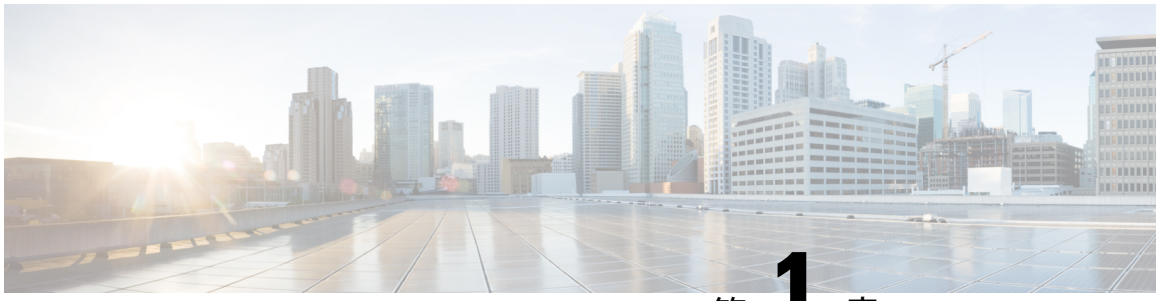
Cisco IOS XE 17（Cisco ASR 920 シリーズ）LANスイッチング コンフィギュレーションガイド

初版：2023 年 9 月 20 日

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

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

Resilient Ethernet Protocol の設定

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）の代替となります。REPはネットワーク 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、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。

（注） コンバージェンス値は、Cisco IOS XE 3.17 リリース以降で改善されています。

Resilient Ethernet Protocol の制約事項

- 制御フレームに関しては、REP ALT ポートはタグ付き（トランク EFP の一部）の制御フレームのみをブロックし、タグなし（タグなしEFPの一部）の制御フレームはブロックしません。
- 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の高損失が発生します。
- 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、ネットワーク接続が失われます。

- IGMP スヌーピングでの REP フラップを回避するには、280 ミリ秒を超える LSL タイマーを使用します。
- REP フラップを回避するには、520 ミリ秒の LSL タイマーを使用します。
- REP フラップを回避するために、レイヤ 3 パケットがホスト Q にパントされるレートを 1000 パケット/秒未満にする必要があります。ホスト Q のクレジット制限は 1000 パケット/秒です。
- STP キュー内の REP LSL パケットがドロップすることはありません。
- REP は、インターフェイスに設定されたトランク EFP でのみサポートされます。
- REP 対応ポートは EFP 設定をサポートしません。
- 推奨される最小 REP LSL タイマー値は 200 ミリ秒です。
- REP ポートは、以下のような状況でトポロジリストから削除されます。REP 設定の動的変更を導入するために、上記の動作に基づいてトラフィックループを回避するように設計されています。
  - 古いポートが削除された後に新しいポートが追加された場合。
  - 両方の REP ポートが削除された場合。
  - ポートが、エッジまたはエッジネイバーなしポートの場合。

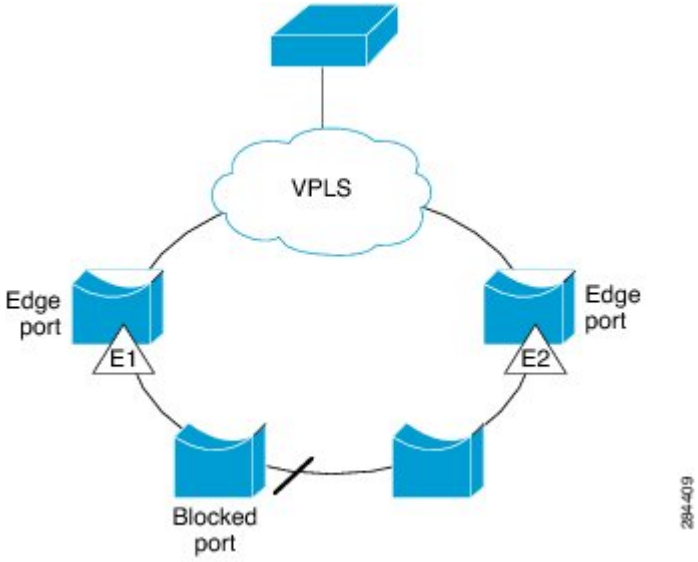
REP に関する情報

REP セグメント

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 ルータは同じセグメントに属するポートを複数持たず、各セグメント ポートにある外部ネイバーは 1 つだけです。セグメントは共有メディアを経由できますが、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。

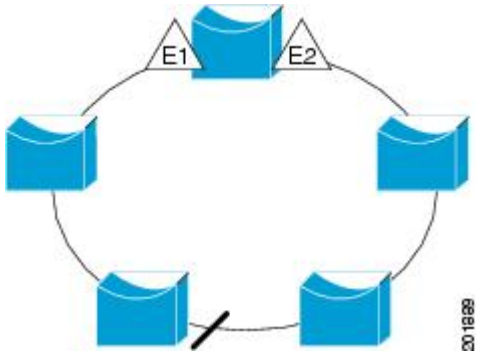
図 *1 : REP* オープン セグメント



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

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

図 *2 : REP* リング セグメント



REP セグメントには、次のような特徴があります。

- セグメント内の全ポートが動作可能な場合、1ポート（代替ポートと呼ばれる）が各VLANでブロック ステートとなります。VLAN ロード バランシングが設定されている場合は、セグメント内の 2 つのポートが VLAN のブロック ステートを制御します。

- セグメント内の1つまたは複数のポートが動作不能になると、リンク障害が発生して、すべてのポートがすべての VLAN トラフィックを転送して、接続性を確保します。
- リンク障害の場合、できるだけ早期に代替ポートのブロックが解除されます。障害リンクが復旧すると、ネットワークの中断を最小限に抑えるようにVLAN単位で論理的にブロックされたポートが選択されます。

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

リンク完全性

REP は、リンク完全性を確認するためにエッジ ポート間でエンドツーエンド ポーリング メカニズムを使用していません。ローカル リンク障害検出を実装しています。インターフェイスがイネーブルの場合、REP リンク ステータス レイヤ（LSL）が REP 認識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。REP LSL がネイバーを検出するまで、すべての VLAN がインターフェイスでブロックされます。ネイバーが特定されたあと、REPが代替ポートとなるネイバー ポートと、トラフィックを転送するポートを決定します。

セグメント内のポートごとに、一意のポート ID が割り当てられます。ポート ID フォーマットは、スパニングツリーアルゴリズムで使用されるものと類似しており、ポート番号（ブリッジ上で一意）と、関連 MAC アドレス（ネットワーク内で一意）から構成されます。セグメント ポートが起動すると、LSL がセグメント ID とポート ID を含むパケットを送信します。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。セグメント ポートは、次のような状態では動作可能になりません。

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

各ポートは、直近のネイバーと隣接関係を確立します。ネイバー関係が確立されると、ポートがセグメントの1つのブロックされたポート（代替ポート）を決定するようにネゴシエートします。その他のポートのブロックは解除されます。デフォルトでは、REP パケットは PortFast ブリッジ プロトコル データ ユニット（BPDU）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、現時点でセグメントに障害が発生した場合に Blocked Port Advertisement（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 が物理リンク ベースで動作し、VLAN 単位ベースで動作しないため、全 VLAN で必要なのは 1 つの hello メッセージだけなので、プロトコルの負荷が低減します。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 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。このセグメントに属さないスイッチは、メッセージをデータ トラフィックとして処理します。ドメイン全体で専用の管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

予想されるコンバージェンス復旧時間はローカル セグメントで 200 ms 未満です。

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 ロード 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場合、次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のポート ID を識別するには、そのポートについて **show interface rep detail** コマンドを入力します。
- セグメント内のポートのネイバー オフセット番号を入力します。これは、エッジ ポートのダウンストリーム ネイバー ポートを識別するものです。ネイバー オフセット番号の範囲は、-256 ～ +256 で、0 値は無効です。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負数は、セカンダリ エッジ ポート（オフセット番号 -1）とそのダウンストリーム ネイバーを示します。

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

- **preferred** キーワードを入力します。これにより、**rep segment preferred** 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。

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 バランシングは、次の 2 通りの方法のいずれかでトリガーできます。

- プライマリエッジポートのあるルータ上で **rep preempt segment** *segment-id* 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* コマンドを入力すると、プリエンプト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ます。

（注） 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、VLAN ロード バランシングは開始されません。

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 エッジ ポートで受信されると、ネットワークでメッセージが生成され、メッセージ内で特定された 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 ポートによってしか VLAN ロードバランシングは開始されず、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。

VLAN 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 ポートを再設定する必要があります。VLANロードバランシング設定を変更すると、プライマリエッジポートでは、再び **rep preempt segment** コマンドが実行されるか、ポート障害および復旧の後で設定済みプリエンプト遅延期間が経過してから、新しいVLANロードバランシング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 プロトコルの対話

REP は STP または Flex Link と対話しませんが、両方と共存できます。セグメントに属しているポートはスパニングツリーの制御から削除されるため、セグメント ポートでは STP BPDU の送受信は行われません。したがって、STP はセグメント上で実行できません。

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

REP ポート

REP セグメント内のポートは、3 つの役割またはステート（障害、オープン、または代替）のいずれかになります。

- 標準セグメント ポートとして設定されたポートは、障害ポートとして起動します。
- ネイバーとの隣接関係が確立されると、ポートは代替ポート ステートに移行して、インターフェイス内の全 VLAN をブロックします。ブロックされたポートのネゴシエーショ

ンが発生し、セグメントが安定すると、ブロックされたポートの1つは代替ロールのままになり、他のすべてのポートがオープン ポートとなります。

- リンク内に障害が発生すると、すべてのポートが障害ステートに移行します。代替ポートが障害通知を受信すると、ポートはすべての VLAN を転送するオープン ステートに変更されます。

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、このポートは指定ブロッキング ポートです。PortFast BPDU ガード拡張機能が設定されている場合、または STP がディセーブルになっている場合、ポートはフォワーディング ステートになります。

VPLS との REP 統合

一般に、Virtual Private LAN Service（VPLS）のネットワーク コアでは、すべてのノードが完全メッシュ トポロジで接続され、各ノードは他のすべてのノードと接続されています。完全メッシュ トポロジでは、ノードが他のノードにデータを再送信する必要はありません。図3では、共通リングによって、パケットを他のネットワーク プロバイダー エッジ（N-PE）ルータに転送できるパスが提供され、スプリット ホライズン モデルを無効にします。

REP は共通リンク接続をエミュレーションし、REP リングは VPLS のフルメッシュモデルをサポートしますが、スプリットホライズンのプロパティを維持するため、スーパーループは存在しません。エミュレーションされた共通リンクは Clustering over the WAN（CWAN）ラインカードを使用します。これは VPLS アップリンクにも使用されます。このエミュレーションされた共通リンクは、リングから VPLS アップリンクまたはリングの反対側にデータを転送し、VPLS コア ネットワークから着信するデータをブロックして、Hierarchical-VPLS（H-VPLS）トポロジのアクセス疑似ワイヤを処理します。

REP のデフォルト設定

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

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

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

REP セグメントと REP 管理 VLAN

セグメントは、チェーンで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 モードでセグメントにポートを追加します。2 つのエッジ ポートをセグメント内に設定して、1 つをプライマリ エッジ ポート、もう 1 つをデフォルトでセカンダリ エッジ ポートにします。1 セグメント内のプライマリ エッジ ポートは 1 つだけです。たとえば、異なるスイッチのポートで、プライマリ エッジ ポートとしてセグメントで 2 つのポートを設定すると、REP はそのいずれかをプライマリ エッジ ポートとして選択します。オプションで、セグメント STCN および VLAN ロード バランシングを送信する場所を設定することもできます。REP 管理 VLAN の設定方法の詳細については、「*REP* 管理 *VLAN* の設定」のセクションを参照してください。

REP 設定時の注意事項

REP の設定時には、次の注意事項に従ってください。

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

- 1 つのルータ上で 1 つのポートだけがセグメントで設定される場合、このポートは 1 つのエッジ ポートである必要があります。
- 1 つのルータ上で 2 つのポートが同じセグメントに属する場合、両方のポートはエッジ ポートであるか、通常のセグメント ポートである必要があります。
- 1 つのルータ上で 2 つのポートが同じセグメントに属し、1 つがエッジ ポートとして設定され、もう1つが通常のセグメントポートとして設定された場合（設定ミス）、エッジ ポートは通常のセグメント ポートとして処理されます。

- REPインターフェイスはブロックされた状態になり、ブロック解除できるようになるまでブロックされた状態のまま残ります。突然の接続切断を避けるために、このステータスを認識しておく必要があります。
- REP 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
- ルータごとに最大 22 の REP セグメントを設定できます。

トランク EFP の REP サポート

Resilient Ethernet Protocol（REP）は、Cisco ASR 920 シリーズ ルータのインターフェイスレベルのトランクEFPポートで設定できます。トランクEFPポートでは、複数のブリッジドVLANサービスを実行することができます。トランク EFP は 1000 回線の VLAN のみサポートします。VLAN は、トランク EFP ポートでブロックまたはフォワーディング ステートに設定できます。ユーザは、ポートで REP をイネーブルにする必要があります。デフォルトでは、REP はすべてのポートでディセーブルです。

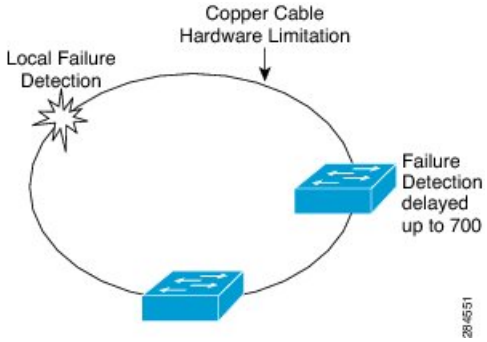
REP 設定可能タイマー

リング ネットワーク トポロジでは、Fast Last Link Status（LSL）プロセスがネイバー ポートを検出し、そのポートとの接続を維持します。ポートのタイマーは、200 ～ 10000 ミリ秒の範囲で LSL フレームを受信するように設定できます。LSL フレームがネイバー ポートから 200 ～ 10000ミリ秒の範囲で受信されない場合、ルータ間のリンクはダウンしていると見なされます。リンクを起動しトラフィックを復元するために、切断操作とアクションが実行されます。

リングネットワークトポロジでは、REP が 50 ミリ秒以内でトラフィックを収束できない場合があります。たとえば、トポロジが銅ケーブルの場合、銅インターフェイスのハードウェア制限により、REP はトラフィックの収束に失敗する可能性があります。このようなシナリオでは、リモート エンドがローカル ポートのシャットダウン障害を検出するために最大で 700 ミリ秒かかる場合があります。REP LSL は、リモート側で高いタイマー粒度と速い障害検出を達成できるように強化されました。

次の図は、銅線インターフェイスのハードウェア制限による障害検出の遅延を示しています。

図 *3*: 障害検出の遅延



REP Fast Hello での SSO サポート

ルータがクラッシュした場合、ルータがアクティブモードになり、REP Fast Hello パケットの送信を開始するまでに 3 ～ 5 秒かかります。**lsl age out timer** コマンドで設定されたエージングアウトタイマーの値が 3 秒より短い場合、リモートエンドはポート障害を検出し、再コンバージェンスします。再コンバージェンス後に、ルータは特殊なタイプ、長さ、および値（TLV）を持つ BPDU を接続ポートに送信します。ルータは、次の REP スリーウェイ リンク完全性チェックに失敗しないように、ポートのローカルおよびリモートのシーケンス番号を学習します。REP のステートフルスイッチオーバー（SSO）のサポートは、LSL インターバルの期限が切れる前に、Fast Hello パケットがルータから送信できるようにします。

REP 非ネイバー エッジ サポート

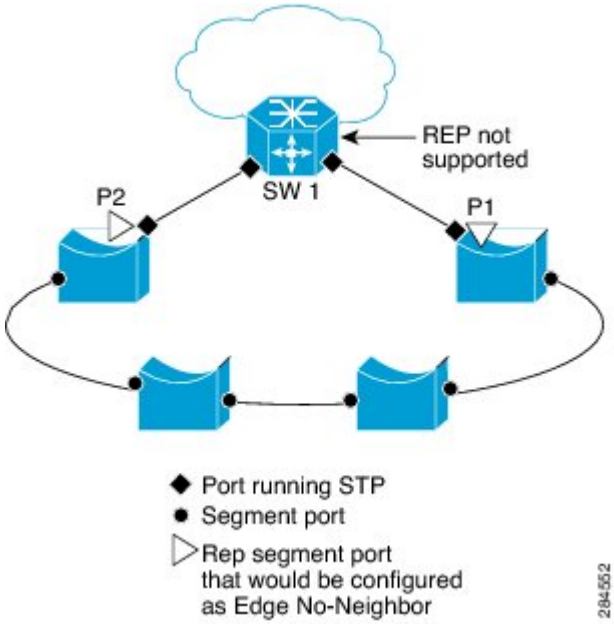
リング ネットワーク トポロジでは、集約ノードで REP がサポートされません。REP セグメントは、スイッチの収束を達成するために、ネイバーのないポートで作成できます。次の図は、リング トポロジの非ネイバー エッジ ポートとしての P1 および P2 を示します。この設定で P1 および P2 はトラフィックをブロックすることがあります。リンクのいずれかに障害が発生した場合、REP 設定のすべてのスイッチが収束します。P1 および P2 はエッジではないため、次のタスクをサポートしていません。

- VLAN ロード バランシングを実行します。
- 他のセグメントおよびスパニングツリープロトコル（STP）へのトポロジ変更を検出します。
- プリエンプション処理できるポートを選択します。
- 完全なセグメント トポロジを表示します。

非ネイバー エッジ サポートは、内部ネイバーがある新しいタイプのエッジを定義できるようにします。次の図では、P1 および P2 は中間セグメント ポートではなく、非ネイバー エッジ ポートとして設定されます。これらのポートはエッジポートのプロパティを継承し、上に示されている制約を克服します。したがって、非ネイバーエッジ ポート（P1 または P2）はマルチ

スパニングツリー（MST）プロトコル、Topology Change Notification（TCN）、および別のセグメントの REP TCN を集約スイッチに送信できます。

図 *4 :* 非ネイバー エッジ ポートがあるリング トポロジ



REP の設定方法

REP 管理 VLAN の設定

VLAN ロード バランシング中のリンク障害または VLAN ブロッキング通知関連のメッセージ リレーで遅延が起こらないようにするには、REP は通常のマルチキャスト アドレスにハードウェア フラッド レイヤ（HFL）でパケットを大量に送信します。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。ドメイン全体の管理 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。

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。

- ルータとセグメント上には管理 VLAN は 1 つだけとなります。ただし、これはソフトウェアによって強制的に設定されません。
- 管理 VLAN を設定しない場合、デフォルトは VLAN 1 です。
- インターフェイスで REP を設定するには、REP 管理 VLAN がトランクの EFP カプセル化のリストに含まれていることを確認します。

手順の概要

1. **enable**

2. **configure terminal**
3. **rep admin vlan** *vlan-id*
4. **end**
5. **show interface** [*interface-id*] **rep** [**detail**]
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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	**rep admin vlan** *vlan-id* 例： `Router(config)# rep admin vlan 2`	REP 管理 VLAN を設定します。 • 管理 VLAN を指定します。範囲は 2 ～ 4094 です。デフォルトは VLAN 1 です。
ステップ 4	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show interface** [*interface-id*] **rep** [**detail**] 例： `Router# show interface gigabitethernet0/1 rep detail`	指定したインターフェイスの REP 設定およびステータスを表示します。 • 物理インターフェイスまたはポート チャネル ID を入力します。
ステップ 6	**copy running-config startup-config** 例： `Router# copy running-config startup-config`	（任意）ルータ 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。

