



## Resilient Ethernet Protocol

- [Resilient Ethernet Protocol](#) (1 ページ)
- [Resilient Ethernet Protocol Fast](#) (8 ページ)
- [REP ゼロタッチプロビジョニング](#) (10 ページ)
- [Resilient Ethernet Protocol の設定](#) (14 ページ)
- [Resilient Ethernet Protocol 設定の監視](#) (26 ページ)
- [Resilient Ethernet Protocol の機能履歴](#) (30 ページ)

## Resilient Ethernet Protocol

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



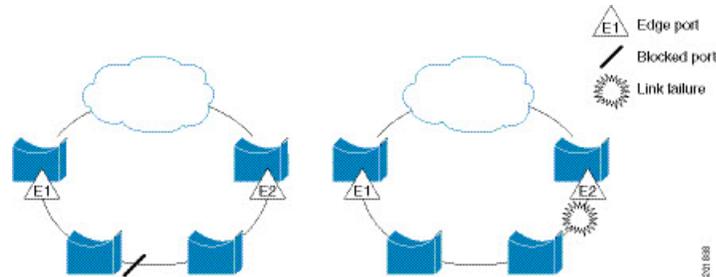
(注) REP は、Network Essentials ライセンスの Cisco Catalyst IE9300 高耐久性シリーズスイッチの Cisco IOS XE Cupertino 17.9.x 以降のリリースでサポートされています。

REP セグメントは相互接続されたポートのチェーンで、セグメント ID が設定されます。各セグメントは、標準 (非エッジ) セグメントポートと、2つのユーザ設定のエッジポートで構成されています。1 スイッチに、同じセグメントに属することができるポートは2つまでで、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、トランクポート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な場合、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。ブロックされたポートは、代替ポート (ALTポート) とも呼ばれます。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転送状態に戻り、ネットワークの中断を最小限に抑えます。

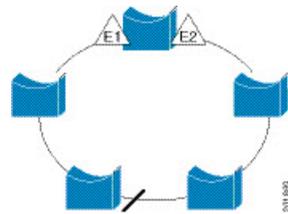
図 1: REP オープンセグメント



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。セグメント内のスイッチ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 ALT 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とも呼ばれるクローズドセグメントで、同じルータ上に両方のエッジポートがあります。この設定を使用すると、セグメント内の任意の2ルータ間で冗長接続を形成することができます。

図 2: REP リングセグメント



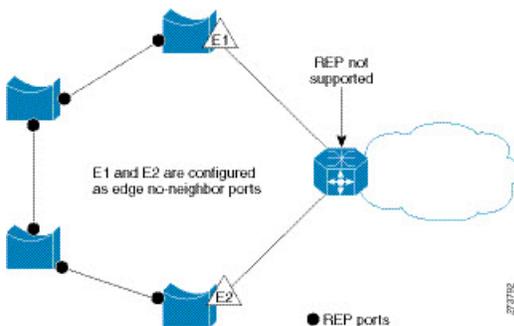
REP セグメントには、次のような特徴があります。

- セグメント内の全ポートが動作可能な場合、1ポート（ALT ポートと呼ばれる）が各 VLAN でブロック状態となります。VLAN 負荷分散が設定されている場合は、セグメント内の2つの ALT ポートが VLAN のブロック状態を制御します。
- ポートが動作不能になり、リンク障害が発生すると、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。

アクセスリングトポロジでは、次の図に示すように、ネイバースイッチで REP がサポートされない場合があります。この場合、そのスイッチ側のポート（E1 と E2）を非ネイバークエッジポートとして設定できます。非ネイバークエッジポートは、STP トポロジ変更通知（TCN）をアグリゲーションスイッチに送信するように設定できます。

図 3: 非ネイバークエッジポート



REP には次のような制限事項があります。

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

## リンク完全性

REP は、リンク完全性の確認にエッジポート間でエンドツーエンドポーリング機能を使用しません。ローカルリンク障害検出を実装しています。REP リンクステータスレイヤ（LSL）が REP 対応ネイバークを検出して、セグメント内の接続性を確立します。ネイバークが検出されるまで、インターフェイス上ですべての VLAN がブロックされます。ネイバークが特定されたあと、REP が代替ポートとなるネイバークポートと、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、スパンニングツリーアルゴリズムで使用されるものと類似しており、ポート番号（ブリッジ上で一意）と、関連 MAC アドレス（ネットワーク内で一意）から構成されます。セグメントポートが起動すると、ポートの LSL がセグメント ID およびポート ID を含むパケットの送信を開始します。ポートは、同じセグメント内のネイバークとのスリーウェイハンドシェイクを実行したあとで、動作可能と宣言されます。

次のような場合、セグメントポートは動作可能になりません。

- ネイバークに同じセグメント ID がない
- 複数のネイバークに同じセグメント ID がある

- ネイバーがピアとして、ローカルポートに確認応答しない

各ポートは、直近のネイバーと隣接関係を確立します。ネイバーとの隣接関係が確立されると、代替ポートとして機能する、セグメントのブロックされたポートを決定するようにポートが相互にネゴシエートします。その他のすべてのポートのブロックは解除されます。デフォルトでは、REP パケットはブリッジプロトコルデータユニットクラスの MAC アドレスに送信されます。パケットは、シスコマルチキャストアドレスにも送信されますが、セグメントに障害が発生した場合にブロックされたポートのアドバタイズ (BPA) メッセージの送信だけに使用されます。パケットは、REP が動作していない装置によって廃棄されます。

## 高速コンバージェンス

REP は、物理リンク ベースで動作し、VLAN 単位ベースでは動作しません。すべての VLAN に対して 1 つの hello メッセージしか必要ないため、プロトコル上の負荷が軽減されます。指定セグメント内の全スイッチで一貫して VLAN を作成し、REP トランク ポート上に同じ許容 VLAN を設定することを推奨します。ソフトウェアでのメッセージのリレーによって発生する遅延を回避するために、REP ではいくつかのパケットを通常マルチキャストアドレスにフラッドリングします。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ドリングされます。セグメントに属していないスイッチは、これらのメッセージをデータトラフィックとして扱います。ドメイン全体または特定のセグメントの管理 VLAN を設定することで、これらのメッセージのフラッドリングを制御することができます。

## VLAN 負荷分散

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 負荷分散に常に参加しているのがプライマリ エッジポートです。REP VLAN バランシングは、設定された代替ポートでいくつかの VLAN をブロックし、プライマリ エッジポートでその他の全 VLAN をブロックすることで実行されます。VLAN 負荷分散を設定する際に、次の 3 種類の方法のいずれかを使用して代替ポートを指定できます。

