# MPLS トラフィック エンジニアリングにおけるパス、リンク、およびノード保護のコンフィギュレーション ガイド

初版：2014 年 03 月 28 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

# 最初にお読みください

### Cisco IOS XE 16 に関する重要な情報

Cisco IOS XE Release 3.7.0E（Catalyst スイッチ用）および Cisco IOS XE Release 3.17S（アクセスおよびエッジ ルーティング用）の 2 つのリリースが、集約された単一のリリース バージョンとして Cisco IOS XE 16 に統合され、進化しました。スイッチングおよびルーティングのポートフォリオに含まれる幅広いアクセス製品とエッジ製品を盛り込んだ単一のリリースが実現します。

（注） 技術構成ガイドにある機能情報の表には、その機能がいつ導入されたかが記載されています。その機能で他のプラットフォームがいつサポートされるようになったかについては、記載されている場合とされていない場合があります。特定の機能がご使用のプラットフォームでサポートされているかどうかを確認するには、製品のランディング ページに掲載されている技術構成ガイドを参照してください。ご使用の製品のランディング ページに技術構成ガイドが表示されていれば、機能はそのプラットフォームでサポートされていることを意味します。

第 2 章

# MPLS トラフィック エンジニアリング：Fast Reroute リンクとノード保護

MPLS トラフィック エンジニアリング - 高速リルート リンクおよびノード保護機能は、リンク保護（ラベル スイッチド パス（LSP）の単一リンクだけをバイパスするバックアップ トンネル）、ノード保護（LSP 上のネクストホップ ノードをバイパスするバックアップ トンネル）、および高速再ルーティング（FRR）機能を提供します。

# 機能情報の確認

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

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、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。

# MPLS トラフィック エンジニアリング - 高速リルート リンクおよびノード保護の前提条件

ネットワークが、次の Cisco IOS XE 機能をサポートしている必要があります。

- IP シスコ エクスプレス フォワーディング
- マルチプロトコル ラベル スイッチング（MPLS）

ネットワークが、次のプロトコルの少なくとも 1 つをサポートしている必要があります。

- Intermediate System-to-Intermediate System（IS-IS）
- Open Shortest Path First（OSPF）

FRR リンクおよびノードの保護を設定する前に、次の作業を完了していることが前提となります。ただし、MPLS トラフィック エンジニアリング（TE）トンネルはまだ設定していなくてもかまいません。

- 関連するすべてのルータおよびインターフェイス上での MPLS TE のイネーブル化
- MPLS TE トンネルの設定

# MPLS トラフィック エンジニアリング - 高速リルート リンクおよびノード保護の制約事項

- インターフェイスが MPLS グローバル ラベル割り当てを使用する必要があります。
- ルータの MPLS-TE 向け物理インターフェイス、ギガビットイーサネット（GE）向けの高速リルート（FRR）、Packet over SONET（POS）は 50 ミリ秒（ms）のフェールオーバーに対応しています。ただし（設定可能であっても）、GE のサブインターフェイス、論理インター

フェイスとカッパー インターフェイス（高速イーサネット インターフェイスなど）は、50 ミリ秒のフェールオーバーに対応していません。また、FRR は ATM インターフェイスでは設定できません。

- FRR リンク保護モードのフェールオーバー時間は、リンクをポイントするプレフィックスの数に関係しません。
- Cisco IOS XE は、MPLS-TE トンネルでの QoS をサポートしていません。
- draft-pan-rsvp-fastreroute-00.txt で説明されているように、バックアップ トンネルのヘッドエンドおよびテールエンドのルータが FRR を実装している必要があります。
- バックアップ トンネルは保護されません。LSP がアクティブにバックアップ トンネルを使用している場合、バックアップ トンネルに障害が発生すると、LSP は切断されます。
- バックアップ トンネルをアクティブに使用している LSP のプロモーションは考慮されません。LSP がアクティブにバックアップ トンネルを使用している場合、より適切なバックアップ トンネルが使用可能になっても、アクティブな LSP はそのバックアップ トンネルに切り替わりません。
- リソース予約プロトコル（RSVP）グレースフル リスタートもイネーブルになっているルータ上では、FRR Hello をイネーブルにすることができません。
- LSP の FRR がアクティブになっている場合、ローカル修復ポイント（PLR）ルータにステートフル スイッチオーバー（SSO）が発生すると、高速リルート可能な MPLS TE LSP は正常に回復できません。

# MPLS トラフィック エンジニアリング - 高速リルート リンクおよびノード保護の設定に関する情報

## 高速再ルーティング

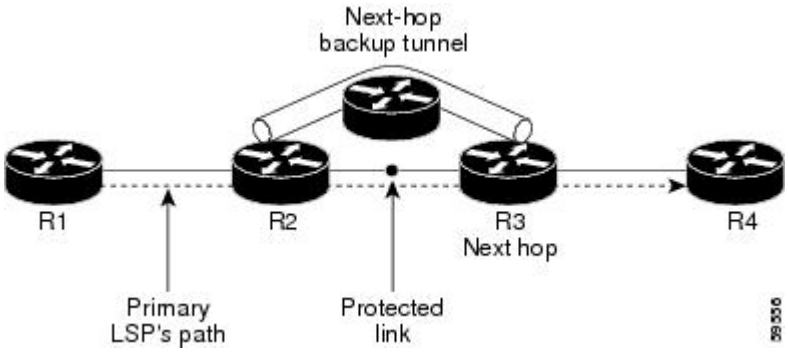
高速再ルーティング（FRR）は、リンクおよびノードの障害から MPLS TE LSP を保護するためのメカニズムです。具体的には、障害ポイントの LSP をローカルに修復し、その LSP 上でのデータフローを停止することなく、LSP のヘッドエンド ルータを新しく置き換えるエンドツーエンド LSP の確立を試行します。FRR は、保護対象 LSP を、障害が発生したリンクまたはノードをバイパスするバックアップ トンネル経由でリルートすることにより、LSP をローカルに修復します。

## リンク保護

LSP のパスの単一リンクだけをバイパスするバックアップ トンネルが、リンク保護を提供します。パス上のリンクに障害が発生した場合、バックアップ トンネルは、LSP のトラフィックをネクスト ホップにリルートする（障害の発生したリンクをバイパスする）ことによって LSP を保護します。これらは、障害ポイントの向こう側にある LSP のネクスト ホップで終端するため、ネク

ストホップ（NHOP）バックアップ トンネルと呼ばれます。次の図は、NHOP バックアップ トンネルを示しています。

**図 *1*：*NHOP* バックアップ トンネル**

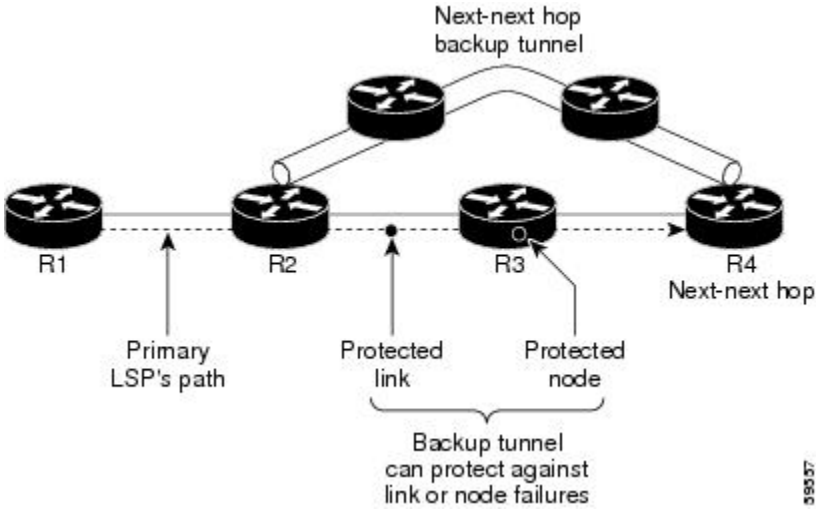



# ノード保護

FRR により、LSP に対するノード保護が提供されます。LSP パス上のネクストホップ ノードをバイパスするバックアップ トンネルは、LSP パスのネクストホップ ノードの次のノードで終端して、結果としてネクストホップ ノードをバイパスするため、ネクストネクストホップ（NNHOP）バックアップ トンネルと呼ばれます。LSP パス上のノードに障害が発生した場合は、NNHOP バックアップ トンネルが LSP を保護します。具体的には、障害のアップストリームにあるノードをイネーブルにして、障害の発生したノードの周囲の LSP とそのトラフィックをネクストネクストホップにリルートします。FRR では、ノード障害を短時間で検出できるように、RSVP Hello の使用がサポートされています。また、NNHOP バックアップ トンネルは、障害の発生したリンクおよびノードをバイパスするため、リンク障害からの保護も提供しています。

次の図は、NNHOP バックアップ トンネルを示しています。

**図 2：*NNHOP* バックアップ トンネル**




LSP がバックアップ トンネルを使用している場合、何らかの変更によって LSP がバックアップ トンネルとして適切でなくなると、その LSP は切断されます。次のような変更がこれに該当します。

- バックアップ トンネルのバックアップ帯域幅が縮小された。
- バックアップ トンネルのバックアップ帯域幅タイプが、プライマリ LSP と互換性のないタイプに変更された。
- プライマリ LSP が変更されたために、FRR がディセーブルになった（**nomplstraffic-engfast-reroute** コマンドが入力された。）

# 帯域幅保護

NHOP および NNHOP バックアップ トンネルを使用すると、リルートされた LSP の帯域幅保護を提供できます。これは、バックアップ帯域幅と呼ばれます。バックアップ帯域幅は、NHOP または NNHOP バックアップ トンネルと関連付けることができます。これにより、特定のバックアップ トンネルで保護できるバックアップ帯域幅の大きさがルータに通知されます。ルータが LSP をバックアップ トンネルにマップするとき、帯域幅保護によって、十分なバックアップ帯域幅がある場合にだけ、指定されたバックアップ トンネルが使用されます。ルータは、最大限の帯域幅保護を提供するために、どの LSP がどのバックアップ トンネルを使用するかを選択します。つまり、ルータは、保護できる LSP の数が最大限になるような方法を、LSP をバックアップ トンネルにマップする最良の方法として決定します。トンネルのマッピングおよびバックアップ帯域幅の割り当てについては、「バックアップ トンネルの選択手順」セクションを参照してください。

bandwidth protection desired ビットが設定された LSP では、帯域幅保護を提供するバックアップ トンネルの選択権限が大きくなります。つまり、これらの LSP は、そのビットが設定されていない

他の LSP をプリエンプション処理できます。詳細は、「帯域幅保護されたバックアップ トンネルを取得する LSP のプライオリティ設定」セクションを参照してください。

# RSVP Hello の動作

RSVP Hello を使用すると、RSVP ノードは、ネイバー ノードが到達不能になった場合にそれを検出できます。これにより、ノードツーノードの障害検出が可能になります。このような障害が検出された場合、リンク層の通信障害のときと同様の方法で処理されます。

リンク層障害の通知が使用可能でない場合（たとえば、ファスト イーサネットなど）、またはリンク層により提供される障害検出メカニズムが十分でないためにノード障害をタイムリーに検出できない場合、FRR では RSVP Hello を使用できます。

Hello を実行しているノードは、各間隔で Hello Request をネイバー ノードに送信します。受信側ノードが Hello を実行している場合、このノードは Hello Ack を使用して応答します。4 間隔が経過しても送信側ノードが Ack を受信できない場合、または不正なメッセージが受信された場合、送信側ノードはネイバーが停止していることを宣言し、FRR に通知します。

設定可能なパラメータは 2 つあります。

- Hello 間隔：**ip rsvp signalling hello refresh interval** コマンドを使用します。
- 送信側ノードでネイバーが停止していると宣言されるまでにミスされる確認応答メッセージの数：**ip rsvp signalling hello refresh misses** コマンドを使用します。

# RSVP Hello のインスタンス

Hello インスタンスは、特定のルータ インターフェイス IP アドレスおよびリモート IP アドレスに対して RSVP Hello を実装します。多数の Hello Request が送信されるため、ルータ リソースに負担がかかります。このため、Hello インスタンスを作成するのは必要な場合だけにし、不要になったインスタンスは削除してください。

次の 2 種類の Hello インスタンスがあります。

### アクティブな Hello インスタンス

LSP の高速リルートの準備ができているが、ネイバーが到達不能な場合、アクティブな Hello インスタンスが必要となります。この状態の LSP を少なくとも 1 つ持つネイバーに対して、アクティブな Hello インスタンスを 1 つずつ作成します。

アクティブな Hello インスタンスは、定期的に Hello Request メッセージを送信し、応答として Hello Ack メッセージを予期します。予期されている Ack メッセージを受信できない場合、アクティブな Hello インスタンスは、そのネイバー（リモートの IP アドレス）が到達不能である（失われている）ことを宣言します。そのネイバーを通過する LSP の高速リルートを行うことができます。

到達不能なネイバーに対する LSP を持たない Hello インスタンスがある場合、その Hello インスタンスを削除しないでください。アクティブな Hello インスタンスをパッシブな Hello インスタンス

に変更します。これは、Hello Request をこのインスタンスに送信しているアクティブなインスタンスがネイバー ルータ上に存在する可能性があるためです。

### パッシブな Hello インスタンス

パッシブな Hello インスタンスは（Ack メッセージを送信して）Hello Request メッセージに応答しますが、Hello Request メッセージを開始しないため、LSP の高速リルートは行われません。複数のインターフェイスを持つネイバーは、異なるネイバーに対して、または同じネイバーに対して、複数の Hello インスタンスを実行できます。

Hello インスタンスが存在しないネイバーから、IP ヘッダー内に送信元 IP アドレスと宛先 IP アドレスのペアが含まれる Hello Request が受信されると、パッシブな Hello インスタンスが作成されます。

このインスタンスに対して 10 分以内に Hello メッセージが受信されない場合は、パッシブ インスタンスを削除してください。

## バックアップ トンネル サポート

バックアップ トンネル サポートには、次の機能があります。

### バックアップ トンネルは FRR をサポートするためにネクストネクスト ホップで終端できる

ネクストネクストホップで終端するバックアップ トンネルは、ダウンストリームのリンクとノードの両方を保護します。これにより、リンクおよびノードの障害に対する保護が可能になります。詳細については、ノード保護, （6 ページ）を参照してください。

### 複数のバックアップ トンネルが同じインターフェイスを保護できる

1 つのインターフェイスを保護できるバックアップ トンネルの数に制限はありません（メモリ制限を除く）。多くのトポロジでは、ノード保護をサポートするために、保護インターフェイスごとに複数のバックアップ トンネルをサポートする必要があります。これらのバックアップ トンネルは同じ宛先で終端することも、異なる宛先で終端することもできます。つまり、1 つの保護インターフェイスに対して、複数の NHOP または NNHOP バックアップ トンネルを設定できます。これにより、冗長性とロード バランシングを実現できます。

複数のバックアップ トンネルで 1 つのインターフェイスを保護することは、ノード保護のために必要とされるだけでなく、次のような利点もあります。

- 冗長性：一方のバックアップ トンネルが停止すると、他方のバックアップ トンネルが LSP を保護します。
- バックアップ容量の増加：保護インターフェイスが大容量リンクであり、同じ容量を持つバックアップ パスが 1 つも存在しない場合、その 1 つの大容量リンクを複数のバックアップ トンネルによって保護できます。このリンクを使用している LSP は異なるバックアップ トンネルにフェールオーバーするため、障害発生時にはすべての LSP が適切な帯域幅保護（リルート）を受けることができます。帯域幅保護が必要でない場合、ルータは使用可能なすべてのバックアップ トンネルに LSP を分散させます（つまり、複数のバックアップ トンネル

の間でロード バランシングを行います）。詳細については、バックアップ トンネルの選択手順, （13 ページ）を参照してください。

異なる宛先で終端するバックアップ トンネル, （12 ページ）と『同じ宛先で終端するバックアップ トンネル』セクションで例を示しています。

### バックアップ トンネルによりスケーラビリティが提供される

1 つのバックアップ トンネルで複数の LSP を保護できます。さらに、1 つのバックアップ トンネルで複数のインターフェイスを保護できます。これを、多対 1（N:1）の保護と呼びます。N:1 保護では、たとえば 1 つのバックアップ トンネルが 5000 の LSP を保護する場合、バックアップ パスに沿った各ルータが 1 つの追加トンネルを維持します。

1 対 1 の保護は、保護の必要な LSP ごとに個別のバックアップ トンネルを使用する必要があるときに行います。N:1 の保護は、1 対 1（1:1）の保護に比べてスケーラビリティ上のメリットが大きくなります。1:1 保護では、たとえば 5000 のバックアップ トンネルが 5000 の LSP を保護する場合、バックアップ パスに沿った各ルータは 5000 の追加トンネルの状態を維持する必要があります。

## バックアップ帯域幅保護

バックアップ帯域幅保護には、次の機能があります。

### バックアップ トンネルの帯域幅保護

障害発生時に、リルートされた LSP によりパケットが伝送されるだけでなく、Quality of Service（QoS）も維持できます。

### バックアップ トンネルの帯域幅プール指定

特定のバックアップ トンネルを使用できる LSP のタイプを制限できます。サブプール帯域幅を使用する LSP だけが使用できるように、またはグローバル プール帯域幅が使用できるように、バックアップ トンネルを制限できます。このため、音声とデータに対して別々のバックアップ トンネルを使用できます。たとえば、音声に使用するバックアップ トンネルでは帯域幅保護を提供し、データに使用するバックアップ トンネルでは（場合により）帯域幅保護を提供しないように設定できます。

### 半ダイナミックなバックアップ トンネル パス

バックアップ トンネルのパスは、ダイナミックに決定されるように設定できます。このためには、リリース 12.0(14)ST で追加された IP 明示アドレス除外機能を使用します。この機能を使用すると、半ダイナミックな NHOP バックアップ トンネル パスは、保護対象のリンクを除外するだけで指定できます。半ダイナミックな NNHOP バックアップ トンネル パスは、保護対象のノードを除外するだけで設定できます。

### 帯域幅保護されたバックアップ トンネルを取得する LSP のプライオリティ設定

NHOP または NNHOP バックアップ トンネルが十分にない場合、またはすべての LSP を保護するための十分なバックアップ帯域幅がない場合は、帯域幅保護されたバックアップ トンネルを取得するためのプライオリティを LSP に付与できます。これは特に、データを伝送する LSP よりも音声を伝送する LSP に高いプライオリティを付与する場合に有用です。

この機能をアクティブにするには、**tunnelmplstraffic-engfast-reroutebw-protect** コマンドを入力して、「bandwidth protection desired」ビットを設定します。『LSP 上での高速リルートの有効化』の設定タスクを参照してください。必ずしもこのような LSP が帯域幅保護を受けるとはかぎりません。必要な場合に、このような LSP の方が帯域幅保護を受ける可能性が高くなります。

帯域幅保護ビットが設定されていない LSP は、デモートできます。デモーションとは、帯域幅保護ビット セットのある LSP にバックアップを提供するために、1 つ以上の LSP が、割り当てられたバックアップ トンネルから削除されることです。デモーションは、バックアップ帯域幅が不足している場合にだけ行われます。

デモートされた LSP は、保護されていない状態になります（つまり、バックアップ トンネルを持たなくなります）。次の定期的なプロモーション サイクルの間に、現在保護されていないすべての LSP（デモートされた LSP を含む）に対して可能なかぎり最良のバックアップ トンネルを見つけるように試行されます。LSP は同レベルまたは低いレベルの保護を受けることもあれば、保護を受けないこともあります。

ルータがデモート対象の LSP を決定する方法については、『バックアップ保護プリエンプション アルゴリズム』セクションを参照してください。

# RSVP Hello

RSVP Hello を使用すると、ルータは、ネイバー ノードが停止したが、そのネイバーへのインターフェイスがまだ動作中である場合、それを検出できます。この機能は、リンク層メカニズムによってネクストホップ ノードの障害が検出できない場合や、リンク層障害の通知が使用可能でない場合（たとえば、ギガビット イーサネットなど）に特に有用です。これにより、ルータは LSP をそのバックアップ トンネルに切り替え、パケット損失を回避できます。

RSVP Hello の詳細については、RSVP Hello の動作, （8 ページ）を参照してください。

## 高速リルート操作

### 高速リルート アクティベーション

次の 2 つのメカニズムによって、ルータで LSP がそのバックアップ トンネルに切り替わります。

- インターフェイス停止通知
- RSVP Hello ネイバー停止通知

ルータのリンクまたはネイバー ノードに障害が発生すると、インターフェイス停止通知によってルータはこの障害を検出します。GSR Packet over SONET（PoS）インターフェイスでは、この通

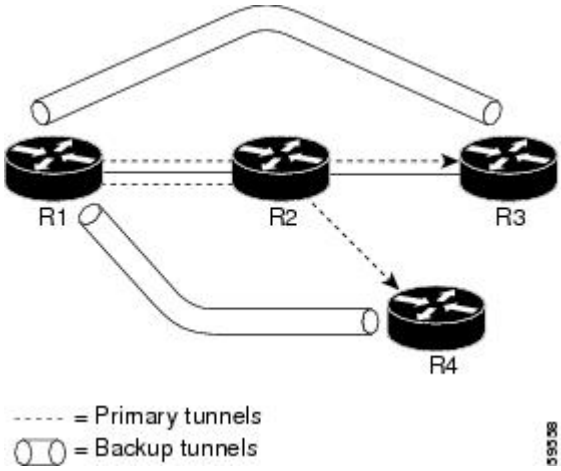
知が非常に高速に行われます。インターフェイスが停止したことをルータが認識すると、ルータはそのインターフェイスを出るLPSを、それぞれのバックアップ トンネルに切り替えます（バックアップ トンネルがある場合）。

RSVP Helloは、FRRをトリガーするためにも使用できます。インターフェイス上にRSVP Helloが設定されている場合、メッセージが定期的にネイバー ルータに送信されます。応答を受信できない場合、Helloはネイバーが停止していることを宣言します。これにより、そのインターフェイスを出るLSPはすべて、それぞれのバックアップ トンネルに切り替わります。

## 異なる宛先で終端するバックアップ トンネル

次の図に、異なる宛先で終端する複数のバックアップ トンネルを持つインターフェイスを示します。また、多くのトポロジにおいて、ノード保護をサポートするために保護インターフェイスごとに複数のバックアップ トンネルをサポートする必要がある理由を示しています。

**図 *3*：異なる宛先で終端するバックアップ トンネル**



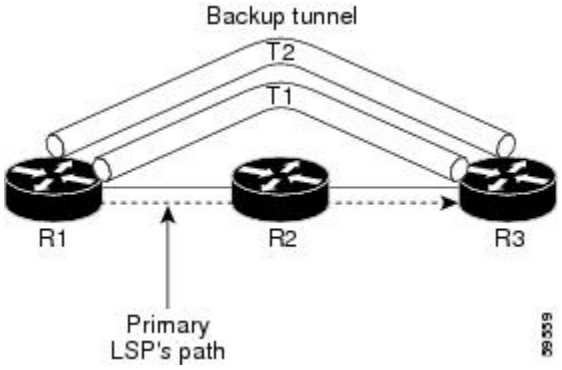

この図では、R1上の単一のインターフェイスが複数のバックアップ トンネルを必要としています。LSPは、次のルートを通過します。

- R1、R2、R3
- R1、R2、R4

ノードR2の障害発生時に備えた保護を提供するには、2つのNNHOPバックアップ トンネル（R3で終端するバックアップ トンネルと、R4で終端するバックアップ トンネル）が必要です。

## 同じ宛先で終端するバックアップ トンネル

次の図に、冗長性およびロード バランシングのために同じロケーションで終端するバックアップ トンネルを使用する方法を示します。冗長性およびロード バランシングは、NHOPバックアップ トンネルとNNHOPバックアップ トンネルの両方に対して使用できます。




この図では、3 つのルータ（R1、R2、および R3）があります。R1 では、R2 を通過せずに R1 から R3 に移動する 2 つの NNHOP バックアップ トンネル（T1 および T2）があります。

冗長性があれば、R2 に障害が発生した場合や、R1 から R2 へのリンクに障害が発生した場合、どちらのバックアップ トンネルも使用できます。一方のバックアップ トンネルが停止した場合は、もう一方のバックアップ トンネルを使用できます。LSP は、最初に確立されるときに、バックアップ トンネルに割り当てられます。これは、障害発生前に完了しています。

ロード バランシングにより、どちらのバックアップ トンネルにもすべての LSP をバックアップするための十分な帯域幅がない場合、両方のトンネルを使用できます。一部の LSP は一方のバックアップ トンネルを使用し、その他の LSP はもう一方のバックアップ トンネルを使用します。ルータによって、LSP をバックアップ トンネルに割り当てる最良の方法が決定されます。

## バックアップ トンネルの選択手順

次のいずれかのイベントが発生した場合、LSP がシグナリングされると、その LSP に FRR 保護を提供する LSP パス上の各ノードが、LSP のバックアップ トンネルを選択します。

- ネクスト ホップへのリンクに障害が発生した。
- ネクスト ホップに障害が発生した。

障害発生前にノードが LSP のバックアップ トンネルを選択することにより、障害発生時に LSP をバックアップ トンネルにすばやくリルートできます。

LSP をバックアップ トンネルにマップするには、次のすべての条件が満たされている必要があります。

- LSP が FRR で保護されている。つまり、LSP が **tunnel mpls traffic-eng fast-reroute** コマンドを使用して設定されている。
- バックアップ トンネルが動作している。
- バックアップ トンネルが IP アドレス（通常はループバック アドレス）を持つように設定されている。
- バックアップ トンネルが、この LSP の発信インターフェイスを保護するように設定されている（インターフェイスが **mpls traffic-eng backup-path** コマンドを使用して設定されている）。
- バックアップ トンネルが LSP の保護インターフェイスを通過しない。

- バックアップ トンネルが LSP の NHOP または NNHOP で終端している。NNHOP トンネルであるバックアップ トンネルは、LSP の NHOP を追加しません。
- LSP およびバックアップ トンネルの帯域幅保護の要件と制約（ある場合）が満たされている。帯域幅保護の考慮事項については、帯域幅保護，（14 ページ）を参照してください。

## 帯域幅保護

バックアップ トンネルは、次の 2 種類のバックアップ帯域幅を保護するように設定できます。

- 制限付きバックアップ帯域幅：バックアップ トンネルが帯域幅保護を提供します。このバックアップ トンネルを使用するすべての LSP の帯域幅の合計が、バックアップ トンネルのバックアップ帯域幅を超えることはできません。LSP をこのタイプのバックアップ トンネルに割り当てる場合、十分なバックアップ帯域幅が存在している必要があります。
- 制限なしバックアップ帯域幅：バックアップ トンネルは帯域幅保護を提供しません（つまり、ベストエフォート型の保護が存在します）。このバックアップ トンネルにマップされた LSP で使用される帯域幅の大きさに制限はありません。ゼロ帯域幅が割り当てられた LSP は、制限なしバックアップ帯域幅のバックアップ トンネルしか使用できません。

## 制限付き帯域幅バックアップ トンネルのロード バランシング

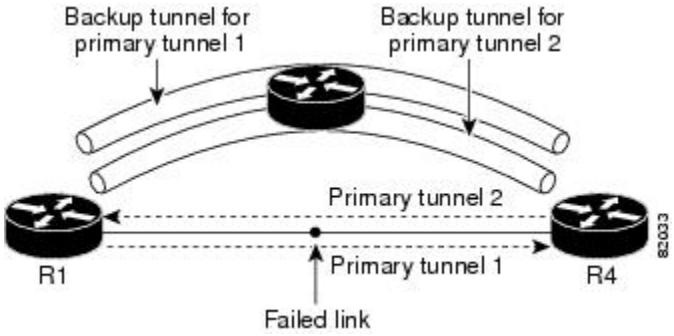
特定の LSP を保護するための十分なバックアップ帯域幅を持つバックアップ トンネルが、複数存在することがあります。この場合、ルータが、使用可能な最小バックアップ帯域幅のバックアップ トンネルを選択します。このアルゴリズムによって、フラグメンテーションが制限されるため、使用可能な最大バックアップ帯域幅が維持されます。

制限付きバックアップ帯域幅を指定した場合、リンクまたはノードの障害発生時の帯域幅保護は「保証」されません。たとえば、インターフェイスの障害発生時にトリガーされる NHOP バックアップ トンネルと NNHOP バックアップ トンネルのセットがすべて、ネットワーク トポロジ上のリンクを共有することがありますが、このバックアップ トンネル セットを使用してすべての LSP をサポートするだけの十分な帯域幅がこのリンクにない場合があります。

次の図では、両方のバックアップ トンネルが同じリンクおよびホップを通過しています。ルータ R1 と R4 の間のリンクに障害が発生すると、プライマリ トンネル 1 のバックアップ トンネルとプ

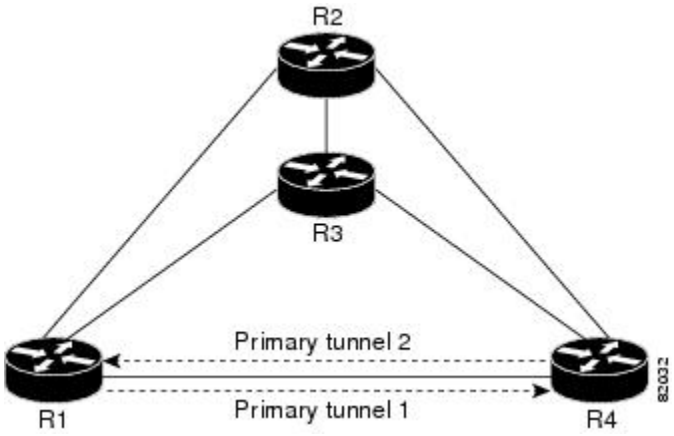
ライマリ トンネル 2 のバックアップ トンネルが同時にトリガーされます。この 2 つのバックアップ トンネルが、ネットワーク内の 1 つのリンクを共有できます。

**図 *4*：*1* つのリンクを共有する複数のバックアップ トンネル**




次の図では、プライマリ トンネル 1 のバックアップ トンネルはルータ R1-R2-R3-R4 を通過でき、プライマリ トンネル 2 のバックアップ トンネルはルータ R4-R2-R3-R1 を通過できます。この場合、R1-R4 に障害が発生すると、リンク R2-R3 が過負荷になることがあります。

**図 *5*：過負荷になったリンク**




## 制限なし帯域幅バックアップ トンネルのロード バランシング

制限なしバックアップ帯域幅を持つ複数のバックアップ トンネルが、1 つのインターフェイスを保護できます。この場合、ある LSP に対するバックアップ トンネルの選択時に、ルータは、最小バックアップ帯域幅を持つバックアップ トンネルを選択します。このアルゴリズムにより、LSP の帯域幅に基づいて、バックアップ トンネル間で均等に LSP が分散されます。LSP がゼロ帯域幅を要求している場合、ルータは、保護している LSP の数が最も少ないバックアップ トンネルを選択します。

## プール タイプおよびバックアップ トンネル

デフォルトでは、バックアップ トンネルは、任意のプール（グローバルプールまたはサブプール）から割り当てる LSP に対して保護を提供します。ただし、グローバルプール帯域幅を使用する LSP だけ、またはサブプール帯域幅を使用する LSP だけを保護するようにバックアップ トンネルを設定することもできます。

## トンネル選択のプライオリティ

ここでは、次の内容について説明します。

### NHOP バックアップ トンネルと NNHOP バックアップ トンネル

1 つの LSP を、複数のバックアップ トンネル（LSP の NNHOP で終端するバックアップ トンネルと、LSP の NHOP で終端するバックアップ トンネル）により保護できます。この場合、ルータは、NNHOP で終端するバックアップ トンネルを選択します（つまり、FRR は NHOP バックアップ トンネルよりも NNHOP バックアップ トンネルを優先します）。

次の表に、トンネル選択のプライオリティを示します。最初に選択されるのは、サブプールまたはグローバル プールから帯域幅を獲得する、制限付き帯域幅を持つ NNHOP バックアップ トンネルです。このようなバックアップ トンネルがない場合、次（2）に選択されるのは、任意のプールから制限付き帯域幅を獲得するネクストネクスト ホップ バックアップ トンネルです。優先順位が 1（最良）から 8（最悪）の順にバックアップ トンネルが選択されます。選択肢 3 は、大きさの制限がないサブプールまたはグローバルプール帯域幅を持つ NNHOP バックアップ トンネルです。

**表 *1*：トンネル選択のプライオリティ**

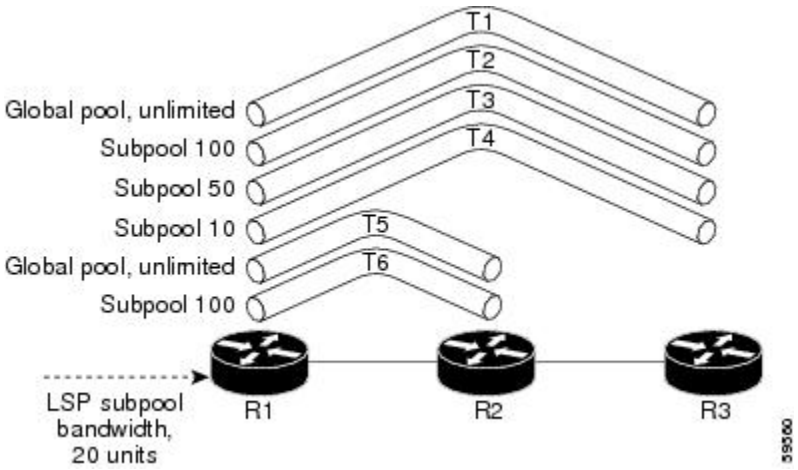
| 優先順位 | バックアップ トンネルの宛先 | 帯域幅プール | 帯域幅の大きさ |
|---|---|---|---|
| 1（最良） | NNHOP | サブプールまたはグローバル プール | Limited |
| 2 | NNHOP | いずれか（Any） | Limited |
| 3 | NNHOP | サブプールまたはグローバル プール | Unlimited |
| 4 | NNHOP | いずれか（Any） | Unlimited |
| 5 | NHOP | サブプールまたはグローバル プール | Limited |
| 6 | NHOP | いずれか（Any） | Limited |

| 優先順位 | バックアップトンネルの宛先 | 帯域幅プール | 帯域幅の大きさ |
|---|---|---|---|
| 7 | NHOP | サブプールまたはグローバル プール | Unlimited |
| 8（最悪） | NHOP | いずれか（Any） | Unlimited |

次の図に、現在使用可能なグローバル プールおよびサブプール帯域幅の指定された大きさに基づいて、バックアップ トンネルが選択される手順の例を示します。

（注） NHOP バックアップ トンネルと NNHOP バックアップ トンネルに十分なバックアップ帯域幅がない場合、LSP が伝送するデータのタイプは考慮されません。たとえば、データ LSP よりも前にシグナリングされない音声 LSP は、保護されないことがあります。バックアップ トンネルの使用に優先順位を付けるためには、「バックアップ保護優先アルゴリズム」セクションを参照してください。

**図 *6*：複数のバックアップ トンネルからの選択**




この例では、LSP には、20 ユニット（キロビット/秒）のサブプール バックアップ帯域幅が必要です。最良バックアップ トンネルは、次のようにして選択されます。

1. バックアップ トンネル T1 から T4 までは、NNHOP で終端するため、最初に考慮されます。
2. トンネル T4 は、サブプール バックアップ帯域幅を 10 ユニットしか持たないため、除外されます。
3. トンネル T1 は、グローバルプール帯域幅を使用して LSP を保護するだけなので、除外されます。

4 トンネル T3 は T2 よりも優先的に選択されます。両方とも十分なバックアップ帯域幅がありますが、T3 の方が使用可能なバックアップ帯域幅が少ないためです（多い方のバックアップ帯域幅は T2 上に維持されます）。

5 トンネル T5 と T6 は、NHOP で終端するため、考慮する必要はありません。このため、NNHOP で終端する T3 の方が、これらよりも優先されます。

### Promotion

LSP のバックアップ トンネルが選択されたあとで、状況が変わったために、この選択を再評価する必要が生じることがあります。この再評価は、成功した場合、プロモーションと呼ばれます。次のような状況がこれに該当します。

1 新しいバックアップ トンネルが出現した。

2 この LSP に対して現在選択されているバックアップ トンネルが停止した。

3 バックアップ トンネルの使用可能なバックアップ帯域幅が増加した。たとえば、トンネルで保護されている LSP が、ヘッドエンドにより、別のパスを使用するように再最適化された場合などです。

ケース 1 とケース 2 では、LSP のバックアップ トンネルがすぐに評価されます。ケース 3 に対処するには、LSP からバックアップ トンネルへのマッピングを定期的に再評価します。デフォルトでは、バックグラウンドの再評価は 5 分ごとに実行されます。この間隔は、**mplstraffic-engfast-reroutetimers** コマンドを使用して設定できます。

### バックアップ保護プリエンプション アルゴリズム

LSP に「bandwidth protection desired」ビットを設定すると、その LSP は、帯域幅保護を提供するバックアップ トンネルの選択権限が大きくなり、そのビット セットを持たない他の LSP をプリエンプション処理できます。

NNHOP バックアップ トンネル上に十分なバックアップ帯域幅がないが、NHOP バックアップ トンネルにはある場合、帯域幅保護されている LSP は、NNHOP LSP をプリエンプション処理せず、NHOP 保護を使用します。

1 つのバックアップ トンネルを使用する LSP が複数存在し、帯域幅を提供するために 1 つ以上の LSP をデモートする必要がある場合、デモート対象の LSP を決定する際に使用できるユーザ設定可能な方法（アルゴリズム）が 2 つあります。

- 無駄な帯域幅の大きさを最小限にする。
- デモートされる LSP の数を最小限にする。

たとえば、バックアップ トンネル上に 10 ユニットのバックアップ帯域幅が必要な場合は、次のいずれかをデモートできます。

- 100 ユニットの帯域幅を使用する単一の LSP：必要な帯域幅より多くの帯域幅が使用可能になりますが、無駄も多くなります。

- 1 ユニットずつ帯域幅を使用する 10 個の LSP：無駄な帯域幅はなくなりますが、影響を受ける LSP が多くなります。

デフォルトのアルゴリズムでは、デモートされる LSP の数が最小限にされます。無駄な帯域幅の大きさを最小限にするためのアルゴリズムに変更するには、**mplstraffic-engfast-reroutebackup-prot-preemptionoptimize-bw** コマンドを入力します。

## 帯域幅保護に関する考慮事項

帯域幅保護を確実に行うには、数多くの方法があります。次の表で、3 つの方式のメリットとデメリットについて説明します。

**表 *2*：帯域幅保護の方式**

| 方式 | 利点 | 欠点 |
|---|---|---|
| バックアップ トンネルに対して帯域幅を明示的に予約 | この方式は簡単です。 | 個別的な障害からの保護を行う複数のバックアップ トンネルが帯域幅を共有できるようにすることが課題です。 |
| ゼロ帯域幅でシグナリングされたバックアップ トンネルを使用 | 個別的な障害からの保護に使用される帯域幅を共有する方法が提供され、帯域幅をより経済的に使用できます。 | ゼロ帯域幅トンネルの適切な配置の決定が複雑になる場合があります。 |
| バックアップ帯域幅保護 | 音声トラフィックの帯域幅保護が確実に行われます。 | 十分なバックアップ帯域幅がない場合、バックアップ帯域幅保護が設定された LSP に帯域幅が必要になると、バックアップ帯域幅保護が設定されていない LSP をいつでもデモートできます。 |

シスコ実装の FRR では、特定のアプローチが強制されることはなく、上記のいずれのアプローチも使用できます。ただし、幅広い設定選択肢がある場合は、それらの選択肢が特定の帯域幅保護方針と一致していることを確認してください。

次の各項では、適切な設定を選択する際の重要事項について説明します。

### 明示的にシグナリングされた帯域幅を持つバックアップ トンネルを使用

バックアップ トンネルに対して、次の 2 つの帯域幅パラメータを設定する必要があります。

- シグナリングされた実際の帯域幅
- バックアップ帯域幅

バックアップ トンネルの帯域幅要件をシグナリングするには、**tunnelmplstraffic-engbandwidth** コマンドを使用して、バックアップ トンネルの帯域幅を設定します。

バックアップ トンネルのバックアップ帯域幅を設定するには、**tunnelmplstraffic-engbackup-bw** コマンドを使用します。

シグナリングされた帯域幅は、バックアップ トンネルのパス上の LSR が、アドミッション コントロールを実行し、適切な帯域幅計算を行うために使用します。

バックアップ帯域幅は、ローカル修復ポイント（PLR）（つまり、バックアップ トンネルのヘッドエンド）が、障害発生時にこのバックアップ トンネルにリルートできるプライマリ トラフィックの量を決定するために使用します。

適切な動作が確実に行われるように、両方のパラメータを設定する必要があります。シグナリングされた帯域幅とバックアップ帯域幅の数値は、同じであることが必要です。

### 保護対象の帯域幅プールと、バックアップ トンネルにより帯域幅が予約される帯域幅プール

**tunnelmplstraffic-engbandwidth** コマンドを使用すると、次の値を設定できます。

- バックアップ トンネルにより予約される帯域幅の大きさ
- 帯域幅を予約する必要のある DS-TE 帯域幅プール

（注） 選択できるプールは 1 つだけです（つまり、バックアップ トンネルは、グローバル プールかサブプールのいずれか一方だけから帯域幅を明示的に予約できます）。

**tunnelmplstraffic-engbackup-bw** コマンドを使用すると、このバックアップ トンネルを使用するためにトラフィックに割り当てる必要のある帯域幅プールを指定できます。複数のプールを指定できます。

保護対象の帯域幅プールと、バックアップ トンネルによりその帯域幅が取り込まれる帯域幅プールとの間に、直接の対応関係はありません。

特定のリンク上で 10 Kbps のサブプール トラフィックに対する帯域幅保護を実現するには、次のコマンドを任意に組み合わせて設定します。

- **tunnelmplstraffic-engbandwidthsub-pool10**

**tunnelmplstraffic-engbackup-bwsub-pool10**

- **tunnelmplstraffic-engbandwidthglobal-pool10**

**tunnelmplstraffic-engbackup-bwsub-pool10global-poolunlimited**

- **tunnelmplstraffic-engbandwidthglobal-pool40**

**tunnelmplstraffic-engbackup-bwsub-pool10global-pool30**

### ゼロ帯域幅でシグナリングされたバックアップ トンネルの使用

帯域幅保護が必要な場合でも、ゼロ帯域幅でシグナリングされたバックアップ トンネルを使用すると有効なことが多くあります。帯域幅が明示的に予約されていないと、帯域幅が保証されないように思われがちです。しかし、必ずしもそうではありません。

