。

EtherChannel は、単一の論理リンクにバンドルする個別のイーサネット リンクで構成されます。

図 *19 :* 一般的な *EtherChannel* 構成



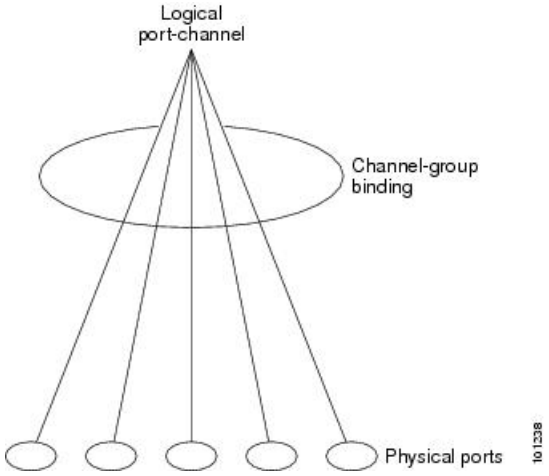
各 EtherChannel は、互換性のある設定のイーサネット ポートを 8 つまで使用して構成できます。

チャネル グループおよびポートチャネル インターフェイス

EtherChannel は、チャネル グループとポートチャネル インターフェイスから構成されます。チャネル グループはポートチャネル インターフェイスに物理ポートをバインドします。ポートチャネル インターフェイスに適用した設定変更は、チャネル グループにまとめてバインドされるすべての物理ポートに適用されます。

図 *20* : 物理ポート、チャネル グループおよびポートチャネル インターフェイスの関係

channel-group コマンドは、物理ポートおよびポートチャネル インターフェイスをまとめてバインドします。各 EtherChannel には 1 ～ 128 までの番号が付いたポートチャネル論理インターフェイスがあります。ポートチャネル インターフェイス番号は、**channel-group** インターフェイス コンフィギュレーション コマンドで指定した番号に対応しています。



- レイヤ 2 ポートの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャネル インターフェイスを動的に作成します。

  また、**interface port-channel** *port-channel-number* 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、ポートチャネル論理インターフェイスを手動で作成することもできます。ただし、その場合、論理インターフェイスを物理ポートにバインドするには、**channel-group** *channel-group-number* コマンドを使用する必要があります。*channel-group-number* は *port-channel-number* と同じ値に設定することも、違う値を使用することもできます。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポートチャネルを作成します。

- レイヤ 3 ポートの場合は、**interface port-channel** グローバル コンフィギュレーション コマンド、およびそのあとに **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、論理インターフェイスを手動で作成する必要があります。その後、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。

- レイヤ 3 ポートでレイヤ 3 インターフェイスとしてインターフェイスを設定するには、**no switchport** インターフェイスコマンドを使用した上で **channel-group** インターフェイス コンフィギュレーション コマンドを使用して動的にポートチャネル インターフェイスを作成します。

関連トピック

ポートチャネル論理インターフェイスの作成

EtherChannel 設定時の注意事項

EtherChannel のデフォルト設定 （111 ページ）

レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）
物理インターフェイスの設定

Port Aggregation Protocol; ポート集約プロトコル

ポート集約プロトコル（PAgP）はシスコ独自のプロトコルで、Cisco devicesおよび PAgP をサポートするベンダーによってライセンス供与されたdevicesでのみ稼働します。PAgP を使用すると、イーサネット ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できます。

deviceまたはdevice スタックは PAgP を使用することによって、PAgP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似している（スタック内の単一device上の）ポートを、単一の論理リンク（チャネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、PAgP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。リンクを EtherChannel にグループ化した後で、PAgP は単一device ポートとして、スパニングツリーにそのグループを追加します。

PAgP モード

PAgP モードは、PAgP ネゴシエーションを開始する PAgP パケットをポートが送信できるか、または受信した PAgP パケットに応答できるかを指定します。

表 *11 : EtherChannel PAgP* モード

モード	説明
auto	ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。これにより、PAgP パケットの送信は最小限に抑えられます。
desirable	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。EtherChannel メンバが、スイッチ スタックにある異なるスイッチから（クロススタック EtherChannel）の場合、このモードがサポートされます。

スイッチポートは、**auto** モードまたは **desirable** モードに設定された相手ポートとだけ PAgP パケットを交換します。**on** モードに設定されたポートは、PAgP パケットを交換しません。

auto モードおよび **desirable** モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ 2 EtherChannel の場合は、トランク ステートおよび VLAN 番号などの基準に基づいて）、ポートで EtherChannel を形成できるようにします。

PAgP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **desirable** モードのポートは、**desirable** または **auto** モードの別のポートと EtherChannel を形成できます。
- **auto** モードのポートは、**desirable** モードの別のポートと EtherChannel を形成できます。

両ポートとも LACP ネゴシエーションを開始しないため、**auto** モードのポートは、**auto** モードの別のポートと EtherChannel を形成することはできません。

関連トピック

レイヤ 2 EtherChannel の設定 （115 ページ）
EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （111 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）
ポートチャネル論理インターフェイスの作成
物理インターフェイスの設定

サイレント モード

PAgP 対応のデバイスにスイッチを接続する場合、**non-silent** キーワードを使用すると、スイッチポートを非サイレント動作用に設定できます。**auto** モードまたは **desirable** モードとともに **non-silent** モードを指定しなかった場合は、サイレントモードが指定されていると見なされます。

サイレント モードを使用するのは、PAgP 非対応で、かつほとんどパケットを送信しないデバイスにスイッチを接続する場合です。サイレント パートナーの例は、トラフィックを生成しないファイル サーバ、またはパケット アナライザなどです。この場合、サイレント パートナーに接続された物理ポート上で PAgP を稼働させると、このスイッチ ポートが動作しなくなります。ただし、サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。

関連トピック

レイヤ 2 EtherChannel の設定 （115 ページ）
EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （111 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）
ポートチャネル論理インターフェイスの作成
物理インターフェイスの設定

PAgP 学習方式およびプライオリティ

ネットワーク デバイスは、PAgP 物理ラーナーまたは集約ポート ラーナーに分類されます。物理ポートによってアドレスを学習し、その知識に基づいて送信を指示するデバイスは物理ラーナーです。集約（論理）ポートによってアドレスを学習するデバイスは、集約ポート ラーナーです。学習方式は、リンクの両端で同一の設定にする必要があります。

デバイスとそのパートナーが両方とも集約ポート ラーナーの場合、論理ポートチャネル上のアドレスを学習します。デバイスは EtherChannel のいずれかのポートを使用することによって、

送信元にパケットを送信します。集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。

PAgP は、パートナー デバイスが物理ラーナーの場合およびローカル デバイスが集約ポート ラーナーの場合には自動検出できません。したがって、物理ポートでアドレスを学習するには、ローカルデバイスに手動で学習方式を設定する必要があります。また、負荷の分散方式を送信元ベース分散に設定して、指定された送信元 MAC アドレスが常に同じ物理ポートに送信されるようにする必要もあります。

グループ内の 1 つのポートですべての伝送を行うように設定して、他のポートをホット スタンバイに使用することもできます。選択された 1 つのポートでハードウェア信号が検出されなくなった場合は、数秒以内に、グループ内の未使用のポートに切り替えて動作させることができます。パケット伝送用に常に選択されるように、ポートを設定するには、 **pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用してプライオリティを変更します。プライオリティが高いほど、そのポートが選択される可能性が高まります。

（注） CLI で **physical-port** キーワードを指定した場合でも、device がサポートするのは、集約ポート上でのアドレスラーニングのみです。**pagp learn-method** コマンドおよび **pagp port-priority** コマンドは、device のハードウェアには影響を及ぼしませんが、Catalyst 1900 スイッチなど、物理ポートによるアドレスラーニングのみをサポートしているデバイスと PAgP の相互運用性を確保するために必要です。

device のリンクパートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して物理ポートラーナーとして device を設定することを推奨します。また、**port-channel load-balance src-mac** 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、送信元 MAC アドレスに基づいて負荷分散方式を設定することを推奨します。すると、deviceは送信元アドレスを学習した EtherChannel 内の同じポートを使用して、物理ラーナーにパケットを送信します。この状況では、**pagp learn-method** コマンドのみを使用します。

関連トピック

PAgP 学習方式およびプライオリティの設定 （124 ページ）
EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （111 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ （135 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）

PAgP と他の機能との相互作用

ダイナミック トランキング プロトコル（DTP）および Cisco Discovery Protocol（CDP）は、EtherChannel の物理ポートを使用してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で PAgP プロトコル データ ユニット（PDU）を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つ

が EtherChannel に MAC アドレスを提供します。レイヤ 3 EtherChannel の場合、**interface port-channel** グローバル コンフィギュレーション コマンドを経由してインターフェイスが作成された直後に、アクティブな device により MAC アドレスが割り当てられます。

PAgP が PAgP PDU を送受信するのは、PAgP が auto モードまたは desirable モードでイネーブルになっている、稼働状態のポート上だけです。

Link Aggregation Control Protocol

LACP は IEEE 802.3ad で定義されており、Cisco devicesが IEEE 802.3ad プロトコルに適合した devices間のイーサネット チャネルを管理できるようにします。LACP を使用すると、イーサネット ポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

deviceまたはdevice スタックは LACP を使用することによって、LACP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の倫理リンク（チャネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポートパラメータ制約です。たとえば、LACP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。リンクをまとめて EtherChannel を形成した後で、LACP は単一device ポートとして、スパニングツリーにそのグループを追加します。

ポート チャネル内のポートの独立モード動作が変更されます。CSCtn96950 では、デフォルトでスタンドアロン モードが有効になっています。LACP ピアから応答が受信されない場合、ポート チャネル内のポートは中断状態に移動されます。

LACP モード

LACP モードでは、ポートが LACP パケットを送信できるか、LACP パケットの受信のみができるかどうかを指定します。

表 *12 : EtherChannel LACP* モード

モード	説明
active	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。
passive	ポートはパッシブ ネゴシエーション ステートになります。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。これにより、LACP パケットの送信を最小限に抑えます。

active モードおよび **passive LACP** モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ 2 EtherChannel の場合は、トランク ステートおよび VLAN 番号などの基準に基づいて）、ポートで EtherChannel を形成できるようにします。

LACP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **active** モードのポートは、**active** または **passive** モードの別のポートと EtherChannel を形成できます。
- 両ポートとも LACP ネゴシエーションを開始しないため、**passive** モードのポートは、**passive** モードの別のポートと EtherChannel を形成することはできません。

関連トピック

レイヤ 2 EtherChannel の設定 （115 ページ）
EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （111 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）

LACP とリンクの冗長性

LACP ポートチャネルの最小リンクおよびLACP の最大バンドルの機能を使用して、LACP ポートチャネル動作、帯域幅の可用性およびリンク冗長性をさらに高めることができます。

LACP ポートチャネルの最小リンク機能：

- LACP ポート チャネルでリンクし、バンドルする必要があるポートの最小数を設定します。
- 低帯域幅の LACP ポート チャネルがアクティブにならないようにします。
- 必要な最低帯域幅を提供する十分なアクティブ メンバ ポートがない場合、LACP ポート チャネルが非アクティブになるようにします。

LACP の最大バンドル機能：

- LACP ポート チャネルのバンドル ポートの上限数を定義します。
- バンドル ポートがより少ない場合のホット スタンバイ ポートを可能にします。たとえば、5 個のポートがある LACP ポート チャネルで、3 個の最大バンドルを指定し、残りの 2 個のポートをホット スタンバイ ポートとして指定できます。

関連トピック

LACP 最大バンドル機能の設定 （126 ページ）
LACP ホット スタンバイ ポートの設定：例 （138 ページ）
LACP ポート チャネルの最小リンク機能の設定 （128 ページ）

LACP と他の機能との相互作用

DTP および CDP は、EtherChannel の物理ポートを介してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で LACP PDU を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つ

が EtherChannel に MAC アドレスを提供します。レイヤ 3 EtherChannel の場合、**interface port-channel** グローバル コンフィギュレーション コマンドを経由してインターフェイスが作成された直後に、アクティブな device により MAC アドレスが割り当てられます。

LACP が LACP PDU を送受信するのは、LACP が active モードまたは passive モードでイネーブルになっている稼働状態のポートとの間だけです。

EtherChannel の On モード

EtherChannel **on** モードは、EtherChannel を手動で設定するために使用できます。**on** モードでは、ネゴシエーションを行わずにポートは強制的に EtherChannel に参加されます。**on** モードは、リモートデバイスが PAgP または LACP をサポートしていない場合に役立つことがあります。**on** モードでは、リンクの両端の devices が **on** モードに設定されている場合のみ、使用可能な EtherChannel が存在します。

同じチャネルグループ内で**on**モードに設定されているポートは、互換性のあるポート特性（速度やデュプレックスなど）を備えている必要があります。互換性のないポートは、**on** モードに設定されている場合でも、一時停止されます。

注意 **on**モードを使用する場合は、注意する必要があります。これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。グループの設定を誤ると、パケット損失またはスパニングツリーループが発生することがあります。

ロードバランシングおよび転送方式

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャネル内の 1 つのリンクを選択する数値に縮小することによって、チャネル内のリンク間でトラフィックのロード バランシングを行います。MAC アドレス、IP アドレス、送信元アドレス、宛先アドレス、または送信元と宛先両方のアドレスに基づいた負荷分散など、複数の異なるロードバランシング モードから 1 つを指定できます。選択したモードは、device上で設定されているすべての EtherChannel に適用されます。

（注） レイヤ 3 等コスト マルチ パス（ECMP）のロード バランシングは、送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびレイヤ 4 プロトコルに基づいています。フラグメント化されたパケットは、これらのパラメータを使用して計算されたアルゴリズムに基づいて 2 つの異なるリンクで処理されます。これらのパラメータのいずれかを変更すると、ロード バランシングが実行されます。

ロードバランシングおよび転送方式を設定するには、**port-channel load-balance** および **port-channel load-balance extended** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

EtherChannel ロードバランシングの設定 （121 ページ）
EtherChannel 設定時の注意事項
レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）
EtherChannel のデフォルト設定 （111 ページ）
レイヤ 3 EtherChannel 設定時の注意事項 （114 ページ）

MAC アドレス転送

送信元 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、ロード バランシングを行うために、送信元ホストが異なるパケットはそれぞれ異なるチャネルポートを使用しますが、送信元ホストが同じパケットは同じチャネル ポートを使用します。

宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの宛先ホストの MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、宛先が同じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャネル ポートに転送されます。

送信元および宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、送信元および宛先の両方の MAC アドレスに基づいてチャネル ポート間で分配されます。この転送方式は、負荷分散の送信元 MAC アドレス転送方式と宛先 MAC アドレス転送方式を組み合わせたものです。特定のdeviceに対して送信元 MAC アドレス転送と宛先 MAC アドレス転送のどちらが適切であるかが不明な場合に使用できます。送信元および宛先 MAC アドレス転送の場合、ホスト A からホスト B、ホスト A からホスト C、およびホスト C からホスト B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

関連トピック

EtherChannel ロードバランシングの設定 （121 ページ）
EtherChannel 設定時の注意事項
レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）
EtherChannel のデフォルト設定 （111 ページ）
レイヤ 3 EtherChannel 設定時の注意事項 （114 ページ）