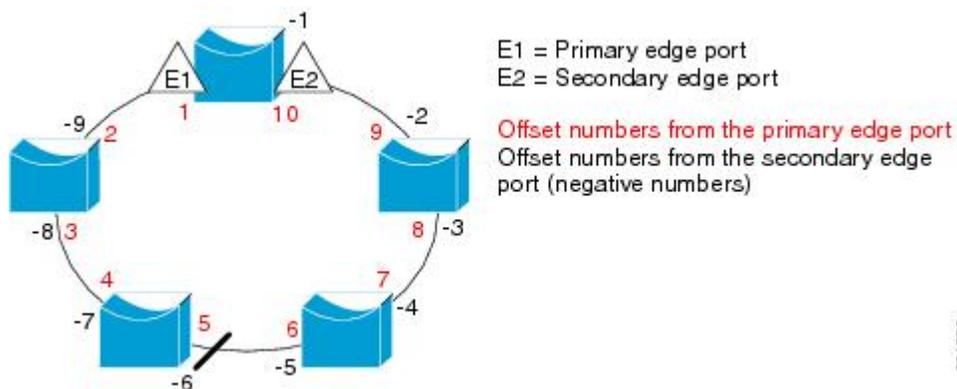
- インターフェイスにポート ID を入力します。セグメント内のポート ID を識別するには、ポートの **show interface rep detail** インターフェイス コンフィギュレーション コマンドを入力します。
- **preferred** キーワードを入力します。これにより、**rep segment segment-id preferred** インターフェイス コンフィギュレーション コマンドで優先代替ポートとしてすでに設定されているポートを選択します。
- セグメント内のポートのネイバー オフセット番号を入力します。これは、エッジポートの下流ネイバー ポートを識別するものです。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 エッジポートの下流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) とその下流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下流の位置を識別することで、プライマリエッジポートのオフセット番号を設定します。番号1はプライマリエッジポートのオフセット番号なので、オフセット番号1は入力しないでください。

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

図 4: セグメント内のネイバーオフセット番号



REP セグメントが完了すると、すべての VLAN がブロックされます。VLAN 負荷分散を設定する際には、次の 2 種類の方法のいずれかを使用して発動条件を設定する必要があります。

- プライマリエッジポートのあるスイッチ上で **rep preempt segment segment-id** 特権 EXEC コマンドを入力することで、いつでも手動で VLAN 負荷分散を発動することができます。
- **rep preempt delay seconds** インターフェイス コンフィギュレーション コマンドを入力すると、プリエンブション遅延時間を設定できます。リンク障害が発生して回復すると、設定されたプリエンブション期間の経過後に VLAN 負荷分散が開始されます。設定時間が経過する前に別のポートで障害が発生した場合、遅延タイマーが再開されることに注意してください。



- (注) VLAN 負荷分散が設定されている場合、手動での介入またはリンク障害および回復によって発動されるまで、動作が開始されません。

VLAN 負荷分散が発動されると、プライマリ エッジ ポートがメッセージを送信して、セグメント内の全インターフェイスにプリエンプションについて警告します。メッセージがセカンダリポートで受信されると、メッセージがネットワークに送信され、メッセージ内で指定された VLAN セットをブロックするように代替ポートに通知し、残りの VLAN をブロックするようにプライマリ エッジ ポートに通知します。

またすべての VLAN をブロックするために、セグメント内の特定ポートを設定できます。プライマリ エッジ ポートだけによって VLAN 負荷分散が開始され、セグメントが両端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 負荷分散設定を決定します。

負荷分散を再設定するには、プライマリ エッジ ポートを再設定します。負荷分散設定を変更すると、プライマリ エッジ ポートでは、**rep preempt segment** コマンドが実行されるか、ポート障害および復旧のあとで設定済みプリエンプト遅延期間が経過してから、新規設定が実行されます。エッジポートを通常セグメントポートに変更しても、既存の VLAN 負荷分散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。

## スパニングツリーとの相互作用

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

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

## Resilient Ethernet Protocol (REP) ネゴシエート



(注) REP ネゴシエートは、アップリンクポートでのみ機能します。

REP とスパニングツリープロトコル (STP) は、2つの異なるループ回避プロトコルです。REP には、コンバージェンス時間の点で STP よりも優れた点があります。REP は、リング内で単一のリンク障害が発生した場合に冗長経路を提供できるように、リングトポロジで動作するように設定できます。

シスコのスイッチは、デフォルトで STP が有効になっています。STP が有効になっているスイッチが (新しいノードの追加または既存のノードの交換のために) すでに実行中の REP リングに挿入されると、次の条件が適用されます。

- 新しいスイッチにより、REP リングが切断されます。

- 新しいスイッチは、REP リングの一部として設定されるまで、リングを介して通信できません。

REP ネゴシエート機能は、REP ステータスをピアとネゴシエートすることで、これらの問題を解決しようとします。次の表に、REP ネゴシエーションイベントが発動するタイミングと実行するアクションを示します。ここでは、両方のピアがネゴシエート中、いずれのピアもネゴシエートしていないという、2つのイベントがあります。

SELFREP をネゴシエート	PEERS REP をネゴシエート	発動されるイベント	動作
True	True	REPN	REP を設定
True	False	REPNN	STP を設定
False	X	REPNN	STP のまま

この機能は、3つの異なるプロトコルに依存して必要なデータを取得し、正しい設定を決定します。関連するさまざまなプロトコルとその目的を次に示します。

- **STP** : デフォルトでは、STP はシスコスイッチのすべてのポートで有効になっています。
- **REP** : カスタマーネットワークを設定して、コンバージェンス時間と冗長性改善のために REP リングを形成します。
- **Cisco Discovery Protocol (CDP)** : この機能は、CDP メッセージを介して送信されるユーザー定義の TLV に依存して、インターフェイスの正しい (STP または REP) 設定をネゴシエートします。

## REP ポート

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

- 標準セグメントポートとして設定されたポートは、障害ポートとして起動します。
- ネイバーとの隣接関係が確立されると、ポートは代替ポート状態に移行して、インターフェイス内の全 VLAN をブロックします。ブロックされたポートのネゴシエーションが実施され、セグメントが安定すると、1つのブロックされたポートが代替役に留まり、他のすべてのポートがオープンポートになります。
- リンク内で障害が発生すると、すべてのポートが障害状態に遷移します。代替ポートは、障害通知を受信すると、すべての VLAN を転送するオープン状態に遷移します。

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

スパニングツリー ポートとして再設定されたセグメント ポートは、スパニングツリー設定に従って再起動します。デフォルトでは、これは指定ブロッキング ポートです。PortFast が設定されていたり、STP が無効の場合、ポートは転送状態になります。

## Resilient Ethernet Protocol Fast

Resilient Ethernet Protocol (REP) Fast を使用すると、スイッチの銅線ギガビットイーサネット (GE) ポートでのリンク障害の検出とコンバージェンスを高速化できます。

REP は当初、ファストイーサネット (FE 10/100) ポート用に設計されました。ファイバ GE ポートでもリンクダウン検出時間は 10 ms ですが、GE 銅線インターフェイスでは、リンク喪失検出時間および回復時間が 750 ~ 350 ms となります。その結果、GE 光ファイバインターフェイスでは、対応する銅線インターフェイスよりもはるかに迅速にリンク損失と回復を検出できます。つまり、GE 銅線インターフェイスを使用すると、REP のコンバージェンス時間が大幅に長くなります。

