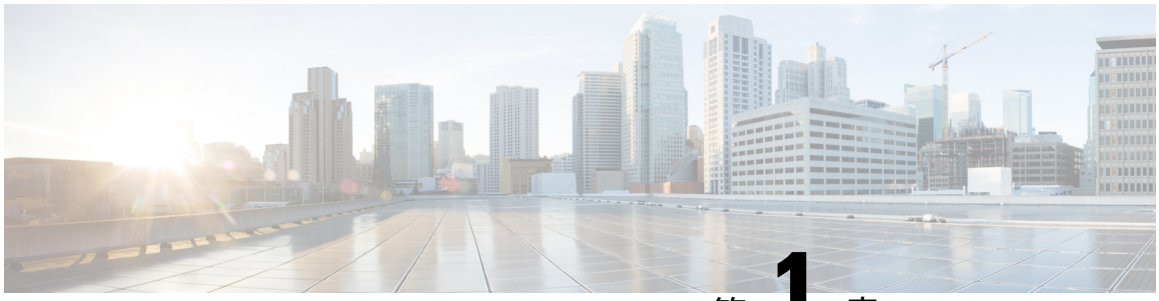
Cisco IOS リリース 15.2(8)E（Catalyst マイクロスイッチ シリーズ）レイヤ 2 コンフィギュレーション ガイド

初版：2021 年 4 月 26 日

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

目 次



第 1 章

スパニングツリー プロトコルの設定

STP の制約事項

- ルートデバイスとしてデバイスを設定しようとする場合、ルートデバイス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 をサポートするデバイス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 をサポートするデバイスがルートデバイス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デバイス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 によってデバイス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デバイスは、バックボーンまたはディストリビューション デバイスでなければなりません。アクセスデバイス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。

STP について

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。このループがネットワークに発生すると、エンドステーションにメッセージが重複して到着す

る可能性があります。デバイスは、複数のレイヤ 2 インターフェイス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デバイスを 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デバイス、またはバックアップの役割が指定されているデバイスはルートデバイスです。 少なくとも *1* つのポートに役割が指定されているデバイスは、指定デバイスを意味します。

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。デバイスは、スパニングツリーフレーム（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。デバイスはこれらのフレームを転送せずに、ループのないパスを構成するために使用します。 BPDU には、送信側デバイスおよびそのポートについて、デバイスおよび MAC アドレス、デバイスプライオリティ、ポートプライオリティ、パスコストなどの情報が含まれます。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デバイス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。

デバイスの 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） デフォルトでは、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。

- デバイス上の各 VLAN に関連付けられた一意のブリッジ ID（デバイスプライオリティおよび MAC アドレス）。
- ルートデバイス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）。

ネットワーク内のデバイスに電源が入ると、各機能はルートデバイスとして機能します。各デバイスは、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。

- 送信デバイスがルートデバイスとして識別するデバイスの一意のブリッジ ID。
- ルートまでのスパニングツリー パス コスト
- 送信デバイスのブリッジ 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

デバイスは、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 をデバイスのルートポート上で受信した場合、そのデバイスが指定デバイス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。

デバイスは、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。デバイスが下位 BPDU を受信した LAN の指定デバイスである場合、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。

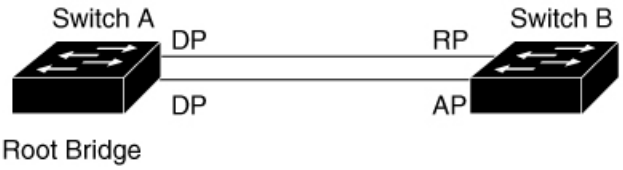
BPDU の交換によって、次の処理が行われます。

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

  VLAN ごとに、デバイスプライオリティが最も高い（最も小さい数字の優先順位の値）デバイスがルートデバイスとして選択されます。すべてのデバイスがデフォルトのプライオリティ（32768）で設定されている場合、VLAN 内で MAC アドレスの最も小さいデバイスがルートデバイスになります。デバイスのプライオリティ値は、次の図のようにブリッジ ID の最上位ビットを占めます。

- デバイスごとに（ルートデバイスを除く）、ルートポートが 1 つ選択されます。このポートは、デバイスがルートデバイスにパケットを転送するとき、最適な（コストが最小の）パスを提供します。
- ルートデバイスへの最短距離は、パスコストに基づいてデバイスごとに計算されます。
- LAN セグメントごとに指定デバイスが選択されます。指定デバイスは、その LAN からルートデバイス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。指定デバイスが LAN への接続に使用したポートは、指定ポートと呼ばれます。

図 *1:* スパニングツリー ポート ステート



DP = 指定ポート

RP = ルート ポート

AP = 割り当てポート

（注） **logging event spanning tree** コマンドが複数のインターフェイスに設定され、トポロジが変更されると、複数のロギングメッセージが発生し、CPU 使用率が高くなることがあります。これにより、スイッチが STP Bpdu の処理をドロップまたは遅延させる可能性があります。

この動作を防ぐには、**logging event spanning tree** および **logging event status** コマンドを削除するか、コンソールへのロギングを無効にします。

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デバイス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。

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、それぞれのデバイスに固有の ルート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、同一のデバイスは設定された各 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。デバイス上の各 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 バイトはデバイスプライオリティに使用され、残りの 6 バイトがデバイスの MAC アドレスから取得されます。

デバイスでは IEEE 802.1t スパニングツリー拡張機能がサポートされ、従来はデバイスプライオリティに使用されていたビットの一部が VLAN ID として使用されるようになりました。その結果、デバイスに割り当てられる MAC アドレスが少なくなり、より広い範囲の VLAN ID をサポートできるようになり、しかもブリッジ ID の一意性を損なうこともありません。

従来はデバイス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、デバイスプライオリティ、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。

拡張システム ID のサポートにより、ルートデバイス、セカンダリルートデバイス、および VLAN のデバイス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、デバイスのプライオリティ値を変更すると、デバイスがルートデバイス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 のルートデバイスに 24576 に満たないデバイスプライオリティが設定されている場合は、デバイスはその VLAN について、自身のプライオリティを最小のデバイス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 デバイス 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。

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。

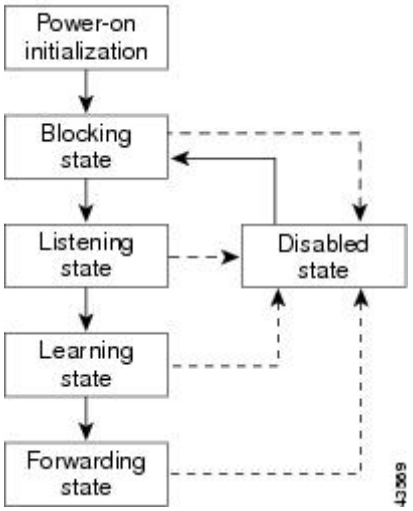
スパニングツリーを使用しているデバイスの各レイヤ2インターフェイスは、次のいずれかのステートになります。

- 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、デバイス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、デバイス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、デバイス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、デバイスの各インターフェイスにBPDUが送信されます。デバイスは最初、他のデバイスと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デバイスがルートまたはルートデバイスになるかが確立されます。ネットワーク内にデバイスが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デバイスの初期化後、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。

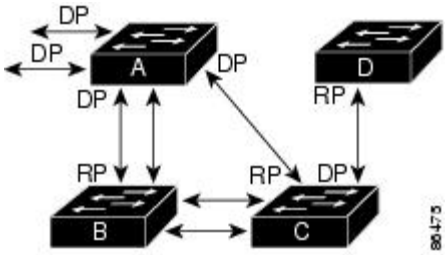
- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信しません。

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デバイス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 アドレスを持つデバイスがルートデバイスになります。

図 *3:* スパニングツリー トポロジ

デバイス A はルートデバイスとして選択されます。すべてのデバイスのデバイスプライオリティがデフォルト（32768）に設定されていて、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 が最適なルートデバイスとは限りません。ルートデバイスになるように、最適なデバイス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、最適なデバイスをルートとした新しいトポロジが形成されま



RP = Root Port
す。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。

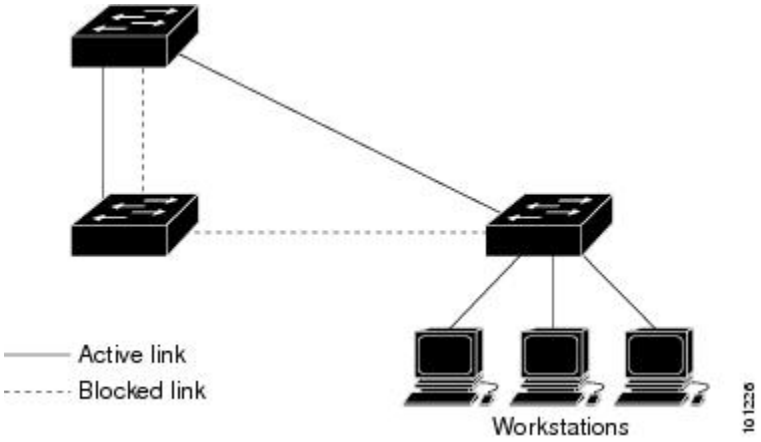
たとえば、デバイス B のあるポートがギガビット イーサネット リンクで、デバイス B 上の別のポート（10/100 リンク）がルートポートであると仮定します。ネットワーク トラフィックはギガビット イーサネット リンクに流す方が効率的です。ギガビット イーサネット ポートのスパニングツリー ポート プライオリティをルート ポートより高くする（数値を小さくする）と、ギガビット イーサネット ポートが新しいルート ポートになります。

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 つのデバイス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、デバイス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。

スパニングツリーがイネーブルな場合、デバイスの CPU は 0x0180C2000000 および 0x0180C2000010 宛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な場合は、デバイスは、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、デバイスは 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、デバイスで設定されたエージング間隔がそのまま保持されます。

スパニングツリー モードおよびプロトコル

このデバイス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+ はデバイス上の各 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 つのルートデバイスがあります。このルートデバイスは、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デバイスに伝送します。このプロセスにより、各デバイス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+：Rapid PVST+ はデバイス上のデフォルトの STP モードです。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）、デバイス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。

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、デバイスは最大 64 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、デバイスは最大 64 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。

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+ デバイスを複数の 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+ を実行しているデバイスと PVST+ を実行しているデバイスが存在する場合、Rapid PVST+ デバイスと PVST+ デバイス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、ルートデバイスは Rapid PVST+ でなければなりません。PVST+ インスタンスでは、ルートデバイスは PVST+ デバイスでなければなりません。PVST+ デバイスはネットワークのエッジに配置する必要があります。

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

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

IEEE 802.1Q トランクを介して Cisco デバイスを他社製のデバイスに接続する場合、Cisco デバイスは 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、デバイスは PVST+ ではなく Rapid PVST+ を使用します。デバイスは、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 デバイス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 デバイスからなるクラウドにより分離された Cisco デバイスによって維持されます。Cisco デバイスを分離する他社製の IEEE 802.1Q クラウドは、デバイス間の単一トランクリンクとして扱われます。

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。

VLAN ブリッジ スパニングツリー

シスコ VLAN ブリッジ スパニングツリーは、フォールバック ブリッジング機能（ブリッジ グループ）で使用し、DECnet などの IP 以外のプロトコルを 2 つ以上の VLAN ブリッジ ドメインまたはルーテッドポート間で伝送します。VLAN ブリッジ スパニングツリーにより、ブリッジ グループは個々の VLAN スパニングツリーの上部にスパニングツリーを形成できるので、VLAN 間で複数の接続がある場合に、ループが形成されないようにします。また、ブリッジングされている VLAN からの個々のスパニングツリーが単一のスパニングツリーに縮小しないようにする働きもします。

VLAN ブリッジ スパニングツリーをサポートするには、一部のスパニングツリー タイマーを増やします。フォールバックブリッジング機能を使用するには、デバイスで IP サービスフィーチャセットをイネーブルにする必要があります。

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）
デバイスプライオリティ	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

STP の設定方法

スパニングツリー モードの変更

デバイスは次の 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、デバイスは 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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**} 例： `Device(config)# spanning-tree mode pvst`	スパニングツリーモードを設定します。 • 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。 （注） デフォルトでは、デバイスは Rapid PVST+ を実行します。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	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。ポート チャネルの範囲は 1 ～ 6 です。
ステップ 5	**spanning-tree link-type point-to-point** 例： `Device(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、デバイス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。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**clear spanning-tree detected-protocols** 例： `Device# clear spanning-tree detected-protocols`	デバイス上のいずれかのポートがレガシー IEEE 802.1D デバイス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デバイス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、このデバイスで Rapid PVST+ が稼働していることを指定デバイスが検出する場合のオプションです。

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no spanning-tree vlan** *vlan-id* 例：	*vlan-id* に指定できる範囲は 1 ～ 4094 です。

	コマンドまたはアクション	目的
	`Device(config)# no spanning-tree vlan 300`	
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ルート デバイスの設定

デバイスは、設定されているアクティブな VLAN ごとに個別のスパニングツリー インスタンスを保持します。ブリッジ ID は、デバイスのプライオリティおよびデバイスの MAC アドレスで構成されていて、各インスタンスに関連付けられます。それぞれの VLAN では、最小のブリッジ ID を持つデバイスが VLAN のルートスイッチになります。

特定の VLAN でデバイス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、デバイス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、ルートデバイスのデバイス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、デバイスは指定された 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、このデバイスを指定された VLAN のルートに設定できます。

（注） ネットワークが、拡張システム ID をサポートするデバイス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 をサポートするデバイスがルートデバイス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デバイス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 によってデバイス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デバイスは、バックボーンまたはディストリビューションデバイスでなければなりません。アクセスデバイス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デバイス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、デバイスは、その直径のネットワークで最適な hello タイム、転送遅延時間、最大エージング タイムを自動的に設定し、これによって収束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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]] 例： `Device(config)# spanning-tree vlan 20-24 root primary diameter 4 hello-time 5`	指定された VLAN のルートになるように、デバイスを設定します。 • *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デバイスの最大数を指定します。範囲は 2 ～ 7 です。 •（任意）**hello-time***seconds* seconds には、ルートスイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。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 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