IP アドレス転送

送信元 IP アドレスベース転送の場合、パケットは、着信パケットの送信元 IP アドレスに基づいて EtherChannel ポート間で分配されます。ロード バランシングを行うために、IP アドレスが異なるパケットはチャネルでそれぞれ異なるポートを使用しますが、IP アドレスが同じパケットはチャネルで同じポートを使用します。

宛先 IP アドレスベース転送の場合、パケットは着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。ロード バランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは、チャネルの異なるチャネル ポートに送信できます。異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常にチャネルの同じポートに送信されます。

送信元と宛先 IP アドレスベース転送の場合、パケットは着信パケットの送信元および宛先の両方の IP アドレスに基づいて EtherChannel ポート間で分配されます。この転送方式は、送信元 IP アドレスベース転送方式と宛先 IP アドレスベース転送方式を組み合わせたもので、特定のdeviceに対して送信元 IP アドレスベース転送と宛先 IP アドレスベース転送のどちらが適切であるか不明な場合に使用できます。この方式では、IP アドレス A から IP アドレス B に、IP アドレス A から IP アドレス C に、および IP アドレス C から IP アドレス B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

関連トピック

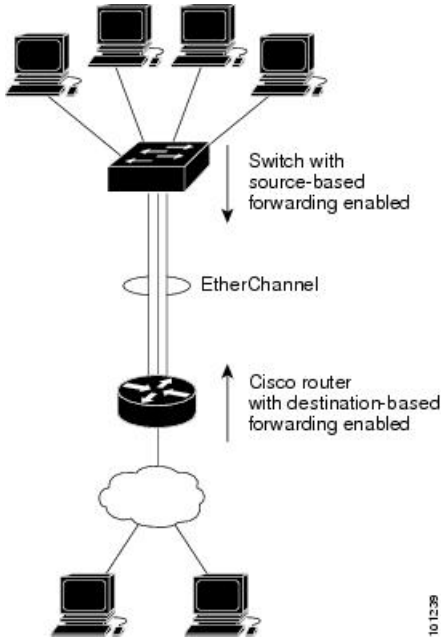
EtherChannel ロードバランシングの設定 （121 ページ）
EtherChannel 設定時の注意事項
レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）
EtherChannel のデフォルト設定 （111 ページ）
レイヤ 3 EtherChannel 設定時の注意事項 （114 ページ）

ロードバランシングの利点

ロードバランシング方式には異なる利点があるため、ネットワーク内のdeviceの位置、および負荷分散が必要なトラフィックの種類に基づいて特定のロードバランシング方式を選択する必要があります。

図 *21* : 負荷の分散および転送方式

次の図では、4 台のワーク ステーションの EtherChannel がルータと通信します。ルータは単一 MAC アドレス デバイスであるため、device EtherChannel で送信元ベース転送を行うことにより、deviceが、ルータで使用可能なすべての帯域幅を使用することが保証されます。ルータは、宛先アドレスベース転送を行うように設定されます。これは、多数のワークステーションで、トラフィックがルータ EtherChannel から均等に分配されることになっているためです。



設定で一番種類が多くなるオプションを使用してください。たとえば、チャネル上のトラフィックが単一 MAC アドレスを宛先とする場合、宛先 MAC アドレスを使用すると、チャネル内の同じリンクが常に選択されます。ただし、送信元アドレスまたはIPアドレスを使用した方が、ロードバランシングの効率がよくなる場合があります。

関連トピック

EtherChannel ロードバランシングの設定 （121 ページ）
EtherChannel 設定時の注意事項
レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）
EtherChannel のデフォルト設定 （111 ページ）
レイヤ 3 EtherChannel 設定時の注意事項 （114 ページ）

EtherChannel およびデバイス スタック

EtherChannel に加入しているポートが含まれているスタック メンバに障害が発生したり、スタックを離れると、アクティブなdeviceにより、障害が発生したスタック device メンバ ポートが削除されます。EtherChannel に残っているポートがある場合、接続は引き続き確保されます。

deviceが既存のスタックに追加されると、新しいdeviceがアクティブなdeviceから実行コンフィギュレーションを受信し、EtherChannel 関連のスタック コンフィギュレーションで更新されます。スタック メンバでは、動作情報（動作中で、チャネルのメンバであるポートのリスト）も受信します。

2 つのスタック間で設定されている EtherChannel がマージされた場合、セルフループ ポートになります。スパニングツリーにより、この状況が検出され、必要な動作が発生します。権利を獲得したdevice スタックにある PAgP 設定または LACP 設定は影響を受けませんが、権利を失った device スタックの PAgP 設定または LACP 設定は、スタックのリブート後に失われます。

デバイス スタックおよび PAgP

PAgP では、アクティブ deviceに障害が発生するか、スタックを離れた場合、スタンバイ device が新しいアクティブ deviceになります。EtherChannel 帯域幅に変更がない場合、スパニングツリーの再コンバージェンスはトリガーされません。新しいアクティブ deviceはアクティブ device の該当項目にスタック メンバの設定を同期します。PAgP 設定は、EtherChannel に古いアクティブ device上にあるポートがない限り、アクティブ deviceの変更後も影響を受けません。

デバイス スタックおよび LACP

LACP の場合、システム ID は、アクティブ deviceから取得したスタック MAC アドレスが使用されます。アクティブ deviceに障害が発生したり、スタックを離れ、スタンバイ deviceが新しいアクティブ deviceが変更になっても、LACP システム ID は変更されません。デフォルトでは、LACP 設定はアクティブ deviceの変更後も影響を受けません。

EtherChannel のデフォルト設定

EtherChannel のデフォルト設定を、次の表に示します。

表 *13 : EtherChannel* のデフォルト設定

機能	デフォルト設定
チャネル グループ	割り当てなし
ポートチャネル論理インターフェイス	未定義
PAgP モード	デフォルトなし。
PAgP 学習方式	すべてのポートで集約ポート ラーニング
PAgP プライオリティ	すべてのポートで 128
LACP モード	デフォルトなし。
LACP 学習方式	すべてのポートで集約ポート ラーニング
LACP ポート プライオリティ	すべてのポートで 32768
LACP システム プライオリティ	32768
LACP システム ID	LACP システムのプライオリティ、deviceまたはスタックの MAC アドレス。
ロード バランシング	device上での負荷分散は着信パケットの送信元MACアドレスに基づきます。

関連トピック

レイヤ 2 EtherChannel の設定 （115 ページ）
EtherChannel の概要
EtherChannel のモード
Devices上の EtherChannel
EtherChannel リンクのフェールオーバー
LACP モード （105 ページ）
PAgP モード （102 ページ）
サイレント モード （103 ページ）
ポートチャネル論理インターフェイスの作成
チャネル グループおよびポートチャネル インターフェイス （100 ページ）
物理インターフェイスの設定
EtherChannel ロードバランシングの設定 （121 ページ）
ロードバランシングおよび転送方式 （107 ページ）

MAC アドレス転送 （108 ページ）
IP アドレス転送 （108 ページ）
ロードバランシングの利点 （109 ページ）
PAgP 学習方式およびプライオリティの設定 （124 ページ）
PAgP 学習方式およびプライオリティ （103 ページ）
LACP システム プライオリティの設定 （129 ページ）
LACP ポート プライオリティの設定 （130 ページ）

EtherChannel 設定時の注意事項

EtherChannel ポートを正しく設定していない場合は、ネットワーク ループおよびその他の問題を回避するために、一部の EtherChannel インターフェイスが自動的にディセーブルになります。設定上の問題を回避するために、次の注意事項に従ってください。

- スイッチまたはスイッチスタックでは、最大 128 の EtherChannel がサポートされています。
- PAgP EtherChannel は、同じタイプのイーサネット ポートを 8 つまで使用して設定します。
- 同じタイプのイーサネット ポートを最大で 16 個備えた LACP EtherChannel を設定してください。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
- EtherChannel 内のすべてのポートを同じ速度および同じデュプレックス モードで動作するように設定します。
- EtherChannel 内のすべてのポートをイネーブルにします。**shutdown** インターフェイス コンフィギュレーション コマンドを使用して無効にされた EtherChannel 内のポートはリンク障害として扱われ、そのトラフィックは EtherChannel 内の残りのポートのいずれかに転送されます。
- グループを初めて作成した際には、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラメータのいずれかで設定を変更した場合は、グループ内のすべてのポートでも変更する必要があります。
  - 許可 VLAN リスト
  - 各 VLAN のスパニングツリー パス コスト
  - 各 VLAN のスパニングツリー ポート プライオリティ
  - スパニングツリー PortFast の設定
- 1 つのポートが複数の EtherChannel グループのメンバになるように設定しないでください。
- EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP および LACP が稼働している複数の EtherChannel グループは、同じスイッチまたはスタック内の別のスイッチ上で共存できます。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。

- アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。
- EtherChannel がデバイスインターフェイスに設定されている場合は、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用して、デバイス上で IEEE 802.1x をグローバルに有効にする前に、インターフェイスから EtherChannel 構成を削除します。

レイヤ 2 EtherChannel 設定時の注意事項

レイヤ 2 EtherChannels を設定する場合は、次の注意事項に従ってください。

- EtherChannel 内のすべてのポートを同じ VLAN に割り当てるか、またはトランクとして設定してください。複数のネイティブ VLAN に接続されるポートは、EtherChannel を形成できません。
- EtherChannel は、トランキング レイヤ 2 EtherChannel 内のすべてのポート上で同じ VLAN 許容範囲をサポートしています。VLAN 許容範囲が一致していないと、PAgP が **auto** モードまたは **desirable** モードに設定されていても、ポートは EtherChannel を形成しません。
- スパニングツリー パス コストが異なるポートは、設定上の矛盾がない限り、EtherChannel を形成できます。異なるスパニングツリー パス コストを設定すること自体は、EtherChannel を形成するポートの矛盾にはなりません。

関連トピック

レイヤ 2 EtherChannel の設定 （115 ページ）
EtherChannel の概要
EtherChannel のモード
Devices上の EtherChannel
EtherChannel リンクのフェールオーバー
LACP モード （105 ページ）
PAgP モード （102 ページ）
サイレント モード （103 ページ）
ポートチャネル論理インターフェイスの作成
チャネル グループおよびポートチャネル インターフェイス （100 ページ）
物理インターフェイスの設定
EtherChannel ロードバランシングの設定 （121 ページ）
ロードバランシングおよび転送方式 （107 ページ）
MAC アドレス転送 （108 ページ）
IP アドレス転送 （108 ページ）
ロードバランシングの利点 （109 ページ）
PAgP 学習方式およびプライオリティの設定 （124 ページ）
PAgP 学習方式およびプライオリティ （103 ページ）

LACP システム プライオリティの設定 （129 ページ）
LACP ポート プライオリティの設定 （130 ページ）

レイヤ 3 EtherChannel 設定時の注意事項

- レイヤ 3 EtherChannel の場合は、レイヤ 3 アドレスをチャネル内の物理ポートでなく、ポートチャネル論理インターフェイスに割り当ててください。

関連トピック

EtherChannel ロードバランシングの設定 （121 ページ）
ロードバランシングおよび転送方式 （107 ページ）
MAC アドレス転送 （108 ページ）
IP アドレス転送 （108 ページ）
ロードバランシングの利点 （109 ページ）

Auto-LAG

Auto-LAG 機能は、スイッチに接続されたポートで EtherChannel を自動的に作成できる機能です。デフォルトでは、Auto-LAG がグローバルに無効にされ、すべてのポート インターフェイスで有効になっています。Auto-LAG は、グローバルに有効になっている場合にのみ、スイッチに適用されます。

Auto-LAG をグローバルに有効にすると、次のシナリオが可能になります。

- パートナー ポート インターフェイス上に EtherChannel が設定されている場合、すべてのポート インターフェイスが自動 EtherChannel の作成に参加します。詳細については、次の表「アクターとパートナー デバイス間でサポートされる *Auto-LAG* 設定」を参照してください。
- すでに手動 EtherChannel の一部であるポートは、自動 EtherChannel の作成に参加することはできません。
- Auto-LAG がすでに自動で作成された EtherChannel の一部であるポート インターフェイスで無効になっている場合、ポート インターフェイスは自動 EtherChannel からバンドル解除されます。

次の表に、アクターとパートナー デバイス間でサポートされる Auto-LAG 設定を示します。

表 *14 :* アクターとパートナー デバイス間でサポートされる *Auto-LAG* 設定

アクター/パートナー	アクティブ	パッシブ	自動
アクティブ	対応	対応	対応
パッシブ	○	x	○
自動	対応	対応	対応

Auto-LAG をグローバルに無効にすると、自動で作成されたすべての Etherchannel が手動 EtherChannel になります。

既存の自動で作成された EtherChannel で設定を追加することはできません。追加するには、最初に **port-channel**<*channel-number*>**persistent** を実行して、手動 EtherChannel に変換する必要があります。

（注） Auto-LAG は自動 EtherChannel の作成に LACP プロトコルを使用します。一意のパートナー デバイスで自動的に作成できる EtherChannel は 1 つだけです。

Auto-LAG 設定時の注意事項

Auto-LAG 機能を設定するときには、次の注意事項に従ってください。

- Auto-LAG がグローバルで有効な場合、およびポート インターフェイスで有効な場合に、ポート インターフェイスを自動 EtherChannel のメンバーにしたくない場合は、ポート インターフェイスで Auto-LAG を無効にします。
- ポート インターフェイスは、すでに手動 EtherChannel のメンバーである場合、自動 EtherChannel にバンドルされません。自動 EtherChannel にバンドルされるようにするには、まずポート インターフェイスで手動 EtherChannel のバンドルを解除します。
- Auto-LAG が有効になり、自動 EtherChannel が作成されると、同じパートナー デバイスで複数の EtherChannel を手動で作成できます。ただし、デフォルトでは、ポートはパートナー デバイスで自動 EtherChannel の作成を試行します。
- Auto-LAG は、レイヤ 2 EtherChannel でのみサポートされています。レイヤ 3 インターフェイスおよびレイヤ 3 EtherChannel ではサポートされていません。
- Auto-LAG は、Cross-Stack EtherChannel でサポートされています。

EtherChannel の設定方法

EtherChannel の設定後、ポートチャネル インターフェイスに適用した設定変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。また、物理ポートに適用した設定変更は、設定を適用したポートだけに作用します。

レイヤ 2 EtherChannel の設定

Layer2 EtherChannel を設定するには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、チャネルグループにポートを割り当てます。このコマンドにより、ポートチャネル論理インターフェイスが自動的に作成されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `デバイス(config)# interface gigabitethernet2/0/1`	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスは、物理ポートです。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
ステップ 3	**switchport mode** {**access** | **trunk**} 例： `デバイス(config-if)# switchport mode access`	すべてのポートをスタティックアクセス ポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。 ポートをスタティックアクセス ポートとして設定する場合は、ポートを 1 つの VLAN にのみ割り当ててください。指定できる範囲は 1 ～ 4094 です。
ステップ 4	**switchport access vlan** *vlan-id* 例： `デバイス(config-if)# switchport access vlan 22`	ポートをスタティックアクセス ポートとして設定する場合は、ポートを 1 つの VLAN にのみ割り当ててください。指定できる範囲は 1 ～ 4094 です。
ステップ 5	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive**} 例： `デバイス(config-if)# channel-group 5`	チャネル グループにポートを割り当て、PAgP モードまたは LACP モードを指定します。 **mode** には、次のキーワードのいずれか 1 つを選択します。