インターフェイスのトランク EFP の設定

始める前に

REP 操作の場合、インターフェイスのトランク EFP を設定する必要があります。このタスクは必須で、トランク EFP の REP サポートを設定する前に行う必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance trunk** *service-instance-id* **ethernet**
5. **encapsulation dot1q vlan** *range*
6. **rewrite ingress tag pop 1 symmetric**
7. **bridge-domain from-encapsulation**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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** *type number* 例： `Router(config)# interface GigabitEthernet 0/0/1`	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 ID を入力します。
ステップ 4	**service instance trunk** *service-instance-id* **ethernet** 例： `Router(config-if)# service instance trunk 1 ethernet`	インターフェイス上でサービスインスタンスを設定し、サービス インスタンス コンフィギュレーション モードを開始します。
ステップ 5	**encapsulation dot1q vlan** *range* 例： `Router(config-if-srv)# encapsulation dot1q vlan 10`	インターフェイス上の dot1q フレーム入力を、適切なサービスインスタンスにマッピングするために使用する照合基準を定義します。 • VLAN-ID の範囲は 1 ～ 20 です。
ステップ 6	**rewrite ingress tag pop 1 symmetric** 例： `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	サービスインスタンスへのフレーム入力で実行されるカプセル化調整を指定します。
ステップ 7	**bridge-domain from-encapsulation** 例： `Router(config-if-srv)# bridge-domain from-encapsulation`	カプセル化からブリッジ ドメインを取得します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Router (config-if-srv)end`	特権 EXEC モードに戻ります。

トランク EFP の REP サポートの設定

始める前に

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

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface type number*
4. **rep segment** *segment-id* [**edge** [**primary**]] [**preferred**]
5. **rep stcn** {**interface** *type number* | **segment** *id-list* | **stp**}
6. **rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}
7. **rep preempt delay** *seconds*
8. **end**
9. **show interface** *type number* **rep** [**detail**]
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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 type number* 例： `Router(config)# interface GigabitEthernet 0/0/1`	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。 • インターフェイスタイプと番号を入力します。

	コマンドまたはアクション	目的
ステップ 4	**rep segment** *segment-id* [**edge** [**primary**]] [**preferred**] 例： `Router(config-if)# rep segment 3 edge preferred`	インターフェイス上で REP をイネーブルにして、セグメント番号を特定します。 • 指定できるセグメント ID の範囲は 1 ～ 1024 です。 （注） 各セグメントに 1 つのプライマリ エッジ ポートを含めて、2 つのエッジ ポートを設定する必要があります。 • （任意）**edge**：エッジ ポートとしてポートを設定します。各セグメントにあるエッジ ポートは 2 つだけです。**primary** キーワードなしで **edge** を入力すると、ポートがセカンダリエッジポートとして設定されます。 • （任意）**primary**：プライマリエッジポート（VLAN ロードバランシングを設定できるポート）としてポートを設定します。 （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。
ステップ 5	**rep stcn** {**interface** *type number* | **segment** *id-list* | **stp**} 例：	（任意）エッジ ポートを STCN を送信するように設定します。

	コマンドまたはアクション	目的
	`Router(config-if)# rep stcn segment 2-5`	• **interface** *type number* キーワードと引数のペアを使用して、STCN を受信するための物理インターフェイスまたはポートチャネルを指定します。 • **segment** *id-list* キーワードと引数のペアを使用して、STCN を受信する 1 つまたは複数のセグメントを指定します。有効な範囲は 1 ～ 1024 です。 • **stp** を入力して、STCN を STP ネットワークに送信します。
ステップ 6	**rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**} 例： `Router(config-if)# rep block port 0009001818D68700 vlan all`	（任意）プライマリ エッジ ポートに VLAN ロードバランシングを設定して、3 つの方法のいずれかを使用して REP 代替ポートを特定し、代替ポートでブロックされるように VLAN を設定します。 • **id** *port-id* キーワードペアを入力して、ポート ID で代替ポートを指定します。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**] コマンドを入力すれば、インターフェイス ポート ID を表示できます。 • *neighbor-offset* 番号を入力して、代替ポートをエッジポートからのダウンストリーム ネイバーとして指定します。有効範囲は -256 ～ 256 で、負数はセカンダリ エッジ ポートからのダウンストリーム ネイバーを示します。**0** の値が無効です。**-1** を入力して、セカンダリエッジポートを代替ポートとして識別します。 （注） プライマリエッジポート（オフセット番号 1）にこのコマンドを入力するので、代替ポートを特定するのにオフセット値 1 を入力できません。 • **preferred** キーワードを入力して、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* キーワードと引数のペアを入力して、1 つの VLAN または VLAN の範囲をブロックします。

	コマンドまたはアクション	目的
		• すべての VLAN をブロックするには、**vlan all** キーワードを入力します。 • 必要な一連の VLAN に設定するために、このコマンドを複数回実行します。既存のリストを置き換えるのではなく、既存のリストにVLANを追加します。 （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 7	**rep preempt delay** *seconds* 例： `Router(config-if)# rep preempt delay 60`	（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使用します。
ステップ 8	**end** 例： `Router(config-if-srv)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show interface** *type number* **rep** [**detail**] 例： `Router# show interface Gigabitethernet0/0/1 rep detail`	（任意）REP インターフェイス コンフィギュレーションを確認します。 • 必要に応じて、インターフェイス タイプおよび番号と、任意で**detail** キーワードを入力します。
ステップ 10	**copy running-config startup-config** 例： `Router# 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 バランシングのプリエンプションの設定

VLAN ロード バランシングのプリエンプションを設定するには、プライマリ エッジ ポートを含むセグメントのあるルータ上で、以下の手順を完了します。

機能制限

プライマリエッジポートでプリエンプション遅延時間を設定する **rep preempt delay** *seconds* コマンドを入力しない場合、デフォルトでは、セグメントでの VLAN ロードバランシングのトリガーは手動になっています。**show rep topology** コマンドを使用して、セグメント内のどのポートがプライマリエッジポートであるかを確認します。

始める前に

VLAN ロード バランシングのプリエンプションを設定する前に、他のすべてのセグメント設定が完了していることを確認してください。VLAN ロードバランシングのプリエンプションはネットワークを中断する可能性があるため、**rep preempt segment** *segment-id* コマンドを入力すると、このコマンドの実行前に確認メッセージが表示されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **rep preempt segment** *segment-id*
4. **end**
5. **show rep topology**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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	**rep preempt segment** *segment-id* 例： `Router(config)# rep preempt segment 1`	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。 • セグメント ID を入力します。 （注） コマンドの実行前に、処理の確認を求められます。
ステップ 4	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show rep topology** 例： `Router# show rep topology`	REP トポロジ情報を表示します。

REP の SNMP トラップ設定

REP 固有のトラップを送信して、簡易ネットワーク管理プロトコル（SNMP）サーバー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。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp mib rep trap-rate** *value*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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	**snmp mib rep trap-rate** *value* 例： `Router(config)# snmp mib rep trap-rate 500`	ルータで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。 （注） トラップを削除するには、**no snmp mib rep trap-rate** コマンドを入力します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Router# 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 6	**copy running-config startup-config** 例： `Router# 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 設定のモニタリング

手順の概要

1. **enable**
2. **show interface** [*interface-id*] **rep** [**detail**]
3. **show rep topology** [**segment** *segment-id*] [**archive**] [**detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**show interface** [*interface-id*] **rep** [**detail**] 例： `Router# show interface gigabitethernet0/1 rep detail`	（任意）指定したインターフェイスのREP設定およびステータスを表示します。 • 必要に応じて、物理インターフェイスまたはポートチャネルIDと、オプションの**detail**キーワードを入力します。
ステップ 3	**show rep topology** [**segment** *segment-id*] [**archive**] [**detail**] 例： `Router# show rep topology`	（任意）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つの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。 • 必要に応じてオプションのキーワードと引数を入力します。

REP 設定可能タイマーの設定

始める前に

REP 操作では、各セグメント インターフェイスで REP をイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]
5. **rep stcn** {**interface** *type number* | **segment** *id-list* | **stp**}
6. **rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}
7. **rep lsl-retries** *number-of-tries*
8. **rep lsl-age-timer** *timer-value*
9. **rep preempt delay** *seconds*
10. **end**
11. **show interface** *type number* **rep** [**detail**]
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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** *type number* 例： `Router(config)# interface Gigabitethernet 0/0/1`	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 タイプと番号を入力します。
ステップ 4	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**] 例： `Router(config-if)# rep segment 1 edge preferred`	インターフェイス上で REP をイネーブルにして、セグメント番号を特定します。 • 指定できるセグメント ID の範囲は 1 ～ 1024 です。 （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。

	コマンドまたはアクション	目的
		• （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）**no-neighbor**：ポートの外部 REP ネイバーを持たないものとしてセグメントエッジを設定します。 • （任意）**primary**：プライマリエッジポート（VLAN ロードバランシングを設定できるポート）としてポートを設定します。 （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。
ステップ 5	**rep stcn** {**interface** *type number* | **segment** *id-list* | **stp**} 例： `Router(config-if)# rep stcn segment 2-5`	（任意）エッジ ポートを STCN を送信するように設定します。 • **interface** *type number* キーワードと引数のペアを使用して、STCN を受信するための物理インターフェイスまたはポートチャネルを指定します。 • **segment** *id-list* キーワードと引数のペアを使用して、STCN を受信する 1 つまたは複数のセグ

	コマンドまたはアクション	目的
		メントを指定します。有効な範囲は 1 ～ 1024 です。 • STCN を STP ネットワークに送信するために、**stp** キーワードを入力します。
ステップ 6	**rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**} 例： `Router(config-if)# rep block port 0009001818D68700 vlan all`	（任意）プライマリ エッジ ポートに VLAN ロードバランシングを設定して、3 つの方法のいずれかを使用して REP 代替ポートを特定し、代替ポートでブロックされるように VLAN を設定します。 • **id** *port-id* キーワードと引数のペアを入力して、ポート ID で代替ポートを指定します。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**] コマンドを入力すれば、インターフェイスポート ID を表示できます。 • *neighbor-offset* 番号を入力して、代替ポートをエッジポートからのダウンストリームネイバーとして指定します。有効範囲は -256 ～ 256 で、負数はセカンダリ エッジ ポートからのダウンストリーム ネイバーを示します。**0** の値が無効です。**-1** を入力して、セカンダリエッジポートを代替ポートとして識別します。 （注） プライマリエッジポート（オフセット番号 1）にこのコマンドを入力するので、代替ポートを特定するのにオフセット値 1 を入力できません。 • **preferred** キーワードを入力して、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* キーワードと引数のペアを入力して、1 つの VLAN または VLAN の範囲をブロックします。 • すべての VLAN をブロックするには、**vlan all** キーワードを入力します。 • 必要な一連の VLAN に設定するために、このコマンドを複数回実行します。既存のリストを

	コマンドまたはアクション	目的
		置き換えるのではなく、既存のリストにVLANを追加します。 （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 7	**rep lsl-retries** *number-of-tries* 例： `Router(config-if)# rep lsl-retries 3`	LSL によって許容されるリトライ回数を設定します。
ステップ 8	**rep lsl-age-timer** *timer-value* 例： `Router(config-if)# rep lsl-age-timer 200`	障害検出時間を設定します。 • 有効値は120～10000です。パフォーマンスを考慮して、最小範囲を200に設定することを推奨します。値を小さくするとパフォーマンスが向上しますが、このコマンドの変更は慎重に考える必要があります。値をむやみに下げると、システムが不安定になる可能性があります。
ステップ 9	**rep preempt delay** *seconds* 例： `Router(config-if)# rep preempt delay 60`	• （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使用します。
ステップ 10	**end** 例： `Router(config-if-srv)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show interface** *type number* **rep** [**detail**] 例： `Router# show interface Gigabitethernet0/0/1 rep detail`	（任意）REP インターフェイスの設定を表示します。 • 必要に応じて、インターフェイス タイプおよび番号と、任意で**detail**キーワードを入力します。

	コマンドまたはアクション	目的
ステップ 12	**copy running-config startup-config** 例： `Router# 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。

非ネイバー エッジ ポートとしての REP の設定

始める前に

REP 操作では、各セグメント インターフェイスで REP をイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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** *type number* 例： `Router(config)# interface GigabitEthernet 0/0/1`	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 タイプと番号を入力します。
ステップ 4	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**] 例： `Router(config-if)# rep segment 1 edge no-neighbor preferred`	インターフェイス上で REP をイネーブルにして、セグメント番号を特定します。 • 指定できるセグメント ID の範囲は 1 ～ 1024 です。 （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。

	コマンドまたはアクション	目的
		• （任意）**edge**：エッジポートとしてポートを設定します。各セグメントにあるエッジポートは 2 つだけです。**primary** キーワードなしで **edge** を入力すると、ポートがセカンダリエッジポートとして設定されます。 • （任意）**no-neighbor**：ポートの外部 REP ネイバーを持たないものとして、セグメントエッジを指定します。 • （任意）**primary**：プライマリエッジポート（VLAN ロードバランシングを設定できるポート）としてポートを設定します。 （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またはVLANロードバランシングの優先ポートであることを指定します。 （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。

例

REP の設定例

REP 管理 VLAN の設定

次に、管理 VLAN を VLAN 100 として設定する例を示します。

```
Router# configure terminal
Router(config)# rep admin vlan 100
Router(config-if)# end
```

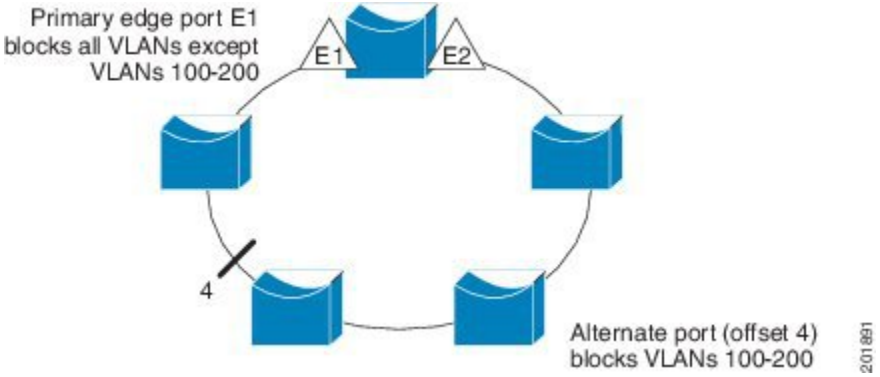
トランク EFP の REP サポートの設定

次に、トランク EFP の REP サポートを設定する例を示します。セグメント 1 のプライマリ エッジ ポートがセグメント 5 を通じて STCN をセグメント 2 に送信するようにインターフェイスを設定し、ポート ID が 0009001818D68700 のポートがセグメント ポート障害とリカバリの後に 60 秒のプリエンプション遅延後、すべての VLAN をブロックするように代替ポートを設定します。

```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/1
Router(config-if)# rep segment 1 edge primary
Router(config-if)# rep stcn segment 2-5
Router(config-if)# rep block port id 0009001818D68700 vlan all
Router(config-if)# rep preempt delay 60
Router(config-if)# service instance trunk 1 ethernet
Router(config-if-srv)# encapsulation dot1q
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain from-encapsulation
Router(config-if-srv)# end
```

次の図に示すようにVLANブロッキングを設定する方法を示します。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。手動によるプリエンプションのあとに、VLAN 100 ～ 200 がこのポートでブロックされ、その他のすべての VLAN がプライマリ エッジ ポート E1（ギガビット イーサネット ポート 0/0/1）でブロックされます。

図 *5 : VLAN* ブロッキングの例




```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/1
Router(config-if)# rep segment 1 edge primary
Router(config-if)# rep block port 4 vlan 100-200
Router(config-if)# end
```

VLAN ロード バランシングのプリエンプションの設定

```
Router>end
Router# configure terminal
Router(config)rep preempt segment 1
Router(config)# end
```

REP の SNMP トラップ設定

次の例は、1 秒あたり 10 トラップの割合で REP トラップを送信するようにルータを設定する方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# snmp mib rep trap-rate 10
Router(config)# end
```

REP 設定のモニタリング

次に、**show interface rep detail** コマンドの出力例を示します。REP インターフェイスの 1 つで **show interface rep detail** コマンドを使用して、REP 設定をモニターして検証します。

```
Router# show interface GigabitEthernet 0/0/1 rep detail

GigabitEthernet0/1 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
Load-balancing block port: none
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
```

REP 設定可能タイマーの設定