リンクダウン検出時間を改善するため、REP インターフェイスが REP Fast モードに設定されている場合は、より高速なリンク障害検出 (5 ~ 10 ms 以内) を発動するビーコンメカニズムが実装されています。スイッチには、REP インターフェイスごとに 2 つのタイマーがあります。最初のタイマーは 3 ms ごとに開始され、ビーコンフレームをネイバーノードに送信します。フレームの送受信が成功すると、両方のタイマーがリセットされます。送信後にパケットが受信されない場合は、2 番目のタイマーが開始され、10ms 以内の受信を確認します。パケットが受信されない場合、タイマーの期限が切れたときにリンクダウンメッセージがスイッチに送信されます。

REP Fast は、個々のリンク単位で動作します。REP プロトコルには影響しません。REP Fast が機能するには、リンクの両端で REP Fast をサポートする必要があります。REP Fast は REP 用に設定された任意のインターフェイスリンクペアで使用できますが、もともとはギガビット銅線リンクの問題を解決するために作成されました。REP Fast によって、ギガビット銅線インターフェイスでのリンク障害検出がより迅速になります。

REP リングには、通常の REP リングと REP Fast リングを混在させることができます。REP Fast を使用するインターフェイスは、通常動作の一環として 1 秒間に 3,000 パケットを送信します。REP Fast を有効にしても設定されたインターフェイスのペアでのみ動作するため、REP リングサイズには影響しません。REP Fast はビーコンフレームを生成する必要があるため、1 台の REP ノード上で一度に REP Fast を設定できるインターフェイスは 6 つのみです。

ネイバーが確認応答し、REP Fast モードに設定された場合、50 ms 以内にコンバージェンスが発生します。ネイバースイッチが REP Fast 機能をサポートしていない場合は、通常の REP モードを使用してリンクのアップ/ダウンを検出する必要があります。この場合、リンクの両端で Fast モードを無効にする必要があります。

REP Fast の設定について詳しくは、このガイドの「[REP Fast の設定](#)」を参照してください。

## REP Fast の設定

REP Fast を設定するには、次の手順を実行します。

## 始める前に

「REP の設定」の説明に従って、スイッチで REP を有効にし、REP トポロジを設定します。

**ステップ 1** 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。

```
configure terminal
```

**ステップ 2** インターフェイスを指定してインターフェイス設定モードを開始します。

```
interface interface-id
```

**ステップ 3** REP Fast を有効にします。

```
REP fastmode
```

**ステップ 4** 特権 EXEC モードに戻ります。

```
end
```

## 例

```
gabitEthernet 1/0/1
switch-RJ(config-if)#rep seg
switch-RJ(config-if)#rep segment ?
<1-1024> Between 1 and 1024

switch-RJ(config-if)#rep segment 10
switch-RJ(config-if)#rep fastmode
switch(config)#int <interface number>
switch(config-if)#
switch(config-if)#rep ?
    fastmode      REP fastmode
switch (config-if)#rep fastmode ?
    <cr> <cr>

switch#sh run int <interface number>
Building configuration...

Current configuration : 89 bytes
!
interface <interface number>
    switchport mode trunk
    rep segment <segment id>
    rep fastmode
end
switch#

switch#sh run int <interface number>
Building configuration...

Current configuration : 89 bytes
!
interface <interface number>
    switchport mode trunk
    rep segment <segment id>
    rep fastmode
end
```

## REP ゼロタッチプロビジョニング

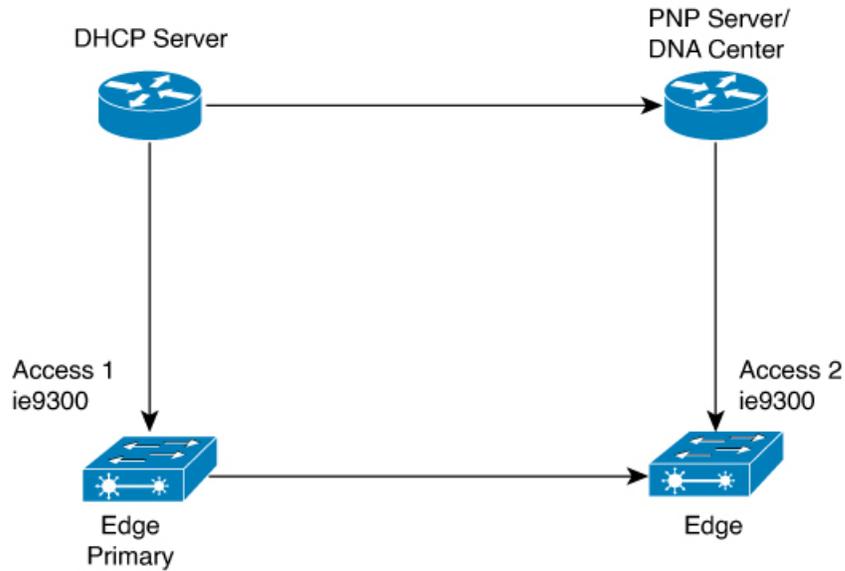
ルータやスイッチなどのネットワークデバイスをオンラインで展開して完全に機能させるには、事前にかかなりの量の手動による設定が必要です。ゼロタッチプロビジョニング (ZTP) テクノロジーによってこれらのプロセスが自動化され、手動による設定を最小限に抑えるか、まったく行うことなくネットワークデバイスを機能する状態へと立ち上げます。Cisco ネットワーク プラグアンドプレイ (PnP) および自動インストール デイゼロ ソリューションは、エンタープライズ ネットワークおよび産業用ネットワークを利用するお客様にシンプルかつセキュアなユニファイド/統合オフリングを提供することで、既存ネットワーク向けの更新のプロビジョニングにおけるデバイスのロールアウトを簡易化します。ただし、Resilient Ethernet Protocol (REP) の設計方法により、PnP は REP をサポートしません。REP ZTP 機能が導入される前は、デイゼロの REP リングプロビジョニングには手動による介入が必要でした。REP ZTP 機能によって REP LSL パケットに新しい Type-Length-Value (TLV) 拡張が導入され、ゼロタッチテクノロジーを使用した REP リングの設定をサポートします。

## REP およびデイゼロ

ZTP を使用した一般的なスイッチの展開では、NVRAM にスタートアップ コンフィギュレーションがないスイッチで Cisco Open Plug-n-Play (PnP) エージェントが起動し、DHCP 検出プロセスが開始されます。このプロセスでは、スイッチに必要な IP 設定を DHCP サーバーから取得します。DHCP サーバーは、DHCP メッセージでベンダー固有のオプション 43 を使用して追加情報を挿入するように設定できます。DHCP サーバーは、オプション 60 と文字列「cisco pnp」を含む DHCP DISCOVER メッセージをスイッチから受信すると、要求元のスイッチに PnP サーバーの IP アドレスまたはホスト名を送信します。スイッチが DHCP 応答を受信すると、PnP エージェントは応答からオプション 43 を抽出して、PnP サーバーの IP アドレスまたはホスト名を取得します。次に、スイッチ上の PnP エージェントは、PnP サーバーと通信するためにこの IP アドレスまたはホスト名を使用します。最後に、PnP サーバーは、プロビジョニングを完了するために必要なデイゼロ設定をスイッチにダウンロードします。