	コマンドまたはアクション	目的
	`mode auto`	• **auto** –PAgP 装置が検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。このキーワードは、EtherChannel メンバがdevices スタックの異なるdeviceのものである場合にはサポートされません。 • **desirable** –無条件に PAgP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。このキーワードは、EtherChannel メンバがdevices スタックの異なるdeviceのものである場合にはサポートされません。 • **on** – : PAgP または LACP を使用せずにポートが強制的にチャネル化されます。**on** モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポートグループが、**on**モードの別のポートグループに接続する場合だけです。 • **non-silent** –（任意）device が PAgP 対応のパートナーに接続されている場合、ポートが **auto** または **desirable** モードになると非サイレント動作を行うように device ポートを設定します。**non-silent** を指定しなかった場合は、サイレントが指定されたものと見なされます。サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。

	コマンドまたはアクション	目的
		• **active**：LACP 装置が検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • **passive** –：ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。
ステップ 6	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

EtherChannel の概要
EtherChannel のモード
Devices上の EtherChannel
EtherChannel リンクのフェールオーバー
LACP モード （105 ページ）
PAgP モード （102 ページ）
サイレント モード （103 ページ）
EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （111 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）

レイヤ 3 EtherChannel の設定

レイヤ 3 EtherChannel にイーサネット ポートを割り当てるには、この手順を実行します。この手順は必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： デバイス(config)# **interface gigabitethernet 1/0/2**	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
ステップ 4	**no ip address** 例： デバイス(config-if)# **no ip address**	物理ポートに割り当てられている IP アドレスがないことを確認します。
ステップ 5	**no switchport** 例： デバイス(config-if)# **no switchport**	ポートをレイヤ 3 モードにします。
ステップ 6	**channel-group** *channel-group-number* **mode** { **auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive** }	チャネル グループにポートを割り当て、PAgP モードまたは LACP モードを指定します。

	コマンドまたはアクション	目的
	例： デバイス(config-if)# **channel-group 5 mode auto**	**mode** には、次のキーワードのいずれか 1 つを選択します。 • **auto**：PAgP 装置が検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。このキーワードは、EtherChannel メンバがdevice スタックの異なるdevicesのものである場合にはサポートされません。 • **desirable**：無条件に PAgP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。このキーワードは、EtherChannel メンバがdevice スタックの異なるdevicesのものである場合にはサポートされません。 • **on**：PAgP や LACP を使用しないで、ポートを強制的にチャネル化します。**on** モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポートグループが、**on**モードの別のポートグループに接続する場合だけです。 • **non-silent**（任意）device が PAgP 対応のパートナーに接続されている場合、ポートが **auto** または **desirable** モードになると非サイレント動作を行うように device ポートを設定します。**non-silent** を指定しなかった場合は、サイレントが指定されたものと見なされます。サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。サイレントを設定すると、

	コマンドまたはアクション	目的
		PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。 • **active**：LACP 装置が検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートはLACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • **passive** –：ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。
ステップ 7	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

EtherChannel ロードバランシングの設定

複数の異なる転送方式の 1 つを使用するように EtherChannel ロードバランシングを設定できます。

このタスクはオプションです。

手順

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

	コマンドまたはアクション	目的
ステップ 2	**port-channel load-balance** { **dst-ip** | **dst-mac** | **dst-mixed-ip-port** | **dst-port** | **extended** [**dst-ip** | **dst-mac** | **dst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**] | **src-dst-ip** | **src-dst-mac** **src-dst-mixed-ip-port src-dst-portsrc-ip** | **src-mac** | **src-mixed-ip-port** | **src-port**} 例： `デバイス(config)# port-channel load-balance src-mac`	EtherChannel のロードバランシング方式を設定します。 デフォルトは **src-mac**です。 次のいずれかの負荷分散方式を選択します。 • **dst-ip**：宛先ホストの IP アドレスを指定します。 • **dst-mac**：着信パケットの宛先ホストの MAC アドレスを指定します。 • **dst-mixed-ip-port**：ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **dst-port**：宛先 TCP/UDP ポートを指定します。 • **extended**：標準コマンドで使用可能なもの以外に、送信元および宛先の方式を組み合わせた、拡張ロードバランシング方式を指定します。 • **ipv6-label**：IPv6 フロー ラベルを指定します。 • **l3-proto**：レイヤ 3 プロトコルを指定します。 • **src-dst-ip**：送信元および宛先ホストの IP アドレスを指定します。 • **src-dst-mac**：送信元および宛先ホストの MAC アドレスを指定します。 • **src-dst-mixed-ip-port**：送信先および宛先ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **src-dst-port**：送信元および宛先 TCP/UDP ポートを指定します。 • **src-ip**：送信元ホストの IP アドレスを指定します。 • **src-mac**：着信パケットの送信元 MAC アドレスを指定します。

	コマンドまたはアクション	目的
		• **src-mixed-ip-port**：送信元ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **src-port**：送信元 TCP/UDP ポートを指定します。
ステップ 3	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ロードバランシングおよび転送方式 （107 ページ）
MAC アドレス転送 （108 ページ）
IP アドレス転送 （108 ページ）
ロードバランシングの利点 （109 ページ）
EtherChannel 設定時の注意事項
レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）
EtherChannel のデフォルト設定 （111 ページ）
レイヤ 3 EtherChannel 設定時の注意事項 （114 ページ）

EtherChannel 拡張ロードバランシングの設定

ロードバランシング方式を組み合わせて使用する場合には、拡張ロードバランシングを設定します。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**port-channel load-balance extended** [**dst-ip** | **dst-mac dst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**] 例：	EtherChannel 拡張ロードバランシング方式を設定します。 デフォルトは **src-mac**です。

	コマンドまたはアクション	目的
	デバイス(config)# **port-channel load-balance extended dst-ip dst-mac src-ip**	次のいずれかの負荷分散方式を選択します。 • **dst-ip**：宛先ホストの IP アドレスを指定します。 • **dst-mac**：着信パケットの宛先ホストの MAC アドレスを指定します。 • **dst-port**：宛先 TCP/UDP ポートを指定します。 • **ipv6-label**：IPv6 フロー ラベルを指定します。 • **l3-proto**：レイヤ 3 プロトコルを指定します。 • **src-ip**：送信元ホストの IP アドレスを指定します。 • **src-mac**：着信パケットの送信元 MAC アドレスを指定します。 • **src-port**：送信元 TCP/UDP ポートを指定します。
ステップ 3	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。

PAgP 学習方式およびプライオリティの設定

このタスクはオプションです。

手順

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

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `デバイス(config)# interface gigabitethernet 1/0/2`	伝送ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**pagp learn-method physical-port** 例： `デバイス(config-if)# pagp learn-method physical port`	PAgP 学習方式を選択します。 デフォルトでは、**aggregation-port learning** が選択されています。つまり、EtherChannel 内のポートのいずれかを使用して、deviceがパケットを送信元に送信します。集約ポートラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。 物理ポートラーナー `is`である別のdeviceに接続する**physical-port**を選択します。 **port-channel load-balance** グローバル コンフィギュレーション コマンドを **src-mac** に設定してください。 学習方式はリンクの両端で同じ方式に設定する必要があります。
ステップ 4	**pagp port-priority** *priority* 例： `デバイス(config-if)# pagp port-priority 200`	選択したポートがパケット伝送用として選択されるように、プライオリティを割り当てます。 *priority* に指定できる範囲は 0 ～ 255 です。デフォルト値は 128 です。プライオリティが高いほど、ポートが PAgP 伝送に使用される可能性が高くなります。
ステップ 5	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

PAgP 学習方式およびプライオリティ （103 ページ）
EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （111 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ （135 ページ）

レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）

LACP ホット スタンバイ ポートの設定

LACP がイネーブルの場合、ソフトウェアはデフォルトで、チャネルにおける LACP 互換ポートの最大数（最大 16 個のポート）の設定を試みます。一度にアクティブにできる LACP リンクは 8 つだけです。残りの 8 個のリンクがホット スタンバイ モードになります。アクティブ リンクの 1 つが非アクティブになると、ホット スタンバイ モードのリンクが代わりにアクティブになります。

チャネルでアクティブ ポートの最大数を指定することでデフォルト動作を上書きできます。この場合、残りのポートがホット スタンバイ ポートになります。たとえばチャネルで最大 5 個のポートを指定した場合、11 個までのポートがホット スタンバイ ポートになります。

9 つ以上のリンクが EtherChannel グループとして設定された場合、ソフトウェアは LACP プライオリティに基づいてアクティブにするホット スタンバイ ポートを決定します。ソフトウェアは、LACP を操作するシステム間のすべてのリンクに、次の要素（プライオリティ順）で構成された一意のプライオリティを割り当てます。

- LACP システム プライオリティ
- システム ID（device MAC アドレス）
- LACP ポート プライオリティ
- ポート番号

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。プライオリティは、ハードウェア上の制約がある場合に、すべての互換ポートが集約されないように、スタンバイ モードにするポートを決定します。

アクティブ ポートかホット スタンバイ ポートかを判別するには、次の（2 つの）手順を使用します。まず、数値的に低いシステム プライオリティとシステム ID を持つシステムの方を選びます。次に、ポート プライオリティおよびポート番号の値に基づいて、そのシステムのアクティブ ポートとホット スタンバイ ポートを決定します。他のシステムのポート プライオリティとポート番号の値は使用されません。

ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響を与えるように、LACP システム プライオリティおよび LACP ポート プライオリティのデフォルト値を変更できます。

LACP 最大バンドル機能の設定

ポート チャネルで許可されるバンドル化された LACP ポートの最大数を指定すると、ポート チャネル内の残りのポートがホット スタンバイ ポートとして指定されます。

ポート チャネルの LACP ポートの最大数を設定するには、特権 EXEC モードで開始して、次の手順に従います。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *channel-number* 例： `デバイス(config)# interface port-channel 2`	ポート チャネルのインターフェイス コンフィギュレーション モードを開始します。 指定できる範囲は 1 ～ 128 です。
ステップ 3	**lacp max-bundle** *max-bundle-number* 例： `デバイス(config-if)# lacp max-bundle 3`	ポートチャネル バンドルで LACP ポートの最大数を指定します。 指定できる範囲は 1 ～ 8 です。
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

関連トピック

LACP とリンクの冗長性 （106 ページ）
LACP ホット スタンバイ ポートの設定：例 （138 ページ）

LACP ポートチャネル スタンドアロン ディセーブルの設定

ポート チャネルのスタンドアロン EtherChannel メンバー ポート ステートをディセーブルにするには、ポート チャネル インターフェイスで次の作業を行います。

手順

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

	コマンドまたはアクション	目的
ステップ 2	**interface port-channel** *channel-group* 例： デバイス(config)# **interface port-channel** *channel-group*	設定するポート チャネル インターフェイスを選択します。
ステップ 3	**port-channel standalone-disable** 例： デバイス(config-if)# **port-channel standalone-disable**	ポートチャネル インターフェイスのスタンドアロン モードをディセーブルにします。
ステップ 4	**end** 例： デバイス(config-if)# **end**	設定モードを終了します。
ステップ 5	**show etherchannel** 例： デバイス# **show etherchannel** *channel-group* **port-channel** デバイス# **show etherchannel** *channel-group* **detail**	設定を確認します。

LACP ポート チャネルの最小リンク機能の設定

リンク アップ状態で、リンク アップ ステートに移行するポート チャネル インターフェイスの EtherChannel でバンドルする必要のあるアクティブ ポートの最小数を指定できます。EtherChannel の最小リンクを使用して、低帯域幅 LACP EtherChannel がアクティブになることを防止できます。また、LACP EtherChannel にアクティブ メンバー ポートが少なすぎて、必要な最低帯域幅を提供できない場合、この機能により LACP EtherChannel が非アクティブになります。

ポート チャネルに必要なリンクの最小数を設定する。次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	デバイス# **configure terminal**	
ステップ 3	**interface port-channel** *channel-number* 例： デバイス(config)# **interface port-channel 2**	ポートチャネルのインターフェイス コンフィギュレーション モードを開始します。 *channel-number* の範囲は 1 ～ 63 です。
ステップ 4	**port-channel min-links** *min-links-number* 例： デバイス(config-if)# **port-channel min-links 3**	リンク アップ状態で、リンク アップ ステートに移行するポート チャネル インターフェイスの EtherChannel でバンドルする必要のあるメンバ ポートの最小数を指定できます。 *min-links-number* の範囲は 2 ～ 8 です。
ステップ 5	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

LACP とリンクの冗長性 （106 ページ）
LACP ホット スタンバイ ポートの設定：例 （138 ページ）

LACP システム プライオリティの設定

lacp system-priority 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、LACP をイネーブルにしているすべての EtherChannel に対してシステムプライオリティを設定できます。LACP を設定済みの各チャネルに対しては、システムプライオリティを設定できません。デフォルト値を変更すると、ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響します。

どのポートがホットスタンバイモードにあるか確認するには、**show etherchannel summary** 特権 EXEC コマンドを使用します（H ポートステートフラグで表示）。

LACP システムプライオリティを設定するには、次の手順に従います。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	デバイス> **enable**	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lacp system-priority** *priority* 例： デバイス(config)# **lacp system-priority 32000**	LACP システム プライオリティを設定します。 指定できる範囲は 1 ～ 65535 です。デフォルトは 32768 です。 値が小さいほど、システム プライオリティは高くなります。
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。

関連トピック

EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （111 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ （135 ページ）

LACP ポート プライオリティの設定

デフォルトでは、すべてのポートは同じポート プライオリティです。ローカル システムのシステム プライオリティおよびシステム ID の値がリモート システムよりも小さい場合は、LACP EtherChannel ポートのポート プライオリティをデフォルトよりも小さな値に変更して、最初にアクティブになるホット スタンバイ リンクを変更できます。ホット スタンバイ ポートは、番号が小さい方が先にチャネルでアクティブになります。どのポートがホット スタンバイ モードにあるか確認するには、**show etherchannel summary** 特権 EXEC コマンドを使用します（H ポート ステート フラグで表示）。

（注） LACP がすべての互換ポートを集約できない場合（たとえば、ハードウェアの制約が大きいリモート システム）、EtherChannel 中でアクティブにならないポートはすべてホット スタンバイ ステートになり、チャネル化されたポートのいずれかが機能しない場合に限り使用されます。

LACP ポート プライオリティを設定するには、次の手順に従います。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `デバイス(config)# interface gigabitethernet 1/0/2`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**lacp port-priority** *priority* 例： `デバイス(config-if)# lacp port-priority 32000`	LACP ポート プライオリティを設定します。 指定できる範囲は 1 ～ 65535 です。デフォルトは 32768 です。値が小さいほど、ポートが LACP 伝送に使用される可能性が高くなります。
ステップ 5	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （111 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （113 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ （135 ページ）

LACP 高速レート タイマーの設定

LACP タイマー レートを変更することにより、LACP タイムアウトの時間を変更することができます。**lacp rate** コマンドを使用し、LACP がサポートされているインターフェイスで受信される LACP 制御パケットのレートを設定します。タイムアウト レートは、デフォルトのレート（30 秒）から高速レート（1 秒）に変更することができます。このコマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* 例： `デバイス(config)# interface gigabitEthernet 2/1`	インターフェイスを設定し、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	**lacp rate** {**normal** | **fast**} 例： `デバイス(config-if)# lacp rate fast`	LACP がサポートされているインターフェイスで受信される LACP 制御パケットのレートを設定します。 • タイムアウトレートをデフォルトにリセットするには、**no lacp rate** コマンドを使用します。
ステップ 5	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show lacp internal** 例：	設定を確認します。