```
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/4
Router(config-if)# rep segment 4 edge preferred
Router(config-if)# rep stcn segment 2-5
Router(config-if)# rep block port 0009001818D68700 vlan all
Router(config-if)# rep lsl-retries 3
Router(config-if)# rep lsl-age-timer 200
Router(config-if)# rep preempt delay 300
Router(config-if)# exit
Router# show interface GigabitEthernet 0/0/1 rep detail
Router# copy running-config startup-config
```

REP 非ネイバー エッジ サポートの設定

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet0/2
Router(config-if)# rep segment t1 edge no-neighbor primary
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
LAN スイッチング コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用上のガイドライン、および例	『Cisco IOS LAN Switching Command Reference』
スパニングツリー プロトコルの概要	『Spanning Tree Protocol (STP)/802.1D』

関連項目	マニュアル タイトル
スパニングツリー PortFast BPDU ガード拡張機能	『Spanning Tree PortFast BPDU Guard Enhancement』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

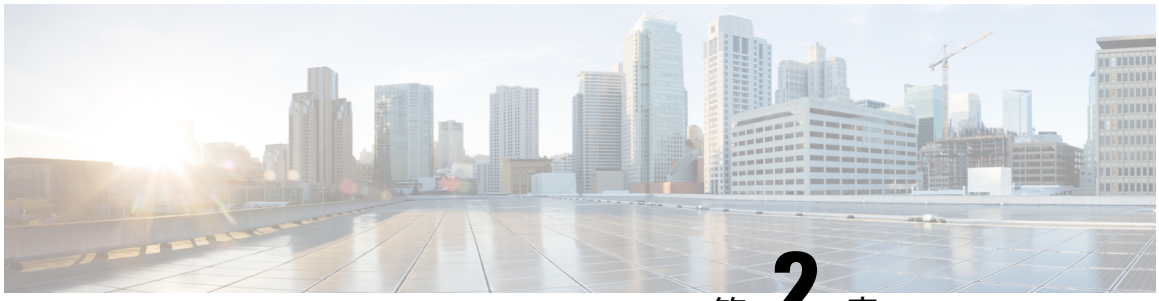
Resilient Ethernet Protocol の機能情報

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。

表 *1 : Resilient Ethernet Protocol* の機能情報

機能名	リリース	機能情報
Resilient Ethernet Protocol	Cisco IOS XE Release 3.13.0S	この機能は、Cisco ASR 920 シリーズ アグリゲーション サービス ルータ（ASR-920-12CZ-A、ASR-920-12CZ-D、ASR-920-4SZ-A、ASR-920-4SZ-D）に導入されました。



第 2 章

REP アクセスゲートウェイ

Resilient Ethernet Protocol（REP）は、高速障害検出と回復を提供するように設計されたリング保護プロトコルです。REP Edge ネイバーなし（RENN）ポートは、REP セグメントのエッジにあるポートであり、REP をサポートしないピア デバイスに接続されます。この機能を使用すると、エラーが検出されたときに CFM が REP に通知できます。これにより、CFM を使用して Edge リンクのステータスをモニターし、REP がアクションを実行できます。

この機能では、REP の通信により、REP アクセスゲートウェイ（REP-AG）が設定された Cisco ASR 900 シリーズ ルータおよび Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ間でのイーサネット障害検出（EFD）通知が有効になります。

REP アクセスゲートウェイの前提条件

- 非 REP デバイスポートに接続されたインターフェイスは、REP エッジ NN ポートとして設定する必要があります。
- CCM 通知は、REP エッジ NN ポートでのみ処理されます。
- ポート MEP は REP AG でのみサポートされます。ポート MEP は単一のホップを保護するように設定され、CFM を通してリンク ステートを監視するために使用されます。『Configuring Ethernet Connectivity Fault Management in a Service Provider Network』を参照してください。
- EFD はダウン MEP でサポートされます。ダウン MEP は、MEP が設定されているポートに接続された回線を経由して、CFM フレームを送受信します。『Configuring Ethernet Connectivity Fault Management in a Service Provider Network』を参照してください。

REP アクセスゲートウェイの制約事項

- REP AG は、ポート MEP でのみサポートされます。
- REP デバイスと非 REP デバイスの間でリンクダウンが確認された場合、コンバージェンス時間は銅線接続の方が長くなります。
- EFD は、ポート MEP および EFP MEP でサポートされます。
- EFD がサポートされている MA の CCM 間隔には制限があります。
- EFD はトランク EFP ではサポートされません。
- EFD 通知は、MA ごとに 1 つのクライアントに対してのみサポートされます。EFD 通知は、G-8032 と REP の両方で同時にサポートできません。
- EFD のインターフェイスまたは EFP で設定できる MEP は 1 つだけです。
- ピアノードからリンクステータスレイヤ（LSL）フレームを受信する REP エッジネイバーなし（ENN）設定ポートは、自動的に REP ポートに変換されます。

  REP デバイスに自動的に設定されたログメッセージ **%REP-6-AUTOCONFIG: Interface GigabitEthernet< >** が表示されます。
- REP は、**efd notify rep**（CCM）なしで、ポートチャネル インターフェイスでサポートされます。
- コンバージェンス時間は 100 ～ 200 ミリ秒です。

REP アクセスゲートウェイに関する情報

ネットワークでは、リンク障害が発生すると、REP ネットワークに直接接続されている非 REP デバイスネットワーク（アクセスゲートウェイ）が障害通知を送信するため、REP ネットワークはトラフィックを代替ルートへと再ルーティングできます。ただし、REP Edge ネイバーなし（REP ENN）をサポートするアクセスデバイスは、REP Edge ネイバーなしポートとして設定された 1 つのインターフェイスのみをサポートするため、REP アクセスゲートウェイ（REP AG）デバイスのアーキテクチャはサポートされません。

高速障害検出は、接続障害マネージャ（CFM）と REP 間の通信を有効にすることで確立できます。エッジ ポートの CFM は、モニター対象リンクで障害が検出された場合に REP に通知し、適切な再コンバージェンス アクションを実行できるようにします。

通信のメカニズムでは、REP がイーサネット障害検出（EFD）クライアントとして登録されます。これにより、設定可能なしきい値を超える CFM 障害が発生すると、REP への通知がトリガーされます。

（注） ルータで EFD 通知をトリガーするには、CFM を設定する必要があります。

REP アクセスゲートウェイの機能強化

REP デバイスと非 REP デバイスが接続されているネットワークでは、リンク障害が発生すると、REP ネットワークに直接接続されている非 REP デバイスネットワーク（アクセスゲートウェイ）が障害通知を送信するため、REP ネットワークはトラフィックを代替ルートへと再ルーティングできます。ただし、REP Edge ネイバーなし（REP ENN）をサポートするアクセスデバイスは、REP Edge ネイバーなしポートとして設定された 1 つのインターフェイスのみをサポートするため、REP アクセスゲートウェイ（REP AG）デバイスのアーキテクチャはサポートされません。

REP-AG が設定されたデバイスでの高速障害検出は、接続障害マネージャ（CFM）と REP 間の通信を有効にすることで実現できます。エッジポートの CFM は、モニター対象リンクで障害が検出された場合に REP に通知し、適切な再コンバージェンスアクションを実行できるようにします。

通信のメカニズムでは、REP がイーサネット障害検出（EFD）クライアントとして登録されます。これにより、設定可能なしきい値を超える CFM 障害が発生すると、REP への通知がトリガーされます。

REP アクセスゲートウェイの設定方法

EFD 通知のイネーブル化

始める前に

CFM IEEE は、EFD 通知をイネーブルする前にイネーブルする必要があります。詳細については、『Configuring Ethernet Connectivity Fault Management in a Service Provider Network』を参照してください。

CFM 設定の詳細については、『Carrier Ethernet Configuration Guide, Cisco IOS XE Release (Cisco ASR 900 Series)』、『』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** {*short-ma-name* | **number** *MA-number* | **vlan-id** *primary-vlan-id* | **vpn-id** *vpn-id*} {**vlan** *vlan-id* | **port** | **evc** *evc-name*} **direction** {**up** | **down**}
5. **continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**]

6. **continuity-check** [**interval** *cc-interval*]
7. **efd notify** {**g8032** | **rep**}
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**ethernet cfm domain** *domain-name* **level** *level-id* 例： `Router(config)# ethernet cfm domain Customer level 7`	指定されたメンテナンス レベルで CFM メンテナンス ドメインを定義し、CLI をイーサネット CFM コンフィギュレーション モードにします。
ステップ 4	**service** {*short-ma-name* | **number** *MA-number* | **vlan-id** *primary-vlan-id* | **vpn-id** *vpn-id*} {**vlan** *vlan-id* | **port** | **evc** *evc-name*} **direction** {**up** | **down**} 例： `Device(config-ecfm)# service s1 port`	メンテナンスドメイン内にメンテナンスアソシエーションを設定し、イーサネット接続障害管理（CFM）サービス コンフィギュレーション モードを開始します。
ステップ 5	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] 例： `Router(config-ecfm-srv)# continuity-check`	CCM の送信をイネーブルにします。
ステップ 6	**continuity-check** [**interval** *cc-interval*] 例： `Device(config-ecfm-srv)# continuity-check interval 10s`	各サービスについてパラメータを設定し、CCM が送信される間隔を設定します。
ステップ 7	**efd notify** {**g8032** | **rep**} 例： `Router(config)# efd notify rep`	• **g8032**：MA で G.8032 通知をイネーブルにします。 • **rep**：MA で REP 通知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） 1 つのインスタンスでは MA に対して G.8032 通知または REP 通知のいずれかを設定できます。たとえば、MA に対して G.8032 通知がイネーブルになっているときに REP 通知をイネーブルにすると、G.8032 通知はディセーブルになります。
ステップ 8	**end** 例： `Device(config-erp-profile)# end`	ユーザ EXEC モードに戻ります。

設定例

例：REP AG EFD の設定

以下に、ルータで EFD 通知がイネーブルになっている場合の例を示します。

```
ethernet cfm ieee
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache hold-time 60
ethernet cfm domain d1 level 6
 service s1 port
  continuity-check
  continuity-check interval 100ms
  efd notify rep
end
..
1


interface GigabitEthernet0/1/2
ethernet cfm mep domain d1 mpid 3 service s1
 service instance trunk 1 ethernet
  encapsulation dot1q 209-212
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
end
..
!


interface GigabitEthernet0/1/3
ethernet cfm mep domain d1 mpid 4 service s1
 service instance trunk 1 ethernet
  encapsulation dot1q 209-212
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
end
```

```
..
!
```

REP アクセスゲートウェイの確認

例：REP AG EFD 通知の確認

ステータス EFD を表示するには、 **show interface** コマンドを使用します。

- 次の例は、インターフェイスの EFD ステータスを示します。

```
Router# show interface gigabitethernet 0/1/7 rep detail

 Interface Gi0/1/7
---
GigabitEthernet1/7   REP enabled

Segment-id: 1 (Primary Edge No-Neighbor)
PortID: 000DE8BA70DD3000
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 001878DA6ED817002FF3
Port Role: Open
Blocked VLAN: empty
Admin-vlan: 2
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: STP
EFD State : Enabled
EFD Status : Clear
LSL PDU rx: 0, tx: 0
HFL PDU rx: 32, tx: 1
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 18
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

- 次の例は、REP トポロジを示します。

```
Router# show rep topolgy

REP Segment 911
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
node3            Te0/0/12   Pri* Alt
node3            Gi0/0/11        Open
node4            Gi0/0/11        Open
node4            Gi0/0/0         Open
node2            Gi0/0/0         Open
node2            Gi0/0/7    Sec* Open
```

- 以下は、 CFM EFD MEP 情報の例です。

（注） **show ethernet cfm efd mep** コマンドを実行する前に、コンフィギュレーション モードで service internal を設定します。

```
Router# show ethernet cfm efd mep

Domain d1, Service s1: notify REP, EFD not triggered
    ID Interface  SrvcInst Defect        Threshold     Triggered?
    ---- ---------- -------- ------------- ------------- ----------
     4 Te0/0/12   N/A      None          DefMACstatus  No
```

以下は、障害が検出されたときの CFM EFD MEP 情報の例です。

```
Router# show ethernet cfm efd meps | sec ring1
Domain dom1_ring1, Service ser1_ring1: notify REP, EFD not triggered
ID    Interface  SrvcInst   Defect     Threshold   Triggered?
----  ---------  --------   -------    ---------  ----------
3     Te0/0/12    NA        None      DefMACstatus  No
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS マスター コマンド リスト	『Cisco IOS Master Command List, All Releases』
『Carrier Ethernet Configuration Guide, Cisco IOS XE Release (Cisco ASR 900 Series)』	『Carrier Ethernet Configuration Guide, Cisco IOS XE Release (Cisco ASR 900 Series)』

標準

標準	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

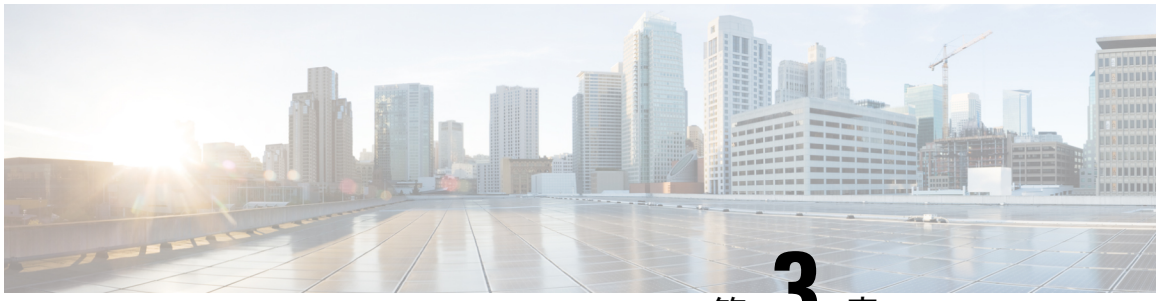
MIB	MIB のリンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html



第 3 章

単方向リンク検出（UDLD）プロトコル

単方向リンク検出プロトコルは、スパニングツリーのループなどの望ましくない状況が発生する前に単方向接続を検出してディセーブルにするレイヤ 2 プロトコルです。

UDLD プロトコルの制約事項

- ギガビットイーサネット、10 ギガビットイーサネット、およびファスト イーサネット インターフェイスでのみサポートされます。
- 基本的な UDLD 機能のみサポートされます。

UDLD プロトコルに関する情報

UDLD の概要

シスコ独自の UDLD プロトコルにより、LAN ポートに接続された光ファイバまたは銅製（カテゴリ 5 ケーブルなど）イーサネットケーブルを使用して接続されたデバイスで、ケーブルの物理構成をモニターし、単方向リンクの存在を検出することができます。単方向リンクはスパニング ツリー トポロジ ループなど、さまざまな問題の原因となるため、単方向リンクが検出された場合、UDLD は影響を受けた LAN ポートをシャットダウンして、該当するユーザーにアラートを表示します。

UDLD は、レイヤ 1 プロトコルと協調してリンクの物理ステータスを検出するレイヤ 2 プロトコルです。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 LAN 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方向接続、および他のプロトコルの誤動作を防止します。

リンク上でローカルデバイスが送信したトラフィックはネイバーで受信されるが、ネイバーから送信されたトラフィックはローカルデバイスで受信されない場合に、単方向リンクが発生します。対になったファイバケーブルのうち一方の接続が切断された場合、自動ネゴシエーションがアクティブである限り、そのリンクはアップ状態が維持されなくなります。このようなシナリオでは、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ 1 で両方の光ファイバが正常に動作している場合は、レイヤ 2 で UDLD が、これらの光ファイルが正しく接続されているかどうか、および正しいネイバー間でトラフィックが双方向に流れているかを調べます。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。

ルータは、UDLD がイネーブルの LAN ポートのネイバーデバイスに、UDLD パケットを定期的に送信します。このパケットが一定時間内にエコーバックされ、かつ特定の確認応答（エコー）がない場合には、そのリンクは単方向リンクとしてフラグ付けされ、LAN ポートがシャットダウンされます。単方向リンクが正しく識別されディセーブルされるようにするには、リンクの両端のデバイスで UDLD プロトコルがサポートされている必要があります。

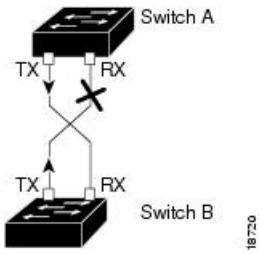
UDLD は、インターフェイスの誤配線または誤動作によるイーサネット光ファイバおよび銅線インターフェイス上の単方向リンクを検出し、ディセーブルにします。

（注） UDLD は、不要なトラフィックの送信を避けるために、すべてのポートでデフォルトでディセーブルになっています。

光ファイバインターフェイスを設定するには、グローバルレベルで **udld** コマンドを有効にします。銅線インターフェイスの場合は、インターフェイスレベルで **udld port** コマンドを有効にします。

UDLD のメカニズムを下図に示します。

図 *6:* 単方向リンク



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インターフェイスの誤接続に起因する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、光ファイバ リンクやツイストペア リンク上の片方向トラフィックに起因する単一方向リンク、および光ファイバ リンク上のインターフェイスの誤接続に起因する単一方向リンクも検出できます。

UDLD 通常モード

通常モードの UDLD は、光ファイバ インターフェイスの光ファイバが誤接続されている場合に単方向リンクを検出しますが、レイヤ 1 メカニズムは、この誤接続を検出しません。インターフェイス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は、単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 は単方向リンクを検出できません。その場合、論理リンクは不明となり、UDLD はインターフェイスをディセーブルにしません。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 メカニズムはリンクの物理的な問題を検出しないため、リンクは稼働状態でなくなります。この場合、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。

UDLD アグレッシブモード

UDLD アグレッシブモードは、そのモードをサポートするネットワーク デバイス間のポイントツーポイントのリンク上にのみ設定します。UDLD アグレッシブモードをイネーブルに設定した場合、UDLD ネイバー関係が確立されている双方向リンク上のポートは UDLD パケットの受信を停止します。UDLD はネイバーとの接続を再確立しようとします。再試行が 8 回失敗すると、ポートはディセーブルになります。

スパニング ツリー ループを防止するため、間隔がデフォルトの 15 秒である非アグレッシブな UDLD でも、（デフォルトのスパニング ツリー パラメータを使用して）ブロッキング ポートがフォワーディング ステートに移行する前に、単方向リンクをシャットダウンすることができます。

UDLD は、いずれかのモードが有効になっている場合、次のシナリオでトラフィックが廃棄されないように、リンク上のポートをエラーディセーブルできます。以下は通常モードまたはアグレッシブモードです。

- リンクの一方の側でポート（TX または RX）スタックを使用している場合。
- リンクの一方の側がダウンしているが、もう一方の側がアップしたままの場合。

UDLD の機能

UDLD は、次の機能を実行します。

- UDLD が設定されているアクティブなすべてのインターフェイスにプローブパケットを送信し、各デバイスにネイバーに関する情報を提供します。
- ネイバーに関する情報を確認し、更新したネイバー情報をキャッシュテーブルに保持します。
- UDLD パケットを送信する新しいネイバーを検出したり、ネイバーがキャッシュの再同期を要求したりすると、複数のエコーメッセージを送信します。
- 単方向の接続が検出されると、影響を受けるポートをシャットダウンして、ユーザーに通知します。UDLD プロトコルにより単方向リンクが正しく識別されその使用が禁止される

ようにするためには、リンクの両端のデバイスで UDLD がサポートされている必要があります。

- アグレッシブモードがイネーブルの場合、双方向リンク上のポートが UDLD パケットを受信しなくなると、ネイバーとの接続を再確立します。この再試行に 8 回失敗すると、ポートはディセーブル状態になります。

単方向リンクの検出

UDLD は 2 つのメカニズムを使用して動作します。

ネイバー データベース メンテナンス

UDLD は、すべてのアクティブ インターフェイスで Hello パケット（別名アドバタイズメントまたはプローブ）を定期的に送信して、他の UDLD 対応ネイバーについて学習し、各デバイスがネイバーに関しての最新情報を維持できるようにします。スイッチが 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、スイッチが新しい hello メッセージを受信すると、古いエントリが新しいエントリで置き換えられます。UDLD の稼働中にインターフェイスをディセーブルにしたり、インターフェイスで UDLD をディセーブルにしたり、またはスイッチをリセットした場合はいつでも、設定変更によって影響を受けたインターフェイスの既存のキャッシュ エントリがすべて消去されます。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 は検出メカニズム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 モードのときは、リンクは単一方向であると見なされ、インターフェイスはシャットダウンされます。通常モードにある UDLD が、アドバタイズまたは検出段階にあり、すべてのネイバーのキャッシュ エントリが期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。アグレッシブ モードをイネーブルにしていて、ポートのすべてのネイバーがアドバタイズまたは検出段階で期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。高速な一連のメッセージの送受信後に、リンク ステートが不確定のままの場合、UDLD はポートをシャットダウンします。

UDLD プロトコルの設定方法

UDLD プロトコルのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **udld** {**enable** | **aggressive**}
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**udld** {**enable**	**aggressive**} 例： `Router(config)# udld enable`	ルータでUDLDプロトコルをイネーブル化します。
ステップ 4	**end** 例： `Device(config-erp-profile)# end`	ユーザ EXEC モードに戻ります。

インターフェイスレベルでの UDLD プロトコルのイネーブル化

手順の概要

1. **interface** *interface-id*
2. **udld port** [**aggressive**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interface** *interface-id* 例： `Router(config)# interface gigabitethernet0/0/1`	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。
ステップ 2	**udld port** [**aggressive**] 例： `Router(config)# udld port aggressive`	特定のポート上で UDLD をイネーブルにします。aggressive キーワードを入力してアグレッシブモードをイネーブルにします。光ファイバ LAN ポートの場合、このコマンドはudld enable グローバル コンフィギュレーション コマンドによる設定を上書きします。 光ファイバ以外の LAN ポートで 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。

インターフェイスレベルでの UDLD プロトコルのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **udld port** [**aggressive**]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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： `Router(config)# interface gigabitethernet0/0/1`	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。

	コマンドまたはアクション	目的
ステップ 4	**udld port** [**aggressive**] 例： `Router(config)# udld port aggressive`	特定のポート上で UDLD をイネーブルにします。aggressive キーワードを入力してアグレッシブモードをイネーブルにします。光ファイバ LAN ポートの場合、このコマンドはudld enable グローバル コンフィギュレーション コマンドによる設定を上書きします。 光ファイバ以外の LAN ポートで 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 5	**end** 例： `Device(config-erp-profile)# end`	ユーザ EXEC モードに戻ります。

UDLD プローブメッセージ間隔のイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **udld message time** *interval*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**udld message time** *interval* 例： `Router(config)# udld message time 90`	UDLD プローブメッセージ間の時間を秒単位で設定します。有効な範囲は 7 ～ 90 秒です。デフォルトは 15 秒です。

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

UDLD プロトコルのリカバリ

UDLDリカバリが有効な場合、UDLDエラーによって無効になったポートのリセットの終了を試行します。デフォルトのリカバリタイマーは 300 秒です。

手順の概要

1. **enable**
2. **configure terminal**
3. **udld recovery** *inteval*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**udld recovery** *inteval* 例： `Router(config)# udld recovery`	ルータで UDLD リカバリをイネーブル化します。 • *inteval*：リカバリ時間間隔を設定します。有効な範囲は 30 ～ 86400 秒です。デフォルト値は 300 秒です。
ステップ 4	**end** 例： `Device(config-erp-profile)# end`	ユーザ EXEC モードに戻ります。

ポートのリセット

手順の概要

1. **enable**
2. **udld reset**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**udld reset** 例： `Router# udld reset`	UDLD によってシャットダウンされたポートをリセットします。
ステップ 3	**end** 例： `Device(config-erp-profile)# end`	ユーザ EXEC モードに戻ります。

設定例

例：UDLD プロトコルの設定

以下に、ルータの UDLD の例を示します。