次のタスク

ルートデバイスとしてデバイスを設定した後で、**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。

セカンダリ ルート デバイスの設定

デバイスをセカンダリルートとして設定すると、デバイス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、プライマリルートデバイスに障害が発生した場合に、このデバイスが指定された VLAN のルートデバイス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デバイスが、デフォルトのデバイスプライオリティの 32768 を使用しているためにルートデバイス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デバイスに対して実行すると、複数のバックアップルートデバイスを設定できます。**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デバイス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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]] 例： `Device(config)# spanning-tree vlan 20-24 root secondary diameter 4 hello-time 5`	指定された VLAN のセカンダリルートになるように、デバイスを設定します。 • *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デバイスの最大数を指定します。指定できる範囲は 2 ～ 7 です。 •（任意）**hello-time***seconds* seconds には、ルートスイッチによってコンフィギュレーション メッセージが

	コマンドまたはアクション	目的
		生成される間隔を秒数で指定します。指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。 プライマリルートデバイス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： `Device(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

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	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： `Device(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

	コマンドまたはアクション	目的
		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： `Device(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： `Device(config-if)# end`	特権 EXEC モードに戻ります。

パス コストの設定

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。

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定する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： `Device(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： `Device(config-if)# spanning-tree vlan 10,12-15,20 cost 300`	VLAN 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。 • *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。

	コマンドまたはアクション	目的
		• *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： `Device(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。

VLAN のデバイス プライオリティの設定

デバイスプライオリティを設定して、スタンドアロンデバイスがルートデバイス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。多くの場合、**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 コマンドを使用して、デバイスのプライオリティを変更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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **priority** *priority* 例：	VLAN のデバイス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

	コマンドまたはアクション	目的
	`Device(config)# spanning-tree vlan 20 priority 8192`	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、デバイスがルートデバイス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： `Device(config-if)# end`	特権 EXEC モードに戻ります。

hello タイムの設定

hello タイムはルートデバイス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。

（注） このコマンドの使用には注意してください。hello タイムの変更には、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 コマンドの使用を推奨します。

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **hello-time** *seconds* 例： `Device(config)# spanning-tree vlan 20-24 hello-time 3`	VLAN の hello タイムを設定します。hello タイムはルートデバイス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。これらのメッセージは、デバイスが動作していることを示します。 • *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 4	**end** 例： `Device(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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**spanning-tree vlan** *vlan-id* **forward-time** *seconds* 例： `Device(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： `Device(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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **max-age** *seconds* 例：	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、デバイスが再設定を試す前にスパニングツ

	コマンドまたはアクション	目的
	`Device(config)# spanning-tree vlan 20 max-age 30`	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： `Device(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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**spanning-tree transmit hold-count** *value* 例： `Device(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： `Device(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。

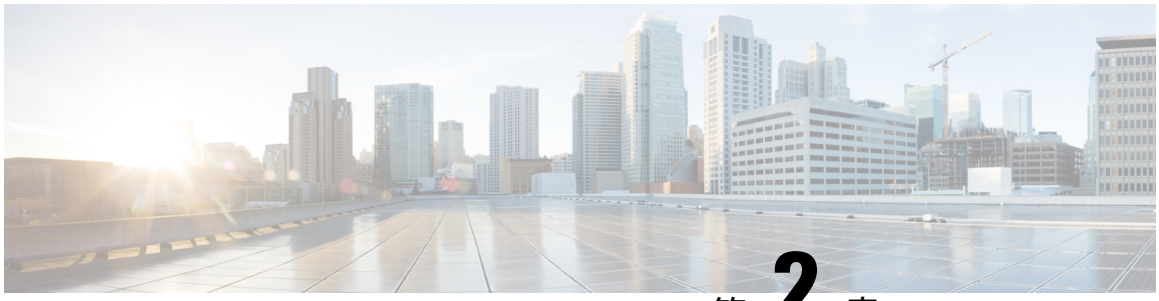
オプションのスパニングツリー機能の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

機能名	リリース	機能情報
オプションのスパニングツリー機能	Cisco IOS Release 15.2(7)E3k	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

MSTP の前提条件

- 2 つ以上のデバイス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。
- 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。
- 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）のルート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。クラウド内のデバイスを手動で設定しなければならない場合もあります。

MSTP の制約事項

- 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 リージョン内の各デバイスで 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。
- ルートデバイスとしてデバイスを設定した後で、**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

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。

デバイスが 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。

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 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。
- デバイスが 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

ルート スイッチ

デバイスは、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。デバイス ID は、デバイスのプライオリティおよびデバイスの MAC アドレスで構成されていて、各インスタンスに関連付けられます。VLANのグループでは、最小のデバイス ID を持つデバイスがルートデバイスになります。

デバイスをルートとして設定する場合は、デバイス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、デバイスが、指定したスパニング ツリー インスタンスのルートデバイスになるようにします。このコマンドを入力すると、デバイスはルートデバイスのデバイス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 という値でデバイス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、そのデバイス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デバイスに 24576 に満たないデバイスプライオリティが設定されている場合は、デバイスは自身のプライオリティを最小のデバイス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 デバイス 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、デバイスプライオリティ、および拡張システム ID」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 をサポートするデバイス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 をサポートするデバイスがルートデバイス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スイッチ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 によってデバイス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デバイスは、バックボーンまたはディストリビューションデバイスでなければなりません。アクセスデバイス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デバイスホップカウント）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、デバイスは、その直径のネットワークで最適な hello タイム、転送遅延時間、最大エージング タイムを自動的に設定し、これによって収束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。

（注） スイッチをルート スイッチとして設定した後に、**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、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。

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 設定により、各デバイスが属する 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、リージョンのデバイスを設定します。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。

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（ルートデバイス 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 ルートになります。これは、リージョン内で最も小さいデバイス ID、および CIST ルートに対するパスコストを持つデバイスです。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 デバイスは初期化時に、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。デバイスはすべての MST インスタンスを初期化し、そのすべてのルートであることを主張します。デバイスは、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（低いデバイス 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。

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 デバイス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 デバイスから構成される 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 は領域内のすべての MSTP デバイスを接続し、スイッチドドメイン全体を網羅する CIST でサブツリーのように見えます。サブツリーのルートは CIST リージョナル ルートです。隣接する STP デバイスおよび MST 領域には、MST 領域が仮想デバイスのように見えます。

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デバイスと相互作用し、最終的なスパニングツリートポロジを算出します。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（デバイスプライオリティ、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 デバイスは、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 デバイスと通信します。MSTP デバイスは、MSTP BPDU を使用して MSTP デバイスと通信します。

IEEE 802.1s の用語

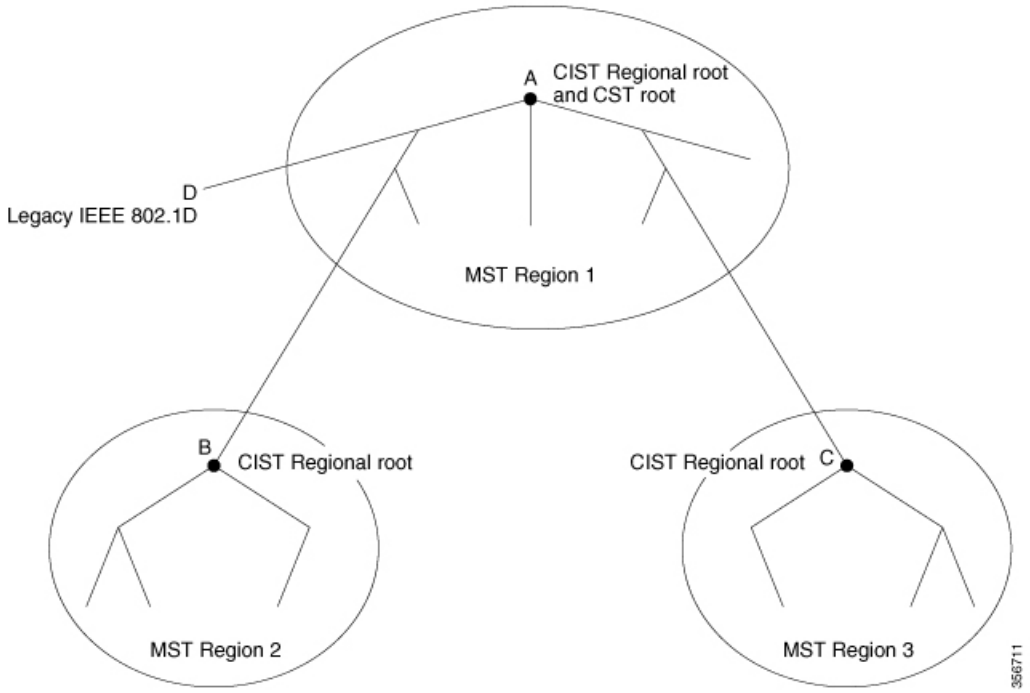
シスコの先行標準実装で使用される一部の MST 命名規則は、一部の内部パラメータまたはリージョン パラメータを識別するように変更されました。これらのパラメータは、ネットワーク全体に関連している外部パラメータと違い、MST リージョン内でのみ影響があります。CIST はネットワーク全体を網羅するスパニングツリー インスタンスのため、CIST パラメータのみ、内部修飾子やリージョナル修飾子ではなく外部修飾子が必要です。

- 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デバイスです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。このコストは MST 領域内で変化しません。MST リージョンは、CIST への単一デバイス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、この仮想デバイス、およびどの領域にも属さないデバイスの間で計算されるルート パス コストです。
- CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。CIST ルートが領域内にない場合、CIST リージョナル ルートは領域内の CIST ルートに最も近いデバイスです。CIST リージョナルルートは、IST のルートデバイスとして動作します。
- 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。

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 デバイス（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* リージョナルルート、*CST* ルート



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デバイスは、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。デバイスは、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、デバイスは BPDU を廃棄し、ポート用に維持されている情報をエージングします。

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 にも接続します。つまり、単一スパニングツリーデバイスまたは MST 設定が異なるデバイスのいずれかである指定デバイスに接続します。

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、デバイスおよび 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 デバイス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、送信デバイス ID を持つ RSTP またはレガシー IEEE 802.1Q デバイスの部分に、CIST リージョナルルートデバイス ID フィールドが加えられたことです。リージョン全体は、一貫した送信者デバイス ID をネイバーデバイスに送信し、単一仮想デバイス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デバイス ID が同じである BPDU をデバイス 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。
- 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。

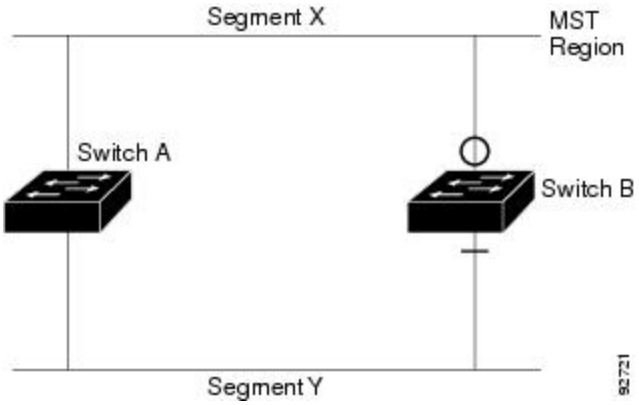
レガシーデバイスと標準デバイスの相互運用

先行標準デバイス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先行標準ポートを識別できます。標準デバイスと先行標準デバイスの間にあるリージョンは形成できませんが、CIST を使用することで相互運用できます。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。デバイスが先行標準BPDU送信用に設定されていないポートで先行標準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:* 標準デバイスと先行標準デバイスの相互運用

A が標準のデバイスで、B が先行標準のデバイスとして、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 のルートデバイスです。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先行標準 BPDU を 1 つ送信すると、AY は先行標準デバイスが Y に接続されていることを検出できず、標準 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。

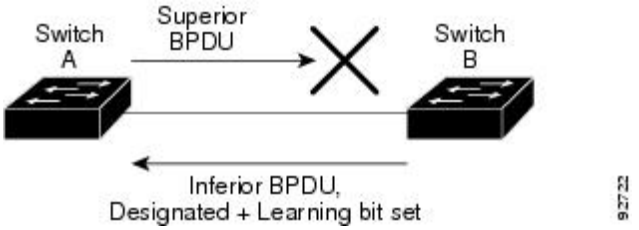
単一方向リンク障害の検出

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 はルートデバイスであり、デバイス 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。デバイス A はこの情報を使用し、ルータ A が送信する上位 BPDU にデバイス B が反応しないこと、およびデバイス B がルートデバイス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、デバイス 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。



IEEE 802.1D STP との相互運用性

MSTP が稼働しているデバイスは、IEEE 802.1D 準拠のレガシーデバイス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。このデバイスは、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デバイスは、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、デバイスが 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。これはレガシーデバイスが指定デバイスでない限り、レガシーデバイス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。このデバイスの接続先デバイスが領域に加わったとき、デバイスは境界ロールをポートに割り当て続けることもあります。プロトコル移行プロセスを再開するには（強制的にネイバーデバイス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デバイスがRSTPデバイスであれば、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 デバイスは、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 に接続します。つまり、単一スパニングツリーデバイスまたは MST 設定が異なるデバイスのいずれかである指定デバイスに接続します。

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 はデバイスをルートデバイスとして最も高いデバイスプライオリティ（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：デバイスがルートデバイスにパケットを転送するとき、最適な（コストが最小の）パスを提供します。
- 指定ポート：指定デバイスに接続し、その LAN からルートデバイスにパケットを転送するとき、パスコストを最低にします。指定デバイスがLANへの接続に使用したポートは、指定ポートと呼ばれます。
- 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デバイス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。2 つのポートがポイントツーポイント リンクによってループバックで接続した場合、または共有 LAN セグメントへの複数の接続がデバイスにある場合に限り、バックアップ ポートは存在できます。
- 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 *6 :* 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	×
イネーブル	リスニング	廃棄	×
イネーブル	ラーニング	ラーニング	○
イネーブル	転送	転送	○
ディセーブル	ディセーブル	廃棄	×

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、デバイス、デバイスポート、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 デバイス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