	コマンドまたはアクション	目的
	デバイス# **show lacp internal** デバイス# **show lacp counters**	

グローバルな Auto-LAG の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[**no**] **port-channel auto** 例： デバイス(config)# **port-channel auto**	スイッチ上の Auto-LAG 機能をグローバルで有効にします。スイッチ上の Auto-LAG 機能をグローバルで無効にするには、このコマンドの no 形式を使用します。 （注） デフォルトでは、auto-LAG 機能は各ポート上でイネーブルになっています。
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show etherchannel auto** 例： デバイス# **show etherchannel auto**	EtherChannel が自動的に作成されたことが表示されます。

ポート インターフェイスでの Auto-LAG の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： デバイス(config)# **interface gigabitethernet 1/0/1**	Auto-LAG を有効にするポート 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	[**no**] **channel-group auto** 例： デバイス(config-if)# **channel-group auto**	（任意）個々のポート インターフェイスで Auto-LAG 機能を有効にします。個々のポート インターフェイス上で Auto-LAG 機能を無効にするには、このコマンドの no 形式を使用します。 （注） デフォルトでは、auto-LAG 機能は各ポート上でイネーブルになっています。
ステップ 5	**end** 例： デバイス(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show etherchannel auto** 例： デバイス# **show etherchannel auto**	EtherChannel が自動的に作成されたことが表示されます。

次のタスク

Auto-LAG での持続性の設定

自動で作成された EtherChannel を手動のものに変更し、既存の EtherChannel に設定を追加するには、persistence コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**port-channel** *channel-number* **persistent** 例： `デバイス# port-channel 1 persistent`	自動で作成された EtherChannel を手動のものに変更し、EtherChannel に設定を追加することができます。
ステップ 3	**show etherchannel summary** 例： `デバイス# show etherchannel summary`	EtherChannel 情報を表示します。

EtherChannel、PAgP、および LACP ステータスのモニタ

この表に記載されているコマンドを使用して EtherChannel、PAgP、および LACP ステータスを表示できます。

表 *15 : EtherChannel*、*PAgP*、および *LACP* ステータスのモニタ用コマンド

コマンド	説明
clear lacp ｛ *channel-group-number* **counters** ｜ **counters** ｝	LACP チャネル グループ情報およびトラフィック カウンタをクリアします。
clear pagp ｛ *channel-group-number* **counters** ｜ **counters** ｝	PAgP チャネル グループ情報およびトラフィック カウンタをクリアします。
show etherchannel ［ *channel-group-number* ｛ **detail** ｜ **load-balance** ｜ **port** ｜ **port-channel** ｜ **protocol** ｜ **summary** ｝］［**detail** ｜ **load-balance** ｜ **port** ｜ **port-channel** ｜ **protocol** ｜ **auto** ｜ **summary** ］	EtherChannel 情報が簡潔、詳細に、1 行のサマリー形式で表示されます。負荷分散方式またはフレーム配布方式、ポート、ポート チャネル、プロトコル、および Auto-LAG 情報も表示されます。

コマンド	説明
show pagp ［ *channel-group-number* ］ { **counters** ｜ **internal** ｜ **neighbor** }	トラフィック情報、内部PAgP設定、ネイバー情報などの PAgP 情報が表示されます。
show pagp ［ *channel-group-number* ］ **dual-active**	デュアルアクティブ検出ステータスが表示されます。
show lacp ［ *channel-group-number* ］{ **counters** ｜ **internal** ｜ **neighbor** ｜**sys-id**}	トラフィック情報、内部LACP設定、ネイバー情報などの LACP 情報が表示されます。
show running-config	設定エントリを確認します。
show etherchannel load-balance	ポートチャネル内のポート間のロードバランシング、またはフレーム配布方式を表示します。

関連トピック

PAgP 学習方式およびプライオリティの設定 （124 ページ）
PAgP 学習方式およびプライオリティ （103 ページ）
LACP システム プライオリティの設定 （129 ページ）
LACP ポート プライオリティの設定 （130 ページ）

EtherChannel の設定例

レイヤ 2 EtherChannel の設定：例

この例では、スタック内の 1 つのdeviceに EtherChannel を設定する例を示します。2 つのポートを VLAN 10 のスタティックアクセスポートとして、PAgP モードが **desirable** であるチャネル 5 に割り当てます。

```
デバイス# configure terminal
デバイス(config)# interface range gigabitethernet2/0/1 -2
デバイス(config-if-range)# switchport mode access
デバイス(config-if-range)# switchport access vlan 10
デバイス(config-if-range)# channel-group 5 mode desirable non-silent
デバイス(config-if-range)# end
```

この例では、スタック内の 1 つのdeviceに EtherChannel を設定する例を示します。2 つのポートは VLAN 10 のスタティックアクセス ポートとして、LACP モードが active であるチャネル 5 に割り当てられます。 **active :**

```
デバイス# configure terminal
デバイス(config)# interface range gigabitethernet2/0/1 -2
```

```
デバイス(config-if-range)# switchport mode access
デバイス(config-if-range)# switchport access vlan 10
デバイス(config-if-range)# channel-group 5 mode active
デバイス(config-if-range)# end
```

次の例では、クロススタック EtherChannel を設定する方法を示します。LACP パッシブ モードを使用して、VLAN 10 内のスタティックアクセス ポートとしてスタック メンバ 1 のポートを 2 つ、スタック メンバ 2 のポートを 1 つチャネル 5 に割り当てます。

```
デバイス# configure terminal
デバイス(config)# interface range gigabitethernet2/0/4 -5
デバイス(config-if-range)# switchport mode access
デバイス(config-if-range)# switchport access vlan 10
デバイス(config-if-range)# channel-group 5 mode passive
デバイス(config-if-range)# exit
デバイス(config)# interface gigabitethernet3/0/3
デバイス(config-if)# switchport mode access
デバイス(config-if)# switchport access vlan 10
デバイス(config-if)# channel-group 5 mode passive
デバイス(config-if)# exit
```

PoE または LACP ネゴシエーションのエラーは、スイッチからアクセスポイント（AP）に 2 つのポートを設定した場合に発生する可能性があります。このシナリオは、ポートチャネルの設定をスイッチ側で行うと回避できます。詳細については、次の例を参照してください。

```
interface Port-channel1
  switchport access vlan 20
 switchport mode access
  switchport nonegotiate
  no port-channel standalone-disable   <--this one
  spanning-tree portfast
```

（注） ポートがポートのフラッピングに関する LACP エラーを検出した場合は、次のコマンドも含める必要があります。 **no errdisable detect cause pagp-flap**

レイヤ 3 EtherChannel の設定：例

この例では、レイヤ 3 インターフェイスの設定方法を示します。2 つのポートは、LACP モードが **active** であるチャネル 5 に割り当てられます。

```
デバイス# configure terminal
デバイス(config)# interface range gigabitethernet2/0/1 -2
デバイス(config-if-range)# no ip address
デバイス(config-if-range)# no switchport
デバイス(config-if-range)# channel-group 5 mode active
デバイス(config-if-range)# end
```

この例では、クロススタック レイヤ 3 EtherChannel の設定方法を示します。スタック メンバー 2 の 2 つのポートとスタック メンバー 3 の 1 つのポートは、LACP active モードでチャネル 7 に割り当てられます。

```
デバイス# configure terminal
デバイス(config)# interface range gigabitethernet2/0/4 -5
デバイス(config-if-range)# no ip address
デバイス(config-if-range)# no switchport
デバイス(config-if-range)# channel-group 7 mode active
デバイス(config-if-range)# exit
デバイス(config)# interface gigabitethernet3/0/3
デバイス(config-if)# no ip address
デバイス(config-if)# no switchport
デバイス(config-if)# channel-group 7 mode active
デバイス(config-if)# exit
```

LACP ホット スタンバイ ポートの設定：例

この例では、少なくとも 3 個のアクティブ ポートがある場合にアクティブ化される EtherChannel を設定する例を示します（ポート チャネル 2）。これは、7 個のアクティブ ポートとホット スタンバイ ポートとしての最大 9 個の残りのポートから構成されます。

```
デバイス# configure terminal
デバイス(config)# interface port-channel 2
デバイス(config-if)# port-channel min-links 3
デバイス(config-if)# lacp max-bundle 7
```

次に、ポート チャネル 42 のスタンドアロン EtherChannel メンバ ポート ステートをディセーブルにする例を示します。

```
デバイス(config)# interface port-channel channel-group
デバイス(config-if)# port-channel standalone-disable
```

次に、設定を確認する例を示します。

```
デバイス# show etherchannel 42 port-channel | include Standalone
Standalone Disable  = enabled
デバイス# show etherchannel 42 detail | include Standalone
Standalone Disable  = enabled
```

関連トピック

LACP 最大バンドル機能の設定 （126 ページ）
LACP とリンクの冗長性 （106 ページ）
LACP ポート チャネルの最小リンク機能の設定 （128 ページ）

Auto-LAG の設定：例

次に、スイッチに Auto-LAG を設定する例を示します。

```
device> enable
device# configure terminal
device (config)# port-channel auto
device (config-if)# end
device#  show etherchannel auto
```

次の例は、自動的に作成された EtherChannel の概要を示します。

```
device# show etherchannel auto
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SUA)        LACP      Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

次の例は、**port-channel** 1 **persistent** コマンドを実行した後の自動 EtherChannel の概要を示します。

```
device# port-channel 1 persistent

device# show etherchannel summary
Switch# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

EtherChannels の追加リファレンス

関連資料

関連項目	マニュアル タイトル
レイヤ2コマンドリファレンス	『*Layer 2/3 Command Reference (Catalyst 3650 Switches)*』

標準および RFC

標準/RFC	タイトル
なし	—

MIB

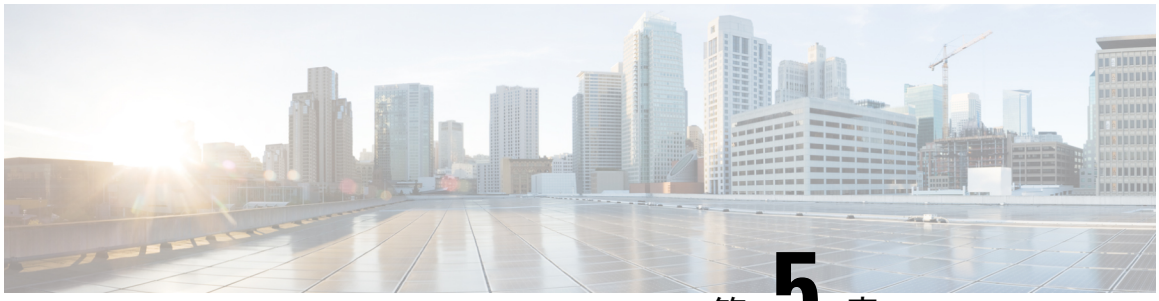
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

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

EtherChannels の機能情報

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	この機能が導入されました。
Cisco IOS 15.2(3)E2、Cisco IOS XE 3.7.2E	Auto-LAG機能が導入されました。



第 5 章

Resilient Ethernet Protocol の設定

機能情報の確認

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

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

REP の概要

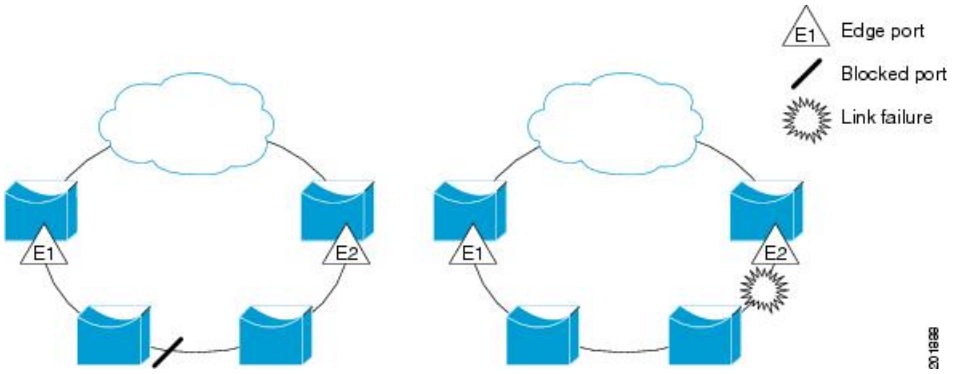
Resilient Ethernet Protocol（REP）はシスコ独自のプロトコルで、スパニングツリー プロトコル（STP）に代わるプロトコルとして、ネットワーク ループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。REP は、セグメントに接続されているポートのグループを制御することで、セグメントがブリッジングループを作成するのを防ぎ、セグメント内のリンク障害に応答します。REP は、より複雑なネットワークを構築するための基盤を提供し、VLAN ロード バランシングをサポートします。

REP セグメントは、相互接続されたポートのチェーンで、セグメント ID が設定されます。各セグメントは、標準（非エッジ）セグメント ポートと、2 つのユーザ設定エッジ ポートで構成されています。1 ルータは同じセグメントに属するポートを複数持たず、各セグメント ポート

にある外部ネイバーは1つだけです。セグメントは共有メディアを通過できますが、どのリンクであっても同じセグメントに属することができるのは2ポートだけです。REPはトランクのイーサネット フロー ポイント（EFP）インターフェイスでのみサポートされます。

次の図に、4 つのスイッチにまたがる 6 つのポートで構成されているセグメントの例を示します。ポート E1 および E2 がエッジ ポートとして設定されています。（左側のセグメントのように）すべてのポートが動作可能の場合、斜線で表しているように単一ポートがブロックされます。ネットワークに障害が発生した場合、ブロックされたポートがフォワーディング ステートに戻り、ネットワークの中断を最小限に抑えます。

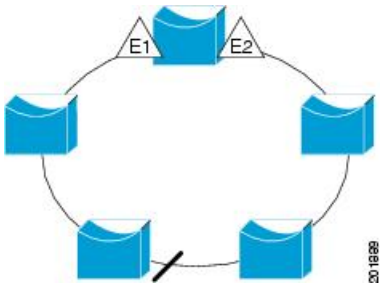
図 *22 : REP* オープン セグメント



上の図に示されたセグメントは、オープンセグメントで、2つのエッジポート間は接続されていません。REP セグメントはブリッジング ループの原因とならないため、セグメント エッジを安全に任意のネットワークに接続できます。セグメント内のルータに接続されているすべてのホストには、エッジポートを通じて残りのネットワークに接続する方法が2つありますが、いつでもアクセス可能なのは 1 つだけです。いずれかのセグメントまたは REP セグメントのいずれかのポートに障害が発生した場合、REP はすべてのポートのブロックを解除し、他のゲートウェイ経由で接続できるようにします。

下の図に示すセグメントはリング セグメントであり、同じルータ上に両方のエッジ ポートがあります。この設定を使用すると、セグメント内の任意の2ルータ間で冗長接続を形成することができます。