次の図は、REP ZTP を導入する前のデイゼロでの REP リングのプロビジョニング例を示しています。

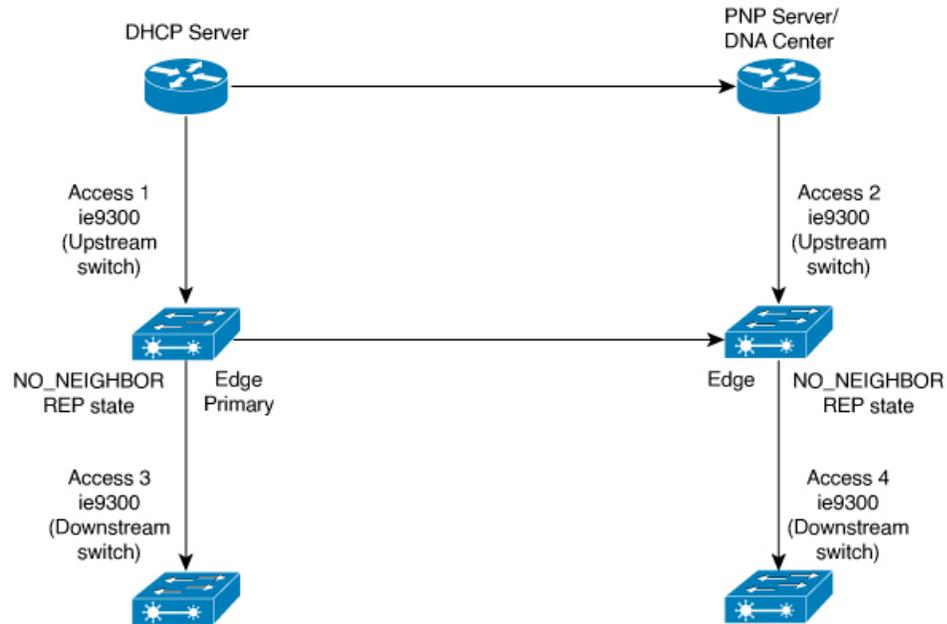
図 5: REP リングへのエッジノードの追加



(注) DHCP サーバーと PnP サーバー/Cisco DNA センターは、REP リングには含まれていません。

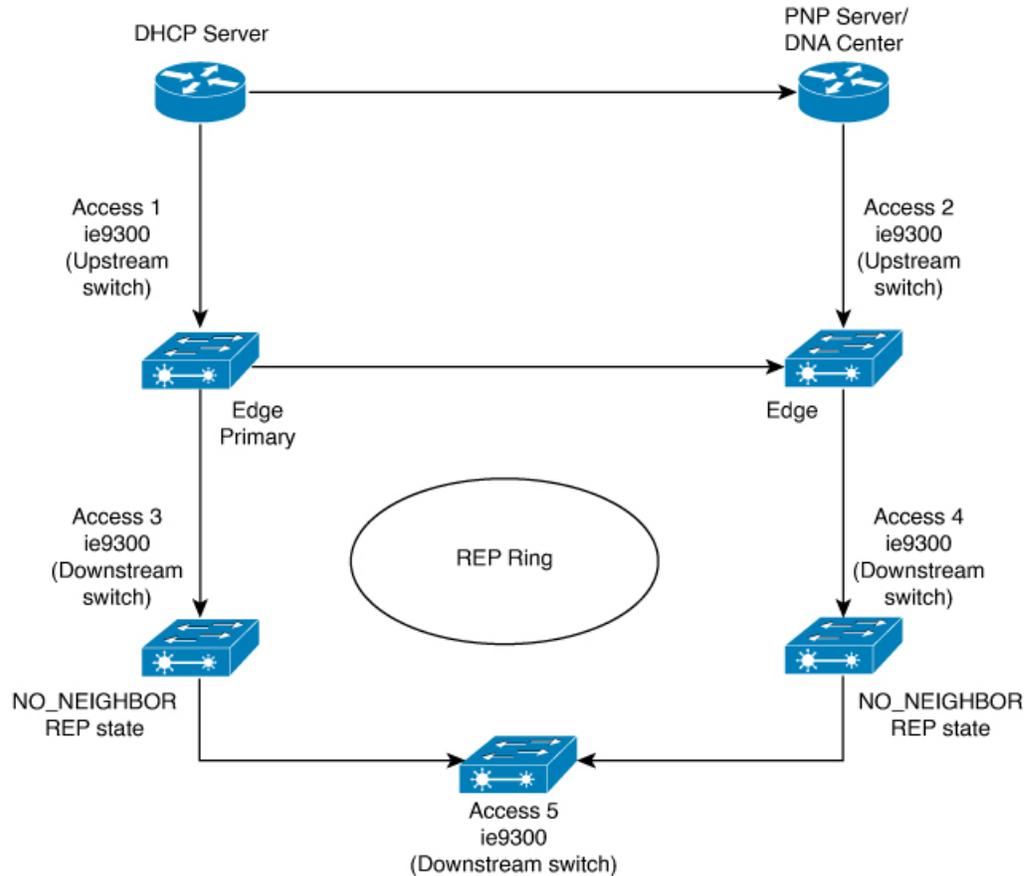
プロビジョニングされるノードの最初のセットは、図内の Access 1 と Access 2 です。これらが REP リングの 2 つのエッジノードとなります。PnP では Access 1 のプライマリエッジおよび Access 2 のセカンダリエッジとしてダウンリンクポートが設定されていることに注意してください。

図 6: 下流ノードの追加



Access 3 または Access 4 のいずれかの電源がオンになると、REP エッジプライマリポートは REP プロトコルのネゴシエーションを開始し、ネイバーポートが REP 対応ポートではないことを検出します（スイッチは PnP のプロビジョニング後にのみ REP リングに追加されます。前述のように、最初に DHCP サーバーに接続する必要があります）。上流スイッチポートに REP が設定され、下流スイッチが PnP でオンボードされると、REP ポートは REP ピアを検出できないため、NO\_NEIGHBOR 状態になります。NO\_NEIGHBOR 状態では、REP でそのポート上のすべての VLAN がブロックされます。これは、REP 状態が NO\_NEIGHBOR であるため、PnP スタートアップ VLAN 上の新しいスイッチから受信した DHCP ディスカバリメッセージが上流スイッチによって破棄されることを意味します。REP リングに追加されたすべての新しいスイッチに対して、ブロックされたポートの同じシーケンスが続きます（次の図の Access 5 を参照）。

図 7: NO\_NEIGHBOR の REP 状態



## REP ZTP の概要

REP ZTP 拡張機能では、上流スイッチと下流スイッチの両方がこの機能に対応している必要があります。新しい下流スイッチの電源がオンになると、PNP/自動インストールが開始されます。上流スイッチのインターフェイスが REP 用に設定されており、下流スイッチはデフォルトでは REP ではないため、下流スイッチへのインターフェイスはブロックされます（上流スイッチは REP\_NO\_NEIGHBOR 状態です）。