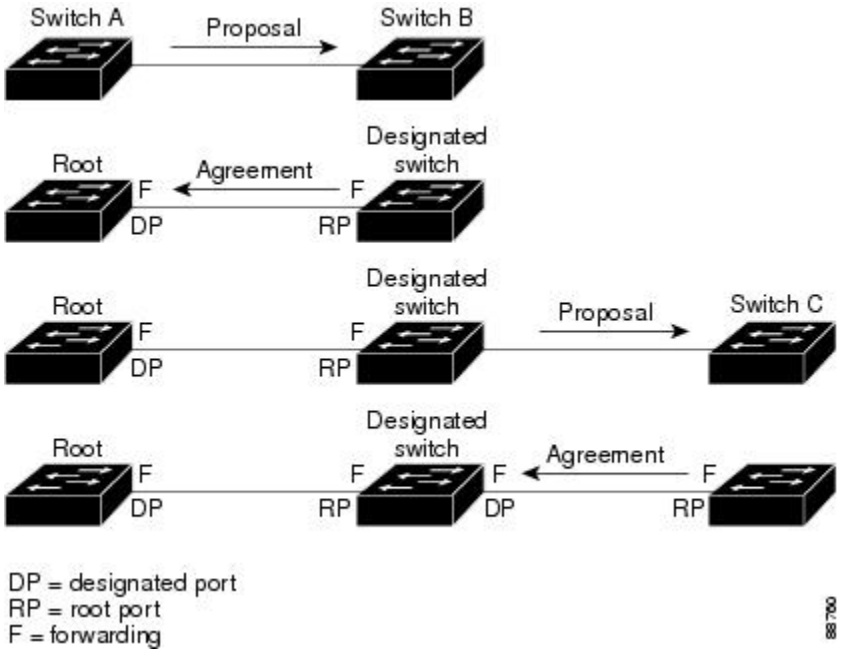
デバイス A がデバイス B にポイントツーポイントリンクで接続され、すべてのポートはブロッキングステートになっています。デバイス A のプライオリティがデバイス B のプライオリティよりも数値的に小さいとします。デバイス A は提案メッセージ（提案フラグを設定した設定 BPDU）をデバイス B に送信し、指定デバイスとしてそれ自体を提案します。

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、デバイス 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イ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。このハンドシェイク処理を繰り返して、もう 1 つのデバイスがアクティブトポロジに加わります。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。

デバイス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

デバイス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。

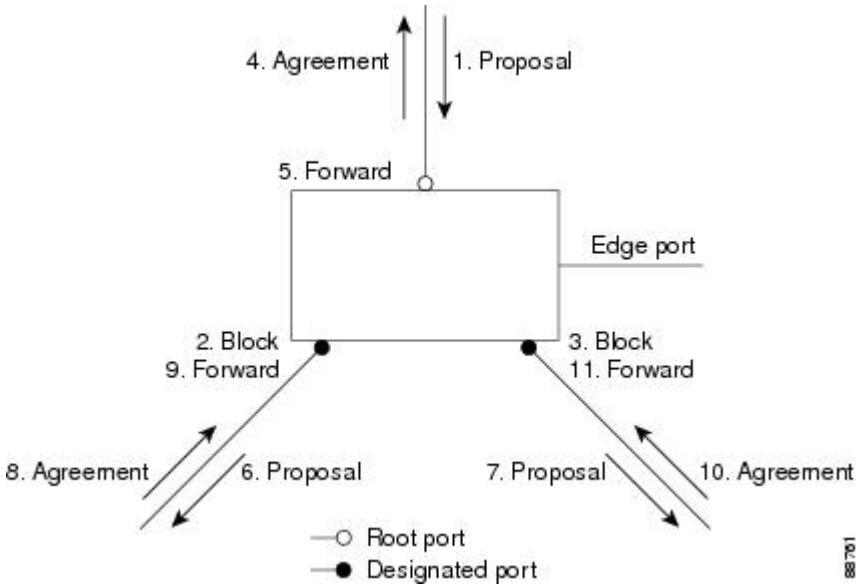
その他すべてのポートを同期化する場合、ルートポートで受信した優位ルート情報でデバイスは同期化されます。デバイスのそれぞれのポートは、次のような場合に同期化します。

- 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

すべてのポートが同期化されてから、デバイスは、ルートポートに対応する指定デバイス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デバイス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 *7: RSTP BPDU* フラグ

ビット	機能
0	トポロジーの変化（TC）
1	提案
2 ～ 3: 00 01 10 11	ポートの役割： 不明 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）

送信側デバイスは RSTP BPDU の提案フラグを設定し、その LAN の指定デバイス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。

送信側デバイスは、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 デバイスとの相互運用性を保つために、RSTP デバイスは 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（小さいデバイス 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、デバイス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、デバイス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デバイス 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 デバイスは、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 デバイスは TCN BPDU の処理と生成を行います。
- 確認：RSTP デバイスは、指定ポートで IEEE 802.1D デバイスから 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 デバイス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デバイス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 デバイスは、DP またはルートポートを介して別のデバイスから 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。デバイス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 デバイス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、デバイス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。

デバイス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 デバイス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 デバイスが 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 が稼働しているデバイスは、IEEE 802.1D 準拠のレガシーデバイス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。このデバイスは、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 デバイスは、レガシー BPDU、別のリージョンに関連付けられている MST 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、デバイスが 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。これはレガシーデバイスが指定デバイスでない限り、レガシーデバイス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、接続するデバイスがリージョンに加入していると、デバイス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。

MSTP のデフォルト設定

表 *8 : 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
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

MST と PVST+ の相互運用性について（PVST+ シミュレーション）

PVST+ シミュレーション機能は、MST と Rapid PVST+ との間にシームレスな相互運用性を実現します。ポート単位またはグローバルに有効化または無効化できます。PVST+ シミュレーションは、デフォルトでイネーブルになっています。

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

この機能を無効にすると、スイッチは MST 領域と PVST+ 領域との対話を停止します。MST 対応ポートは、Rapid PVST+ 対応ポートに接続されたことを検出すると、PVST ピア不整合（ブロッキング）状態に移行します。このポートは、Shared Spanning Tree Protocol（SSTP）BPDU の受信を停止するまでは不整合状態を維持し、受信停止後は通常の STP 送信プロセスを再開します。

たとえば、PVST+ シミュレーションを無効にすることにより、正しく設定されていないスイッチと、STP モードが MSTP 以外であるネットワーク（デフォルトモードは Rapid-PVST+）との接続を、防止することができます。

（同一リージョン内の）MST スイッチを PVST+ スイッチと対話させるよう設定する場合は、次の注意事項に従ってください。

- MST リージョン内のすべての VLAN に対するルートを設定します。次の例を参照してください。

```
Device# show spanning-tree mst interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 of MST00 is root forwarding
Edge port: no             (trunk) port guard : none    (default)
Link type: point-to-point (auto)  bpdu filter: disable (default)
Boundary : boundary       (PVST)  bpdu guard : disable (default)
Bpdus sent 10, received 310

Instance Role Sts Cost  Prio.Nbr    Vlans mapped
-------- ---- --- ---------- -------- -------------------------------
0        Root FWD 20000 128.1       1-2,4-2999,4000-4094
3        Boun FWD 20000 128.1       3,3000-3999
```

  MST スイッチに属する境界ポートは、PVST+ をシミュレートし、すべての VLAN に PVST+ BPDU を送信します。

  PVST+ スイッチ上でループ ガードをイネーブルにすると、MST スイッチの設定が変更されたときに、ポートが loop-inconsistent ステートに変化する可能性があります。loop-inconsistent 状態を解消するには、PVST+ スイッチ上でループ ガードをいったん無効にしてから再有効化する必要があります。

- MST スイッチの PVST+ サイド内にある VLAN の一部またはすべてに対して、ルートを配置しないでください。境界の MST スイッチが指定ポート上の VLAN のすべてまたは一部に対する PVST+ BPDU を受信すると、ルート ガードによってそのポートがブロッキング ステートになります。

- PVST+ スイッチを 2 つの異なる MST リージョンに接続すると、PVST+ スイッチからのトポロジ変更が最初の MST リージョンから先へ伝達されません。この場合、トポロジ変更は VLAN がマッピングされているインスタンスで伝播されるだけです。トポロジ変更は

最初の MST リージョンに対してローカルのままで、その他のリージョンの Cisco Access Manager（CAM）エントリはフラッシュされません。他の MST リージョンにもトポロジ変更が認識されるようにするには、IST に VLAN をマッピングするか、またはアクセス リンクを介して 2 つのリージョンに PVST+ スイッチを接続します。

- PVST+シミュレーションを無効にすると、ポートがすでに他の不整合状態にある間、PVST+ ピア不整合も起こる可能性があるので、注意してください。たとえば、すべての STP インスタンスのルート ブリッジは、MST または Rapid PVST+ のどちらかの側に属している必要があります。すべての STP インスタンスのルート ブリッジがどちらか一方の側に属していないと、ポートは PVST+ シミュレーション不整合状態になります。

注 すべての STP インスタンスのルート ブリッジを、MST 側に配置することを推奨します。

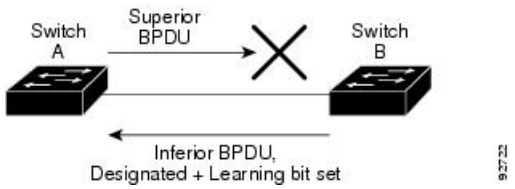
単方向リンク障害の検出について

IEEE 802.1D-2004 RSTP および IEEE 802.1Q-2005 MSTP 標準には単方向リンク障害を検出する解決メカニズムが含まれており、ユーザによる設定は必要ありません。

スイッチにより、受信する BPDU のポートのロールおよびステートの一貫性がチェックされ、ブリッジング ループを発生させる可能性のある単方向リンク障害が検出されます。指定ポートが矛盾を検出するとロールは維持されますが、状態は廃棄（ブロッキング）ステートに戻ります。これは、接続に矛盾が生じた場合、ブリッジング ループを開始するよりも接続を中断する方が好ましいためです。

たとえば、次の図では、スイッチ A がルート ブリッジ スイッチで、スイッチ B が指定ポートです。スイッチ A からの BPDU は、スイッチ B に向かうリンク上で失われます。

図 *10*：単一方向リンク障害の検出

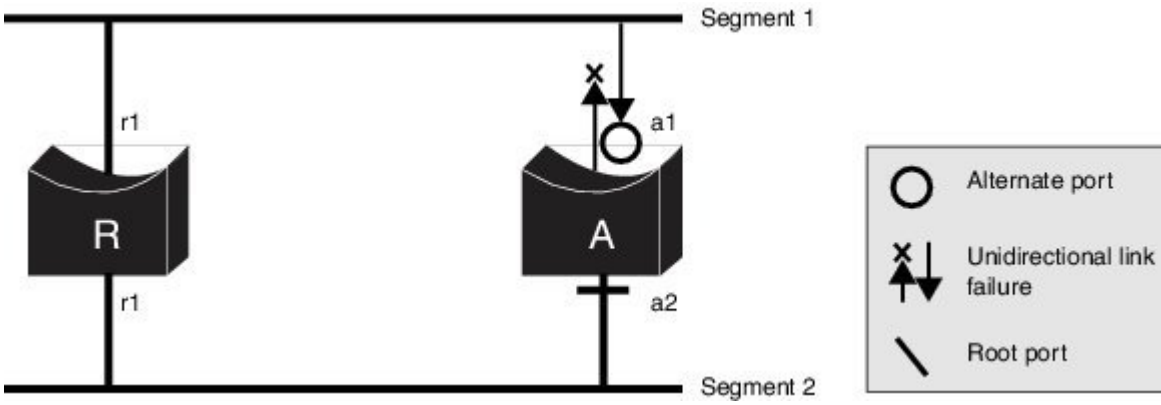


Rapid PVST+（802.1w）および MST BPDU には送信ポートのロールとステートが含まれるので、ロールがルート ブリッジではなく指定ポートであるという理由からスイッチ B が送信対象の優位 BPDU に反応しないことを、スイッチ A は（下位 BPDU から）検出します。 結果として、スイッチ A は自身のポートをブロックし（またはブロックを維持して）、ブリッジ処理のループを回避します。結果として、スイッチ A は自身のポートをブロックし（またはブロックを維持して）、ブリッジ処理のループを回避します。

解決メカニズムに関して、次のガイドラインと制約事項に留意してください。

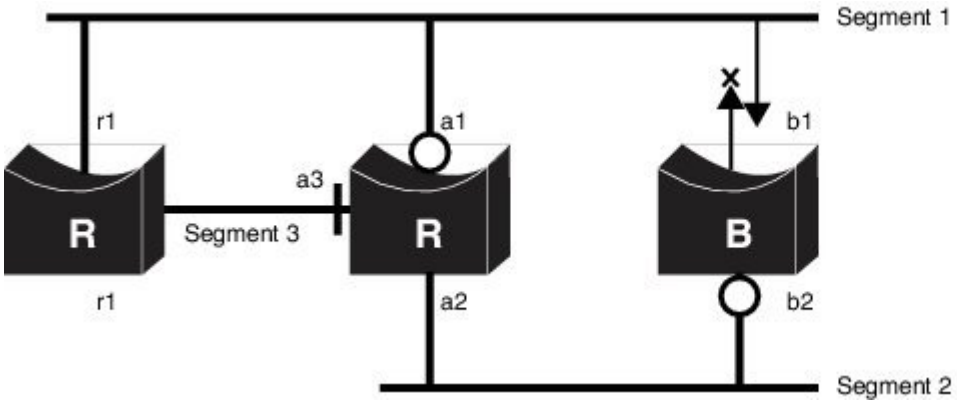
- RSTP または MST を実行するスイッチ上でのみ機能します（解決メカニズムは、BPDU を開始するポートのロールとステートを読み取る必要があります）。
- 接続が失われる原因になることがあります。たとえば、次の図のブリッジ A は、ルート ポートとして選択したポートでの送信ができません。この状況の結果として、接続が失われます（r1 と r2 は指定ポート、a1 はルート ポート、a2 は代替ポートです。A と R の間には 1 方向の接続しかありません）。

図 *11* : 接続の消失



- 共有セグメントで永久ブリッジング ループが発生する原因になることがあります。たとえば、次の図で、ブリッジ R の優先順位が最も高く、ポート b1 は共有セグメント 1 からのトラフィックを受信できずセグメント 1 の下位指定情報を送信していると仮定します。r1 と a1 はどちらもこの不整合を検出できます。ただし、現在の解決メカニズムでは、廃棄に戻るのは r1 のみであり、ルート ポート a1 は永久ループを開きます。ただし、この問題は、ポイントツーポイント リンクによって接続されたレイヤ 2 スイッチド ネットワークでは発生しません。