```
show running-config | i udld
udld enable
udld message time 7
udld recovery
udld recovery interval 30
```

UDLD プロトコルの確認

例：UDLD プロトコルの確認

ポートの UDLD プロトコルのステータスを表示するには、**show udld** コマンドを使用します。

- 次の例では、ルータのすべてのポートの UDLD プロトコルを表示しています。

```
Router# show udld
 Interface Te0/0/0
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5

    Entry 1
    ---
    Expiration time: 40
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: FOX1736P0JP
    Port ID: Te0/1/0
    Neighbor echo 1 device: FOX1709P3D0
    Neighbor echo 1 port: Te0/0/0

    Message interval: 15
    Time out interval: 5
    CDP Device name: RSP1B

Interface Gi0/2/0
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5

    Entry 1
    ---
    Expiration time: 33
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: FOC1528V27K
    Port ID: Gi0/2
    Neighbor echo 1 device: FOX1709P3D0
    Neighbor echo 1 port: Gi0/2/0

    Message interval: 15
    Time out interval: 5
    CDP Device name: RSP1A

Interface Gi0/2/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5

    Entry 1
    ---
    Expiration time: 33
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: FOC1639V1Z4
```

```
    Port ID: Gi0/4
    Neighbor echo 1 device: FOX1709P3D0
    Neighbor echo 1 port: Gi0/2/1

    Message interval: 15
    Time out interval: 5
    CDP Device name: RSP1A

Interface Gi0/2/2
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Advertisement
Message interval: 15
Time out interval: 5
No neighbor cache information stored

Interface Gi0/2/3
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Link down
Message interval: 15
Time out interval: 5
No neighbor cache information stored

Interface Gi0/2/4
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Gi0/2/5
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Gi0/2/6
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown
.
.
.
```

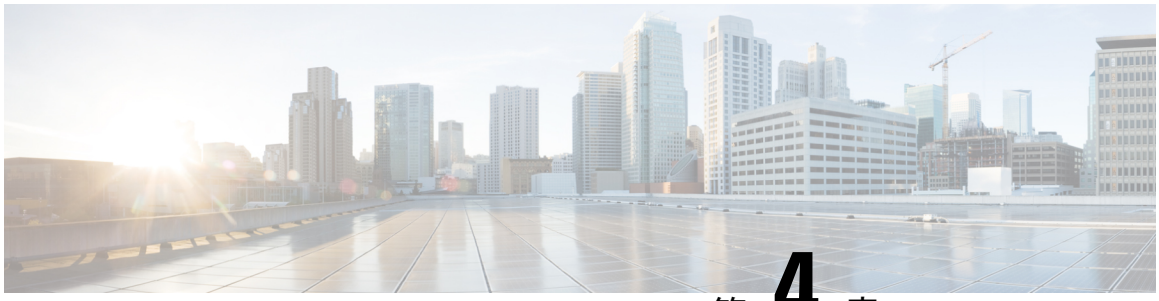
- 次の例では、10 個のギガビット イーサネット インターフェイスの UDLD プロトコルを表示しています。

```
Router# show udld tengigabitethernet 0/0/0

Interface Te0/0/0
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5

    Entry 1
```

```
    ---
    Expiration time: 43
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: FOX1736P0JP
    Port ID: Te0/1/0
    Neighbor echo 1 device: FOX1709P3D0
    Neighbor echo 1 port: Te0/0/0

    Message interval: 15
    Time out interval: 5
    CDP Device name: RSP1B

Router# show running-config | i udld
udld enable
udld message time 15
udld recovery
udld recovery interval 30
```

- 次の例では、UDLD プロトコルネイバーを表示しています。

```
Router# show udld neighbors

Port          Device Name     Device ID     Port ID        Neighbor State
------------ ------------- ------------ ------------ ----------------
Te0/0/0         FOX1736P0JP     1            Te0/1/0         Bidirectional
Gi0/2/0         FOC1528V27K     1            Gi0/2           Bidirectional
Gi0/2/1         FOC1639V1Z4     1            Gi0/4           Bidirectional
```



第 4 章

自動 Media Sense の設定

Cisco ASR 920 シリーズ（ASR-920-12CZ-A および ASR-920-12CZ-D）は、8 つのデュアルメディアポートをサポートします。デュアルメディアポートは、RJ45 モードまたは SFP（光ファイバ）モードで動作します。AMS は、メディアデュアルポートのいずれかでリンクアクティビティを検出し、通信用のリンクをイネーブル化します。デフォルトでは、リンク接続がない場合、リンク状態は down になります。メディアが接続されると、AMS は接続を検出してリンクを確立し、リンク状態を up にします。同じポートに RJ45 リンクと光ファイバリンクの両方が接続されている場合、ポートは光ファイバモードで up になります。

自動 Media Sense の設定の制約事項

- 100% の回線速度でメディアタイプが RJ45 から SFP に、またはその逆に変更されると、ポートはダウンします。回避策として、トラフィックを停止し、ポートで shut/no shut 操作を実行します。
- デフォルトでは、メディアタイプが auto-select に選択されている場合、自動ネゴシエーションが常に有効になります。
- ポート 4 ～ 11 では、同じポートを同時に RJ45 または SFP として使用することはできません。

自動 Media Sense に関する情報

デュアルメディアは、PHY レベルでサポートされています。Cisco ASR 920 シリーズ（ASR-920-12CZ-A および ASR-920-12CZ-D）は、8 つのデュアルメディアポートをサポートします。すべてのメディアタイプモードは、IOS インターフェイス コンフィギュレーション コマンドで制御されます。

- メディアタイプ「auto」は自動メディア検出用です。

- メディアタイプ「rj45」は rj45 モード用です。
- メディアタイプ「sfp」は SFP モード用です。

ポート番号 4 ～ 11 は、RJ45 またはファイバモードのいずれかで動作します。

表 *2 : Cisco ASR 920* シリーズ 前面パネルのポート配置

1G SFP のみ		1G AMS ポート								10G SFP+
1	3	5	7	9	11	5x	7x	9x	11x	13
0	2	4	6	8	10	[4x]	6x	8x	10x	12

自動 Media Sense の設定方法

メディア タイプの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **media-type** {**auto-select** | **rj45** | **sfp**}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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： `Router(config)# interface gigabitEthernet 0/0/5`	設定するデュアルメディアポートを指定し、インターフェイス設定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	**media-type** {**auto-select** | **rj45** | **sfp**} 例： `Router (config-if)# media-type sfp`	インターフェイスとデュアルメディアアップリンクポートのタイプを選択します。キーワードの意味は次のとおりです。 • **auto-select**：スイッチが動的にタイプを選択します。RJ-45 モジュールと SFP モジュールの両方が動作している場合、ポートは SFP モードで動作します。SFP モジュールのリンクがダウンすると、ポートは RJ-45 モードに切り替わります。SFP モジュールのリンクが回復すると、モードは RJ-45 から SFP に戻ります。auto-select モードでは、スイッチにより両方のタイプが速度およびデュプレックスの自動ネゴシエーションに設定されます（デフォルト）。これは AMS ポートのデフォルトのメディアタイプ設定です。 • **rj45**：スイッチが SFP モジュールインターフェイスをディセーブル化します。このポートに SFP モジュールを接続する場合、RJ-45 側がダウンしている、または接続していない場合でも、リンクを確立することはできません。このモードでは、デュアルパーパス ポートは 10/100/1000BASE-TX インターフェイスと同様の動作をします。このインターフェイス タイプに対応した速度およびデュプレックスの設定が可能です。 • **sfp**：スイッチが RJ-45 インターフェイスをディセーブル化します。この RJ-45 ポートにケーブルを接続している場合、SFP モジュール側がダウンしている、または SFP モジュールが接続していない場合でも、リンクを確立することはできません。インストールされている SFP モジュールのタイプに基づいて、このインターフェイス タイプに対応した速度およびデュプレックスの設定が可能です。
ステップ 5	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

設定例

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitEthernet 0/0/5
Router (config-if)# media-type sfp
Router(config-if)# end
```

メディア タイプの確認

手順の概要

1. **enable**
2. **show running-config interface** *interface-id*
3. **show interface** *interface-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**show running-config interface** *interface-id* 例： `Router> show running-config interface gigabitEthernet 0/0/6`	ポートに設定されているメディアタイプが表示されます。
ステップ 3	**show interface** *interface-id* 例： `Router> show interface gigabitEthernet 0/0/6`	ポートが動作しているメディアタイプが表示されます。

メディアタイプ設定の確認例

メディアタイプ設定の確認例を以下に示します。

```
 Part I

Router> enable
Router>show running-config interface gigabitEthernet 0/0/5
Building configuration...

Current configuration : 95 bytes
!
interface GigabitEthernet0/0/5
 no ip address
 media-type auto-select
 negotiation auto
```

```
Router> end


Part II

Router> enable
Router> show interfaces gigabitEthernet 0/0/5
GigabitEthernet0/0/5 is up, line protocol is up
  Hardware is 12xGE-2x10GE-FIXED, address is badb.adba.de85 (bia badb.adba.de85)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is SX
  output flow-control is off, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo.

Router> end
```

（注） メディアタイプは次のとおりです。

- SX：GLC-SX-SMD が接続されています。
- ZX：GLC-ZX-SMD が接続されています。
- RJ45：銅線モードが接続されています。

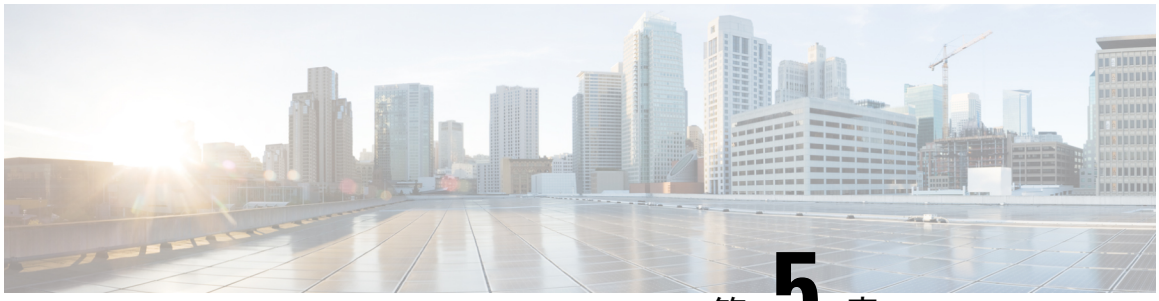
メディアタイプの設定のトラブルシューティング

特定のポートの PHY レベルのメディアタイプを判定するには、**show platform software agent iomd 0/0 phy <port_num> 1 14** コマンドを使用します。

```
Router> enable
Router# show platform software agent iomd 0/0 phy 5 1 14

Port Number: 5
Device/Page: 0x1
Register   : 0x14
Value      : 0xa084
```

（注） レジスタの値によって、メディアタイプの設定が分かります。

- 0xa084：ポートは SFP モードで動作しています。
- 0xa045：ポートは RJ45 モードで動作しています。



第 5 章

Flex Link の設定

この章では、Flex Link の設定方法について説明します。これは、レイヤ 2 インターフェイスのペアで、一方のインターフェイスが他方のインターフェイスのバックアップとして機能するように設定されています。

Flex Link の設定の制約事項

- Flex Link は、NCS 4201 および NCS 4202 ルータでのみサポートされます。
- 任意のアクティブ リンクに対して設定可能な Flex Link バックアップ リンクは 1 つだけで、アクティブ インターフェイスとは異なるインターフェイスでなければなりません。
- インターフェイスが所属できる Flex Link ペアは 1 つだけです。インターフェイスは、1 つだけのアクティブ リンクのバックアップ リンクにすることができます。アクティブ リンクは別の Flex Link ペアに属することはできません。
- どちらのリンクも、EtherChannel およびポートチャネルに属するポートには設定できません。
- バックアップリンクはアクティブリンクと同じタイプ（ファストイーサネット、ギガビットイーサネット）でなくてもかまいません。
- STP は Flex Link ポートでディセーブルです。スイッチ上で STP が設定されている場合でも、Flex Link は STP が設定されているすべての VLAN の STP に参加しません。STP が実行されていない場合、設定されているトポロジでループがないかを確認してください。
- Flex Link は、トランク EFP でのみサポートされます。
- 双方向トラフィックでは、MAC アドレスのブラックホール化により、FlexLink コンバージェンスが一方向で高くなります。

Flex Link について

この機能は、スパニングツリープロトコル（STP）の代替ソリューションとして提供され、STP をオフにしても、基本的なリンク冗長性は確保されます。Flex Link は、通常、ルータで STP を実行しない場合に、サービスプロバイダーまたは企業ネットワークで設定されます。ルータが STP を実行中の場合、STP がすでにリンクレベルの冗長性またはバックアップを提供しているので Flex Link の設定は必要ありません。Flex Link はトランク EFP でのみサポートされており、他の EVC ではサポートされません。

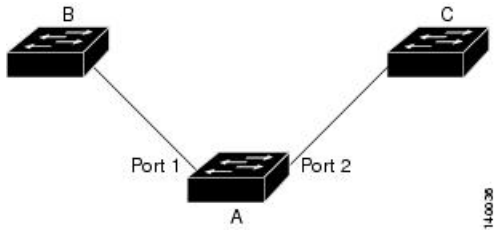
次の 2 つの Flex Link モードがサポートされています。

- Active-Alone 転送方式
- Active-Backup-Both 転送方式

Active-Alone 転送方式

次の概略図では、スイッチ A のポート 1 およびポート 2 がアップリンク スイッチ B およびアップリンク スイッチ C に接続されています。これらは Active-Backup-Both 転送モードの Flex Link として設定されているため、両インターフェイスとも、トラフィックを転送します。ポート 1 がアクティブリンクの場合、すべての相互包含的 VLAN（アクティブ/バックアップ インターフェイスの両方が設定された共通 VLAN）はアクティブインターフェイスで転送され、相互排他的 VLAN はそれぞれのアクティブ/バックアップ インターフェイスから転送されます。ポート 1 がダウンすると、ポート 2 は自身の排他的 VLAN とともに、共通 VLAN のトラフィックのみ転送を開始します。アクティブインターフェイス設定により排他的 VLAN に属するすべてのトラフィックは、ポート 1 が動作状態に戻るまでドロップされます。

図 *7: Active-Alone* 転送方式



Active Alone 転送方式の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **no shutdown**
5. **ethernet backup interface** *interface-id*

6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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： `Router(config)# interface gigabitEthernet 0/0/5`	インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポートチャネル（論理インターフェイス）に設定できます。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 4	**no shutdown** 例： `Router(config-if)# no shutdown`	必要な場合に、ポートをイネーブルにします。デフォルトでは、UNI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 5	**ethernet backup interface** *interface-id* 例： `Router(config)# ethernet backup interface gigabitEthernet 0/0/5`	物理レイヤ 2 インターフェイス（またはポートチャネル）を、インターフェイスを装備した Flex Link ペアの一部として設定します。1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 6	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

設定例

```
On Active interface(Port 5)

Router> enable
Router# configure terminal
Router# service instance trunk 1000 ethernet
Router# encapsulation dot1q 1-1000
Router# rewrite ingress tag pop 1 symmetric
Router# bridge-domain from-encapsulation


Backup interface (Port 6)
```

```
Router> enable
Router# configure terminal
Router# service instance trunk 1000 ethernet
Router# encapsulation dot1q 1-1000
Router# rewrite ingress tag pop 1 symmetric
Router# bridge-domain from-encapsulation
```

Flexlink Configuration

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitEthernet 0/0/5
Router(config-if)# no shutdown
Router(config-if)# ethernet backup interface gigabitEthernet 0/0/6
Router(config-if)# end
```

Active Alone 転送方式の設定の確認

手順の概要

1. **enable**
2. **configure terminal**
3. **show ethernet backup detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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	**show ethernet backup detail** 例： `Router# show ethernet backup detail`	これにより、Flex Link の設定が表示されます。

[Configuration Output]

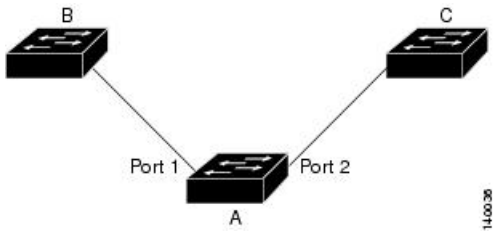
```
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/0/5    Te0/0/12                Active Up/Backup Standby
        Preemption Mode  : off
        Multicast Fast Convergence  : Off
```

```
Bandwidth : 1000000 Kbit (Gi0/0/3), 1000000 Kbit (Te0/0/12)
Mac Address Move Update Vlan : auto
Forwarding  : Active-Only
```

Active-Backup-Both 転送方式

次の概略図では、スイッチ A のポート 1 およびポート 2 がアップリンクスイッチ B およびアップリンクスイッチ C に接続されています。これらは Active-Backup-Both 転送モードの Flex Link として設定されているため、両インターフェイスとも、トラフィックを転送します。ポート 1 がアクティブリンクの場合、すべての相互包含的 VLAN（アクティブ/バックアップ インターフェイスの両方が設定された共通 VLAN）はアクティブインターフェイスで転送され、相互排他的 VLAN はそれぞれのアクティブ/バックアップ インターフェイスから転送されます。ポート 1 がダウンすると、ポート 2 は自身の排他的 VLAN とともに、共通 VLAN のトラフィックのみ転送を開始します。アクティブインターフェイス設定により排他的 VLAN に属するすべてのトラフィックは、ポート 1 が動作状態に戻るまでドロップされます。

図 *8 : Active-Backup-Both* 転送方式



Active-Backup-Both 転送方式の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **no shutdown**
5. **ethernet backup interface** *interface-id* **prefer forwarding**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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
	`Router# configure terminal`	
ステップ 3	**interface** *interface-id* 例： `Router(config)# interface gigabitEthernet 0/0/8`	インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポートチャネル（論理インターフェイス）に設定できます。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 4	**no shutdown** 例： `Router(config-if)# no shutdown`	必要な場合に、ポートをイネーブルにします。デフォルトでは、UNI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 5	**ethernet backup interface** *interface-id* **prefer forwarding** 例： `Router(config)# ethernet backup interface gigabitEthernet 0/0/8 prefer forwarding`	物理レイヤ 2 インターフェイス（またはポートチャネル）を、インターフェイスを装備した Flex Link ペアの一部として設定します。1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 6	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

設定例

```
On Active interface(Port 7)

Router> enable
Router# configure terminal
Router# service instance trunk 1000 ethernet
Router# encapsulation dot1q 1-512
Router# rewrite ingress tag pop 1 symmetric
Router# bridge-domain from-encapsulation


Backup interface (Port 8)

Router> enable
Router# configure terminal
Router# service instance trunk 1000 ethernet
Router# encapsulation dot1q 512-1000
Router# rewrite ingress tag pop 1 symmetric
Router# bridge-domain from-encapsulation


Flexlink Configuration

Router> enable
Router# configure terminal
```

```
Router(config)# interface gigabitEthernet 0/0/8
Router(config-if)# no shutdown
Router(config-if)# ethernet backup interface gigabitEthernet 0/0/8 prefer forwarding

Router(config-if)# end
```

Active-Backup-Both 転送方式の設定の確認

手順の概要

1. **enable**
2. **configure terminal**
3. **show ethernet backup detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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	**show ethernet backup detail** 例： `Router# show ethernet backup detail`	これにより、Flex Link の設定が表示されます。

[Configuration Output]