次のような状況について検討します。

- リンク保護だけが必要な場合
- サブプール トラフィックにだけ帯域幅保護が必要な場合

予約可能な最大サブプール値が *n* である保護対象リンク AB ごとに、ノード A からノード B へのパスが存在し、予約可能な最大グローバル プール値と最大サブプール値の差が少なくとも *n* になっていることがあります。ネットワーク内の各リンクにこのようなパスが見つかる可能性がある場合、このようなパス上に、すべてのバックアップ トンネルを帯域幅の予約なしで確立できます。単一のリンク障害が発生した場合、1 つだけのバックアップ トンネルがそのパス上のいずれかのリンクを使用します。そのパスでは（グローバル プール内で）少なくとも *n* の帯域幅が使用可能であるため、サブプール トラフィックをプライオリティ キューに分類するためのマーキングとスケジューリングが設定されていれば、サブプール帯域幅が保証されます。

このアプローチにより、個別的なリンク障害を保護する複数のバックアップ トンネル間でグローバルプール帯域幅を共有することが可能になります。バックアップ トンネルは、障害発生後短時間の間だけ（影響を受ける LSP が、使用可能なサブプール帯域幅でそれらの LSP を他のパスにリルートするまで）使用されることが予期されます。相互に関連しない複数のリンクに障害が発生することは、ほとんどありません（ノードまたは共有リスク リンク グループ（SRLG）に障害がない場合にかぎります。このような場合は、複数のリンク障害が発生します）。したがって、実際にはリンク障害は個別的である可能性が高いと仮定できます。このような「個別的な障害の前提」を、明示的に帯域幅を予約することなくシグナリングされたバックアップ トンネルと組み合わせることにより、効率的な帯域幅共有が可能になり、大幅な帯域幅節約につながります。

サブプール トラフィックを保護するバックアップ トンネルは、いずれのプールからも帯域幅を取り込みません。グローバル プールを使用するプライマリ トラフィックは、グローバル プール全体を使用できます。また、サブプールを使用するプライマリ トラフィックは、サブプール全体を使用できます。ただし、単一のリンク障害が発生した場合、サブプール トラフィックに対する完全な帯域幅保証が行われます。

ノード保護と SRLG 保護に対しても、同様のアプローチを使用できます。ただし、ノード障害と SRLG 障害ではいずれも複数のリンクに同時に障害が発生するため、バックアップ トンネルの配置場所の決定がさらに複雑になります。したがって、影響を受けるすべてのリンクを通過するトラフィックを保護するバックアップ トンネルを、互いに独立して計算することはできません。別々の障害に対応するリンクのグループを保護するバックアップ トンネルは、互いに独立して計算できるため、同様の帯域幅節約を実現できます。

### シグナリングされた帯域幅とバックアップ帯域幅

（バックアップ トンネルのヘッドエンドであるルータが）バックアップ帯域幅をローカルに使用して、特定のバックアップ トンネル上にリルートできるプライマリ LSP とその数を決定します。ルータは、これらの LSP の帯域幅要件の組み合わせがバックアップ帯域幅を超えないようにします。

このため、バックアップ トンネルがゼロ帯域幅でシグナリングされていても、このバックアップ トンネルにより保護されるトラフィックの実際の帯域幅要件に対応する値を使用して、バックアップ帯域幅を設定する必要があります。バックアップ トンネルの帯域幅要件が明示的にシグナリングされている場合とは異なり、シグナリングされた帯域幅の値（ゼロ）は、バックアップ帯域幅の値とは異なります。

# MPLS トラフィック エンジニアリング - 高速リルート リンクおよびノード保護の設定方法

ここでは、MPLS TE LSP が設定されているネットワークに FRR 保護を追加することを前提としています。

## LSP 上での高速リルートの有効化

LSP は、高速リルート可能として設定されている場合だけ、バックアップ トンネルを使用できます。これを行うには、各 LSP のヘッドエンドで次のコマンドを入力します。

### 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **tunnelmplstraffic-engfast-reroute** [**bw-protect**]

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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 | **interfacetunnel***number*<br><br>例：<br>`Router(config)# interface tunnel 1000` | 指定したトンネルのインターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 4 | **tunnelmplstraffic-engfast-reroute** [**bw-protect**]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect` | リンクまたはノードの障害発生時に、MPLS TE トンネルで、確立されたバックアップ トンネルを使用できるようにします。 |

# ネクスト ホップまたはネクストネクスト ホップへのバックアップ トンネルの作成

バックアップ トンネルの作成は、基本的に他のトンネルの作成と同じです。ネクストホップまたはネクストネクスト ホップへのバックアップ トンネルを作成するには、バックアップ トンネルのヘッドエンドとなるノード（つまり、ダウンストリームのリンクまたはノードに障害が発生する可能性のあるノード）上で、次のコマンドを入力します。これらのコマンドを入力するノードは、サポートされているプラットフォームであることが必要です。「機能情報の確認」セクションを参照してください。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipunnumbered***interface-typeinterface-number*
5. **tunneldestination***ip-address*
6. **tunnelmodemplstraffic-eng**
7. **tunnelmplstraffic-engpath-option**[**protect**] *preference-number*{**dynamic** | **explicit**|{**name***path-name* | *path-number*}}[**lockdown**]
8. **ipexplicit-pathname***word*
9. **exclude-address***ip-address*

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **interfacetunnel***number*<br><br>例：<br><br>`Router(config)# interface tunnel 1` | 新しいトンネル インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **ipunnumbered***interface-typeinterface-number*<br><br>例：<br><br>`Router(config-if)# ip unnumbered loopback 0` | このトンネル インターフェイスに、インターフェイス Loopback0 の IP アドレスと同じ IP アドレスを割り当てます。<br><br>（注） このコマンドは、Lookback0 が IP アドレスとともに設定されるまでは有効になりません。 |
| ステップ 5 | **tunneldestination***ip-address*<br><br>例：<br><br>`Router(config-if)# tunnel destination 10.3.3.3` | トンネルが終端するデバイスの IP アドレスを指定します。このアドレスは、保護対象となる LSP の NHOP または NNHOP であるデバイスのルータ ID にする必要があります。 |
| ステップ 6 | **tunnelmodemplstraffic-eng**<br><br>例：<br><br>`Router(config-if)# tunnel mode mpls traffic-eng` | トンネルのカプセル化モードを MPLS TE に設定します。 |
| ステップ 7 | **tunnelmplstraffic-engpath-option**[**protect**] *preference-number*{**dynamic** \| **explicit**\|{**name***path-name* \| *path-number*}}[**lockdown**]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit avoid-protected-link` | MPLS TE トンネルのパス オプションを設定します。ルータ コンフィギュレーション モードを開始します。 |
| ステップ 8 | **ipexplicit-pathname***word*<br><br>例：<br><br>`Router(config-router)# ip explicit-path name avoid-protected-link` | IP 明示パス用のコマンド モードを開始し、指定されたパスを作成します。明示パス コマンド 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 9 | **exclude-address***ip-address*<br><br>例：<br><br>例：<br><br>例：<br><br>例：<br><br>例：<br><br>例：<br><br>`Router(config-ip-expl-path)# exclude-address 3.3.3.3` | リンク保護の場合は、保護対象のリンクの IP アドレスを指定します。ノード保護の場合は、保護対象のノードのルータ ID を指定します。<br><br>（注） バックアップ トンネル パスはダイナミックにも明示的にもできます。exclude-address を使用する必要はありません。バックアップ トンネルは保護対象のリンクまたはノードを回避する必要があるため、**exclude-address** コマンドを使用すると役立ちます。<br>（注） **exclude-address** コマンドを使用してバックアップ トンネルのパスを指定するときは、インターフェイス IP アドレスを除外してリンクを除外する（NHOP バックアップ トンネルを作成する場合）か、ルータ ID アドレスを除外してノードを回避する（NNHOP バックアップ トンネルを作成する場合）必要があります。 |

# 保護インターフェイスへのバックアップ トンネルの割り当て

1 つ以上のバックアップ トンネルを保護インターフェイスに割り当てるには、バックアップ トンネルのヘッドエンドとなるノード（つまり、ダウンストリームのリンクまたはノードに障害が発生する可能性のあるノード）上で、次のコマンドを入力します。これらのコマンドを入力するノードは、サポートされているプラットフォームであることが必要です。「機能情報の確認」セクションを参照してください。

（注） インターフェイスに IP アドレスを割り当てて、MPLS TE トンネル機能がイネーブルになるようにインターフェイスを設定する必要があります。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typeslot*/*port*
4. **mplstraffic-engbackup-pathtunnel***interface*

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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***typeslot/port*<br><br>例：<br><br>例：<br><br>例：<br><br>例：<br><br>例：<br>`Router(config)# interface POS 5/0` | 設定を物理インターフェイス レベルに移動し、後続のコンフィギュレーション コマンドを、*type* の値で識別された特定の物理インターフェイスに指定します。*slot* および *port* は、設定するスロットおよびポートを識別します。インターフェイスは、サポートされているインターフェイスであることが必要です。「機能情報の確認」セクションを参照してください。インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **mplstraffic-engbackup-pathtunnel***interface*<br><br>例：<br>`Router(config-if)# mpls traffic-eng backup-path tunnel 2` | リンクまたはノードの障害が発生した場合に、このインターフェイスを出る LSP がこのバックアップ トンネルを使用できるようにします。<br>（注） このコマンドを何回か入力して、複数のバックアップ トンネルを同じ保護インターフェイスと関連付けることができます。 |

# バックアップ トンネルへのバックアップ帯域幅およびプール タイプの関連付け

バックアップ帯域幅をバックアップ トンネルに関連付け、バックアップ トンネルを使用できる LSP のタイプを指定するには、次のコマンドを入力します。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **tunnelmplstraffic-engbackup-bw** {*bandwidth* | [**sub-pool** {*bandwidth* | **Unlimited**}] [**global-pool** {*bandwidth* | **Unlimited**}]

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **interfacetunnel***number*<br><br>例：<br><br>`Router(config)# interface tunnel 2` | 指定したトンネルのインターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **tunnelmplstraffic-engbackup-bw** {*bandwidth* \| [**sub-pool** {*bandwidth* \| **Unlimited**}] [**global-pool** {*bandwidth* \| **Unlimited**}]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000` | 帯域幅をバックアップ トンネルに関連付け、指定されたプールから帯域幅を割り当てられた LSP がこのトンネルを使用できるかどうかを指定します。 |

# バックアップ帯域幅保護の設定

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **tunnelmplstraffic-engfast-reroute** [**bw-protect**]
4. **mplstraffic-engfast-reroutebackup-prot-preemption** [**optimize-bw**]

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`Router# configure terminal` | インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | **tunnelmplstraffic-engfast-reroute** [**bw-protect**]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect` | MPLS TE トンネルが、リンクまたはノードの障害発生時に、確立されたバックアップ トンネルを使用できるようにします。<br><br>• **bw-protect** キーワードを指定すると、帯域幅保護されたバックアップ トンネルを使用するための LSP プライオリティが付与されます。グローバル コンフィギュレーション モードを開始します。 |
| ステップ 4 | **mplstraffic-engfast-reroutebackup-prot-preemption** [**optimize-bw**]<br><br>例：<br><br>`Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw` | バックアップ保護プリエンプションアルゴリズムを、デモートされる LSP の数を最小限にするアルゴリズムから、無駄な帯域幅の大きさを最小限にするアルゴリズムに変更します。 |

# リンクおよびノード障害を高速検出するためのインターフェイスの設定

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typeslot*/*port*
4. **posais-shut**
5. **posreport** {**b1-tca** | **b2-tca** | **b3-tca** | **lais** | **lrdi** | **pais** | **plop** | **prdi** | **rdool** | **sd-ber** | **sf-ber** | **slof** | **slos**}

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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***typeslot*/*port*<br><br>例：<br>`Router(config)# interface pos0/0` | インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **posais-shut**<br><br>例：<br>`Router(config-if)# pos ais-shut` | POS インターフェイスが管理シャットダウン ステートになったときに、ラインのアラーム表示信号（LAIS）を送信します。 |
| ステップ 5 | **posreport** {**b1-tca** \| **b2-tca** \| **b3-tca** \| **lais** \| **lrdi** \| **pais** \| **plop** \| **prdi** \| **rdool** \| **sd-ber** \| **sf-ber** \| **slof** \| **slos**}<br><br>例：<br>`Router(config-if)# pos report lrdi` | 選択した SONET アラームが POS インターフェイス用のコンソールに記録されるようにします。 |

# 高速リルートの動作状態の確認

## 手順の概要

1. **showmplstraffic-engtunnelsbrief**
2. **showiprsvpsenderdetail**
3. **showmplstraffic-engfast-reroutedatabase**
4. **showmplstraffic-engtunnelsbackup**
5. **showmplstraffic-engfast-reroutedatabase**
6. **showiprsvpreservation**

## 手順の詳細

**ステップ 1** **showmplstraffic-engtunnelsbrief**

このコマンドを使用して、バックアップ トンネルが動作していることを確認します。

例：

```
Router# show mpls traffic-eng tunnels brief
```

次に、**show mpls traffic-eng tunnels brief** コマンドのサンプル出力を示します。

例：

```
Signalling Summary:
    LSP Tunnels Process:           running
    RSVP Process:                  running
    Forwarding:                    enabled
    Periodic reoptimization:       every 3600 seconds, next in 1706 seconds
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
Router_t1                        10.112.0.12      -         PO4/0/1   up/up
Router_t2                        10.112.0.12      -         unknown   up/down
Router_t3                        10.112.0.12      -         unknown   admin-down
Router_t1000                     10.110.0.10      -         unknown   up/down
Router_t2000                     10.110.0.10      -         PO4/0/1   up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

**ステップ 2** **showiprsvpsenderdetail**

このコマンドを使用して、LSP が適切なバックアップ トンネルによって保護されていることを確認します。

次に、障害発生前に PLR で **show ip rsvp sender detail** コマンドが入力されたときのサンプル出力を示します。

例：

```
Router# show ip rsvp sender detail
```

```
PATH:
 Tun Dest:   10.10.0.6  Tun ID: 100  Ext Tun ID: 10.10.0.1
 Tun Sender: 10.10.0.1  LSP ID: 31
 Path refreshes:
  arriving: from PHOP 10.10.7.1 on Et0/0 every 30000 msecs
 Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0x7) Local Prot desired, Label Recording, SE Style
  session Name: R1_t100
 ERO: (incoming)
  10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
  10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
 RRO:
   10.10.7.1/32, Flags:0x0 (No Local Protection)
   10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP) !Available to NNHOP
   10.10.1.1/32, Flags:0x0 (No Local Protection)
 Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
   Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
 Fast-Reroute Backup info:
   Inbound  FRR: Not active
   Outbound FRR: No backup tunnel selected
 Path ID handle: 50000416.
 Incoming policy: Accepted. Policy source(s): MPLS/TE
 Status: Proxy-terminated
```

**ステップ 3** **showmplstraffic-engfast-reroutedatabase**
**clear ip rsvp hello instance counters** コマンドを入力して、次のことを確認します。

- MPLS TE FRR ノード保護がイネーブルになっている。
- 特定タイプの LSP がバックアップ トンネルを使用できる。

次のコマンド出力は、保護されている LSP を表しています。

例：

```
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected Tunnel      In-label   intf/label       FRR intf/label     Status
Tunne110              Tun        pos5/0:Untagged  Tu0:12304          ready
Prefix item frr information:
Prefix        Tunnel  In-label   Out intf/label   FRR intf/label     Status
10.0.0.11/32  Tu110   Tun hd     pos5/0:Untagged  Tu0:12304          ready
LSP midpoint frr information:
LSP identifier        In-label   Out intf/label   FRR intf/label     Status
10.0.0.12 1 [459]     16         pos0/1:17        Tu2000:19          ready
```

LDP がイネーブルになっていない場合、すべてのプレフィックスが単一のリライトを使用するため、個別のプレフィックス アイテムは表示されません。特定の IP プレフィックスがこの画面に表示されていない場合、その IP プレフィックスが FRR 保護されていることを確認するには、**show mpls forwarding-table** *ip-address* **detail** コマンド内にそのプレフィックスを入力します。画面の最後の行に、そのプレフィックスが保護されているかどうかが示されます。

例：

```
Router# show mpls forwarding-table 10.0.0.11 detail

Local    Outgoing    Prefix         Bytes tag    Outgoing     Next Hop
tag      tag or VC   or Tunnel Id   switched     interface
Tun hd   Untagged    10.0.0.11/32   48           pos5/0       point2point
          MAC/Encaps=4/8, MTU=1520, Tag Stack{22}
```

```
48D18847 00016000
No output feature configured
Fast Reroute Protection via (Tu0, outgoing label 12304)
```

**ステップ 4** **showmplstraffic-engtunnelsbackup**

バックアップ トンネルが動作するには、LSP がリルート可能になっている必要があります。LSP のヘッドエンドで、**show run int tunnel** *tunnel-number* コマンドを入力します。出力に **tunnel mpls traffic-eng fast-reroute** コマンドが含まれている必要があります。このコマンドが含まれていない場合は、トンネルに対してこのコマンドを入力してください。

バックアップ トンネルの起点のルータ上で、**show mpls traffic-eng tunnels backup** コマンドを入力します。次にサンプルのコマンド出力を示します。

例：

```
Router# show mpls traffic-eng tunnels backup

Router_t578
  LSP Head, Tunnel578, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0, PO1/1, PO3/3
    Protected lsps: 1
    Backup BW: any pool unlimited; inuse: 100 kbps
Router_t5710
  LSP Head, Tunnel5710, Admin: admin-down, Oper: down
  Src 10.55.55.55, Dest 10.7.7.7, Instance 0
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/1
    Protected lsps: 0
    Backup BW: any pool unlimited; inuse: 0 kbps
Router_t5711
  LSP Head, Tunnel5711, Admin up, Oper: up
  Src 10.55.55.55,, Dest 10.7.7.7, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0
    Protected lsps: 2
    Backup BW: any pool unlimited; inuse: 6010 kbps
```

コマンド出力により、次のことを確認できます。

- バックアップ トンネルが存在している：この LSP の NHOP または NNHOP で終端するバックアップ トンネルが存在することを確認します。[Dest] フィールド内で LSP の NHOP または NNHOP を検索します。
- バックアップ トンネルが動作している：バックアップ トンネルが動作していることを確認するには、[State] フィールド内で「Up」を検索します。
- バックアップ トンネルが LSP のインターフェイスに関連付けられている：LSP のインターフェイスがこのバックアップ トンネルを使用できるように設定されていることを確認します。保護フィールド リスト内で LSP の出力インターフェイスを検索します。
- バックアップ トンネルに十分な帯域幅がある：バックアップ トンネルが保有できる帯域幅を制限した場合は、障害発生時にこのバックアップ トンネルを使用する LSP を確保できるだけの帯域幅がバックアップ トンネルにあることを確認します。LSP の帯域幅は、LSP のヘッドエンドにある **tunnel mpls traffic-eng bandwidth** 行によって定義されます。バックアップ トンネル上の使用可能な帯域幅を判断するには、[cfg] フィールドと [inuse] フィールドを参照してください。障害発生時にこのバックアップ トンネルを使用する LSP に対して十分な帯域幅がない場合は、追加のバックアップ トンネルを作

成するか、**tunnel mpls traffic-eng bandwidth** コマンドを使用して、既存のトンネルのバックアップ帯域幅を広げます。

（注） 十分な帯域幅の大きさを決定するために、オフラインでのキャパシティ プランニングが必要になることがあります。

- バックアップ トンネルに適切な帯域幅タイプが割り当てられている：このバックアップ トンネルを使用できる LSP のタイプを（サブプールまたはグローバル プールに）制限した場合、その LSP がバックアップ トンネルに適したタイプであることを確認します。LSP のタイプは、この LSP のヘッドエンドにある行 **tunnel mpls traffic-eng bandwidth** によって定義されています。この行に「subpool」という語が含まれている場合、LSP はサブプール帯域幅を使用します。含まれていない場合は、グローバル プール帯域幅を使用します。**tunnel mpls traffic-eng bandwidth** コマンドの出力を参照して、LSP タイプが、バックアップ トンネルが保有できるタイプと一致していることを確認します。

また、バックアップ トンネルのヘッドエンドにあるルータ上で **debug ip rsvp fast-reroute** コマンドおよび **debug mpls traffic-eng fast-reroute** コマンドを入力することにより、デバッグを有効にすることもできます。続いて、次の手順を実行します。

1. プライマリ トンネルに対して **shutdown** コマンドを入力します。
2. プライマリ トンネルに対して **no shutdown** コマンドを入力します。
3. デバッグ出力を参照します。

**ステップ 5** **showmplstraffic-engfast-reroutedatabase**
**clear ip rsvp hello instance counters** コマンドを入力して、次のことを確認します。

- MPLS TE FRR ノード保護がイネーブルになっている。
- 特定タイプの LSP がバックアップ トンネルを使用できる。

次のコマンド出力は、保護されている LSP を表しています。

例：

```
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected Tunnel   In-label   intf/label       FRR intf/label      Status
Tunnel10           Tun        pos5/0:Untagged  Tu0:12304           ready
Prefix item frr information:
Prefix        Tunnel  In-label    Out intf/label   FRR intf/label Status
10.0.0.11/32  Tu110   Tun hd      pos5/0:Untagged  Tu0:12304      ready
LSP midpoint frr information:
LSP identifier       In-label Out intf/label   FRR intf/label   Status
10.0.0.12 1 [459]    16       pos0/1:17        Tu2000:19        ready
```

（注） LDP がイネーブルになっていない場合、すべてのプレフィックスが単一のリライトを使用するため、個別のプレフィックスアイテムは表示されません。特定の IP プレフィックスがこの画面に表示されていない場合、その IP プレフィックスが FRR 保護されていることを確認するには、**show mpls forwarding-table** *ip-address* **detail** コマンド内にそのプレフィックスを入力します。画面の最後の行に、そのプレフィックスが保護されているかどうかが示されます。

例：

```
Router# show mpls forwarding-table 10.0.0.11 detail

Local    Outgoing    Prefix         Bytes tag    Outgoing     Next Hop
tag      tag or VC   or Tunnel Id   switched     interface
Tun hd   Untagged    10.0.0.11/32   48           pos5/0       point2point
          MAC/Encaps=4/8, MTU=1520, Tag Stack{22}
          48D18847 00016000
          No output feature configured
          Fast Reroute Protection via (Tu0, outgoing label 12304)
```

**ステップ 6** **showiprsvpreservation**

次に、プライマリ LSP のヘッドエンドに入力された **show ip rsvp reservation** コマンドの出力例を示します。プライマリ LSP のヘッドエンドにコマンドを入力すると、この LSP が通過する各ホップでの FRR のステータス（つまり、ローカル保護）などが表示されます。各ホップの情報は、Resv メッセージとともに末尾から先頭に移動する Record Route Object（RRO）内に収集されます。

例：

```
Router# show ip rsvp reservation detail
Reservation:
  Tun Dest: 10.1.1.1  Tun ID: 1  Ext Tun ID: 172.16.1.1
  Tun Sender: 172.16.1.1  LSP ID: 104
  Next Hop: 172.17.1.2 on POS1/0
  Label: 18 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  RRO:
    172.18.1.1/32, Flags:0x1 (Local Prot Avail/to NHOP)
      Label subobject: Flags 0x1, C-Type 1, Label 18
    172.19.1.1/32, Flags:0x0 (Local Prot Avail/In Use/Has BW/to NHOP)
      Label subobject: Flags 0x1, C-Type 1, Label 16
    172.19.1.2/32, Flags:0x0 (No Local Protection)
      Label subobject: Flags 0x1, C-Type 1, Label 0
  Resv ID handle: CD000404.
  Policy: Accepted. Policy source(s): MPLS/TE
```

プライマリ LSP に関して、次の点に注意してください。

- プライマリ LSP には、最初のホップで NHOP バックアップ トンネルを使用するような保護が設定されています。
- また、2 番めのホップで NHOP バックアップ トンネルをアクティブに使用するような保護が設定されています。
- 3 番めのホップでは、ローカルな保護は設定されていません。

RRO 画面には、ホップごとに次の情報が表示されます。

- ローカル保護が使用可能かどうか（つまり、LSP によりバックアップ トンネルが選択されているかどうか）
- ローカル保護が使用中かどうか（つまり、LSP が、選択したバックアップ トンネルを現在使用しているかどうか）

- 選択されたバックアップ トンネルは、NHOP バックアップ トンネルか NNHOP バックアップ トンネルのいずれであるか
- このホップで使用されるバックアップ トンネルが帯域幅保護を提供するかどうか

## トラブルシューティングのヒント

ここでは、次の内容について説明します。

### LSP が Ready のまま Active にならない

次のいずれかのイベントが発生すると、PLR で LSP は Ready から Active に移行します。

- プライマリ インターフェイスが停止した：プライマリ インターフェイス（LSP の発信インターフェイス）が停止した場合、LSP がバックアップ トンネルを使用する準備が完了すれば、LSP はアクティブ状態に移行し、そのデータがバックアップ トンネル上を流れるようになります。一部のプラットフォームおよびインターフェイス タイプ（たとえば、GSR POS インターフェイスなど）では、このイベントを非常にすばやく検出する高速インターフェイス停止ロジックがあります。このロジックが存在しないプラットフォームでは、検出時間が遅くなります。このようなプラットフォームでは、RSVP Hello を有効にすると動作する場合があります（次の箇条書き項目「Hello によりネクスト ホップが停止していることが検出された」を参照）。
- Hello によりネクスト ホップが停止していることが検出された：プライマリ インターフェイス（LSP の発信インターフェイス）上で Hello が有効になっている場合、LSP のネクストホップが到達不能になると、そのネクストホップが停止していると宣言されます。このイベントによって、LSP はそのバックアップ トンネルをアクティブに使用し始めます。プライマリ インターフェイスが停止していなくても、ネクストホップは停止していると宣言されることに注意してください。たとえば、リブート、ソフトウェア、またはハードウェアの問題によってネクスト ホップが応答を停止した場合、Hello が、このネクスト ホップを使用して LSP をトリガーし、そのバックアップ トンネルに切り替えます。また、Hello は、ギガビット イーサネットなど、インターフェイスは動作しているが（リンク層のライブネス検出メカニズムがないために）使用可能になっていないインターフェイス上で FRR をトリガーする支援も行います。

### プライマリ トンネルにより動作中のバックアップ トンネルが選択されない

バックアップ トンネルが動作中であるのに、プライマリ トンネル（LSP）によってバックアップ トンネルとして選択されない場合は、バックアップ トンネルに対して次のコマンドを入力します。

- **シャットダウン**
- **noshutdown**

（注） バックアップ トンネルのステータスを変更した場合、そのバックアップ トンネルに対してバックアップ トンネル選択アルゴリズムが再実行されます。現在そのバックアップ トンネルが選択されている（つまり、バックアップ トンネルを使用する準備ができている）LSP は、そのバックアップ トンネルとの関連付けが解除されてから、そのバックアップ トンネルまたは別のバックアップ トンネルと再び関連付けられます。これは一般に安全であり、通常は同じLSPがそのバックアップ トンネルにマップされます。ただし、そのバックアップ トンネルをアクティブに使用しているLSPがある場合、そのバックアップ トンネルをシャットダウンすると、それらの LSP が切断されます。

### 拡張 RSVP コマンドにより有用な情報が表示される

次の RSVP コマンドは拡張されて、FRR ステートの検証や FRR のトラブルシューティング時に役立つ情報が表示されるようになりました。

- **showiprsvprequest**：アップストリーム予約ステート（つまり、このノードがアップストリーム送信する Resv メッセージに関連する情報）を表示します。
- **showiprsvpreservation**：受信された Resv メッセージに関する情報を表示します。
- **showiprsvpsender**：受信される path メッセージに関する情報を表示します。

これらのコマンドは、データ ステートではなく、コントロール プレーン ステートを表示します。つまり、これらのコマンドは、LSP のシグナリングに使用される RSVP メッセージ（Path および Resv）に関する情報を表示します。LSP 上を転送されるデータ パケットの詳細については、**showmplsforwarding** コマンドを使用してください。

### RSVP Hello によりネイバー ノードが到達不能であることが検出される

RSVP Hello 機能を使用すると、RSVP ノードは、ネイバー ノードが到達不能になった場合にそれを検出できます。リンク層障害の通知が使用可能でなく、番号なしのリンクが使用されていない場合、またはリンク層により提供される障害検出メカニズムが十分でないためにタイムリーにノード障害を検出できない場合は、この機能を使用してください。Hello を操作できるようにするには、Hello をルータでグローバルに設定し、さらに特定のインターフェイス上でも設定する必要があります。

### Hello インスタンスが作成されていない

Hello インスタンスが作成されていない場合は、次の手順を実行します。

- RSVP Hello がルータ上でグローバルにイネーブルになっているかどうかを判断します。**iprsvpsignallinghello**（コンフィギュレーション）コマンドを入力します。
- RSVP Hello が、LSP が通過するインターフェイス上でイネーブルになっているかどうかを判断します。**iprsvpsignallinghello**（インターフェイス）コマンドを入力します。

- **showiprsvpsender** コマンドの出力を表示することにより、少なくとも 1 つの LSP にバックアップ トンネルがあることを確認します。「Ready」の値は、バックアップ トンネルが選択されていることを示します。

### 「No entry at index (error may self-correct, RRO may not yet have propagated from downstream node of interest)」というエラーメッセージがローカル修復ポイントで出力される

FRR は、ダウンストリームから到着する Resv メッセージ内の RRO に依存しています。LSP が高速リルート可能であることを示す SESSION_ATTRIBUTE ビットが含まれる path メッセージを受信するルータは、対応する Resv メッセージに RRO を組み込む必要があります。

LSP が FRR 用に設定されているが、ダウンストリーム ルータから到着する Resv に不完全な RRO が含まれる場合、「No entry at index (error may self-correct, RRO may not yet have propagated from downstream node of interest)」というメッセージが出力されます。不完全な RRO とは、NHOP または NNHOP で RRO にエントリが組み込まれなかった RRO のことです。

このエラーは、通常、RRO エントリが不足しているために NHOP または NNHOP に関する情報が十分でなく、この LSP に対して NHOP または NNHOP へのバックアップ トンネルを選択できないことを示しています。

この状況が一時的に発生しても、問題が自動的に修正されることもあります。あとから Resv メッセージが完全な RRO とともに受信された場合は、エラーメッセージを無視してください。

エラーが修正されたかどうかを判断するには、**clearirsvphelloinstancecounters** コマンドを入力して、Resv メッセージ内の RRO を表示します。問題の LSP だけを表示するには、出力フィルタ キーワードを使用します。

### ローカル修復ポイントで「Couldn't get rsbs (error may self-correct when Resv arrives)」というエラーメッセージが出力される

Resv メッセージがダウンストリームから到着するまで、PLR は LSP のバックアップ トンネルを選択できません。

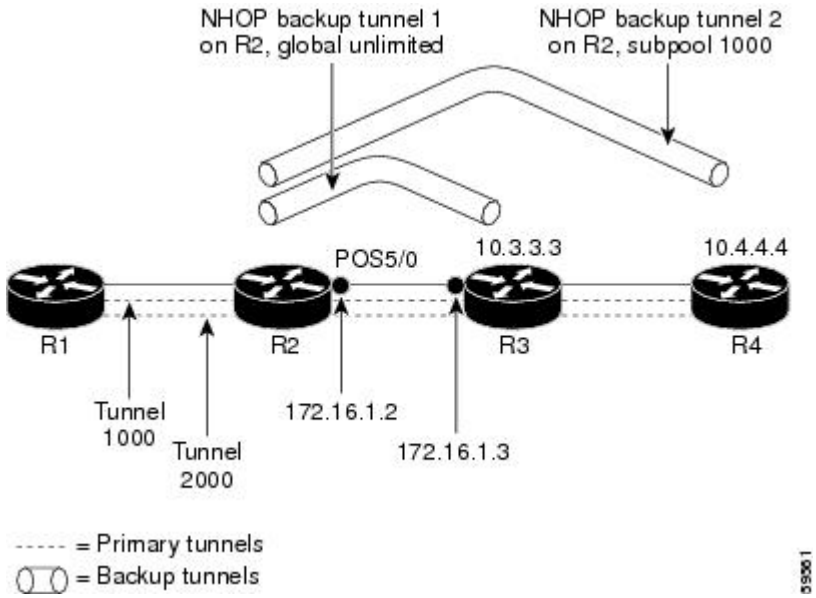
このエラーが発生した場合、通常は何か問題があることを示しています。たとえば、この LSP に対して予約が存在しないなどです。この問題をトラブルシューティングするには、**debugiprsvpreservation** コマンドを使用してデバッグを有効にします。

このエラーメッセージが発生しても、無視できる場合もあります。たとえば、Resv メッセージがダウンストリームから到着する前に LSP が変更された場合などです。変更されると、PLR が LSP に対するバックアップ トンネルの選択を試行することがあります。このとき、この LSP に対して Resv メッセージが到着していないと、選択は失敗します（それにより、このエラーメッセージが表示されます）。

# MPLS トラフィック エンジニアリング：高速リルートリンクおよびノード保護の設定例

これらの例は、次の図に関連しています。

図 7：バックアップ トンネル




## すべてのトンネルに対する高速リルートの有効化：例

ルータ R1 上で、保護対象のトンネル（トンネル 1000 とトンネル 2000）ごとにインターフェイス コンフィギュレーション モードを開始します。パス上でリンクまたはノードの障害が発生した場合に、これらのトンネルがバックアップ トンネルを使用できるようにします。

トンネル 1000 は、サブプールから 10 ユニットの帯域幅を使用します。

トンネル 2000 は、グローバル プールから 5 ユニットの帯域幅を使用します。**tunnel mpls traffic-eng fast-reroute** コマンド内で **bw-prot** を指定することにより、「bandwidth protection desired」ビットが設定されています。

```
Router(config)# interface Tunnel 1000
Router(config-if)# tunnel mpls traffic-eng fast-reroute
Router(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 10
Router(config)# interface Tunnel2000
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-prot
Router(config-if)# tunnel mpls traffic-eng bandwidth 5
```

# NHOP バックアップ トンネルの作成：例

ルータ R2 上に、R3 への NHOP バックアップ トンネルを作成します。このバックアップ トンネルは、リンク 172.1.1.2 の使用を回避する必要があります。

```
Router(config)# ip explicit-path name avoid-protected-link
Router(cfg-ip-expl-path)# exclude-address 172.1.1.2
Explicit Path name avoid-protected-link:
____1: exclude-address 172.1.1.2
Router(cfg-ip_expl-path)# end
Router(config)# interface Tunnel 1
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel destination 10.3.3.3
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit avoid-protected-link
```

# NNHOP バックアップ トンネルの作成：例

ルータ R2 上に、R4 への NNHOP バックアップ トンネルを作成します。このバックアップ トンネルは R3 を回避する必要があります。

```
Router(config)# ip explicit-path name avoid-protected-node

Router(cfg-ip-expl-path)# exclude-address 10.3.3.3
Explicit Path name avoid-protected-node:
____1: exclude-address 10.3.3.3
Router(cfg-ip_expl-path)# end

Router(config)# interface Tunnel 2

Router(config-if)# ip unnumbered loopback0

Router(config-if)# tunnel destination 10.4.4.4

Router(config-if)# tunnel mode mpls traffic-eng

Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit avoid-protected-node
```

# 保護インターフェイスへのバックアップ トンネルの割り当て

1 つ以上のバックアップ トンネルを保護インターフェイスに割り当てるには、バックアップ トンネルのヘッドエンドとなるノード（つまり、ダウンストリームのリンクまたはノードに障害が発生する可能性のあるノード）上で、次のコマンドを入力します。これらのコマンドを入力するノードは、サポートされているプラットフォームであることが必要です。「機能情報の確認」セクションを参照してください。

（注） インターフェイスに IP アドレスを割り当てて、MPLS TE トンネル機能がイネーブルになるようにインターフェイスを設定する必要があります。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typeslot*/*port*
4. **mplstraffic-engbackup-pathtunnel***interface*

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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***typeslot*/*port*<br><br>例：<br><br>例：<br><br>例：<br><br>例：<br><br>例：<br>`Router(config)# interface POS 5/0` | 設定を物理インターフェイス レベルに移動し、後続のコンフィギュレーション コマンドを、*type* の値で識別された特定の物理インターフェイスに指定します。*slot* および *port* は、設定するスロットおよびポートを識別します。インターフェイスは、サポートされているインターフェイスであることが必要です。「機能情報の確認」セクションを参照してください。インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **mplstraffic-engbackup-pathtunnel***interface*<br><br>例：<br>`Router(config-if)# mpls traffic-eng backup-path tunnel 2` | リンクまたはノードの障害が発生した場合に、このインターフェイスを出る LSP がこのバックアップ トンネルを使用できるようにします。<br>（注） このコマンドを何回か入力して、複数のバックアップ トンネルを同じ保護インターフェイスと関連付けることができます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|

# バックアップ トンネルへのバックアップ帯域幅およびプール タイプの関連付け

バックアップ帯域幅をバックアップ トンネルに関連付け、バックアップ トンネルを使用できる LSP のタイプを指定するには、次のコマンドを入力します。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **tunnelmplstraffic-engbackup-bw** {*bandwidth* | [**sub-pool** {*bandwidth* | **Unlimited**}] [**global-pool** {*bandwidth* | **Unlimited**}]

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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 | **interfacetunnel***number*<br><br>例：<br>`Router(config)# interface tunnel 2` | 指定したトンネルのインターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 4 | **tunnelmplstraffic-engbackup-bw** {*bandwidth* \| [**sub-pool** {*bandwidth* \| **Unlimited**}] [**global-pool** {*bandwidth* \| **Unlimited**}]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000` | 帯域幅をバックアップ トンネルに関連付け、指定されたプールから帯域幅を割り当てられた LSP がこのトンネルを使用できるかどうかを指定します。 |

# バックアップ帯域幅保護の設定：例

次の例では、バックアップ帯域幅保護が設定されています。

（注） このグローバル設定が必要なのは、バックアップ保護プリエンプション アルゴリズムを、デモートされる LSP の数を最小限にするアルゴリズムから、無駄な帯域幅の大きさを最小限にするアルゴリズムに変更する場合だけです。

```
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect
Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw
```

# リンクおよびノード障害を高速検出するためのインターフェイスの設定：例

次の例では、pos ais-shut が設定されています。

```
Router(config)# interface pos 0/0

Router(config-if)# pos ais-shut
```

次の例では、OS インターフェイス上に report lrdi が設定されています。

```
Router(config)# interface pos 0/0
Router(config-if)# pos report lrdi
```

# RSVP Hello および POS シグナルの設定：例

Hello は、ルータ上でグローバルに設定し、さらに FRR 保護の必要な特定のインターフェイス上でも設定する必要があります。Hello を設定するには、次のコンフィギュレーション コマンドを使用します。

- **iprsvpsignallinghello**（コンフィギュレーション）：ルータ上でグローバルに Hello を有効にします。
- **iprsvpsignallinghello**（インターフェイス）：FRR 保護が必要なインターフェイス上で Hello を有効にします。

次のコンフィギュレーション コマンドは、省略可能です。

- **iprsvpsignallinghellodscp**：Hello メッセージの IP ヘッダー内にある DiffServ コード ポイント（DSCP）値を設定します。
- **iprsvpsignallinghellorefreshmisses**：ノードが、そのネイバーとの通信が停止していると見なすまでに失うことが可能な行内の確認応答の数を指定します。
- **iprsvpsignallinghellorefreshinterval**：Hello Request 間隔を設定します。
- **iprsvpsignallinghellostatistics**：ルータ上の Hello 統計を有効にします。

設定例については、『*MPLS Traffic Engineering (TE): Link and Node Protection, with RSVP Hellos Support*, Release 12.0(24)S』の「Command Reference」にある Hello コマンドの説明を参照してください。

FRR 障害を検出するための POS シグナリングを設定するには、**pos report all** コマンドを入力するか、次のコマンドを入力して個々のレポートを要求します。