図 *12* : 共有セグメントのブリッジング ループ



MSTP 機能の設定方法

MST リージョンの設定および 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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst configuration** 例： `Device(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： `Device(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。 • **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。

	コマンドまたはアクション	目的
		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： `Device(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： `Device(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： `Device(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： `Device(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： `Device(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：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	

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、デバイス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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst** *instance-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]] 例： `Device(config)# spanning-tree mst 0 root primarydiameter 4 hello-time 5`	デバイスをルートデバイスとして設定します。 • *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。 •（任意）**diameter** *net-diameter* には、任意の 2 つのエンドステーション間デバイスの最大数を指定します。範囲は 2 ～ 7 です。このキー

	コマンドまたはアクション	目的
		ワードは、MSTI インスタンス 0 の場合に使用できます。 • （任意）**hello-time***seconds* seconds には、ルートスイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。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 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

セカンダリ ルート デバイスの設定

拡張システム ID をサポートするデバイスをセカンダリルートとして設定する場合、デバイス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。プライマリルートデバイスで障害が発生した場合は、このデバイスが指定インスタンスのルートデバイス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デバイスが、デフォルトのデバイスプライオリティの 32768 を使用しているためにルートデバイス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デバイスに対して実行すると、複数のバックアップルートデバイスを設定できます。**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デバイス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、デバイス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。

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
	`Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst** *instance-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]] 例： `Device(config)# spanning-tree mst 0 root secondary diameter 4 hello-time 5`	デバイスをセカンダリルートデバイスとして設定します。 • *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。 • （任意）**diameter** *net-diameter* には、任意の 2 つのエンドステーション間デバイスの最大数を指定します。範囲は 2 ～ 7 です。このキーワードは、MSTI インスタンス 0 の場合に使用できます。 • （任意）**hello-time***seconds* seconds には、ルートスイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。 プライマリ ルート スイッチ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。
ステップ 4	**end** 例： `Device(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

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。

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、デバイスで指定されて有効になっている必要があります。

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定する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： `Device(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

	コマンドまたはアクション	目的
		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： `Device(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。

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、デバイス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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定する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、物理ポートとポート チャネル論理インターフェイスがあります。ポート チャネルの範囲は 1 ～ 6 です。
ステップ 4	**spanning-tree mst** *instance-id* **cost** *cost* 例： `Device(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： `Device(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。

デバイスのプライオリティの設定

デバイスのプライオリティを変更すると、デバイスがルートデバイス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** i*nstance-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、デバイスをルートまたはセカンダリルートデバイス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デバイス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、デバイス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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst** *instance-id* **priority** *priority* 例：	デバイス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

	コマンドまたはアクション	目的
	`Devic(config)# spanning-tree mst 0 priority 40960`	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、デバイスがルートデバイスとして選択される可能性が高くなります。 使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。これらは唯一の許容値です。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

hello タイムの設定

hello タイムはルートデバイス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、デバイスで指定されて有効になっている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	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
	`Device# configure terminal`	
ステップ 3	**spanning-tree mst hello-time** *seconds* 例： `Device(config)# spanning-tree mst hello-time 4`	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 タイムはルートデバイス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、デバイス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： `Device(config)# end`	特権 EXEC モードに戻ります。

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、デバイス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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst forward-time** *seconds* 例： `Device(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

	コマンドまたはアクション	目的
		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。 *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： `Device(config)# end`	特権 EXEC モードに戻ります。

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、デバイスで指定されて有効になっている必要があります。

手順

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

	コマンドまたはアクション	目的
	`Device(config)# end`	

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、デバイスで指定されて有効になっている必要があります。

手順

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

高速移行を保証するリンク 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デバイスの単一ポートに、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、デバイス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。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定する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イスがあります。VLAN ID の範囲は 1 ～ 4094 です。ポート チャネルの範囲は 1 ～ 6 です。
ステップ 4	**spanning-tree link-type point-to-point** 例： `Device(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：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-if)# end`	

ネイバー タイプの指定

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、デバイス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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定する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： `Device(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。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

プロトコル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、ネイバーデバイスとの再ネゴシエーションを強制します。また、デバイスを MST モードに戻します。これは、IEEE 802.1D BPDU の受信後にデバイスがそれらを受信しない場合に必要です。

デバイスでプロトコルの移行プロセスを再開する（隣接するデバイス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、デバイス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。

手順

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

ステップ 2	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：
	`Device# clear spanning-tree detected-protocols`
	または
	`Device# clear spanning-tree detected-protocols interface`
		デバイスが 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、デバイスでさらにレガシー 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。

PVST+ シミュレーションの設定

PVST+ シミュレーションは、デフォルトでイネーブルになっています。つまり、すべてのポートが、Rapid PVST+ モードで動作する接続先デバイスと自動的に相互運用します。機能を無効にしてから再設定したい場合は、次の作業を参照してください。

PVST+ シミュレーションをグローバルに有効にするには、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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst simulate pvst global** 例： `Device(config)# spanning-tree mst simulate pvst global`	PVST+ シミュレーションをグローバルに有効化します。 Rapid PVST+ モードで動作する接続先デバイスとスイッチとの自動的な相互運用を回避するには、コマンドの **no** バージョンを入力します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ポート上での PVST+ シミュレーションの有効化

特定のポート上で PVST+ シミュレーションを有効化するには、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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するポートを選択します。
ステップ 4	**spanning-tree mst simulate pvst** 例： `Device(config-if)# spanning-tree mst simulate pvst`	特定のインターフェイスで PVST+ シミュレーションを有効化します。 指定したインターフェイスと MST を実行していない接続スイッチとの自動的な相互運用を回避するには、**spanning-tree mst simulate pvst disable** コマンドを入力します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show spanning-tree summary** 例： `Device# show spanning-tree summary`	設定を確認します。

MSTP の設定例

例：PVST+ シミュレーション

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

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

次に、Rapid PVST+ を実行している接続先デバイスとポートが自動的に相互運用しないようにする例を示します。

```
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# spanning-tree mst simulate pvst disable
```

次の出力例は、PVST+ シミュレーション無効時にポートで SSTP BPDU を受信した場合に受け取るシステム メッセージを示しています。

```
Message
SPANTREE_PVST_PEER_BLOCK: PVST BPDU detected on port %s [port number].

Severity
Critical

Explanation
A PVST+ peer was detected on the specified interface on the switch.
PVST+ simulation feature is disabled, as a result of which the interface
 was moved to the spanning tree
Blocking state.

Action
Identify the PVST+ switch from the network which might be configured
incorrectly.
```

次の出力例は、インターフェイスのピア不整合が解消したときに受け取るシステムメッセージを示しています。

```
Message
SPANTREE_PVST_PEER_UNBLOCK: Unblocking port %s [port number].

Severity
Critical

Explanation
The interface specified in the error message has been restored to normal
 spanning tree state.

Action
None.
```

この例は、ポート 0/1 を設定して PVST+ シミュレーションを無効にし、そのポートがピアタイプ不整合状態にあるときの、スパニングツリーステータスを示しています。

```
Device# show spanning-tree
VLAN0010
  Spanning tree enabled protocol mstp
  Root ID Priority  32778
          Address   0002.172c.f400
```

```
         This bridge is the root
         Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
           Address  0002.172c.f400
         Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
         Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Gi0/1           Desg BKN*4         128.270 P2p *PVST_Peer_Inc
```

次に、MSTP モードで PVST+ シミュレーションが有効である場合のスパニング ツリーの概要の例を示します。

```
Device# show spanning-tree summary
Switch is in mst mode (IEEE Standard)
Root bridge for: MST0
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long
PVST Simulation Default is enabled
Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
MST0                          2         0        0          0
 2
---------------------- -------- --------- -------- ---------- ----------
1 mst                         2         0        0          0
 2
```

次に、STP モードで PVST+ シミュレーションが無効である場合のスパニング ツリーの概要の例を示します。

```
Device# show spanning-tree summary
Switch is in mst mode (IEEE Standard)
Root bridge for: MST0
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long
PVST Simulation Default is disabled
Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
MST0                           2         0        0          0
```

```
 2
---------------------- -------- --------- -------- ---------- ----------
1 mst                           2         0        0          0
 2
```

次に、スイッチが MSTP モードでない場合、つまりスイッチが PVST または Rapid-PVST モードの場合のスパニング ツリーの概要の例を示します。出力文字列は現在の STP モードを表示します。

```
Device# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001, VLAN2001-VLAN2002
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is short
PVST Simulation Default is enabled but inactive in rapid-pvst mode
Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                       2         0        0          0
 2
VLAN2001                       2         0        0          0
 2
VLAN2002                       2         0        0          0
 2
---------------------- -------- --------- -------- ---------- ----------
3 vlans                        6         0        0          0
 6
```

この例は、PVST+シミュレーションがグローバルに有効な場合（デフォルト設定）のインターフェイスの詳細を示しています。

```
Device# show spanning-tree interface 0/1 detail
Port 269 (GigabitEthernet1/0/1) of VLAN0002 is forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.297.
   Designated root has priority 32769, address 0013.5f20.01c0
   Designated bridge has priority 32769, address 0013.5f20.01c0
   Designated port id is 128.297, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   PVST Simulation is enabled by default
   BPDU: sent 132, received 1
```

この例は、PVST+シミュレーションがグローバルに無効な場合のインターフェイスの詳細を示しています。

```
Device# show spanning-tree interface 0/1 detail
Port 269 (GigabitEthernet1/0/1) of VLAN0002 is forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.297.
```

```
   Designated root has priority 32769, address 0013.5f20.01c0
   Designated bridge has priority 32769, address 0013.5f20.01c0
   Designated port id is 128.297, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   PVST Simulation is disabled by default
   BPDU: sent 132, received 1
```

この例は、PVST+シミュレーションがポートで明示的に有効化されている場合のインターフェイスの詳細を示しています。

```
Device# show spanning-tree interface 0/1 detail
Port 269 (GigabitEthernet1/0/1) of VLAN0002 is forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.297.
   Designated root has priority 32769, address 0013.5f20.01c0
   Designated bridge has priority 32769, address 0013.5f20.01c0
   Designated port id is 128.297, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   PVST Simulation is enabled
   BPDU: sent 132, received 1
```

この例は、ポートで PVST+ シミュレーション機能が無効になっており PVST ピア不整合が検出された場合のインターフェイスの詳細を示しています。

```
Device# show spanning-tree interface 0/1 detail
Port 269 (GigabitEthernet1/0/1) of VLAN0002 is broken (PVST Peer Inconsistent)
   Port path cost 4, Port priority 128, Port Identifier 128.297.
   Designated root has priority 32769, address 0013.5f20.01c0
   Designated bridge has priority 32769, address 0013.5f20.01c0
   Designated port id is 128.297, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   PVST Simulation is disabled
   BPDU: sent 132, received 1
```

例：単方向リンク障害の検出

この例は、ポート **0/1 detail** を設定して PVST+ シミュレーションを無効にし、ポートが現在ピアタイプ不整合状態にあるときの、スパニングツリーステータスを示しています。

```
Device# show spanning-tree
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority 32778
             Address  0002.172c.f400
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID  Priority 32778 (priority 32768 sys-id-ext 10)
             Address  0002.172c.f400
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Gi0/1            Desg BKN 4         128.270  P2p Dispute
```

この例は、競合する状態が検出された場合のインターフェイスの詳細を示しています。

```
Device# show spanning-tree interface 1/0/1 detail
Port 269 (GigabitEthernet1/0/1) of VLAN0002 is designated blocking (dispute)
   Port path cost 4, Port priority 128, Port Identifier 128.297.
   Designated root has priority 32769, address 0013.5f20.01c0
   Designated bridge has priority 32769, address 0013.5f20.01c0
   Designated port id is 128.297, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 132, received 1
```

MST の設定およびステータスのモニタリング

表 *9 : MST* ステータスを表示するコマンド

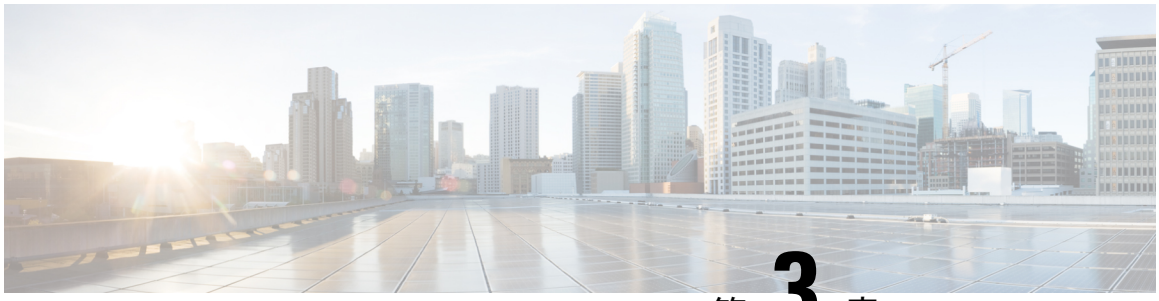
show spanning-tree mst configuration	MST リージョンの設定を表示します。
show spanning-tree mst configuration digest	現在の MSTCI に含まれる MD5 ダイジェストを表示します。
show spanning-tree mst	すべてのインスタンスの MST 情報を表示します。 （注） このコマンドは、リンクアップ動作可能状態のポートの情報を表示します。
show spanning-tree mst *instance-id*	指定インスタンスの MST 情報を表示します。 （注） このコマンドは、ポートがリンクアップ動作可能状態の場合にのみ情報を表示します。
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。

MSTP の機能情報

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

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

機能名	リリース	機能情報
MSTP	Cisco IOS Release 15.2(7)E3k	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の制約事項

- PortFast は、スパニング ツリーがコンバージェンスするまでにインターフェイスが待機する時間を最短にするため、これはエンドステーションに接続されているインターフェイスで使用される場合のみ有用です。他のスイッチに接続するインターフェイスで PortFast をイネーブルにすると、スパニングツリーのループが生じることがあります。