図 *23 : REP* リング セグメント



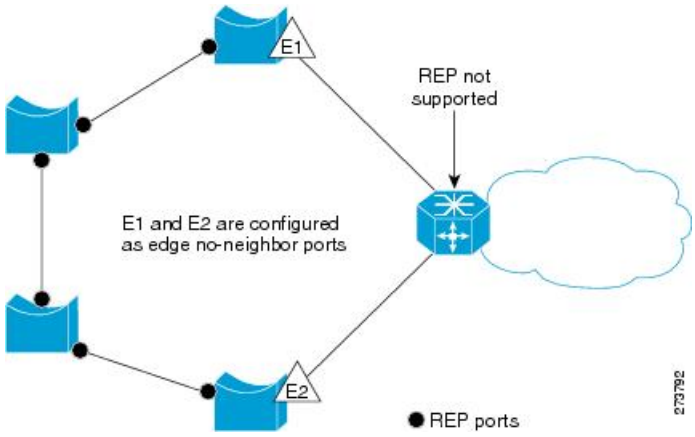
REP セグメントには、次のような特徴があります。

- セグメント内の全ポートが動作可能な場合、1ポート（代替ポートと呼ばれる）が各VLANでブロック ステートとなります。VLAN ロード バランシングが設定されている場合は、セグメント内の 2 つのポートが VLAN のブロック ステートを制御します。
- セグメント内の1つまたは複数のポートが動作不能になると、リンク障害が発生して、すべてのポートがすべての VLAN トラフィックを転送して、接続性を確保します。
- リンク障害の場合、できるだけ早期に代替ポートのブロックが解除されます。障害リンクが復旧すると、ネットワークの中断を最小限に抑えるようにVLAN単位で論理的にブロックされたポートが選択されます。

REP セグメントに基づいて、ほとんどのネットワーク タイプを構成することができます。またREPはプライマリ エッジ ポートで制御され、セグメント内の任意のポートで発生するVLANロード バランシングをサポートします。

アクセス リング トポロジでは、下の図に示すように、ネイバー スイッチでREPがサポートされない場合があります。この場合、そのスイッチ側のポート（E1 と E2）を非ネイバー エッジ ポートとして設定できます。これらのポートは、エッジ ポートのすべての特性を継承するため、他のエッジ ポートと同じように設定できます。たとえば、STP や REP のトポロジ変更通知を集約スイッチに送信するように設定することもできます。この場合、送信されるSTPトポロジ変更通知（TCN）は、Multiple Spanning-Tree（MST）STP メッセージです。

図 *24*：非ネイバー エッジ ポート



REP には次のような制限事項があります。

- 各セグメント ポートを設定する必要があります。設定を間違えると、ネットワーク内でフォワーディング ループが発生します。
- REPはセグメント内の単一障害ポートだけを管理できます。REPセグメント内の複数ポート障害の場合、ネットワークの接続が中断します。
- 冗長ネットワーク内だけに REP を設定します。冗長性のないネットワークに REP を設定すると、接続が失われます。

リンク完全性

REP は、リンク完全性の確認にエッジ ポート間でエンドツーエンド ポーリング機能を使用しません。ローカル リンク障害検出を実装しています。REP リンク ステータス レイヤ（LSL）が REP 対応ネイバーを検出して、セグメント内の接続性を確立します。すべての VLAN は、ネイバーが検出されるまでインターフェイス上でブロックされます。ネイバーが特定されたあと、REP が代替ポートとなるネイバー ポートと、トラフィックを転送するポートを決定します。

セグメント内のポートごとに、一意のポート ID が割り当てられます。ポート ID フォーマットは、スパニングツリーアルゴリズムで使用されるものと類似しており、ポート番号（ブリッジ上で一意）と、関連 MAC アドレス（ネットワーク内で一意）から構成されます。セグメント ポートが起動すると、ポートの LSL がセグメント ID およびポート ID を含むパケットの送信を開始します。ポートは、同じセグメント内のネイバーとのスリーウェイ ハンドシェイクを実行したあとで、動作可能と宣言されます。

次のような場合、セグメント ポートは動作可能になりません。

- ネイバーに同じセグメント ID がない
- 複数のネイバーに同じセグメント ID がある
- ネイバーがピアとして、ローカル ポートに確認応答しない

各ポートは、直近のネイバーと隣接関係を確立します。ネイバー関係が確立されると、ポートがセグメントの 1 つのブロックされたポート（代替ポート）を決定するようにネゴシエートします。その他のポートのブロックは解除されます。デフォルトで、REP パケットは BPDU クラス MAC アドレスに送信されます。パケットは、シスコ マルチキャスト アドレスにも送信できますが、セグメントに障害が発生した場合にブロックされたポートのアドバタイズ（BPA）メッセージの送信だけに使用されます。パケットは、REP が動作していない装置によって廃棄されます。

短時間でのコンバージェンス

REP は、物理リンク ベースで動作し、VLAN 単位ベースでは動作しません。すべての VLAN に対して 1 つの hello メッセージしか必要ないため、プロトコル上の負荷が軽減されます。指定セグメント内の全スイッチで継続的に VLAN を作成し、REP トランク ポート上に同じ許容 VLAN を設定することを推奨します。ソフトウェアでのメッセージのリレーによって発生する遅延を回避するために、REP ではいくつかのパケットを通常のマルチキャスト アドレスにフラッディングすることも可能です。これらのメッセージはハードウェア フラッド レイヤ（HFL）で動作し、REP セグメントだけではなくネットワーク全体にフラッディングされます。セグメントに属していないスイッチは、これらのメッセージをデータ トラフィックとして扱います。ドメイン全体または特定のセグメントの管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

予想されるコンバージェンス復旧時間は、150 ～ 500 ms で、最大 1000 の MAC と 5 つの VLAN となります。マルチキャスト トラフィックの予想されるコンバージェンス復旧時間は、300 ～ 500 ms で、最大 100 のグループと 5 つの VLAN となります。

VLAN ロード バランシング

REP セグメント内の 1 つのエッジ ポートがプライマリ エッジ ポートとして機能し、もう一方がセカンダリ エッジ ポートとなります。セグメント内の VLAN ロード バランシングに常に参加しているのがプライマリ エッジ ポートです。REP VLAN バランシングは、設定された代替ポートでいくつかの VLAN をブロックし、プライマリ エッジ ポートでその他の全 VLAN をブロックすることで実行されます。VLAN ロード バランシングを設定する際に、次の 3 種類の方法のいずれかを使用して代替ポートを指定できます。

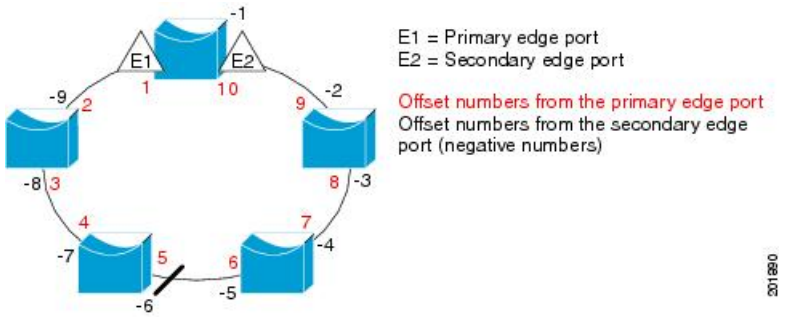
- インターフェイスにポート ID を入力します。セグメント内のポート ID を識別するには、ポートの **show interface rep** detail インターフェイス コンフィギュレーション コマンドを入力します。
- セグメント内のポートのネイバー オフセット番号を入力します。これは、エッジ ポートのダウンストリーム ネイバー ポートを識別するものです。ネイバー オフセット番号の範囲は、-256 ～ +256 で、0 値は無効です。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負数は、セカンダリ エッジ ポート（オフセット番号 -1）とそのダウンストリーム ネイバーを示します。

（注） プライマリ（またはセカンダリ）エッジポートからポートのダウンストリーム位置を識別することで、プライマリ エッジ ポートのオフセット番号を設定します。番号 1 はプライマリ エッジ ポート自体のオフセット番号なので、オフセット番号 1 は入力しないでください。

下の図に、E1 がプライマリ エッジ ポートで E2 がセカンダリ エッジ ポートの場合の、セグメントのネイバーオフセット番号を示します。リングの内側にある赤い番号は、プライマリ エッジ ポートからのオフセット番号で、リングの外側にある黒い番号がセカンダリ エッジ ポートからのオフセット番号です。正のオフセット番号（プライマリ エッジ ポートからのダウンストリーム位置）または負のオフセット番号（セカンダリ エッジ ポートからのダウンストリーム位置）のいずれかにより、（プライマリ エッジ ポートを除く）全ポートを識別できます。E2 がプライマリ エッジ ポートになるとオフセット番号 1 となり、E1 のオフセット番号が -1 になります。

- **preferred** キーワードを入力します。これにより、**rep segment***segment-id***preferred** インターフェイス コンフィギュレーション コマンドで優先代替ポートとしてすでに設定されているポートを選択します。

図 *25 :* セグメント内のネイバー オフセット番号



REP セグメントが完了すると、すべての VLAN がブロックされます。VLAN ロード バランシングを設定する際には、次の2種類の方法のいずれかを使用してトリガーを設定する必要もあります。

- プライマリ エッジ ポートのあるスイッチ上で **rep preempt segment** *segment-id* 特権 EXEC コマンドを入力することで、いつでも手動で VLAN ロード バランシングをトリガーすることができます。
- **rep preempt delay** *seconds* 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、プリエンプション遅延時間を設定できます。リンク障害が発生して回復すると、設定されたプリエンプション期間の経過後に VLAN ロード バランシングが開始されます。設定時間が経過する前に別のポートで障害が発生した場合、遅延タイマーが再開されることに注意してください。

（注） VLAN ロード バランシングが設定されている場合、手動での介入またはリンク障害および回復によってトリガーされるまで、動作が開始されません。

VLAN ロード バランシングがトリガーされると、プライマリ エッジ ポートがメッセージを送信して、セグメント内の全インターフェイスにプリエンプションについて警告します。メッセージがセカンダリ ポートで受信されると、これがネットワークに反映され、メッセージ内で指定された VLAN セットをブロックするように代替ポートに通知し、残りの VLAN をブロックするようにプライマリ エッジ ポートに通知します。

またすべての VLAN をブロックするために、セグメント内の特定ポートを設定できます。プライマリ エッジ ポートだけによって VLAN ロード バランシングが開始され、セグメントが各エンドでエッジ ポートによって終端されていない場合開始することができません。プライマリ エッジ ポートは、ローカル VLAN ロード バランシング設定を決定します。

ロード バランシングを再設定するには、プライマリ エッジ ポートを再設定します。ロード バランシング設定を変更すると、プライマリ エッジ ポートでは、再び **rep preempt segment** コマンドが実行されるか、ポート障害および復旧のあとで設定済みプリエンプト遅延期間が経過してから、新規設定が実行されます。エッジ ポートを通常セグメント ポートに変更しても、既存の VLAN ロード バランシング ステータスは変更されません。新規エッジ ポートを設定すると、新規トポロジ設定になる可能性があります。

スパニングツリー インタラクション

REP は STP とやり取りしませんが、共存はできます。セグメントに属しているポートはスパニングツリーの制御から削除されるため、セグメント ポートでは STP BPDU の送受信は行われません。したがって、STP はセグメント上で実行できません。

STP リング コンフィギュレーションから REP セグメント コンフィギュレーションに移行するには、まずリング内の単一ポートをセグメントの一部として設定し、次にセグメント数を最小限にするように隣接するポートを設定します。各セグメントには、常にブロックされたポートが含まれているので、セグメントが複数になるとブロックされたポートも複数になり、接続が失われる可能性があります。セグメントがエッジポートの場所まで両方向に設定されたら、次にエッジ ポートを設定します。

REP ポート

REP セグメントは、障害ポート、オープン ポート、および代替ポートで構成されます。

- 標準セグメント ポートとして設定されたポートは、障害ポートとして起動します。
- ネイバー との隣接関係が確立されると、ポートは代替ポート ステートに移行して、インターフェイス内の全 VLAN をブロックします。ブロックされたポートのネゴシエーションが発生して、セグメントが安定すると、ブロックされたポートのうちの 1 つが代替ロールのままになって他のすべてのポートがオープン ポートになります。
- リンク内に障害が発生すると、すべてのポートが障害ステートに移行します。代替ポートは、障害通知を受信すると、すべての VLAN を転送するオープン ステートに遷移します。

通常セグメント ポートをエッジ ポートに変換しても、エッジ ポートを通常セグメント ポートに変換しても、必ずトポロジ変更が発生するわけではありません。エッジポートを通常セグメント ポートに変更する場合、設定されるまで VLAN ロード バランシングは実装されません。VLAN ロード バランシングの場合、セグメント内に 2 つのエッジ ポートを設定する必要があります。

スパニングツリー ポートとして再設定されたセグメント ポートは、スパニングツリー設定に従って再起動します。デフォルトでは、これは指定ブロッキング ポートです。PortFast が設定されていたり、STP がディセーブルの場合、ポートはフォワーディング ステートになります。

REP の設定方法

セグメントは、チェーンで相互接続しているポートの集合で、セグメント ID が設定されています。REP セグメントを設定するには、REP 管理 VLAN を設定し（またはデフォルト VLAN 1 を使用し）、次にインターフェイス コンフィギュレーション モードを使用してセグメントにポートを追加します。2 つのエッジ ポートをセグメント内に設定して、1 つをプライマリ エッジ ポート、もう 1 つをデフォルトでセカンダリ エッジ ポートにします。1 セグメント内のプライマリ エッジ ポートは 1 つだけです。別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグ

メントのプライマリ エッジ ポートとして機能させます。オプションで、セグメント トポロジ変更通知（STCN）およびVLANロードバランシングを送信する場所を設定することもできます。

REP のデフォルト設定

REPはすべてのインターフェイス上でディセーブルです。イネーブルにする際に、エッジポートとして設定されていなければインターフェイスは通常セグメント ポートになります。

REPをイネーブルにする際に、STCNの送信はディセーブルで、すべてのVLANはブロックされ、管理 VLAN は VLAN 1 になります。

VLANロードバランシングがイネーブルの場合、デフォルトは手動でのプリエンプションで、遅延タイマーはディセーブルになっています。VLAN ロード バランシングが設定されていない場合、手動でのプリエンプション後のデフォルト動作は、プライマリ エッジ ポートで全 VLAN がブロックとなります。

REP 設定時の注意事項

REP の設定時には、次の注意事項に従ってください。

- まず1ポートの設定から始めて、セグメント数とブロックされたポートの数を最小限に抑えるように隣接するポートを設定することを推奨します。
- 外部ネイバーが設定されておらずセグメント内では3つ以上のポートに障害が発生した場合、1ポートがデータ パス用のフォワーディング ステートになり、設定中の接続性の維持に役立ちます。**show rep interface** コマンド出力では、このポートのポートロールは「Fail Logical Open」と表示され、他の障害ポートのポートロールは「Fail No Ext Neighbor」と表示されます。障害ポートの外部ネイバーが設定されている場合、ポートは代替ポート ステートに移行して、代替ポート選択メカニズムに基づいて最終的にオープン ステートになるか、代替ポートのままになります。
- REP ポートは、レイヤ 2 IEEE 802.1Q またはトランク ポートのいずれかである必要があります。
- 同じ許可 VLAN のセットでセグメント内のすべてのトランク ポートを設定することを推奨します。
- Telnet接続を通じてREPを設定する際には注意してください。これは、別のREPインターフェイスがブロック解除のメッセージを送信するまで、REP はすべての VLAN をブロックするためです。同じインターフェイス経由でルータにアクセスするTelnetセッションで REP をイネーブルにすると、ルータへの接続が失われることがあります。
- 同じセグメントやインターフェイスで REP と STP を実行することはできません。
- STP ネットワークを REP セグメントに接続する場合、接続はセグメント エッジであることを確認してください。エッジで実行されていないSTP接続は、REPセグメントではSTPが実行されないため、ブリッジング ループが発生する可能性があります。すべての STP BPDU は、REP インターフェイスで廃棄されます。