```
pos ais-shut
pos report rdool
pos report lais
pos report lrdi
pos report pais
pos report prdi
pos report sd-ber
```

# その他の参考資料

ここでは、（RSVP Hello がサポートされた）MPLS TE：リンクおよびノード保護（高速トンネル インターフェイス停止検出付き）機能の関連資料について説明します。

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| IS-IS | • 『*Cisco IOS IP Routing Protocols Command Reference*』<br>• 『Configuring a Basic IS-IS Network』 |
| MPLS トラフィック エンジニアリング コマンド | 『*Cisco IOS Multiprotocol Label Switching Command Reference*』 |

| 関連項目 | マニュアル タイトル |
|---|---|
| OSPF | • 『*Cisco IOS IP Routing Protocols Command Reference*』<br>• 『Configuring OSPF』 |
| RSVP コマンド | • 『*Cisco IOS Multiprotocol Label Switching Command Reference*』<br>• 『*Cisco IOS Quality of Service Solutions Command Reference*』 |

### 標準

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

### MIB

| MIB | MIB のリンク |
|---|---|
| この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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 XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索し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。<br>http://www.cisco.com/go/mibs |

### RFC

| RFC | Title |
|---|---|
| RFC 4090 | 『Fast Reroute Extensions to RSVP-TE for LSP Tunnels』 |

### シスコのテクニカル サポート

| 説明 | Link |
|---|---|
| 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。<br>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。<br>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/en/US/support/index.html |

# MPLS トラフィック エンジニアリング：高速リルートリンクおよびノード保護の機能情報

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 *3*：*MPLS* トラフィック エンジニアリング：高速リルートリンクおよびノード保護の機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| MPLS トラフィック エンジニアリング：Fast Reroute リンクとノード保護 | | MPLS トラフィック エンジニアリング：Fast Reroute リンクとノード保護機能は、リンク保護（ラベル スイッチド パス（LSP）の単一リンクだけをバイパスするバックアップ トンネル）、ノード保護（LSP 上のネクストホップ ノードをバイパスするバックアップ トンネル）、および FRR 機能（バックアップ トンネル サポート、バックアップ帯域幅保護、RSVP Hello）をサポートします。 |

| 機能名 | リリース | 機能情報 |
|---|---|---|
| | | 次のコマンドが導入または変更されました。<br>**clearipsvphelloinstancecounters**、<br>**clearipsvphelloinstancestatistics**、<br>**clearipsvphellostatistics**、<br>**debugipsvphello**、<br>**ipsvpsignallinghello**（設定）、<br>**ipsvpsignallinghello**（インターフェイス）、<br>**ipsvpsignallinghellodscp**、<br>**ipsvpsignallinghellorefreshinterval**、<br>**ipsvpsignallinghellorefreshmisses**、<br>**ipsvpsignallinghellostatistics**、<br>**mplstraffic-engbackup-pathtunnel**、<br>**mplstraffic-engfast-reroutebackup-protepreemption**、<br>**mplstraffic-engfast-reroutetimers**、<br>**showipsvpfastbw-protect**、<br>**showipsvpfastdetail**、<br>**showipsvphello**、<br>**showipsvphelloinstancedetail**、<br>**showipsvphelloinstancesummary**、<br>**showipsvphellostatistics**、<br>**showipsvpinterfacedetail**、<br>**showipsvprequest**、<br>**showipsvpreservation**、<br>**showipsvpsender**、<br>**showmplstraffictunnelbackup**、<br>**showmplstraffic-engfast-reroutedatabase**、<br>**showmplstraffic-engtunnels**、<br>**showmplstraffic-engtunnelssummary**、<br>**tunnelmplstraffic-engbackup-bw**、<br>**tunnelmplstraffic-engfast-reroute**。 |
| | | |

# 用語集

**バックアップ帯域幅**：NHOP および NNHOP バックアップ トンネルを使用すると、リルートされた LSP の帯域幅保護を提供できます。

**バックアップトンネル**：リンクまたはノードの障害発生時に他の（プライマリ）トンネルのトラフィックを保護するために使用される MPLS TE トンネル。

**帯域幅**：リンクの使用可能なトラフィック容量。

**シスコエクスプレスフォワーディング**：ルート参照を保存することにより、ルータ内のパケットの転送を短時間で行うための手段。

**企業ネットワーク**：会社などの組織内でほとんどの主要点を接続する大規模かつ多種多様なネットワーク。

**高速リルート**：ヘッドエンドで新しい LSP を確立しながら、障害のあるリンクまたはノード周囲の一時ルーティングをイネーブルにする手順。

**グローバルプール**：MPLS トラフィック エンジニアリングのリンクまたはノードに割り当てられた合計帯域幅。

**ヘッドエンド**：特定の LSP の起点となり、その LSP を管理するルータ。これは、LSP パス上の最初のルータです。

**ホップ**：2 つのネットワーク ノード間（たとえば、2 つのルータ間）のデータ パケットの通路。

**インスタンス**：Hello インスタンスは、特定のルータ インターフェイス アドレスおよびリモート IP アドレスに対して RSVP Hello 拡張機能を実装します。アクティブな Hello インスタンスは、定期的に Hello Request メッセージを送信し、応答として Hello ACK メッセージを予期します。予期されている ACK メッセージを受信できない場合、アクティブな Hello インスタンスは、そのネイバー（リモートの IP アドレス）が到達不能である（つまり失われている）ことを宣言します。これにより、このネイバーを通過する LSP の高速リルートが行われることがあります。

**インターフェイス**：ネットワーク接続。

**IntermediateSystem-to-IntermediateSystem**：（IS-IS）。このリンクステート階層型ルーティング プロトコルでは、Intermediate System（IS）ルータを呼び出して、単一のメトリックに基づいてルーティング情報を交換することにより、ネットワーク トポロジを決定します。

**リンク**：隣接するノード間のポイントツーポイント接続。隣接するノード間に複数のリンクが存在することがあります。リンクとは、送信者と受信者の間の回線または伝送パスおよびすべての関連装置からなるネットワーク通信チャネルのことです。回線または伝送リンクと呼ばれることもあります。

**制限付きバックアップ帯域幅**：帯域幅保護を提供するバックアップ トンネル。

**ロードバランシング**：プライマリ リンク上で特定のしきい値を超えた場合に、トラフィックを代替リンクにシフトする設定手法。イベントが発生したためにトラフィックが方向を変えた場合に、代替装置が設定されている必要があるという点で、ロード バランシングは冗長性と似ています。ロード バランシングにおいては、必ずしも代替装置が障害発生時にだけ動作する冗長装置である必要はありません。

**LSP**：ラベルスイッチド パス。MPLS がパケットを転送する 2 つのルータ間の接続。

**マージポイント**：バックアップ トンネルの終端。

**MPLS**：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ネットワーク コアにおいて使用されるパケット転送テクノロジー。これにより、スイッチング ノードにデータの転送方法を指示するためのデータ リンク層ラベルが適用されるため、ネットワーク層ルーティングで通常行われる転送よりも高速でスケーラブルな転送が行われます。

**MPLSグローバルラベル割り当て**：ルータ内のすべてのインターフェイスに対して 1 つのラベル領域があります。たとえば、あるインターフェイスに入ってきたラベル100は、別のインターフェイスに入ってきたラベル 100 と同じように処理されます。

**NHOP**：ネクスト ホップ。LSP のパス上の次のダウンストリーム ノード。

**NHOPバックアップトンネル**：ネクストホップ バックアップ トンネル。障害ポイントの先にある LSP のネクスト ホップで終端し、障害ポイントのすぐアップストリームにあるホップを起点とするバックアップ トンネル。このバックアップ トンネルは、障害の発生したリンクをバイパスし、障害発生前にこのリンクを使用していたプライマリ LSP を保護するために使用されます。

**NNHOP**：Next-Next HOP（ネクストネクスト ホップ）。LSP のパス上の次のダウンストリーム ノードの後ろのノード。

**NNHOPバックアップトンネル**：ネクストホップから 1 つめのホップのバックアップ トンネル。障害ポイントの先にある LSP のネクストネクスト ホップで終端し、障害ポイントのすぐアップストリームにあるホップを起点とするバックアップ トンネル。このバックアップ トンネルは、障害の発生したリンクまたはノードをバイパスし、障害発生前にこのリンクまたはノードを使用していたプライマリ LSP を保護するために使用されます。

**ノード**：ネットワーク接続のエンドポイント、つまりネットワーク内の複数の回線に共通する接合部。複数のノードをリンクで相互接続することができます。これらのノードは、ネットワーク内のコントロール ポイントとなります。ノードは、プロセッサ、コントローラ、またはワークステーションです。

**OSPF**：Open Shortest Path First。IS-IS プロトコルから派生した、リンクステート階層型の内部ゲートウェイ プロトコル ルーティング アルゴリズム。OSPF 機能には、最小コストによるルーティング、マルチパスのルーティング、およびロード バランシングが含まれます。

**プライマリLSP**：当初、障害発生前に保護インターフェイスを介してシグナリングされていた最後の LSP。プライマリ LSP は、障害の前の LSP です。

**プライマリトンネル**：障害が発生した場合に高速リルートされる LSP に割り当てられたトンネル。バックアップ トンネルをプライマリ トンネルにすることはできません。

**プロモーション**：新しいバックアップ トンネルが出現した場合などは、LSP に対して選択されていたバックアップ トンネルが再評価されます。この再評価は、成功すると、プロモーションと呼ばれます。

**保護インターフェイス**：1 つ以上のバックアップ トンネルが関連付けられたインターフェイス。

**冗長性**：デバイス、サービス、または接続を重複させて、障害発生時に、冗長なデバイス、サービス、または接続が、障害が発生したこれらの作業を実行できるようにすること。

**RSVP**：Resource Reservation Protocol（リソース予約プロトコル）。カスタマーがインターネットサービスのために要求をシグナリング（予約をセットアップ）する際に使用するプロトコル。これにより、カスタマーはそのネットワーク部分を経由してデータを伝送することを許可されます。

**スケーラビリティ**：ネットワークの拡大に伴って、リソース使用量の程度がどれだけ迅速に増加するかを示すインジケータ。

**SRLG**：Shared Risk Link Group（共有リスク リンク グループ）。一緒に停止する可能性の高いリンクのセット。

**ステート**：ルータが各 LSP に関して保守する必要のある情報。この情報は、トンネルをリルートする場合に使用されます。

**サブプール**：MPLS トラフィック エンジニアリングのリンクまたはノードにおける、より限定的な帯域幅。サブプールは、リンクまたはノードの全体的なグローバル プール帯域幅の一部です。

**テールエンド**：LSP が終端するルータ。これは、LSP のパス上の最後のルータです。

**トポロジ**：企業ネットワーキング構造内のネットワーク ノードおよびメディアの物理的な配置。

**トンネル**：2 つのピア間（2 台のルータ間など）のセキュアな通信パス。

**制限なしバックアップ帯域幅**：帯域幅（ベストエフォート型）保護を提供しないバックアップ トンネル（つまり、ベストエフォート型保護を提供します）。

第 3 章

# RSVP Hello サポートによる MPLS TE リンクとノード保護

（RSVP Hello がサポートされた）MPLS TE：リンクおよびノード保護（高速トンネル インターフェイス停止検出付き）機能は、次の高速再ルーティング（FRR）機能を提供します。

- ネクストネクスト ホップ ルータで終端して、リンクおよびノードの障害からダウンストリームのリンクとノードの両方を保護するバックアップ トンネル。1 つのインターフェイスを保護できるバックアップ トンネルの数に制限はありません（メモリ制限を除く）。バックアップ トンネルは、複数のラベル スイッチド パス（LSP）および複数のインターフェイスを保護できるため、スケーラブルです。
- バックアップ帯域幅保護。これにより、特定種類のデータ（音声など）を伝送する LSP 用のバックアップ トンネルにプライオリティを割り当てることができます。
- 高速トンネル インターフェイス停止検出。ヘッドエンド ルータによって LSP 上に障害の発生したリンクが検出されると、即時、強制的に「汎用的な」（高速リルート トンネルに限定されない）インターフェイス トンネルは無効になります。
- リソース予約プロトコル（RSVP）Hello。これを使用すると、ノード障害の検出を短時間で行うことができます。

• 用語集，101 ページ

# 機能情報の確認

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

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、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。

# RSVP Hello サポートによる MPLS TE リンクとノード保護の前提条件

このドキュメントが説明する機能に対応するには、ネットワークが、次の Cisco IOS XE 機能をサポートしている必要があります。

- IP シスコ エクスプレス フォワーディング
- MPLS

ネットワークが、次のプロトコルの少なくとも 1 つをサポートしている必要があります。

- Intermediate System-to-Intermediate System（IS-IS）
- Open Shortest Path First（OSPF）

# RSVP Hello サポートによる MPLS TE リンクとノード保護の制約事項

- インターフェイスが MPLS グローバル ラベル割り当てを使用する必要があります。
- このドキュメントで説明されているように、バックアップ トンネルのヘッドエンドおよびテールエンドのルータが FRR を実装している必要があります。
- バックアップ トンネルは保護されません。LSP がアクティブにバックアップ トンネルを使用している場合、バックアップ トンネルに障害が発生すると、LSP は切断されます。
- バックアップ トンネルをアクティブに使用している LSP のプロモーションは考慮されません。このため、LSP がアクティブにバックアップ トンネルを使用している場合、より適切な

バックアップ トンネルが使用可能になっても、アクティブな LSP はそのバックアップ トンネルに切り替わりません。

# RSVP Hello サポートによる MPLS TE リンクとノード保護に関する情報

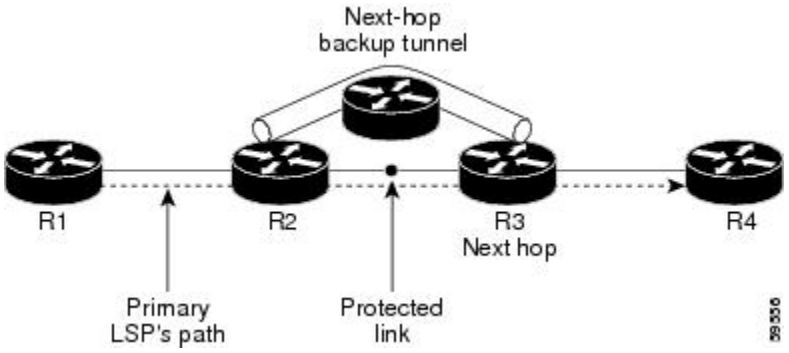
## 高速再ルーティング

高速再ルーティング（FRR）は、リンクおよびノードの障害から MPLS TE LSP を保護するためのメカニズムです。具体的には、障害ポイントの LSP をローカルに修復し、その LSP 上でのデータフローを停止することなく、LSP のヘッドエンド ルータを新しく置き換えるエンドツーエンド LSP の確立を試行します。FRR は、障害が発生したリンクまたはノードをバイパスするバックアップ トンネルを介して再ルーティングすることによって、保護されている LSP をローカルに修復します。

## リンク保護

LSP のパスの単一リンクだけをバイパスするバックアップ トンネルが、リンク保護を提供します。パス上のリンクに障害が発生した場合、バックアップ トンネルは、LSP のトラフィックをネクスト ホップにリルートする（障害の発生したリンクをバイパスする）ことによって LSP を保護します。これらは、障害ポイントの向こう側にある LSP のネクスト ホップで終端するため、ネクスト ホップ（NHOP）バックアップ トンネルと呼ばれます。次の図は、NHOP バックアップ トンネルを示しています。

**図 *8*：*NHOP* バックアップ トンネル**

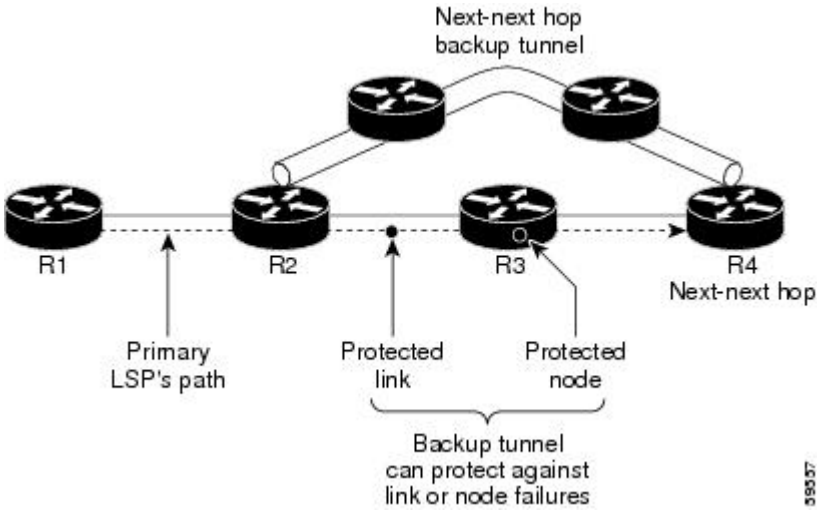


# ノード保護

FRR により、LSP に対するノード保護が提供されます。LSP パス上のネクストホップ ノードをバイパスするバックアップ トンネルは、LSP パスのネクストホップ ノードの次のノードで終端して、結果としてネクストホップ ノードをバイパスするため、ネクストネクストホップ（NNHOP）バックアップ トンネルと呼ばれます。LSP パス上のノードに障害が発生した場合は、NNHOP バックアップ トンネルが LSP を保護します。具体的には、障害のアップストリームにあるノードをイネーブルにして、障害の発生したノードの周囲の LSP とそのトラフィックをネクストネクストホップにリルートします。FRR では、ノード障害を短時間で検出できるように、RSVP Hello の使用がサポートされています。また、NNHOP バックアップ トンネルは、障害の発生したリンクおよびノードをバイパスするため、リンク障害からの保護も提供しています。

次の図は、NNHOP バックアップ トンネルを示しています。

**図 *9*：*NNHOP* バックアップ トンネル**




LSP がバックアップ トンネルを使用している場合、何らかの変更によって LSP がバックアップ トンネルとして適切でなくなると、その LSP は切断されます。ここでいう変更には次のようなものがあります。

- バックアップ トンネルのバックアップ帯域幅が縮小された。
- バックアップ トンネルのバックアップ帯域幅タイプが、プライマリ LSP と互換性のないタイプに変更された。
- プライマリ LSP が変更されたために、FRR がディセーブルになった（**nomplstraffic-engfast-reroute** コマンドが入力された。）

# 帯域幅保護

NHOP および NNHOP バックアップ トンネルを使用すると、リルートされた LSP の帯域幅保護を提供できます。これは、バックアップ帯域幅と呼ばれます。バックアップ帯域幅は、NHOP または NNHOP バックアップ トンネルと関連付けることができます。これにより、特定のバックアップ トンネルで保護できるバックアップ帯域幅の大きさがルータに通知されます。ルータが LSP をバックアップ トンネルにマップするとき、帯域幅保護によって、十分なバックアップ帯域幅がある場合にだけ、指定されたバックアップ トンネルが使用されます。ルータは、最大限の帯域幅保護を提供するために、どの LSP がどのバックアップ トンネルを使用するかを選択します。つまり、ルータは、保護できる LSP の数が最大限になるような方法を、LSP をバックアップ トンネルにマップする最良の方法として決定します。トンネルのマッピングおよびバックアップ帯域幅の割り当てについては、バックアップ トンネルの選択手順, （13 ページ）を参照してください。

bandwidth protection desired ビットが設定された LSP では、帯域幅保護を提供するバックアップ トンネルの選択権限が大きくなります。つまり、これらの LSP は、そのビットが設定されていない他の LSP をプリエンプション処理できます。詳細は、「帯域幅保護されたバックアップ トンネルを取得する LSP のプライオリティ設定」セクションを参照してください。

# 高速トンネル インターフェイス停止検出

高速トンネル インターフェイス停止検出は、ヘッドエンド ルータによって LSP 上に障害の発生したリンクが検出されると、即時、強制的に「汎用」（高速リルート トンネルに限定されない）インターフェイス トンネルを無効にします。

この機能は **tunnel mpls traffic-eng interface down delay** を使用して設定します。この機能が設定されていない場合、トンネルが機能停止し、トラフィックの転送にヘッドエンド/中継ポイント ルータによって選択される代替パスを使用するようになるまでに遅延が生じます。これはデータ トラフィックの場合には許容できますが、音声トラフィックの場合は許容できません。音声トラフィックは TE トンネルに依存して、LSP が停止するとすぐに停止するためです。

# RSVP Hello

RSVP Hello については、次の各項で説明します。

## RSVP Hello の動作

RSVP Hello を使用すると、RSVP ノードは、ネイバー ノードが到達不能になった場合にそれを検出できます。これにより、ノードツーノードの障害検出が可能になります。このような障害が検出された場合、リンク層の通信障害のときと同様の方法で処理されます。

リンク層障害の通知が使用可能でない場合（たとえば、ファスト イーサネットなど）、またはリンク層により提供される障害検出メカニズムが十分でないためにノード障害をタイムリーに検出できない場合、FRR では RSVP Hello を使用できます。

Hello を実行しているノードは、各間隔で Hello Request をネイバー ノードに送信します。受信側ノードが Hello を実行している場合、このノードは Hello Ack を使用して応答します。4 間隔が経過しても送信側ノードが Ack を受信できない場合、または不正なメッセージが受信された場合、送信側ノードはネイバーが停止していることを宣言し、FRR に通知します。

設定可能なパラメータは 2 つあります。

- Hello 間隔：**ip rsvp signalling hello refresh interval** コマンドを使用します。
- 送信側ノードでネイバーが停止していると宣言されるまでにミスされる確認応答メッセージの数：**ip rsvp signalling hello refresh misses** コマンドを使用します。

（注） RSVP Hello 処理が頻繁に行われるためにルータの CPU 使用率が高くなっている場合、送信されていない Hello メッセージが原因でエラーが発生している可能性があります。

## Hello インスタンス

Hello インスタンスは、特定のルータ インターフェイス アドレスおよびリモート IP アドレスに対して RSVP Hello を実装します。Hello インスタンスは、送信される Hello Request の数が多く、ルータ リソースに負荷がかかるため、非常にコストがかかります。このため、Hello インスタンスを作成するのは必要な場合だけにし、不要になったインスタンスは削除してください。

次の 2 種類の Hello インスタンスがあります。

- Hello インスタンス, （56 ページ）
- Hello インスタンス, （56 ページ）

### アクティブな Hello インスタンス

LSP の高速リルートの準備ができているが、ネイバーが到達不能な場合、アクティブな Hello インスタンスが必要となります。この状態の LSP を少なくとも 1 つ持つネイバーに対して、アクティブな Hello インスタンスを 1 つずつ作成します。

アクティブな Hello インスタンスは、定期的に Hello Request メッセージを送信し、応答として Hello Ack メッセージを予期します。予期されている Ack メッセージを受信できない場合、アクティブな Hello インスタンスは、そのネイバー（リモートの IP アドレス）が到達不能である（失われている）ことを宣言します。そのネイバーを通過する LSP の高速リルートを行うことができます。

到達不能なネイバーに対する LSP を持たない Hello インスタンスがある場合、その Hello インスタンスを削除しないでください。アクティブな Hello インスタンスをパッシブな Hello インスタンスに変更します。これは、Hello Request をこのインスタンスに送信しているアクティブなインスタンスがネイバー ルータ上に存在する可能性があるためです。

#### パッシブな Hello インスタンス

パッシブな Hello インスタンスは（Ack メッセージを送信して）Hello Request メッセージに応答しますが、Hello Request メッセージを開始しないため、LSP の高速リルートは行われません。複数のインターフェイスを持つネイバーは、異なるネイバーに対して、または同じネイバーに対して、複数の Hello インスタンスを実行できます。

Hello インスタンスが存在しないネイバーから、IP ヘッダー内に送信元 IP アドレスと宛先 IP アドレスのペアが含まれる Hello Request が受信されると、パッシブな Hello インスタンスが作成されます。

このインスタンスに対して 10 分以内に Hello メッセージが受信されない場合は、パッシブ インスタンスを削除してください。

### Hello コマンド

RSVP Hello は次のコマンドで構成されています。コマンドの詳細については、『Cisco IOS Multiprotocol Label Switching Command Reference』を参照してください。

- RSVP Hello 設定コマンド
- RSVP Hello 統計コマンド
- RSVP Hello 表示コマンド
- RSVP Hello デバッグコマンド

## RSVP Hello サポートによる MPLS TE リンクとノード保護の機能

（RSVP Hello がサポートされた）MPLS TE：リンクおよびノード保護（高速トンネル インターフェイス停止検出付き）には、次の機能が含まれます。

### バックアップ トンネル サポート

バックアップ トンネル サポートには、次の機能があります。

#### バックアップ トンネルは FRR をサポートするためにネクストネクスト ホップで終端できる

ネクストネクストホップルータで終端して、リンクおよびノードの障害からダウンストリームのリンクとノードの両方を保護するバックアップ トンネル。詳細については、ノード保護, （54 ページ）を参照してください。

#### 複数のバックアップ トンネルが同じインターフェイスを保護できる

1 つのインターフェイスを保護できるバックアップ トンネルの数に制限はありません（メモリ制限を除く）。多くのトポロジでは、ノード保護をサポートするために、保護インターフェイスごとに複数のバックアップ トンネルをサポートする必要があります。これらのバックアップ トンネルは同じ宛先で終端することも、異なる宛先で終端することもできます。つまり、1 つの保護イ

ンターフェイスに対して、複数の NHOP または NNHOP バックアップ トンネルを設定できます。これにより、冗長性とロード バランシングを実現できます。

この機能は、ノード保護のために必要となるだけでなく、次のような利点もあります。

- 冗長性：一方のバックアップ トンネルが停止すると、他方のバックアップ トンネルが LSP を保護します。
- バックアップ容量の増加：保護インターフェイスが大容量リンクであり、同じ容量を持つバックアップ パスが 1 つも存在しない場合、その 1 つの大容量リンクを複数のバックアップ トンネルによって保護できます。このリンクを使用している LSP は異なるバックアップ トンネルにフェールオーバーするため、障害発生時にはすべての LSP が適切な帯域幅保護（リルート）を受けることができます。帯域幅保護が必要でない場合、ルータは使用可能なすべてのバックアップ トンネルに LSP を分散させます（つまり、複数のバックアップ トンネルの間でロード バランシングを行います）。詳細については、バックアップ トンネルの選択手順，（13 ページ）を参照してください。

異なる宛先で終端するバックアップ トンネル，（61 ページ）と同じ宛先で終端するバックアップ トンネル，（12 ページ）で例を示しています。

### 拡張性

バックアップ トンネルは、複数の LSP および複数のインターフェイスを保護できるため、スケーラブルです。これは、多対 1（N:1）の保護を提供します。N:1 の保護は、保護の必要な LSP ごとに個別のバックアップ トンネルを使用する必要のある 1 対 1（1:1）の保護に比べて、スケーラビリティ上のメリットが大きくなります。

1:1 保護の例：たとえば 5,000 のバックアップ トンネルが 5,000 の LSP を保護する場合、バックアップ パスに沿った各ルータは 5,000 の追加トンネルの状態を維持する必要があります。

N:1 の保護の例：1 つのバックアップ トンネルで 5,000 個の LSP を保護し、バックアップ パス上の各ルータが追加のトンネルを 1 つずつ管理する場合。

## バックアップ帯域幅保護

バックアップ帯域幅保護には、次の機能があります。

### バックアップ トンネルの帯域幅保護

障害発生時に、リルートされた LSP によりパケットが伝送されるだけでなく、Quality of Service（QoS）も維持できます。

### バックアップ トンネルの帯域幅プール指定

特定のバックアップ トンネルを使用できる LSP のタイプを制限できます。サブプール帯域幅を使用する LSP だけが使用できるように、またはグローバル プール帯域幅が使用できるように、バックアップ トンネルを制限できます。このため、音声とデータに対して別々のバックアップ トンネルを使用できます。たとえば、音声に使用するバックアップ トンネルでは帯域幅保護を提供し、

データに使用するバックアップ トンネルでは（場合により）帯域幅保護を提供しないように設定できます。

### 半ダイナミックなバックアップ トンネル パス

バックアップ トンネルのパスは、ダイナミックに決定されるように設定できます。このためには、リリース 12.0(14)ST で追加された IP 明示アドレス除外機能を使用します。この機能を使用すると、半ダイナミックな NHOP バックアップ トンネル パスは、保護対象のリンクを除外するだけで指定できます。半ダイナミックな NNHOP バックアップ トンネル パスは、保護対象のノードを除外するだけで設定できます。

### 帯域幅保護されたバックアップ トンネルを取得する LSP のプライオリティ設定

NHOP または NNHOP バックアップ トンネルが十分にない場合、またはすべての LSP を保護するための十分なバックアップ帯域幅がない場合は、帯域幅保護されたバックアップ トンネルを取得するためのプライオリティを LSP に付与できます。これは特に、データを伝送する LSP よりも音声を伝送する LSP に高いプライオリティを付与する場合に有用です。

この機能をアクティブにするには、**tunnelmplstraffic-engfast-reroutebw-protect** コマンドを入力して、「bandwidth protection desired」ビットを設定します。『LSP 上での高速リルートの有効化』の設定タスクを参照してください。必ずしもこのような LSP が帯域幅保護を受けるとはかぎりません。必要な場合に、このような LSP の方が帯域幅保護を受ける可能性が高くなります。

帯域幅保護ビットが設定されていない LSP は、デモートできます。デモーションとは、帯域幅保護ビット セットのある LSP にバックアップを提供するために、1 つ以上の LSP が、割り当てられたバックアップ トンネルから削除されることです。デモーションは、バックアップ帯域幅が不足している場合にだけ行われます。

デモートされた LSP は、保護されていない状態になります（つまり、バックアップ トンネルを持たなくなります）。次の定期的なプロモーション サイクルの間に、現在保護されていないすべての LSP（デモートされた LSP を含む）に対して可能なかぎり最良のバックアップ トンネルを見つけるように試行されます。LSP は同レベルまたは低いレベルの保護を受けることもあれば、保護を受けないこともあります。

ルータがデモート対象の LSP を決定する方法については、『バックアップ保護プリエンプション アルゴリズム』セクションを参照してください。

## RSVP Hello

RSVP Hello を使用すると、ルータは、ネイバー ノードが停止したが、そのネイバーへのインターフェイスがまだ動作中である場合、それを検出できます。この機能は、リンク層メカニズムによってネクストホップ ノードの障害が検出できない場合や、リンク層障害の通知が使用可能でない場合に特に有用です。これにより、ルータは LSP をそのバックアップ トンネルに切り替え、パケット損失を回避できます。

RSVP Hello の詳細については、RSVP Hello, （55 ページ）を参照してください。

# 高速リルート操作

ここでは、次の内容について説明します。

## 高速リルート アクティベーション

次の 3 つのメカニズムによって、LSP がそれぞれのバックアップ トンネルに切り替わります。

- インターフェイス停止通知
- 信号消失
- RSVP Hello ネイバー停止通知

ルータのリンクまたはネイバー ノードに障害が発生すると、インターフェイス停止通知によってルータはこの障害を検出します。Packet over SONET（POS）インターフェイスでは、この通知が非常に高速に行われます。インターフェイスが停止したことをルータが認識すると、ルータはそのインターフェイスを出る LPS を、それぞれのバックアップ トンネルに切り替えます（バックアップ トンネルがある場合）。

POS インターフェイスとは異なり、ギガビット イーサネットではリンク障害を検出する警告はありません。ケーブル切断やリモート エンドのレーザー停止によりリンクが断続すると、ギガビット イーサネット カードの光モジュール（GBIC または SFP）は信号消失（LOS）を検出します。LOS は障害を検出し、スイッチオーバーを開始するために使用されます。

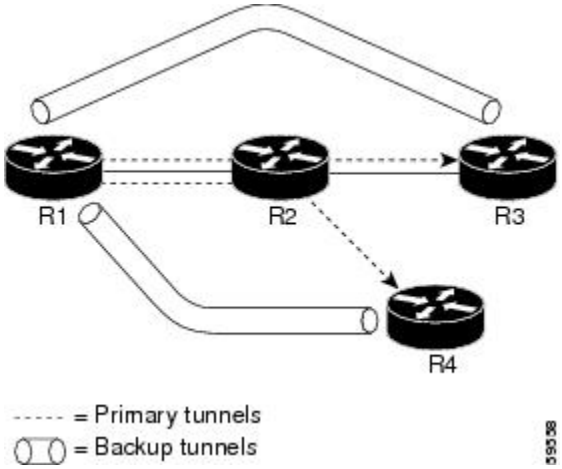
RSVP Hello は、FRR をトリガーするためにも使用できます。インターフェイス上に RSVP Hello が設定されている場合、メッセージが定期的にネイバー ルータに送信されます。応答を受信できない場合、Hello はネイバーが停止していることを宣言します。これにより、そのインターフェイスを出る LSP はすべて、それぞれのバックアップ トンネルに切り替わります。

Fast Reroute は ATM インターフェイス上でも作動します。インターフェイスは、障害検出に RSVP Hello を使用する必要があります。

## 異なる宛先で終端するバックアップ トンネル

次の図に、異なる宛先で終端する複数のバックアップ トンネルを持つインターフェイスを示します。また、多くのトポロジにおいて、ノード保護をサポートするために保護インターフェイスごとに複数のバックアップ トンネルをサポートする必要がある理由を示しています。

**図 *10*：異なる宛先で終端するバックアップ トンネル**



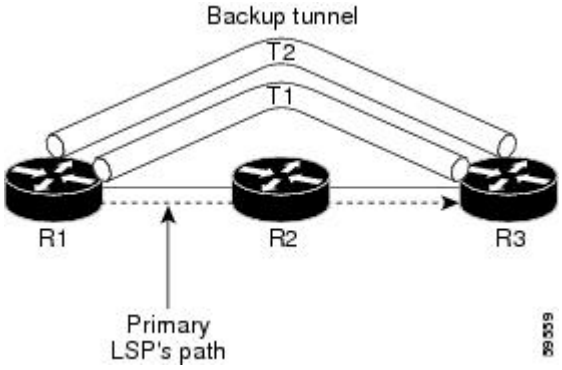

この図では、R1 上の単一のインターフェイスが複数のバックアップ トンネルを必要としています。LSP は、次のルートを通過します。

- R1、R2、R3
- R1、R2、R4

ノード R2 の障害発生時に備えた保護を提供するには、2 つの NNHOP バックアップ トンネル（R3 で終端するバックアップ トンネルと、R4 で終端するバックアップ トンネル）が必要です。

## 同じ宛先で終端するバックアップ トンネル

次の図に、冗長性およびロード バランシングのために同じロケーションで終端するバックアップ トンネルを使用する方法を示します。冗長性およびロード バランシングは、NHOP バックアップ トンネルと NNHOP バックアップ トンネルの両方に対して使用できます。




この図では、3 つのルータ（R1、R2、および R3）があります。R1 では、R2 を通過せずに R1 から R3 に移動する 2 つの NNHOP バックアップ トンネル（T1 および T2）があります。

冗長性があれば、R2 に障害が発生した場合や、R1 から R2 へのリンクに障害が発生した場合、どちらのバックアップ トンネルも使用できます。一方のバックアップ トンネルが停止した場合は、もう一方のバックアップ トンネルを使用できます。LSP は、最初に確立されるときに、バックアップ トンネルに割り当てられます。これは、障害発生前に完了しています。

ロード バランシングにより、どちらのバックアップ トンネルにもすべての LSP をバックアップするための十分な帯域幅がない場合、両方のトンネルを使用できます。一部の LSP は一方のバックアップ トンネルを使用し、その他の LSP はもう一方のバックアップ トンネルを使用します。ルータによって、LSP をバックアップ トンネルに割り当てる最良の方法が決定されます。

## バックアップ トンネルの選択手順

次のいずれかのイベントが発生した場合、LSP がシグナリングされると、その LSP に FRR 保護を提供する LSP パス上の各ノードが、LSP のバックアップ トンネルを選択します。

- ネクスト ホップへのリンクに障害が発生した。
- ネクスト ホップに障害が発生した。

障害発生前にノードが LSP のバックアップ トンネルを選択することにより、障害発生時に LSP をバックアップ トンネルにすばやくリルートできます。

LSP をバックアップ トンネルにマップするには、次のすべての条件が満たされている必要があります。

- LSP が FRR で保護されている。つまり、LSP が **tunnel mpls traffic-eng fast-reroute** コマンドを使用して設定されている。
- バックアップ トンネルが動作している。
- バックアップ トンネルが IP アドレス（通常はループバック アドレス）を持つように設定されている。
- バックアップ トンネルが、この LSP の発信インターフェイスを保護するように設定されている（インターフェイスが **mpls traffic-eng backup-path** コマンドを使用して設定されている）。

- バックアップ トンネルが LSP の保護インターフェイスを通過しない。
- バックアップ トンネルが LSP の NHOP または NNHOP で終端している。NNHOP トンネルであるバックアップ トンネルは、LSP の NHOP を追加しません。
- LSP およびバックアップ トンネルの帯域幅保護の要件と制約（ある場合）が満たされている。帯域幅保護の考慮事項については、帯域幅保護, （14 ページ）を参照してください。

## 帯域幅保護

バックアップ トンネルは、次の 2 種類のバックアップ帯域幅を保護するように設定できます。

- 制限付きバックアップ帯域幅：バックアップ トンネルが帯域幅保護を提供します。このバックアップ トンネルを使用するすべての LSP の帯域幅の合計が、バックアップ トンネルのバックアップ帯域幅を超えることはできません。LSP をこのタイプのバックアップ トンネルに割り当てる場合、十分なバックアップ帯域幅が存在している必要があります。
- 制限なしバックアップ帯域幅：バックアップ トンネルは帯域幅保護を提供しません（つまり、ベストエフォート型の保護が存在します）。このバックアップ トンネルにマップされた LSP で使用される帯域幅の大きさに制限はありません。ゼロ帯域幅が割り当てられた LSP は、制限なしバックアップ帯域幅のバックアップ トンネルしか使用できません。

## 制限付き帯域幅バックアップ トンネルのロード バランシング

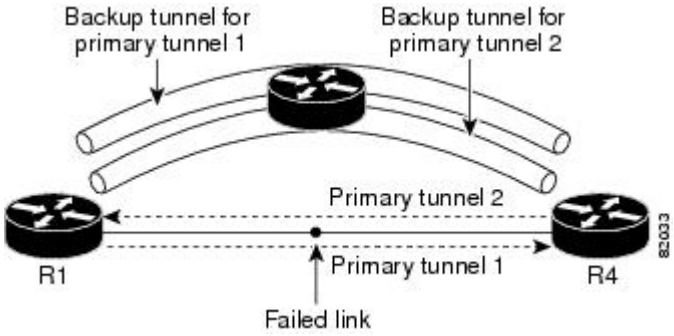
特定の LSP を保護するための十分なバックアップ帯域幅を持つバックアップ トンネルが、複数存在することがあります。この場合、ルータが、使用可能な最小バックアップ帯域幅のバックアップ トンネルを選択します。このアルゴリズムによって、フラグメンテーションが制限されるため、使用可能な最大バックアップ帯域幅が維持されます。

制限付きバックアップ帯域幅を指定した場合、リンクまたはノードの障害発生時の帯域幅保護は「保証」されません。たとえば、インターフェイスの障害発生時にトリガーされる NHOP バックアップ トンネルと NNHOP バックアップ トンネルのセットがすべて、ネットワーク トポロジ上のリンクを共有することがありますが、このバックアップ トンネル セットを使用してすべての LSP をサポートするだけの十分な帯域幅がこのリンクにない場合があります。

次の図では、両方のバックアップ トンネルが同じリンクおよびホップを通過しています。ルータ R1 と R4 の間のリンクに障害が発生すると、プライマリ トンネル 1 のバックアップ トンネルとプ

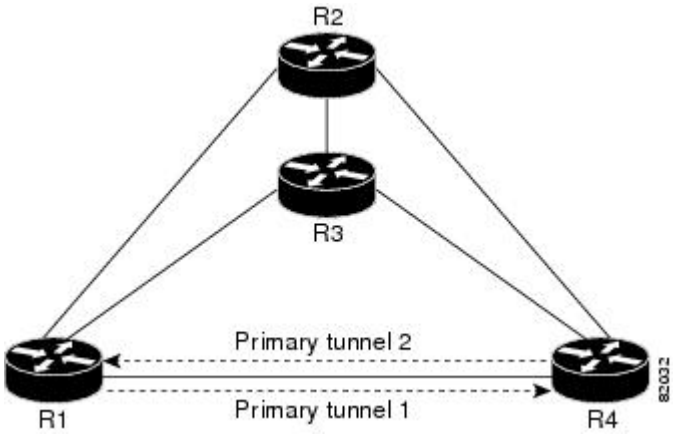
ライマリ トンネル 2 のバックアップ トンネルが同時にトリガーされます。この 2 つのバックアップ トンネルが、ネットワーク内の 1 つのリンクを共有できます。

**図 *11* : *1* つのリンクを共有する複数のバックアップ トンネル**




次の図では、プライマリ トンネル 1 のバックアップ トンネルはルータ R1-R2-R3-R4 を通過でき、プライマリ トンネル 2 のバックアップ トンネルはルータ R4-R2-R3-R1 を通過できます。この場合、R1-R4 に障害が発生すると、リンク R2-R3 が過負荷になることがあります。

**図 *12* : 過負荷になったリンク**




## 制限なし帯域幅バックアップ トンネルのロード バランシング

制限なしバックアップ帯域幅を持つ複数のバックアップ トンネルが、1 つのインターフェイスを保護できます。この場合、ある LSP に対するバックアップ トンネルの選択時に、ルータは、最小バックアップ帯域幅を持つバックアップ トンネルを選択します。このアルゴリズムにより、LSP の帯域幅に基づいて、バックアップ トンネル間で均等に LSP が分散されます。LSP がゼロ帯域幅を要求している場合、ルータは、現在保護している LSP の数が最も少ないバックアップ トンネルを選択します。

## プール タイプおよびバックアップ トンネル

デフォルトでは、バックアップ トンネルは、任意のプール（グローバルプールまたはサブプール）から割り当てるLSPに対して保護を提供します。ただし、グローバル プール帯域幅を使用するLSPだけ、またはサブプール帯域幅を使用するLSPだけを保護するようにバックアップ トンネルを設定することもできます。

## トンネル選択のプライオリティ

ここでは、次の内容について説明します。

### NHOP バックアップ トンネルと NNHOP バックアップ トンネル

1 つの LSP を、複数のバックアップ トンネル（LSP の NNHOP で終端するバックアップ トンネルと、LSP の NHOP で終端するバックアップ トンネル）により保護できます。この場合、ルータは、NNHOP で終端するバックアップ トンネルを選択します（つまり、FRR は NHOP バックアップ トンネルよりも NNHOP バックアップ トンネルを優先します）。

次の表に、トンネル選択のプライオリティを示します。最初に選択されるのは、サブプールまたはグローバル プールから帯域幅を獲得する、制限付き帯域幅を持つ NNHOP バックアップ トンネルです。このようなバックアップ トンネルがない場合、次（2）に選択されるのは、任意のプールから制限付き帯域幅を獲得するネクストネクスト ホップ バックアップ トンネルです。優先順位が 1（最良）から 8（最悪）の順にバックアップ トンネルが選択されます。選択肢 3 は、大きさの制限がないサブプールまたはグローバル プール帯域幅を持つ NNHOP バックアップ トンネルです。

表 *4*：トンネル選択のプライオリティ

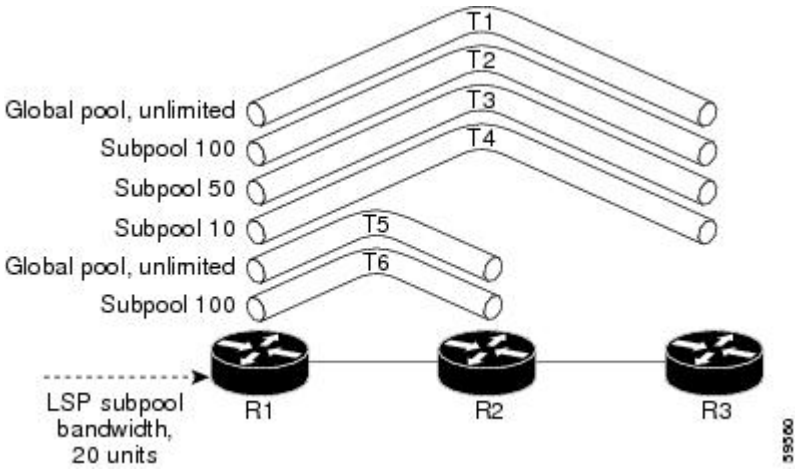
| 優先順位 | バックアップ トンネルの宛先 | 帯域幅プール | 帯域幅の大きさ |
|---|---|---|---|
| 1（最良） | NNHOP | サブプールまたはグローバル プール | Limited |
| 2 | NNHOP | いずれか（Any） | Limited |
| 3 | NNHOP | サブプールまたはグローバル プール | Unlimited |
| 4 | NNHOP | いずれか（Any） | Unlimited |
| 5 | NHOP | サブプールまたはグローバル プール | Limited |
| 6 | NHOP | いずれか（Any） | Limited |

| 優先順位 | バックアップ トンネルの宛先 | 帯域幅プール | 帯域幅の大きさ |
|---|---|---|---|
| 7 | NHOP | サブプールまたはグローバル プール | Unlimited |
| 8（最悪） | NHOP | いずれか（Any） | Unlimited |

次の図に、現在使用可能なグローバル プールおよびサブプール帯域幅の指定された大きさに基づいて、バックアップ トンネルが選択される手順の例を示します。

（注） NHOP バックアップ トンネルと NNHOP バックアップ トンネルに十分なバックアップ帯域幅がない場合、LSP が伝送するデータのタイプは考慮されません。たとえば、データ LSP よりも前にシグナリングされない音声 LSP は、保護されないことがあります。バックアップ トンネルの使用に優先順位を付けるためには、「バックアップ保護優先アルゴリズム」セクションを参照してください。

**図 *13*：複数のバックアップ トンネルからの選択**




この例では、LSP には、20 ユニット（kbps）のサブプール バックアップ帯域幅が必要です。最良バックアップ トンネルは、次のようにして選択されます。

1. バックアップ トンネル T1 から T4 までは、NNHOP で終端するため、最初に考慮されます。
2. トンネル T4 は、サブプール バックアップ帯域幅を 10 ユニットしか持たないため、除外されます。
3. トンネル T1 は、グローバルプール帯域幅を使用して LSP を保護するだけなので、除外されます。

4 トンネル T3 は T2 よりも優先的に選択されます。両方とも十分なバックアップ帯域幅がありますが、T3 の方が使用可能なバックアップ帯域幅が少ないためです（多い方のバックアップ帯域幅は T2 上に維持されます）。

5 トンネル T5 と T6 は、NHOP で終端するため、考慮する必要はありません。このため、NNHOP で終端する T3 の方が、これらよりも優先されます。

### Promotion

LSP のバックアップ トンネルが選択されたあとで、状況が変わったために、この選択を再評価する必要が生じることがあります。この再評価は、成功した場合、プロモーションと呼ばれます。次のような状況がこれに該当します。

1 新しいバックアップ トンネルが出現した。

2 この LSP に対して現在選択されているバックアップ トンネルが停止した。

3 バックアップ トンネルの使用可能なバックアップ帯域幅が増加した。たとえば、トンネルで保護されている LSP が、ヘッドエンドにより、別のパスを使用するように再最適化された場合などです。

4 バックアップ トンネルの使用可能なバックアップ帯域幅が減少した。

ケース 1 とケース 2 では、LSP のバックアップ トンネルがすぐに評価されます。ケース 3 とケース 4 に対処するには、LSP からバックアップ トンネルへのマッピングを定期的に再評価します。デフォルトでは、バックグラウンドの再評価は 5 分ごとに実行されます。この間隔は、**mplstraffic-engfast-reroutetimers** コマンドを使用して設定できます。

ケース 4 の応答は次のとおりです。

バックアップ トンネルの帯域幅が減少すると、残りの帯域幅がこのトンネルがバックアップであるすべてのプライマリ パスの帯域幅の合計よりも大きい間はプロモーションは実行されません。このポリシーは、プライマリ パス保護の不要な中断を防ぎます。

バックアップ トンネルの帯域幅が、割り当てられているすべてのプライマリ パスを代用するのに必要となるすべての帯域幅を下回ると、プロモーションが実行されます。

### バックアップ保護プリエンプション アルゴリズム

LSP に「bandwidth protection desired」ビットを設定すると、その LSP は、帯域幅保護を提供するバックアップ トンネルの選択権限が大きくなり、そのビット セットを持たない他の LSP をプリエンプション処理できます。

NNHOP バックアップ トンネル上に十分なバックアップ帯域幅がないが、NHOP バックアップ トンネルにはある場合、帯域幅保護されている LSP は、NNHOP LSP をプリエンプション処理せず、NHOP 保護を使用します。

1 つのバックアップ トンネルを使用する LSP が複数存在し、帯域幅を提供するために 1 つ以上の LSP をデモートする必要がある場合、デモート対象の LSP を決定する際に使用できるユーザ設定可能な方法（アルゴリズム）が 2 つあります。

- 無駄な帯域幅の大きさを最小限にする。

- デモートされる LSP の数を最小限にする。

たとえば、バックアップ トンネル上に 10 ユニットのバックアップ帯域幅が必要な場合は、次のいずれかをデモートできます。

- 100 ユニットの帯域幅を使用する単一の LSP：必要な帯域幅より多くの帯域幅が使用可能になりますが、無駄も多くなります。
- 1 ユニットずつ帯域幅を使用する 10 個の LSP：無駄な帯域幅はなくなりますが、影響を受ける LSP が多くなります。

デフォルトのアルゴリズムは、デモートされる LSP の数を最小にします。無駄な帯域幅の大きさを最小限にするためのアルゴリズムに変更するには、**mplstraffic-engfast-reroutebackup-prot-preemptionoptimize-bw** コマンドを入力します。

## 帯域幅保護に関する考慮事項

帯域幅保護を確実に行うには、数多くの方法があります。次の表で、3 つの方式のメリットとデメリットについて説明します。

**表 *5*：帯域幅保護の方式**

| 方式 | 利点 | 欠点 |
|---|---|---|
| バックアップ トンネルに対して帯域幅を明示的に予約 | この方式は簡単です。 | 個別的な障害からの保護を行う複数のバックアップ トンネルが帯域幅を共有できるようにすることが課題です。 |
| ゼロ帯域幅でシグナリングされたバックアップ トンネルを使用 | 個別的な障害からの保護に使用される帯域幅を共有する方法が提供され、帯域幅をより経済的に使用できます。 | ゼロ帯域幅トンネルの適切な配置の決定が複雑になる場合があります。 |
| バックアップ帯域幅保護 | 音声トラフィックの帯域幅保護が確実に行われます。 | 十分なバックアップ帯域幅がない場合、バックアップ帯域幅保護が設定された LSP に帯域幅が必要になると、バックアップ帯域幅保護が設定されていない LSP をいつでもデモートできます。 |

シスコ実装の FRR では、特定のアプローチが強制されることはなく、上記のいずれのアプローチも使用できます。ただし、幅広い設定選択肢がある場合は、それらの選択肢が特定の帯域幅保護方針と一致していることを確認してください。

次の各項では、適切な設定を選択する際の重要事項について説明します。

### 明示的にシグナリングされた帯域幅を持つバックアップ トンネル

バックアップ トンネルには設定を要する帯域幅パラメータが 2 つあります。

- シグナリングされた実際の帯域幅
- バックアップ帯域幅

バックアップ トンネルの帯域幅要件をシグナリングするには、**tunnel mpls traffic-eng bandwidth** コマンドを使用して、バックアップ トンネルの帯域幅を設定します。

バックアップ トンネルのバックアップ帯域幅を設定するには、**tunnel mpls traffic-eng backup-bw** コマンドを使用します。

シグナリングされた帯域幅は、バックアップ トンネルのパス上の LSR が、アドミッション コントロールを実行し、適切な帯域幅計算を行うために使用します。

バックアップ帯域幅は、PLR（ローカル修復ポイント：バックアップ トンネルのヘッドエンド）が、障害発生時にこのバックアップ トンネルにリルートできるプライマリ トラフィックの量を決定するために使用します。

適切な動作が確実に行われるように、両方のパラメータを設定する必要があります。シグナリングされた帯域幅とバックアップ帯域幅の数値は、同じである必要があります。

#### 保護対象の帯域幅プールと、バックアップ トンネルにより帯域幅が予約される帯域幅プール

**tunnel mpls traffic-eng bandwidth** コマンドを使用すると、次の値を設定できます。

- バックアップ トンネルにより予約される帯域幅の大きさ
- 帯域幅を予約する必要のある DS-TE 帯域幅プール

（注） 選択できるプールは 1 つだけです（つまり、バックアップ トンネルは、グローバル プールかサブプールのいずれか一方だけから帯域幅を明示的に予約できます）。

**tunnel mpls traffic-eng backup-bw** コマンドを使用すると、このバックアップ トンネルを使用するためにトラフィックに割り当てる必要のある帯域幅プールを指定できます。複数のプールを指定できます。

保護対象の帯域幅プールと、バックアップ トンネルによりその帯域幅が取り込まれる帯域幅プールとの間に、直接の対応関係はありません。

例：この例では、次の設定が前提になっています。

- 帯域幅保護は、サブプール トラフィックにだけ必要であり、グローバル プールを使用するベストエフォート型のトラフィックには必要でない。
- サブプール トラフィックがプライオリティ キューを使用し、グローバル プール トラフィックのプライオリティがそれより低くなるように、スケジューリングが設定されている。

特定のリンク上で 10 Kbps のサブプール トラフィックに対する帯域幅保護を実現するには、次のコマンドを任意に組み合わせます。

- **tunnelmplstraffic-engbandwidthsub-pool10**

**tunnelmplstraffic-engbackup-bwsub-pool10**

- **tunnelmplstraffic-engbandwidthglobal-pool10**

**tunnelmplstraffic-engbackup-bwsub-pool10global-poolunlimited**

- **tunnelmplstraffic-engbandwidthglobal-pool40**

**tunnelmplstraffic-engbackup-bwsub-pool10global-pool30**

## ゼロ帯域幅でシグナリングされたバックアップ トンネル

帯域幅保護が必要な場合でも、ゼロ帯域幅でシグナリングされたバックアップ トンネルを使用すると有効なことが多くあります。帯域幅が明示的に予約されていないと、帯域幅が保証されないように思われがちです。しかし、必ずしもそうではありません。

次のような状況について検討します。

- リンク保護だけが必要な場合
- サブプール トラフィックにだけ帯域幅保護が必要な場合

最大予約可能サブプールの値が S の保護対象リンク AB ごとに、ノード A からノード B へのパスが存在し、最大予約可能グローバル プールと最大予約可能サブプールの差が少なくとも S になっていることがあります。ネットワーク内の各リンクにこのようなパスが見つかる可能性がある場合、このようなパス上に、すべてのバックアップ トンネルを帯域幅の予約なしで確立できます。単一のリンク障害が発生した場合、1 つだけのバックアップ トンネルがそのパス上のいずれかのリンクを使用します。そのパスでは（グローバル プール内で）少なくとも S の帯域幅が使用可能であるため、サブプール トラフィックをプライオリティ キューに分類するためのマーキングとスケジューリングが設定されていれば、サブプール帯域幅が保証されます。

上記のアプローチにより、個別的なリンク障害を保護する複数のバックアップ トンネル間でグローバルプール帯域幅を共有することが可能になります。バックアップ トンネルは、障害発生後短時間の間だけ（影響を受ける LSP が、使用可能なサブプール帯域幅でそれらの LSP を他のパスにリルートするまで）使用されることが予期されます。相互に関連しない複数のリンクに障害が発生することは、ほとんどありません（ノードまたは SRLG に障害がない場合にかぎります。これらに障害があると、複数のリンク障害が発生します）。したがって、実際にはリンク障害は個別的である可能性が高いと仮定できます。このような「個別的な障害の前提」を、明示的に帯域幅を予約することなくシグナリングされたバックアップ トンネルと組み合わせることにより、効率的な帯域幅共有が可能になり、大幅な帯域幅節約につながります。

サブプール トラフィックを保護するバックアップ トンネルは、いずれのプールからも帯域幅を取り込みません。グローバル プールを使用するプライマリ トラフィックは、グローバル プール全体を使用できます。また、サブプールを使用するプライマリ トラフィックは、サブプール全体を使用できます。ただし、単一のリンク障害が発生した場合、サブプール トラフィックに対する完全な帯域幅保証が行われます。

ノード保護と SRLG 保護に対しても、同様のアプローチを使用できます。ただし、ノード障害と SRLG 障害ではいずれも複数のリンクに同時に障害が発生するため、バックアップ トンネルの配置場所の決定がさらに複雑になります。したがって、影響を受けるすべてのリンクを通過するトラフィックを保護するバックアップ トンネルを、互いに独立して計算することはできません。別々の障害に対応するリンクのグループを保護するバックアップ トンネルは、互いに独立して計算できるため、同様の帯域幅節約を実現できます。

### シグナリングされた帯域幅とバックアップ帯域幅

（バックアップ トンネルのヘッドエンドであるルータが）バックアップ帯域幅をローカルに使用して、特定のバックアップ トンネル上にリルートできるプライマリ LSP とその数を決定します。ルータは、これらの LSP の帯域幅要件の組み合わせがバックアップ帯域幅を超えないようにします。

このため、バックアップ トンネルがゼロ帯域幅でシグナリングされていても、このバックアップ トンネルにより保護されるトラフィックの実際の帯域幅要件に対応する値を使用して、バックアップ帯域幅を設定する必要があります。バックアップ トンネルの帯域幅要件が明示的にシグナリングされている場合とは異なり、シグナリングされた帯域幅の値（ゼロ）は、バックアップ帯域幅の値とは異なります。

# RSVP Hello サポートによる MPLS TE リンクとノード保護の機能の設定方法

ここでは、MPLS TE LSP が設定されているネットワークに FRR 保護を追加することを前提としています。

設定作業を実行する前に、次の作業を完了していることを確認してください。ただし、MPLS TE トンネルはまだ設定していなくてもかまいません。

- 関連するすべてのルータおよびインターフェイス上での MPLS TE のイネーブル化
- MPLS TE トンネルの設定

MPLS TE トンネルの設定方法を確認するには、『Cisco IOS XE Multiprotocol Label Switching Configuration Guide』を参照してください。

以下のセクションでは、リンクやノードの障害からネットワークの LSP を保護するための FRR の使用方法を説明します。各作業は、必須と任意に分けられています。

（注） これらの設定作業は任意の順序で実行できます。

（注） NNHOP バックアップ トンネルは、NHOP を経由できません。

# LSP 上での高速リルートの有効化

LSP は、高速リルート可能として設定されている場合だけ、バックアップ トンネルを使用できます。LSP 上で Fast Reroute を有効にするには、次のタスクを実行します。各 LSP のヘッドエンドでコマンドを入力します。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **tunnelmplstraffic-engfast-reroute** [**bw-protect**] [**node-protect**]
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 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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 | **interfacetunnel***number*<br><br>例：<br>`Router(config)# interface tunnel 1000` | 指定したトンネルのインターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **tunnelmplstraffic-engfast-reroute** [**bw-protect**] [**node-protect**]<br><br>例：<br>`Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect node-protect` | リンクまたはノードの障害発生時に、MPLS TE トンネルで、確立されたバックアップ トンネルを使用できるようにします。 |
| ステップ 5 | **end**<br><br>例：<br>`Router(config-if)# end` | 特権 EXEC モードに戻ります。 |

# ネクスト ホップまたはネクストネクスト ホップへのバックアップ トンネルの作成

ネクスト ホップまたはネクストネクスト ホップへのバックアップ トンネルを作成するには、次のタスクを実行します。バックアップ トンネルのヘッドエンドとなるノード（つまり、ダウンストリームのリンクまたはノードに障害が発生する可能性のあるノード）上で、次のコマンドを入力します。

バックアップ トンネルの作成は、基本的に他のトンネルの作成と同じです。次のコマンドはいずれも新しいものではありません。

（注） **exclude-address** コマンドを使用してバックアップ トンネルのパスを指定するときは、インターフェイス アドレスを除外してリンクを除外する（NHOP バックアップ トンネルを作成する場合）か、ルータ ID アドレスを除外してノードを回避する（NNHOP バックアップ トンネルを作成する場合）必要があります。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipunnumbered***typenumber*
5. **tunneldestination***A.B.C.D*
6. **tunnelmodemplstraffic-eng**
7. **tunnelmplstraffic-engpath-option***number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*}} [**lockdown**]
8. **ipexplicit-pathname***name*
9. **exclude-address***address*
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 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **interfacetunnel***number*<br><br>例：<br><br>`Router(config)# interface tunnel 1` | 新しいトンネルインターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **ipunnumbered***typenumber*<br><br>例：<br><br>`Router(config-if)# ip unnumbered loopback0` | このトンネル インターフェイスに、インターフェイス Loopback0 の IP アドレスと同じ IP アドレスを割り当てます。<br><br>（注） このコマンドは、Lookback0 が IP アドレスとともに設定されるまでは有効になりません。 |
| ステップ 5 | **tunneldestination***A.B.C.D*<br><br>例：<br><br>`Router(config-if)# tunnel destination 10.3.3.3` | トンネルが終端するデバイスの IP アドレスを指定します。<br><br>• このアドレスは、保護対象となる LSP の NHOP または NNHOP であるデバイスのルータ ID にする必要があります。 |
| ステップ 6 | **tunnelmodemplstraffic-eng**<br><br>例：<br><br>`Router(config-if)# tunnel mode mpls traffic-eng` | トンネルのカプセル化モードを MPLS TE に設定します。 |
| ステップ 7 | **tunnelmplstraffic-engpath-option***number* {**dynamic** \| **explicit** {**name** *path-name* \| *path-number*}} [**lockdown**]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 300 explicit name avoid-protected-link` | MPLS TE トンネルのパス オプションを設定します。 |
| ステップ 8 | **ipexplicit-pathname***name*<br><br>例：<br><br>`Router(config)# ip explicit-path name avoid-protected-link` | IP 明示パスのサブコマンド モードを入力して、指定されたパスを作成します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 9 | **exclude-address***address*<br><br>例：<br><br>`Router(cfg-ip-expl-path)# exclude-address 10.3.3.3` | リンク保護の場合は、保護対象のリンクの IP アドレスを指定します。<br><br>• ノード保護の場合は、このコマンドで保護対象のノードのルータ ID を指定します。<br><br>（注） バックアップ トンネルパスはダイナミックにも明示的にもできます。exclude-address を使用する必要はありません。バックアップ トンネルは保護対象のリンクまたはノードを回避する必要があるため、除外されたアドレスを使用すると役立ちます。 |
| ステップ 10 | **end**<br><br>例：<br><br>`Router(cfg-ip-expl-path)# end` | 特権 EXEC モードに戻ります。 |

# 保護インターフェイスへのバックアップ トンネルの割り当て

保護されたインターフェイスに 1 つまたは複数のバックアップ トンネルを割り当てるには、次のタスクを実行します。バックアップ トンネルのヘッドエンドとなるノード（つまり、ダウンストリームのリンクまたはノードに障害が発生する可能性のあるノード）上で、次のコマンドを入力します。

（注） インターフェイスに IP アドレスを割り当てて、MPLS TE トンネル機能がイネーブルになるようにインターフェイスを設定する必要があります。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typeslot*/*subslot*/*port*[**.***subinterface-number*]
4. **mplstraffic-engbackup-pathtunnel***tunnel-id*
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 | **イネーブル化**<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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***typeslot/subslot/port*[**.***subinterface-number*]<br><br>例：<br>`Router(config)# interface POS1/0/0` | インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。<br>• *type* 引数で、設定するインターフェイスのタイプを指定します。<br>• *slot* 引数はシャーシのスロット番号です。スロット情報については、該当するハードウェア マニュアルを参照してください。SPA インターフェイス プロセッサ（SIP）については、プラットフォーム固有の SPA ハードウェア インストレーション ガイドまたはプラットフォーム固有の SPA ソフトウェア設定ガイドの対応する「Identifying Slots and Subslots for SIPs and SPAs」トピックを参照してください。<br>• */subslot* キーワードと引数のペアは SPA が搭載されている SIP のセカンダリ スロット番号を指定します。スラッシュ（/）が必要です。<br><br>サブスロット情報については、プラットフォーム固有の SPA ハードウェア インストレーション ガイドおよびプラットフォーム固有の SPA ソフトウェア設定ガイドの対応する「Specifying the Interface Address on an SPA」トピックを参照してください。<br>• */port* キーワードと引数のペアはポートまたはインターフェイス番号を指定します。スラッシュ（/）が必要です。<br><br>ポート情報については、該当するハードウェア マニュアルを参照してください。SPA については、プラットフォーム固有の SPA ソフトウェア設定ガイドの対応する「Specifying |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | the Interface Address on a SPA」トピックを参照してください。<br>• *.subinterface-number* キーワードと引数のペアは 1 から 4294967293 の範囲にあるサブインターフェイス番号を指定します。ピリオド（.）の前の番号は、このサブインターフェイスが属する番号と一致する必要があります。 |
| ステップ 4 | **mplstraffic-engbackup-pathtunnel***tunnel-id*<br>例：<br>`Router(config-if)# mpls traffic-eng backup-path tunnel2` | リンクまたはノードの障害が発生した場合に、このインターフェイスを出る LSP がこのバックアップ トンネルを使用できるようにします。<br>（注） このコマンドを何回か入力して、複数のバックアップ トンネルを同じ保護インターフェイスと関連付けることができます。 |
| ステップ 5 | **end**<br>例：<br>`Router(config-if)# end` | 特権 EXEC モードに戻ります。 |

# バックアップ トンネルへのバックアップ帯域幅およびプール タイプの関連付け

バックアップ帯域幅をバックアップ トンネルに関連付け、バックアップ トンネルを使用できる LSP のタイプを指定するには、次のタスクを実行します。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **tunnelmplstraffic-engbackup-bw**{*bandwidth* | [**sub-pool** {*bandwidth* | **unlimited**}][**global-pool** {*bandwidth* | **unlimited**}]} [**any** {*bandwidth* | **unlimited**}]
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 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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 | **interfacetunnel***number*<br><br>例：<br>`Router(config)# interface tunnel 2` | 指定したトンネルのインターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **tunnelmplstraffic-engbackup-bw** {*bandwidth* \| [**sub-pool** {*bandwidth* \| **unlimited**}][**global-pool** {*bandwidth* \| **unlimited**}]} [**any** {*bandwidth* \| **unlimited**}]<br><br>例：<br>`Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000` | 帯域幅をバックアップ トンネルに関連付け、指定されたプールから帯域幅を割り当てられた LSP がこのトンネルを使用できるかどうかを指定します。 |
| ステップ 5 | **end**<br><br>例：<br>`Router(config-if)# end` | 特権 EXEC モードに戻ります。 |

# バックアップ帯域幅保護の設定

バックアップ帯域幅保護を設定するには、次の作業を実行します。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **tunnelmplstraffic-engfast-reroute** [**bw-protect**]
5. **exit**
6. **mplstraffic-engfast-reroutebackup-prot-preemption** [**optimize-bw**]
7. **exit**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **interfacetunnel***number*<br><br>例：<br><br>`Router(config)# interface tunnel 2` | 指定したトンネルのインターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **tunnelmplstraffic-engfast-reroute** [**bw-protect**]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect` | MPLS TE トンネルが、リンクまたはノードの障害発生時に、確立されたバックアップ トンネルを使用できるようにします。<br><br>• **bw-protect** キーワードを指定すると、帯域幅保護されたバックアップ トンネルを使用するための LSP プライオリティが付与されます。 |
| ステップ 5 | **exit**<br><br>例：<br><br>`Router(config-if)# exit` | グローバル コンフィギュレーション モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **mplstraffic-engfast-reroutebackup-prot-preemption** [**optimize-bw**]<br><br>例：<br><br>`Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw` | バックアップ保護プリエンプション アルゴリズムを、デモートされる LSP の数を最小限にするアルゴリズムから、無駄な帯域幅の大きさを最小限にするアルゴリズムに変更します。 |
| ステップ 7 | **exit**<br><br>例：<br><br>`Router(config-if)# exit` | 特権 EXEC モードに戻ります。 |

# リンクおよびノード障害を高速検出するためのインターフェイスの設定

リンクおよびノード障害が高速検出されるようにインターフェイスを設定するには、次のタスクを実行します。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typeslot*/*subslot*/*port*[**.***subinterface-number*]
4. **posais-shut**
5. **posreport** {**b1-tca** | **b2-tca** | **b3-tca** | **lais** | **lrdi** | **pais** | **plop** | **prdi** | **rdool** | **sd-ber** | **sf-ber** | **slof** | **slos**}
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 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configureterminal**<br><br>例：<br>`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***typeslot*/*subslot*/*port*[**.***subinterface-number*]<br><br>例：<br>`Router(config)# interface pos0/0/0` | インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **posais-shut**<br><br>例：<br>`Router(config-if)# pos ais-shut` | Packet over SONET（POS）インターフェイスが管理シャットダウン ステートになったときに、ラインのアラーム表示信号（LAIS）を送信します。 |
| ステップ 5 | **posreport** {**b1-tca** \| **b2-tca** \| **b3-tca** \| **lais** \| **lrdi** \| **pais** \| **plop** \| **prdi** \| **rdool** \| **sd-ber** \| **sf-ber** \| **slof** \| **slos**}<br><br>例：<br>`Router(config-if)# pos report lrdi` | 選択した SONET アラームが POS インターフェイス用のコンソールに記録されるようにします。 |
| ステップ 6 | **end**<br><br>例：<br>`Router(config-if)# end` | 特権 EXEC モードに戻ります。 |

# 高速トンネルインターフェイス停止のためのインターフェイスの設定

高速トンネル インターフェイス停止用にインターフェイスを設定するには、次の手順を実行します。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **tunnelmplstraffic-enginterfacedowndelay***time*
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 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **interfacetunnel***number*<br><br>例：<br><br>`Router(config)# interface tunnel 1000` | インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **tunnelmplstraffic-enginterfacedowndelay***time*<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng interface down delay 0` | ヘッドエンド ルータにより LSP の停止が検出されるとすぐに、トンネルを強制的に停止します。 |
| ステップ 5 | **end**<br><br>例：<br><br>`Router(config-if)# end` | 特権 EXEC モードに戻ります。 |

# 高速リルートの動作状態の確認

FRR が機能することを確認するには、次のタスクを実行します。

### 手順の概要

1. **showmplstraffic-engtunnelsbrief**
2. **showiprsvpsenderdetail**
3. **showmplstraffic-engfast-reroutedatabase**
4. **showmplstraffic-engtunnelsbackup**
5. **showmplstraffic-engfast-reroutedatabase**
6. **showiprsvpreservation**

## 手順の詳細

**ステップ 1** **showmplstraffic-engtunnelsbrief**

このコマンドを使用して、バックアップ トンネルが動作していることを確認します。

例：