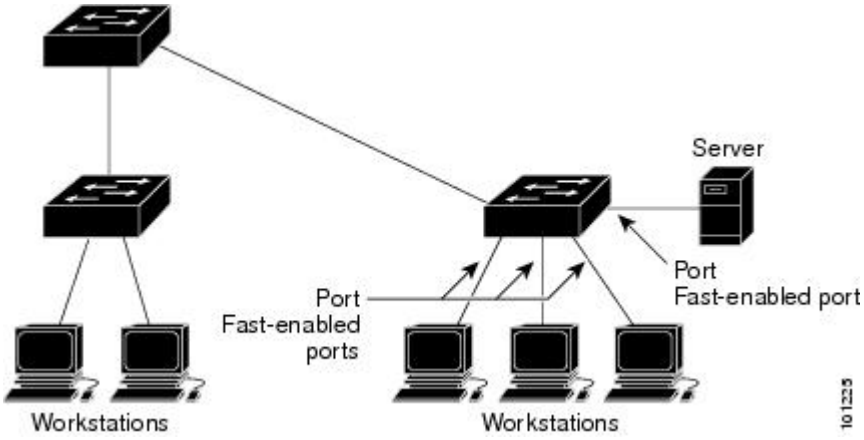
オプションのスパニングツリー機能について

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 *13 : 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。

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。

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。

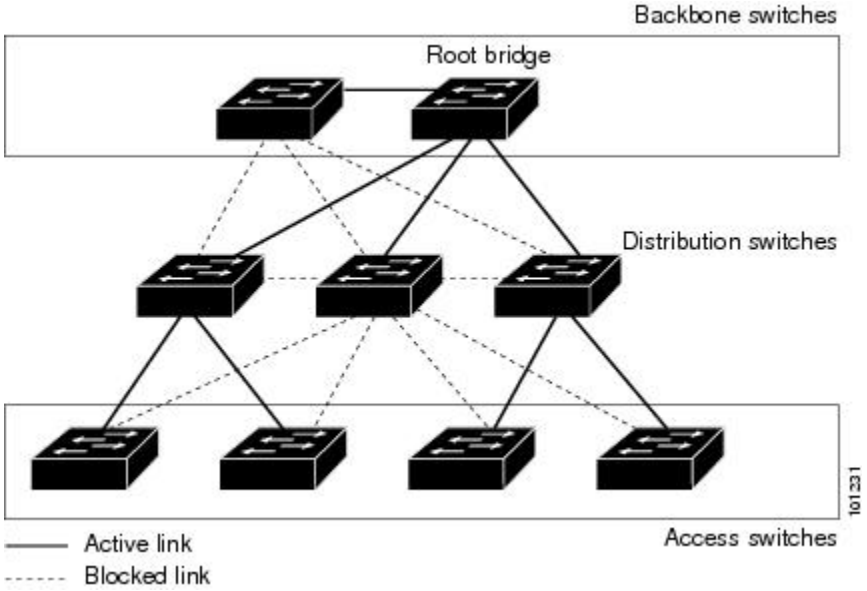
スイッチ全体または1つのインターフェイスでBPDUフィルタリング機能をイネーブルにできます。

UplinkFast

図 *14 :* 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 *15* : 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。

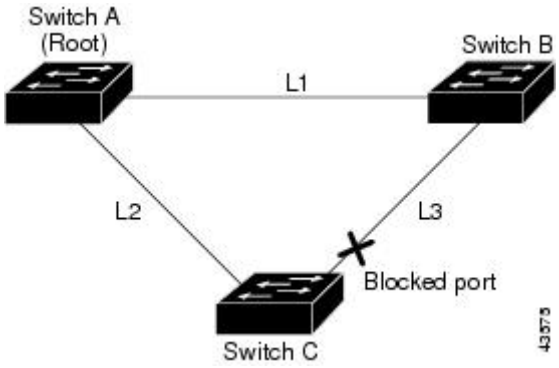
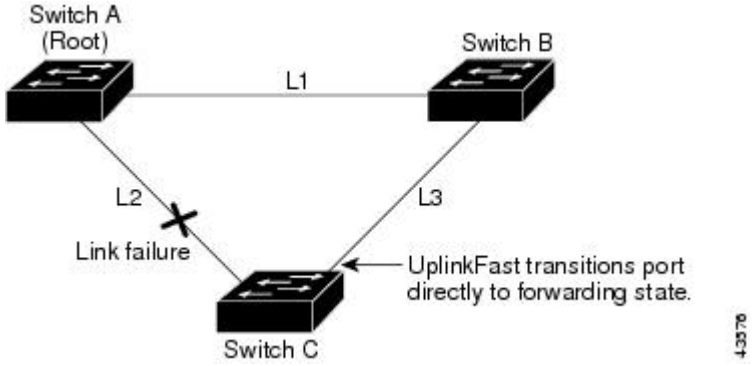


図 *16* : 直接リンク障害が発生したあとの *UplinkFast* の例

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。



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。

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 *17*：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。

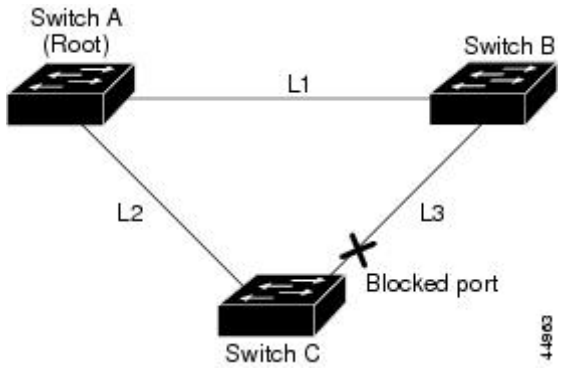


図 *18*：間接リンク障害が発生したあとの *BackboneFast* の例

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。

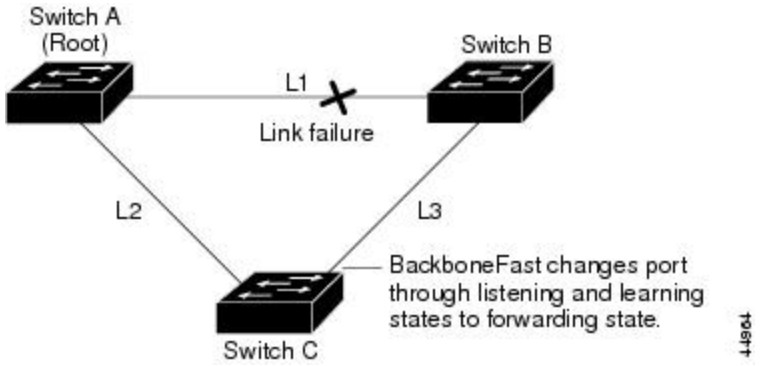
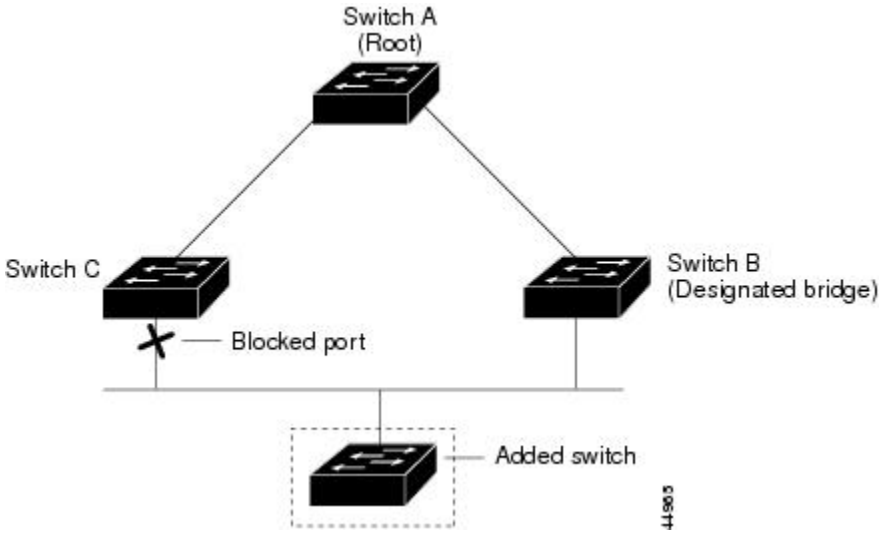


図 *19* : メディア共有型トポロジにおけるスイッチの追加

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。



EtherChannel ガード

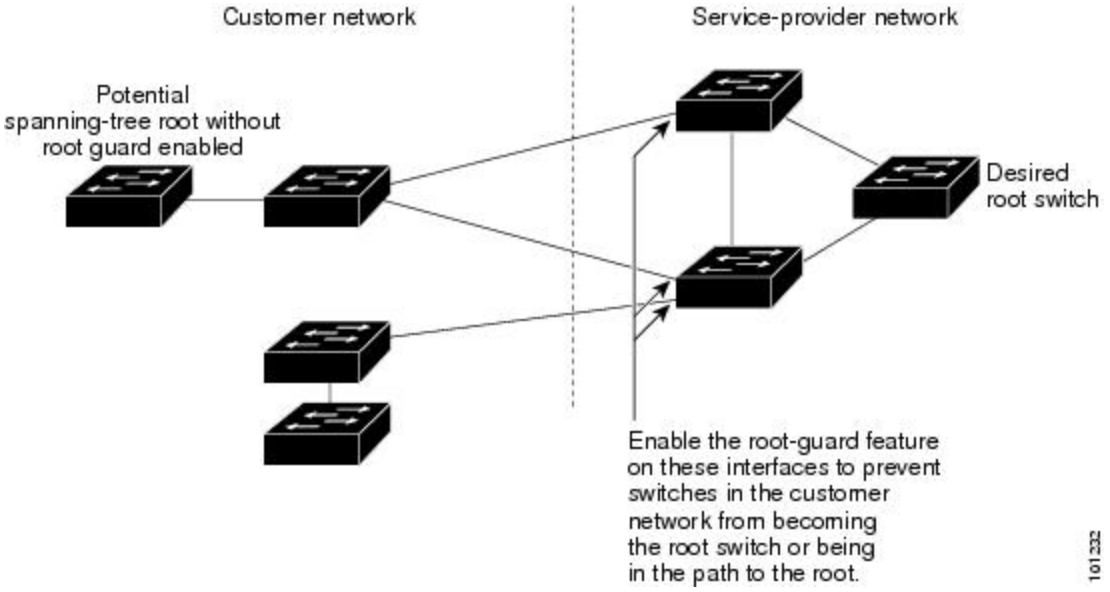
EtherChannel ガードを使用すると、スイッチと接続したデバイス間での EtherChannel の設定の矛盾を検出できます。スイッチ インターフェイスは EtherChannel として設定されているものの、もう一方のデバイスのインターフェイスではその設定が行われていない場合、設定の矛盾が発生します。また、EtherChannel の両端でチャネルのパラメータが異なる場合にも、設定の矛盾が発生します。

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。

ルート ガード

図 *20 :* 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。

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。

STP PortFast ポート タイプ

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

インターフェイスが接続されているデバイスのタイプによって、スパニング ツリー ポートを下記のいずれかのポート タイプに設定できます。

- PortFast エッジ ポート：レイヤ 2 ホストに接続されます。これにはアクセス ポートまたはエッジ トランク ポート（**portfast edge trunk**）のいずれかを使用できます。このタイプのポート インターフェイスは、リスニング ステートとラーニング ステートをバイパスして、直接フォワーディング ステートに移行します。1 台のワークステーションまたはサーバに接続されたレイヤ 2 アクセス ポート上で PortFast エッジを使用すると、スパニング ツリーのコンバージェンスを待たずに、デバイスがただちにネットワークに接続されます。

  インターフェイスでブリッジ プロトコル データ ユニット（BPDU）が受信されても、スパニングツリーがポートをブロッキング ステートにしません。スパニング ツリーは、設定されたステートが *port fast edge* のままでトポロジ変更への参加を開始している場合でも、ポートの動作ステートを *non-port fast* に設定します。

（注） レイヤ 2 スイッチまたはブリッジに接続しているポートをエッジ ポートとして設定すると、ブリッジングループが発生することがあります。

- PortFast ネットワーク ポート：レイヤ 2 スイッチまたはブリッジのみに接続されます。Bridge Assurance は PortFast ネットワーク ポート上でのみ有効になります。詳細については、*Bridge Assurance* を参照してください。

（注） レイヤ 2 にホスト接続されたポートをスパニング ツリー ネットワーク ポートとして設定すると、そのポートは自動的にブロッキング ステートになります。

- PortFast 標準ポート：スパニング ツリー ポートのデフォルト タイプです。

（注） Cisco IOS リリース 15.2(4) E または IOS XE 3.8.0E 以降、グローバルまたはインターフェイス コンフィギュレーション モードで **spanning-tree portfast** [trunk] コマンドを入力すると、このコマンドが **spanning-tree portfast edge** [trunk] として自動的に保存されます。

Bridge Assurance

Bridge Assurance は、単方向リンク（リンクまたはポートの一方向のみのトラフィック）または隣接スイッチの機能不全が原因で発生するループ状態を防止するのに役立ちます。ここで言う機能不全とは、トラフィックの転送はまだ可能だが STP の実行ができなくなってしまったスイッチ（ブレインデッド スイッチ）のことを指します。

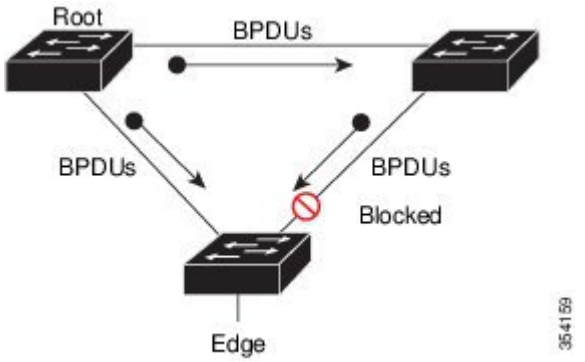
動作中のすべてのネットワーク ポート（代替ポートとバックアップ ポートを含む）に、BPDU が hello タイムごとに送出されます。Bridge Assurance では、すべてのネットワーク ポートのポイントツーポイント リンクでの BPDU の受信がモニタされます。割り当てられた hello タイム期間内にポートが BPDU を受信しない場合、ポートはブロック状態（フレームの転送が停止するポート不整合状態と同じ）になります。ポートが BPDU の受信を再開すると、ポートは通常のスパニング ツリー動作を再開します。

（注） Bridge Assurance をサポートするのは、Rapid PVST+ および MST スパニング ツリー プロトコルのみです。PVST+ は Bridge Assurance をサポートしません。