上流スイッチのインターフェイスがブロックされていても、REPLSL パケットは下流スイッチに送信されます。これは正常です。REP ZTP 機能の拡張により、下流スイッチは新しい TLV を使用して REP LSL パケットの送信を開始し、ネイバーが PNP プロビジョニングを試行していることを上流スイッチに通知します。

上流スイッチが新しい TLV でこの REPLSL を読み取ると、PNP スタートアップ VLAN のインターフェイスのみがブロック解除されます。上流インターフェイスがメンバーになっている他のすべての VLAN は、引き続きブロックされます。上流スイッチはこのインターフェイスの PNP スタートアップ VLAN 上でパケットを転送しているため、下流スイッチは PNP プロセスを完了できます。

この機能の目的は、新しいスイッチが手動による介入なしに REP リングに参加できるようにすることです。上流スイッチのインターフェイスは、下流スイッチが自身の設定を受信し、自身のインターフェイスを REP 用に設定するまで、スタートアップ VLAN のブロックを解除したままにします。PNP プロセスに障害が発生した場合、上流スイッチのインターフェイスは PNP スタートアップ VLAN をブロッキング状態に戻します。下流スイッチが受信した設定でインターフェイスが REP 用に設定されると、上流スイッチは PNP スタートアップ VLAN をブロッキング状態に戻します。

PnP スタートアップ VLAN のブロック解除を要求するために、新しい TLV を使用して REP LSL を送信する下流の動作は、スタートアップ コンフィギュレーションのないスイッチのデフォルト動作です。PNP スタートアップ VLAN をブロック解除状態にするうえで、セキュリティ上の理由から、上流スイッチでは下流スイッチへのインターフェイスを明示的に有効にする必要があります。インターフェイスレベルのコマンドは `rep ztp-enable` です。[REP ZTP の設定 \(25 ページ\)](#) を参照してください。



(注) 上流スイッチは、複数の REP リングの一部として、複数の下流ネイバーに接続できます。PnP スタートアップ VLAN は、下流スイッチが接続されているインターフェイスでのみブロック解除されます。

## Resilient Ethernet Protocol の設定

セグメントは、チェーンで相互接続されているポートの集合で、セグメント ID が設定されています。REP セグメントを設定するには、REP 管理 VLAN を設定し（またはデフォルト VLAN 1 を使用し）、次にインターフェイス コンフィギュレーションモードを使用してセグメントにポートを追加します。2つのエッジポートをセグメント内に設定して、デフォルトで1つをプライマリ エッジポート、もう1つをセカンダリ エッジポートにします。1セグメント内のプライマリ エッジポートは1つだけです。別のスイッチのポートなど、セグメント内で2つのポートをプライマリ エッジポートに設定すると、REP がそのうちのいずれかを選択してセグメントのプライマリ エッジポートとして機能させます。必要に応じて、STCN および VLAN 負荷分散が送信される場所を設定できます。

### REP のデフォルト設定

- REP はすべてのインターフェイス上で無効です。有効にする際に、エッジポートとして設定されていない場合は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 を有効にする際に、STCN の送信タスクは無効で、すべての VLAN はブロックされ、管理 VLAN は VLAN 1 になります。
- VLAN 負荷分散が有効の場合、デフォルトは手動でのプリエンブションで、遅延タイマーは無効になっています。VLAN 負荷分散が設定されていない場合、手動でのプリエンブ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 Fast はデフォルトで無効になっています。
- REP ゼロタッチプロビジョニングは、グローバルレベルではデフォルトで有効に、インターフェイスレベルでは無効になっています。

## REP の設定ガイドラインと制限事項

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ポートがデータ経路用の転送状態になり、設定中の接続性の維持に役立ちます。  
**show interfaces rep** コマンド出力では、このポートのポート役割は「Fail Logical Open」と表示され、他の障害ポートのポート役割は「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状態に移行して、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状態になるか、代替ポートのままになります。
- REP ポートは、レイヤ 2 IEEE 802.1Q またはトランクポートのいずれかにする必要があります。
- 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。
- SSH または Telnet 接続を通じて REP を設定する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 SSH または Telnet セッションで REP を有効にすると、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 BPDUs は、REP インターフェイスで廃棄されます。
- REP がスイッチの 2 ポートで有効の場合、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。
  - 同じ REP セグメントに属することができるスイッチ上のポートは 2 つだけです。
  - セグメント内にスイッチ上の 1 ポートだけが設定されている場合、そのポートがエッジポートとなります。
  - 同じセグメント内に属するスイッチに 2 つのポートがある場合、両方のポートがエッジポートであるか、両方のポートが通常セグメントポートであるか、一方が通常ポ

トでもう一方が非ネイバー エッジポートである必要があります。一つのスイッチ上のエッジポートと通常セグメントポートが同じセグメントに属することはできません。

- スイッチ上の 2 ポートが同じセグメントに属していて、1 つがエッジポートとして設定され、もう 1 つが通常セグメントポートに設定されている場合（設定ミス）、エッジポートは通常セグメントポートとして扱われます。
- REP インターフェイスはブロックされた状態になり、ブロック解除しても安全になるまでブロックされた状態のままです。突然の接続切断を避けるために、このステータスを認識しておく必要があります。
- REP はネイティブ VLAN 上においてすべての LSL PDU をタグなしフレームで送信します。シスコマルチキャストアドレスに送信された BPA メッセージは、管理 VLAN で送信されます。これはデフォルトで VLAN 1 です。
- ネイバーからの hello が受信されないままどのくらいの時間が経過すると REP インターフェイスがダウンするかを設定できます。 **rep lsl-age-timer** インターフェイスコンフィギュレーション コマンドを使用して、120 ~ 10000 ミリ秒の時間を設定します。次に、LSL Hello タイマーはエージングタイマーの値を 3 で割った値に設定されます。通常の動作では、ピアスイッチのエージングタイマーが満了になって hello メッセージが確認されるまでに LSL hello が 3 回送信されます。 **rep lsl-age-timer** は、非 REP Fast 銅線ギガビットインターフェイスにのみ使用します。他のすべてのインターフェイスでは、 **rep lsl-age-timer** を使用するメリットがありません。
  - EtherChannel ポートチャネルインターフェイスでは、1000 ミリ秒未満の LSL エージングタイマー値はサポートされていません。ポートチャネルで 1000 ミリ秒未満の値を設定しようとする、エラーメッセージが表示されてコマンドが拒否されます。
  - **lsl-age-timer** は、通常のリンクダウン検出がコンバージェンス時間に対して遅すぎる場合に使用することを目的としています。  
FastEthernet 接続と光ファイバ接続には、 **lsl-age-timer** は必要ありません。ギガビット銅線では、 **lsl-age-timer** の代わりに REP Fast を使用できます。
- REP ポートは、次のポートタイプのいずれかに設定できません。
  - スイッチドポートアナライザ（SPAN）宛先ポート
  - トンネルポート
  - アクセスポート
- REP は EtherChannel でサポートされていますが、EtherChannel に属する個別のポートではサポートされません。
- スイッチは、最大 4 つの REP セグメントと 3 つの REP Fast セグメントをサポートします。
- REP リングのサイズに制限はありません。REP リングサイズが 20 ノードを超えると、目的のコンバージェンスに到達できない場合があります。