```
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/0/3    Te0/0/12                Active Up/Backup Standby
        Preemption Mode  : off
        Multicast Fast Convergence  : Off
        Bandwidth : 1000000 Kbit (Gi0/0/3), 1000000 Kbit (Te0/0/12)
        Mac Address Move Update Vlan : auto
        Forwarding  : Active-Backup-Both
```

サポートされない機能

以下の機能はサポートされません。

- MMU 通知

- IGMP 高速コンバージェンス
- プリエンプションのサポート
- ポートチャネル インターフェイスでの Flex Link のサポート
- EVC での Flex Link のサポート
- VLB を使用する Flex Link
- IP が設定された物理インターフェイス上の Flex Link
- Flexlink は REP/G8032 が設定されたインターフェイスには設定できません。逆も同様です。
- STP はグローバルにイネーブルにできますが、Flex Link が設定されたインターフェイスのみには適用されません。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

標準および RFC

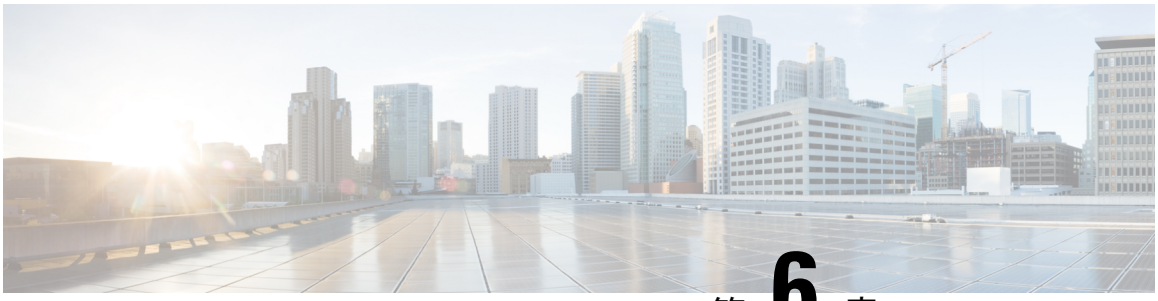
標準/RFC	タイトル
このマニュアルに記載された機能によってサポートされている特定の標準規格および RFC はありません。	—

MIB

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

シスコのテクニカル サポート

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



第 6 章

ITU-T G.8032 イーサネットリング保護スイッチング

ITU-T G.8032 イーサネットリング保護スイッチング機能により、イーサネット レイヤ リングトポロジの保護スイッチングメカニズムが実装されます。この機能は、ITU-T G.8032 で定義されている G.8032 イーサネットリング保護（ERP）プロトコルを使用して、リングトポロジでイーサネットトラフィックを保護し、イーサネットレイヤのリング内でループが発生しないようにします。ループは、事前設定されたリンクまたは障害リンクのいずれかでトラフィックをブロックすることで防止されます。

ITU-T G.8032 イーサネットリング保護スイッチング設定の前提条件

- イーサネットフローポイント（EFP）とトランクのイーサネットフローポイント（TEFP）を設定する必要があります。

ITU-T G.8032 イーサネットリング保護スイッチングについて

リング保護リンク

イーサネットリングは、複数のイーサネットリングノードで構成されます。各イーサネットリングノードは、2 個の独立したリングリンクを使用して、隣接イーサネットリングノードに接続されます。リングリンクは、ネットワークに影響を及ぼすループの編成を防止します。イーサネット リングは、イーサネット リングを保護するために特定のリンクを使用します。この特定のリンクは、リング保護リンク（RPL）と呼ばれます。リング リンクは、リング リンク（別名リング ポート）の2個の隣接するイーサネット リング ノードとポートで区切られます。イーサネットリングには、最低 2 つのイーサネットリングノードが必要です。

ITU-T G.8032 イーサネットリング保護スイッチングの機能

イーサネットリング保護には、以下のような機能があります。

- ループ回避
- 学習、転送、およびフィルタリングデータベース（FDB）メカニズムの使用

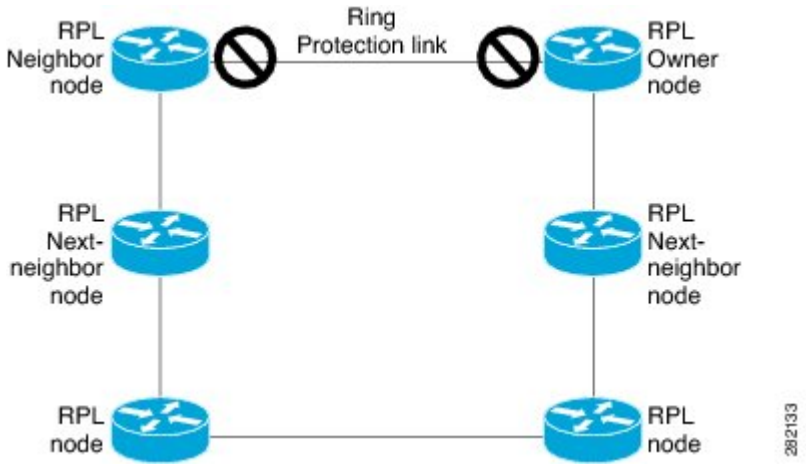
イーサネットリングでのループ回避は、リング保護リンク（RPL）以外のすべてで常にトラフィック フローを確保することで行います。

RPL のタイプ（または RPL ノード）とその機能には、以下があります。

- RPL オーナー：ループがイーサネットトラフィックで形成されないように、RPL を介してトラフィックをブロックします。リングには RPL オーナーは 1 つだけ存在します。
- RPL ネイバーノード：RPL に隣接するイーサネットリングノードです。通常の状態で RPL の終了をブロックします。このノード タイプはオプションであり、保護されている場合 RPL の使用を防止します。
- RPL の次のネイバーノード：次のネイバーノードは、RPL オーナーノードまたは RPL ネイバーノードに隣接するイーサネットリングノードです。これは、主にリングでの FDB フラッシュ最適化に使用されます。このノードはオプションです。

次の図は G.8032 イーサネットリングトポロジの例です。

図 *9 : G.8032* イーサネットリングトポロジ



R-APS 制御メッセージ

リング上のノードは、リング自動保護スイッチング（R-APS）メッセージと呼ばれる制御メッセージを使用して、リング保護リンク（RPL）のオン/オフを切り替えるアクティビティを制御します。リンクの障害によって、障害が発生したリンクに面するポートをノードがブロックした後で、障害が発生したリンクに隣接するノードの両方の方向にR-APS信号障害（R-APS SF）メッセージがトリガーされます。このメッセージの取得時に、RPLオーナーは、RPLポートのブロックを解除します。

（注） リングの単一のリンク障害によって、ループフリー トポロジが確保されます。

CFM プロトコルとリンク障害

リングリンクおよびノード障害を検出するために、接続障害管理（CFM）メッセージと回線ステータスメッセージが使用されます。回復フェーズ中に、障害が発生したリンクが復元されると、復元されたリンクに隣接するノードは、リング自動保護スイッチング（R-APS）No Request（R-APS NR）メッセージを送信します。このメッセージの取得時に、リング保護リンク（RPL）オーナーはRPLポートをブロックし、R-APS NRとR-APS RPL（R-APS NR、RB）メッセージを送信します。このメッセージにより、リング内のRPLオーナー以外のその他すべてのノードが、すべてのブロックされたポートのブロックを解除します。イーサネットリング保護（ERP）プロトコルは、リングトポロジの単方向障害と複数のリンク障害シナリオの両方で機能します。

（注） G.8032 イーサネットリング保護（ERP）プロトコルは、3.3 ミリ秒（ms）の間隔で CFM 連続性チェックメッセージ（CCM）を使用します。この間隔（選択したプラットフォームでのみサポート）では、SONETに匹敵するスイッチング時間パフォーマンスとループフリートラフィックを実現できます。

G.8032 リングでサポートされるコマンドと機能

G.8032 リングは、次の基本的なオペレータ管理コマンドをサポートします。

- Force switch（FS）：オペレータは、特定のリング ポートを強制的にブロックできます。Force Switch コマンドについては、次の点に注意してください。
  - 既存の SF 状態がある場合でも有効です。
  - リングには複数の FS コマンドがサポートされます。
  - 即時のメンテナンス操作を可能にするために使用できます。
- Manual switch（MS）：オペレータは、特定のリングポートを手動でブロックできます。MS コマンドについては、次の点に注意してください。
  - 既存の FS または信号障害（SF）状態では無効です。
  - 新しい FS または SF 状態によって上書きされます。
  - 同じデバイスで複数の MS コマンドを複数回実行すると、すべての MS コマンドがキャンセルされます。

    リング内の異なるデバイスで同じインスタンスに対して複数の MS コマンドを実行すると、2 番目のデバイスで実行したコマンドは拒否されます。
- Clear：リングポートで既存の FS または MS コマンドを取り消します。Clear コマンドは、非リバーティブモード状態をクリアするために、リング保護リンク（RPL）のオーナーで使用されます。

G.8032 リングは、複数のインスタンスをサポートできます。インスタンスは、物理的なリングに実行される論理リングです。このようなインスタンスは、リング上での VLAN のロードバランシングなど、さまざまな理由で使用されます。たとえば、奇数番号の VLAN がリングの 1 方向に送信され、偶数番号の VLAN がもう一方の方向に送信されることがあります。特定の VLAN は 1 つのインスタンスだけで設定できます。これらは複数のインスタンスと重複できません。そうしないと、データトラフィックまたはリング自動保護スイッチング（R-APS）メッセージが論理リング間で伝送される可能性があり、これは望ましくありません。

（注） G.8032 イーサネット リング保護スイッチング バージョン 1 およびバージョン 2 がサポートされています。

G.8032 ERP タイマー

G.8032 は、競合状態および不要なスイッチング操作を回避するために異なる ERP タイマーを使用することを指定します。

- 遅延タイマー：リング保護リンク（RPL）をブロックする前に、ネットワークが安定していることを確認するために RPL オーナーによって使用されます。遅延タイマーについては、次の点に注意してください。
  - 信号障害（SF）状態の後で、SF が断続的に中断していないことを確認するために、Wait-to-Restore（WTR）タイマーが使用されます。
  - WTR タイマーはオペレータが設定できます。デフォルトの時間間隔は 5 分です。時間間隔の範囲は 1 ～ 12 分です。
  - 強制切り替え（FS）または手動切り替え（MS） コマンドの実行後、バックグラウンド状態でないことを確認するために、Wait-to-Block（WTB）タイマーが使用されます。

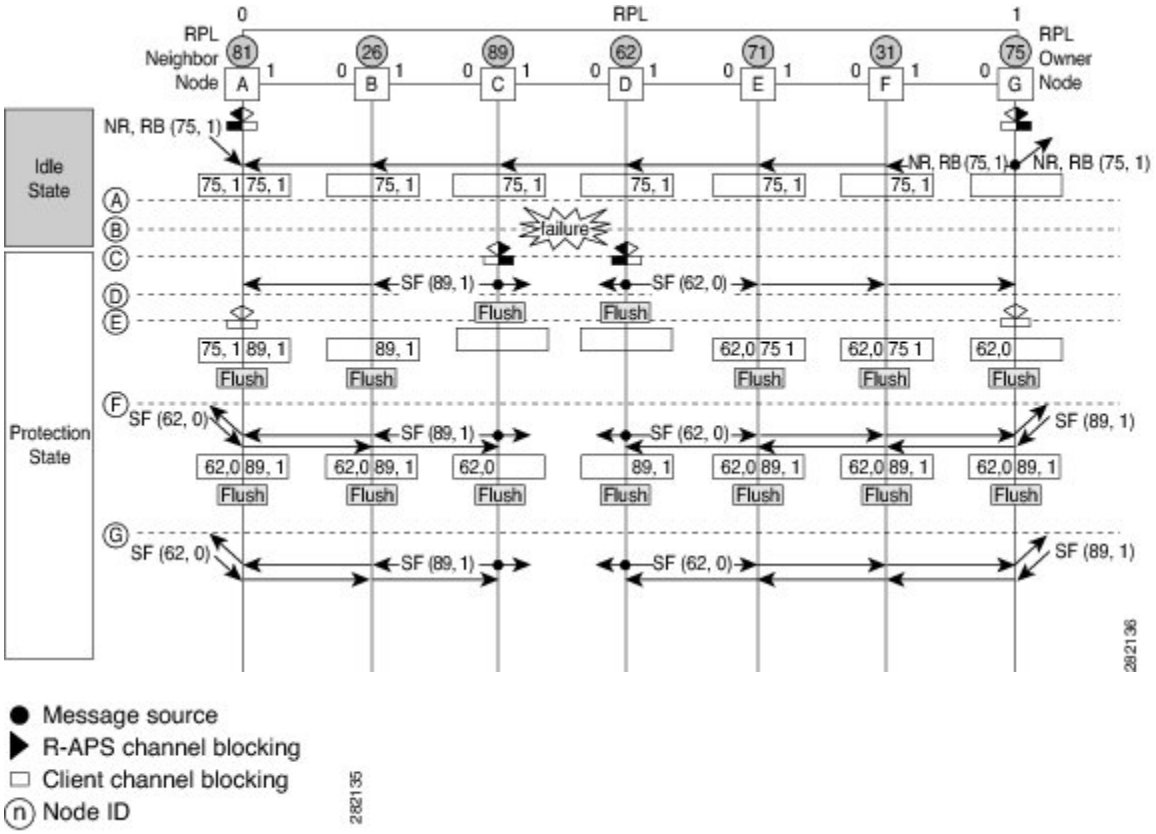
（注） WTB タイマー間隔は、WTR タイマー間隔よりも短い場合があります。

- ガードタイマー：状態の変更時にすべてのノードで使用されます。ガードタイマーは、潜在的な古いメッセージが不要な状態変更を引き起こさないようにします。ガードタイマーは設定できます。デフォルトの時間間隔は 500 ミリ秒です。時間間隔の範囲は 10 ～ 2000 ミリ秒です。
- 推奨されるガードタイマーは 500 ミリ秒です。
- hold-off タイマー：断続的なリンク障害をフィルタリングするために、基盤となるイーサネットレイヤによって使用されます。hold-off タイマーは設定できます。デフォルトの時間間隔は 0 秒です。時間間隔の範囲は 0 ～ 10 秒です。障害は、このタイマーの期限が切れた場合だけリング保護メカニズムに報告されます。

単一リンクの障害と回復における保護スイッチング機能

次の図に、単一のリンク障害時の保護スイッチング機能を示します。

図 *10 :* 単一リンク障害時の *G.8032* イーサネットリング保護スイッチング



この図は、7 つのイーサネットリングノードで構成されたイーサネットリングトポロジを表しています。リング保護リンク（RPL）は、イーサネットリングノード A と G の間のリングリンクです。このトポロジでは、RPL の両端がブロックされます。イーサネット リング ノード G は RPL オーナー ノードで、イーサネット リング ノード A は RPL ネイバー ノードです。

単一リンク障害での動作を以下に説明します。

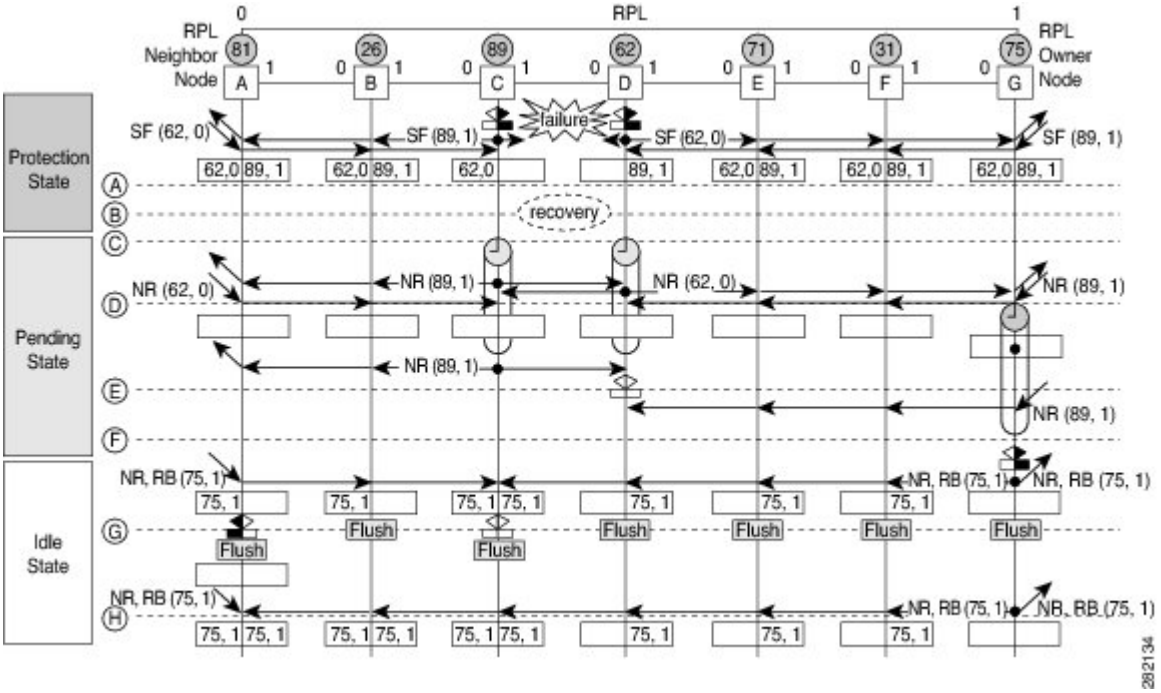
1. リンクが正常な状態で動作しています。
2. 障害が発生します。
3. イーサネットリングノード C と D は、ローカルの信号障害（SF）を検出して、hold-off 時間間隔後に障害が発生したリングポートをブロックし、FDB フラッシュを実行します。
4. イーサネットリングノード C と D は、SF 状態が続いている間、両方のリングポートの（ノード ID と双方向パス保護リング（BPR）ID のペア）とともにリング自動保護スイッチング（R-APS）メッセージの定期的な送信を開始します。
5. R-APS SF メッセージを受信するすべてのイーサネットリングノードが FDB フラッシュを実行します。RPL オーナーノード G と RPL ネイバーノード A が R-APS SF メッセージを受信すると、イーサネットリングノードは自身の RPL の終端をブロック解除し、FDB フラッシュを実行します。

6. 2 番目の R-APS SF メッセージを受信するすべてのイーサネットリングノードは、FDB フラッシュを再度実行します。このフラッシュは、ノード ID と BPR ベース コンフィギュレーションのためです。

7. R-APS SF メッセージがイーサネットリングで検出され、SF の状態が安定していることが示されます。これ以降の R-APS SF メッセージは、さらなるアクションをトリガーしません。

次の図は、単一リンク障害が発生した場合のリバーティブ操作を示しています。

図 *11* : 単一リンク障害回復（リバーティブ操作）



単一リンク障害でのリバーティブ（回復）操作を以下に説明します。

1. リンクが安定した SF 状態で動作しています。

2. リンク障害回復が行われます。

3. イーサネットリングノード C と D は、SF 状態のクリアを検出し、ガードタイマーを開始して、両方のリングポートで R-APS No Request（NR）メッセージの定期的な送信を開始します（ガードタイマーは、R-APS メッセージの受信を防止します）。

4. イーサネットリングノードが R-APS NR メッセージを受信すると、受信側リングポートのノード ID および BPR 識別子のペアが削除され、RPL オーナーノードは Wait-to-Restore（WTR）タイマーを開始します。

5. イーサネットリングノード C と D でガードタイマーの期限が切れると、新しい R-APS メッセージが送信された場合にノードがこれを受け入れることがあります。イーサネットリン

グノード D は、イーサネットリングノード C から上位のノード ID を持つ R-APS NR メッセージを受信し、障害が発生していないリングポートのブロックを解除します。

6. WTR タイマーの期限が切れると、RPL オーナーノードは、RPL の終端をブロックし、（ノード ID と BPR 識別子のペア）を持つ R-APS（NR または route blocked（RB））メッセージを送信し、FDB フラッシュを実行します。

7. イーサネットリングノード C が R-APS（NR または RB）メッセージを受信すると、ブロックされたリングポートのブロックを解除し、R-APS NR メッセージの送信を停止します。一方、RPL ネイバーノード A が R-APS NR または RB メッセージを受信すると、ノードは RPL の終端をブロックします。さらに、イーサネットリングノード A ～ F は、RAPS NR または RB メッセージを受信したときに、FDB フラッシュを実行します。これは、ノード ID と BPR ベース コンフィギュレーションのためです。

イーサネット フロー ポイント

イーサネットフローポイント（EFP）は、プロバイダーエッジ（PE）ルータにある転送判断ポイントであり、インターフェイス内の多数のレイヤ 2 のフロー判断に関する自由度をネットワーク設計者に提供します。1 つの物理ポートに複数の EFP が設定できます（設定数は 1 デバイスからそれ以上までさまざまです）。EFP は、インターフェイス上の Ethernet Virtual Connection（EVC：イーサネット仮想コネクション）の論理境界点です。複数のユーザー ネットワーク インターフェイス（UNI）を使用する EVC では、EVC が経由するすべてのデバイスの関連する入出力インターフェイスに EFP が必要です。

EFP は任意のレイヤ 2 トラフィックポートに設定できます。ただし、通常は UNI ポートに設定されます。EFP では、次のパラメータ（一致基準）を設定できます。

- 特定の VLAN、VLAN 範囲、または VLAN のリスト（100-150 または 100,103,110）のフレーム
- タグのない（タグなし）フレーム
- 同じ二重タグ（VLAN タグ）が指定されたフレーム
- 同じサービスクラス（CoS）値があるフレーム

正しい一致点が見つかるまで、フレームは設定された各一致基準を通過します。フレームが一致基準のいずれにも一致しない場合、そのフレームはドロップされます。フレームのドロップを回避するために、デフォルトの基準を設定できます。

ブリッジドメイン（BD）からのカプセル化を使用して、TEFP と呼ばれる新しいタイプの TEFP を設定できます。スイッチに設定されているすべての BD は、カプセル化された TEFP の VLAN リストに含まれています。TEFP は、**encapsulation dot1q from-bd** コマンドによりカプセル化されます。この機能は、イーサネット EFP とレイヤ 2 ブリッジドメイン コンポーネント間で以下のように動作します。

- BD がシステムに存在し、ブリッジドメインからカプセル化された TEFP が作成された場合、すべての BD がブリッジドメインからカプセル化された TEFP の VLAN リストに追加されます。

- ブリッジドメインからカプセル化された TEFP がシステムに存在し、新しい BD が作成された場合、BD はシステム内のブリッジドメインからカプセル化されたすべての TEFP の VLAN リストに追加されます。
- ブリッジドメインからカプセル化された TEFP がシステムに存在し、BD が削除され、削除された BD が既存の TEFP または EFP に含まれていない場合、システム内のブリッジドメインからカプセル化されたすべての TEFP からその BD は削除されます。

EFP では、次のタイプのコマンドを使用できます。

- 書き換えコマンド：各 EFP で、次のアクションを使用して VLAN タグ管理を指定できます。
  - Pop：1）1 つのタグを取り出します。2）2 つのタグを取り出します。
  - Push：1 つのタグを挿入します。
  - Translate：1 to 1）タグの値を変更します。1 to 2）1 つのタグを取り出し、2 つのタグを挿入します。2 to 1）2 つのタグを取り出し、1 つのタグを挿入します。2 to 2）2 つのタグの値を変更します。
- 転送コマンド：各 EFP は、EFP に入るフレームの転送コマンドを指定します。転送コマンドは EFP ごとに 1 つだけ設定できます。以下の転送オプションがあります。
  - 疑似回線トンネルへのレイヤ 2 ポイントツーポイント転送
  - ブリッジドメイン エンティティへのマルチポイントブリッジ転送
  - 2 つの異なるインターフェイス間のローカルのスイッチ間転送
- 機能コマンド：各 EFP で、QoS の機能またはパラメータを変更したり、ACL を更新したりできます。

サービスインスタンスおよび関連付けられる EFP

レイヤ 2 ポートにサービス インスタンスを設定すると、EVC 機能を設定する疑似ポートまたは EFP が作成されます。各サービス インスタンスは、インターフェイスごとに一意の番号を持ちますが、異なるポート上のサービスインスタンス同士は関係を持たないため、異なるインターフェイスで同じ番号を使用できます。

EFP は、ユーザ定義の基準に基づいて、同じ物理ポートからのフレームを、そのポートに関連付けられた複数のサービスインスタンスの 1 つに分類します。各 EFP に、異なる転送アクションと動作を関連付けることができます。

EFP が作成されたとき、初期状態は UP です。次の状況では、状態が DOWN に変わります。

- ユーザが EFP を明示的にシャット ダウンする。
- EFP が関連付けられているメインインターフェイスが停止しているか、削除されている。
- EFP がブリッジ ドメインに属する場合に、そのブリッジ ドメインが停止している。

• EFP が、特定の機能の問題防止手段として、強制停止されている。

レイヤ 2 インターフェイスに EFP を作成し、サービス インスタンス コンフィギュレーション モードを開始するには、**service instance ethernet** 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。サービスインスタンス コンフィギュレーションモードは、インターフェイス単位でサービスインスタンスに適用される、管理プレーンとコントロールデータプレーンのすべての属性とパラメータを設定するために使用します。サービスインスタンス番号はEFP ID です。

デバイスがサービスインスタンス コンフィギュレーション モードを開始すると、次のオプションを設定できます。

• default：コマンドをデフォルトに設定します。

• description：サービスインスタンスの説明を追加します。

• encapsulation：イーサネットフレームの一致基準を設定します。

• exit：サービス インスタンス コンフィギュレーション モードを終了します。

• no：コマンドを無効にするか、またはデフォルト値を設定します。

• shutdown：サービスインスタンスを停止します。

ITU-T G.8032 イーサネットリング保護スイッチング設定の制約事項

表 *3:* 機能の履歴

機能名	リリース情報	機能説明
IEEE 802.1Q EFP への G.8032 のサポート	Cisco IOS XE Bengaluru 17.6.1	この機能は、IEEE 802.1Q イーサネットフローポイント（EFP）で G.8032 イーサネットリング保護をサポートします。このリリース以前は、IEEE 802.1Q での G.8032 イーサネットリング保護は、トランク イーサネット フローポイント（TEFP）でのみサポートされていました。

ITU-T G.8032 イーサネットリング保護スイッチングの設定には以下の制約事項があります。

（注） 有効な Cisco IOS XE Bengaluru 17.6.1, G.8032 は、RSP3 モジュールの IEEE 802.1Q での EFP と TEFP の両方でサポートされます。

- G.8032 は、物理インターフェイスおよびポートチャネル インターフェイスの EFP ブリッジドメインでのみサポートされます。
- G.8032 は、カプセル化タイプが dot1q、dot1ad、QinQ、または dot1ad-dot1Q の EFP でのみサポートされます。
- G.8032 は、相互接続インターフェイスではサポートされません。
- G.8032 は、リングあたり最大 2 つの ERP インスタンスを持つ最大 8 つの ERP リングをサポートします。
- 包含的または排他的 VLAN リストの設定中にリンク フラップが発生します。
- 管理者は、接続障害管理（CFM）の設定を変更する前にシャットダウンすることを強くお勧めします。
- 障害が発生した場合は、CFM 設定で **efd notify** コマンドを使用して、G.8032 に障害を通知する必要があります。
- G.8032 のサポートは、通常のインターフェイスでのみ要求され、ポートチャネルでは要求されません。
- G.8032 イーサネットリング保護スイッチングバージョン 1 およびバージョン 2 がサポートされています。
- BFD IPv4 および IPv6 シングルホップがサポートされています。BFD エコーモードはサポートされていません。

RSP3 の EFP での ITU-T G.8032 イーサネットリング保護プロトコルの設定には、以下の制約事項が適用されます。

- G.8032 リングに参加している EFP での VLAN 範囲の追加はサポートされません。
- TEFP と同様に、G.8032 は **rewrite action as pop1 symmetric** コマンドを使用する IEEE 802.1Q EFP でのみサポートされます。
- G.8032 が IEEE 802.1Q EFP で設定されている場合、G.8032 プロトコルに参加しているポートには TEFP を設定しないでください。