次に、Bridge Assurance によってネットワークをブリッジング ループから保護する例を示します。

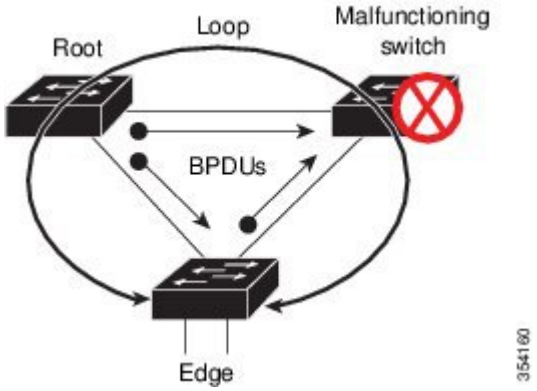
次の図は、標準的な STP トポロジを使用するネットワークを示しています。

図 *21* : 標準的な *STP* トポロジのネットワーク



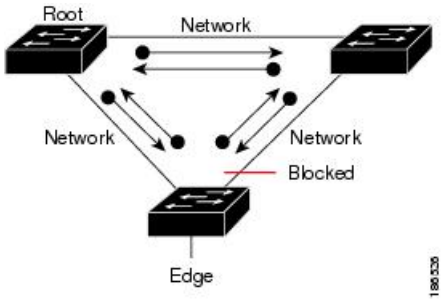
次の図は、デバイスで障害が発生し（ブレインデッド）、Bridge Assurance が有効でないときにネットワークで発生する可能性のある問題を示しています。

図 *22* : スイッチの機能不全によるネットワーク ループ



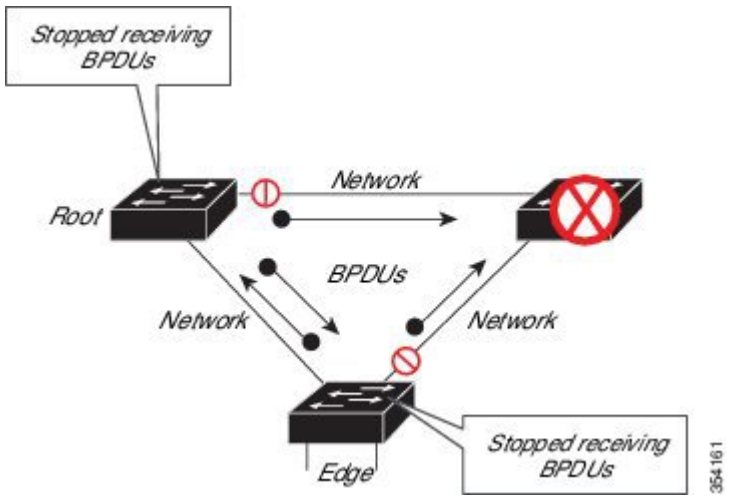
次の図は、Bridge Assurance が有効になっているネットワークで、すべての STP ネットワーク ポートから双方向 BPDU が発行される一般的な STP トポロジを示しています。

図 *23* : *Bridge Assurance* を実行している *STP* トポロジのネットワーク



次の図は、スイッチの機能不全によるネットワークループの図に示した潜在的なネットワーク問題を、ネットワークで Bridge Assurance を有効にすることによって回避する様子を示しています。

図 *24 : Bridge Assurance* によるネットワーク上の問題の回避



ポートがブロック/ブロック解除されると、システムは syslog メッセージを生成します。次の出力例は、それぞれの場合に生成されるログを示しています。

BRIDGE_ASSURANCE_BLOCK

```
Sep 17 09:48:16.249 PDT: %SPANTREE-2-BRIDGE_ASSURANCE_BLOCK: Bridge Assurance blocking
port GigabitEthernet1/0/1 on VLAN0001.
```

BRIDGE_ASSURANCE_UNBLOCK

```
Sep 17 09:48:58.426 PDT: %SPANTREE-2-BRIDGE_ASSURANCE_UNBLOCK: Bridge Assurance unblocking
 port GigabitEthernet1/0/1 on VLAN0001.
```

Bridge Assurance を有効にする際は、次の注意事項に従ってください。

- グローバルな有効化または無効化のみ可能です。
- これは、代替ポートとバックアップ ポートを含め、動作中のすべてのネットワーク ポートに適用されます。
- Bridge Assurance をサポートするのは、Rapid PVST+ および MST スパニング ツリー プロトコルのみです。PVST+ は Bridge Assurance をサポートしません。
- Bridge Assurance が正しく動作するには、ポイントツーポイント リンクの両端で Bridge Assurance がサポートおよび設定されている必要があります。リンクの一端のデバイスで Bridge Assurance が有効であっても、他端のデバイスで有効になっていない場合、接続ポートはブロックされ、Bridge Assurance 不整合状態となります。Bridge Assurance は、ネットワーク全体でイネーブルにすることを推奨します。

- ポート上で Bridge Assurance をイネーブルにするには、BPDU フィルタリングと BPDU Guard をディセーブルにする必要があります。
- Bridge Assurance は、Loop Guard とともにイネーブルにできます。
- Bridge Assurance は、ルート ガードとともにイネーブルにできます。後者は、ネットワークでのルート ブリッジの配置を強制する方法を提供するように設計されています。

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	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** {**disable** | **edge** | **network**} 例： `Device(config-if)# spanning-tree portfast edge`	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。 追加オプションには次のキーワードを入力します。 • インターフェイスで PortFast をディセーブルにするには、**disable** と入力します。 • インターフェイスで PortFast エッジをイネーブルにするには、**edge** と入力します。 • インターフェイスで PortFast ネットワークをイネーブルにするには、**network** と入力します。 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： `Device(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。

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	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 4	**spanning-tree portfast edge** 例： `Device(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 5	**end** 例： `Device(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。

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree portfast edge bpdufilter default** 例： `Device(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：	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

	コマンドまたはアクション	目的
	`Device(config)# interface gigabitethernet 1/0/2` 例：	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： `Device(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： `Device(config-if)# end`	特権 EXEC モードに戻ります。

冗長リンク用 UplinkFast のイネーブル化

（注） UplinkFast をイネーブルにすると、スイッチのすべての 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 用に、UplinkFast 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。UplinkFast 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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree uplinkfast** [**max-update-rate** *pkts-per-second*] 例： `Device(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。
ステップ 4	**end** 例： `Device(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。

UplinkFast のディセーブル化

この手順は任意です。

UplinkFast 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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no spanning-tree uplinkfast** 例： `Device(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 をディセーブルにします。
ステップ 4	end 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

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。

BackboneFast のイネーブル化

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree backbonefast** 例： `Device(config)# spanning-tree backbonefast`	BackboneFast をイネーブルにします。
ステップ 4	end 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

EtherChannel ガードのイネーブル化

デバイスで 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。

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

	コマンドまたはアクション	目的
ステップ 3	**spanning-tree etherchannel guard misconfig** 例： `Device(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： `Device(config-if)# end`	特権 EXEC モードに戻ります。

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デバイス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。

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

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。

デバイスで 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。デバイス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：
	`Device# show spanning-tree active`
	または
	`Device# 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree loopguard default** 例： `Device(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： `Device(config-if)# end`	特権 EXEC モードに戻ります。

PortFast ポート タイプの有効化

このセクションでは、PortFast ポート タイプを有効化するさまざまな手順について説明します。

デフォルト ポート ステートのグローバル設定

デフォルト PortFast のステートを設定するには、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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree portfast** [**edge** | **network** | **normal**] **default** 例： `Device(config)# spanning-tree portfast default`	スイッチ上のすべてのインターフェイスのデフォルト状態を設定します。次のオプションがあります。 • （任意）**edge**：すべてのインターフェイスをエッジ ポートとして設定します。このコマンドでは、すべてのポートがホストまたはサーバに接続されているものとします。 • （任意）**network**：すべてのインターフェイスをスパニング ツリー ネットワーク ポートとして設定します。このコマンドでは、すべてのポートがスイッチまたはブリッジに接続されているものとします。Bridge Assurance は、デフォルトですべてのネットワーク ポート上で有効化されています。 • （任意）**normal**：すべてのインターフェイスを通常のスパニングツリー ポートとして設定します。標準ポートは、任意のタイプのデバイスに接続できます。 • **default**：デフォルトのポート タイプは「normal」です。
ステップ 4	end 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

指定したインターフェイスでの PortFast エッジの設定

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

（注） このタイプのポートの目的は、アクセス ポートがスパニング ツリーのコンバージェンスを待機する時間を最小限に抑えることです。したがって、アクセスポートで使用したときに最も効果を発揮します。別のスイッチに接続しているポートで PortFast エッジを有効にすると、スパニング ツリー ループが作成されるリスクがあります。

指定のインターフェイスにエッジ ポートを設定する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* | **port-channel** *port_channel_number* 例： `Device(config)# interface gigabitethernet 1/0/2`	設定するインターフェイスを選択します。
ステップ 4	**spanning-tree portfast edge** [**trunk**] 例： `Device(config-if)# spanning-tree portfast trunk`	エンド ワークステーションまたはサーバに接続されたレイヤ 2 アクセス ポート上でエッジの動作を有効にします。 • （任意）**trunk** キーワード：トランク ポート上のエッジの動作を有効化します。リンクがトランクである場合、このキーワードを使用します。このコマンドを使用するのは、VLANの終端となっており、そこからの STP BPDU がポートで受信されることのない、エンド ホストのデバイスに接続されているポート上

	コマンドまたはアクション	目的
		のみとします。このようなエンドホスト デバイスには、ブリッジングをサポートするように設定されていないルータ上のワークステーション、サーバ、ポートなどがあります。 • PortFast エッジを無効にするには、コマンドの **no** バージョンを使用します。
ステップ 5	end 例： `Device(config-if)# end`	設定モードを終了します。
ステップ 6	**show running interface** *interface-id* | **port-channel** *port_channel_number* 例： `Device# show running interface gigabitethernet 1/0/2`	設定を確認します。

指定したインターフェイスでの PortFast ネットワーク ポートの設定

レイヤ2スイッチおよびブリッジに接続されているポートをネットワーク ポートとして設定できます。

（注） Bridge Assurance は PortFast ネットワーク ポート上でのみ有効になります。詳細については、*Bridge Assurance* を参照してください。

ポートをネットワーク ポートとして設定するには、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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	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
	`Device# configure terminal`	
ステップ 3	**interface** *interface-id* | **port-channel** *port_channel_number* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを選択します。
ステップ 4	**spanning-tree portfast network** 例： `Device(config-if)# spanning-tree portfast network`	エンド ワークステーションまたはサーバに接続されたレイヤ 2 アクセス ポート上でエッジの動作を有効にします。 • ポートをネットワーク ポートとして設定します。Bridge Assurance をグローバルに有効化している場合、スパニング ツリー ネットワーク ポート上で Bridge Assurance が自動的に実行されます。 • PortFast を無効にするには、コマンドの **no** バージョンを使用します。
ステップ 5	end 例： `Device(config-if)# end`	設定モードを終了します。
ステップ 6	**show running interface** *interface-id* | **port-channel** *port_channel_number* 例： `Device# show running interface gigabitethernet 1/0/1`	設定を確認します。

Bridge Assurance の有効化

Bridge Assurance を設定するには、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：	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
	`Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree bridge assurance** 例： `Device(config)# spanning-tree bridge assurance`	スイッチのすべてのネットワーク ポートで Bridge Assurance をイネーブルにします。 デフォルトでは、[Bridge Assurance] はイネーブルになっています。 この機能を無効にするには、このコマンドの **no** バージョンを使用します。ブリッジ保証をディセーブルにすると、すべての設定済みネットワーク ポートが標準のスパニングツリー ポートとして動作します。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show spanning-tree summary** 例： `Device# show spanning-tree summary`	スパニング ツリー情報を表示し、Bridge Assurance が有効になっているかを示します。

オプションのスパニングツリー機能の設定例

例：指定したインターフェイスでの PortFast エッジの設定

次の例は、GigabitEthernetインターフェイス 1/0/1 でエッジの動作を有効化する方法を示しています。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# spanning-tree portfast edge
Switch(config-if)# end
Switch#
```

次に、設定を確認する例を示します。

```
Switch# show running-config interface gigabitethernet 1/0/1
Building configuration...
Current configuration:
!
interface GigabitEthernet1/0/1
no ip address
switchport
switchport access vlan 200
switchport mode access
spanning-tree portfast edge
end
```

次の例は、ポート GigabitEthernet1/0/1 が現在エッジ状態にあることを表示するための方法を示しています。

```
Switch# show spanning-tree vlan 200
VLAN0200
Spanning tree enabled protocol rstp
Root ID Priority 2
Address 001b.2a68.5fc0
Cost 3
Port 125 (GigabitEthernet1/5/9)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 2 (priority 0 sys-id-ext 2)
Address 7010.5c9c.5200
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 0 sec
Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Desg FWD 4 128.1 P2p Edge
```

例：指定したインターフェイスでの PortFast ネットワーク ポートの設定

この例は、GigabitEthernet インターフェイス 1/0/1 をネットワークポートとして設定する方法を示しています。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# spanning-tree portfast network
Switch(config-if)# end
Switch#
```

次に、設定を確認する例を示します。

```
Switch# show running-config interface gigabitethernet 1/0/1
Building configuration...
Current configuration:
!
interface GigabitEthernet1/0/1
no ip address
switchport
switchport access vlan 200
switchport mode access
spanning-tree portfast network
end
```

この例は、show spanning-tree vlan の出力を示しています。

```
Switch# show spanning-tree vlan
Sep 17 09:51:36.370 PDT: %SYS-5-CONFIG_I: Configured from console by console2

VLAN0002
  Spanning tree enabled protocol rstp
  Root ID    Priority    2
             Address     7010.5c9c.5200
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    2      (priority 0 sys-id-ext 2)
             Address     7010.5c9c.5200
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  0   sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Desg FWD 4         128.1    P2p Edge
Po4                 Desg FWD 3         128.480  P2p Network
Gi4/0/1             Desg FWD 4         128.169  P2p Edge
Gi4/0/47            Desg FWD 4         128.215  P2p Network

Switch#
```

例：Bridge Assurance の設定

この出力は、ポート GigabitEthernet 1/0/1 がネットワークポートとして設定され、現在 Bridge Assurance 不整合状態にあることを示しています。