REP Fast の設定時には、次の注意事項に従ってください。

- この機能を有効にするには、リンクの両端で REP Fast を設定しなければなりません。
- REP セグメントには、ギガビット光ファイバとギガビット銅線を混在させることができます。ギガビット銅線インターフェイスに REP Fast がある場合、単一障害からのコンバージェンスに必要な 50 ミリ秒の要件を達成できます。REP Fast は一つの REP セグメント内に混在、すなわち一部のインターフェイスのみを REP Fast にすることができます。
- 次の制限事項に注意してください。
  - 最大 3 つの REP セグメントで REP Fast を有効にできます。
  - MAC Sec はサポートされていません。
  - オーバースタックはサポートされていません。
  - EtherChannel を介した REP Fast はサポートされていません。

## REP ZTP 設定時の注意事項

- REP ZTP では、Cisco Catalyst IE9300 高耐久性シリーズ スイッチに PnP 機能が存在する必要があります。
- NO\_NEIGHBOR 状態での REP の動作は、Cisco IOS XE 17.14.1 以降で変更されています。NO\_NEIGHBOR 状態でのポート転送動作のこの一時的な状態変化により、DHCP 要求メッセージが DHCP サーバーに到達し、新しいスイッチの PnP プロビジョニングがブロック解除されます。PnP の完了後に REP 状態機械に影響が出ることはありません。
- NO\_NEIGHBOR 状態での REP の動作の変更は、Cisco IOS XE 17.14.1 以降の REP ゼロタッチプロビジョニング (ZTP) にのみ適用されます。PnP 機能が存在しない場合、通常の REP 機能は期待どおりに動作します。
- REP ZTP 機能は、ファイバアップリンクポートで REP bpduleak/ネゴシエートされた機能と共存します。
- REP ZTP 機能は、EtherChannel が下流のインターフェイスにデフォルトで存在しないため、上流スイッチの EtherChannel インターフェイスではデイゼロ向けに使用できません。REP ZTP は、物理インターフェイスでのみ機能します。
- REP ZTP は、銅線 (ダウンリンク) インターフェイスと光ファイバ (アップリンク) インターフェイスの両方でサポートされます。
- REP ZTP は、REP ZTP によるサポートを要求する Cisco IOS XE を実行している他の IE スイッチング製品とのみ相互運用できます。

## REP 管理 VLAN の設定

リンク障害メッセージ、および負荷分散時の VLAN ブロッキング通知によって作成される遅延を回避するため、REP はハードウェアフラッドレイヤ (HFL) で通常のマルチキャストア

ドレスにパケットをフラッディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。管理 VLAN を設定することで、これらのメッセージのフラッディングを制御できます。

REP 管理 VLAN を設定する場合、次の注意事項に従ってください。

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

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

#### 手順の概要

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	<b>enable</b> 例： Device> <b>enable</b>	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	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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	<b>rep admin vlan <i>vlan-id</i></b> 例： Device(config)# <b>rep admin vlan 2</b>	管理 VLAN を指定します。範囲は 2 ~ 4094 です。 管理 VLAN をデフォルトの 1 に設定するには、 <b>no rep admin vlan</b> グローバル コンフィギュレーション コマンドを入力します。
ステップ 4	<b>end</b> 例： Device(config)# <b>end</b>	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	<b>show interface [<i>interface-id</i>] rep detail</b> 例： Device# <b>show interface gigabitethernet1/0/1 rep detail</b>	(任意) REP インターフェイスの設定を検証します。

	コマンドまたはアクション	目的
ステップ 6	<b>copy running-config startup config</b> 例： Device# <b>copy running-config startup config</b>	(任意) スイッチスタートアップコンフィギュレーションファイルに設定を保存します。

## REP インターフェイスの設定

REP を設定する場合、各セグメントインターフェイスで REP を有効にして、セグメント ID を指定します。このタスクは必須で、他の REP 設定の前に実行する必要があります。また、各セグメントにプライマリおよびセカンダリ エッジ ポートを設定する必要があります。それ以外の手順はすべてオプションです。

インターフェイスで REP を有効にし、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 interface-id**
4. **switchport mode trunk**
5. **rep segment segment-id [edge [no-neighbor] [primary]] [preferred]**
6. **rep stcn {interface interface id | segment id-list | stp}**
7. **rep block port {id port-id | neighbor-offset preferred} vlan {vlan-list | all}**
8. **rep preempt delay seconds**
9. **rep lsl-age-timer value**
10. **end**
11. **show interface [interface-id] 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	<b>enable</b> 例： Device> <b>enable</b>	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	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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	<b>interface interface-id</b> 例： Device(config)# <b>interface gigabitethernet1/0/1</b>	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ2インターフェイスまた

	コマンドまたはアクション	目的
		はポート チャネル（論理インターフェイス）に設定できます。
ステップ 4	<b>switchport mode trunk</b> 例： Device(config-if)# <b>switchport mode trunk</b>	インターフェイスをレイヤ 2 トランク ポートとして設定します。
ステップ 5	<b>rep segment segment-id [edge [no-neighbor] [primary]] [preferred]</b> 例： Device(config-if)# <b>rep segment 1 edge no-neighbor primary</b>	<p>インターフェイス上で REP を有効にして、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。</p> <p>(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。</p> <p>これらの任意のキーワードは利用可能です。</p> <ul style="list-style-type: none"> <li>• (任意) <b>edge</b> : 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。<b>primary</b> キーワードなしで <b>edge</b> キーワードを入力すると、ポートがセカンドリッジポートとして設定されます。</li> <li>• (任意) <b>primary</b> : プライマリエッジポート (VLAN 負荷分散を設定できるポート) としてポートを設定します。</li> <li>• (任意) <b>no-neighbor</b> : 外部 REP ネイバーを持たないエッジポートとしてポートを設定します。ポートはエッジポートのすべてのプロパティを継承し、エッジポートの場合と同様にプロパティを設定できます。</li> </ul> <p>(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 <b>primary</b> 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。特権 EXEC モードで <b>show rep topology</b> 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。</p>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• (任意) <b>preferred</b> : ポートが優先代替ポートであるか、VLAN 負荷分散の優先ポートであるかを示します。</li> </ul> <p>(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。</p>
<b>ステップ 6</b>	<b>rep stcn {interface <i>interface id</i>   segment <i>id-list</i>   stp}</b> 例 : <pre>Device(config-if)# rep stcn segment 25-50</pre>	<p>(任意) STCN を送信するようにエッジポートを設定します。</p> <ul style="list-style-type: none"> <li>• <b>interface <i>interface-id</i></b> : 物理インターフェイスまたはポートチャネルを指定して、STCNを受け取ります。</li> <li>• <b>segment <i>id-list</i></b> : STCNを受け取る1つ以上のセグメントを特定します。有効な範囲は1～1024です。</li> <li>• <b>stp</b> : STCNをSTPネットワークに送信します。</li> </ul> <p>(注) STCNをSTPネットワークに送信するために <b>rep stcn stp</b> コマンドを設定する場合は、スパンニング ツリー (MST) モードがネイバーなしのエッジノード上に必要です。</p>
<b>ステップ 7</b>	<b>rep block port {id <i>port-id</i>   neighbor-offset   preferred} vlan {<i>vlan-list</i>   all}</b> 例 : <pre>Device(config-if)# rep block port id 0009001818D68700 vlan 1-100</pre>	<p>(任意) プライマリエッジポートに VLAN 負荷分散を設定して、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 (<b>id <i>port-id</i></b>、<b>neighbor_offset</b>、<b>preferred</b>)、代替ポートでブロックされるように VLAN を設定します。</p> <ul style="list-style-type: none"> <li>• <b>id <i>port-id</i></b> : ポート ID で代替ポートを特定します。セグメント内の各ポートにポート ID が自動的に生成されます。 <b>show interface type number rep [detail]</b> 特権 EXEC コマンドを入力し、インターフェイスポート ID を表示できます。</li> <li>• <b>neighbor_offset</b> : エッジポートからの下流ネイバーとして代替ポートを特定するための番号。有効範囲は -256～256 で、負数はセカンダリエッジポートからの下流ネイバーを示します。<b>0</b>の値は無効です。<b>-1</b>を入力すると、セカンダリ</li> </ul>