```
Router# show mpls traffic-eng tunnels brief

Signalling Summary:
    LSP Tunnels Process:           running
    RSVP Process:                  running
    Forwarding:                    enabled
    Periodic reoptimization:       every 3600 seconds, next in 1706 seconds
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
Router_t1                        10.112.0.12      -         PO2/0/1   up/up
Router_t2                        10.112.0.12      -         unknown   up/down
Router_t3                        10.112.0.12      -         unknown   admin-down
Router_t1000                     10.110.0.10      -         unknown   up/down
Router_t2000                     10.110.0.10      -         PO2/0/1   up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

**ステップ 2** **showiprsvpsenderdetail**

このコマンドを使用して、LSP が適切なバックアップ トンネルによって保護されていることを確認します。

次に、障害発生前に PLR で **showiprsvpsenderdetail** コマンドが入力されたときのサンプル出力を示します。

例：

```
Router# show ip rsvp sender detail

PATH:
 Tun Dest:   10.10.0.6  Tun ID: 100  Ext Tun ID: 10.10.0.1
 Tun Sender: 10.10.0.1  LSP ID: 31
 Path refreshes:
  arriving: from PHOP 10.10.7.1 on FE0/0/0 every 30000 msecs
 Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0x7) Local Prot desired, Label Recording, SE Style
  session Name: R1_t100
 ERO: (incoming)
  10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
  10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
 RRO:
   10.10.7.1/32, Flags:0x0 (No Local Protection)
   10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP) !Available to NNHOP
   10.10.1.1/32, Flags:0x0 (No Local Protection)
 Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
   Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
 Fast-Reroute Backup info:
   Inbound  FRR: Not active
   Outbound FRR: No backup tunnel selected
 Path ID handle: 50000416.
 Incoming policy: Accepted. Policy source(s): MPLS/TE
 Status: Proxy-terminated
```

**ステップ 3** **showmplstraffic-engfast-reroutedatabase**

**clearirpsvphelloinstancecounters** コマンドを入力して、次のことを確認します。

- MPLS TE FRR ノード保護が有効になっている。
- 特定タイプの LSP がバックアップ トンネルを使用できる。

次のコマンド出力は、保護されている LSP を表しています。

例：

```
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected tunnel              In-label Out intf/label     FRR intf/label   Status
Tunnel500                     Tun hd   AT2/0/0.100:Untagg Tu501:20         ready
Prefix item frr information:
Prefix              Tunnel     In-label Out intf/label     FRR intf/label   Status
10.0.0.8/32         Tu500      18       AT2/0/0.100:Pop ta Tu501:20          ready
10.0.8.8/32         Tu500      19       AT2/0/0.100:Untagg Tu501:20          ready
10.8.9.0/24         Tu500      22       AT2/0/0.100:Untagg Tu501:20          ready
LSP midpoint item frr information:
LSP identifier                In-label Out intf/label   FRR intf/label   Status
```

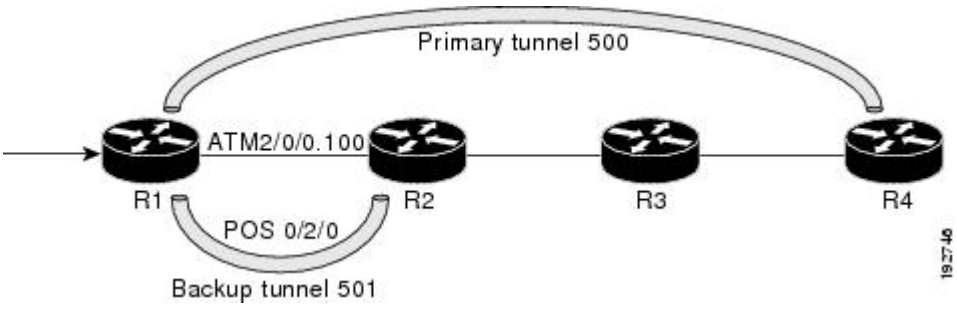
LDP がイネーブルになっていない場合、すべてのプレフィックスが単一のリライトを使用するため、個別のプレフィックス アイテムは表示されません。特定の IP プレフィックスがこの画面に表示されていない場合、その IP プレフィックスが FRR 保護されていることを確認するには、**showmplsforwarding-table***ip-address***detail** コマンド内にそのプレフィックスを入力します。画面の最後の行に、そのプレフィックスが保護されているかどうかが示されます。

例：

```
Router# show mpls forwarding-table 10.0.0.11 32 detail

Local     Outgoing    Prefix         Bytes tag    Outgoing     Next Hop
tag       tag or VC   or Tunnel Id   switched     interface
Tun hd    Untagged    10.0.0.11/32   48           pos1/0/0     point2point
           MAC/Encaps=4/8, MTU=1520, Tag Stack{22}
           48D18847 00016000
           No output feature configured
           Fast Reroute Protection via (Tu0, outgoing label 12304)
```

次のコマンド出力は、FRR プライマリ トンネルが ATM インターフェイスを経由し、バックアップ トンネルが POS インターフェイスを経由する場合に保護される LSP を示しています。次の図に示すように、インターフェイス ATM 2/0/0.100 がバックアップ トンネル 501 によって保護されています。

図 *14*：***Protected LSPs***



この図は、保護されている LSP を示しています。

- プライマリ トンネルは 500 です。そのパスは、ATM 2/0/0.100 によって R1 から R2 に、続いて R2 から R3、R3 から R4 の順に通過します。
- FRR バックアップ トンネルは 501 です。パスは POS 0/2/0 を介した R1 から R2 です。
- インターフェイス ATM 2/0/0.100 は、バックアップ トンネル 501 によって保護されます。

例：

```
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected tunnel In-label Out intf/label  FRR intf/label Status
Tunnel500 Tun hd AT2/0/0.100:Untagg Tu501:20 ready
Prefix item frr information:
Prefix Tunnel In-label Out intf/label   FRR intf/label Status
10.0.0.8/32 Tu500 18 AT2/0/0.100:Pop ta Tu501:20 ready
10.0.8.8/32 Tu500 19 AT2/0/0.100:Untagg Tu501:20 ready
10.8.9.0/24 Tu500 22 AT2/0/0.100:Untagg Tu501:20 ready
LSP midpoint item frr information:
LSP identifier In-label Out intf/label FRR intf/label Status
```

次のコマンド出力は、FRR バックアップ トンネルが ATM インターフェイスを経由する場合に保護される LSP を示しています。

例：

```
Router# show mpls traffic-eng fast-reroute database

Tunnel head end item frr information:
Protected tunnel In-label   Out intf/label FRR intf/label Status
Tunnel500 Tun hd PO0/2/0:Untagged Tu501:20 ready
Prefix item frr information:
Prefix Tunnel In-label Out intf/label FRR intf/label Status
10.0.0.8/32 Tu500 18 PO0/2/0:Pop tag  Tu501:20 ready
10.0.8.8/32 Tu500 19 PO0/2/0:Untagged Tu501:20 ready
10.8.9.0/24 Tu500 22 PO0/2/0:Untagged Tu501:20 ready
LSP midpoint item frr information:
LSP identifier In-label Out intf/label FRR intf/label Status
```

**ステップ 4** **showmplstraffic-engtunnelsbackup**

バックアップ トンネルが動作するには次の条件があります。

- **LSP が再ルーティング可能であること**：LSP のヘッドエンドで、**showruninttunnel***tunnel-number* コマンドを入力します。出力に **tunnelmplstraffic-engfast-reroute** コマンドが含まれている必要があります。このコマンドが含まれていない場合は、トンネルに対してこのコマンドを入力してください。

バックアップ トンネルの起点のルータ上で、**showmplstraffic-engtunnelsbackup** コマンドを入力します。次にサンプルのコマンド出力を示します。

例：

```
Router# show mpls traffic-eng tunnels backup
Router_t578
  LSP Head, Tunnel578, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 1
```

```
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0/0, PO1/1/0, PO0/3/3
    Protected lsps: 1
    Backup BW: any pool unlimited; inuse: 100 kbps
Router_t5710
  LSP Head, Tunnel5710, Admin: admin-down, Oper: down
  Src 10.55.55.55, Dest 10.7.7.7, Instance 0
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/1/0
    Protected lsps: 0
    Backup BW: any pool unlimited; inuse: 0 kbps
Router_t5711
  LSP Head, Tunnel5711, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.7.7.7, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0/0
    Protected lsps: 2
    Backup BW: any pool unlimited; inuse: 6010 kbps
```

コマンド出力により、次のことを確認できます。

- バックアップ トンネルが存在している：この LSP の NHOP または NNHOP で終端するバックアップ トンネルが存在することを確認します。[Dest] フィールド内で LSP の NHOP または NNHOP を検索します。
- バックアップ トンネルが動作している：バックアップ トンネルが動作していることを確認するには、[State] フィールド内で「Up」を検索します。
- バックアップ トンネルが LSP のインターフェイスに関連付けられている：LSP のインターフェイスがこのバックアップ トンネルを使用できるように設定されていることを確認します。保護フィールド リスト内で LSP の出力インターフェイスを検索します。
- バックアップ トンネルに十分な帯域幅がある：バックアップ トンネルが保有できる帯域幅を制限した場合は、障害発生時にこのバックアップ トンネルを使用する LSP を確保できるだけの帯域幅がバックアップ トンネルにあることを確認します。LSP の帯域幅は、LSP のヘッドエンドにある行 **tunnelmplstraffic-engbandwidth** によって定義されています。バックアップ トンネル上の使用可能な帯域幅を判断するには、[cfg] フィールドと [inuse] フィールドを参照してください。障害発生時にこのバックアップ トンネルを使用する LSP に収容する十分な帯域幅がない場合は、追加のバックアップ トンネルを作成するか、**tunnelmplstraffic-engbandwidth** コマンドを使用して、既存のトンネルのバックアップ帯域幅を大きくします。

（注） 十分な帯域幅の大きさを決定するために、オフラインでのキャパシティ プランニングが必要になることがあります。

- バックアップ トンネルに適切な帯域幅タイプが割り当てられている：このバックアップ トンネルを使用できる LSP のタイプを（サブプールまたはグローバル プールに）制限した場合、その LSP がバックアップ トンネルに適したタイプであることを確認します。LSP のタイプは、この LSP のヘッドエンドにある行 **tunnelmplstraffic-engbandwidth** によって定義されています。この行に「subpool」という語が含まれている場合、LSP はサブプール帯域幅を使用します。含まれていない場合は、グローバル プール帯域幅を使用します。上のコマンドの出力を参照して、LSP タイプが、バックアップ トンネルが保有できるタイプと一致していることを確認します。

上記のいずれのアクションも成功しない場合は、バックアップ トンネルのヘッドエンドであるルータ上で **debugiprsvpfast-reroute** コマンドと **debugmplstraffic-engfast-reroute** コマンドを入力して、デバッグを有効にします。続いて、次の手順を実行します。

1. プライマリ トンネルに対して **shutdown** コマンドを入力します。
2. プライマリ トンネルに対して **noshutdown** コマンドを入力します。
3. デバッグ出力を参照します。

**ステップ 5** **showmplstraffic-engfast-reroutedatabase**
**cleariprsvphelloinstancecounters** コマンドを入力して、次のことを確認します。

- MPLS TE FRR ノード保護が有効になっている。
- 特定タイプの LSP がバックアップ トンネルを使用できる。

次のコマンド出力は、保護されている LSP を表しています。

例：

```
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected Tunnel   In-label   intf/label         FRR intf/label      Status
Tunnel10           Tun        pos1/0/0:Untagged  Tu0:12304           ready
Prefix item frr information:
Prefix        Tunnel  In-label    Out intf/label     FRR intf/label Status
10.0.0.11/32  Tu110   Tun hd      pos1/0/0:Untagged  Tu0:12304      ready
LSP midpoint frr information:
LSP identifier       In-label Out intf/label     FRR intf/label   Status
10.0.0.12 1 [459]    16       pos0/1/0:17        Tu2000:19        ready
```

（注） LDP がイネーブルになっていない場合、すべてのプレフィックスが単一のリライトを使用するため、個別のプレフィックスアイテムは表示されません。特定の IP プレフィックスがこの画面に表示されていない場合、その IP プレフィックスが FRR 保護されていることを確認するには、**showmplsforwarding-table***ip-address***detail** コマンド内にそのプレフィックスを入力します。画面の最後の行に、そのプレフィックスが保護されているかどうかが示されます。

例：

```
Router# show mpls forwarding-table 10.0.0.11 32 detail

Local    Outgoing    Prefix         Bytes tag    Outgoing       Next Hop
tag      tag or VC   or Tunnel Id   switched     interface
Tun hd   Untagged    10.0.0.11/32   48           pos1/0/0       point2point
          MAC/Encaps=4/8, MTU=1520, Tag Stack{22}
          48D18847 00016000
          No output feature configured
          Fast Reroute Protection via (Tu0, outgoing label 12304)
```

**ステップ 6** **showiprsvpreservation**
次に、プライマリ LSP のヘッドエンドに入力された **showiprsvpreservation** コマンドの出力例を示します。プライマリ LSP のヘッドエンドにコマンドを入力すると、この LSP が通過する各ホップでの FRR のステータス（つまり、ローカル保護）などが表示されます。各ホップの情報は、Resv メッセージとともに末尾から先頭に移動する Record Route Object（RRO）内に収集されます。

例：

```
Router# show ip rsvp reservation detail
Reservation:
  Tun Dest:   10.1.1.1  Tun ID: 1  Ext Tun ID: 10.1.1.1
  Tun Sender: 10.1.1.1  LSP ID: 104
  Next Hop: 10.1.1.2 on POS1/0/0
  Label: 18 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  RRO:
    10.1.1.1/32, Flags:0x1 (Local Prot Avail/to NHOP)
      Label subobject: Flags 0x1, C-Type 1, Label 18
    10.1.1.1/32, Flags:0x0 (Local Prot Avail/In Use/Has BW/to NHOP)
      Label subobject: Flags 0x1, C-Type 1, Label 16
    10.1.1.2/32, Flags:0x0 (No Local Protection)
      Label subobject: Flags 0x1, C-Type 1, Label 0
  Resv ID handle: CD000404.
  Policy: Accepted. Policy source(s): MPLS/TE
```

プライマリ LSP に関して、次の点に注意してください。

- プライマリ LSP には、最初のホップで NHOP バックアップ トンネルを使用するような保護が設定されています。
- また、2 番めのホップで NHOP バックアップ トンネルをアクティブに使用するような保護が設定されています。
- 3 番めのホップでは、ローカルな保護は設定されていません。

RRO 画面には、ホップごとに次の情報が表示されます。

- ローカル保護が使用可能かどうか（つまり、LSP によりバックアップ トンネルが選択されているかどうか）
- ローカル保護が使用中かどうか（つまり、LSP が、選択したバックアップ トンネルを現在使用しているかどうか）
- 選択されたバックアップ トンネルは、NHOP バックアップ トンネルか NNHOP バックアップ トンネルのいずれであるか
- このホップで使用されるバックアップ トンネルが帯域幅保護を提供するかどうか

## トラブルシューティングのヒント

ここでは、次の内容について説明します。

### LSP が Ready のまま Active にならない

次のいずれかのイベントが発生すると、PLR で LSP は Ready から Active に移行します。

- プライマリ インターフェイスが停止した：プライマリ インターフェイス（LSP の発信インターフェイス）が停止した場合、LSP がバックアップ トンネルを使用する準備が完了すれば、LSP はアクティブ状態に移行し、そのデータがバックアップ トンネル上を流れるようになります。一部のプラットフォームおよびインターフェイス タイプ（たとえば、GSR POS インターフェイスなど）では、このイベントを非常にすばやく検出する高速インターフェイス停止ロジックが追加されています。このロジックが存在しないプラットフォームでは、検出時間が遅くなります。このようなプラットフォームでは、RSVP Hello を有効にすると動作する場合があります（次の箇条書き項目「Hello によりネクスト ホップが停止していることが検出された」を参照）。
- Hello によりネクスト ホップが停止していることが検出された：プライマリ インターフェイス（LSP の発信インターフェイス）上で Hello が有効になっている場合、LSP のネクストホップが到達不能になると、そのネクストホップが停止していると宣言されます。このイベントによって、LSP はそのバックアップ トンネルをアクティブに使用し始めます。プライマリ インターフェイスが停止していなくても、ネクストホップは停止していると宣言されることに注意してください。たとえば、リブート、ソフトウェア、またはハードウェアの問題によってネクスト ホップが応答を停止した場合、Hello が、このネクスト ホップを使用して LSP をトリガーし、そのバックアップ トンネルに切り替えます。また、Hello は、ギガビット イーサネットなど、インターフェイスは動作しているが（リンク層のライブネス検出メカニズムがないために）使用可能になっていないインターフェイス上で FRR をトリガーする支援も行います。

### プライマリ トンネルにより動作中のバックアップ トンネルが選択されない

バックアップ トンネルが動作中であるのに、プライマリ トンネル（LSP）によってバックアップ トンネルとして選択されない場合は、バックアップ トンネルに対して次のコマンドを入力します。

- **シャットダウン**
- **noshutdown**

（注） バックアップ トンネルのステータスを変更した場合、そのバックアップ トンネルに対してバックアップ トンネル選択アルゴリズムが再実行されます。現在そのバックアップ トンネルが選択されている（つまり、バックアップ トンネルを使用する準備ができている）LSP は、そのバックアップ トンネルとの関連付けが解除されてから、そのバックアップ トンネルまたは別のバックアップ トンネルと再び関連付けられます。これは一般に安全であり、通常は同じ LSP がそのバックアップ トンネルにマップされます。ただし、そのバックアップ トンネルをアクティブに使用している LSP がある場合、そのバックアップ トンネルをシャットダウンすると、それらの LSP が切断されます。

### 拡張 RSVP コマンド

次の RSVP コマンドは拡張されて、FRR ステートの検証や FRR のトラブルシューティング時に役立つ情報が表示されるようになりました。

- **showiprsvprequest**：アップストリーム予約ステート（つまり、このノードがアップストリーム送信する Resv メッセージに関連する情報）を表示します。
- **showiprsvpreservation**：受信された Resv メッセージに関する情報を表示します。
- **showiprsvpsender**：受信される Path メッセージに関する情報を表示します。