- TEFP から EFP への移行中は、両方のリングポートをシャットダウンする必要があります。これにより、サービスが中断します。
- TEFP を EFP に移行する際は、包含的 VLAN および排他的 VLAN の両方のリストに存在するすべてのデータ VLAN をリングポートから削除してください。リングポートのこれらの VLAN をすべて再設定します。

- EFP で G.8032 を設定する場合、カプセル化 VLAN とブリッジドメインの値はサービスインスタンス内で同じである必要があります。サービスインスタンスでは、カプセル化VLANとブリッジドメインに異なる値を使用できません。
- 開いたリングの構成では、**RPL neighbor** コマンドは必要ありません。

ITU-T G.8032 イーサネットリング保護スイッチングの設定方法

イーサネット リング プロファイルの設定

イーサネット リング プロファイルを設定する手順は、次のとおりです。

手順の概要

1. **enable**
2. **configure terminal**
3. **ethernet ring g8032 profile** *profile-name*
4. **timer** {**guard** *seconds* | **hold-off** *seconds* | **wtr** *minutes*}
5. **non-revertive**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**ethernet ring g8032 profile** *profile-name* 例： `Device(config)# ethernet ring g8032 profile profile1`	イーサネット リング プロファイルを作成し、イーサネットリングプロファイ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	**timer** {**guard** *seconds* | **hold-off** *seconds* | **wtr** *minutes*} 例：	ガード、hold-off、および wait-to-restore（WTR）タイマーの間隔を指定します。

	コマンドまたはアクション	目的
	`Device(config-erp-profile)# timer hold-off 5`	
ステップ 5	**non-revertive** 例： `Device(config-erp-profile)# non-revertive`	非リバーティブ イーサネット リング インスタンスを指定します。 • デフォルトでは、イーサネット リング インスタンスはリバーティブです。
ステップ 6	**end** 例： `Device(config-erp-profile)# end`	ユーザ EXEC モードに戻ります。

イーサネット CFM MEP の設定

イーサネット接続障害管理（CFM）メンテナンスエンドポイント（MEP）の設定は任意ですが、高速障害検出と CFM モニタリングの観点から推奨されます。CFM モニタリングを設定する場合は、次の点に注意してください。

- スタティックリモート MEP（RMEP）チェックを有効にする必要があります。
- イーサネット障害検出を有効にするように MEP を設定する必要があります。

イーサネット接続障害管理（CFM）メンテナンスエンドポイント（MEP）の設定については、『*Carrier Ethernet Configuration Guide*』の「Configuring Ethernet Connectivity Fault Management in a Service Provider Network」モジュールを参照してください。

サービスのイーサネット障害検出のイネーブル化

サービスのイーサネット障害検出（EFD）をイネーブル化して高速コンバージェンスを実現するには、次の手順を実行します。

（注） リンク保護は RSP3 モジュールではサポートされていません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ethernet cfm global**
4. **ethernet cfm domain***domain-name* **level** *level-id* [**direction outward**]
5. **service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [**port** | **vlan** *vlan-id* [**direction down**]]
6. **continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**]

7. **efd notify g8032**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**ethernet cfm global** 例： `Device(config)# ethernet cfm global`	イーサネット CFM をグローバルにイネーブル化します。
ステップ 4	**ethernet cfm domain***domain-name* **level** *level-id* [**direction outward**] 例： `Device(config)# ethernet cfm domain G8032 level 4`	ODU 1 の CFM ドメインを設定し、イーサネット CFM 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	**service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [**port** | **vlan** *vlan-id* [**direction down**]] 例： `Device(config-ecfm)# service 8032_service evc 8032-evc vlan 1001 direction down`	ODU 1 のメンテナンス アソシエーションを定義し、イーサネット CFM サービス インスタンス コンフィギュレーション モードを開始します。
ステップ 6	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] 例： `Device(config-ecfm-srv)# continuity-check interval 3.3ms`	連続性チェック メッセージ（CCM）の送信をイネーブルにします。
ステップ 7	**efd notify g8032** 例： `Device(config-ecfm-srv)# efd notify g8032`	現在の障害アラーム プライオリティと一致する障害が検出またはクリアされたときに、登録されたプロトコルへの CFM による通知をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(config-ecfm-srv)# end`	ユーザ EXEC モードに戻ります。

イーサネット保護リングの設定

イーサネット保護リング（EPR）を設定する手順は、次のとおりです。

手順の概要

1. **enable**
2. **configure terminal**
3. **ethernet ring g8032** *ring-name*
4. **port0 interface** *type number*
5. **monitor service instance** *instance-id*
6. **exit**
7. **port1** {**interface***type number* | **none**}
8. **monitor service instance** *instance-id*
9. **exit**
10. **exclusion-list vlan-ids** *vlan-id*
11. **open-ring**
12. **instance** *instance-id*
13. **description** *descriptive-name*
14. **profile** *profile-name*
15. **rpl** {**port0** | **port1**} {**owner** | **neighbor** | **next-neighbor** }
16. **inclusion-list vlan-ids** *vlan-id*
17. **aps-channel**
18. **level** *level-value*
19. **port0 service instance** *instance-id*
20. **port1 service instance** {*instance-id* | **none** }
21. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**ethernet ring g8032** *ring-name* 例： `Device(config)# ethernet ring g8032 ring1`	イーサネットリングを指定し、イーサネット リング ポート 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	**port0 interface** *type number* 例： `Device(config-erp-ring)# port0 interface gigabitethernet 0/1/0`	インターフェイスのローカルノードのポート 0 をイーサネット リングに接続し、イーサネット リング保護モードを開始します。
ステップ 5	**monitor service instance** *instance-id* 例： `Device(config-erp-ring-port)# monitor service instance 1`	イーサネットサービスインスタンスを割り当てて、リング ポート（port0）をモニターし、リングの障害を検出します。
ステップ 6	**exit** 例： `Device(config-erp-ring-port)# exit`	イーサネット リング ポート コンフィギュレーション モードを終了します。
ステップ 7	**port1** {**interface***type* *number* | **none**} 例： `Device(config-erp-ring)# port1 interface gigabitethernet 0/1/1`	インターフェイスのローカルノードのポート 1 をイーサネットリングに接続し、イーサネットリング保護モードを開始します。
ステップ 8	**monitor service instance** *instance-id* 例： `Device(config-erp-ring-port)# monitor service instance 2`	イーサネットサービスインスタンスを割り当てて、リングポート（port1）をモニターし、リングの障害を検出します。 • ポート 1 が接続されているインターフェイスは、メインインターフェイスのサブインターフェイスである必要があります。
ステップ 9	**exit** 例： `Device(config-erp-ring-port)# exit`	イーサネット リング ポート コンフィギュレーション モードを終了します。
ステップ 10	**exclusion-list vlan-ids** *vlan-id* 例：	イーサネットリング保護メカニズムによって保護されていない VLAN を指定します。

	コマンドまたはアクション	目的
	`Device(config-erp-ring)# exclusion-list vlan-ids 2`	
ステップ 11	**open-ring** 例： `Device(config-erp-ring)# open-ring`	開いたリングとしてイーサネットリングを指定します。デフォルトでは、イーサネットリング上の各ノードは閉じています。ITU-T G.8032 イーサネットの開いたリングの各ノードで、**open-ring** コマンドを設定する必要があります。
ステップ 12	**instance** *instance-id* 例： `Device(config-erp-ring)# instance 1`	イーサネット リング インスタンスを設定し、イーサネット リング インスタンス コンフィギュレーション モードを開始します。
ステップ 13	**description** *descriptive-name* 例： `Device(config-erp-inst)# description cisco_customer_instance`	イーサネット リング インスタンスに対して説明的な名前を指定します。
ステップ 14	**profile** *profile-name* 例： `Device(config-erp-inst)# profile profile1`	イーサネット リング インスタンスに関連付けるプロファイルを指定します。
ステップ 15	**rpl** {**port0** | **port1**} {**owner** | **neighbor** | **next-neighbor** } 例： `Device(config-erp-inst)# rpl port0 neighbor`	RPL オーナー、ネイバー、または次のネイバーとしてローカルノードのイーサネットリングポートを指定します。
ステップ 16	**inclusion-list vlan-ids** *vlan-id* 例： `Device(config-erp-inst)# inclusion-list vlan-ids 11`	イーサネットリング保護メカニズムによって保護されている VLAN を指定します。 （注） VLAN は、インターフェイスで設定されている VLAN の内部または同じである必要があります。
ステップ 17	**aps-channel** 例： `Device(config-erp-inst)# aps-channel`	イーサネット リング インスタンス aps-channel コンフィギュレーション モードを開始します。
ステップ 18	**level** *level-value* 例：	イーサネットリング上のノードの自動保護スイッチング（APS）メッセージレベルを指定します。

	コマンドまたはアクション	目的
	`Device(config-erp-inst-aps)# level 5`	• イーサネットリング内のすべてのノードは、同じレベルに設定する必要があります。
ステップ 19	**port0 service instance** *instance-id* 例： `Device(config-erp-inst-aps)# port0 service instance 100`	APS チャネル情報を port0 に関連付けます。
ステップ 20	**port1 service instance** {*instance-id* | **none** } 例： `Device(config-erp-inst-aps)# port1 service instance 100`	APS チャネル情報を port1 に関連付けます。
ステップ 21	**end** 例： `Device(config-erp-inst-aps)# end`	ユーザ EXEC モードに戻ります。

トポロジ変更通知の伝達の設定

トポロジ変更通知（TCN）の伝達を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ethernet tcn-propagation G8032 to {REP | G8032}**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**ethernet tcn-propagation G8032 to {REP | G8032}** 例： `Device(config)# ethernet tcn-propagation G8032 to G8032`	送信元プロトコルから宛先プロトコルへのトポロジ変更通知（TCN）の伝達を許可します。 • 送信元プロトコルと宛先プロトコルは、プラットフォームやリリースによって異なります。
ステップ 4	**end** 例： `Device(config)# end`	ユーザ EXEC モードに戻ります。

サービス インスタンスの設定

サービスインスタンスを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *instance-id* **ethernet** [*evc-id*]
5. **encapsulation dot1q** *vlan-id* [**native**]
6. **bridge-domain** *bridge-id* [**split-horizon** [**group** *group-id*]]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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** *type number* 例： `Device(config)# interface gigabitethernet 0/1/0`	インターフェイス タイプおよび番号を指定します。

	コマンドまたはアクション	目的
ステップ 4	**service instance** *instance-id* **ethernet** [*evc-id*] 例： `Device(config-if)# service instance 101 ethernet`	インターフェイス上でサービスインスタンス（EVC のインスタンス）を作成し、サービスインスタンス コンフィギュレーション モードを開始します。
ステップ 5	**encapsulation dot1q** *vlan-id* [**native**] 例： `Device(config-if-srv)# encapsulation dot1q 13`	インターフェイス上の入力 dot1q フレームを、適切なサービスインスタンスにマッピングするために使用する照合基準を定義します。
ステップ 6	**bridge-domain** *bridge-id* [**split-horizon** [**group** *group-id*]] 例： `Device(config-if-srv)# bridge-domain 12`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。
ステップ 7	**end** 例： `Device(config-if-srv)# end`	サービスインスタンス コンフィギュレーション モードを終了します。

イーサネットリング保護（ERP）スイッチング設定の確認

ERP スイッチング設定を確認するには、以下のコマンドを任意に使用します。順番はありません。

（注） 包含リストで VLAN を追加または削除する場合は、次のルールに従ってください。

- VLAN を包含リストに追加する場合は、まずインターフェイスに追加してから、G.8032 包含リストに追加する必要があります。
- 包含リストから VLAN を削除する場合は、G.8032 包含リストから削除した後に、インターフェイスから削除する必要があります。

除外リストでの VLAN の追加または削除はサポートされていません。

手順の概要

1. **enable**
2. **show ethernet ring g8032 status** [*ring-name*] [**instance** [*instance-id*]]
3. **show ethernet ring g8032 brief** [*ring-name*] [**instance** [*instance-id*]]
4. **show ethernet ring g8032 summary**
5. **show ethernet ring g8032 statistics** [*ring-name*] [**instance** [*instance-id*]]

6. **show ethernet ring g8032 profile** [*profile-name*]
7. **show ethernet ring g8032 port status interface** [*type number*]
8. **show ethernet ring g8032 configuration** [*ring-name*] **instance** [*instance-id*]
9. **show ethernet ring g8032 trace** {**ctrl** [*ring-name* **instance** *instance-id*] | **sm**}
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**show ethernet ring g8032 status** [*ring-name*] [**instance** [*instance-id*]] 例： `Device# show ethernet ring g8032 status RingA instance 1`	ERP インスタンスのステータスの概要を表示します。
ステップ 3	**show ethernet ring g8032 brief** [*ring-name*] [**instance** [*instance-id*]] 例： `Device# show ethernet ring g8032 brief`	ERP インスタンスの機能状態の簡単な説明を表示します。
ステップ 4	**show ethernet ring g8032 summary** 例： `Device# show ethernet ring g8032 summary`	ERP スイッチングプロセスの各状態の ERP インスタンス数を概略表示します。
ステップ 5	**show ethernet ring g8032 statistics** [*ring-name*] [**instance** [*instance-id*]] 例： `Device# show ethernet ring g8032 statistics RingA instance 1`	ERP インスタンスについて受信したイベントおよびリング自動保護スイッチング（R-APS）メッセージの数を表示します。
ステップ 6	**show ethernet ring g8032 profile** [*profile-name*] 例： `Device# show ethernet ring g8032 profile gold`	1 つ以上の ERP プロファイルの設定を表示します。
ステップ 7	**show ethernet ring g8032 port status interface** [*type number*] 例：	インターフェイスのイーサネットリングポートのステータス情報を表示します。

	コマンドまたはアクション	目的
	`Device# show ethernet ring g8032 port status interface  gigabitethernet 0/0/1`	
ステップ 8	**show ethernet ring g8032 configuration** [*ring-name*] **instance** [*instance-id*] 例： `Device# show ethernet ring g8032 configuration RingA instance 1`	ERP インスタンス設定マネージャの詳細を表示します。
ステップ 9	**show ethernet ring g8032 trace** {**ctrl** [*ring-name* **instance** *instance-id*] | **sm**} 例： `Device# show ethernet ring g8032 trace sm`	ERP トレースに関する情報を表示します。
ステップ 10	**end** 例： `Device# end`	特権 EXEC モードに戻ります。

ITU-T G.8032 イーサネットリング保護スイッチングの設定例

例：イーサネットリング保護スイッチングの設定

イーサネットリング保護（ERP）スイッチングの設定例を以下に示します。