（注） この出力ではポートタイプがネットワークおよび*BA_Inc と表示されています。これは、ポートが不整合状態にあることを示しています。

```
Device# show spanning-tree
VLAN0010
Spanning tree enabled protocol rstp
Root ID Priority 32778
Address 0002.172c.f400
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
Address 0002.172c.f400
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface Role Sts   Cost    Prio.   Nbr    Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1    Desg BKN*4 128.270 Network, P2p *BA_Inc
```

この例は、show spanning-tree summary の出力を示しています。

```
Device# sh spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001-VLAN0002, VLAN0128
EtherChannel misconfig guard            is enabled
Extended system ID                      is enabled
Portfast Default                        is network
```

```
Portfast Edge BPDU Guard Default        is disabled
Portfast Edge BPDU Filter Default       is disabled
Loopguard Default                       is enabled
PVST Simulation Default                 is enabled but inactive in rapid-pvst mode
Bridge Assurance                        is enabled
UplinkFast                              is disabled
BackboneFast                            is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                     0         0        0          5          5
VLAN0002                     0         0        0          4          4
VLAN0128                     0         0        0          4          4
---------------------- -------- --------- -------- ---------- ----------
3 vlans                      0         0        0         13         13

Device#
```

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

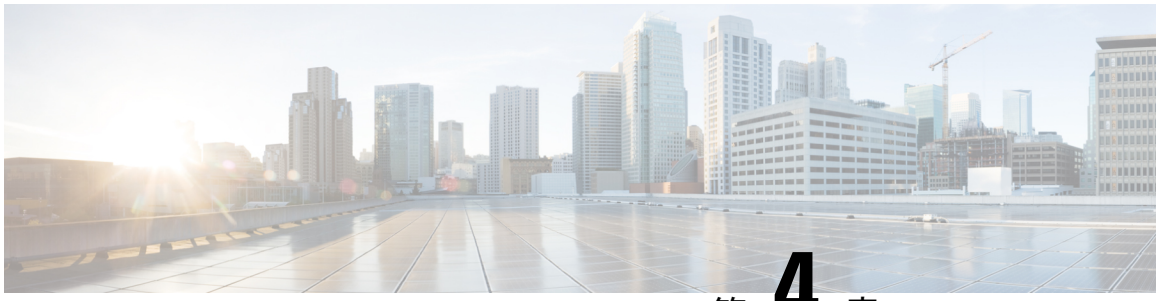
コマンド	目的
show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree mst interface *interface-id*	指定インターフェイスのMST情報を表示します。
show spanning-tree summary [**totals**]	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の機能情報

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

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

機能名	リリース	機能情報
オプションのスパニングツリー機能	Cisco IOS Release 15.2(7)E3k	この機能が導入されました。



第 4 章

Resilient Ethernet Protocol の設定

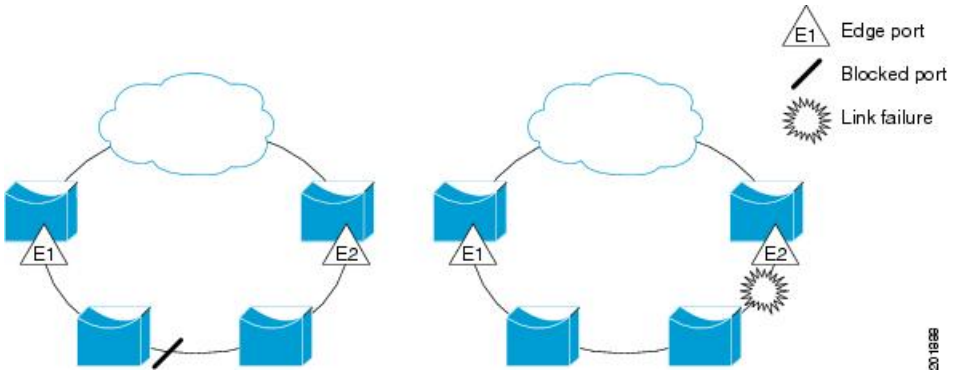
Resilient Ethernet Protocol の概要

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 つのユーザ設定のエッジ ポートで構成されています。1 つのデバイス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経由できますが、どのリンクでも同じセグメントに属することができるポートは 2 つだけです。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。

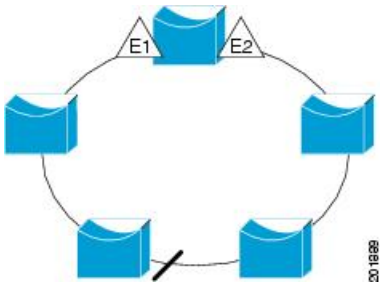
図 *25 : REP* オープン セグメント



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。セグメント内のデバイス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。

次の図に示すセグメントはリング セグメントであり、同じデバイス上に両方のエッジ 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デバイス間で冗長接続を形成することができます。

図 *26 : REP* リング セグメント



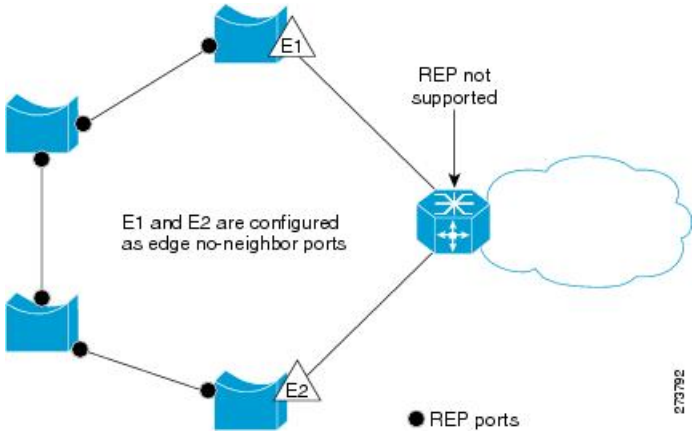
REP セグメントには、次のような特徴があります。

- 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（セグメント内の任意のポート）で制御される 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、次の図に示すように、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。その場合、送信される STP トポロジ変更通知（TCN）は、マルチ スパニングツリー（MST）STP メッセージになります。

図 *27*：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。ネイバーが検出されるまで、インターフェイス上ですべての VLAN がブロックされます。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。ネイバーとの隣接関係が確立されると、代替ポートとして機能する、セグメントのブロックされたポートを決定するようにポートが相互にネゴシエートします。その他のすべてのポートのブロックは解除されます。デフォルトでは、REP パケットはブリッジ プロトコル データ ユニットクラスの 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。

高速コンバージェンス

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。

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。

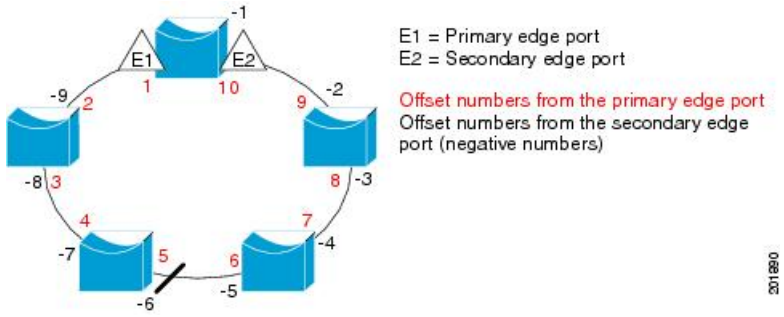
- インターフェイスにポート ID を入力します。セグメント内のポート ID を識別するには、ポートの **show interface rep detail** インターフェイス コンフィギュレーション コマンドを入力します。

- **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。
- 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。

次の図に、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。

図 *28* : 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、メッセージがネットワークに送信され、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、**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 機能とは対話しませんが、共存は可能です。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、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実施され、セグメントが安定すると、1 つのブロックされたポートが代替ロールに留まり、他のすべてのポートがオープン ポートになります。
- リンク内で障害が発生すると、すべてのポートが障害ステートに遷移します。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。

Resilient Ethernet Protocol の設定方法

セグメントは、チェーンで相互接続され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、デフォルトで 1 つをプライマリ エッジ ポート、もう 1 つをセカンダリ 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。必要に応じて、STCN および VLAN ロード バランシングが送信される場所を設定できます。

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 の送信タスクはディセーブルで、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。
- 別の REP インターフェイスがブロックを解除する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、Telnet 接続で REP を設定するときは注意してください。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 ポートを設定する必要があります。これを行わないと、設定ミスが発生します。
- REP がスイッチの 2 つのポートでイネーブルである場合、両方のポートが通常セグメント ポートまたはエッジ ポートのいずれか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。しかし、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。したがって、突然の切断を避けるために REP インターフェイスの状態には注意する必要があります。
- REP はネイティブ VLAN にすべての 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 64 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**rep admin vlan** *vlan-id* 例： `Device(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： `Device(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： `Device(config)# show interface gigabitethernet 1/0/1 rep detail`	（任意）REP インターフェイスの設定を検証します。
ステップ 5	**copy running-config startup config** 例： `Device# 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 を設定する場合、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 を指定します。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。それ以外の手順はすべてオプションです。

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。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。
ステップ 4	**switchport mode trunk** 例： `Device# 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**] 例： `Device# rep segment 1 edge no-neighbor primary`	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。 （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。 これらの任意のキーワードは利用可能です。 • （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** キーワードを入力すると、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

	コマンドまたはアクション	目的
		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。ポートはエッジポートのすべてのプロパティを継承し、エッジポートの場合と同様にプロパティを設定できます。 （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。

	コマンドまたはアクション	目的
ステップ 6	**rep stcn** {**interface** *interface id* | **segment** *id-list* | **stp**} 例： `Device# rep stcn segment 25-50`	（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** コマンドを設定する場合は、スパニング ツリー（MST）モード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**} 例： `Device# rep block port id 0009001818D68700 vlan 1-100`	（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（**id** *port-id*、*neighbor_offset*、**preferred**）、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

	コマンドまたはアクション	目的
		トを代替ポートとして識別します。 （注） プライマリ エッジ ポート（オフセット番号 1）に **rep block port** 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* 例： `Device# rep preempt delay 100`	（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。 • 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* 例： `Device# rep lsl-age-timer 2000`	（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。

	コマンドまたはアクション	目的
		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** 例： `Device(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 11	**show interface** ［*interface-id*］ **rep** [**detail**] 例： `Device# show interface gigabitethernet 1/0/1 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** 例： `Device(config)# 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* 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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2		
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 4	**rep preempt segment** *segment-id*
	例：
	`Device# rep preempt segment 100`
	`The command will cause a momentary traffic disruption.`
	`Do you still want to continue? [confirm]`
		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 5	**show rep topology segment** *segment-id* 例： `Device# show rep topology segment 100`	（任意）REP トポロジの情報を表示します。
ステップ 6	**end** 例： `Device# end`	特権 EXEC モードを終了します。

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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**snmp mib rep trap-rate** *value* 例： `Device(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： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** 例： `Device# 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： `Device# 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。

Resilient Ethernet Protocol 設定のモニタリング

このトピックのコマンドを使用して、REP インターフェイスと REP トポロジの詳細を表示できます。

- **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。

  例：

```
Device# show interfaces TenGigabitEthernet4/1/1 rep detail

TenGigabitEthernet4/1/1 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
```

```
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

- **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。

  例：

```
Device# show rep topology

REP Segment 1
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
10.64.106.63     Te5/4      Pri  Open
10.64.106.228    Te3/4           Open
10.64.106.228    Te3/3           Open
10.64.106.67     Te4/3           Open
10.64.106.67     Te4/4           Alt
10.64.106.63     Te4/4      Sec  Open

REP Segment 3
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
10.64.106.63     Gi50/1     Pri  Open
SVT_3400_2       Gi0/3           Open
SVT_3400_2       Gi0/4           Open
10.64.106.68     Gi40/2          Open
10.64.106.68     Gi40/1          Open
10.64.106.63     Gi50/2     Sec  Alt
```

Resilient Ethernet Protocol の設定例

ここでは、次の設定例について説明します。

例：REP 管理 VLAN の設定

次に、管理VLANをVLAN 100として設定して、REPインターフェイスの1つに**show interface rep detail**コマンドを入力して設定を確認する例を示します。

```
Device# configure terminal
Device(config)# rep admin vlan 100
Device(config)# end
Device# show interface gigabitethernet1/0/1 rep detail

GigabitEthernet1/0/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E7144680
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 0002001121A2D5800E4D
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 100
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190
```

次に、セグメントごとに管理 VLAN を作成する例を示します。ここでは、VLAN 2 は REP セグメント 2 でのみ管理 VLAN として設定されます。設定されていない残りのすべてのセグメントは、デフォルトで VLAN 1 が管理 VLAN となります。

```
Device# configure terminal
Device(config)# rep admin vlan 2 segment 2
Device(config)# end
```

例：REP インターフェイスの設定

次に、インターフェイスをセグメント 1 のプライマリ エッジ ポートに設定し、STCN をセグメント 2 ～ 5 に送信し、代替ポートをポート ID 0009001818D68700 のポートとして設定して、セグメント ポート障害および回復後の 60 秒のプリエンプション遅延後にすべての VLAN をブロックする例を示します。このインターフェイスは、ネイバーからの hello が受信されないまま 6000 ミリ秒が経過するとダウンするように設定されています。

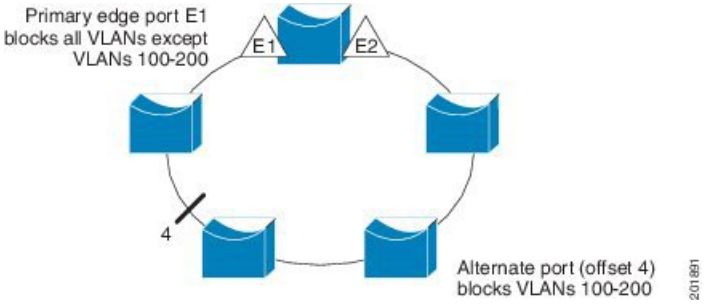
```
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# rep segment 1 edge primary
Device(config-if)# rep stcn segment 2-5
Device(config-if)# rep block port 0009001818D68700 vlan all`
Device(config-if)# rep preempt delay 60
Device(config-if)# rep lsl-age-timer 6000
Device(config-if)# end
```

次に、インターフェイスに外部 REP ネイバーがない場合の同じ設定の例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# rep segment 1 edge no-neighbor primary
Device(config-if)# rep stcn segment 2-5
Device(config-if)# rep block port 0009001818D68700 vlan all
Device(config-if)# rep preempt delay 60
Device(config-if)# rep lsl-age-timer 6000
Device(config-if)# end
```