- 同じ許容 VLAN セットでセグメント内のすべてのトランク ポートを設定する必要があります。そうでない場合、設定ミスが発生します。
- REP がスイッチの 2 ポートでイネーブルの場合、両方のポートが通常セグメント ポートまたはエッジ ポートである必要があります。REP ポートは以下の規則に従います。
  - スイッチ上の REP ポートの数に制限はありませんが、同じ REP セグメントに属することができるスイッチ上のポートは 2 つだけです。
  - セグメント内にスイッチ上の 1 ポートだけが設定されている場合、そのポートがエッジ ポートとなります。
  - 同じセグメント内に属するスイッチに 2 つのポートがある場合、両方のポートがエッジポートであるか、両方のポートが通常セグメント ポートであるか、一方が通常ポートでもう一方が非ネイバー エッジ ポートである必要があります。スイッチ上のエッジ ポートと通常セグメント ポートが同じセグメントに属することはできません。
  - スイッチ上の 2 ポートが同じセグメントに属していて、1 つがエッジ ポートとして設定され、もう 1 つが通常セグメント ポートに設定されている場合（設定ミス）、エッジ ポートは通常セグメント ポートとして扱われます。
- REP インターフェイスはブロックされた状態になり、ブロック解除できるようになるまでブロックされた状態のまま残ります。突然の接続切断を避けるために、このステータスを認識しておく必要があります。
- REP はネイティブ VLAN 上においてすべての LSL PDU をタグなしフレームで送信します。シスコ マルチキャスト アドレスに送信された BPA メッセージは、管理 VLAN で送信されます。これはデフォルトで VLAN 1 です。
- ネイバーからの hello が受信されないままどのくらいの時間が経過すると REP インターフェイスがダウンするかを設定できます。**rep lsl-age-timer** value インターフェイス コンフィギュレーション コマンドを使用して、120 ～ 10000 ミリ秒の時間を設定します。LSL hello タイマーは、このエージング タイマーの値を 3 で割った値に設定されます。通常の動作では、ピア スイッチのエージング タイマーが満了になって hello メッセージが確認されるまでに LSL hello が 3 回送信されます。
  - EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。ポート チャネルで 1000 ミリ秒未満の値を設定しようとすると、エラー メッセージが表示されてコマンドが拒否されます。
- REP ポートは、次のポート タイプのいずれかに設定できません。
  - スイッチド ポート アナライザ（SPAN）宛先ポート
  - トンネル ポート
  - アクセスポート
- REP は EtherChannel でサポートされていますが、EtherChannel に属する個別のポートではサポートされません。

- スイッチごとに最大 26 の REP セグメントを設定できます。

REP 管理 VLAN の設定

リンク障害メッセージ、およびロード バランシング時の VLAN ブロッキング通知によって作成される遅延を回避するため、REP はハードウェア フラッド レイヤ（HFL）で通常のマルチキャスト アドレスにパケットをフラッディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。管理 VLAN を設定することで、これらのメッセージのフラッディングを制御できます。

REP 管理 VLAN を設定する場合、次の注意事項に従ってください。

- 管理 VLAN を設定しない場合、デフォルトは VLAN 1 です。
- すべてのセグメントに対し 1 つの管理 VLAN をスイッチで設定できます。
- 管理 VLAN は RSPAN VLAN になりません。

REP 管理 VLAN を設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**rep admin vlan** *vlan-id* 例： `デバイス(config)# rep admin vlan 2`	管理 VLAN を指定します。範囲は 2 ～ 4094 です。 管理 VLAN をデフォルトの 1 に設定するには、**no rep admin vlan** グローバル コンフィギュレーション コマンドを入力します。
ステップ 3	**end** 例： `デバイス(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 4	**show interface**［*interface-id*］**rep detail** 例： `デバイス# show interface gigabitethernet1/1 rep detail`	（任意）REP インターフェイスの設定を検証します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup config** 例： デバイス# **copy running-config startup config**	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

REP インターフェイスの設定

REP 動作の場合、各セグメント インターフェイスで REP をイネーブルにして、セグメント ID を指定する必要があります。このタスクは必須で、他の REP 設定の前に実行する必要があります。また、各セグメントにプライマリおよびセカンダリ エッジ ポートを設定する必要があります。その他のステップはすべて任意です。

インターフェイスで REP をイネーブルにし、設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id*	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レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。指定できるポート チャネルの範囲は 1 ～ 48 です。
ステップ 4	**switchport mode trunk**	インターフェイスをレイヤ 2 トランク ポートとして設定します。
ステップ 5	**rep segment** *segment-id* [**edge** [**no-neighbor**] [[**primary**]] [**preferred**]	インターフェイス上で REP をイネーブルにして、セグメント番号を特定します。指定できるセグメント ID の範囲は 1 ～ 1024 です。これらの任意のキーワードは利用可能です。

	コマンドまたはアクション	目的
		（注） 各セグメントに1つのプライマリ エッジ ポートを含めて、2つのエッジポートを設定する必要があります。 • （任意）**edge**：エッジポートとしてポートを設定します。各セグメントにあるエッジ ポートは2つだけです。**primary** キーワードなしで **edge** を入力すると、ポートがセカンダリエッジポートとして設定されます。 • （任意）**primary**：プライマリエッジポート（VLAN ロードバランシングを設定できるポート）としてポートを設定します。 • （任意）**no-neighbor**：エッジポートとして外部REP ネイバーを使用せずにポートを設定します。そのポートはエッジポートのすべての特性を継承するため、他のエッジポートと同じように設定できます。 （注） 各セグメントにあるプライマリエッジポートは1つだけですが、2 つの異なるスイッチにエッジポートを設定して **primary** キーワードを両方のスイッチに入力しても、その設定は有効です。ただし、REP ではセグメント プライマリ エッジ ポートとして 1 つのポートだけが選択されます。**show rep topology** 特権 EXEC コマンドを入力すると、セグメントのプライマリエッジポートを特定できます。 • （任意）**preferred**：ポートが優先代替ポートであるか、VLAN ロー

	コマンドまたはアクション	目的
		ドバランシングの優先ポートであるかを示します。 （注） ポートを優先に設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。
ステップ 6	**rep stcn** {**interface** *interface id* | **segment** *id-list* | **stp**}	（任意）STCN を送信するようにエッジ ポートを設定します。 • **interface** *interface -id*：物理インターフェイスまたはポート チャネルを指定して、STCN を受け取ります。 • **segment** *id-list*：STCN を受け取る 1 つ以上のセグメントを特定します。有効な範囲は 1 ～ 1024 です。 • **stp**：STCN を STP ネットワークに送信します。 （注） STCN を STP ネットワークに送信するために rep stcn stp を設定する場合は、スパニング ツリー モード mst がネイバーなしのエッジ ノード上に必要です。
ステップ 7	**rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}	（任意）プライマリ エッジ ポートに VLAN ロード バランシングを設定して、3 つの方法のいずれかを使用して REP 代替ポートを特定し、代替ポートでブロックされるように VLAN を設定します。 • **id***port-id*：ポート ID で代替ポートを特定します。セグメント内の各ポートにポート ID が自動的に生成されます。**show interface** *type number* **rep** [**detail**] 特権 EXEC コマ

	コマンドまたはアクション	目的
		ンドを入力し、インターフェイスポート ID を表示できます。 • *neighbor_offset*：エッジポートからのダウンストリーム ネイバーとして代替ポートを特定するための番号。有効範囲は -256 ～ 256 で、負数はセカンダリ エッジポートからのダウンストリーム ネイバーを示します。**0** の値が無効です。**-1** を入力して、セカンダリエッジポートを代替ポートとして識別します。ネイバーオフセット番号付けの例については、図 25 : セグメント内のネイバー オフセット番号（148ページ）を参照してください。 （注） プライマリ エッジ ポート（オフセット番号 1）にこのコマンドを入力するので、代替ポートを特定するのにオフセット値 1 を入力できません。 • **preferred**：すでに VLAN ロードバランシングの優先代替ポートとして指定されている通常セグメント ポートを選択します。 • **vlan** *vlan-list*：1 つの VLAN または VLAN の範囲をブロックします。 • **vlan all**：すべての VLAN をブロックします。 （注） REP プライマリ エッジ ポート上にだけこのコマンドを入力します。
ステップ 8	**rep preempt delay** *seconds*	（任意）プリエンプト遅延時間を設定します。 • リンク障害が発生して復旧した後に、VLAN ロードバランシングを自動的にトリガーするには、このコマンドを使用します。

	コマンドまたはアクション	目的
		• 遅延時間の範囲は 15 ～ 300 秒です。デフォルトは、遅延時間のない手動によるプリエンプションです。 （注） REP プライマリ エッジ ポート上にだけこのコマンドを入力します。
ステップ 9	**rep lsl-age-timer** *value*	（任意）ネイバーからの hello が受信されないままどのくらいの時間（ミリ秒）が経過すると REP インターフェイスがダウンするかを設定します。 指定できる範囲は 120 ～ 10000 ミリ秒（40 ミリ秒単位）です。デフォルト値は 5000 ミリ秒（5 秒）です。 （注） • EtherChannel ポート チャネルインターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。 • リンクのフラップを避けるため、リンクの両方のポートに同じ LSL エージが設定されている必要があります。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show interface** ［*interface-id*］ **rep** [**detail**]	（任意）REP インターフェイスの設定を表示します。
ステップ 12	**copy running-config startup-config**	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

VLAN ロード バランシングの手動によるプリエンプションの設定

プライマリエッジポートで **rep preempt delay***seconds* rep preempt delay seconds インターフェイス コンフィギュレーション コマンドを入力しないで、プリエンプション時間遅延を設定する

場合、デフォルトではセグメントで VLAN ロードバランシングを手動でトリガーします。手動で VLAN ロード バランシングをプリエンプトする前に、他のすべてのセグメント設定が完了しているかどうか確認してください。**rep preempt delay segment** *segment-id* コマンドを入力すると、プリエンプションによってネットワークが中断する可能性があるため、コマンド実行前に確認メッセージが表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**rep preempt segment** *segment-id*	手動により、セグメント上の VLAN ロード バランシングをトリガーします。 実行前にコマンドを確認する必要があります。
ステップ 2	**show rep topology segment** *segment-id*	REP トポロジ情報を表示します。

REP の SNMP トラップ設定

REP 固有のトラップを送信して、簡易ネットワーク管理プロトコル（SNMP）サーバにリンクの動作状態の変更およびすべてのポート役割の変更を通知するようにルータを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp mib rep trap-rate** *value* 例： `Switch(config)# snmp mib rep trap-rate 500`	スイッチで REP トラップの送信をイネーブルにして、1 秒あたりのトラップの送信数を設定します。 • 1 秒あたりのトラップの送信数を入力します。範囲は 0 ～ 1000 です。デフォルトは 0（制限なし、発生するたびにトラップが送信される）です。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**show running-config** 例： `Switch# show running-config`	（任意）実行コンフィギュレーションを表示します。これを使用してREPトラップ コンフィギュレーションを検証できます。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

REP のモニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	**show interface**［*interface-id*］**rep**［**detail**］	特定のインターフェイスまたはすべてのインターフェイスのREPの設定とステータスを表示します。 • （任意）**detail**：インターフェイス固有の REP 情報を表示します。
ステップ 2	**show rep topology**［**segment** *segment-_id*］［**archive** ］［**detail**］	セグメント内のプライマリおよびセカンダリ エッジ ポートを含む、1 セグメントまたは全セグメントの REP トポロジ情報を表示します。 • （任意）**archive**：最後の安定したトポロジを表示します。 （注） アーカイブのトポロジは、スイッチをリロードすると保持されません。 • （任意）**detail**：詳細なアーカイブ情報を表示します。

REP に関する追加情報

関連資料

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

標準および RFC

標準/RFC	タイトル
なし	—

MIB

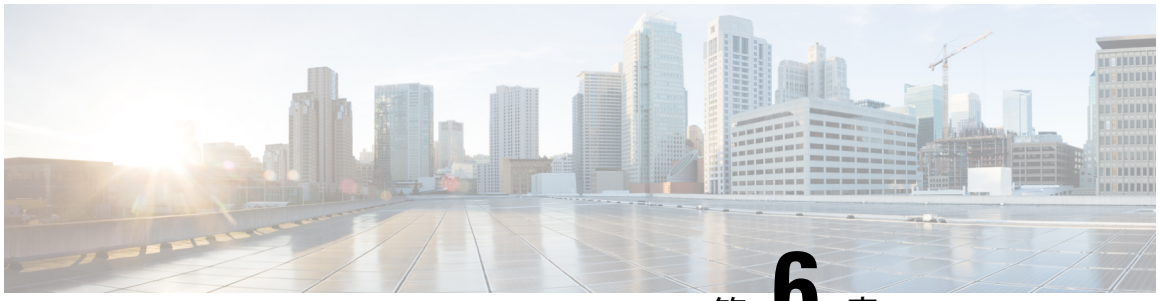
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

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

REP の機能情報

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



第 6 章

単方向リンク検出の設定

機能情報の確認

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

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

UDLD 設定の制約事項

次に、単方向リンク検出（UDLD）設定の制約事項を示します。

- UDLD 対応ポートが別のdeviceの UDLD 非対応ポートに接続されている場合、このポートは単一方向リンクを検出できません。
- モード（通常またはアグレッシブ）を設定する場合、リンクの両側に同じモードを設定します。

- インターフェイス モードで **udld enable** を設定しないでください。この設定は、デバイスでは実施可能ですが、インターフェイスの実行コンフィギュレーションでは表示されません。

⚠

注意 ループ ガードは、ポイントツーポイント リンクでのみサポートされます。リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

UDLD について

UniDirectional Link Detection（UDLD）は、光ファイバまたはツイストペア イーサネット ケーブルを通して接続されたデバイスからケーブルの物理設定をモニタリングしたり、単一方向リンクの存在を検出できるようにするためのレイヤ2プロトコルです。このプロトコルが単一方向リンクを正常に識別してディセーブルにするには、接続されたすべてのデバイスで UDLD プロトコルがサポートされている必要があります。UDLDは単一方向リンクを検出すると、影響を受けるポートをディセーブルにして警報を発信します。単一方向リンクは、スパニングツリー トポロジ ループをはじめ、さまざまな問題を引き起こす可能性があります。

動作モード

UDLD は、2 つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。通常モードの UDLD は、光ファイバ接続におけるポートの誤った接続による単一方向リンクを検出できます。アグレッシブ モードの UDLD は、光ファイバ リンクおよびツイストペア リンク上の片方向トラフィックと、光ファイバ リンク上のポートの誤った接続による単一方向リンクも検出できます。

通常およびアグレッシブの両モードの UDLD は、レイヤ 1 のメカニズムを使用して、リンクの物理ステータスを学習します。レイヤ1では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバー ID の検出、誤って接続されたポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 と 2 の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

ローカルデバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカルデバイスが受信しない場合に、単一方向リンクが発生します。

通常モード

通常モードの UDLD は、光ファイバ ポートの光ファイバが誤って接続されている場合に単一方向リンクを検出しますが、レイヤ1メカニズムは、この誤った接続を検出しません。ポートが正しく接続されていてもトラフィックが片方向である場合、単一方向リンクを検出するはずのレイヤ1メカニズムがこの状況を検出できないため、UDLDは単一方向リンクを検出できま