```
ethernet ring g8032 profile profile_ABC
 timer wtr 1
 timer guard 100
 timer hold-off  1

ethernet ring g8032 major_ring_ABC
 exclusion-list vlan-ids 1000
 port0 interface  GigabitEthernet 0/0/1
  monitor service instance 103
 port1 interface  GigabitEthernet 0/1/0
  monitor service instance 102
 instance 1
  profile profile_ABC
  rpl port0 owner
  inclusion-list vlan-ids 100
  aps-channel
   port0 service instance 100
   port1 service instance 100
  !
```

```
interface GigabitEthernet0/1/0
mtu 9216
 no ip address
 negotiation auto
 service instance trunk 1 ethernet
  encapsulation dot1q 60-61
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation

 !
!
```

例：サービスのイーサネット障害検出のイネーブル化

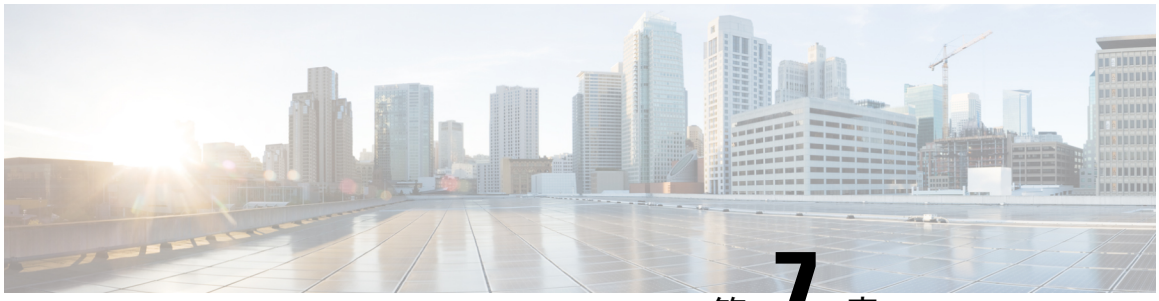
```
ethernet cfm domain G8032 level 4
service 8032_service evc 8032-evc vlan 1001 direction down
  continuity-check
  continuity-check interval 3.3ms
  offload sampling 1000
  efd notify g8032
ethernet ring g8032 profile TEST
timer wtr 1
timer guard 100
ethernet ring g8032 open
open-ring
port0 interface GigabitEthernet0/1/3
  monitor service instance 1001
port1 none
instance 1
  profile TEST
  inclusion-list vlan-ids 2-500,1001
  aps-channel
   port0 service instance 1001
   port1 none
  !
!
instance 2
  profile TEST
  rpl port0 owner
  inclusion-list vlan-ids 1002,1005-2005
  aps-channel
   port0 service instance 1002
   port1 none
  !

interface GigabitEthernet0/1/3
no ip address
load-interval 30
shutdown
negotiation auto
storm-control broadcast level 10.00
storm-control multicast level 10.00
storm-control unicast level 90.00
service instance 1 ethernet
  encapsulation untagged
  l2protocol peer lldp
  bridge-domain 1
!
service instance trunk 10 ethernet
  encapsulation dot1q 2-500,1005-2005
  rewrite ingress tag pop 1 symmetric
```

```
  bridge-domain from-encapsulation
!
service instance 1001 ethernet 8032-evc
  encapsulation dot1q 1001
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1001
  cfm mep domain G8032 mpid 20
!
service instance 1002 ethernet 8032-evc-1
  encapsulation dot1q 1002
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1002
!
End
```

例：イーサネットリング保護の設定の確認

次に、**show ethernet ring g8032 configuration** コマンドの出力例を示します。このコマンドを使用して、入力した設定が有効かどうかを確認するとともに、未設定のパラメータの有無を確認します。

```
Device# show ethernet ring g8032 configuration

ethernet ring ring0
 Port0: GigabitEthernet0/0/0 (Monitor: GigabitEthernet0/0/0)
 Port1: GigabitEthernet0/0/4 (Monitor: GigabitEthernet0/0/4)
 Exclusion-list VLAN IDs: 4001-4050
 Open-ring: no
 Instance 1
  Description:
  Profile:     opp
  RPL:
  Inclusion-list VLAN IDs: 2,10-500
  APS channel
   Level: 7
   Port0: Service Instance 1
   Port1: Service Instance 1
  State: configuration resolved
```



第 7 章

マルチ スパニングツリー プロトコル

マルチ スパニングツリープロトコル（MSTP）は、複数および独立したスパニングツリーを同じ物理ネットワークに作成できるようにするSTPバリアントです。各スパニングツリーのパラメータは、ループフリー トポロジを形成するために、ルート ブリッジとして別のネットワーク デバイスを選択するか、別のパスを選択するように、別個に設定できます。その結果、特定の物理インターフェイスを一部のスパニングツリーではブロックして、その他のツリーではブロック解除できます。

マルチ スパニングツリーを設定すると、使用中の VLAN セットをツリー間で分割できます。たとえば、VLAN 1 ～ 100 をスパニングツリー 1 に割り当てて、VLAN 101 ～ 200 をスパニングツリー 2 に割り当てて、VLAN 201 ～ 300 を VLAN 3 に割り当てることができます。各スパニングツリーには、異なるアクティブ リンクとの別のアクティブ トポロジがあるため、VLAN に基づいて、利用可能な冗長リンク間でデータ トラフィックを分割できます（ロード バランシングの実行）。

MSTP の設定に関する制約事項

- RSTP はサポートされません。MSTP のインスタンスが作成されない場合は、RSTP をサポートするために、すべての VLAN が MSTI 0 にマッピングされます。
- PVSTP はサポートされません。
- 16 個のインスタンスのみサポートします。
- タグなし EVC は、MST ループ検出には参加しません。

MST プロトコルの設定方法

ここでは、MSTP を設定する手順を説明します。

マルチ スパニング ツリー プロトコルのイネーブル化

デフォルトでは、MSTP はすべてのインターフェイスでディセーブルになっています。各インターフェイスで MSTP を明示的にイネーブルにする必要はありません。グローバル設定をオンにすると、すべてのインターフェイスでイネーブル化されます。

複数のスパニング ツリー プロトコルの設定

MST の設定手順について説明します。

手順の概要

1. **configure**
2. **spanning-tree mode mst**
3. **spanning-tree mst configuration**
4. **instance** *vlan-id* **vlan** *vlan-range*
5. **name** *region*
6. **revision** *revision -number*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `Device> configure`	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	**spanning-tree mode mst** 例： `Device> spanning-tree mode mst`	MSTP コンフィギュレーション モードをイネーブルにします。
ステップ 3	**spanning-tree mst configuration** 例： `Device(config)#spanning-tree mst configuration`	MSTP コンフィギュレーション サブモードを開始します。
ステップ 4	**instance** *vlan-id* **vlan** *vlan-range* 例： `Device(config-mstp-inst)# instance 1 vlan 450-480`	VLAN を MST インスタンスにマッピングします。
ステップ 5	**name** *region* 例： `Device(config-mstp)# name m1`	MSTP 領域の名前を設定します。
ステップ 6	**revision** *revision -number* 例：	MSTP 領域のリビジョン レベルを設定します。

	コマンドまたはアクション	目的
	`Device(config-mstp)#)revision 1`	
ステップ 7	**end** 例： `Device(config-mstp-if)# end`	特権 EXEC モードに戻ります。

MST インターフェイスでのタグなし EFP の設定

MST でのタグなし EFP を設定する手順について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface number*
4. **no ip address**
5. **service instance** *number* **ethernet** *[name]*
6. **bridge-domain** *bridge-id*
7. **encapsulation untagged dot1q** {any|vlan-id [,vlan-id [-vlan-d]]}
8. **l2protocol peer stp**
9. **end**

手順の詳細

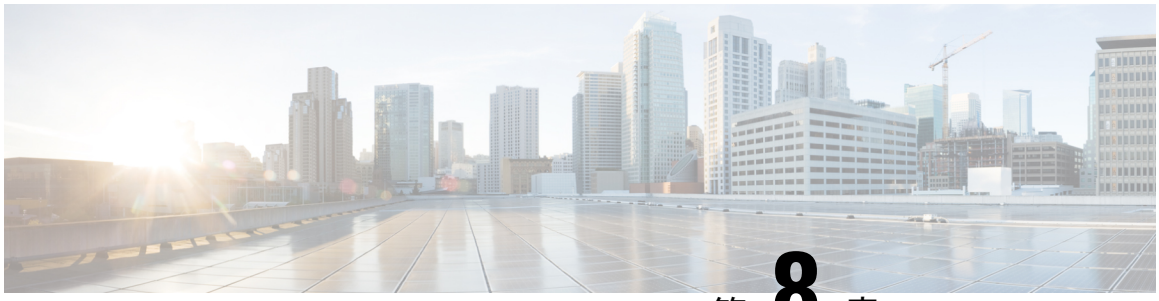
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface number* 例： `Router(config)# interface gigabitEthernet 0/0/5`	設定するギガビット イーサネット インターフェイスを指定します。slot/subslot/port：インターフェイスの場所を指定します。
ステップ 4	**no ip address** 例： `Router (config-if)# no ip address`	インターフェイスの IP アドレスをディセーブルにします。
ステップ 5	**service instance** *number* **ethernet** *[name]* 例： `Router (config-if)#service instance 200 ethernet`	EFP（サービスインスタンス）を設定し、サービス インスタンス 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 6	**bridge-domain** *bridge-id* 例： `Router (config-if-srv)# bridge-domain from-encapsulation`	カプセル化VLAN番号から取得したブリッジドメイン ID を使用して、EFP トランク ポートのブリッジドメインリストを作成します。
ステップ 7	**encapsulation untagged dot1q** {any|vlan-id [,vlan-id [-vlan-d]]} 例： `Router (config-if-srv)# encapsulation dot1q 20`	カプセル化を設定します。インターフェイスの入力 dot1q またはタグなしフレームを適切なサービスインスタンスにマッピングする一致基準を定義します。
ステップ 8	**l2protocol peer stp** 例： `Router (config-if-srv)# l2protocol peer stp`	EFPサービスインスタンスが設定されたポート上のネイバーとピアリングするようSTPを設定します。
ステップ 9	**end** 例： `Device(config-mstp-if)# end`	特権 EXEC モードに戻ります。

設定例

サービスインスタンス上のネイバーとピアリングするよう STP を設定する方法の例を以下に示します。