	コマンドまたはアクション	目的
		<p>リエッジポートを代替ポートとして識別します。</p> <p>(注) プライマリエッジポート (オフセット番号 1) に <b>rep block port</b> 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 は入力できません。</p> <ul style="list-style-type: none"> <li>• <b>preferred</b> : すでに VLAN 負荷分散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。</li> <li>• <b>vlan vlan-list</b> : 1 つの VLAN または VLAN の範囲をブロックします。</li> <li>• <b>vlan all</b> : すべての VLAN をブロックします。</li> </ul> <p>(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。</p>
ステップ 8	<p><b>rep preempt delay seconds</b></p> <p>例 :</p> <pre>Device(config-if)# rep preempt delay 100</pre>	<p>(任意) プリエンプション遅延時間を設定します。</p> <ul style="list-style-type: none"> <li>• リンク障害が発生して復旧した後に、VLAN 負荷分散を自動的に発動するには、このコマンドを使用します。</li> <li>• 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ブションです。</li> </ul> <p>(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。</p>
ステップ 9	<p><b>rep lsl-age-timer value</b></p> <p>例 :</p> <pre>Device(config-if)# rep lsl-age-timer 2000</pre>	<p>(任意) ネイバーからの hello が受信されないままどのくらいの時間 (ミリ秒) が経過すると REP インターフェイスがダウンするかを設定します。</p> <p>指定できる範囲は 120 ~ 10000 ミリ秒 (40 ミリ秒単位) です。デフォルト値は 5000 ミリ秒 (5 秒) です。</p>

	コマンドまたはアクション	目的
		(注) <ul style="list-style-type: none"> <li>• EtherChannel ポート チャンネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。</li> <li>• リンクのフラップを避けるため、リンクの両方のポートに同じ LSL エージが設定されていることを確認します。</li> </ul>
ステップ 10	<b>end</b> 例： Device (config-if) # <b>end</b>	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 11	<b>show interface [interface-id] rep [detail]</b> 例： Device# <b>show interface gigabitethernet1/0/1 rep detail</b>	(任意) REP インターフェイスの設定を表示します。
ステップ 12	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config startup-config</b>	(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 負荷分散の手動によるプリエンプションの設定

プライマリエッジポートで **rep preempt delay seconds** インターフェイス コンフィギュレーション コマンドを入力してプリエンプション遅延時間を設定しない場合、デフォルトでは手動により当該セグメントの VLAN 負荷分散を発動します。手動で VLAN 負荷分散をプリエンプトする前に、他のすべてのセグメント設定が完了しているかどうか確認してください。 **rep preempt delay segment segment-id** コマンドを入力すると、プリエンプションによってネットワークが中断する可能性があるため、コマンド実行前に確認メッセージが表示されます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	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	<b>rep preempt segment segment-id</b> 例： Device# <b>rep preempt segment 100</b> The command will cause a momentary traffic	手動により、セグメント上の VLAN 負荷分散を発動します。 実行前にコマンドを確認する必要があります。

	コマンドまたはアクション	目的
	disruption. Do you still want to continue? [confirm]	
ステップ 3	<b>show rep topology segment <i>segment-id</i></b> 例： Device# <b>show rep topology segment 100</b>	(任意) REP トポロジの情報を表示します。
ステップ 4	<b>end</b> 例： Device# <b>end</b>	特権 EXEC モードを終了します。

## REP の SNMP トラップ設定

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

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	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	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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	<b>snmp mib rep trap-rate <i>value</i></b> 例： Device(config)# <b>snmp mib rep trap-rate 500</b>	スイッチで REP トラップの送信を有効にして、1 秒あたりのトラップの送信数を設定します。  • 1 秒あたりのトラップの送信数を入力します。 範囲は 0 ~ 1000 です。デフォルトは 0 (制限なし、発生するたびにトラップが送信される) です。
ステップ 4	<b>end</b> 例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b> 例： Device# <b>show running-config</b>	(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。

	コマンドまたはアクション	目的
ステップ 6	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config startup-config</b>	(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 ZTP の設定

REP ZTPを設定するには、グローバルレベルおよびインターフェイスレベルで有効または無効にします。デフォルトの状態は、次のとおりです。

- グローバルレベル：有効
- インターフェイスレベル：無効

下流デバイスに接続されている上流デバイスインターフェイスのインターフェイスレベルで、この機能を明示的に有効にする必要があります。有効にすると、そのインターフェイスだけが下流スイッチから通知を受信し、PnP スタートアップ VLAN をブロックまたはブロック解除します。



(注) DNAC または PNP サーバーの設定を適用する場合、ユーザーはこの CLI 設定を設定テンプレートに明示的に追加して、機能を有効にする必要があります。

**ステップ 1** 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。

```
Switch# configure terminal
```

**ステップ 2** REP ZTP をグローバルに有効にします。

```
Switch(config)# rep ztp
```

REP ZTP を無効にするには、Switch(config)# **no rep ztp** コマンドの **no** 形式を使用します。

**ステップ 3** 下流デバイスに接続されている上流デバイスインターフェイスで、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。

```
Switch(config)# interface <interface-name>
```

**ステップ 4** インターフェイスで REP ZTP を有効にします。

```
Switch(config-if)#rep ztp-enable
```

インターフェイスで REP ZTP を無効にするには、Switch(config-if)#**no rep ztp-enable** コマンドの **no** 形式を使用します。