せん。この場合、論理リンクは不確定と見なされ、UDLD はポートをディセーブルにしません。

UDLD が通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションがアクティブであると、レイヤ1メカニズムがリンクの物理的な問題を検出するため、リンクは稼働状態でなくなります。この場合は、UDLD は何のアクションも行わず、論理リンクは不確定と見なされます。

関連トピック

UDLD のグローバルなイネーブル化 （167 ページ）
インターフェイスでの UDLD のイネーブル化 （169 ページ）

アグレッシブモード

アグレッシブ モードでは、UDLD はこれまでの検出方法で単一方向リンクを検出します。アグレッシブ モードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイントリンクの単一方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

- 光ファイバ リンクまたはツイストペア リンクで、ポートの 1 つがトラフィックを送受信できない。
- 光ファイバ リンクまたはツイストペア リンクで、ポートの 1 つがダウンし、残りのインターフェイスが稼働している。
- ケーブルのうち 1 本の光ファイバが切断されている。

これらの場合、UDLD は影響を受けたポートをディセーブルにします。

ポイントツーポイントリンクでは、UDLD hello パケットをハートビートと見なすことができ、ハートビートがあればリンクは正常です。逆に、ハートビートがないということは、双方向リンクを再確立できない限り、リンクをシャットダウンする必要があることを意味しています。

レイヤ1の観点からケーブルの両方の光ファイバが正常な状態であれば、アグレッシブ モードの UDLD はそれらの光ファイバが正しく接続されているかどうか、およびトラフィックが正しいネイバー間で双方向に流れているかどうかを検出します。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは自動ネゴシエーションでは実行できません。

関連トピック

UDLD のグローバルなイネーブル化 （167 ページ）
インターフェイスでの UDLD のイネーブル化 （169 ページ）

単一方向の検出方法

UDLD は、2 つの方法で動作します。

- ネイバー データベース メンテナンス
- イベントドリブン検出およびエコー

関連トピック

UDLD のグローバルなイネーブル化 （167 ページ）
インターフェイスでの UDLD のイネーブル化 （169 ページ）

ネイバー データベース メンテナンス

UDLD は、アクティブな各ポート上で hello パケット（別名アドバタイズまたはプローブ）を定期的に送信して、他の UDLD 対応ネイバーに関して学習し、各デバイスがネイバーに関する情報を常に維持できるようにします。

deviceが hello メッセージを受信すると、エージング タイム（ホールド タイムまたは存続可能時間）が経過するまで、情報をキャッシュします。古いキャッシュ エントリの期限が切れる前に、deviceが新しい hello メッセージを受信すると、deviceが古いエントリを新しいエントリで置き換えます。

UDLDの実行中にポートがディセーブルになったり、ポート上でUDLDがディセーブルになったり、またはdeviceをリセットした場合、UDLD は設定変更の影響を受けるポートの既存のキャッシュ エントリをすべてクリアします。UDLDは、ステータス変更の影響を受けるキャッシュの一部をフラッシュするよう、ネイバーに通知するメッセージを1つまたは複数送信します。このメッセージは、キャッシュを継続的に同期するためのものです。

イベントドリブン検出およびエコー

UDLD は検出動作としてエコーを利用します。UDLD デバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続の UDLD デバイス側の検出ウィンドウを再起動して、エコー メッセージを返送します。この動作はすべてのUDLDネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLDモードに応じてシャットダウンされることがあります。UDLDが通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。UDLDがアグレッシブ モードにある場合は、リンクは単一方向と見なされ、ポートはディセーブルになります。

関連トピック

UDLD のグローバルなイネーブル化 （167 ページ）
インターフェイスでの UDLD のイネーブル化 （169 ページ）

UDLD リセット オプション

インターフェイスが UDLD でディセーブル化された場合、次のオプションの 1 つを使用して UDLD をリセットできます。

- **udld reset** インターフェイス コンフィギュレーション コマンドです。
- **no shutdown** インターフェイス コンフィギュレーション コマンドに続いて **shutdown** インターフェイス コンフィギュレーション コマンドを入力すると、ディセーブル化されたポートを再起動できます。

- **no udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドの後に **udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドが続くと、無効なポートが再度イネーブルになります。
- **no udld port** インターフェイス コンフィギュレーション コマンドに続いて **udld port** [**aggressive**] 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、無効なファイバー オプティック ポートがイネーブルになります。
- **errdisable recovery cause udld** 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、UDLD の errdisable ステートから自動回復するタイマーをイネーブルにできます。さらに、**errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンドでは、udld errdisable ステートから回復する時間を指定します。

関連トピック

UDLD のグローバルなイネーブル化 （167 ページ）
インターフェイスでの UDLD のイネーブル化 （169 ページ）

UDLD のデフォルト設定

表 *16 : UDLD* のデフォルト設定

機能	デフォルト設定
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別の UDLD イネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバ ポート上でディセーブル
ポート別の UDLD イネーブル ステート（ツイストペア（銅製）メディア用）	すべてのイーサネット 10/100 および 1000BASE-TX ポート上でディセーブル
UDLD アグレッシブ モード	ディセーブル

関連トピック

UDLD のグローバルなイネーブル化 （167 ページ）
インターフェイスでの UDLD のイネーブル化 （169 ページ）

UDLD の設定方法

UDLD のグローバルなイネーブル化

アグレッシブ モードまたは通常モードでUDLDをイネーブルにし、device上のすべての光ファイバ ポートに設定可能なメッセージ タイマーを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**udld** {**aggressive** | **enable** | **message time** *message-timer-interval*} 例： `デバイス(config)# udld enable message time 10`	UDLD モードの動作を指定します。 • **aggressive**：すべての光ファイバ ポートにおいて、アグレッシブ モードでUDLDをイネーブルにします。 • **enable**：device上のすべての光ファイバポート上で、UDLDを通常モードでイネーブルにします。UDLDはデフォルトでディセーブルです。 個々のインターフェイスの設定は、**udld enable** グローバル コンフィギュレーション コマンドの設定を上書きします。 • **message time** *message-timer-interval*：アドバタイズメント フェーズにあり、双方向リンクが検出されたポートでの UDLD プローブ メッセージの時間間隔を設定します。有効な範囲は 1 ～ 90 秒です。デフォルト値は 15 です。 （注） このコマンドが作用するのは、光ファイバ ポートだけです。他のポートタイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーション コマンドを使用します。 UDLDをディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	デバイス(config)# **end**	

関連トピック

UDLD のモニタおよびメンテナンス
アグレッシブモード （165 ページ）
通常モード （164 ページ）
単一方向の検出方法 （165 ページ）
イベントドリブン検出およびエコー （166 ページ）
UDLD リセット オプション （166 ページ）
UDLD のデフォルト設定 （167 ページ）

インターフェイスでの UDLD のイネーブル化

アグレッシブ モードまたは通常モードをイネーブルにする、またはポート上で UDLD をディセーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： デバイス# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： デバイス(config)# **interface gigabitethernet 1/0/1**	UDLD用にイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**udld port** [**aggressive**] 例： デバイス(config-if)# **udld port aggressive**	UDLD はデフォルトでディセーブルです。 • **udld port**：指定されたポート上で、UDLDを通常モードでイネーブルにします。 • **udld port aggressive**：（任意）指定されたインターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。

	コマンドまたはアクション	目的
		（注） 特定の光ファイバポート上で UDLD をディセーブルにする場合は、 **no udld port** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

UDLD のモニタおよびメンテナンス
アグレッシブモード （165 ページ）
通常モード （164 ページ）
単一方向の検出方法 （165 ページ）
イベントドリブン検出およびエコー （166 ページ）
UDLD リセット オプション （166 ページ）
UDLD のデフォルト設定 （167 ページ）

UDLD のモニタおよびメンテナンス

コマンド	目的
show udld [*interface-id* | **neighbors**]	指定されたポートまたはすべてのポートの UDLD ステータスを表示します。

UDLD の追加リファレンス

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	『*Layer 2/3 Command Reference (Catalyst 3650 Switches)*』

標準および RFC

標準/RFC	タイトル
なし	—

MIB

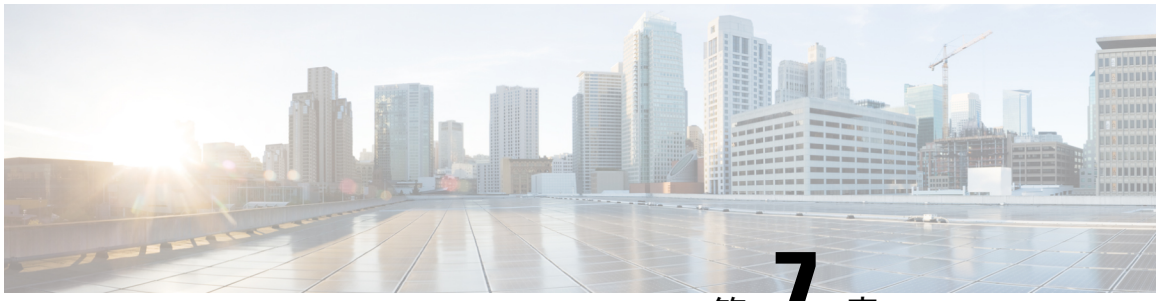
MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

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

UDLD の機能情報

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



第 7 章

IEEE 802.1Q トンネリングの設定

IEEE 802.1Q トンネリングについて

IEEE 802.1Q トンネリングは、サービスプロバイダーのネットワークを越えて複数のカスタマーのトラフィックを運び、その他のカスタマーのトラフィックに影響を与えずに、それぞれのカスタマーの VLAN およびレイヤ 2 プロトコルの設定を維持する必要があるサービスプロバイダー用に設計された機能です。

サービス プロバイダ ネットワークにおける IEEE 802.1Q トンネルポート

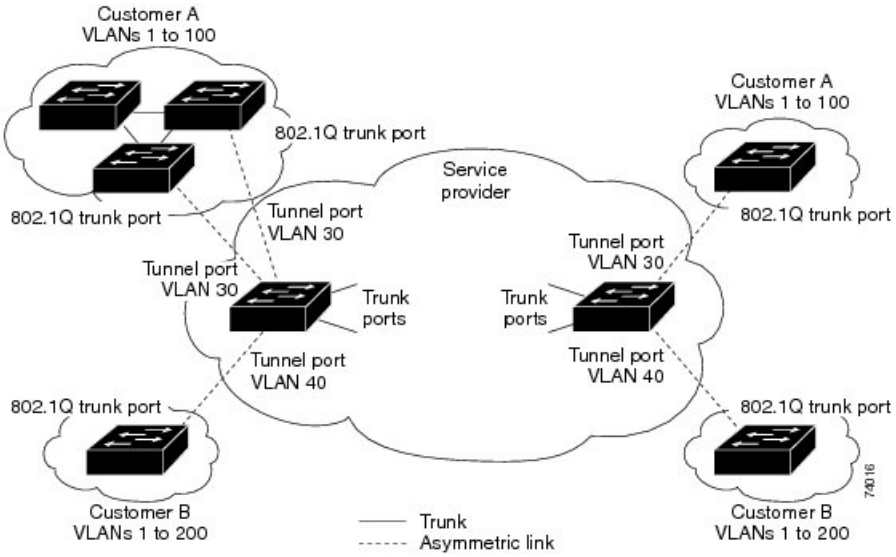
サービス プロバイダーのビジネス カスタマーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービスプロバイダー ネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混合してしまうことがあります。それぞれのカスタマーに VLAN ID の固有の範囲を割り当てると、カスタマーの設定が制限され、IEEE 802.1Q 仕様の VLAN 制限（4096）を簡単に超えてしまうことがあります。

サービス プロバイダーは、IEEE 802.1Q トンネリング機能を使用すると、単一の VLAN を使用して、複数の VLAN を含むカスタマーをサポートできます。カスタマーの VLAN ID は、同一 VLAN にあるように見えても保護され、さまざまなカスタマーのトラフィックは、サービスプロバイダー ネットワーク内で区別されます。IEEE 802.1Q トンネリングを使用する場合、VLAN-in-VLAN 階層構造およびタグ付きパケットへの再タグ付けによって、VLAN スペースを拡張できます。IEEE 802.1Q トンネリングをサポートするように設定したポートは、トンネル ポートと呼ばれます。トンネリングを設定する場合は、トンネリング専用の VLAN ID にト

ンネル ポートを割り当てます。それぞれのカスタマーには別個のサービスプロバイダーVLAN ID が必要ですが、その VLAN ID ではすべてのカスタマーの VLAN がサポートされます。

適切な VLAN ID で通常どおりにタグ付けされたカスタマーのトラフィックは、カスタマー デバイスの IEEE 802.1Q トランク ポートからサービスプロバイダーのエッジ deviceのトンネル ポートに発信されます。カスタマーデバイスとエッジdevice間のリンクは、片方がIEEE 802.1Q トランク ポートとして設定され、もう一方がトンネル ポートとして設定されるため、非対称です。それぞれのカスタマーに固有のアクセスVLAN IDには、トンネル ポート インターフェイスを割り当てます。

図 *26 :* サービス プロバイダー ネットワークにおける *IEEE 802.1Q* トンネル ポート

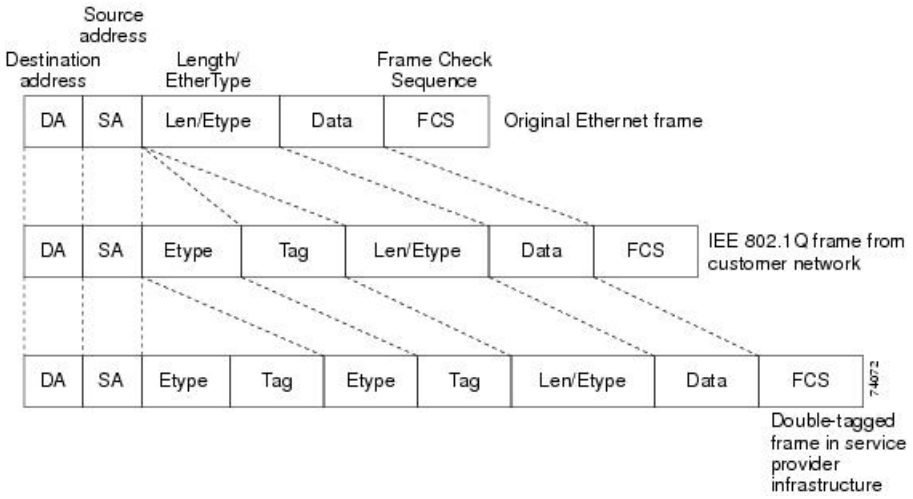


カスタマーのトランク ポートからサービス プロバイダーのエッジ deviceのトンネル ポートに発信されるパケットには、通常、適切なVLAN IDとともにIEEE 802.1Qタグが付いています。これらのタグ付きパケットは、device内部ではそのまま保持され、トランク ポートを出てサービスプロバイダー ネットワークに入る時点で、カスタマーに固有の VLAN ID を含む、IEEE 802.1Qタグのもう1つのレイヤ（メトロ タグと呼ばれる）でカプセル化されます。カスタマーの元の IEEE 802.1Q タグは、カプセル化されたパケット内で保護されます。このため、サービスプロバイダー ネットワークに入るパケットには、カスタマーのアクセス VLAN ID を含む外部（メトロ）タグ、および着信トラフィックのものである内部 VLAN ID という、二重のタグが付きます。