```
interface GigabitEthernet0/0/0
no ip address
negotiation auto
service instance trunk 10 ethernet
  encapsulation dot1q 10-20
  bridge-domain from-encapsulation
!
service instance 1024 ethernet
  encapsulation untagged
  l2protocol peer stp
  bridge-domain 1024
!
end
```



第 8 章

PVST+ および RPVST+ の設定

この章では、シスコルータのポートベースのVLANにスパニングツリープロトコル（STP）を設定する方法について説明します。このルータは、IEEE 802.1D 標準に準拠した Per-VLAN Spanning-Tree plus（PVST+）とシスコ独自の拡張機能の組み合わせか、もしくは IEEE 802.1w 標準に準拠した Rapid Per-VLAN Spanning-Tree plus（Rapid PVST+）プロトコルを使用できます。

マルチ スパニング ツリー プロトコル（MSTP）の詳細と、複数の VLAN を同じスパニングツリー インスタンスにマッピングする方法については、「マルチ スパニング ツリー プロトコル」の章を参照してください。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

（注） この機能は、Cisco NCS 4201 および NCS 4202 でのみ使用できます。

STP の概要

STP は、ネットワーク上でループを防止しながら、パスの冗長性を実現するレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークの正常な動作を実現するには、どの 2 つのステーション間でもアクティブ パスを 1 つにする必要があります。エンド ステーション間に複数のアクティブ パスがあると、ネットワーク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。また、スイッチも複数のレイヤ 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が出てきます。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スイッチを 1 つ選択します。スパニングツリー アルゴリズムは、アクティブ トポロジでのポートの役割に基づいて各ポートに役割を割り当てることにより、スイッチド レイヤ 2 ネットワーク上で最良のループフリー パスを算出します。

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

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。スイッチは、定期的にブリッジ プロトコル データ ユニット（BPDU）と呼ばれるスパニングツリー フレームを送受信します。スイッチはこのフレームを転送しませんが、このフレームを使用してループフリー パスを構築します。BPDU には、送信側スイッチおよびそのポートについて、スイッチおよび MAC アドレス、スイッチ 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 スイッチおよびルート 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。

スイッチの 2 つのポートがループの一部になっている場合、スパニングツリー ポート プライオリティとパス コストの設定値によって、どちらのポートをフォワーディング ステートにするか、どちらをブロッキング ステートにするかが制御されます。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。パス コストの値は、メディアの速度を表します。

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。

- 各スイッチのそれぞれの VLAN に対応付けられた一意のブリッジ ID（スイッチ プライオリティおよび MAC アドレス）
- ルート スイッチに対するスパニングツリー パス コスト。
- 各レイヤ 2 STP 対応インターフェイスに関連付けられたポート ID（ポート プライオリティおよび MAC アドレス）

ネットワーク内のスイッチに電源が投入されると、それぞれがルート スイッチとして機能します。各スイッチは、自身のすべてのポートのうち STP 対応ポートだけを介して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。各コンフィギュレーション BPDU には、次の情報が含まれます。

- 送信側スイッチがルート スイッチと見なしたスイッチの固有ブリッジ ID
- ルートまでのスパニングツリー パス コスト
- 送信側スイッチのブリッジ 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

スイッチは、優位の情報（より小さいブリッジ ID、より低いパス コストなど）を格納したコンフィギュレーション BPDU を受信すると、そのポートのためにこの情報を保存します。スイッチは、この BPDU をルート ポートで受信した場合は、更新されたメッセージ付きで、自身が指定スイッチであるすべての接続 LAN に対して BPDU を転送します。

そのポートに対して現在保存されているものより下位の情報を格納したコンフィギュレーション BPDU を受信した場合は、BPDU は廃棄されます。スイッチが、下位 BPDU の送信元の LAN の指定スイッチである場合は、そのポート用に保存された最新情報を格納した 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 台のスイッチがルート スイッチ（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。

各 VLAN で、スイッチのプライオリティが最も高い（プライオリティ値が数値的に最も小さい）スイッチがルート スイッチとして選定されます。すべてのスイッチがデフォルトのプライオリティ（32768）で設定されている場合は、VLAN 内で最小の MAC アドレスを持つスイッチがルート スイッチになります。スイッチプライオリティ値は、「スイッチプライオリティ値および拡張システム ID」および「スパニングツリータイマー」の各表に示されるように、ブリッジ ID の最上位ビットを占めます。

- 各スイッチ（ルート スイッチを除く）に対して 1 つのルート ポートが選択されます。このポートは、スイッチによってパケットがルート スイッチに転送されるときに、最適なパス（最小コスト）を提供します。
- スイッチごとに、パス コストに基づいてルート スイッチまでの最短距離が計算されます。
- 各 LAN セグメントの指定スイッチが選定されます。指定スイッチでは、LAN からルート スイッチへのパケット転送の場合、パス コストが最小となります。指定スイッチが LAN に接続するポートのことを指定ポートと呼びます。

スイッチド ネットワーク上のすべての地点からルート スイッチ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、スイッチ プライオリティ、および拡張システム ID

IEEE 802.1D 規格では、各スイッチに一意のブリッジ識別子（ブリッジ ID）を設定する必要があります。この ID によってルート スイッチの選択が制御されます。各 VLAN は、PVST+ および Rapid PVST+ 搭載の異なる論理ブリッジと見なされるので、各スイッチは、設定されている VLAN ごとに異なるブリッジ ID を備えている必要があります。スイッチ上の各 VLAN には一意の 8 バイト ブリッジ ID が設定されます。最上位の 2 バイトはスイッチのプライオリティに使用し、残りの 6 バイトは、スイッチの MAC アドレスとなっています。

スイッチでは IEEE 802.1t スパニングツリー拡張機能がサポートされ、従来はスイッチ 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、スイッチに割り当てられる 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。表「スイッチプライオリティ値および拡張システム ID」に示すように、従来はスイッチ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 *4:* スイッチ プライオリティ値および拡張システム *ID*

スイッチ 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、スイッチ 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 スイッチ、セカンダリ ルート スイッチ、および VLAN のスイッチ 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、スイッチのプライオリティ値を変更すると、ルート スイッチ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。詳細については、「ルート スイッチの設定」、「セカンダリ ルート スイッチの設定」、および「VLAN のスイッチ プライオリティの設定」の各セクションを参照してください。

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。STP ポート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可能性があります。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スイッチの各レイヤ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。

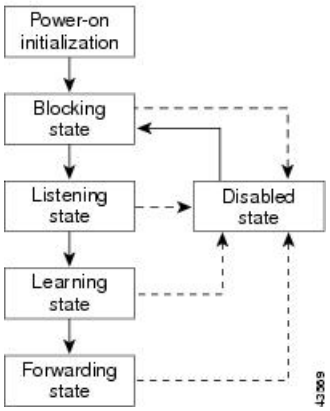
- ブロッキング：インターフェイスはフレーム転送に関与しません。
- リスニング：スパニングツリーでインターフェイスがフレーム転送に参加する必要があると判断された場合、ブロッキング ステートの次に最初に遷移するステート。
- ラーニング：インターフェイスはフレーム転送に関与する準備をしている状態です。
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：インターフェイスはスパニングツリーに含まれません。シャットダウン ポートであるか、ポート上にリンクがないか、またはポート上でスパニングツリー インスタンスが稼働していないためです。

スパニングツリーに参加するポートは、次の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

次の図は、インターフェイスがステート間をどのように移行するかを示します。

図 *12 :* スパニングツリー インターフェイス ステート



スパニングツリーはデフォルトでは有効になっていません。スパニングツリーモードが選択されると、ポート上の各 VLAN は、ブロッキングステートを経て、過渡的にリスニングおよびラーニングステートになります。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 アルゴリズムによってレイヤ 2 スパニングツリー インターフェイスがフォワーディング ステートになる場合には、次のプロセスが発生します。

1. インターフェイスをブロッキング ステートに遷移させるプロトコル情報をスパニングツリーが待っている間、そのインターフェイスはリスニング ステートの状態です。
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 ステートで、スイッチがデータベース転送のためにエンド ステーションの位置情報を学習している間、インターフェイスはフレーム転送を引き続きブロックします。
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、スイッチの各インターフェイスにまたは各スイッチSTPポートにBPDUが送信されます。スイッチは最初、他のスイッチとBPDUを交換するまで、ルートとして動作します。このBPDU交換によって、ネットワーク上のどのスイッチがルート、つまりルートスイッチであるかが確立されます。ネットワークにスイッチが1台しかない場合は、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。スイッチの初期化後、スパニングツリーに参加しているインターフェイスは常にブロッキング 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。

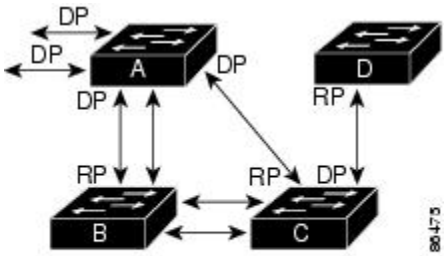
• インターフェイス上で受信したフレームを廃棄します。

- 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。

スイッチまたはポートがルート スイッチ 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スイッチがデフォルトのスパニングツリー設定でイネーブルになっている場合、最小の MAC アドレスを持つスイッチがルート スイッチになります。下図では、スイッチ A がルートスイッチとして選定されます（すべてのスイッチのスイッチプライオリティがデフォルト（32768）に設定されており、スイッチ A の MAC アドレスが最小であるため）。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、スイッチ A が最適なルートスイッチとは限りません。ルート スイッチになるように、最適なスイッチ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、最適なスイッチをルートとした新しいトポロジが形成されます。

図 *13 :* スパニングツリー トポロジ



RP = Root Port
DP = Designated Port

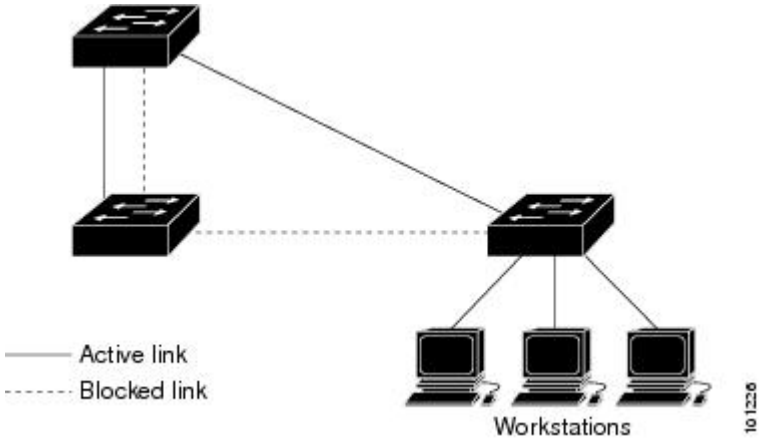
スパニングツリートポロジがデフォルトのパラメータに基づいて算出された場合、スイッチドネットワークの送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない場合があります。たとえば、ルートポートよりプライオリティの高いインターフェイスに高速リンクを接続すると、ルートポートが変更される可能性があります。最高速のリンクをルート ポートにすることが重要です。

たとえば、スイッチ B のあるポートがギガビットイーサネットリンクで、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

次の図に示すように、スパニングツリーに参加する2つのスイッチインターフェイスを別のデバイス、または2台の異なるデバイスに接続することにより、スパニングツリーによる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 プライオリティとポート ID が加算され、値の小さいリンクがスパニングツリーによってディセーブルにされます。

図 *14* : スパニングツリーおよび冗長接続



EtherChannel グループを使用して、スイッチ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 モードおよびプロトコル

以下のスパニングツリーモードとプロトコルがサポートされます。

- 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+ はスイッチ上の各 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 つのルートスイッチがあります。このルート スイッチは、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スイッチに伝送します。このプロセスにより、各スイッチがネットワークに関する共通の情報を持つようになるので、ネットワーク トポロジが確実に維持されます。

- Rapid PVST+：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。Rapid PVST+ は、PVST+ と互換性があり

ます。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）、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+ に移行するのに、複雑な 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、（IEEE802.1 W に基づいて）RSTP の上で稼働します。これは、転送遅延をなくし、ルート ポートと指定ポートを迅速にフォワーディング ステートに移行することで、スパニングツリーの高速コンバージェンスに対応します。MSTP を稼働する場合、RSTP は必須です。

  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。詳細については、「マルチスパニング ツリー プロトコル」の章を参照してください。

  サポートされるスパニング ツリー インスタンスの数については、PVST+ および RPVST+ の制約事項 （104 ページ） を参照してください。

PVST+ および RPVST+ の制約事項

- PVST+ または Rapid PVST+ モードでは、スイッチは最大 128 のスパニングツリー インスタンスをサポートします。
- STP を実行するすべての EFP で **l2protocol peer stp** コマンドを設定する必要があります。

  l2protocol peer stp は、入力方向での STP BPDU の処理方法（ドロップまたはプロセス）に影響しますが、出力方向の STP BPDU には影響しません。ASR 920 ルータは、常に出力方向に STP BPDU を送信します。
- PortFast トランクは、グローバルモードではなくインターフェイスモードで設定した場合にのみ機能します。
- ルートガードは、グローバルモードではなくインターフェイスモードで設定した場合にのみ機能します。

スパニングツリーの相互運用性と下位互換性

次の表に、ネットワークでサポートされるスパニングツリーモード間の相互運用性と下位互換性を示します。

表 *5 : PVST+*、*MSTP*、および *Rapid PVST+* の相互運用性

	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（制限あり）	あり

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+ スイッチを複数の 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+ が稼働しているスイッチと PVST+ が稼働しているスイッチが存在する場合、Rapid PVST+ スイッチと PVST+ スイッチを別のスパニングツリー インスタンスに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 スイッチは Rapid PVST+ スイッチでなければなりません。PVST+ インスタンスでは、ルート スイッチは PVST+ スイッチでなければなりません。PVST+ スイッチはネットワークのエッジに配置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

次の表は、デフォルトのスパニングツリー設定を示しています。

表 *6 :* 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 のポートでイネーブルです。
スパニングツリー モード	ディセーブル
スイッチ 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 Mbps：4 100 Mbps：19 10 Mbps：100

PVST+ および RPVST+ の設定

機能	デフォルト設定
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 Mbps：4 100 Mbps：19 10 Mbps：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

PVST+ および RPVST+ の設定

スイッチは、MSTP、PVST+、Rapid PVST+ の 3 つのスパニングツリーモードをサポートします。

（注） デフォルトでは、スパニングツリーはディセーブルです。

スパニングツリーモードを設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **spanning-tree mode** {**pvst** | **rapid-pvst**
3. **spanning-tree vlan** *vlan-range*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	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	**spanning-tree mode** {**pvst**	**rapid-pvst**	スイッチの STP ポート でスパニングツリー 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。 • rapid PVST+ をイネーブルにするには、**rapid-pvst** を選択します。

	コマンドまたはアクション	目的
ステップ 3	**spanning-tree vlan** *vlan-range*	指定した VLAN 範囲で STP を設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

EFP/TEFP での STP ピアの設定

EFP/TEFP での L2 プロトコルピアを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface TenGigabitEthernet***slot/subslot/port*
3. **no ip address**
4. **service instance trunk** *trunk id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **rewrite ingress tag pop 1 symmetric**
7. **l2protocol peer stp**
8. **bridge-domain from encapsulation**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： router#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 TenGigabitEthernet***slot/subslot/port* 例： router(config)#interface TenGigabitEthernet0/0/27	設定するギガビット イーサネット インターフェイスを指定します。 slot/subslot/port：インターフェイスの場所を指定します。
ステップ 3	**no ip address** 例： router(config-if)#no ip address	インターフェイスの IP アドレスをディセーブルにします。
ステップ 4	**service instance trunk** *trunk id* **ethernet** 例： router(config-if)#service instance trunk 1 ethernet	インターフェイスでイーサネット サービス インスタンスを設定し、イーサネット サービス 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 5	**encapsulation dot1q** *vlan-id* 例： router(config-if-srv)#encapsulation dot1q 1-100	インターフェイスの 802.1Q フレーム入力を適切なサービスインスタンスにマップするための一致基準を定義します。
ステップ 6	**rewrite ingress tag pop 1 symmetric** 例： router(config-if-serve)#rewrite ingress tag pop 1 symmetric	サービスインスタンスに入るフレームで実行されるカプセル化調整を指定します。
ステップ 7	**l2protocol peer stp** 例： router(config-if-srv)#l2protocol peer stp	EFP サービスインスタンスが設定されたポート上のネイバーとピアリングするよう STP を設定します。
ステップ 8	**bridge-domain from encapsulation** 例： router(config-if-srv)#bridge-domain from encapsulation	インターフェイスで EFP のサポートを設定します。
ステップ 9	**end** 例： router(config-ip)# end	特権 EXEC モードに戻ります。

（注） STP を実行するすべての EFP で **l2protocol peer stp** コマンドを設定する必要があります。

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。

VLAN 単位でスパニングツリーをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **no spanning-tree vlan** *vlan-id*
3. **end**

4. **show spanning-tree vlan** *vlan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no spanning-tree vlan** *vlan-id*	*vlan-id* に指定できる範囲は 1 ～ 4094 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	入力内容を確認します。

スパニングツリーを再びイネーブルにするには、**spanning-tree vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。

PVST/RPVST 設定の確認

次のコマンドを使用して、PVST および RPVST の設定を確認します。

```
router#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     a89d.21ed.bbbd
             Cost        6
             Port        18 (GigabitEthernet0/0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     b0aa.7754.553d
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  0   sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0/7             Altn BLK 4         128.14   P2p
Gi0/0/11            Root FWD 4         128.18   P2p


router#show spanning-tree interface gigabitEthernet 0/0/7 detail

Port 14 (GigabitEthernet0/0/7) of VLAN0001 is alternate blocking
Port path cost 4, Port priority 128, Port Identifier 128.14.
Designated root has priority 32769, address a89d.21ed.bbbd
Designated bridge has priority 32769, address b0aa.7737.9dbd
Designated port id is 128.14, designated path cost 4
Timers: message age 4, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 91, received 8394
```

```
router#show spanning-tree summary

Switch is in pvst mode
Root bridge for: none
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
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    1         0        0          1          2
VLAN0002                    1         0        0          1          2
VLAN0003                    1         0        0          1          2
VLAN0004                    1         0        0          1          2
VLAN0005                    1         0        0          1          2
VLAN0006                    1         0        0          1          2
```

ルート スイッチの設定

スイッチは、スイッチ上で設定されているアクティブ VLAN ごとに 1 つずつ、個別のスパニングツリー インスタンスを維持します。各インスタンスには、スイッチ プライオリティとスイッチの MAC アドレスからなるブリッジ ID が対応付けられます。VLAN ごとに、ブリッジ ID が最小のスイッチがその VLAN のルート スイッチになります。

特定の VLAN でスイッチがルートになるように設定するには、 **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、スイッチプライオリティをデフォルト値（32768）からかなり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 スイッチのスイッチ プライオリティをチェックします。拡張システム ID をサポートするため、スイッチは指定された 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、このスイッチを指定された VLAN のルートに設定できます。

指定された VLAN のルートスイッチに 24576 に満たないスイッチプライオリティが設定されている場合、スイッチはその VLAN について、自身のプライオリティを最小のスイッチ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 スイッチ プライオリティの最下位ビットの値です。ページ 14-4 の表 14-1 を参照）。

（注） ルートスイッチとして設定する必要のある値が 1 未満の場合、**spanning-tree vlan** *vlan-id* **root** グローバル コンフィギュレーション コマンドは失敗します。

ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルート スイッチになることはほぼありません。拡張システム ID によって、旧ソフトウェアが稼働する接続スイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチ プライオリティ値が増大します。

（注） 各スパニングツリー インスタンスのルート スイッチは、バックボーン スイッチまたはディストリビューション スイッチにする必要があります。アクセス スイッチをスパニングツリーのプライマリ 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スイッチホップカウント）を指定するには、**diameter** キーワードを指定します。ネットワークの直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムをスイッチが自動的に設定するので、コンバージェンスの所要時間を大幅に短縮できます。**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） ルートスイッチとしてスイッチを設定した後で、**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。

スイッチが特定の VLAN のルートになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **spanning-tree vlan** *vlan-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]
3. **end**
4. **show spanning-tree detail**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**spanning-tree vlan** *vlan-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	指定された VLAN のルートになるように、スイッチを設定します。 • *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の最大スイッチ数を指定します。指定できる範囲は 2 ～ 7 です。

	コマンドまたはアクション	目的
		• （任意）**hello-time** *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 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree detail**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no spanning-tree vlan** *vlan-id* **root** グローバル コンフィギュレーション コマンドを使用します。

セカンダリ ルート スイッチの設定

スイッチをセカンダリ ルートとして設定すると、スイッチ 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。したがって、プライマリ ルート スイッチで障害が発生した場合に、このスイッチが指定された VLAN のルート スイッチになる可能性が高くなります。これは、他のネットワークスイッチがデフォルトのスイッチプライオリティ 32768 を使用し、ルートスイッチになる可能性が低いことが前提です。

複数のスイッチでこのコマンドを実行すると、複数のバックアップ ルート スイッチを設定できます。**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。

スイッチが特定の VLAN のセカンダリ ルートになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **spanning-tree vlan** *vlan-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]
3. **end**
4. **show spanning-tree detail**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**spanning-tree vlan** *vlan-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	指定された VLAN のセカンダリ ルートになるように、スイッチを設定します。 • *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の最大スイッチ数を指定します。指定できる範囲は 2 ～ 7 です。 •（任意）**hello-time** *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。「ルート スイッチの設定」を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree detail**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no spanning-tree vlan** *vlan-id* **root** グローバル コンフィギュレーション コマンドを使用します。

ポート プライオリティの設定

ループが発生すると、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 ステートにするスパニングツリー ポートを選択します。STP に最初に選択させたいポートには高いプライオリティ値（小さい数値）を、最後に選択させたいポートには低いプライオリティ値（大きい数値）を割り当てることができます。すべてのスパニングツリー ポートが同じプライオリティ値を持つ場合、スパニングツリーはインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにして、残り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 ポートのポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **spanning-tree port-priority** *priority*
4. **end**
5. 次のいずれかを実行します。
   - show spanning-tree interface *interface-id*
   - **show spanning-tree vlan** *vlan-id*
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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*	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。 （注） インターフェイスが VLAN である場合は、VLAN のスパニングツリーがイネーブルに設定されているポートだけがスパニングツリーを実行します。インターフェイスがポートチャネルである場合は、ポートチャネルのすべてのメンバーは、スパニングツリーがイネーブルに設定されている必要があります。
ステップ 3	**spanning-tree port-priority** *priority*	スパニングツリー ポートのポート プライオリティを設定します。 *priority* に指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	次のいずれかを実行します。 • show spanning-tree interface *interface-id* • **show spanning-tree vlan** *vlan-id*	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

（注） **show spanning-tree 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。

デフォルトのスパニングツリー設定に戻す場合は、**no spanning-tree** [**vlan** *vlan-id* **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と連動します（スパニングツリーを実行するポートまたはスパニングツリーを実行する複数のポートのポートチャネル）。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 NNI（またはポート チャネル）が同じコスト値を使用している場合、スパニングツリーはインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにして、残りのインターフェイスをブロックします。

インターフェイスのコストを設定するには、特権EXECモードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **spanning-tree cost** *cost*
4. **end**
5. 次のいずれかを実行します。
   - show spanning-tree interface *interface-id*
   - **show spanning-tree vlan** *vlan-id*
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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*	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、物理インターフェイ

	コマンドまたはアクション	目的
		ス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*）があります。
ステップ 3	**spanning-tree cost** *cost*	インターフェイスに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 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	次のいずれかを実行します。 • show spanning-tree interface *interface-id* • **show spanning-tree vlan** *vlan-id*	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

（注） **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。

デフォルト設定に戻す場合は、 **no spanning-tree** [**vlan** *vlan-id*] **cost** インターフェイス コンフィギュレーション コマンドを使用します。

VLAN のスイッチ プライオリティの設定

スイッチ プライオリティを設定して、スイッチがルート スイッチに選出される可能性を高くできます。

（注） このコマンドの使用には注意してください。通常、スイッチのプライオリティを変更するには **spanning-tree vlan** *vlan-id* **root primary** および **spanning-tree vlan** *vlan-id* **root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

VLAN のスイッチ プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **spanning-tree vlan** *vlan-id* **priority** *priority*
3. **end**
4. **show spanning-tree vlan** *vlan-id*
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**spanning-tree vlan** *vlan-id* **priority** *priority*	VLAN のスイッチ 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* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。数値が小さいほど、スイッチがルート スイッチとして選択される可能性が高くなります。 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 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no spanning-tree vlan** *vlan-id* **priority** グローバル コンフィギュレーション コマンドを使用します。

スパニングツリー タイマーの設定

表 7: スパニングツリーのタイマー

変数	説明
ハロー タイマー	スイッチから他のスイッチへ hello メッセージをブロードキャストする頻度を制御します。
転送遅延タイマー	STP ポートが転送を開始するまでの、リスニング ステートおよびラーニング ステートが継続する時間を制御します。
最大エージング タイマー	STP ポートで受信したプロトコル情報が、スイッチに保管される時間を制御します。

hello タイムの設定

hello タイムを変更することによって、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設定できます。

（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、Hello タイムを変更することを推奨します。

VLAN の hello タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **spanning-tree vlan** *vlan-id* **hello-time** *seconds*
3. **end**
4. **show spanning-tree vlan** *vlan-id*
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**spanning-tree vlan** *vlan-id* **hello-time** *seconds*	VLAN の hello タイムを設定します。hello タイムはルート スイッチがコンフィギュレーション メッセージを生成する間隔です。これらのメッセージは、スイッチがアクティブであることを意味します。 • *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* の範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no spanning-tree vlan** *vlan-id* **hello-time** グローバル コンフィギュレーション コマンドを使用します。

VLAN の転送遅延時間の設定

VLAN の転送遅延時間を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **spanning-tree vlan** *vlan-id* **forward-time** *seconds*
3. **end**
4. **show spanning-tree vlan** *vlan-id*
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**spanning-tree vlan** *vlan-id* **forward-time** *seconds*	VLAN の転送時間を設定します。転送遅延は、スパニングツリーのラーニングおよびリスニング 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、スパニングツリー ポートが待機する秒数です。

	コマンドまたはアクション	目的
		• *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* の範囲は 4 ～ 30 で、デフォルトは 15 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no spanning-tree vlan** *vlan-id* **forward-time** グローバル コンフィギュレーション コマンドを使用します。

VLAN の最大エージング タイムの設定

VLAN の最大エージング タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順の概要

1. **configure terminal**
2. **spanning-tree vlan** *vlan-id* **max-age** *seconds*
3. **end**
4. **show spanning-tree vlan** *vlan-id*
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**spanning-tree vlan** *vlan-id* **max-age** *seconds*	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、再構成を試行するまでにスイッチがスパニングツリー コンフィギュレーション 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。

	コマンドまたはアクション	目的
		• *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 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show spanning-tree vlan** *vlan-id*	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no spanning-tree vlan** *vlan-id* **max-age** グローバル コンフィギュレーション コマンドを使用します。

スパニングツリー ステータスの表示

スパニングツリーステータスを表示するには、以下の特権 EXEC コマンドを任意に使用します。

表 *8* : スパニングツリー ステータス表示用のコマンド

コマンド	目的
show spanning-tree active	アクティブなスパニングツリー インターフェイスだけに関するスパニングツリー情報を表示します。
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*	特定のスパニングツリー 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 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。

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

show spanning-tree 特権 EXEC コマンドの他のキーワードについては、このリリースに対応するコマンドリファレンスを参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。