次に、図 5 のように VLAN ブロッキング コンフィギュレーションを設定する例を示します。代替ポートは、ネイバー オフセット番号 4 のネイバーです。手動プリエンプションのあと、VLAN 100 ～ 200 はこのポートでブロックされ、その他すべての VLAN はプライマリ エッジ ポート E1（ギガビット イーサネット ポート 1/1）でブロックされます。

図 *29 : VLAN* ブロッキングの例



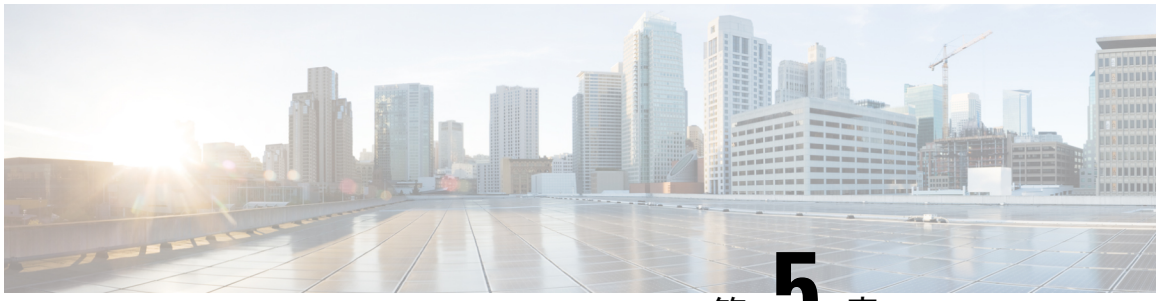

```
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# rep segment 1 edge primary
Device(config-if)# rep block port 4 vlan 100-200
Device(config-if)# end
```

Resilient Ethernet Protocol の機能情報

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

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

機能名	リリース	機能情報
Resilient Ethernet Protocol	Cisco IOS Release 15.2(7)E3k	この機能が導入されました。



第 5 章

EtherChannel の設定

EtherChannel の制約事項

- 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 のポートがトランク ポートとして設定されている場合、すべてのポートを同じモード（Inter-Switch Link（ISL）または IEEE 802.1Q）で設定する必要があります。

EtherChannel について

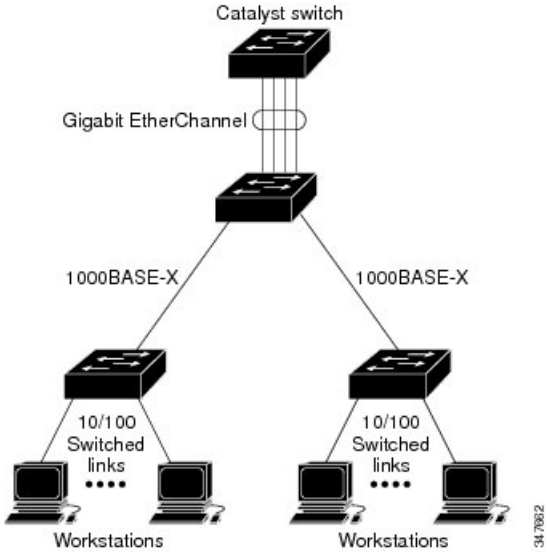
ここでは、EtherChannel について説明します。

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 *30* : 一般的な *EtherChannel* 構成



EtherChannel の最大数は 6 に制限されています。

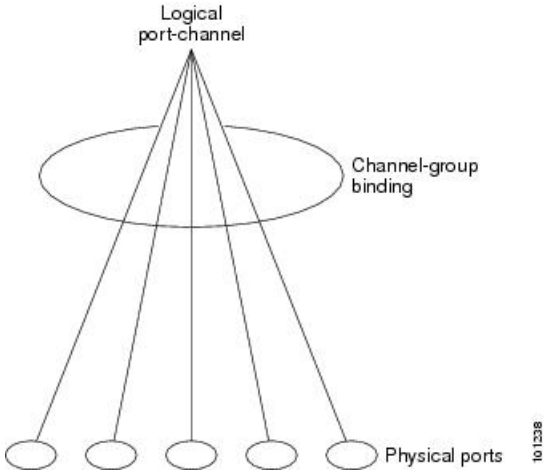
各 EtherChannel は、互換性のある設定のイーサネット ポートを 8 つまで使用して構成できます。

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 *31* : 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 ～ 6 番の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。

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 デバイスおよび 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デバイスでのみ稼働します。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。

スイッチは 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（単一のスイッチ上の）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。リンクをまとめて EtherChannel を形成した後で、PAgP は単一スイッチ 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。

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。

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。

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、スイッチ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、スイッチ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。

PAgP と仮想スイッチとの相互作用およびデュアルアクティブ検出

仮想スイッチは、仮想スイッチ リンク（VSL）により接続された複数のコア スイッチであり、それらのスイッチ間で制御情報とデータ トラフィックを伝送します。スイッチのうちの 1 つはアクティブ モードです。その他のスイッチはスタンバイ モードです。冗長性のため、リモート スイッチはリモート サテライト リンク（RSL）によって仮想スイッチに接続されます。

2 つのスイッチ間の VSL に障害が発生すると、一方のスイッチは他方のスイッチのステータスを認識しません。両方のスイッチがアクティブ モードになり、ネットワークを、重複したコンフィギュレーション（IP アドレスおよびブリッジ ID の重複を含む）を伴うデュアルアクティブの状態にする可能性があります。ネットワークがダウンする場合もあります。

デュアルアクティブの状態を防止するために、コア スイッチは PAgP プロトコル データ ユニット（PDU）を RSL を介してリモート スイッチに送信します。PAgP PDU はアクティブ スイッチを識別し、リモート スイッチは、コア スイッチが同期化するように PDU をコア スイッチに

転送します。アクティブ スイッチに障害が発生した場合、またはアクティブ スイッチがリセットされた場合は、スタンバイ スイッチがアクティブスイッチの役割を引き継ぎます。VSL がダウンした場合は、1つのコア スイッチが他のコア スイッチのステータスを認識し、その状態を変更しません。

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。

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）

LACP は IEEE 802.3ad で定義されており、シスコデバイスが IEEE 802.3ad プロトコルに適合したデバイス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。

スイッチは 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 は単一スイッチ 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。

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。

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、リンクの両端のデバイスが **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。

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 システムプライオリティおよびデバイス MAC アドレス

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。

- 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、同じデバイス上で共存できます。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。
- EtherChannel の一部としてセキュア ポートを設定したり、セキュア ポートの一部として EtherChannel を設定したりしないでください。
- アクティブまたはまだアクティブでない EtherChannel メンバとなっているポートを、IEEE802.1X 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。
- ダウンストリームの Etherchannel インターフェイスの一部となる個々のインスターフェイスでリンクステート トラッキングをイネーブルにしないでください。

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。

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	対応	なし	対応
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。

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

レイヤ2 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	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： `Device(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： `Device(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： `Device(config-if)# channel-group 5 mode auto`	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。 *channel-group-number* の範囲は 1 ～ 6 です。

	コマンドまたはアクション	目的
		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。 • **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。 • **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）デバイスが 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スイッチ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。 • **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

	コマンドまたはアクション	目的
		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： `Device(config-if)# 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface 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： `Device(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、デバイスがパケットを送信元に

	コマンドまたはアクション	目的
		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。 is物理ポートラーナーである別のデバイスに接続する**physical-port**を選択します。 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： `Device(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： `Device(config-if)# end`	特権 EXEC モードに戻ります。

LACP ホット スタンバイ ポートの設定

イネーブルの場合、LACP はチャネル内の LACP 互換ポート数を最大に設定しようとします（最大 16 ポート）。同時にアクティブになれる LACP リンクは 8 つだけです。リンクが追加されるとソフトウェアによってホット 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。

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（デバイス 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 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： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lacp system-priority** *priority* 例： `Device(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。

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

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： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	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。

	コマンドまたはアクション	目的
ステップ 4	**lacp port-priority** *priority* 例： `Device(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： `Device(config-if)# end`	特権 EXEC モードに戻ります。

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： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface port-channel** *channel-number* 例： `Device(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* に指定できる範囲は、1 ～ 6 です。

	コマンドまたはアクション	目的
ステップ 4	**port-channel min-links** *min-links-number* 例： `Device(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： `Device(config)# end`	特権 EXEC モードに戻ります。

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： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* 例： `Device(config)# interface gigabitethernet 2/0/1`	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。

	コマンドまたはアクション	目的
ステップ 4	**lacp rate** {**normal** | **fast**} 例： `Device(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： `Device(config)# end`	特権 EXEC モードに戻ります。

ステップ 6	**show lacp internal**
	例：
	`Device# show lacp internal`
	`Device# show lacp counters`
		設定を確認します。

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： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[**no**] **port-channel auto** 例： `Device(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。

	コマンドまたはアクション	目的
		（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： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show etherchannel auto** 例： `Device# 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： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	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： `Device(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。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show etherchannel auto** 例： `Device# show etherchannel auto`	EtherChannel が自動的に作成されたことが表示されます。

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： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**port-channel** *channel-number* **persistent** 例： `Device# 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： `Device# 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。

コマンド	説明
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。
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。

EtherChannel の設定例

ここでは、EtherChannel の設定例を示します。

レイヤ2 EtherChannel の設定：例

次の例では、単一のデバイス上で、EtherChannel を設定する方法を示します。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。

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

次の例では、単一のデバイス上で、EtherChannel を設定する方法を示します。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 :**

```
Device# configure terminal
Device(config)# interface range gigabitethernet 1/0/1 - 2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode active
Device(config-if-range)# end
```

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**

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)
```

LACP ポート チャネルの最小リンクの設定例

次の例は、LACP ポート チャネル最小リンク数の設定方法を示しています。

```
Device > enable
Device# configure terminal
Device(config)# interface port-channel 5
Device(config-if)# port-channel min-links 3
Device#  show etherchannel 25 summary
Device# end
```

スタンドアロン スイッチで最小リンク要件が満たされない場合、ポート チャネルにフラグが設定され SM/SN または RM/RN ステートが割り当てられます。

```
 Device# show etherchannel 5 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 N- not in use, no aggregration
f - failed to allocate aggregator
M - not in use, no aggregation due to minimum links not met
m- not in use, port not aggregated due to minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 6
Number of aggregators: 6

 Group   Port-channel   Protocol    Ports
------+-------------+-----------+-----------------------------------------------
 6       Po25(RM)        LACP        Gi1/3/1(D) Gi1/3/2(D) Gi2/2/25(D) Gi2/2/26(W)
```

例：LACP 高速レート タイマーの設定

次の例は LACP レートの設定方法を示しています。

```
Device> enable
Device# configure terminal
```

```
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# lacp rate fast
Device(config-if)# exit
Device(config)# end
Device# show lacp internal
Device# show lacp counters
```

次に、**show lacp internal** コマンドの出力例を示します。

```
Device# show lacp internal
Flags: S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs
A - Device is in Active mode P - Device is in Passive mode
Channel group 6
LACP port Admin Oper Port Port
Port Flags State Priority Key Key Number State
Te1/49 FA bndl 32768 0x19 0x19 0x32 0x3F
Te1/50 FA bndl 32768 0x19 0x19 0x33 0x3F
Te1/51 FA bndl 32768 0x19 0x19 0x34 0x3F
Te1/52 FA bndl 32768 0x19 0x19 0x35 0x3F
```

次に、**show lacp counters** コマンドの出力例を示します。

```
Device# show lacp counters

LACPDUs Marker Marker Response LACPDUs
Port Sent Recv Sent Recv Sent Recv Pkts Err
---------------------------------------------------------------------
Channel group: 6
Te1/1/27 2 2 0 0 0 0 0
Te2/1/25 2 2 0 0 0 0 0
```

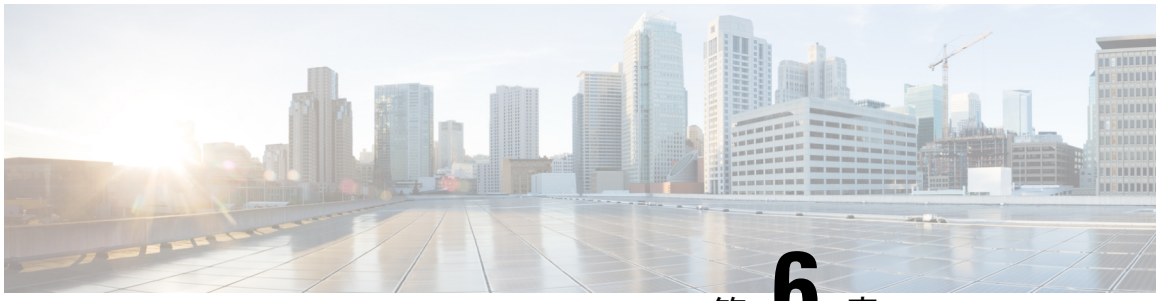
EtherChannels の機能情報

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

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

表 *16 : EtherChannels* の機能情報

機能名	リリース	機能情報
EtherChannel の設定	Cisco IOS Release 15.2(7)E3k	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

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 対応ポートが別のデバイスの 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。

⚠

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。

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。

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

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。

デバイスが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、デバイスが新しいhelloメッセージを受信すると、デバイス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、またはデバイス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。

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。

UDLD のデフォルト設定

表 *17 : 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

UDLD の設定方法

ここでは、UDLD の設定方法について説明します。

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、デバイス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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**udld** {**aggressive** | **enable** | **message time** *message-timer-interval*} 例： `Device(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**：デバイス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。

	コマンドまたはアクション	目的
		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： `Device(config)# end`	特権 EXEC モードに戻ります。

インターフェイス上での 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Device(config)# interface 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： `Device(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： `Device(config-if)# end`	特権 EXEC モードに戻ります。

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 の設定に関する機能情報

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

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

表 *18 : UDLD* の設定に関する機能情報

機能名	リリース	機能情報
UDLD の設定	Cisco IOS Release 15.2(7)E3k	この機能が導入されました。