これらのコマンドは、データ ステートではなく、コントロール プレーン ステートを表示します。つまり、これらのコマンドは、LSP のシグナリングに使用される RSVP メッセージ（Path および Resv）に関する情報を表示します。LSP 上を転送されるデータ パケットの詳細については、**showmplsforwarding** コマンドを使用してください。

### RSVP Hello

RSVP Hello 機能を使用すると、RSVP ノードは、ネイバー ノードが到達不能になった場合にそれを検出できます。リンク層障害の通知が使用可能でなく、番号なしのリンクが使用されていない場合、またはリンク層により提供される障害検出メカニズムが十分でないためにタイムリーにノード障害を検出できない場合は、この機能を使用してください。Hello を操作できるようにするには、Hello をルータでグローバルに設定し、さらに特定のインターフェイス上でも設定する必要があります。

### Hello インスタンスが作成されていない

Hello インスタンスが作成されていない場合は、次の手順を実行します。

- RSVP Hello がルータ上でグローバルにイネーブルになっているかどうかを判断します。**ip rsvp signalling hello**（コンフィギュレーション）コマンドを入力します。
- RSVP Hello が、LSP が通過するインターフェイス上でイネーブルになっているかどうかを判断します。**ip rsvp signalling hello**（インターフェイス）コマンドを入力します。
- **show ip rsvp sender** コマンドの出力を表示することにより、少なくとも 1 つの LSP にバックアップ トンネルがあることを確認します。「Ready」の値は、バックアップ トンネルが選択されていることを示します。

### 「No entry at index (error may self-correct, RRO may not yet have propagated from downstream node of interest)」というエラーメッセージがローカル修復ポイントで出力される

FRR は、ダウンストリームから到着する Resv メッセージ内のレコード ルート オブジェクト（RRO）に依存しています。LSP が高速リルート可能であることを示す SESSION_ATTRIBUTE ビットが含まれる Path メッセージを受信するルータは、対応する Resv メッセージに RRO を組み込む必要があります。

LSP が FRR 用に設定されているが、ダウンストリーム ルータから到着する Resv に不完全な RRO が含まれる場合、「No entry at index (error may self-correct, RRO may not yet have propagated from downstream node of interest)」というメッセージが出力されます。不完全な RRO とは、NHOP または NNHOP で RRO にエントリが組み込まれなかった RRO のことです。

このエラーは、通常、RRO エントリが不足しているために NHOP または NNHOP に関する情報が十分でなく、この LSP に対して NHOP または NNHOP へのバックアップ トンネルを選択できないことを示しています。

この状況が一時的に発生しても、問題が自動的に修正されることもあります。あとから Resv メッセージが完全な RRO とともに受信された場合は、エラーメッセージを無視してください。

エラーが修正されたかどうかを判断するには、**clear ip rsvp hello instance counters** コマンドを入力して、Resv メッセージ内の RRO を表示します。問題の LSP だけを表示するには、出力フィルタキーワードを使用します。

### ローカル修復ポイントで「Couldn't get rsbs (error may self-correct when Resv arrives)」というエラーメッセージが出力される

Resv メッセージがダウンストリームから到着するまで、PLR は LSP のバックアップ トンネルを選択できません。

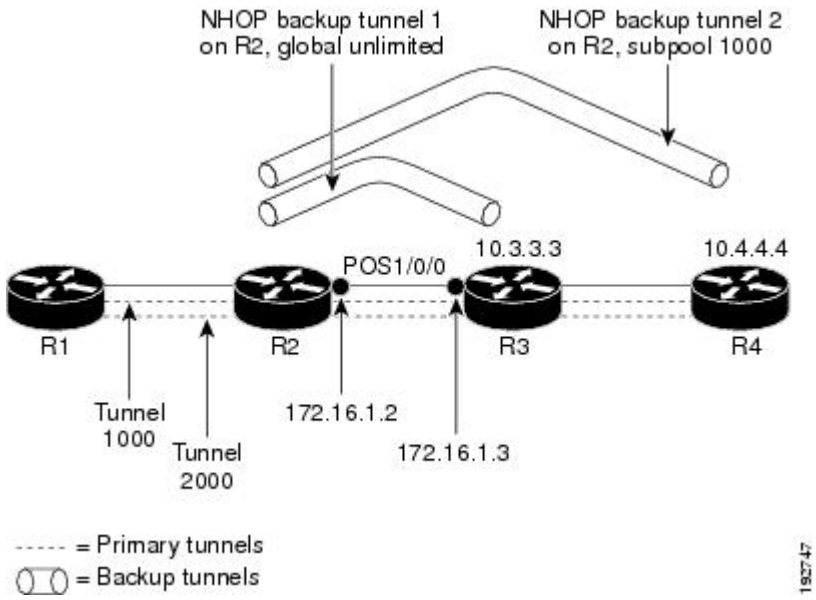
このエラーが発生した場合、通常は何か問題があることを示しています。たとえば、この LSP に対して予約が存在しないなどです。この問題をトラブルシューティングするには、**debug ip rsvp reservation** コマンドを使用してデバッグを有効にします。

このエラーメッセージが発生しても、無視できる場合もあります。たとえば、Resv メッセージがダウンストリームから到着する前に LSP が変更された場合などです。変更されると、PLR が LSP に対するバックアップ トンネルの選択を試行することがあります。このとき、この LSP に対して Resv メッセージが到着していないと、選択は失敗します（それにより、このエラーメッセージが表示されます）。

# RSVP Hello サポートによるリンクとノード保護の設定例

これらの例は、次の図に関連しています。

図 *15* : バックアップ トンネル




## すべてのトンネルに対する高速リルートの有効化：例

ルータ R1 上で、保護対象のトンネル（トンネル 1000 とトンネル 2000）ごとにインターフェイス コンフィギュレーション モードを開始します。パス上でリンクまたはノードの障害が発生した場合に、これらのトンネルがバックアップ トンネルを使用できるようにします。

トンネル 1000 は、サブプールから 10 ユニットの帯域幅を使用します。

トンネル 2000 は、グローバル プールから 5 ユニットの帯域幅を使用します。**tunnel mpls traffic-eng fast-reroute** コマンド内でそれぞれ **bw-prot**、**node-prot** を指定することにより、「bandwidth protection desired」ビットと「node protection desired」ビットが設定されています。

```
Router(config)# interface Tunnel1000
Router(config-if)# tunnel mpls traffic-eng fast-reroute
Router(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 10
Router(config-if)# exit
Router(config)# interface Tunnel2000
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-prot node-prot
Router(config-if)# tunnel mpls traffic-eng bandwidth 5
Router(config-if)# end
```

# NHOP バックアップ トンネルの作成：例

ルータ R2 上に、R3 への NHOP バックアップ トンネルを作成します。このバックアップ トンネルは、リンク 10.1.1.2 の使用を回避する必要があります。

```
Router(config)# ip explicit-path name avoid-protected-link
Router(cfg-ip-expl-path)# exclude-address 10.1.1.2

Explicit Path name avoid-protected-link:
____1: exclude-address 10.1.1.2
Router(cfg-ip_expl-path)# end

Router(config)# interface Tunnel1

Router(config-if)# ip unnumbered loopback0

Router(config-if)# tunnel destination 10.3.3.3
Router(config-if)# tunnel mode mpls traffic-eng0

Router(config-if)# tunnel mpls traffic-eng path-option explicit avoid-protected-link
```

# NNHOP バックアップ トンネルの作成：例

ルータ R2 上に、R4 への NNHOP バックアップ トンネルを作成します。このバックアップ トンネルは R3 を回避する必要があります。

```
Router(config)# ip explicit-path name avoid-protected-node

Router(cfg-ip-expl-path)# exclude-address 10.3.3.3

Explicit Path name avoid-protected-node:
____1: exclude-address 10.3.3.3
Router(cfg-ip_expl-path)# end

Router(config)# interface Tunnel2

Router(config-if)# ip unnumbered loopback0

Router(config-if)# tunnel destination 10.4.4.4

Router(config-if)# tunnel mode mpls traffic-eng0

Router(config-if)# tunnel mpls traffic-eng path-option explicit avoid-protected-node
```

# 保護インターフェイスへのバックアップ トンネルの割り当ての例

ルータ R2 上で、両方のバックアップ トンネルをインターフェイス POS1/0/0 に関連付けます。

```
Router(config)# interface POS1/0/0

Router(config-if)# mpls traffic-eng backup-path tunnel1

Router(config-if)# mpls traffic-eng backup-path tunnel2
```

# バックアップトンネルへのバックアップ帯域幅およびプールタイプの関連付けの例

バックアップ トンネル 1 は、グローバル プールから帯域幅を取り込む LSP だけが使用します。バックアップ トンネル 1 は帯域幅保護を提供しません。バックアップ トンネル 2 は、サブプールから帯域幅を取り込む LSP だけが使用します。バックアップ トンネル 2 は、最大 1000 ユニットの帯域幅保護を提供します。

```
Router(config)# interface Tunnel1
Router(config-if)# tunnel mpls traffic-eng backup-bw global-pool Unlimited
Router(config)# interface Tunnel2
Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000
```

# バックアップ帯域幅保護の設定：例

次の例では、バックアップ帯域幅保護が設定されています。

（注） このグローバル設定が必要なのは、バックアップ保護プリエンプション アルゴリズムを、デモートされる LSP の数を最小限にするアルゴリズムから、無駄な帯域幅の大きさを最小限にするアルゴリズムに変更する場合だけです。

```
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect
Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw
```

# リンクおよびノード障害を高速検出するためのインターフェイスの設定：例

次の例では、pos ais-shut が設定されています。

```
Router(config)# interface pos0/0/0
Router(config-if)# pos ais-shut
```

次の例では、OS インターフェイス上に report lrdi が設定されています。

```
Router(config)# interface pos0/0/0
Router(config-if)# pos report lrdi
```

# 高速トンネル インターフェイス停止のためのインターフェイスの設定：例

次の例では、ヘッドエンドルータによってLSPが停止したことが検出されるとすぐに、トンネル1000が停止します。

```
Router(config)# interface tunnel 1000
Router(config-if)# tunnel mpls traffic-eng interface down delay 0
```

# RSVP Hello および POS シグナルの設定：例

Helloは、ルータ上でグローバルに設定し、さらにFRR保護の必要な特定のインターフェイス上でも設定する必要があります。Helloを設定するには、次のコンフィギュレーション コマンドを使用します。

- **iprsvpsignallinghello**（コンフィギュレーション）：ルータ上でグローバルにHelloを有効にします。
- **iprsvpsignallinghello**（インターフェイス）：FRR保護が必要なインターフェイス上でHelloを有効にします。

次のコンフィギュレーション コマンドは、省略可能です。

- **iprsvpsignallinghellodscp**：Helloメッセージの IP ヘッダー内にある DSCP 値を設定します。
- **iprsvpsignallinghellorefreshmisses**：ノードが、そのネイバーとの通信が停止していると見なすまでに失うことが可能な行内の確認応答の数を指定します。
- **iprsvpsignallinghellorefreshinterval**：Hello Request 間隔を設定します。
- **iprsvpsignallinghellostatistics**：ルータ上の Hello 統計を有効にします。

FRR障害を検出するためのPOSシグナリングを設定するには、**pos report all** コマンドを入力するか、次のコマンドを入力して個々のレポートを要求します。

- **posais-shut**
- **posreportrdool**
- **posreportlais**
- **posreportlrdi**
- **posreportpais**
- **posreportprdi**
- **posreportsd-ber**

# その他の参考資料

ここでは、（RSVP Hello がサポートされた）MPLS TE：リンクおよびノード保護（高速トンネルインターフェイス停止検出付き）機能の関連資料について説明します。

## 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| IS-IS | • 『*Cisco IOS IP Routing Protocols Command Reference*』<br>• 『Configuring a Basic IS-IS Network』 |
| MPLS トラフィック エンジニアリング コマンド | 『*Cisco IOS Multiprotocol Label Switching Command Reference*』 |
| OSPF | • 『*Cisco IOS IP Routing Protocols Command Reference*』<br>• 『Configuring OSPF』 |
| RSVP コマンド | • 『*Cisco IOS Multiprotocol Label Switching Command Reference*』<br>• 『*Cisco IOS Quality of Service Solutions Command Reference*』 |

## 標準

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

### MIB

| MIB | MIB のリンク |
|---|---|
| この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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 XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索し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。<br>http://www.cisco.com/go/mibs |

### RFC

| RFC | Title |
|---|---|
| RFC 4090 | 『Fast Reroute Extensions to RSVP-TE for LSP Tunnels』 |

### シスコのテクニカル サポート

| 説明 | Link |
|---|---|
| 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。<br>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。<br>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/en/US/support/index.html |

# RSVP Hello サポートによるリンクとノード保護の機能の情報

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 *6*：（*RSVP Hello* がサポートされた）*MPLS TE*：リンクおよびノード保護（高速トンネル インターフェイス停止検出付き）の機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| （RSVP Hello がサポートされた）MPLS TE：リンクおよびノード保護（高速トンネル インターフェイス停止検出付き） | Cisco IOS XE Release 2.3 | |

| 機能名 | リリース | 機能情報 |
| --- | --- | --- |
| | | （RSVP Hello がサポートされた）MPLS TE：リンクおよびノード保護（高速トンネル インターフェイス停止検出付き）機能は、次の高速再ルーティング（FRR）機能を提供します。<br>• バックアップ トンネルは、ネクストネクスト ホップ ルータで終端して、リンクおよびノードの障害からダウンストリームのリンクとノードの両方を保護します。1つのインターフェイスを保護できるバックアップ トンネルの数に制限はありません（メモリ制限を除く）。バックアップ トンネルは、複数の LSP および複数のインターフェイスを保護できるため、スケーラブルです。<br>• バックアップ帯域幅保護。これにより、特定種類のデータ（音声など）を伝送する LSP 用のバックアップ トンネルにプライオリティを割り当てることができます。<br>• 高速トンネル インターフェイス停止検出。ヘッドエンド ルータによって LSP 上に障害の発生したリンクが検出されると、即時、強制的に「汎用的な」（高速リルート トンネルに限定されない）インターフェイス トンネルは無効になります。<br>• リソース予約プロトコル（RSVP）Hello。これを使 |

| 機能名 | リリース | 機能情報 |
|---|---|---|
| | | 用すると、ノード障害の検出を短時間で行うことができます。<br><br>Cisco IOS リリース XE 2.3 では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。<br><br>次のコマンドが導入または変更されました。**tunnel mpls traffic-eng interface down delay**。 |

# 用語集

**バックアップ帯域幅**：NHOP および NNHOP バックアップ トンネルを使用すると、リルートされた LSP の帯域幅保護を提供できます。

**バックアップトンネル**：リンクまたはノードの障害発生時に他の（プライマリ）トンネルのトラフィックを保護するために使用される MPLS TE トンネル。

**帯域幅**：リンクの使用可能なトラフィック容量。

**シスコエクスプレスフォワーディング**：ルート参照を保存することにより、ルータ内のパケットの転送を短時間で行うための手段。

**企業ネットワーク**：会社などの組織内でほとんどの主要点を接続する大規模かつ多種多様なネットワーク。

**高速リルート**：ヘッドエンドで新しい LSP を確立しながら、障害のあるリンクまたはノード周囲の一時ルーティングをイネーブルにする手順。

**ギガビットイーサネット**：1996 年に Institute of Electrical and Electronics Engineers（IEEE）802.3z 規格委員会によって承認された、高速イーサネットの規格。

**グローバルプール**：MPLS トラフィック エンジニアリングのリンクまたはノードに割り当てられた合計帯域幅。

**ヘッドエンド**：特定の LSP の起点となり、その LSP を管理するルータ。これは、LSP パス上の最初のルータです。

**ホップ**：2 つのネットワーク ノード間（たとえば、2 つのルータ間）のデータ パケットの通路。

**インスタンス**：Hello インスタンスは、特定のルータ インターフェイス アドレスおよびリモート IP アドレスに対して RSVP Hello 拡張機能を実装します。アクティブな Hello インスタンスは、定期的に Hello Request メッセージを送信し、応答として Hello ACK メッセージを予期します。予期

されている Ack メッセージを受信できない場合、アクティブな Hello インスタンスは、そのネイバー（リモートの IP アドレス）が到達不能である（つまり失われている）ことを宣言します。これにより、このネイバーを通過する LSP の高速リルートが行われることがあります。

**インターフェイス**：ネットワーク接続。

**IntermediateSystem-to-IntermediateSystem**：（IS-IS）。このリンクステート階層型ルーティングプロトコルでは、Intermediate System（IS）ルータを呼び出して、単一のメトリックに基づいてルーティング情報を交換することにより、ネットワーク トポロジを決定します。

**リンク**：隣接するノード間のポイントツーポイント接続。隣接するノード間に複数のリンクが存在することがあります。送信者と受信者の間の回線または伝送パスおよびすべての関連装置からなるネットワーク通信チャネル。回線または伝送リンクと呼ばれることもあります。

**制限付きバックアップ帯域幅**：帯域幅保護を提供するバックアップ トンネル。

**ロードバランシング**：プライマリ リンク上で特定のしきい値を超えた場合に、トラフィックを代替リンクにシフトする設定手法。イベントが発生したためにトラフィックが方向を変えた場合に、代替装置が設定されている必要があるという点で、ロード バランシングは冗長性と似ています。ロード バランシングにおいては、必ずしも代替装置が障害発生時にだけ動作する冗長装置である必要はありません。

**LSP**：ラベルスイッチド パス。2 つのルータ間に設定された接続。この接続では、パケットを伝送するためにラベル スイッチングが使用されます。LSP の目的は、データ パケットを伝送することです。

**マージポイント**：バックアップ トンネルの終端。

**MPLS**：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ネットワークコアにおいて使用されるパケット転送テクノロジー。これにより、スイッチング ノードにデータの転送方法を指示するためのデータ リンク層ラベルが適用されるため、ネットワーク層ルーティングで通常行われる転送よりも高速でスケーラブルな転送が行われます。

**MPLSグローバルラベル割り当て**：ルータ内のすべてのインターフェイスに対して 1 つのラベル領域があります。たとえば、あるインターフェイスに入ってきたラベル 100 は、別のインターフェイスに入ってきたラベル 100 と同じように処理されます。

**NHOP**：ネクスト ホップ。LSP のパス上の次のダウンストリーム ノード。

**NHOPバックアップトンネル**：ネクストホップ バックアップ トンネル。障害ポイントの先にある LSP のネクスト ホップで終端し、障害ポイントのすぐアップストリームにあるホップを起点とするバックアップ トンネル。このバックアップ トンネルは、障害の発生したリンクをバイパスし、障害発生前にこのリンクを使用していたプライマリ LSP を保護するために使用されます。

**NNHOP**：Next-Next HOP（ネクストネクスト ホップ）。LSP のパス上の次のダウンストリーム ノードの後ろのノード。

**NNHOPバックアップトンネル**：ネクストホップから 1 つめのホップのバックアップ トンネル。障害ポイントの先にある LSP のネクストネクスト ホップで終端し、障害ポイントのすぐアップストリームにあるホップを起点とするバックアップ トンネル。このバックアップ トンネルは、障害の発生したリンクまたはノードをバイパスし、障害発生前にこのリンクまたはノードを使用していたプライマリ LSP を保護するために使用されます。

**ノード**：ネットワーク接続のエンドポイント、つまりネットワーク内の複数の回線に共通する接合部。複数のノードをリンクで相互接続することができます。これらのノードは、ネットワーク内のコントロール ポイントとなります。ネットワーク接続のエンドポイント、つまりネットワーク内の複数の回線に共通する接合部。ノードは、プロセッサ、コントローラ、またはワークステーションです。

**OSPF**：Open Shortest Path First。IS-IS プロトコルから派生した、リンクステート階層型の内部ゲートウェイ プロトコル ルーティング アルゴリズム。OSPF 機能には、最小コストによるルーティング、マルチパスのルーティング、およびロード バランシングが含まれます。

**プライマリLSP**：当初、障害発生前に保護インターフェイスを介してシグナリングされていた最後の LSP。障害の前の LSP。

**プライマリトンネル**：障害が発生した場合に高速リルートされる LSP に割り当てられたトンネル。バックアップ トンネルをプライマリ トンネルにすることはできません。

**プロモーション**：新しいバックアップ トンネルが出現した場合などは、LSP に対して選択されていたバックアップ トンネルが再評価されます。この再評価は、成功すると、プロモーションと呼ばれます。

**保護インターフェイス**：1 つ以上のバックアップ トンネルが関連付けられたインターフェイス。

**冗長性**：デバイス、サービス、または接続を重複させて、障害発生時に、冗長なデバイス、サービス、または接続が、障害が発生したこれらの作業を実行できるようにすること。

**RSVP**：Resource Reservation Protocol（リソース予約プロトコル）。カスタマーがインターネット サービスのために要求をシグナリング（予約をセットアップ）する際に使用する IETF プロトコル。これにより、カスタマーはそのネットワーク部分を経由してデータを伝送することを許可されます。

**スケーラビリティ**：ネットワークの拡大に伴って、リソース使用量の程度がどれだけ迅速に増加するかを示すインジケータ。

**ステート**：ルータが各 LSP に関して保守する必要のある情報。この情報は、トンネルをリルートする場合に使用されます。

**サブプール**：MPLS トラフィック エンジニアリングのリンクまたはノードにおける、より限定的な帯域幅。サブプールは、リンクまたはノードの全体的なグローバル プール帯域幅の一部です。

**テールエンド**：LSP が終端するルータ。これは、LSP のパス上の最後のルータです。

**トポロジ**：企業ネットワーキング構造内のネットワーク ノードおよびメディアの物理的な配置。

**トンネル**：2 つのピア間（2 台のルータ間など）のセキュアな通信パス。

**制限なしバックアップ帯域幅**：帯域幅（ベストエフォート型）保護を提供しないバックアップ トンネル（つまり、ベストエフォート型保護を提供します）。

第 4 章

# MPLS トラフィック エンジニアリング：自動トンネル プライマリおよびバックアップ

MPLS トラフィック エンジニアリング - 自動トンネル プライマリおよびバックアップ機能を使用すると、ルータがバックアップ トンネルをダイナミックに構築したり、マルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）トンネルが設定されているすべてのインターフェイスで 1 ホップ プライマリ トンネルをダイナミックに作成したりできるようになります。

プライマリ 1 ホップ自動トンネルおよびバックアップ自動トンネルを使用するルータには、ステートフル スイッチオーバー（SSO）冗長性を設定できます。

# 機能情報の確認

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

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、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。

# MPLS トラフィック エンジニアリング - 自動トンネル プライマリおよびバックアップの前提条件

- ルータに TE を設定する。

# MPLS トラフィック エンジニアリング - 自動トンネル プライマリおよびバックアップの制約事項

- TE 自動トンネルを介してトラフィックをルーティングするようにスタティック ルートを設定することはできません。自動トンネルの場合、トンネルの選択に自動ルートだけを使用する必要があります。

# MPLS トラフィック エンジニアリング：自動トンネル プライマリおよびバックアップに関する情報

## MPLS トラフィック エンジニアリング - 自動トンネル プライマリおよびバックアップの概要

MPLS トラフィック エンジニアリング - 自動トンネル プライマリおよびバックアップ機能には、次の特長があります。

- バックアップ自動トンネル：ルータがバックアップ トンネルをダイナミックに構築できるようにします。

- プライマリ 1 ホップ自動トンネル：ルータが、MPLS TE トンネルが設定されているすべてのインターフェイスで 1 ホップ プライマリ トンネルをダイナミックに作成できるようにします。

バックアップ トンネルが存在しない場合、次のタイプのバックアップ トンネルが作成されます。

- ネクスト ホップ（NHOP）
- ネクストネクスト ホップ（NNHOP）

# MPLS トラフィック エンジニアリング - 自動トンネル プライマリおよびバックアップ機能の利点

- バックアップ トンネルは自動的に構築されるため、ユーザが各バックアップ トンネルを事前に設定し、保護対象のインターフェイスにそのバックアップ トンネルを割り当てる必要はありません。
- 1 ホップ プライマリ トンネルのダイナミック作成により、保護対象のトンネルに対して高速再ルーティング（FRR）オプションを使用して MPLS TE トンネルを設定する必要がなくなります。
- 保護は拡張されます。ただし、TE トンネルを使用していない IP トラフィック、または TE トンネルを使用していないラベル配布プロトコル（LDP）ラベルはFRR で保護されません。

# MPLS トラフィック エンジニアリング

MPLS は、インターネット技術特別調査委員会（IETF）により指定されたフレームワークであり、ネットワークを介するトラフィック フローの効率的な指定、ルーティング、フォワーディング、およびスイッチングを可能にします。

TE は、ハイプライオリティのトラフィックに常に十分な帯域幅が確保されるように、帯域割り当てを調整するプロセスです。

MPLS TE では、上流のルータが特定のトラフィック ストリームのネットワーク トンネルを作成してから、そのトンネルに使用可能な帯域幅を設定します。

# MPLS トラフィック エンジニアリング バックアップ自動トンネル

MPLS バックアップ自動トンネルは、高速リルートが可能な TE ラベル スイッチド パス（LSP）を保護します。LSP の保護に MPLS バックアップ自動トンネルを使用しない場合、次の作業を行う必要がありました。

- 各バックアップ トンネルを事前に設定します。
- 保護対象のインターフェイスにバックアップ トンネルを割り当てます。

LSP は、次の状況でリソース予約プロトコル（RSVP）FRR からのバックアップ保護を要求します。

- 最初の RSVP Resv メッセージを受信した場合
- LSP が保護属性なしで確立されたあと、保護属性付きの RSVP パス メッセージを受信した場合
- レコード ルート オブジェクト（RRO）の変更を検出した場合

LSP で使用されているインターフェイスを保護するバックアップ トンネルが存在しない場合、LSP は非保護のままになっていました。

バックアップ自動トンネルを使用すると、必要なときにルータでバックアップ トンネルをダイナミックに構築できます。これにより、MPLS TE トンネルをスタティックに構築する必要がなくなります。

バックアップ トンネルは、次の理由で使用できなくなる場合があります。

- スタティック バックアップ トンネルが設定されていない。
- スタティック バックアップ トンネルは設定されているが、LSP を保護できない。バックアップ トンネルで使用可能な帯域幅が十分でないか、トンネルが別のプールを保護しているか、トンネルがダウンしている可能性があります。

バックアップ トンネルが使用可能でない場合、次の 2 つのバックアップ トンネルがダイナミックに作成されます。

- NHOP：リンク障害から保護
- NNHOP：ノード障害から保護

（注） 最後から 2 番めのホップには、NHOP バックアップ トンネルだけが作成されます。

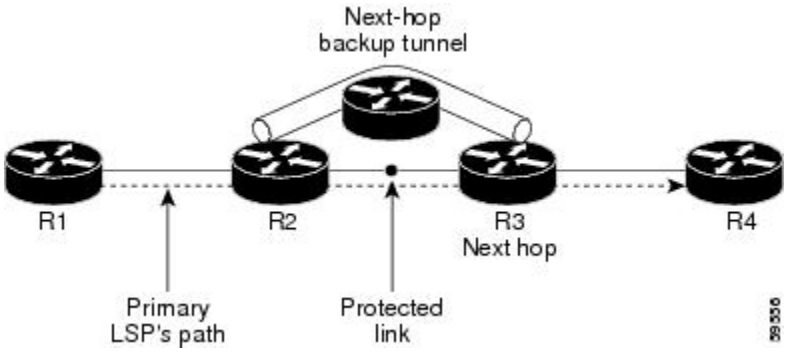
（注） 2 つの LSP が同じ出力インターフェイスと NHOP を共有している場合、3 つ（4 つではない）のバックアップ トンネルが作成されます。これらは NHOP バックアップ トンネルを共有します。

## リンク保護

LSP のパスの単一リンクだけをバイパスするバックアップ トンネルが、リンク保護を提供します。パス上のリンクに障害が発生した場合、バックアップ トンネルは、LSP のトラフィックをネクスト ホップにリルートする（障害の発生したリンクをバイパスする）ことによって LSP を保護します。これらは、障害ポイントの向こう側にある LSP のネクスト ホップで終端するため、ネク

ストホップ（NHOP）バックアップ トンネルと呼ばれます。次の図は、NHOP バックアップ トンネルを示しています。

図 *16*：*NHOP* バックアップ トンネル

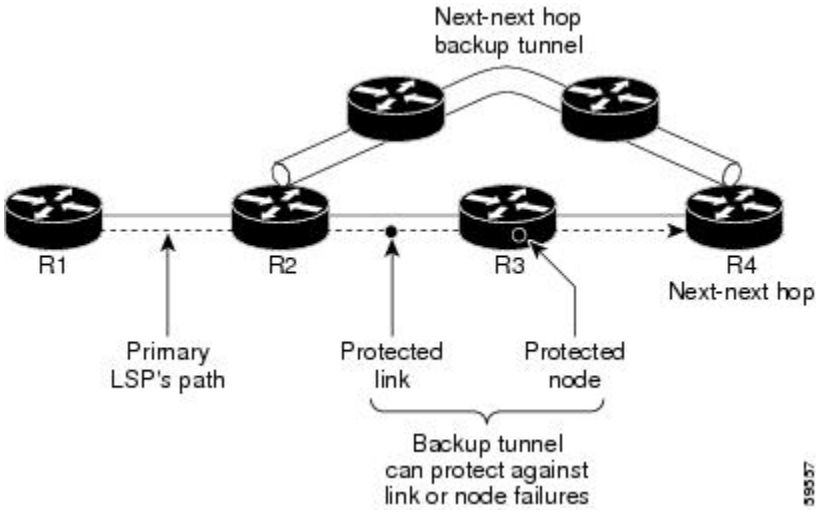



## ノード保護

LSP パスに沿ったネクストホップ ノードをバイパスするバックアップ トンネルは、LSP のネクストホップ ノードの次のノードで終端して、結果としてネクストホップ ノードをバイパスするため、NNHOP バックアップ トンネルと呼ばれます。リンク障害またはノード障害のノード アップストリームで、障害を避けて LSP とトラフィックがネクストホップ ノードにリルートされるようにすることにより、LSP が保護されます。また、NNHOP バックアップ トンネルは、障害の発生したリンクおよびノードをバイパスするため、リンク障害からの保護も提供しています。

次の図は、NNHOP バックアップ トンネルを示しています。

図 *17*：ネクストネクスト ホップ バックアップ トンネル



### 明示パス

明示パスを使用して、次のようにバックアップ自動トンネルが作成されます。

- NHOP では、保護されたリンクの IP アドレスが除外されます。
- NNHOP では、NHOP ルータ ID が除外されます。
- 明示パス名は、_auto-tunnel_tunnel*xxx* です。ここで、*xxx* は、ダイナミックに作成されたバックアップ トンネル ID と一致します。
- **ip unnumbered** コマンドに使用されるインターフェイスのデフォルトは Loopback0 です。これは、別のインターフェイスを使用するようにも設定できます。

### バックアップ自動トンネルの範囲

バックアップ自動トンネルのトンネル範囲は設定可能です。デフォルトでは、最後の 100 個の TE トンネル ID（つまり、65,436 ～ 65,535）が使用されます。使用されているトンネル ID は、自動トンネルによって検出されます。ID は、最も低い番号から割り当てられます。

たとえば、トンネル範囲 1000 ～ 1100 を設定し、スタティックに設定された TE トンネルがその範囲内にある場合、ルータではこれらの ID は使用されません。これらのスタティック トンネルが削除されると、MPLS TE ダイナミック トンネル ソフトウェアでこれらの ID を使用できるようになります。

## MPLS トラフィック エンジニアリング プライマリ自動トンネル

MPLS トラフィック エンジニアリング - 自動トンネル プライマリおよびバックアップ機能を使用すると、ルータが、MPLS トラフィックが設定されているすべてのインターフェイスで 1 ホップ プライマリ トンネルをダイナミックに作成できるようになります。トンネルは、ゼロ帯域幅を使用して作成されます。ゼロ帯域幅が存在する場合、Constraint-based Shortest Path First（CSPF）は Shortest Path First（SPF）と同じになります。そのため、ルータでの自動ルート 1 ホップ プライマリ トンネルの選択は、あたかもトンネルが存在しないかのようになります。これは 1 ホップ トンネルであるため、カプセル化は tag-implicit になります（つまり、タグヘッダーは存在しません）。

### 明示パス

明示パスを使用して、次のように自動トンネルが作成されます。

- 明示パスはダイナミックに作成されます。
- 明示パスには、ネクスト ホップに接続されているインターフェイスの IP アドレスが含まれます。
- 明示パス名は、_auto-tunnel_tunnel*xxx* です。ここで、*xxx* は、ダイナミックに作成された 1 ホップ トンネル ID と一致します。

- **ip unnumbered** コマンドに使用されるインターフェイスのデフォルトは Loopback0 です。これは、別のインターフェイスを使用するようにも設定できます。

### 自動トンネルの範囲

トンネル範囲は設定可能です。デフォルトでは、最後の 100 個の TE トンネル ID（つまり、65,436 ～ 65,535）が使用されます。使用されているトンネル ID は、自動トンネルによって検出されます。ID は、最も低い番号から割り当てられます。

たとえば、トンネル範囲 100 ～ 200 を設定し、スタティックに設定された TE トンネルがその範囲内にある場合、ルータではこれらの ID は使用されません。これらのスタティック トンネルが削除されると、MPLS TE ダイナミック トンネル ソフトウェアで ID を使用できるようになります。

## MPLS トラフィック エンジニアリングのラベルベース転送

ルータはパケットを受信し、パケット内の一部のフィールドを調べて転送先を判断し、それを適切な出力デバイスに送信します。ラベルは、パケットの転送に使用される短い固定長の識別子です。通常、ラベル スイッチング デバイスは、パケットをネクスト ホップに転送する前に、パケット内のラベルを新しい値に置き換えます。このため、転送アルゴリズムはラベル スワッピングと呼ばれます。ラベル スイッチング デバイスは、LSR と呼ばれ、標準の IP コントロール プロトコル（つまり、ルーティング プロトコル、RSVP など）を実行してパケットの転送先を判断します。

## MPLS トラフィック エンジニアリング保護の利点

ここでは、MPLS トラフィック エンジニアリング保護の利点について説明します。

### DeliveryofPacketsDuringaFailure

NNHOP で終端するバックアップ トンネルは、ダウンストリーム リンクとノードの両方を保護します。これにより、リンクおよびノードの障害に対する保護が可能になります。

### 同じインターフェイスを保護する複数のバックアップ トンネル

自動トンネル プライマリおよびバックアップ機能は、ノード保護に必要になるだけでなく、次の利点をもたらします。

- 冗長性：一方のバックアップ トンネルが停止すると、他方のバックアップ トンネルが LSP を保護します。
- バックアップ容量の増加：保護インターフェイスが大容量リンクであり、同じ容量を持つバックアップ パスが 1 つも存在しない場合、その 1 つの大容量リンクを複数のバックアップ トンネルによって保護できます。このリンクを使用している LSP は異なるバックアップ トンネルにフェールオーバーするため、障害発生時にはすべての LSP が適切な帯域幅保護（リ

ルート）を受けることができます。帯域幅保護が必要でない場合、ルータは使用可能なすべてのバックアップ トンネルに LSP を分散させます（つまり、複数のバックアップ トンネルの間でロード バランシングを行います）。

### 拡張性

1 つのバックアップ トンネルで複数の LSP を保護できます。さらに、1 つのバックアップ トンネルで複数のインターフェイスを保護できます。これを、多対 1（N:1）の保護と呼びます。N:1 の保護は、保護の必要な LSP ごとに個別のバックアップ トンネルを使用する必要のある 1 対 1（1:1）の保護に比べて、スケーラビリティ上のメリットが大きくなります。

N:1 保護では、たとえば 1 つのバックアップ トンネルが 5000 の LSP を保護する場合、バックアップ パスに沿った各ルータが 1 つの追加トンネルを維持します。

1:1 保護では、たとえば 5000 のバックアップ トンネルが 5000 の LSP を保護する場合、バックアップ パスに沿った各ルータは 5000 の追加トンネルの状態を維持する必要があります。

### RSVP Hello

RSVP Hello を使用すると、ネイバーがダウンしてもそのネイバーへのインターフェイスが引き続き稼働している状況をルータが検出できるようになります。ネイバーに到達できないことをレイヤ 2 リンク プロトコルで検出できない場合、Hello が検出メカニズムとなります。これにより、ルータがバックアップ トンネルに LSP をスイッチングできるようになり、パケットの損失を回避できます。

## SSO 冗長性の概要

SSO 機能は、Cisco IOS ルータで構成されているネットワークのアベイラビリティを向上させるためのプログラム全体における段階的ステップです。

SSO は特にネットワーク エッジで役立ちます。これは、ネットワーク設計におけるシングル ポイント障害、およびネットワークの停止によりカスタマーのサービスに損失が生じる可能性がある場所を示す二重ルート プロセッサ（RP）を備えたネットワーク エッジ デバイスの保護を提供します。

二重 RP をサポートしているシスコの特定のネットワーキング デバイスでは、SSO は RP 冗長性を活用してネットワークのアベイラビリティを向上させます。この機能は RP の一方をアクティブ プロセッサとして確立し、もう一方の RP をスタンバイ プロセッサとして指定します。次に、これらの間の重要な状態情報を同期します。2 つのプロセッサの初回同期後、SSO はこれらの間の RP ステート情報をダイナミックに維持します。

アクティブ RP に障害が発生したとき、アクティブ RP がネットワーキング デバイスから削除されたとき、またはメンテナンスのために手動で停止されたときに、アクティブ プロセッサからスタンバイ プロセッサへのスイッチオーバーが発生します。

# 自動トンネル バックアップを使用したアフィニティとリンク属性

Cisco IOS Release 15.1(1)S 以降のリリースでは、ダイナミック バックアップ パスの設定時に、アフィニティとリンク属性を MPLS TE 自動トンネル バックアップ機能とともに使用して、リンクを含めるか除外できます。

リンクの場合は、次の例に示すように 32 ビットまでの属性フラグを設定できます。

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet0/0
Router(config-if)# mpls traffic-eng attribute-flags 0x22
```

属性フラグは、パスの選択中にトンネルのアフィニティ ビットと比較されます。

自動トンネル バックアップ機能をイネーブルにすると、次の例に示すようにアフィニティとマスクを任意に指定できます。アフィニティとマスクを指定しない場合は、アフィニティのデフォルトは 0 で、マスクでは 0xFFFF が使用されます。リンク アフィニティを無視するには、アフィニティとマスク 0 を使用します。詳細については、**mplstraffic-engauto-tunnelbackupconfigaffinity** コマンドを参照してください。

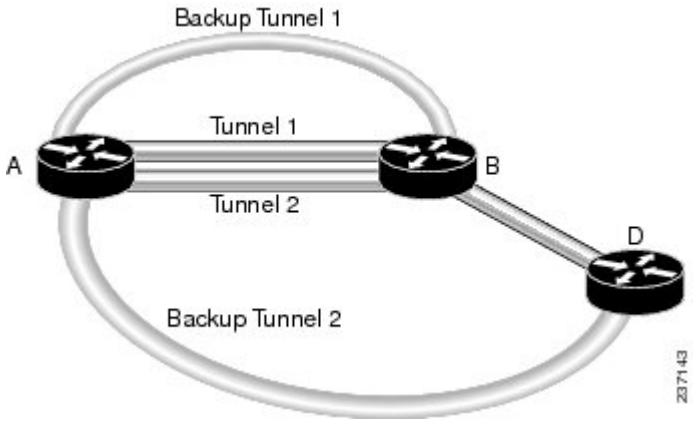
```
Router> enable
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup

Router(config)# mpls traffic-eng auto-tunnel backup config affinity 0x13 mask 0x13
```

**mplstraffic-engauto-tunnelbackupconfigaffinity** コマンドによって設定されるアフィニティまたはマスクは、ダイナミックに作成されたすべてのバックアップ トンネルに使用されます。属性マスクによって、関連のあるリンク属性が決定されます。マスクのビットが 0 の場合、属性は関連しません。マスクのビットが 1 の場合、リンクの属性値と、そのビットに対応するトンネルに設定されたアフィニティは一致する必要があります。

次の図には、2 つのプライマリ トンネルがあります。その 1 つは、ルータ A からルータ B を接続します。もう 1 つのプライマリ トンネルはルータ A からルータ B、そしてルータ D を接続します。すべてのリンクのアトリビュート フラグが 0x22 に設定されています。両方のトンネルで高速リルート保護が必要です。バックアップ トンネルを自動的に作成するには、**mplstraffic-engauto-tunnelbackup** コマンドで自動トンネル バックアップ機能を有効にします。ただし、属性フラグがリンクで設定されているため、ダイナミックに作成されたバックアップ トンネルは起動しません。ダイナミックに作成されたバックアップ トンネルをイネーブルにするには、次のコマンドも発行する必要があります。

Router(config)# mpls traffic-eng auto-tunnel backup config affinity 0x22 mask 0x22

図 *18*：自動トンネル バックアップを使用したリンク属性とアフィニティの指定




# MPLS トラフィック エンジニアリング - 自動トンネル プライマリおよびバックアップの設定方法

## 高速再ルーティングが可能な TE LSP を保護するための MPLS バックアップ自動トンネルの確立

MPLS バックアップ自動トンネルを確立して高速リルートが可能な TE LSP を保護するには、次の作業を実行します。

（注） ステップ 1 ～ 3 だけが必要です。ステップ 3 のあとの追加の手順を実行する場合は、任意の順序で実行できます。

### 手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplstraffic-engauto-tunnelbackup**
4. **mplstraffic-engauto-tunnelbackupnhop-only**
5. **mplstraffic-engauto-tunnelbackuptunnel-num**[**min** *num*] [**max** *num*]
6. **mplstraffic-engauto-tunnelbackuptimersremovalunused***sec*
7. **mplstraffic-engauto-tunnelbackupconfigunnumbered-interface***interface*
8. **mplstraffic-engauto-tunnelbackupconfigaffinity***affinity-value***mask***mask-value*]

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権EXECモードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **mplstraffic-engauto-tunnelbackup**<br><br>例：<br><br>`Router(config)# mpls traffic-eng auto-tunnel backup` | NHOPおよびNNHOPバックアップ トンネルを自動的に構築します。 |
| ステップ 4 | **mplstraffic-engauto-tunnelbackupnhop-only**<br><br>例：<br><br>`Router(config)# mpls traffic-eng auto-tunnel backup nhop-only` | ダイナミック NHOP バックアップ トンネルの作成をイネーブルにします。 |
| ステップ 5 | **mplstraffic-engauto-tunnelbackuptunnel-num**[**min** *num*] [**max** *num*]<br><br>例：<br><br>`Router(config)# mpls traffic-eng auto-tunnel backup tunnel-num min 1000 max 1100` | バックアップ自動トンネル用のトンネル インターフェイス番号の範囲を設定します。 |
| ステップ 6 | **mplstraffic-engauto-tunnelbackuptimersremovalunused***sec*<br><br>例：<br><br>`Router(config)# mpls traffic-eng auto-tunnel backup timers removal unused 50` | タイマーでバックアップ自動トンネルをスキャンし、使用されていないトンネルを削除する頻度を制御します。 |
| ステップ 7 | **mplstraffic-engauto-tunnelbackupconfigunnumbered-interface***interface*<br><br>例：<br><br>`Router(config)# mpls traffic-eng auto-tunnel backup config unnumbered-interface ethernet1/0` | 明示アドレスを使用せずに、指定したインターフェイスでの IP 処理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 | **mplstraffic-engauto-tunnelbackupconfigaffinity***affinity-value***mask***mask-value*]<br><br>例：<br><br>`Router(config)# mpls traffic-eng auto-tunnel backup config affinity 0x22 mask 0x22` | アフィニティ値とマスク フラグを指定します。アフィニティは、トンネルが使用するリンクの属性を決定します。つまり、トンネルがアフィニティを持つ属性です。マスクは、ルータが確認する必要があるリンク属性を決定します。マスクのビットが 0 の場合、リンクまたはそのビットの属性値は関連しません。マスクのビットが 1 の場合、リンクの属性値と、そのビットに対応するトンネルの必要なアフィニティは一致する必要があります。 |

# すべてのネイバーへの MPLS 1 ホップ トンネルの確立

すべてのネイバーへの MPLS 1 ホップ トンネルを確立するには、次の作業を実行します。

（注） ステップ 1 ～ 3 だけが必要です。ステップ 3 のあとの追加の手順を実行する場合は、任意の順序で実行できます。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplstraffic-engauto-tunnelprimaryonehop**
4. **mplstraffic-engauto-tunnelprimarytunnel-num** [**min***num*] [**max***num* ]
5. **mplstraffic-engauto-tunnelprimarytimersremovalrerouted***sec*
6. **mplstraffic-engauto-tunnelprimaryconfigunnumbered***interface*
7. **mplstraffic-engauto-tunnelprimaryconfigmplsip**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **mplstraffic-engauto-tunnelprimaryonehop**<br><br>例：<br><br>`Router(config)# mpls traffic-eng auto-tunnel primary onehop` | すべてのネクストホップへのプライマリ トンネルを自動的に作成します。 |
| ステップ 4 | **mplstraffic-engauto-tunnelprimarytunnel-num** [**min***num*] [**max***num* ]<br><br>例：<br><br>`Router(config)# mpls traffic-eng auto-tunnel primary tunnel-num min 2000 max 2100` | プライマリ自動トンネル用のトンネル インターフェイス番号の範囲を設定します。 |
| ステップ 5 | **mplstraffic-engauto-tunnelprimarytimersremovalrerouted***sec*<br><br>例：<br><br>`Router(config)# mpls traffic-eng auto-tunnel primary timers removal rerouted 400` | 障害が発生したプライマリ自動トンネルを削除するまでの秒数を設定します。 |
| ステップ 6 | **mplstraffic-engauto-tunnelprimaryconfigunnumbered***interface*<br><br>例：<br><br>`Router(config)# mpls traffic-eng auto-tunnel primary config unnumbered ethernet1/0` | 明示アドレスを使用せずに、指定したインターフェイスでの IP 処理をイネーブルにします。 |
| ステップ 7 | **mplstraffic-engauto-tunnelprimaryconfigmplsip**<br><br>例：<br><br>`Router(config)# mpls traffic-eng auto-tunnel primary config mpls ip` | プライマリ自動トンネルで LDP をイネーブルにします。 |

# MPLS トラフィック エンジニアリング：自動トンネル プライマリおよびバックアップの設定例

## 高速リルートが可能な TE LSP を保護するため MPLS バックアップ自動トンネルを確立する：例

（注） 自動トンネリングではバックアップ トンネルを作成できないため、この例には **mpls traffic-eng auto-tunnel backup nhop-only** コマンドが含まれていません。

バックアップ トンネルが存在するかどうかを調べるには、**show ip rsvp fast-reroute** コマンドを入力します。この例は、スタティックに設定されたプライマリ トンネルが存在し、バックアップ トンネルは存在しないことを示しています。

```
Router(config)# show ip rsvp fast-reroute
Primary     Protect   BW         Backup
Tunnel      I/F       BPS:Type   Tunnel:Label  State  Level   Type
------      -------   -------    ------------  ------ -----   ----
R3-PRP_t0   PO3/1     0:G        None          None   None
```

次のコマンドでは、自動トンネルで NHOP および NNHOP バックアップ トンネルが自動的に設定されるようにします。

```
Router(config)# mpls traffic-eng auto-tunnel backup
```

**show ip interface brief** コマンドの出力に示すように、自動トンネリングによってトンネル ID 65436 および 65437 の 2 つのバックアップ トンネルが作成されています。

```
Router# show ip interface brief

Interface              IP-Address      OK? Method Status                Protocol
POS2/0                 10.0.0.14       YES NVRAM  down                  down
POS2/1                 10.0.0.49       YES NVRAM  up                    up
POS2/2                 10.0.0.45       YES NVRAM  up                    up
POS2/3                 10.0.0.57       YES NVRAM  administratively down down
POS3/0                 10.0.0.18       YES NVRAM  down                  down
POS3/1                 10.0.0.33       YES NVRAM  up                    up
POS3/2                 unassigned      YES NVRAM  administratively down down
POS3/3                 unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0     10.0.0.37       YES NVRAM  up                    up
GigabitEthernet4/1     unassigned      YES NVRAM  administratively down down
GigabitEthernet4/2     unassigned      YES NVRAM  administratively down down
Loopback0              10.0.3.1        YES NVRAM  up                    up
Tunnel0                10.0.3.1        YES unset  up                    up
Tunnel65436            10.0.3.1        YES unset  up                    up
Tunnel65437            10.0.3.1        YES unset  up                    up
Ethernet0              10.3.38.3       YES NVRAM  up                    up
Ethernet1              unassigned      YES NVRAM  administratively down down
R3-PRP#
```

次のコマンドでは、自動トンネリングで NNHOP バックアップ トンネルが作成されないようにします。

```
Router# mpls traffic-eng auto-tunnel backup nhop-only
```

次の **show ip rsvp fast-reroute** コマンドの [Type] フィールドは、NHOP トンネルだけが存在することを示しています。

```
Router# show ip rsvp fast-reroute

Primary    Protect  BW Backup
Tunnel     I/F      BPS:Type  Tunnel:Label  State  Level   Type
------     -------  --------  ------------- ------ ------- ----
R3-PRP_t0  PO3/1    0:G       Tu65436:24    Ready  any-unl Nhop
```

次のコマンドでは、最小トンネルインターフェイス番号と最大トンネルインターフェイス番号をそれぞれ 1000 と 1100 に変更します。

```
Router# mpls traffic-eng auto-tunnel backup tunnel-num min 1000 max 1100
```

**show ip rsvp fast-reroute** コマンドと **show ip interface brief** コマンドを入力することによって、ID 番号と自動トンネル バックアップ範囲 ID を確認できます。この例では、1 つのバックアップ トンネルだけがプライマリ トンネルを保護しています。

```
Router# show ip rsvp fast-reroute

Primary                   Protect BW         Backup
Tunnel                    I/F     BPS:Type   Tunnel:Label  State  Level   Type
------                    ------- --------   ------------- ------ -----   ------
R3-PRP_t0                 PO3/1   0:G        Tu1000:24     Ready  any-unl Nhop
Router# show ip interface brief
Interface            IP-Address    OK?  Method  Status                  Protocol
POS2/0               10.0.0.14     YES  NVRAM   down                    down
POS2/1               10.0.0.49     YES  NVRAM   up                      up
POS2/2               10.0.0.45     YES  NVRAM   up                      up
POS2/3               10.0.0.57     YES  NVRAM   administratively down   down
POS3/0               10.0.0.18     YES  NVRAM   down                    down
POS3/1               10.0.0.33     YES  NVRAM   up                      up
POS3/2               unassigned    YES  NVRAM   administratively down   down
POS3/3               unassigned    YES  NVRAM   administratively down   down
GigabitEthernet4/0   10.0.0.37     YES  NVRAM   up                      up
GigabitEthernet4/1   unassigned    YES  NVRAM   administratively down   down
GigabitEthernet4/2   unassigned    YES  NVRAM   administratively down   down
Loopback0            10.0.3.1      YES  NVRAM   up                      up
Tunnel0              10.0.3.1      YES  unset   up                      up
Tunnel65436          10.0.3.1      YES  unset   up                      up
Ethernet0            10.3.38.3     YES  NVRAM   up                      up
Ethernet1            unassigned    YES  NVRAM   administratively down   down
```

自動トンネル バックアップ トンネルのデフォルト トンネル範囲は 65,436 ～ 65,535 です。次の **show ip rsvp fast-reroute** コマンドでは、トンネル範囲 ID を変更します。

```
Router# show ip rsvp fast-reroute

Primary     Protect  BW         Backup
Tunnel       I/F     BPS:Type   Tunnel:Label   State   Level    Type
------      -------  --------   ------------- ------   -----    ------
R3-PRP_t0   PO3/1    0:G        Tu1001:0       Ready   any-unl  N-Nhop
```

結果を表示するには、**show ip interface brief** コマンドを使用します。

```
Router# show ip interface
Router# show ip interface brief

Interface              UP-Address   OK?  Method  Status                  Protocol
POS2/0                 10.0.0.14    YES  NVRAM   down                    down
POS2/1                 10.0.0.49    YES  NVRAM   up                      up
POS2/2                 10.0.0.45    YES  NVRAM   up                      up
POS2/3                 10.0.0.57    YES  NVRAM   up                      up
POS3/0                 10.0.0.18    YES  NVRAM   up                      up
POS3/1                 10.0.0.33    YES  NVRAM   up                      up
POS3/2                 unassigned   YES  NVRAM   administratively down   down
```

```
POS3/3                 unassigned   YES  NVRAM   administratively down  down
Loopback0              10.0.3.1     YES  NVRAM   up                    up
Tunnel0                10.0.3.1     YES  unset   up                    up
Tunnel1000             10.0.3.1     YES  unset   up                    up
Tunnel1001             10.0.3.1     YES  unset   up                    up
Ethernet0              10.3.38.3    YES  NVRAM   up                    up
Ethernet1              unassigned   YES  NVRAM   administratively down  down
```

次の **mpls traffic-eng auto-tunnel backup timers removal unused** コマンドでは、タイマーで 50 秒間隔でバックアップ自動トンネルをスキャンし、使用されていないトンネルを削除するように指定します。

```
Router(config)# mpls traffic-eng auto-tunnel backup timers removal unused 50
```

次の **mpls traffic-eng auto-tunnel backup config unnumbered-interface** コマンドでは、POS インターフェイス 3/1 での IP 処理を有効にします。

```
Router(config)# mpls traffic-eng auto-tunnel backup config unnumbered-interface POS3/1
```

POS3/1 で IP 処理が有効になっていることを確認するには、**show interfaces tunnel** コマンドを入力します。

```
Router# show interfaces tunnel 1001
Tunnel1001 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered.  Using address of POS3/1 (10.0.0.33)
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.0.0, destination 10.0.5.1
  Tunnel protocol/transport Label Switching, sequencing disabled
  Key disabled
  Checksumming of packets disabled
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

次の **mpls traffic-eng auto-tunnel backup config affinity** コマンドは、ダイナミックに作成されたバックアップ トンネルの計算時に役立つアフィニティとリンク属性を指定します。

Router(config)# **mpls traffic-eng auto-tunnel backup config affinity 0x22 mask 0x22**

ダイナミックに作成されたバックアップ トンネルに割り当てられたアフィニティとリンク属性を表示するには、**how mpls traffic-eng auto-tunnel backup** コマンドを入力します。

```
Router# show mpls traffic-eng auto-tunnel backup

State: Enabled
  Tunnel Count: 3 (up:2, down: 1)
  Tunnel ID Range: 65436-65535
  Create Nhop only: Yes
  SRLG: Not configured
  Delete unused tunnels after: 50 Seconds
  Config:
    Unnumbered i/f: Looback0
    Affinity: 0x22/0x22
```

# ネイバーへの MPLS 1 ホップ トンネルの確立：例

自動トンネリングによってすべてのネクストホップへのプライマリ トンネルを自動的に作成する場合、次のコマンドを入力する必要があります。

```
Router(config)# mpls traffic-eng auto-tunnel primary onehop
```

この例では、4 つのプライマリ トンネルが存在し、バックアップ トンネルは存在しません。その設定を確認するには、**show ip rsvp fast-reroute** コマンドと **show ip interface brief** コマンドを入力します。

```
Router# show ip rsvp fast-reroute
Primary                    Protect BW         Backup
Tunnel                     I/F     BPS:Type   Tunnel:Label  State  Level   Type
------                     ------- --------   ------------- ------ -----   ------
R3-PRP_t65337              PO2/2   0:G        None          None   None
R3-PRP_t65338              PO3/1   0:G        None          None   None
R3-PRP_t65339              Gi4/0   0:G        None          None   None
R3-PRP_t65336              PO2/1   0:G        None          None   None
Router# show ip interface brief
Interface              IP-Address    OK?  Method Status                Protocol
POS2/0                 10.0.0.14     YES  NVRAM  down                  down
POS2/1                 10.0.0.49     YES  NVRAM  up                    up
POS2/2                 10.0.0.45     YES  NVRAM  up                    up
POS2/3                 10.0.0.57     YES  NVRAM  administratively down  down
POS3/0                 10.0.0.18     YES  NVRAM  down                  down
POS3/1                 10.0.0.33     YES  NVRAM  up                    up
POS3/2                 unassigned    YES  NVRAM  administratively down  down
POS3/3                 unassigned    YES  NVRAM  administratively down  down
GigabitEthernet4/0     10.0.0.37     YES  NVRAM  up                    up
GigabitEthernet4/1     unassigned    YES  NVRAM  administratively down  down
GigabitEthernet4/2     unassigned    YES  NVRAM  administratively down  down
Loopback0              10.0.3.1      YES  NVRAM  up                    up
Tunnel0                10.0.3.1      YES  unset  administratively down  down
Tunnel65336            10.0.3.1      YES  unset  up                    up
Tunnel65337            10.0.3.1      YES  unset  up                    up
Tunnel65338            10.0.3.1      YES  unset  up                    up
Tunnel65339            10.0.3.1      YES  unset  up                    up
Ethernet0              10.3.38.3     YES  NVRAM  up                    up
Ethernet1              unassigned    YES  NVRAM  administratively down  down
R3-PRP#
```

プライマリ自動トンネルのデフォルト トンネル範囲は 65,336 ～ 65,435 です。次の **mpls traffic-eng auto-tunnel primary tunnel-num** コマンドでは、範囲を 2000 ～ 2100 に変更します。

```
Router(config)# mpls traffic-eng auto-tunnel primary tunnel-num min 2000 max 2100
```

次の **show ip rsvp fast-reroute** コマンドと **show ip interface brief** コマンドの出力例は、トンネル ID が 2000、2001、2002、および 2003 であることを示しています。

```
Router# show ip rsvp fast-reroute
Primary                    Protect BW         Backup
Tunnel                     I/F     BPS:Type   Tunnel:Label  State  Level   Type
------                     ------- --------   ------------- ------ -----   ------
R3-PRP_t2001               PO2/2   0:G        None          None   None
R3-PRP_t2002               PO3/1   0:G        None          None   None
R3-PRP_t2003               Gi4/0   0:G        None          None   None
R3-PRP_t2000               PO2/1   0:G        None          None   None
Router# show ip interface brief

Interface              IP-Address      OK? Method Status                Protocol
POS2/0                 10.0.0.14       YES NVRAM  down                  down
POS2/1                 10.0.0.49       YES NVRAM  up                    up
POS2/2                 10.0.0.45       YES NVRAM  up                    up
POS2/3                 10.0.0.57       YES NVRAM  administratively down down
```

```
POS3/0                 10.0.0.18       YES NVRAM  down                  down
POS3/1                 10.0.0.33       YES NVRAM  up                    up
POS3/2                 unassigned      YES NVRAM  administratively down down
POS3/3                 unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0     10.0.0.37       YES NVRAM  up                    up
GigabitEthernet4/1     unassigned      YES NVRAM  administratively down down
GigabitEthernet4/2     unassigned      YES NVRAM  administratively down down
Loopback0              10.0.3.1        YES NVRAM  up                    up
Tunnel0                10.0.3.1        YES unset  administratively down down
Tunnel2000             10.0.3.1        YES unset  up                    up
Tunnel2001             10.0.3.1        YES unset  up                    up
Tunnel2002             10.0.3.1        YES unset  up                    up
Tunnel2003             10.0.3.1        YES unset  up                    up
Ethernet0              10.3.38.3 '     YES NVRAM  up                    up
Ethernet1              unassigned      YES NVRAM  administratively down down
```

次の **mpls traffic-eng auto-tunnel primary timers** コマンドでは、タイマーで 50 秒間隔でバックアップ自動トンネルをスキャンし、使用されていないトンネルを削除するように指定します。

```
Router(config)# mpls traffic-eng auto-tunnel primary timers removal rerouted 50
```

次の **mpls traffic-eng auto-tunnel primary config unnumbered** コマンドでは、POS インターフェイス 3/1 での IP 処理を有効にします。

```
Router(config)# mpls traffic-eng auto-tunnel primary config unnumbered POS3/1
```

自動トンネリングによってすべてのプライマリ自動トンネルを削除し、再作成するには、次のコマンドを入力します。

```
Router(config)# clear mpls traffic-eng auto-tunnel primary
```

# その他の参考資料

ここでは、MPLS トラフィック エンジニアリング - 自動トンネル プライマリおよびバックアップ機能に関する関連資料について説明します。

### その他の参考資料

| 関連項目 | マニュアル タイトル |
|---|---|
| バックアップ トンネル | 『MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)』 |
| リンク保護 | 『MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)』 |
| MPLS トラフィック エンジニアリング コマンド | 『*Cisco IOS Multiprotocol Label Switching Command Reference*』 |
| SSO | 『*Cisco IOS High Availability Configuration Guide*』 |

### 標準

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

### MIB

| MIB | MIB のリンク |
|---|---|
| この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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。<br>http://www.cisco.com/go/mibs |

### RFC

| RFC | Title |
|---|---|
| この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC の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 | Link |
|---|---|
| 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。<br>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。<br>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/en/US/support/index.html |

# MPLS トラフィック エンジニアリング：自動トンネル プライマリおよびバックアップに関する機能情報

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

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

表 *7*：*MPLS* トラフィック エンジニアリング：自動トンネル プライマリおよびバックアップに関する機能情報

| 機能名 | リリース | 機能の設定情報 |
|---|---|---|
| MPLS トラフィック エンジニアリング：自動トンネル プライマリおよびバックアップ | 12.0(27)S<br>12.2(33)SRA<br>12.2(33)SXH<br>12.4(20)T<br>12.2(33)SRE<br>15.1(1)S<br>Cisco IOS XE Release 2.3 | |

| 機能名 | リリース | 機能の設定情報 |
|---|---|---|
| | | MPLS トラフィック エンジニアリング：自動トンネル プライマリおよびバックアップ機能を使用すると、ルータがバックアップ トンネルをダイナミックに構築したり、MPLS TE トンネルが設定されているすべてのインターフェイスで 1 ホップ プライマリ トンネルをダイナミックに作成したりできるようになります。<br><br>この機能は、Cisco IOS Release 12.0(27)S で導入されました。<br><br>この機能は、Cisco IOS リリース 12.2(33)SRA で統合されました。<br><br>サポートは、Cisco IOS リリース 12.2(33)SXH で追加されました。<br><br>この機能は、Cisco IOS Release 12.4(20)T で統合されました。<br><br>この機能は、Cisco IOS リリース 12.2(33)SRE で統合されました。プライマリ 1 ホップ自動トンネルおよびバックアップ自動トンネルを使用するルータには、SSO 冗長性を設定できます。<br><br>Cisco IOS リリース 15.1(1)S では、ダイナミックに作成された MPLS TE バックアップ トンネルのアフィニティまたはマスクを指定できるよう、この機能は更新されました。<br><br>Cisco IOS XE Release 2.3 では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービスルータに実装されました。<br><br>コマンド **affinity**、**mpls traffic-eng auto-tunnel backup** |

| 機能名 | リリース | 機能の設定情報 |
|---|---|---|
| | | **config** と **show mpls traffic-eng auto-tunnel backup** が導入されました。 |
| MPLS TE 自動トンネル/自動メッシュと SSO との共存 | 15.2(1)T<br>Cisco IOS XE Release 3.5S | この機能は、Cisco IOS XE リリース3.5S で統合されました。<br>この機能は、Cisco IOS Release 15.2(1)T で統合されました。<br>（注） Cisco IOS リリース 15.2(2)S と Cisco IOS XE リリース 3.6S から、自動トンネル、自動メッシュ SSO 共存機能は MPLS TE 自動トンネル、および自動メッシュ機能の SSO サポートに置き換えられました。詳細については、新実装向けの『*MPLS High Availability Configuration Guide*』を参照してください。 |

# 用語集

**バックアップトンネル**：リンクまたはノードの障害発生時に他の（プライマリ）トンネルのトラフィックを保護するために使用される MPLS トラフィック エンジニアリング トンネル。

**出力ルータ**：パケットが発信されるネットワークのエッジにあるルータ。

**高速リルート**：高速リルート（FRR）はリンク障害およびノード障害から MPLS トラフィック エンジニアリング（TE）LSP を保護するためのメカニズム。障害ポイントで LSP をローカルに修復することによって、ヘッドエンドルータがエンドツーエンド LSP を確立してそれらを置き換えようとしたときにデータのフローを継続できるようになります。FRR は、障害が発生したリンクまたはノードをバイパスするバックアップ トンネルを介して再ルーティングすることによって、保護されている LSP をローカルに修復します。

**ホップ**：2 つのネットワーク ノード間（たとえば、2 つのルータ間）のデータ パケットの通路。

**インターフェイス**：ネットワーク接続。

**IPアドレス**：TCP/IPを使用するホストに割り当てられている32ビットアドレス。IPアドレスは、5つのクラス（A、B、C、D、またはE）の1つに属し、ピリオドで区切った4オクテットとして記述されます（ドット付き10進表記）。各アドレスはネットワーク番号、オプションのサブネットワーク番号、およびホスト番号で構成されます。ルーティングにはネットワーク番号とサブネットワーク番号を組み合わせて使用し、ネットワーク内またはサブネットワーク内の個別のホストのアドレス指定にはホスト番号を使用します。IP アドレスからのネットワーク情報とサブネットワーク情報の抽出には、サブネット マスクを使用します。

**IP明示パス**：IPアドレスのリスト。それぞれのIPアドレスは明示パス内のノードまたはリンクを表します。

**LDP**：Label Distribution Protocol（ラベル配布プロトコル）。パケットの転送に使用されるラベル（アドレス）をネゴシエーションするための、MPLS 対応ルータ間の標準プロトコル。

**リンク**：隣接するノード間のポイントツーポイント接続。

**LSP**：ラベルスイッチド パス。ラベル付きパケットが複数のホップを介して通過するパス。このパスは、入力 LSR から開始し、出力 LSR で終了します。

**LSR**：ラベル スイッチ ルータ。パケット内のラベル カプセル化の値に基づいて、パケットを転送するレイヤ 3 ルータ。

**MPLS**：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ネットワークを介してパケット（フレーム）を転送する方式。ネットワークのエッジにあるルータがパケットにラベルを適用できるようにします。ネットワーク コア内の ATM スイッチまたは既存のルータは、最小限のルックアップ オーバーヘッドでラベルに従ってパケットを切り替えることができます。

**ノード**：ネットワーク接続のエンドポイント、つまりネットワーク内の複数の回線に共通する接合部。複数のノードをリンクで相互接続することができます。これらのノードは、ネットワーク内のコントロール ポイントとなります。

**最後から 2 番めのルータ**：最後から 2 番めのルータ、つまり、出力ルータの直前にあるルータ。

**プライマリトンネル**：障害が発生した場合に LSP を高速リルートできる MPLS トンネル。

**ルータ**：1 つ以上のメトリックを使用して、ネットワーク トラフィックを転送すべき最適のパスを決定するネットワーク層装置。ルータは、ネットワーク層情報に基づいて、ネットワーク間でパケットを転送します。

**ルータ ID**：パケットを発信するルータを他のすべてのルータと一意に区別するために使用できる ID。たとえば、ルータのインターフェイスの 1 つの IP アドレスです。

**スケーラビリティ**：ネットワークの拡大に伴って、リソース使用量の程度がどれだけ迅速に増加するかを示すインジケータ。

**トラフィックエンジニアリング**：ネットワーク上で、標準的なルーティング方法が使用された場合に選択されるパスとは異なるパスを経由してトラフィックがルーティングされるようにするために使用する技術やプロセス。

第 5 章

# MPLS トラフィック エンジニアリング（TE）：パス保護

MPLS トラフィック エンジニアリング（TE）：パス保護機能は、マルチプロトコル ラベル スイッチング（MPLS）トラフィックエンジニアリング（TE）トンネルに対して、エンドツーエンドの障害回復メカニズム（完全なパス保護）を提供します。



## 機能情報の確認

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

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、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。

# MPLS トラフィック エンジニアリング（TE）：パス保護の前提条件

- ネットワークで MPLS-TE、Cisco Express Forwarding、および Intermediate System-to-Intermediate System（IS-IS）または Open Shortest Path First（OSPF）がサポートされることを確認してください。
- MPLS をイネーブルにします。
- ルータに TE を設定する。
- **tunnel mpls traffic-eng path-option** コマンドを使用し、プライマリ パス オプションを指定して TE トンネルを設定します。
- ルータが SSO をサポートする場合は、ルータ上でフル モードのリソース予約プロトコル（RSVP）グレースフル リスタートを設定します。
- ルータが SSO をサポートする場合は、NSF 動作に対して、デバイスで SSO を設定する必要があります。

# MPLS トラフィック エンジニアリング（TE）：パス保護の制約事項

- プライマリ パス オプションごとにセカンダリ パスが 1 つのみ存在できます。
- セカンダリ パスで Fast Reroute（FRR）フラグを使用したシグナリングは行われません。
- ダイナミックな冗長パスはサポートされません。
- ヘッドエンド ルータでは、パス保護によるリンクおよびノード保護を使用しないでください。
- 自動メッシュ トンネル テンプレートにはパス保護を設定しないでください。これは、宛先が異なっているため、同じパス オプションを使用して複数の宛先に到達できないからです。
- ロックダウン オプションは保護されたパス オプションではサポートされていません。
- トンネルでは、SSO のイベントの直後にはパス保護はまだ機能しません。1 つのラベル スイッチド パス（LSP）のみがチェックポイントされ、トンネル用に回復されます。パス保護 LSP は RSVP 高可用性（HA）回復が完了するまではシグナリングされません。

# MPLS トラフィック エンジニアリング（TE）：パス保護に関する情報

## トラフィック エンジニアリング トンネル

MPLS TE を使用すると、ネットワーク全体にラベル スイッチド パス（LSP）を構築してトラフィックを転送できます。

（TE トンネルとも呼ばれる）MPLS TE LSP を使用すると、TE トンネルのヘッドエンドによって、そのトラフィックが特定の宛先に到達するために使用するパスを制御できます。この方式は、宛先アドレスだけに基づいてトラフィックを転送する方式よりも柔軟性が高くなります。

トンネルの重要性には差があります。たとえば、VoIP トラフィックを伝送するトンネルと、データ トラフィックを伝送するトンネルが、同じリソースに対して競合する場合があります。MPLS TE を使用すると、一部のトンネルが他のトンネルをプリエンプトするように設定できます。各トンネルにはプライオリティがあり、重要性の高いトンネルが重要性の低いトンネルよりも優先されます。

## パス保護

パス保護では、MPLS TE トンネルに対してエンドツーエンドの障害回復メカニズム（完全なパス保護）を提供します。セカンダリ LSP をあらかじめ確立しておくと、トンネルの TE トラフィックを伝送する保護 LSP を障害から保護できます。保護された LSP に障害がある場合、ヘッドエンド ルータは、トンネルのトラフィックを一時的に伝送するセカンダリ LSP をすぐに有効にします。セカンダリ LSP で障害が発生した場合は、セカンダリ パスの障害がクリアされるまでトンネルのパス保護は機能しなくなります。パス保護を使用できるのは、単一のエリア（OSPF や IS-IS）または Inter-AS（Border Gateway Protocol（BGP）、external BGP（eBGP）、およびスタティック）です。

セカンダリ トンネルへのスイッチオーバーをトリガーする障害検出メカニズムには、次のものがあります。

- リソース予約プロトコル（RSVP）シグナリングからの Path Error または Resv-Tear
- RSVP Hello から、ネイバーが失われたという通知を受信した場合
- 双方向フォワーディング検出（BFD）プロトコルから、ネイバーが失われたという通知を受信した場合
- Interior Gateway Protocol（IGP）から、隣接が停止したという通知を受信した場合
- プライオリティの高い LSP にシグナリングするためのプリエンプションによって発生する保護トンネルの LSP のローカル ティアダウン、Packet over SONET（POS）アラーム、活性挿抜（OIR）などの場合

この他の回復メカニズムには高速再ルーティング（FRR）があります。これは、障害ポイントで LSP をローカルに修復し、リンクおよびノードの障害から MPLS TE LSP だけを保護するメカニズムです。

リンクまたはノードの保護ほど高速ではありませんが、セカンダリ プライマリ パス オプションを設定したり、トンネルのヘッドエンド ルータでダイナミックにパスを再計算したりするよりも、セカンダリ LSP にプリシグナリングする方が高速です。実際の回復時間はトポロジによって異なります。また、伝搬遅延やスイッチ ファブリックの遅延などの遅延要素の影響も受けます。

# 拡張されたパス保護

拡張されたパス保護では、プライマリ パス オプション単位で複数のバックアップ パス オプションをサポートします。特定のプライマリ パス オプションに対して、最大 8 つのバックアップ パス オプションを設定できます。常にアクティブにシグナリングされるのは、設定済みバックアップ パス オプションのうちの 1 つだけです。

**mpls traffic-eng path-option list** コマンドを入力したあとに、**path-option** コマンドの *number* 引数にバックアップ パス優先度を入力できます。ID が小さいほど優先度は高くなります。優先度は、バックアップ パス オプションごとに設定できます。複数のバックアップ パス オプションと単一のバックアップ パス オプションを同時に設定して、プライマリ パス オプションを保護することはできません。

# ISSU

Cisco ISSU プロセスを使用すれば、システムによるパケット転送を中断することなく、Cisco IOS XE ソフトウェアのアップグレードまたはダウングレードを実行することができます。ISSU では、Cisco IOS XE のハイ アベイラビリティ インフラストラクチャ（SSO およびハードウェア冗長性を備えた Cisco NSF）を活用して、システムを稼働させたまま変更することで、ソフトウェアのアップグレードやバージョンの変更の際のダウンタイムがなくなります。これにより、計画的なメンテナンス作業がネットワーク サービスのアベイラビリティに与える影響が小さくなります。つまり、ダウンタイムが短縮され、重要なシステムへのアクセスが改善されます。

パス保護がイネーブルになっている場合に ISSU アップグレードが実行されると、パス保護のパフォーマンスは他の TE 機能のパフォーマンスと同等になります。

# NSF/SSO

Cisco NSF with SSO を使用すると、ネットワーク プロセッサのハードウェアまたはソフトウェアに障害が発生した場合でも、継続してパケットを転送できます。

SSO は、ルート プロセッサ（RP）の 1 つをアクティブ プロセッサとして確立する一方でもう 1 つの RP をセカンダリ プロセッサとして指定してから重要なステート情報を両者間で同期させることによって、ネットワークの可用性を向上できる RP の冗長性を活用します。2 つのプロセッサの初回同期後、SSO はこれらの間の RP ステート情報をダイナミックに維持します。アクティブ RP に障害が発生したとき、アクティブ RP がネットワーキング デバイスから削除されたとき、ま

たはメンテナンスのために手動で停止されたときに、アクティブプロセッサからセカンダリ プロセッサへのスイッチオーバーが発生します。

Cisco NSF は、SSO と連動して、スイッチオーバー後にユーザがネットワークを使用できない時間を最小限に抑えます。NSF の主な目的は、RP のスイッチオーバー後に、継続的に IP パケットを転送することです。Cisco NSF は、SSO 対応のデバイスにおけるルーティング フラップを抑止することによって、ネットワークの安定性を保ちます。

MPLS トラフィック エンジニアリング：パス保護機能は SSO 後に通常の状態に戻ります。パス保護用に設定されたトンネルには、同時にシグナリングされた 2 つの LSP が存在する場合があります。このうち、プライマリ LSP はトラフィックを伝送し、セカンダリ LSP はプライマリ パスで障害が発生した場合にトラフィックを伝送します。スタンバイ RP に同期されるのは、これらの LSP のうちで現在トラフィックを伝送中の LSP に関連する情報だけです。スタンバイ RP は、チェックポイントで記録された情報から、LSP がプライマリかセカンダリかを回復時に判断します。

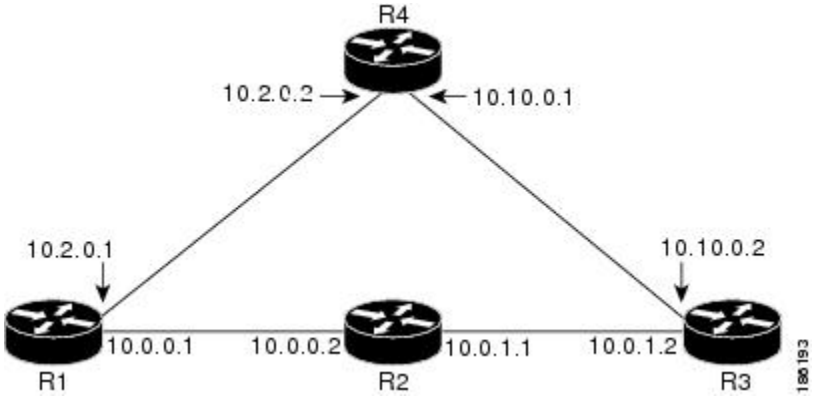
スイッチオーバー時にプライマリ LSP がアクティブだった場合は、プライマリ LSP だけが回復されます。シグナリングされてパス保護を提供したセカンダリ LSP は、TE 回復期間が完了したあとに再びシグナリングされます。セカンダリ LSP はトラフィックを伝送していなかったため、このことはトンネル上のトラフィックに影響しません。

# MPLS トラフィック エンジニアリング（TE）：パス保護の設定方法

## 標準パス保護の設定作業

ここでは、次の作業について説明します（下の図を参照）。

**図 *19*：ネットワーク トポロジ：パス保護**



## セカンダリ パス用の明示パスの設定

プライマリ パスに関連付けられた共通のリンクまたはノードが停止した場合に、これらのリンクまたはノードを含まないセカンダリ パスを指定するには、次の手順を実行して明示パスを設定します。

### 手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipexplicit-path** {**name** *path-name*| **identifier** *number*} [**enable** | **disable**]
4. **index***indexcommandip-address*
5. **exit**
6. **exit**

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **ipexplicit-path** {**name** *path-name*| **identifier** *number*} [**enable** | **disable**]<br><br>例：<br><br>`Router(config)# ip explicit-path name path3441 enable` | 明示パスを作成または変更し、IP 明示パス コマンド モードを開始します。 |
| ステップ 4 | **index***indexcommandip-address*<br><br>例：<br><br>`Router(cfg-ip-exp1-path)# index 1 next-address 10.0.0.1` | 指定したインデックスでパス エントリを挿入または変更します。IP アドレスはノード ID を表します。<br><br>（注） このコマンドはルータごとに 1 回入力します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **exit**<br><br>例：<br>`Router(cfg-ip-exp1-path)# exit` | IP 明示パス コマンド モードを終了し、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 6 | **exit**<br><br>例：<br>`Router(config)# exit` | 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 モードを開始します。 |

## プライマリ パス オプションを保護するセカンダリ パス オプションの割り当て

パスでリンクまたはノードの障害が発生し、ネットワーク内のすべてのインターフェイスが保護されなくなった場合のためにセカンダリ パス オプションを割り当てます。

### 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **tunnelmplstraffic-engpath-optionprotect***number***explicit** {**name** *path-name* | **identifier** *path-number*} [**verbatim**] [**attributes** *string*] [**bandwidth** *kb/s*| **sub-pool** *kb/s*]
5. **exit**
6. **exit**

### 手順の詳細

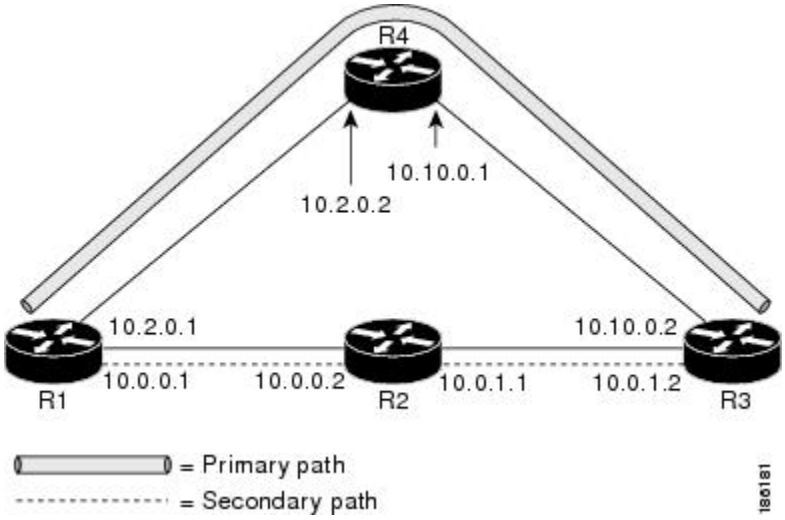
| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`Router# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **interfacetunnel***number*<br><br>例：<br><br>`Router(config)# interface tunnel500` | トンネルインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **tunnelmplstraffic-engpath-optionprotect***number***explicit** {**name** *path-name* \| **identifier** *path-number*} [**verbatim**] [**attributes** *string*] [**bandwidth** *kb/s*\| **sub-pool** *kb/s*]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option protect 10 explicit name path344` | MPLS TE トンネルにセカンダリ パス オプションを設定します。 |
| ステップ 5 | **exit**<br><br>例：<br><br>`Router(config-if)# exit` | インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 6 | **exit**<br><br>例：<br><br>`Router(config)# exit` | 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。 |

## MPLS トラフィック エンジニアリングのパス保護設定の確認

パス保護の設定を確認するには、次の手順を実行します。ステップ 1 と 2 では、次の図を参照してください。

図 *20*：ネットワーク トポロジの確認




### 手順の概要

1. **show running interface tunnel***tunnel-number*
2. **show mpls traffic-eng tunnels***tunnel-interface*
3. **show mpls traffic-eng tunnels***tunnel-interface* [**brief**] **protection**
4. **show ip rsvp high-availability database** {**hello** | **link-management** {**interfaces** | **system**} | **lsp** [**filter destination***ip-address*|**filter lsp-id***lsp-id*|**filter source***ip-address* | **filter tunnel-id***tunnel-id*] | **lsp-head** [**filter***number*] | **summary**}

### 手順の詳細

**ステップ 1** **show running interface tunnel***tunnel-number*

このコマンドは、プライマリ パスおよび保護パス オプションの設定を表示します。

（注） 両方の LSP（つまり、プライマリ パスと保護されたパス）のステータスを表示するには、**show mpls traffic-eng tunnels protection** コマンドを使用します。

例：

```
Router# show running interface tunnel500

Building configuration...
Current configuration : 497 bytes
!
interface Tunnel500
```

```
 ip unnumbered Loopback0
 tunnel destination 10.0.0.9
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 100
 tunnel mpls traffic-eng path-option 10 explicit name path344
 tunnel mpls traffic-eng path-option 20 explicit name path345
 tunnel mpls traffic-eng path-option protect 10 explicit name path3441
 tunnel mpls traffic-eng path-option protect 20 explicit name path348
end
```

**ステップ 2** **show mpls traffic-eng tunnels***tunnel-interface*

このコマンドは、トンネル パス情報を表示します。

[Common Link(s)] フィールドには、ヘッドエンド ルータからテールエンド ルータまでの、プライマリ パスとセカンダリ パスによって共有されるリンクの数が表示されます。

[Common Node(s)] フィールドには、ヘッドエンド ルータおよびテールエンド ルータを除く、プライマリ パスとセカンダリ パスによって共有されるノードの数が表示されます。

次の出力に示すとおり、共通のリンクまたはノードはありません。

例：

```
Router# show mpls traffic-eng tunnels tunnel500
Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
 Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
 Config Parameters:
  Bandwidth: 100 kb/s (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
 Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
 InLabel : -
 OutLabel : FastEthernet1/0/0, 16
 RSVP Signalling Info:
   Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 19
  RSVP Path Info:
   My Address: 10.2.0.1
   Explicit Route: 10.2.0.2  10.10.0.1  10.10.0.2  10.0.0.9
   Record Route: NONE
   Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
   Record Route: NONE
   Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
 Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.2.0.1  10.2.0.2  10.10.0.1  10.10.0.2  10.0.0.9
 History:
  Tunnel:
   Time since created: 11 minutes, 17 seconds
   Time since path change: 8 minutes, 5 seconds
   Number of LSP IDs (Tun_Instances) used: 19
  Current LSP:
   Uptime: 8 minutes, 5 seconds
```

**ステップ 3** **show mpls traffic-eng tunnels***tunnel-interface* [**brief**] **protection**

このコマンドを **protection** キーワードを指定して使用すると、両 LSP（プライマリ パスと保護されたパス）のステータスが表示されます。

（注） プライマリ パス オプションの削除は、リンクのシャット ダウンと同じ結果になります。トラフィックは、使用中の保護されたパスを通過するようになります。

次に、プライマリ LSP が稼働中であり、セカンダリ LSP も稼働して保護を実行中であることを示すコマンド出力例を示します。

例：

```
Router# show mpls traffic-eng tunnels tunnel500 protection
R1_t500
 LSP Head, Tunnel500, Admin: up, Oper: up
 Src 10.1.1.1, Dest 10.0.0.9, Instance 19
 Fast Reroute Protection: None
 Path Protection: 0 Common Link(s), 0 Common Node(s)
  Primary lsp path:10.2.0.1  10.2.0.2
                   10.10.0.1 10.10.0.2
                   10.0.0.9
  Protect lsp path:10.0.0.1  10.0.0.2
                   10.0.1.1  10.0.1.2
                   10.0.0.9
  Path Protect Parameters:
   Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
   Metric Type: TE (default)
  InLabel : -
  OutLabel : FastEthernet0/0/0, 16
  RSVP Signalling Info:
    Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 27
   RSVP Path Info:
    My Address: 10.0.0.1
    Explicit Route: 10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
   RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
```