二重タグ パケットがサービスプロバイダー コア deviceの別のトランク ポートに入ると、device がパケットを処理するときに外部タグが外されます。パケットがその同じコア deviceの別のトランク ポートを出るとき、同じメトロ タグがパケットに再び追加されます。

図 *27*:元の（通常）イーサネット パケット、*IEEE 802.1Q* イーサネット パケット、二重タグ イーサネット パケットの形式

この図は、二重タグ付きパケットのタグ構造を示しています。



パケットがサービス プロバイダー出力deviceのトランク ポートに入ると、deviceがパケットを内部処理する間に外部タグが再び外されます。ただし、パケットがエッジ deviceのトンネル ポートからカスタマー ネットワークに送信されるとき、メトロ タグは追加されません。パケットは通常の IEEE 802.1Q タグ フレームとして送信され、カスタマー ネットワーク内で元の VLAN 番号は保護されます。

上記のネットワークの図では、カスタマー A に VLAN 30、カスタマー B に VLAN 40 が割り当てられています。エッジ deviceのトンネル ポートに入る、IEEE 802.1Q タグが付いたパケットは、サービスプロバイダー ネットワークに入るとき、VLAN ID 30 または 40 を適切に含む外部タグ、および VLAN 100 などの元の VLAN 番号を含む内部タグが付いて二重タグになります。カスタマー A とカスタマー B の両方が、それぞれのネットワーク内で VLAN 100 を含んでいても、外部タグが異なるので、サービスプロバイダー ネットワーク内で区別されます。それぞれのカスタマーは、その他のカスタマーが使用する VLAN 番号スペース、およびサービスプロバイダー ネットワークが使用する VLAN 番号スペースから独立した、独自の VLAN 番号スペースを制御します。

アウトバウンド トンネル ポートでは、カスタマーのネットワーク上の元の VLAN 番号が回復されます。トンネリングとタグ付けを複数レベルにすることもできますが、このリリースの deviceでは 1 レベルだけがサポートされます。

カスタマー ネットワークから発信されるトラフィックにタグ（ネイティブ VLAN フレーム）が付いていない場合、そのパケットのブリッジングまたはルーティングは通常パケットとして行われます。エッジ deviceのトンネル ポートを通ってサービスプロバイダー ネットワークに入るすべてのパケットは、タグが付いていないか、IEEE 802.1Q ヘッダーですでにタグが付いているかに関係なく、タグなしパケットとして扱われます。パケットは、IEEE 802.1Q トランク ポートでサービスプロバイダー ネットワークを通じて送信される場合、メトロ タグ VLAN ID（トンネル ポートのアクセス VLAN に設定）でカプセル化されます。メトロ タグの優先度フィールドは、トンネル ポートで設定されているインターフェイス サービス クラス（CoS）優先度に設定されます（設定されていない場合、デフォルトはゼロです）。

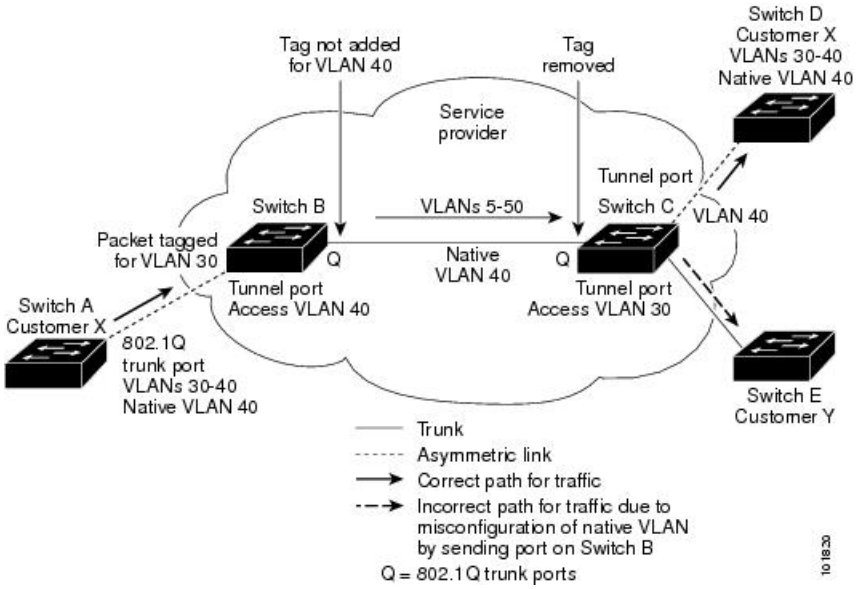
devicesでは、802.1Q トンネリングがポート単位で設定されるため、deviceはスタンドアロン deviceまたはスタック メンバのいずれでもかまいません。すべての設定は、スタック マスターで行われます。

ネイティブ VLAN

エッジ deviceで IEEE 802.1Q トンネリングを設定する場合、サービスプロバイダー ネットワークにパケットを送信するために、IEEE 802.1Q トランク ポートを使用する必要があります。ただし、サービスプロバイダー ネットワークのコアを通過するパケットは、IEEE 802.1Q トランク、ISL トランク、非トランキング リンクのいずれかで送信できます。コア devicesで IEEE 802.1Q トランクを使用する場合、IEEE 802.1Q トランクのネイティブ VLAN は、同一deviceの非トランキング（トンネリング）ポートのネイティブ VLAN と同じであってはなりません。これは、ネイティブ VLAN のトラフィックは、IEEE 802.1Q 送信トランク ポートではタグ付けされないためです。

次のネットワーク図で、VLAN 40 は、サービスプロバイダーネットワークの入力エッジdevice（デバイス B）にある、カスタマー X からの IEEE 802.1Q トランク ポートのネイティブ VLAN として設定されています。カスタマー X のデバイス A は、VLAN 30 のタグ付きパケットを、アクセス VLAN 40 に属する、サービスプロバイダー ネットワークのデバイス B の入力トンネル ポートに送信します。トンネル ポートのアクセス VLAN（VLAN 40）は、エッジ deviceのトランク ポートのネイティブ VLAN（VLAN 40）と同じであるため、トンネル ポートから受信したタグ付きパケットにメトロ タグが追加されません。パケットには VLAN 30 タグだけが付いて、サービスプロバイダー ネットワークで出力エッジ device（デバイス C）のトランク ポートに送信され、出力device トンネルによってカスタマー Y に間違って送信されます。

図 *28 : IEEE 802.1Q* トンネリングおよびネイティブ *VLAN* に潜在する問題



この問題の解決方法は次のとおりです。

- **vlan dot1q tag native** 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ことで、（ネイティブ VLAN を含む）IEEE 802.1Q トランクから発信されるすべてのパケットがタグ付けされるようにエッジdevicesを設定します。すべての IEEE 802.1Q トランクでネイティブ VLANパケットにタグを付けるようにdevicesを設定した場合、devicesはタグなしパケットを受け入れますが、タグ付きパケットだけを送信します。
- エッジ devicesのトランク ポートのネイティブ VLAN ID が、カスタマー VLAN 範囲に含まれないようにしてください。たとえばトランク ポートが VLAN100 ～ 200 のトラフィックを運ぶ場合は、この範囲以外の番号をネイティブ VLAN に割り当てます。

システム MTU

device上のトラフィックに関するデフォルトのシステム MTU は、1500 バイトです。

system mtu *bytes* 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、10 ギガビット イーサネット ポートおよびギガビット イーサネット ポートで 1500 バイトを超えるフレームをサポートするように設定できます。

システム MTU 値とシステム ジャンボ MTU 値には、IEEE 802.1Q ヘッダーは含まれていません。IEEE 802.1Q トンネリング機能では、メトロタグが追加されるとフレームサイズが 4 バイト増加するため、システム MTU サイズに最低 4 バイトを追加することによって、サービス プロバイダ ネットワークのすべてのdevicesが最大フレームを処理できるように設定する必要があります。

たとえば、deviceはこの構成で最大 1496 バイトのフレームサイズをサポートしています。device のシステム MTU 値が 1500 バイトで、 **switchport mode dot1q tunnel** インターフェイス コンフィギュレーションコマンドを使って 10 ギガビットイーサネットまたはギガビットイーサネット device ポートが設定されています。

IEEE 802.1Q トンネリングおよびその他の機能

IEEE 802.1Q トンネリングはレイヤ 2 パケット スイッチングで適切に動作しますが、一部のレイヤ 2 機能およびレイヤ 3 スイッチングの間には非互換性があります。

- トンネル ポートはルーテッド ポートにできません。
- IEEE 802.1Q トンネル ポートを含む VLAN では IP ルーティングがサポートされません。トンネル ポートから受信したパケットは、レイヤ 2 情報だけに基づいて転送されます。トンネル ポートを含むスイッチ仮想インターフェイス（SVI）でルーティングがイネーブルである場合、トンネル ポートから受信したタグなし IP パケットは、スイッチに認識されてルーティングされます。カスタマーは、ネイティブ VLAN を介してインターネットにアクセスできます。このアクセスが必要ない場合は、トンネル ポートを含む VLAN で SVI を設定しないでください。
- フォールバック ブリッジングは、トンネル ポートでサポートされません。トンネル ポートから受信したすべての IEEE 802.1Q タグ付きパケットは IP 以外のパケットとして扱われるので、トンネル ポートが設定されている VLAN でフォールバック ブリッジングが有効

である場合、IP パケットは VLAN を越えて不適切にブリッジングされます。このため、トンネル ポートを含む VLAN ではフォールバック ブリッジングを有効にしないでください。

- トンネル ポートでは IP アクセス コントロール リスト（ACL）がサポートされません。
- レイヤ 3 の Quality of Service（QoS）ACL およびレイヤ 3 情報に関連する他の QoS 機能は、トンネル ポートではサポートされていません。MAC ベース QoS はトンネル ポートでサポートされます。
- IEEE 802.1Q 設定が EtherChannel ポート グループ内で矛盾しない場合、EtherChannel ポート グループにはトンネル ポートとの互換性があります。
- ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、単一方向リンク検出（UDLD）は、IEEE 802.1Q トンネル ポートでサポートされます。
- トンネル ポートとトランク ポートで非対称リンクを手動で設定する必要があるので、ダイナミック トランキング プロトコル（DTP）には IEEE 802.1Q トンネリングとの互換性がありません。
- VLAN トランキング プロトコル（VTP）は、非対称リンクで接続されているデバイス間、またはトンネルを通して通信を行うデバイス間で動作しません。
- IEEE 802.1Q トンネル ポートでは、ループバック検出がサポートされます。
- IEEE 802.1Q トンネル ポートとしてポートを設定すると、スパニングツリー ブリッジ プロトコルデータ ユニット（BPDU）フィルタリングがインターフェイスで自動的に有効になります。Cisco Discovery Protocol（CDP）および Layer Link Discovery Protocol（LLDP）は、インターフェイスで自動的に無効になります。
- IGMP/MLD パケット転送は、IEEE 802.1Q トンネルで有効にできます。これは、サービス プロバイダ ネットワークで IGMP/MLD スヌーピングを無効にすることで実行できます。

IEEE 802.1Q トンネリングのデフォルト設定

デフォルトでは、デフォルト switchport モードが dynamic auto であるため、IEEE 802.1Q トンネルはディセーブルです。すべての IEEE 802.1Q トランク ポートにおける IEEE 802.1Q ネイティブ VLAN パケットのタグ付けもディセーブルです。

IEEE 802.1Q トンネリングの設定方法

ポートを IEEE 802.1Q トンネルポートとして設定するには、次の手順に従います。

始める前に

- カスタマーデバイスおよびエッジ deviceの間で非対称リンクを常に使用する必要があります。カスタマーデバイスのポートを IEEE 802.1Q トランクポートに、エッジ deviceのポートをトンネルポートとして設定してください。

- トンネリングに使用する VLAN だけにトンネル ポートを割り当ててください。
- ネイティブ VLAN と最大伝送単位（MTU）の設定要件に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `デバイス(config)# interface gigabitethernet2/0/1`	トンネル ポートとして設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。これは、カスタマー deviceに接続するサービスプロバイダー ネットワーク内のエッジポートである必要があります。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（ポート チャネル 1 ～ 48）が含まれます。
ステップ 4	**switchport access vlan** *vlan-id* 例： `デバイス(config-if)# switchport access vlan 2`	インターフェイスがトランキングを停止した場合に使用されるデフォルト VLAN を指定します。この VLAN ID は特定カスタマーに固有です。
ステップ 5	**switchport mode dot1q-tunnel** 例： `デバイス(config-if)# switchport mode dot1q-tunnel`	IEEE 802.1Q トンネル ポートとしてインターフェイスを設定します。 （注） ポートを dynamic desirable デフォルト状態に戻すには、**no switchport mode dot1q-tunnel** インターフェイス コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： デバイス(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**vlan dot1q tag native** 例： デバイス(config)# **vlan dot1q tag native**	（任意）すべての IEEE 802.1Q トランク ポートでネイティブ VLAN パケットのタギングがイネーブルになるように deviceを設定します。これを設定せず、カスタマー VLAN ID がネイティブ VLAN と同じである場合、トランク ポートはメトロ タグを適用せず、パケットは誤った宛先に送信される可能性があります。 （注） ネイティブ VLAN パケットのタグ付けをディセーブルにするには、**no vlan dot1q tag native** グローバル コンフィギュレーション コマンドを使用します。
ステップ 8	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 9	次のいずれかを使用します。 • **show dot1q-tunnel** • **show running-config interface** 例： デバイス# **show dot1q-tunnel** または デバイス# **show running-config interface**	IEEE 802.1Q トンネリング用に設定されたポートを表示します。 トンネリング モードになっているポートを表示します。
ステップ 10	**show vlan dot1q tag native** 例：	IEEE 802.1Q ネイティブ VLAN タギング ステータスを表示します。

	コマンドまたはアクション	目的
	デバイス# **show vlan dot1q native**	
ステップ 11	**copy running-config startup-config** 例： デバイス# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

トンネリング ステータスのモニタリング

次の表では、トンネリング ステータスをモニタするために使用するコマンドについて説明します。

表 *17:* トンネリングのモニタリング コマンド

コマンド	目的
show dot1q-tunnel	device の IEEE 802.1Q トンネルポートを表示します。
show dot1q-tunnel interface *interface-id*	特定のインターフェイスがトンネル ポートであるかどうかを確認します。
show vlan dot1q tag native	deviceのネイティブ VLAN タギングのステータスを表示します。

例：IEEE 802.1Q トンネリング ポートの設定

以下の例では、トンネル ポートとしてインターフェイスを設定してネイティブ VLAN パケットのタグ付けをイネーブルにし、設定を確認する方法を示します。 この設定では、スタックメンバー 1 のインターフェイス Gigabit Ethernet 7 に接続するカスタマーの VLAN ID は、VLAN 22 になります。

```
Switch(config)# interface gigabitethernet1/0/7
Switch(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# exit
Switch(config)# vlan dot1q tag native
Switch(config)# end
Switch# show dot1q-tunnel interface gigabitethernet1/0/7
Port
-----
```

```
Gi1/0/1Port
-----
Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

IEEE 802.1Q トンネリングの機能履歴と情報

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

リリース	変更内容
Cisco IOS XE 3.6E	この機能が導入されました。
Cisco IOS XE Denali 16.1.1	この機能がこのリリースに統合されました。