## 例

次に、下流デバイスに接続されている上流デバイスインターフェイスでREP ZTP機能を有効にするために必要な最小設定の例を示します。

```
Switch#show running-config interface gigabitEthernet 1/0/1
Building configuration...

Current configuration : 93 bytes
!
interface GigabitEthernet1/0/1
  switchport mode trunk
  rep segment 100
  rep ztp-enable
end
```

## Resilient Ethernet Protocol 設定の監視

次の例では、**show interface [interface-id] rep [detail]** コマンドの出力を示します。この表示では、アップリンクポートのREP設定とステータスを示します。

```
Device# show interfaces GigabitEthernet1/0/4 rep detail

GigabitEthernet1/0/4 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Disabled
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

次の例では、**show interface [interface-id] rep [detail]** コマンドの出力を示します。この表示では、ダウンリンクポートのREP設定とステータスを示します。

```
Device#show interface GigabitEthernet1/0/5 rep detail

GigabitEthernet1/0/5 REP enabled
Segment-id: 1 (Segment)
PortID: 019B380E4D9ACAC0
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
```

```

Current Key: 019B380E4D9ACAC0696B
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
REP-ZTP Status: Disabled
Preempt Delay Timer: 100 sec
LSL Ageout Timer: 2000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: 09E9380E4D9ACAC0
Configured Load-balancing Block VLAN: 1-100
STCN Propagate to: segment 25
LSL PDU rx: 292, tx: 340
HFL PDU rx: 0, tx: 0
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: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0

```

次の例では、**show rep topology** [*segment segment-id*] [*archive*] [*detail*] コマンドを示します。この表示では、すべてのセグメントの REP トポロジ情報を示します。

```

Device# show rep topology

REP Segment 1
BridgeName      PortName      Edge Role
-----
10.64.106.63    Gi1/0/4       Pri  Open
10.64.106.228  Gi1/0/4       Open
10.64.106.228  Gi1/0/3       Open
10.64.106.67   Gi1/0/3       Open
10.64.106.67   Gi1/0/4       Alt
10.64.106.63   Gi1/0/4       Sec  Open

REP Segment 3
BridgeName      PortName      Edge Role
-----
10.64.106.63    Gi1/011      Pri  Open
SVT_3400_2      Gi1/0/3      Open
SVT_3400_2      Gi1/0/4      Open
10.64.106.68    Gi1/0/2      Open
10.64.106.68    Gi1/0/1      Open
10.64.106.63    Gi1/0/2      Sec  Alt

```

## REP ZTP ステータスの表示

インターフェイスで REP ZTP の状態を確認するには、**show** コマンドを使用します。次の例では、インターフェイス **GigabitEthernet 1/0/1** でこの機能を無効にし、インターフェイス **GigabitEthernet 1/0/2** で有効にしています。 **pnnp\_startup\_vlan** のステータスは「Blocked」です。

**ステップ 1** 特権 EXEC モードで、次のように入力します。

```
show interfaces rep detail
```

例 :

```
GigabitEthernet1/0/1  REP enabled
Segment-id: 100 (Segment)
PortID: 00016C13D5AC4320
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 00026C13D5AC43209DAB
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Disabled
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
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: none
LSL PDU rx: 382, tx: 297
HFL PDU rx: 0, tx: 0
BPA TLV rx: 1, tx: 19
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 95, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 95, tx: 95

GigabitEthernet1/0/2  REP enabled
Segment-id: 100 (Segment)
PortID: 00026C13D5AC4320
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 00026C13D5AC43209DAB
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
REP-ZTP Status: Enabled
REP-ZTP PnP Status: Unknown
REP-ZTP PnP Vlan: 1
REP-ZTP Port Status: Blocked
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
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: none
LSL PDU rx: 11, tx: 11
HFL PDU rx: 0, tx: 0
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: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

ステップ2 show コマンドを再度使用して、**pnp\_startup\_vlan** のステータスを表示します。

下流デバイスが起動すると、接続された上流スイッチインターフェイスに通知を送信し、**pnp\_startup\_vlan** のブロックを解除して DHCP IP アドレスを取得します。さらに、PNP サーバーまたは DNAC との通信も確立します。**show** コマンドを実行すると、ステータスが「Unblocked」と表示されます。

次に示す上流スイッチの **syslog** では、ポートの FWD および BLK について通知しています。PnP によってコンソールが制御され、コンソールで **syslog** を出力できないため、下流スイッチに **syslog** はありません。

```
REP-6-ZTPPORTFWD: Interface GigabitEthernet1/0/2 moved to forwarding on ZTP notification
```

```
REP-6-ZTPPORTBLK: Interface GigabitEthernet1/0/2 moved to blocking on ZTP notification
```

例 :

```
Switch#show interfaces rep detail
GigabitEthernet1/0/1  REP enabled
Segment-id: 100 (Segment)
PortID: 00016C13D5AC4320
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 00026C13D5AC43209DAB
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Disabled
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
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: none
LSL PDU rx: 430, tx: 358
HFL PDU rx: 0, tx: 0
BPA TLV rx: 1, tx: 67
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 107, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 107, tx: 108

GigabitEthernet1/0/2  REP enabled
Segment-id: 100 (Segment)
PortID: 00026C13D5AC4320
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 00026C13D5AC43209DAB
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
REP-ZTP Status: Enabled
REP-ZTP PnP Status: In-Progress
REP-ZTP PnP Vlan: 69
REP-ZTP Port Status: Unblocked
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
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: none
LSL PDU rx: 32, tx: 40
HFL PDU rx: 0, tx: 0
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: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

**ステップ 3** PnP スタートアップ VLAN のインターフェイス状態を確認するには、**show platform hardware l2 stp** コマンドを使用します。

例 :

```
Switch#show platform hardware l2 stp ASIC-num 0 vlan-id 69 [PnP Vlan]
-----STP TABLE START-----
VlanId:1 StpId:0 MemberPort:3 StpState:FORWARDING
VlanId:1 StpId:0 MemberPort:7 StpState:FORWARDING
VlanId:1 StpId:0 MemberPort:25 StpState:FORWARDING
-----STP TABLE END-----
```

**ステップ 4** (オプション) REP ZTP のトラブルシューティングには、次のデバッグコマンドを使用できます。

- **debug rep lsism** : このコマンドは、NO\_NEIGHBOR 状態の LSL 状態機械イベントについて理解するのに役立ちます。
- **debug rep packet** : REP ZTP LSL TLV で LSL パケットをダンプし、ピアクライアントノードの PnP ステータスを確認するには、このコマンドを使用します。

次のタスク

## Resilient Ethernet Protocol の機能履歴

以下の表に、このガイドに記載されている機能のリリースおよび関連情報を示します。この機能は、特に明記されていない限り、最初のリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Cupertino 17.9.x	Resilient Ethernet Protocol Fast	この機能は、このリリースより Cisco Catalyst IE9300 高耐久性シリーズスイッチで使用できるようになりました。
Cisco IOS XE Cupertino 17.14.x	Resilient Ethernet Protocol のゼロタッチプロビジョニング	この機能は、このリリースより Cisco Catalyst IE9300 高耐久性シリーズスイッチで使用できるようになりました。

## 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。