次に、プライマリ LSP が稼働中であり、セカンダリ LSP も稼働してトラフィック伝送がアクティブであることを示すコマンド出力例を示します。

例：

```
Router# show mpls traffic-eng tunnels tunnel500 protection
R1_t500
 LSP Head, Tunnel500, Admin: up, Oper: up
 Src 10.1.1.1, Dest 10.0.0.9, Instance 27
 Fast Reroute Protection: None
 Path Protection: Backup lsp in use.
```

**ステップ 4** **show ip rsvp high-availability database** {**hello** | **link-management** {**interfaces** | **system**} | **lsp** [**filter destination***ip-address*|**filter lsp-id***lsp-id*|**filter source***ip-address* | **filter tunnel-id***tunnel-id*] | **lsp-head** [**filter***number*] | **summary**}

**show ip rsvp high-availability database** コマンドを実行すると、TE で使用される RSVP ハイ アベイラビリティ（HA）の読み取りおよび書き込み用データベースの内容が表示されます。**lsp-head** キーワードを指定すると、コマンド出力にパス保護情報が表示されます。

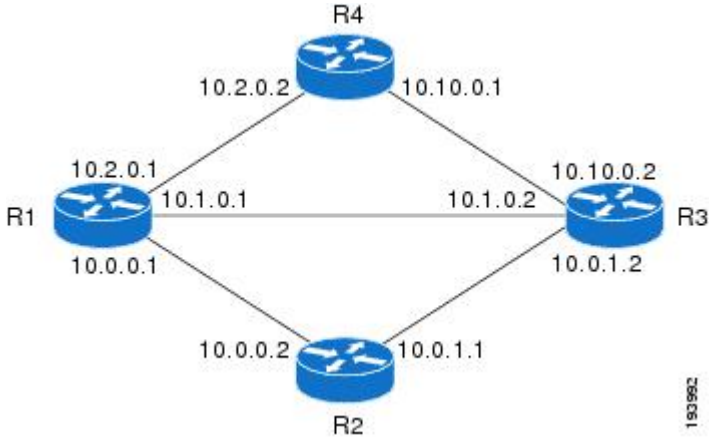
例：

```
Router# show ip rsvp high-availability database lsp-head
LSP_HEAD WRITE DB
 Tun ID: 500
 Header:
  State: Checkpointed  Action: Add
  Seq #: 3             Flags:  0x0
 Data:
  lsp_id: 5, bandwidth: 100, thead_flags: 0x1, popt: 1
  feature_flags: path protection active
  output_if_num: 5, output_nhop: 10,0,0,1
  RRR path setup info
   Destination: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf) flag:0x0
   IGP: ospf, IGP area: 0, Number of hops: 5, metric: 2
   Hop 0: 10.0.0.1, Id: 10.0.0.1 Router Node (ospf), flag:0x0
   Hop 1: 10.0.0.2, Id: 10.0.0.7 Router Node (ospf), flag:0x0
   Hop 2: 10.0.1.1, Id: 10.0.0.7 Router Node (ospf), flag:0x0
   Hop 3: 10.0.1.2, Id: 10.0.0.9 Router Node (ospf), flag:0x0
   Hop 4: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf), flag:0x0
```

# 拡張されたパス保護の設定作業

ここでは、次の作業について説明します（下の図を参照）。

図 *21*：拡張されたパス保護のネットワーク トポロジ




## パス オプション リストの作成

プライマリ パス オプションにバックアップ パスのパス オプション リストを作成するには、次の作業を実行します。

（注） 代わりにセカンダリ パスを使用する場合は、「セカンダリ パス用の明示パスの設定」セクションの手順を実行します。

## 手順の概要

1. イネーブル化
2. **configure terminal**
3. **mpls traffic-eng path-option list** [**name***pathlist-name* | **identifier***pathlist-number*]
4. **path-option***number***explicit** [**name***pathoption-name* | **identifier***pathoption-number*]
5. リスト
6. **no** [*pathoption-name* | *pathoption-number*]
7. **exit**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• 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**<br><br>例：<br><br>`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 | **mpls traffic-eng path-option list** [**name***pathlist-name* \| **identifier***pathlist-number*]<br><br>例：<br><br>`Router(config)# mpls traffic-eng path-option list name pathlist-01` | パス オプション リストを設定し、パス オプション リスト コンフィギュレーション モードを開始します。<br><br>• 入力できるコマンドは、**path-option**、**list**、**no** および **exit** です。 |
| ステップ 4 | **path-option***number***explicit** [**name***pathoption-name* \| **identifier***pathoption-number*]<br><br>例：<br><br>`Router(cfg-pathoption-list)# path-option 10 explicit identifier 200` | （任意）追加、編集、または削除するパス オプションの名前または ID 番号を指定します。*pathoption-number* 値の範囲は 1 ～ 65535 です。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | リスト<br><br>例：<br>`Router(cfg-pathoption-list)# list` | （任意）パス オプションをすべて表示します。 |
| ステップ 6 | **no** [*pathoption-name* \| *pathoption-number*]<br><br>例：<br>`Router(cfg-pathoption-list)# no 10` | （任意）指定されたパス オプションを削除します。 |
| ステップ 7 | **exit**<br><br>例：<br>`Router(cfg-pathoption-list)# exit` | （任意）パスオプション リスト コンフィギュレーション モードを終了し、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。 |

## プライマリ パス オプションを保護するパス オプション リストの割り当て

パスでリンクまたはノードの障害が発生し、ネットワーク内のすべてのインターフェイスが保護されなくなった場合のためにパス オプション リストを割り当てます。上の 3 番めの図を参照してください。

### 手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface tunnel***number*
4. **tunnel mpls traffic-eng path-option protect***number* [**attributes***lsp-attributes* | **bandwidth** {*kbps* | **subpool***kbps*} | **explicit** {**identifier***path-number* | **name***path-name*} | **list** {*pathlist-name***name** | **identifier***pathlist-identifier*}]
5. **exit**

### 手順の詳細

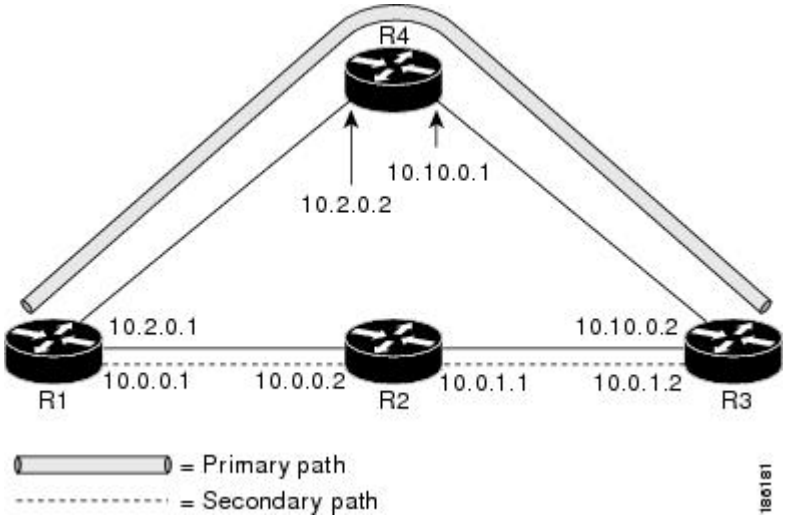
| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configure terminal**<br><br>例：<br>`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 tunnel***number*<br><br>例：<br>`Router(config)# interface tunnel500` | トンネルインターフェイスを設定し、インターフェイスコンフィギュレーションモードを開始します。 |
| ステップ 4 | **tunnel mpls traffic-eng path-option protect***number* [**attributes***lsp-attributes* \| **bandwidth** {*kbps* \| **subpool***kbps*} \| **explicit** {**identifier***path-number* \| **name***path-name*} \| **list** {*pathlist-name***name** \| **identifier***pathlist-identifier*}]<br><br>例：<br>`Router(config-if)# tunnel mpls traffic-eng path-option protect 10 list name pathlist-01` | プライマリ パス オプション 10 を保護するパス オプション リストを設定します。 |
| ステップ 5 | **exit**<br><br>例：<br>`Router(config-if)# exit` | （任意）インターフェイス コンフィギュレーション モードを終了し、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。 |

## MPLS トラフィック エンジニアリングのパス保護設定の確認

パス保護の設定を確認するには、次の手順を実行します。ステップ 1 と 2 では、次の図を参照してください。

図 *22*：ネットワーク トポロジの確認




### 手順の概要

1. **show running interface tunnel***tunnel-number*
2. **show mpls traffic-eng tunnels***tunnel-interface*
3. **show mpls traffic-eng tunnels***tunnel-interface* [**brief**] **protection**
4. **show ip rsvp high-availability database** {**hello** | **link-management** {**interfaces** | **system**} | **lsp** [**filter destination***ip-address*|**filter lsp-id***lsp-id*|**filter source***ip-address* | **filter tunnel-id***tunnel-id*] | **lsp-head** [**filter***number*] | **summary**}

### 手順の詳細

**ステップ 1** **show running interface tunnel***tunnel-number*

このコマンドは、プライマリ パスおよび保護パス オプションの設定を表示します。

（注） 両方の LSP（つまり、プライマリ パスと保護されたパス）のステータスを表示するには、**show mpls traffic-eng tunnels protection** コマンドを使用します。

例：

```
Router# show running interface tunnel500

Building configuration...
Current configuration : 497 bytes
!
interface Tunnel500
```

```
 ip unnumbered Loopback0
 tunnel destination 10.0.0.9
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 100
 tunnel mpls traffic-eng path-option 10 explicit name path344
 tunnel mpls traffic-eng path-option 20 explicit name path345
 tunnel mpls traffic-eng path-option protect 10 explicit name path3441
 tunnel mpls traffic-eng path-option protect 20 explicit name path348
end
```

**ステップ 2** **show mpls traffic-eng tunnels***tunnel-interface*

このコマンドは、トンネル パス情報を表示します。

[Common Link(s)] フィールドには、ヘッドエンド ルータからテールエンド ルータまでの、プライマリ パスとセカンダリ パスによって共有されるリンクの数が表示されます。

[Common Node(s)] フィールドには、ヘッドエンド ルータおよびテールエンド ルータを除く、プライマリ パスとセカンダリ パスによって共有されるノードの数が表示されます。

次の出力に示すとおり、共通のリンクまたはノードはありません。

例：

```
Router# show mpls traffic-eng tunnels tunnel500
Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
 Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
 Config Parameters:
  Bandwidth: 100 kb/s (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
 Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
 InLabel : -
 OutLabel : FastEthernet1/0/0, 16
 RSVP Signalling Info:
   Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 19
  RSVP Path Info:
   My Address: 10.2.0.1
   Explicit Route: 10.2.0.2  10.10.0.1  10.10.0.2  10.0.0.9
   Record Route: NONE
   Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
   Record Route: NONE
   Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
 Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.2.0.1  10.2.0.2  10.10.0.1  10.10.0.2  10.0.0.9
 History:
  Tunnel:
   Time since created: 11 minutes, 17 seconds
   Time since path change: 8 minutes, 5 seconds
   Number of LSP IDs (Tun_Instances) used: 19
  Current LSP:
   Uptime: 8 minutes, 5 seconds
```

**ステップ 3** **show mpls traffic-eng tunnels***tunnel-interface* **[brief] protection**

このコマンドを **protection** キーワードを指定して使用すると、両 LSP（プライマリ パスと保護されたパス）のステータスが表示されます。

（注） プライマリ パス オプションの削除は、リンクのシャット ダウンと同じ結果になります。トラフィックは、使用中の保護されたパスを通過するようになります。

次に、プライマリ LSP が稼働中であり、セカンダリ LSP も稼働して保護を実行中であることを示すコマンド出力例を示します。

例：

```
Router# show mpls traffic-eng tunnels tunnel500 protection
R1_t500
 LSP Head, Tunnel500, Admin: up, Oper: up
 Src 10.1.1.1, Dest 10.0.0.9, Instance 19
 Fast Reroute Protection: None
 Path Protection: 0 Common Link(s), 0 Common Node(s)
  Primary lsp path:10.2.0.1  10.2.0.2
                   10.10.0.1 10.10.0.2
                   10.0.0.9
  Protect lsp path:10.0.0.1  10.0.0.2
                   10.0.1.1  10.0.1.2
                   10.0.0.9
  Path Protect Parameters:
   Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
   Metric Type: TE (default)
  InLabel : -
  OutLabel : FastEthernet1/2/0, 16
  RSVP Signalling Info:
    Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 27
   RSVP Path Info:
    My Address: 10.0.0.1
    Explicit Route: 10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
   RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
```

次に、プライマリ LSP が稼働中であり、セカンダリ LSP も稼働してトラフィック伝送がアクティブであることを示すコマンド出力例を示します。

例：

```
Router# show mpls traffic-eng tunnels tunnel500 protection
R1_t500
 LSP Head, Tunnel500, Admin: up, Oper: up
 Src 10.1.1.1, Dest 10.0.0.9, Instance 27
 Fast Reroute Protection: None
 Path Protection: Backup lsp in use.
```

**ステップ 4** **show ip rsvp high-availability database** {**hello** | **link-management** {**interfaces** | **system**} | **lsp** [**filter destination***ip-address*|**filter lsp-id***lsp-id*|**filter source***ip-address* | **filter tunnel-id***tunnel-id*] | **lsp-head** [**filter***number*] | **summary**}

**show ip rsvp high-availability database** コマンドを実行すると、TE で使用される RSVP ハイ アベイラビリティ（HA）の読み取りおよび書き込み用データベースの内容が表示されます。**lsp-head** キーワードを指定すると、コマンド出力にパス保護情報が表示されます。

例：

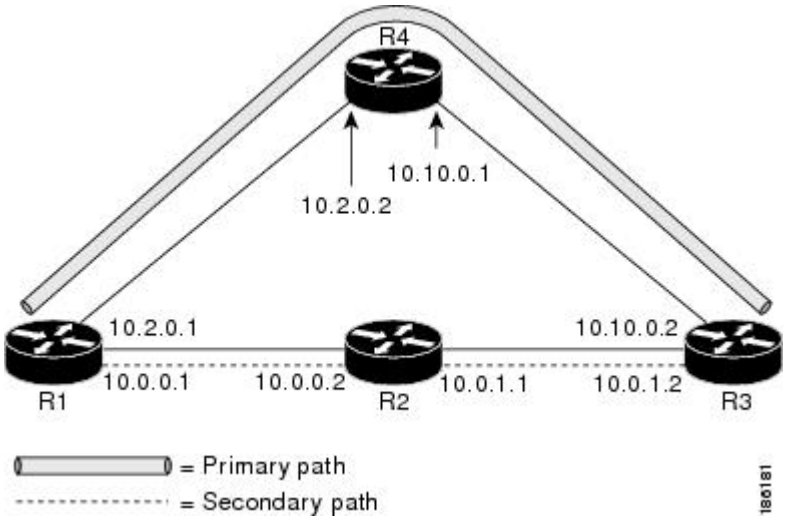
```
Router# show ip rsvp high-availability database lsp-head
LSP_HEAD WRITE DB
 Tun ID: 500
 Header:
  State: Checkpointed  Action: Add
  Seq #: 3             Flags:  0x0
 Data:
  lsp_id: 5, bandwidth: 100, thead_flags: 0x1, popt: 1
  feature_flags: path protection active
  output_if_num: 5, output_nhop: 10,0,0,1
  RRR path setup info
   Destination: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf) flag:0x0
   IGP: ospf, IGP area: 0, Number of hops: 5, metric: 2
   Hop 0: 10.0.0.1, Id: 10.0.0.1 Router Node (ospf), flag:0x0
   Hop 1: 10.0.0.2, Id: 10.0.0.7 Router Node (ospf), flag:0x0
   Hop 2: 10.0.1.1, Id: 10.0.0.7 Router Node (ospf), flag:0x0
   Hop 3: 10.0.1.2, Id: 10.0.0.9 Router Node (ospf), flag:0x0
   Hop 4: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf), flag:0x0
```

# MPLS トラフィック エンジニアリング（TE）：標準パス保護の設定例

## 例：セカンダリ パス用の明示パスの設定

次の図に、プライマリ パスおよびセカンダリ パスを示します。障害が発生すると、セカンダリ パスが使用されます。

図 *23*：プライマリ パスとセカンダリ パス




次の例では、明示パスの名前は path3441 です。**index** コマンドはルータごとに実行します。障害が発生すると、セカンダリ パスが使用されます。

```
Router(config)# ip explicit-path name path3441 enable
Router(cfg-ip-expl-path)# index 1 next 10.0.0.1
Explicit Path name path3441:
    1: next-address 10.0.0.1
Router(cfg-ip-expl-path)# index 2 next 10.0.0.2
Explicit Path name path3441:
    1: next-address 10.0.0.1
    2: next-address 10.0.0.2
Router(cfg-ip-expl-path)# index 3 next 10.0.1.1
Explicit Path name path3441:
    1: next-address 10.0.0.1
    2: next-address 10.0.0.2
    3: next-address 10.0.1.1
Router(cfg-ip-expl-path)# index 4 next 10.0.1.2
Explicit Path name path3441:
    1: next-address 10.0.0.1
    2: next-address 10.0.0.2
    3: next-address 10.0.1.1
    4: next-address 10.0.1.2
Router(cfg-ip-expl-path)# exit
```

# 例：プライマリ パス オプションを保護するセカンダリ パス オプションの割り当て

次の例では、トラフィック エンジニアリング トンネルが設定されています。

```
Router> enable
Router# configure terminal
Router(config-if)# interface tunnel500
Router(config-if)# tunnel mpls traffic-eng path-option protect 10 explicit name path344
```

次の **show running interface** コマンド出力は、パス保護が設定されていることを示しています。トンネル 500 には、（path344 を使用し、path3441 によって保護される）パス オプション 10、および（path345 を使用し、path348 によって保護される）パス オプション 20 が設定されています。

```
Router# show running interface tunnel500
Router# interface tunnel 500
Building configuration...
Current configuration : 497 bytes
!
interface Tunnel500
 ip unnumbered Loopback0
 tunnel destination 10.0.0.9
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 100
 tunnel mpls traffic-eng path-option 10 explicit name path344
 tunnel mpls traffic-eng path-option 20 explicit name path345
 tunnel mpls traffic-eng path-option protect 10 explicit name path3441
 tunnel mpls traffic-eng path-option protect 20 explicit name path348
end
```

# 例：パス保護の前後でのトンネルの設定

**show mpls traffic-eng tunnels** コマンドを実行すると、プライマリ（保護された）パスに関する情報が表示されます。次の出力例は、パス保護が設定されていることを示しています。

```
Router# show mpls traffic-eng tunnels tunnel500
Name: R1_t500   (Tunnel500)   Destination: 10.0.0.9
 Status:
  Admin: up  Oper: up  Path: valid  Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
 Config Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
 Active Path Option Parameters:
    State: explicit path option 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
 InLabel : -
 OutLabel : FastEthernet1/0/0, 16
 RSVP Signalling Info:
   Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 43
  RSVP Path Info:
   My Address: 10.2.0.1
```

```
   Explicit Route: 10.2.0.2  10.10.0.1  10.10.0.2  10.0.0.9
   Record Route: NONE
   Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
   Record Route: NONE
   Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  Shortest Unconstrained Path Info:
   Path Weight: 20 (TE)
   Explicit Route: 10.0.0.1  10.0.0.2  10.0.1.1  10.0.1.2
                   10.0.0.9
 History:
  Tunnel:
   Time since created: 18 minutes, 22 seconds
   Time since path change: 19 seconds
   Number of LSP IDs (Tun_Instances) used: 43
  Current LSP:
   Uptime: 22 seconds
   Selection: reoptimization
  Prior LSP:
   ID: path option 10 [27]
   Removal Trigger: reoptimization completed
```

次の **show mpls traffic-eng tunnels** コマンド出力は、セカンダリ パスに関する情報を示しています。Tunnel500 が保護されています。保護パスが使用されており、プライマリ パスが停止しています。コマンド出力は、プライマリ LSP およびセカンダリ LSP の IP 明示パスを示しています。

```
Router# show mpls traffic-eng tunnels tunnel500 protection

R1_t500
 LSP Head, Tunnel500, Admin: up, Oper: up
 Src 10.1.1.1, Dest 10.0.0.9, Instance 43
 Fast Reroute Protection: None
 Path Protection: 0 Common Link(s), 0 Common Node(s)
  Primary lsp path:10.2.0.1  10.2.0.2
                   10.10.0.1 10.10.0.2
                   10.0.0.9
  Protect lsp path:10.0.0.1  10.0.0.2
                   10.0.1.1  10.0.1.2
                   10.0.0.9
  Path Protect Parameters:
   Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
   Metric Type: TE (default)
  InLabel : -
  OutLabel : FastEthernet0/0/0, 17
  RSVP Signalling Info:
   Src 10.1.1.1,  Dst 10.0.0.9,  Tun_Id 500,  Tun_Instance 44
  RSVP Path Info:
   My Address: 10.0.0.1
   Explicit Route: 10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
   Record Route: NONE
   Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
   Record Route: NONE
   Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
R1#
```

次の **shutdown** コマンドを実行すると、パス保護を使用するインターフェイスがシャットダウンされます。

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet1/0/0
Router(config-if)# shutdown
Router(config-if)# end
Router#
```

次の **show mpls traffic-eng tunnels** コマンドは、保護パスが使用されており、プライマリ パスが停止していることを示しています。

```
Router# show mpls traffic-eng tunnels tunnel500
Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
 Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path option 10, type explicit path344
  path option 20, type explicit path345
  Path Protection: Backup lsp in use.
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
 Config Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
 Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
 InLabel : -
 OutLabel : FastEthernet0/0/0, 17
 RSVP Signalling Info:
   Src 10.1.1.1,  Dst 10.0.0.9,  Tun_Id 500,  Tun_Instance 44
  RSVP Path Info:
   My Address: 10.0.0.1
   Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
   Record Route: NONE
   Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
   Record Route: NONE
   Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
 Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.0.0.1  10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
 History:
  Tunnel:
   Time since created: 23 minutes, 28 seconds
   Time since path change: 50 seconds
   Number of LSP IDs (Tun_Instances) used: 44
 Current LSP:
  Uptime: 5 minutes, 24 seconds
  Selection:
 Prior LSP:
  ID: path option 10 [43]
  Removal Trigger: path error
  Last Error: PCALC:: Explicit path has unknown address, 10.2.0.1
R1#
```

**show mpls traffic-eng tunnels protection** コマンドの [Oper] フィールドにある up 値は、保護が有効であることを示しています。

```
Router# show mpls traffic-eng tunnels tunnel500 protection

R1_t500
 LSP Head, Tunnel500, Admin: up, Oper: up
 Src 10.1.1.1, Dest 10.0.0.9, Instance 44
 Fast Reroute Protection: None
 Path Protection: Backup lsp in use.
R1#
```

次のコマンド シーケンスで **no shutdown** コマンドを実行すると、インターフェイスが再度起動してプライマリ パスがアクティブになります。

```
Router> enable

Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet1/0/0
Router(config-if)# no shutdown
Router(config-if)# end
```

次のコマンド出力は、パス保護が再確立され、プライマリ パスが使用されていることを示しています。

```
Router# show mpls traffic-eng tunnels tunnel500

Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
 Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
 Config Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
 Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
 InLabel : -
 OutLabel : FastEthernet1/0/0, 16
 RSVP Signalling Info:
   Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 52
  RSVP Path Info:
   My Address: 10.2.0.1
   Explicit Route: 10.2.0.2  10.10.0.1  10.10.0.2  10.0.0.9
   Record Route: NONE
   Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
   Record Route: NONE
   Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  Shortest Unconstrained Path Info:
   Path Weight: 20 (TE)
   Explicit Route: 10.0.0.1  10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
  History:
   Tunnel:
    Time since created: 25 minutes, 26 seconds
    Time since path change: 23 seconds
    Number of LSP IDs (Tun_Instances) used: 52
   Current LSP:
   Uptime: 26 seconds
    Selection: reoptimization
   Prior LSP:
    ID: path option 10 [44]
    Removal Trigger: reoptimization completed
R1#
```

次に、**show mpls traffic-eng tunnels** コマンド出力の例を示します。Tunnel500 が保護されています。障害発生後もプライマリ LSP は保護されます。

```
Router# show mpls traffic-eng tunnels tunnel500 protection

R1_t500
 LSP Head, Tunnel500, Admin: up, Oper: up
 Src 10.1.1.1, Dest 10.0.0.9, Instance 52
 Fast Reroute Protection: None
 Path Protection: 0 Common Link(s), 0 Common Node(s)
  Primary lsp path:10.2.0.1   10.2.0.2
                   10.10.0.1  10.10.0.2
                   10.0.0.9
  Protect lsp path:10.0.0.1   10.0.2
                   10.0.1.1 10.0.1.2
                   10.0.0.9
  Path Protect Parameters:
```

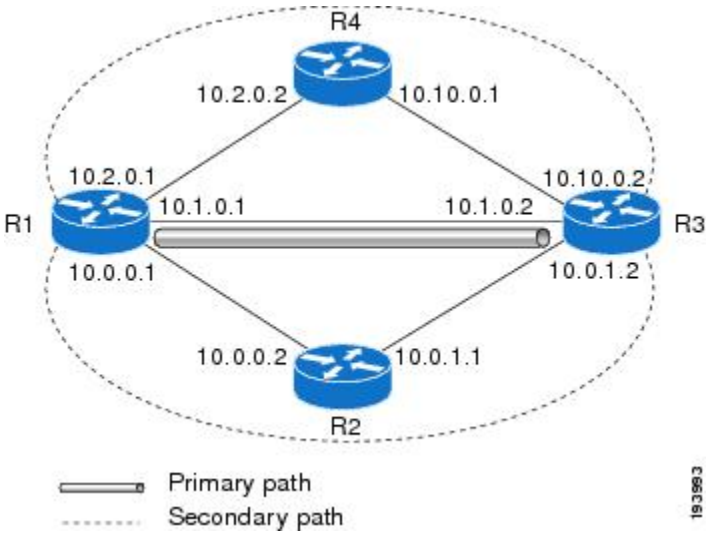
```
   Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
   Metric Type: TE (default)
  InLabel : -
  OutLabel : FastEthernet0/0/0, 16
  RSVP Signalling Info:
    Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 53
   RSVP Path Info:
    My Address: 10.0.0.1
    Explicit Route: 10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
   RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
R1#
```

# MPLS トラフィック エンジニアリング（TE）：拡張されたパス保護の設定例

## パス オプション リストの作成：例

次の図に、拡張されたパス保護のネットワーク トポロジを示します。

拡張されたパス保護の p ネットワーク トポロジ




次の例では、**secondary1** および **secondary2** という名前の 2 つの明示パスを設定します。

```
Router(config)# ip explicit-path name secondary1

Router(cfg-ip-expl-path)# index 1 next 10.0.0.2

Explicit Path name secondary1:
 1: next-address 10.0.0.2
Router(cfg-ip-expl-path)# index 2 next 10.0.1.2

Explicit Path name secondary1:
```

```
 1: next-address 10.0.0.2
 2: next-address 10.0.1.2
Router(cfg-ip-expl-path)# ip explicit-path name secondary2

Router(cfg-ip-expl-path)# index 1 next 10.2.0.2

Explicit Path name secondary2:
 1: next-address 10.2.0.2
Router(cfg-ip-expl-path)# index 2 next 10.10.0.2

Explicit Path name secondary2:
 1: next-address 10.2.0.2
 2: next-address 10.10.0.2
Router(cfg-ip-expl-path)# exit
```

次の例では、バックアップ パスのパス オプション リストを作成します。パス オプション リストは、明示パスを使用して定義します。

```
Router(config)# mpls traffic-eng path-option list name pathlist-01

Router(cfg-pathoption-list)# path-option 10 explicit name secondary1

path-option 10 explicit name secondary1
Router(cfg-pathoption-list)# path-option 20 explicit name secondary2

path-option 10 explicit name secondary1
path-option 20 explicit name secondary2
Router(cfg-pathoption-list)# exit
```

# プライマリ パス オプションを保護するパス オプション リストの割り当ての例

次の例では、トラフィック エンジニアリング トンネルが設定されています。

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface tunnel 2

Router(config-if)# tunnel mpls traffic-eng path-option protect 10 list name secondary-list
```

次の **showrunninginterface** コマンド出力は、パス保護が設定されていることを示しています。トンネル 2 には、パス primary1 を使用して、セカンダリ リストで保護されるパス オプション 10 が設定されています。

```
Router# show running-config interface tunnel 2

Building configuration...
Current configuration : 296 bytes
!
interface Tunnel2
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 103.103.103.103
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 10 explicit name primary1
 tunnel mpls traffic-eng path-option protect 10 list name secondary-list
```

# 例：パス保護の前後でのトンネルの設定

**show mpls traffic-eng tunnels** コマンドを実行すると、プライマリ（保護された）パスに関する情報が表示されます。次の出力例は、パス保護が設定されていることを示しています。

```
Router# show mpls traffic-eng tunnels tunnel500
Name: R1_t500   (Tunnel500)   Destination: 10.0.0.9
 Status:
  Admin: up  Oper: up  Path: valid  Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
 Config Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
 Active Path Option Parameters:
    State: explicit path option 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
 InLabel : -
 OutLabel : FastEthernet1/0/0, 16
 RSVP Signalling Info:
   Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 43
  RSVP Path Info:
   My Address: 10.2.0.1
   Explicit Route: 10.2.0.2  10.10.0.1  10.10.0.2  10.0.0.9
   Record Route: NONE
   Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
   Record Route: NONE
   Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  Shortest Unconstrained Path Info:
   Path Weight: 20 (TE)
   Explicit Route: 10.0.0.1  10.0.0.2  10.0.1.1  10.0.1.2
                   10.0.0.9
 History:
  Tunnel:
   Time since created: 18 minutes, 22 seconds
   Time since path change: 19 seconds
   Number of LSP IDs (Tun_Instances) used: 43
  Current LSP:
   Uptime: 22 seconds
   Selection: reoptimization
  Prior LSP:
   ID: path option 10 [27]
   Removal Trigger: reoptimization completed
```

次の **show mpls traffic-eng tunnels** コマンド出力は、セカンダリ パスに関する情報を示しています。Tunnel500 が保護されています。保護パスが使用されており、プライマリ パスが停止しています。コマンド出力は、プライマリ LSP およびセカンダリ LSP の IP 明示パスを示しています。

```
Router# show mpls traffic-eng tunnels tunnel500 protection

R1_t500
 LSP Head, Tunnel500, Admin: up, Oper: up
 Src 10.1.1.1, Dest 10.0.0.9, Instance 43
 Fast Reroute Protection: None
 Path Protection: 0 Common Link(s), 0 Common Node(s)
  Primary lsp path:10.2.0.1  10.2.0.2
                   10.10.0.1 10.10.0.2
                   10.0.0.9
  Protect lsp path:10.0.0.1  10.0.0.2
                   10.0.1.1  10.0.1.2
```

```
                  10.0.0.9
  Path Protect Parameters:
   Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
   Metric Type: TE (default)
  InLabel : -
  OutLabel : FastEthernet0/0/0, 17
  RSVP Signalling Info:
   Src 10.1.1.1,  Dst 10.0.0.9,  Tun_Id 500,  Tun_Instance 44
  RSVP Path Info:
   My Address: 10.0.0.1
   Explicit Route: 10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
   Record Route: NONE
   Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
   Record Route: NONE
   Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
R1#
```

次の **shutdown** コマンドを実行すると、パス保護を使用するインターフェイスがシャットダウンされます。

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet1/0/0
Router(config-if)# shutdown
Router(config-if)# end
Router#
```

次の **show mpls traffic-eng tunnels** コマンドは、保護パスが使用されており、プライマリ パスが停止していることを示しています。

```
Router# show mpls traffic-eng tunnels tunnel500
Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
 Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path option 10, type explicit path344
  path option 20, type explicit path345
  Path Protection: Backup lsp in use.
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
 Config Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
 Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
 InLabel : -
 OutLabel : FastEthernet0/0/0, 17
 RSVP Signalling Info:
   Src 10.1.1.1,  Dst 10.0.0.9,  Tun_Id 500,  Tun_Instance 44
  RSVP Path Info:
   My Address: 10.0.0.1
   Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
   Record Route: NONE
   Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
   Record Route: NONE
   Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
 Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.0.0.1  10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
 History:
  Tunnel:
   Time since created: 23 minutes, 28 seconds
   Time since path change: 50 seconds
   Number of LSP IDs (Tun_Instances) used: 44
 Current LSP:
```

```
  Uptime: 5 minutes, 24 seconds
  Selection:
 Prior LSP:
  ID: path option 10 [43]
  Removal Trigger: path error
  Last Error: PCALC:: Explicit path has unknown address, 10.2.0.1
R1#
```

**show mpls traffic-eng tunnels protection** コマンドの [Oper] フィールドにある up 値は、保護が有効であることを示しています。

```
Router# show mpls traffic-eng tunnels tunnel500 protection

R1_t500
 LSP Head, Tunnel500, Admin: up, Oper: up
 Src 10.1.1.1, Dest 10.0.0.9, Instance 44
 Fast Reroute Protection: None
 Path Protection: Backup lsp in use.
R1#
```

次のコマンド シーケンスで **no shutdown** コマンドを実行すると、インターフェイスが再度起動してプライマリ パスがアクティブになります。

```
Router> enable

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet1/0/0
Router(config-if)# no shutdown
Router(config-if)# end
```

次のコマンド出力は、パス保護が再確立され、プライマリ パスが使用されていることを示しています。

```
Router# show mpls traffic-eng tunnels tunnel500

Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
 Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
 Config Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
 Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
 InLabel : -
 OutLabel : FastEthernet1/0/0, 16
 RSVP Signalling Info:
   Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 52
  RSVP Path Info:
   My Address: 10.2.0.1
   Explicit Route: 10.2.0.2  10.10.0.1  10.10.0.2  10.0.0.9
   Record Route: NONE
   Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
   Record Route: NONE
   Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  Shortest Unconstrained Path Info:
   Path Weight: 20 (TE)
   Explicit Route: 10.0.0.1  10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
  History:
   Tunnel:
```

```
    Time since created: 25 minutes, 26 seconds
    Time since path change: 23 seconds
    Number of LSP IDs (Tun_Instances) used: 52
   Current LSP:
   Uptime: 26 seconds
    Selection: reoptimization
   Prior LSP:
    ID: path option 10 [44]
    Removal Trigger: reoptimization completed
R1#
```

次に、**show mpls traffic-eng tunnels** コマンド出力の例を示します。Tunnel500 が保護されています。障害発生後もプライマリ LSP は保護されます。

```
Router# show mpls traffic-eng tunnels tunnel500 protection

R1_t500
 LSP Head, Tunnel500, Admin: up, Oper: up
 Src 10.1.1.1, Dest 10.0.0.9, Instance 52
 Fast Reroute Protection: None
 Path Protection: 0 Common Link(s), 0 Common Node(s)
  Primary lsp path:10.2.0.1   10.2.0.2
                   10.10.0.1  10.10.0.2
                   10.0.0.9
  Protect lsp path:10.0.0.1   10.0.2
                   10.0.1.1 10.0.1.2
                   10.0.0.9
  Path Protect Parameters:
   Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
   Metric Type: TE (default)
  InLabel : -
  OutLabel : FastEthernet0/0/0, 16
  RSVP Signalling Info:
    Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 53
   RSVP Path Info:
    My Address: 10.0.0.1
    Explicit Route: 10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
   RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
R1#
```

# 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』 |
| MPLS トラフィック エンジニアリング コマンド | 『*Cisco IOS Multiprotocol Label Switching Command Reference*』 |
| RSVP コマンド | 『*Cisco IOS Quality of Service Solutions Command Reference*』 |

| 関連項目 | マニュアル タイトル |
|---|---|
| IS-IS | • 『*Cisco IOS IP Routing Protocols Command Reference*』<br>• 『Configuring a Basic IS-IS Network』 |
| OSPF | • 『*Cisco IOS IP Routing Protocols Command Reference*』<br>• 『Configuring OSPF』 |
| ISSU | Cisco IOS XE インサービス ソフトウェア アップグレード サポート |
| NSF/SSO | • 『Cisco Nonstop Forwarding』<br>• 『Stateful Switchover』 |

### 標準

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

### MIB

| MIB | MIB のリンク |
|---|---|
| この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。<br>http://www.cisco.com/go/mibs |

### RFC

| RFC | Title |
|---|---|
| この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC の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 | Link |
|---|---|
| ★枠で囲まれた Technical Assistance の場合★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 |

# MPLS トラフィック エンジニアリング パス保護の機能情報

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 *8*：*MPLS* トラフィック エンジニアリング パス保護の機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| 『MPLS Traffic Engineering Path Protection』 | Cisco IOS XE Release 2.3 | MPLS トラフィック エンジニアリング（TE）：パス保護機能は、MPLS TE トンネルに対して、エンドツーエンドの障害回復メカニズム（完全なパス保護）を提供します。<br>この機能は、Cisco IOS XE Release 2.3 に統合されました。<br>次のコマンドが導入または変更されました。**show ip rsvp high-availability database**、**tunnel mpls traffic-eng path-option**、および **tunnel mpls traffic-eng path-option protect**。 |
| ISSU：MPLS トラフィック エンジニアリング（TE）：パス保護 | Cisco IOS XE Release 2.3 | Cisco ISSU プロセスを使用すれば、システムによるパケット転送を中断することなく、Cisco IOS XE ソフトウェアのアップグレードまたはダウングレードを実行することができます。<br>この機能は、Cisco IOS XE Release 2.3 に統合されました。 |
| NSF/SSO：MPLS トラフィック エンジニアリング（TE）：パス保護 | Cisco IOS XE Release 2.3 | Cisco NSF with SSO を使用すると、ネットワーク プロセッサのハードウェアまたはソフトウェアに障害が発生した場合でも、継続してパケットを転送できます。<br>この機能は、Cisco IOS XE Release 2.3 に統合されました。 |

| 機能名 | リリース | 機能情報 |
|---|---|---|
| MPLS TE：拡張されたパス保護 | Cisco IOS XE Release 3.5S | 拡張されたパス保護では、プライマリ パス オプション単位で複数のバックアップ パス オプションをサポートします。<br>この機能は、Cisco IOS XE Release 3.5S に統合されました。<br>次のコマンドが追加または変更されました。**mpls traffic-eng path-option list**、**show mpls traffic-eng path-option list**、**show mpls traffic-eng tunnels**、および **tunnel mpls traffic-eng path-option protect**。 |

# 用語集

**自動トンネルメッシュグループ**：自動トンネル メッシュ グループ（メッシュ グループと呼びます）は、ネットワーク内のエッジ LSR 間の接続セットです。

**バックアップトンネル**：リンクまたはノードの障害発生時に他の（プライマリ）トンネルのトラフィックを保護するために使用される MPLS TE トンネル。

**BGP**：Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。個別のルーティング ポリシーが含まれた個別のルーティング ドメイン（自律システム）間のループフリールーティングを提供するように設計されたドメイン間ルーティング プロトコル。

**シスコエクスプレスフォワーディング**：ルート参照を保存することにより、ルータ内のパケットの転送を短時間で行うための手段。

**高速リルート**：ヘッドエンドで新しい LSP を確立しながら、障害のあるリンクまたはノード周囲の一時ルーティングをイネーブルにする手順。

**グレースフルリスタート**：ノード障害の発生後に RP の再起動を補助するプロセス。

**ヘッドエンド**：特定の LSP の起点となり、その LSP を管理するルータ。これは、LSP パス上の最初のルータです。

**ホップ**：2 つのネットワーク ノード間（たとえば、2 つのルータ間）のデータ パケットの通路。

**インターフェイス**：ネットワーク接続。

**IS-IS**：（Intermediate System-to-Intermediate System）このリンクステート階層型ルーティング プロトコルでは、Intermediate System（IS）ルータを呼び出して、単一のメトリックに基づいてルーティング情報を交換することにより、ネットワーク トポロジを決定します。

**ISSU**：In Service Software Upgrade。ISSU プロセスによって、パケット転送を継続しながらルータレベルで Cisco IOS XE ソフトウェアをアップデートまたは変更できます。

**リンク**：隣接するノード間のポイントツーポイント接続。隣接するノード間に複数のリンクが存在することがあります。リンクとは、送信者と受信者の間の回線または伝送パスおよびすべての関連装置からなるネットワーク通信チャネルのことです。回線または伝送リンクと呼ばれることもあります。

**LSP**：ラベルスイッチド パス。2 つのルータ間に設定された接続。この接続では、パケットを伝送するためにラベル スイッチングが使用されます。LSP の目的は、データ パケットを伝送することです。

**MPLS**：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ネットワークコアにおいて使用されるパケット転送テクノロジー。これにより、スイッチング ノードにデータの転送方法を指示するためのデータ リンク層ラベルが適用されるため、ネットワーク層ルーティングで通常行われる転送よりも高速でスケーラブルな転送が行われます。

**NHOP**：ネクスト ホップ。LSP のパス上の次のダウンストリーム ノード。

**NHOPバックアップトンネル**：ネクストホップ バックアップ トンネル。障害ポイントの先にある LSP のネクスト ホップで終端し、障害ポイントのすぐアップストリームにあるホップを起点とするバックアップ トンネル。このバックアップ トンネルは、障害の発生したリンクをバイパスし、障害発生前にこのリンクを使用していたプライマリ LSP を保護するために使用されます。

**NNHOP**：Next-Next HOP（ネクストネクスト ホップ）。LSP のパス上の次のダウンストリーム ノードの後ろのノード。

**NNHOPバックアップトンネル**：ネクストホップから 1 つめのホップのバックアップ トンネル。障害ポイントの先にある LSP のネクストネクスト ホップで終端し、障害ポイントのすぐアップストリームにあるホップを起点とするバックアップ トンネル。このバックアップ トンネルは、障害の発生したリンクまたはノードをバイパスし、障害発生前にこのリンクまたはノードを使用していたプライマリ LSP を保護するために使用されます。

**ノード**：ネットワーク接続のエンドポイント、つまりネットワーク内の複数の回線に共通する接合部。複数のノードをリンクで相互接続することができます。これらのノードは、ネットワーク内のコントロール ポイントとなります。ノードは、プロセッサ、コントローラ、またはワークステーションです。

**NSF**：Cisco nonstop Forwarding。Cisco NSF は常にステートフル スイッチオーバー（SSO）とともに実行され、レイヤ 3 トラフィックの冗長性を確保します。NSF は SSO と連動して、スイッチオーバー後にネットワークが利用できなくなる時間を最小限にします。NSF の主な目的は、スーパーバイザ エンジンのスイッチオーバー後、IP パケットを転送し続けることです。

**OSPF**：Open Shortest Path First。IS-IS プロトコルから派生した、リンクステート階層型の内部ゲートウェイ プロトコル ルーティング アルゴリズム。OSPF 機能には、最小コストによるルーティング、マルチパスのルーティング、およびロード バランシングが含まれます。

**プライマリLSP**：当初、障害発生前に保護インターフェイスを介してシグナリングされていた最後の LSP。プライマリ LSP は、プライマリ パス オプションを設定するとシグナリングされます。

**プライマリトンネル**：障害が発生した場合に高速リルートされる LSP に割り当てられたトンネル。バックアップ トンネルをプライマリ トンネルにすることはできません。

**保護インターフェイス**：1 つ以上のバックアップ トンネルが関連付けられたインターフェイス。

**ルータ**：1 つ以上のメトリックを使用して、ネットワーク トラフィックを転送すべき最適のパスを決定するネットワーク層装置。ルータは、ネットワーク層情報に基づいて、ネットワーク間でパケットを転送します。

**RP**：ルート プロセッサ。シャーシに搭載される、集中化されたコントロール ユニットの総称です。

**RSVP**：Resource Reservation Protocol（リソース予約プロトコル）。カスタマーがインターネット サービスのために要求をシグナリング（予約をセットアップ）する際に使用する IETF プロトコル。これにより、カスタマーはそのネットワーク部分を経由してデータを伝送することを許可されます。

**セカンダリ LSP**：パス保護を提供するためにシグナリングされる LSP。セカンダリ LSP は、プライマリ LSP を保護します。

**セカンダリパスオプション**：保護を提供するパス オプションの設定。

**SRLG**：Shared Risk Link Group（共有リスク リンク グループ）。（たとえば、基礎となるファイバが同じであるために）一緒に停止する可能性の高いリンクのセット。

**ステート**：ルータが各 LSP に関して保守する必要のある情報。この情報は、トンネルをリルートする場合に使用されます。

**テールエンド**：LSP が終端するルータ。これは、LSP のパス上の最後のルータです。

**TE**：トラフィック エンジニアリング。標準のルーティング方式が使用されていた場合に選択されたであろうパス以外のパス上のネットワーク経由でトラフィックを転送するために使用されるテクニックとプロセス。

**トポロジ**：企業ネットワーキング構造内のネットワーク ノードおよびメディアの物理的な配置。

**トンネル**：2 つのピア間（2 台のルータ間など）のセキュアな通信パス。

**VoIP**：Voice over IP。IP ネットワーク経由で音声トラフィック（電話やファクスなど）を伝送するルータの機能。シスコの音声サポートは、音声パケット テクノロジーを使用して実装されています。

第 6 章

# MPLS トラフィック エンジニアリング：BFD-triggered 高速リルート

MPLS トラフィック エンジニアリング：BFD-triggered 高速リルート機能では、双方向フォワーディング検出（BFD）プロトコルを使用して、あらゆるメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルの高速転送パス障害検出回数を提供することによって、リンクおよびノード保護を取得できます。高速転送パス障害検出に加えて、BFD はネットワーク管理者に整合性のある障害検出方法を提供します。

Hello がサポートされたリソース予約プロトコル（RSVP）を使用して、リンクおよびノード保護を取得するには、『MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)』プロセス モジュールを参照してください。RSVP Hello を使用すると、ルータは、ネイバー ノードが停止したが、そのネイバーへのインターフェイスがまだ動作中である場合、そのことを検出できます。

# 機能情報の確認

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

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、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。

# MPLS トラフィック エンジニアリング：BFD-triggered 高速リルートの前提条件

- BFD を設定します。『*Bidirectional Forwarding Detection*』プロセス モジュールを参照してください。
- 関連するすべてのルータおよびインターフェイス上で MPLS TE をイネーブルにします。
- MPLS TE トンネルを設定します。
- 追加の前提条件については、『MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)』プロセス モジュールを参照してください。

# MPLS トラフィック エンジニアリング：BFD-triggered 高速リルートの制約事項

- 同じインターフェイス上では、BFD および RSVP Hello を設定できません。
- BFD は一部のインターフェイスではサポートされない可能性があります。
- 追加の制約事項については、『MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)』プロセス モジュールを参照してください。

# MPLS トラフィック エンジニアリング：BFD-triggered 高速リルートに関する情報

## 双方向フォワーディング検出

双方向フォワーディング検出（BFD）は、すべてのメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルのために短時間での転送パス障害検出を提供するために設計された検出プロトコルです。高速転送パス障害検出に加えて、BFD はネットワーク管理者に整合性のある障害検出方法を提供します。ネットワーク管理者はBFDを使用して、さまざまなルーティング プロトコルの Hello メカニズムで、変動速度ではなく一定速度で転送パスの障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再コンバージェンス時間の整合性が保たれ、予測可能になります。

## 高速再ルーティング

高速再ルーティング（FRR）は、リンクおよびノードの障害からマルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）ラベル スイッチド パス（LSP）を保護するためのメカニズムです。具体的には、障害ポイントの LSP をローカルに修復し、その LSP 上でのデータ フローを停止することなく、LSP のヘッドエンド ルータを新しく置き換えるエンドツーエンド LSP の確立を試行します。FRR は、障害が発生したリンクまたはノードをバイパスするバックアップ トンネルを介して再ルーティングすることによって、保護されている LSP をローカルに修復します。

## リンク保護

LSP のパスの単一リンクだけをバイパスするバックアップ トンネルが、リンク保護を提供します。パス上のリンクに障害が発生した場合、バックアップ トンネルは、LSP のトラフィックをネクスト ホップにリルートする（障害の発生したリンクをバイパスする）ことによって LSP を保護します。これらは、障害ポイントの向こう側にある LSP のネクスト ホップで終端するため、ネクスト ホップ（NHOP）バックアップ トンネルと呼ばれます。

## ノード保護

FRR により、LSP に対するノード保護が提供されます。LSP パス上のネクストホップ ノードをバイパスするバックアップ トンネルは、LSP パスのネクストホップ ノードの次のノードで終端して、結果としてネクストホップ ノードをバイパスするため、ネクストネクストホップ（NNHOP）バックアップ トンネルと呼ばれます。LSP パス上のノードに障害が発生した場合は、NNHOP バックアップ トンネルが LSP を保護します。具体的には、障害のアップストリームにあるノードをイネーブルにして、障害の発生したノードの周囲の LSP とそのトラフィックをネクストネクスト

ホップにリルートします。FRR では、ノード障害を短時間で検出できるように、RSVP Hello の使用がサポートされています。また、NNHOP バックアップ トンネルは、障害の発生したリンクおよびノードをバイパスするため、リンク障害からの保護も提供しています。

## 帯域幅保護

NHOP および NNHOP バックアップ トンネルを使用すると、リルートされた LSP の帯域幅保護を提供できます。これは、バックアップ帯域幅と呼ばれます。バックアップ帯域幅は、NHOP または NNHOP バックアップ トンネルと関連付けることができます。これにより、特定のバックアップ トンネルで保護できるバックアップ帯域幅の大きさがルータに通知されます。ルータが LSP をバックアップ トンネルにマップするとき、帯域幅保護によって、十分なバックアップ帯域幅がある場合にだけ、指定されたバックアップ トンネルが使用されます。ルータは、最大限の帯域幅保護を提供するために、どの LSP がどのバックアップ トンネルを使用するかを選択します。つまり、ルータは、保護できる LSP の数が最大限になるような方法を、LSP をバックアップ トンネルにマップする最良の方法として決定します。

# MPLS トラフィック エンジニアリング：BFD-triggered 高速リルートの設定方法

ここでは、MPLS TE LSP が設定されているネットワークに FRR 保護を追加する方法を説明します。

以下のセクションでは、リンクやノードの障害からネットワークの LSP を保護するための FRR の使用方法を説明します。各作業は、必須と任意に分けられています。

（注） これらの設定作業は任意の順序で実行できます。

（注） NNHOP バックアップ トンネルは、NHOP バックアップ トンネルを経由できません。

## ルータでの BFD サポートの有効化

### 手順の概要

1. イネーブル化
2. **configureterminal**
3. **iprsvpsignallinghellobfd**
4. **exit**

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **iprsvpsignallinghellobfd**<br><br>例：<br><br>`Router(config)# ip rsvp signalling hello bfd` | MPLS TE リンクおよびノード保護のためにルータで BFD プロトコルをイネーブルにします。 |
| ステップ 4 | **exit**<br><br>例：<br><br>`Router(config)# exit` | 特権 EXEC モードに戻ります。 |

## LSP 上での高速リルートの有効化

LSP は、高速リルート可能として設定されている場合だけ、バックアップ トンネルを使用できます。LSP で FRR をイネーブルにするには、各 LSP のヘッドエンドで次のコマンドを入力します。

### 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **tunnelmplstraffic-engfast-reroute** [**bw-protect**] [**node-protect**]
5. **exit**
6. **exit**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **イネーブル化**<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **interfacetunnel***number*<br><br>例：<br><br>`Router(config)# interface tunnel 1000` | 指定したトンネルのインターフェイス コンフィギュレーション モードを開始します。<br><br>• *number* 引数はトンネルの番号です。 |
| ステップ 4 | **tunnelmplstraffic-engfast-reroute** [**bw-protect**] [**node-protect**]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect node-protect` | リンクまたはノードの障害発生時に、MPLS TE トンネルで、確立されたバックアップ トンネルを使用できるようにします。<br><br>• **bw-protect** キーワードは「bandwidth protection desired」ビットを設定して、バックアップ帯域幅保護を有効にします。<br><br>• **node-protect** キーワードは 「node protection desired」 ビットを設定して、バックアップ帯域幅保護を有効にします。 |
| ステップ 5 | **exit**<br><br>例：<br><br>`Router(config-if)# exit` | インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 6 | **exit**<br><br>例：<br><br>`Router(config)# exit` | 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。 |

# ネクスト ホップまたはネクストネクスト ホップへのバックアップ トンネルの作成

ネクスト ホップまたはネクストネクスト ホップへのバックアップ トンネルを作成するには、次のタスクを実行します。

バックアップ トンネルのヘッドエンドとなるノード（つまり、ダウンストリームのリンクまたはノードに障害が発生する可能性のあるノード）上で、次のコマンドを入力します。コマンドを入力するノードは、サポートされているプラットフォームであることが必要です。「機能情報の確認」セクションを参照してください。

バックアップ トンネルの作成は、基本的に他のトンネルの作成と同じです。

（注） **exclude-address** コマンドを使用してバックアップ トンネルのパスを指定するときは、インターフェイス アドレスを除外してリンクを除外する（NHOP バックアップ トンネルを作成する場合）か、ルータ ID アドレスを除外してノードを回避する（NNHOP バックアップ トンネルを作成する場合）必要があります。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipunnumbered***typenumber*
5. **tunneldestination***ip-address*
6. **tunnelmodemplstraffic-eng**
7. **tunnelmplstraffic-engpath-option***number* {**dynamic** | **explicit** {**name***path-name* | *path-number*}}[**lockdown**]
8. **exit**
9. **ipexplicit-pathname***name*
10. **exclude-address***address*
11. **exit**
12. **exit**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **interfacetunnel***number*<br><br>例：<br><br>`Router(config)# interface tunnel 1` | 新しいトンネル インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。<br><br>• *number* 引数はトンネルの番号です。 |
| ステップ 4 | **ipunnumbered***typenumber*<br><br>例：<br><br>`Router(config-if)# ip unnumbered loopback 0` | 明示的なIPアドレスをインターフェイスに割り当てずにインターフェイス上の IP 処理をイネーブルにします。<br><br>• *type* 引数および *number* 引数では、ルータに IP アドレスが割り当てられている別のインターフェイスのタイプと番号を指定します。番号付けされていない別のインターフェイスは指定できません。<br><br>（注） **ipunnumberedloopback0** コマンドはこのトンネル インターフェイスに、インターフェイス ループバック 0 の IP アドレスと同じ IP アドレスを割り当てます。このコマンドは、ループバック 0 が IP アドレスに設定されるまでは有効になりません。 |
| ステップ 5 | **tunneldestination***ip-address*<br><br>例：<br><br>`Router(config-if)# tunnel destination 10.3.3.3` | トンネル インターフェイスの宛先を指定します。<br><br>• *ip-address* 引数には、ドット付き 10 進表記でトンネルが終端するデバイスの IP アドレスを指定します。このアドレスは、保護対象となる LSP の NHOP または NNHOP であるデバイスのルータ ID にする必要があります。 |
| ステップ 6 | **tunnelmodemplstraffic-eng**<br><br>例：<br><br>`Router(config-if)# tunnel mode mpls traffic-eng` | トンネルのカプセル化モードを MPLS TE に設定します。 |
| ステップ 7 | **tunnelmplstraffic-engpath-option***number* {**dynamic** \| **explicit** {**name***path-name* \| *path-number*}}[**lockdown**]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit name avoid-protected-link` | 指定した IP 明示パス、またはトラフィック エンジニアリング トポロジ データベースからダイナミックに計算されたパスを使用するように、トンネルを設定します。<br><br>• *number* 引数は、パス オプションの優先度を指定する引数です。複数のパス オプションを設定する場合、より低い数値のオプションが優先されます。有効値は 1 ～ 1000 です。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • **dynamic** キーワードは、ラベル スイッチド パス（LSP）がダイナミックに計算されることを示します。<br>• **explicit** キーワードは、LSP のパスが IP 明示パスであることを示します。<br>• **name***path-name* キーワードおよび引数は、トンネルがこのオプションで使用する IP 明示パスのパス名です。<br>• **identifier***path-number* キーワードおよび引数のペアは、トンネルがこのオプションで使用する IP 明示パスのパス番号を指定します。有効な範囲は 1 ～ 65535 です。<br>• **lockdown** キーワードでは、LSP を再最適化できないように指定します。<br>（注） 明示パスが現在使用可能でない場合は、ダイナミック パスが使用されます。 |
| ステップ 8 | **exit**<br>例：<br>`Router(config-if)# exit` | インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。 |
| ステップ 9 | **ipexplicit-pathname***name*<br>例：<br>`Router(config)# ip explicit-path name avoid-protected-link` | IP 明示パスの IP 明示パス モードを入力して、指定されたパスを作成します。<br>• *name* 引数は、明示パスの名前です。 |
| ステップ 10 | **exclude-address***address*<br>例：<br>`Router(cfg-ip-expl-path)# exclude-address 10.3.3.3` | 明示パスからアドレスを除外します。<br>• *address* 引数はリンク保護を行うリンクの IP アドレスを指定します。ノード保護の場合は、これにより保護対象のノードのルータ ID を指定します。<br>（注） バックアップ トンネル パスはダイナミックにも明示的にもできます。除外されたアドレスを使用する必要はありません。バックアップ トンネルは保護対象のリンクまたはノードを回避する必要があるため、除外されたアドレスを使用すると役立ちます。 |
| ステップ 11 | **exit**<br>例：<br>`Router(cfg-ip-expl-path))# exit` | IP 明示パス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 12 | **exit**<br><br>例：<br><br>`Router(config)# exit` | 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。 |

# 保護インターフェイスへのバックアップ トンネルの割り当て

保護されたインターフェイスに 1 つまたは複数のバックアップ トンネルを割り当てるには、次のタスクを実行します。

バックアップ トンネルのヘッドエンドとなるノード（つまり、ダウンストリームのリンクまたはノードに障害が発生する可能性のあるノード）上で、次のコマンドを入力します。コマンドを入力するノードは、サポートされているプラットフォームであることが必要です。「機能情報の確認」セクションを参照してください。

（注） インターフェイスに IP アドレスを割り当てて、MPLS TE トンネル機能がイネーブルになるようにインターフェイスを設定する必要があります。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***type* slot/sub*slot*/*port*[**.***subinterface*]
4. **mplstraffic-engbackup-pathtunnel***tunnel-id*
5. **exit**
6. **exit**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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* slot/sub*slot*/*port*[**.***subinterface*]<br><br>例：<br><br>`Router(config)# interface Gigabitethernet 2/1/0` | インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。<br><br>• *type* 引数で、設定するインターフェイスのタイプを指定します。<br><br>• *slot* 引数はシャーシのスロット番号です。スロット情報については、該当するハードウェア マニュアルを参照してください。SPA インターフェイス プロセッサ（SIP）については、プラットフォーム固有の SPA ハードウェア インストレーション ガイドまたはプラットフォーム固有の SPA ソフトウェア設定ガイドの対応する「Identifying Slots and Subslots for SIPs and SPAs」トピックを参照してください。<br><br>• */subslot* キーワードと引数のペアは SPA が搭載されている SIP のセカンダリ スロット番号を指定します。スラッシュ（/）が必要です。<br><br>サブスロット情報については、プラットフォーム固有の SPA ハードウェア インストレーション ガイドおよびプラットフォーム固有の SPA ソフトウェア設定ガイドの対応する「Specifying the Interface Address on an SPA」トピックを参照してください。<br><br>• */port* キーワードと引数のペアはポートまたはインターフェイス番号を指定します。スラッシュ（/）が必要です。<br><br>ポート情報については、該当するハードウェア マニュアルを参照してください。SPA については、プラットフォーム固有の SPA ソフトウェア設定ガイドの対応する「Specifying the Interface Address on a SPA」トピックを参照してください。<br><br>• ***.subinterface-number*** キーワードと引数のペアは 1 から 4294967293 の範囲にあるサブインターフェイス番号を指定します。ピリオド（.）の前の番号は、このサブインターフェイスが属する番号と一致する必要があります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 4 | **mplstraffic-engbackup-pathtunnel***tunnel-id*<br><br>例：<br><br>`Router(config-if)# mpls traffic-eng backup-path tunnel2` | インターフェイスで障害が検出された場合にバックアップ トンネルを使用する物理インターフェイスを設定します。<br><br>• *tunnel-id* 引数は設定したインターフェイスを出る LSP のリンクまたはノード障害がある場合に使用するバックアップ トンネルを特定する文字列です。<br><br>（注） このコマンドを何回か入力して、複数のバックアップ トンネルを同じ保護インターフェイスと関連付けることができます。 |
| ステップ 5 | **exit**<br><br>例：<br><br>`Router(config-if))# exit` | インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 6 | **exit**<br><br>例：<br><br>`Router(config)# exit` | 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。 |

# 保護インターフェイスで BFD を有効化する

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***type* slot/sub*slot* / *port*[**.***subinterface*]
4. **iprsvpsignallinghellobfd**
5. **bfdinterval***milliseconds***min_rx***milliseconds***multiplier***interval-multiplier*
6. **exit**
7. **exit**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化 | 特権 EXEC モードをイネーブルにします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | 例：<br>`Router> enable` | • パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br>例：<br>`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* slot/sub*slot* / *port*[**.***subinterface*]<br>例：<br>`Router(config)# interface Gigabitethernet 2/1/0` | インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。<br>• *type* 引数で、設定するインターフェイスのタイプを指定します。<br>• *slot* 引数はシャーシのスロット番号です。スロット情報については、該当するハードウェア マニュアルを参照してください。SPA インターフェイス プロセッサ（SIP）については、プラットフォーム固有の SPA ハードウェア インストレーション ガイドまたはプラットフォーム固有の SPA ソフトウェア設定ガイドの対応する「Identifying Slots and Subslots for SIPs and SPAs」トピックを参照してください。<br>• */subslot* キーワードと引数のペアは SPA が搭載されている SIP のセカンダリ スロット番号を指定します。スラッシュ（/）が必要です。<br>サブスロット情報については、プラットフォーム固有の SPA ハードウェア インストレーション ガイドおよびプラットフォーム固有の SPA ソフトウェア設定ガイドの対応する「Specifying the Interface Address on an SPA」トピックを参照してください。<br>• */port* キーワードと引数のペアはポートまたはインターフェイス番号を指定します。スラッシュ（/）が必要です。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | ポート情報については、該当するハードウェア マニュアルを参照してください。SPA については、プラットフォーム固有の SPA ソフトウェア設定ガイドの対応する「Specifying the Interface Address on a SPA」トピックを参照してください。<br>• *.subinterface-number* キーワードと引数のペアは 1 から 4294967293 の範囲にあるサブインターフェイス番号を指定します。ピリオド（.）の前の番号は、このサブインターフェイスが属する番号と一致する必要があります。 |
| ステップ 4 | **iprsvpsignallinghellobfd**<br>例：<br>`Router(config-if)# ip rsvp signalling hello bfd` | MPLS TE リンクおよびノード保護のためにインターフェイスで BFD プロトコルを有効にします。 |
| ステップ 5 | **bfdinterval***milliseconds***min_rx***milliseconds***multiplier***interval-multiplier*<br>例：<br>`Router(config-if)# bfd interval 100 min_rx 100 multiplier 4` | インターフェイスの BFD セッション パラメータを設定します。<br>• **interval** *milliseconds* キーワードおよび引数のペアは BFD 制御パケットが BFD ピアに送信される速度を指定します。milliseconds 引数に設定できる時間の範囲は 50 ～ 999 です。<br>• **min_rx** *milliseconds* キーワードおよび引数のペアは BFD 制御パケットが BFD ピアに受信される速度を指定します。milliseconds 引数に設定できる時間の範囲は 1 ～ 999 です。<br>• **multiplier** *interval-multiplier* キーワードおよび引数のペアは BFD ピアから連続して紛失してよい BFD 制御パケットの数を指定します。この数に達すると、BFD はそのピアが利用不可になっていることを宣言し、レイヤ 3 BFD ピアに障害が伝えられます。multiplier-value 引数に指定できる値の範囲は、3 ～ 50 です。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **exit**<br><br>例：<br>`Router(config-if))# exit` | インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 7 | **exit**<br><br>例：<br>`Router(config)# exit` | 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。 |

# バックアップ トンネルへのバックアップ帯域幅およびプール タイプの関連付け

バックアップ帯域幅をバックアップ トンネルに関連付け、バックアップ トンネルを使用できる LSP のタイプを指定するには、次のタスクを入力します。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **tunnelmplstraffic-engbackup-bw**{*bandwidth* | [**sub-pool** {*bandwidth* | **Unlimited**}] [**global-pool** {*bandwidth* | **Unlimited**}]} [**any** {*bandwidth* | **Unlimited**}]
5. **exit**
6. **exit**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **interfacetunnel***number*<br><br>例：<br><br>`Router(config)# interface tunnel 2` | 指定したトンネルのインターフェイスコンフィギュレーション モードを開始します。<br><br>• *number* 引数はトンネルの番号です。 |
| ステップ 4 | **tunnelmplstraffic-engbackup-bw**{*bandwidth* \| [**sub-pool** {*bandwidth* \| **Unlimited**}] [**global-pool** {*bandwidth* \| **Unlimited**}]} [**any** {*bandwidth* \| **Unlimited**}]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000` | 帯域幅をバックアップ トンネルに関連付け、指定されたプールから帯域幅を割り当てられた LSP がこのトンネルを使用できるかどうかを指定します。 |
| ステップ 5 | **exit**<br><br>例：<br><br>`Router(config-if))# exit` | インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 6 | **exit**<br><br>例：<br><br>`Router(config)# exit` | 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。 |

# バックアップ帯域幅保護の設定

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **tunnelmplstraffic-engfast-reroute** [**bw-protect**]
5. **exit**
6. **mplstraffic-engfast-reroutebackup-prot-preemptionoptimize-bw**
7. **exit**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **interfacetunnel***number*<br><br>例：<br><br>`Router(config)# interface tunnel 2` | 指定したトンネルのインターフェイス コンフィギュレーション モードを開始します。<br><br>• *number* 引数はトンネルの番号です。 |
| ステップ 4 | **tunnelmplstraffic-engfast-reroute** [**bw-protect**]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect` | MPLS TE トンネルが、リンクまたはノードの障害発生時に、確立されたバックアップ トンネルを使用できるようにします。<br><br>• **bw-protect** キーワードを指定すると、帯域幅保護されたバックアップ トンネルを使用するための LSP プライオリティが付与されます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **exit**<br><br>例：<br><br>`Router(config-if)# exit` | インターフェイス コンフィギュレーション モードを終了します。 |
| ステップ 6 | **mplstraffic-engfast-reroutebackup-prot-preemptionoptimize-bw**<br><br>例：<br><br>`Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw` | バックアップ保護プリエンプション アルゴリズムを、デモートされる LSP の数を最小限にするアルゴリズムから、無駄な帯域幅の大きさを最小限にするアルゴリズムに変更します。 |
| ステップ 7 | **exit**<br><br>例：<br><br>`Router(config)# exit` | 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。 |

# 高速リルートの動作状態の確認

## 手順の概要

1. **showmplstraffic-engtunnelsbrief**
2. **showiprsvpsenderdetail**
3. **showmplstraffic-engfast-reroutedatabase**
4. **showmplstraffic-engtunnelsbackup**
5. **showmplstraffic-engfast-reroutedatabase**
6. **showiprsvpreservationdetail**
7. **showiprsvphello**
8. **showiprsvpinterfacedetail**
9. **showiprsvphellobfdnbr**
10. **showiprsvphellobfdnbrdetail**
11. **showiprsvphellobfdnbrsummary**

## 手順の詳細

ステップ 1 **showmplstraffic-engtunnelsbrief**

このコマンドを使用して、バックアップ トンネルが動作していることを確認します。

例：

```
Router# show mpls traffic-eng tunnels brief

Signalling Summary:
    LSP Tunnels Process:           running
    RSVP Process:                  running
    Forwarding:                    enabled
    Periodic reoptimization:       every 3600 seconds, next in 1706 seconds
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
Router_t1                        10.112.0.12      -         Gi4/0/1   up/up
Router_t2                        10.112.0.12      -         unknown   up/down
Router_t3                        10.112.0.12      -         unknown   admin-down
Router_t1000                     10.110.0.10      -         unknown   up/down
Router_t2000                     10.110.0.10      -         Gi4/0/1   up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

**ステップ 2** **showiprsvpsenderdetail**

このコマンドを使用して、LSP が適切なバックアップ トンネルによって保護されていることを確認します。

次に、障害発生前にローカル修復ポイント（PLR）の役割を果たすルータで **showiprsvpsenderdetail** コマンドが入力されたときの出力例を示します。

例：

```
Router# show ip rsvp sender detail

PATH:
 Tun Dest:   10.10.0.6  Tun ID: 100  Ext Tun ID: 10.10.0.1
 Tun Sender: 10.10.0.1  LSP ID: 31
 Path refreshes:
  arriving: from PHOP 10.10.7.1 on Et0/0 every 30000 msecs
 Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0x7) Local Prot desired, Label Recording, SE Style
  session Name: R1_t100
 ERO: (incoming)
  10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
  10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
 RRO:
   10.10.7.1/32, Flags:0x0 (No Local Protection)
   10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP) !Available to NNHOP
   10.10.1.1/32, Flags:0x0 (No Local Protection)
 Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
   Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
 Fast-Reroute Backup info:
   Inbound  FRR: Not active
   Outbound FRR: No backup tunnel selected
 Path ID handle: 50000416.
 Incoming policy: Accepted. Policy source(s): MPLS/TE
 Status: Proxy-terminated
```

**ステップ 3** **showmplstraffic-engfast-reroutedatabase**
**clearipsvphelloinstancecounters** コマンドを入力して、次のことを確認します。

- MPLS TE FRR ノード保護が有効になっている。
- 特定タイプの LSP がバックアップ トンネルを使用できる。

次のコマンド出力は、保護されている LSP を表しています。

例：

```
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected tunnel              In-label Out intf/label   FRR intf/label   Status
Tunnel500                     Tun hd   AT4/0.100:Untagg Tu501:20         ready
Prefix item frr information:
Prefix             Tunnel     In-label Out intf/label    FRR intf/label  Status
10.0.0.8/32        Tu500      18       AT4/0.100:Pop ta  Tu501:20        ready
10.0.8.8/32        Tu500      19       AT4/0.100:Untagg  Tu501:20        ready
10.8.9.0/24        Tu500      22       AT4/0.100:Untagg  Tu501:20        ready
LSP midpoint item frr information:
LSP identifier     In-label Out     intf/label     FRR intf/label     Status
```

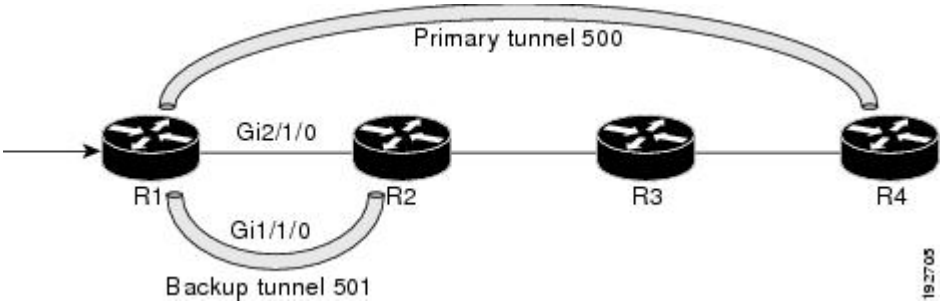
ラベル配布プロトコル（LDP）がイネーブルになっていない場合、すべてのプレフィックスが単一のリライトを使用するため、個別のプレフィックス アイテムは表示されません。特定の IP プレフィックスがこの画面に表示されていない場合、その IP プレフィックスが FRR 保護されていることを確認するには、**showmplsforwarding-table***ip-address***detail** コマンド内にそのプレフィックスを入力します。画面の最後の行に、そのプレフィックスが保護されているかどうかが示されます。

例：

```
Router# show mpls forwarding-table 10.0.0.11 32 detail

Local    Outgoing    Prefix         Bytes tag   Outgoing               Next Hop
tag      tag or VC   or Tunnel Id   switched    interface
Tun hd   Untagged    10.0.0.11/32   48 5/0      Gi5/0    point2point
          MAC/Encaps=4/8, MTU=1520, Tag Stack{22}
          48D18847 00016000
          No output feature configured
          Fast Reroute Protection via (Tu0, outgoing label 12304)
```

次のコマンド出力は、FRR プライマリ トンネルがギガビット イーサネット インターフェイスを経由し、バックアップ トンネルがギガビット イーサネット インターフェイスを経由する場合に保護される LSP を示しています。次の図に示すように、インターフェイス ギガビット イーサネット 2/1/0 がバックアップ トンネル 501 によって保護されています。

**図 *24*：*Protected LSPs***




上の図が示すのは、

- プライマリ トンネル 500：パスは、ギガビット イーサネット 2/1/0 を介した R1 から R2、次に R3、次に R4 です。

- FRR バックアップ トンネル 501：パスは、ギガビット イーサネット 1/1/0 を介した R1 から R2 です。
- インターフェイス ギガビット イーサネット 1/1/0：バックアップ トンネル 501 によって保護されます。

例：

```
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected tunnel In-label Out intf/label FRR intf/label Status
Tunnel500 Tun hd AT4/0.100:Untagg Tu501:20 ready
Prefix item frr information:
Prefix Tunnel In-label Out intf/label FRR intf/label Status
10.0.0.8/32 Tu500 18 AT4/0.100:Pop ta Tu501:20 ready
10.0.8.8/32 Tu500 19 AT4/0.100:Untagg Tu501:20 ready
10.8.9.0/24 Tu500 22 AT4/0.100:Untagg Tu501:20 ready
LSP midpoint item frr information:
LSP identifier In-label Out intf/label FRR intf/label Status
```

次のコマンド出力は、FRR バックアップ トンネルがギガビット イーサネット インターフェイスを経由する場合に保護される LSP を示しています。

例：

```
Router# show mpls traffic-eng fast-reroute database

Tunnel head end item frr information:
Protected tunnel In-label Out intf/label FRR intf/label Status
Tunnel500 Tun hd PO2/0:Untagged Tu501:20 ready
Prefix item frr information:
Prefix Tunnel In-label Out intf/label FRR intf/label Status
10.0.0.8/32 Tu500 18 PO2/0:Pop tag Tu501:20 ready
10.0.8.8/32 Tu500 19 PO2/0:Untagged Tu501:20 ready
10.8.9.0/24 Tu500 22 PO2/0:Untagged Tu501:20 ready
LSP midpoint item frr information:
LSP identifier In-label Out intf/label FRR intf/label Status
```

**ステップ 4** **showmplstraffic-engtunnelsbackup**

バックアップ トンネルが動作するには、LSP がリルート可能になっている必要があります。LSP のヘッドエンドで、**showruninterfacetunnel***tunnel-number* コマンドを入力します。出力に **tunnelmplstraffic-engfast-reroute** コマンドが含まれている必要があります。このコマンドが含まれていない場合は、トンネルに対してこのコマンドを入力してください。

バックアップ トンネルの起点のルータ上で、**showmplstraffic-engtunnelsbackup** コマンドを入力します。次にサンプルのコマンド出力を示します。

例：

```
Router# show mpls traffic-eng tunnels backup
Router_t578
  LSP Head, Tunnel578, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0, PO1/1, PO3/3
    Protected lsps: 1
    Backup BW: any pool unlimited; inuse: 100 kbps
Router_t5710
  LSP Head, Tunnel5710, Admin: admin-down, Oper: down
  Src 10.55.55.55, Dest 10.7.7.7, Instance 0
```

```
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/1
    Protected lsps: 0
    Backup BW: any pool unlimited; inuse: 0 kbps
Router_t5711
  LSP Head, Tunnel5711, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.7.7.7, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0
    Protected lsps: 2
    Backup BW: any pool unlimited; inuse: 6010 kbps
```

コマンド出力により、次のことを確認できます。

- バックアップ トンネルが存在している：この LSP の NHOP または NNHOP で終端するバックアップ トンネルが存在することを確認します。[Dest] フィールド内で LSP の NHOP または NNHOP を検索します。
- バックアップ トンネルが動作している：バックアップ トンネルが動作していることを確認するには、[Oper] フィールド内で「Up」を検索します。
- バックアップ トンネルが LSP のインターフェイスに関連付けられている：LSP のインターフェイスがこのバックアップ トンネルを使用できるように設定されていることを確認します。protected i/fs フィールド リスト内で LSP の出力インターフェイスを検索します。
- バックアップ トンネルに十分な帯域幅がある：バックアップ トンネルが保有できる帯域幅の大きさを制限した場合は、障害発生時にこのバックアップ トンネルを使用する LSP を保有するための十分な帯域幅がバックアップ トンネルにあることを確認します。LSP の帯域幅は、LSP のヘッドエンドにある行 **tunnelmplstraffic-engbandwidth** によって定義されています。バックアップ トンネル上の使用可能な帯域幅を判断するには、[cfg] フィールドと [inuse] フィールドを参照してください。障害発生時にこのバックアップ トンネルを使用する LSP に収容する十分な帯域幅がない場合は、追加のバックアップ トンネルを作成するか、**tunnelmplstraffic-engbandwidth** コマンドを使用して、既存のトンネルのバックアップ帯域幅を大きくします。

（注） 十分な帯域幅の大きさを決定するために、オフラインでのキャパシティ プランニングが必要になることがあります。

バックアップ トンネルに適切な帯域幅タイプが割り当てられている：このバックアップ トンネルを使用できる LSP のタイプを（サブプールまたはグローバル プールに）制限した場合、その LSP がバックアップ トンネルに適したタイプであることを確認します。LSP のタイプは、この LSP のヘッドエンドにある行 **tunnelmplstraffic-engbandwidth** によって定義されています。この行に「sub pool」という語が含まれている場合、LSP はサブプール帯域幅を使用します。含まれていない場合は、グローバル プール帯域幅を使用します。**tunnelmplstraffic-engbandwidth** コマンドの出力を参照して、LSP タイプが、バックアップ トンネルが保有できるタイプと一致していることを確認します。

上記のいずれの確認アクションも成功しない場合は、バックアップ トンネルのヘッドエンドであるルータ上で **debugiprsvpfast-reroute** コマンドと **debugmplstraffic-engfast-reroute** コマンドを入力して、デバッグを有効にします。続いて、次の手順を実行します。

1. プライマリ トンネルに対して **shutdown** コマンドを入力します。
2. プライマリ トンネルに対して **noshutdown** コマンドを入力します。

3 デバッグ出力を参照します。

**ステップ 5** **showmplstraffic-engfast-reroutedatabase**
**cleariprsvphelloinstancecounters** コマンドを入力して、次のことを確認します。

- MPLS TE FRR ノード保護がイネーブルになっている。
- 特定タイプの LSP がバックアップ トンネルを使用できる。

次のコマンド出力は、保護されている LSP を表しています。

例：

```
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected Tunnel   In-label   intf/label       FRR intf/label      Status
Tunne110           Tun        Gi0/1/0:Untagged   Tu0:12304           ready
Prefix item frr information:
Prefix        Tunnel  In-label    Out intf/label  FRR intf/label   Status
10.0.0.11/32  Tu110   Tun hd      Gi0/1/0:Untagged  Tu0:12304        ready
LSP midpoint frr information:
LSP identifier       In-label   Out intf/label   FRR intf/label    Status
10.0.0.12 1 [459]    16         Gi0/1/1:17         Tu2000:19         ready
```

（注） ラベル配布プロトコル（LDP）がイネーブルになっていない場合、すべてのプレフィックスが単一のリライトを使用するため、個別のプレフィックス アイテムは表示されません。特定の IP プレフィックスがこの画面に表示されていない場合、その IP プレフィックスが FRR 保護されていることを確認するには、**showmplsforwarding-table***ip-address***detail** コマンド内にそのプレフィックスを入力します。画面の最後の行に、そのプレフィックスが保護されているかどうかが示されます。

例：

```
Router# show mpls forwarding-table 10.0.0.11 32 detail

Local    Outgoing    Prefix         Bytes tag    Outgoing       Next Hop
tag      tag or VC   or Tunnel Id   switched     interface
Tun hd   Untagged    10.0.0.11/32   48 Gi0/1/0     point2point
          MAC/Encaps=4/8, MTU=1520, Tag Stack{22}
          48D18847 00016000
          No output feature configured
          Fast Reroute Protection via (Tu0, outgoing label 12304)
```

**ステップ 6** **showiprsvpreservationdetail**
次に、プライマリ LSP のヘッドエンドに入力された **showiprsvpreservationdetail** コマンドの出力例を示します。プライマリ LSP のヘッドエンドにコマンドを入力すると、特に、この LSP が通過する各ホップでの FRR のステータス（つまり、ローカル保護）が表示されます。各ホップの情報は、Resv メッセージとともに末尾から先頭に移動する Record Route Object（RRO）内に収集されます。

例：

```
Router# show ip rsvp reservation detail
Reservation:
  Tun Dest:   10.1.1.1  Tun ID: 1  Ext Tun ID: 10.1.1.1
```

```
  Tun Sender: 10.1.1.1  LSP ID: 104
  Next Hop: 10.1.1.2 on Gi1/0/2
  Label: 18 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  RRO:
    10.1.1.1/32, Flags:0x1 (Local Prot Avail/to NHOP)
      Label subobject: Flags 0x1, C-Type 1, Label 18
    10.1.1.1/32, Flags:0x0 (Local Prot Avail/In Use/Has BW/to NHOP)
      Label subobject: Flags 0x1, C-Type 1, Label 16
    10.1.1.2/32, Flags:0x0 (No Local Protection)
      Label subobject: Flags 0x1, C-Type 1, Label 0
  Resv ID handle: CD000404.
  Policy: Accepted. Policy source(s): MPLS/TE
```

プライマリ LSP に関して、次の点に注意してください。

- プライマリ LSP には、最初のホップで NHOP バックアップ トンネルを使用するような保護が設定されています。
- また、2 番めのホップで NHOP バックアップ トンネルをアクティブに使用するような保護が設定されています。
- 3 番めのホップでは、ローカルな保護は設定されていません。

RRO 画面には、ホップごとに次の情報が表示されます。

- ローカル保護が使用可能かどうか（つまり、LSP によりバックアップ トンネルが選択されているかどうか）
- ローカル保護が使用中かどうか（つまり、LSP が、選択したバックアップ トンネルを使用しているかどうか）
- 選択されたバックアップ トンネルは、NHOP バックアップ トンネルか NNHOP バックアップ トンネルのいずれであるか
- このホップで使用されるバックアップ トンネルが帯域幅保護を提供するかどうか

**ステップ 7** **showiprsvphello**

このコマンドを使用して、FRR、リルート（Hello ステート タイマー）、およびグレースフル リスタートの Hello ステータスと統計情報を表示します。次に出力例を示します。

例：

```
Router# show ip rsvp hello

Hello:
 RSVP Hello for Fast-Reroute/Reroute: Enabled
  Statistics: Disabled
 BFD for Fast-Reroute/Reroute: Enabled
 RSVP Hello for Graceful Restart: Disabled
```

**ステップ 8** **showiprsvpinterfacedetail**

このコマンドを使用して、Hello のインターフェイス コンフィギュレーションを表示します。次に出力例を示します。

例：

```
Router# show ip rsvp interface detail

Gi2/1/1:
 RSVP: Enabled
 Interface State: Up
 Bandwidth:
  Curr allocated: 0 bits/sec
  Max. allowed (total): 0 bits/sec
  Max. allowed (per flow): 0 bits/sec
  Max. allowed for LSP tunnels using sub-pools (pool 1): 0 bits/sec
  Set aside by policy (total): 0 bits/sec
 Signalling:
  DSCP value used in RSVP msgs: 0x3F
  Number of refresh intervals to enforce blockade state: 4
 Authentication: disabled
  Key chain: <none>
  Type:  md5
  Window size: 1
  Challenge:  disabled
 FRR Extension:
  Backup Path: Configured (or "Not Configured")
 BFD Extension:
  State: Disabled
  Interval: Not Configured
 RSVP Hello Extension:
  State: Disabled
  Refresh Interval: FRR: 200  , Reroute: 2000
  Missed Acks:      FRR: 4    , Reroute: 4
  DSCP in HELLOs:   FRR: 0x30 , Reroute: 0x30
```

**ステップ 9** **showiprsvphellobfdnbr**

このコマンドを使用して、BFD プロトコルを使用するすべての MPLS トラフィック エンジニアリング リンクおよびノードで保護されたネイバーに関する情報を表示します。次に出力例を示します。コマンド出力は、**showiprsvphellobfdnbrsummary** コマンド出力と同じです。

例：

```
Router# show ip rsvp hello bfd nbr

Client  Neighbor    I/F     State   LostCnt   LSPs
FRR     10.0.0.6    Gi2/1/1  Up      0         1
```

**ステップ 10** **showiprsvphellobfdnbrdetail**

このコマンドを使用して、BFD プロトコルを使用するすべての MPLS トラフィック エンジニアリング リンクおよびノードで保護されたネイバーに関する詳細情報を表示します。

例：

```
Router# show ip rsvp hello bfd nbr detail

 Hello Client Neighbors
 Remote addr 10.0.0.6, Local addr  10.0.0.7
  Type: Active
  I/F: Gi2/1/1
  State: Up (for 00:09:41)
  Clients: FRR
```

```
LSPs protecting: 1 (frr: 1, hst upstream: 0 hst downstream: 0)
Communication with neighbor lost: 0
```

ステップ 11 **showiprsvphellobfdnbrsummary**

このコマンドを使用して、BFD プロトコルを使用するすべての MPLS トラフィック エンジニアリング リンクおよびノードで保護されたネイバーに関する要約情報を表示します。コマンド出力は、**showiprsvphellobfdnbrsummary** コマンド出力と同じです。

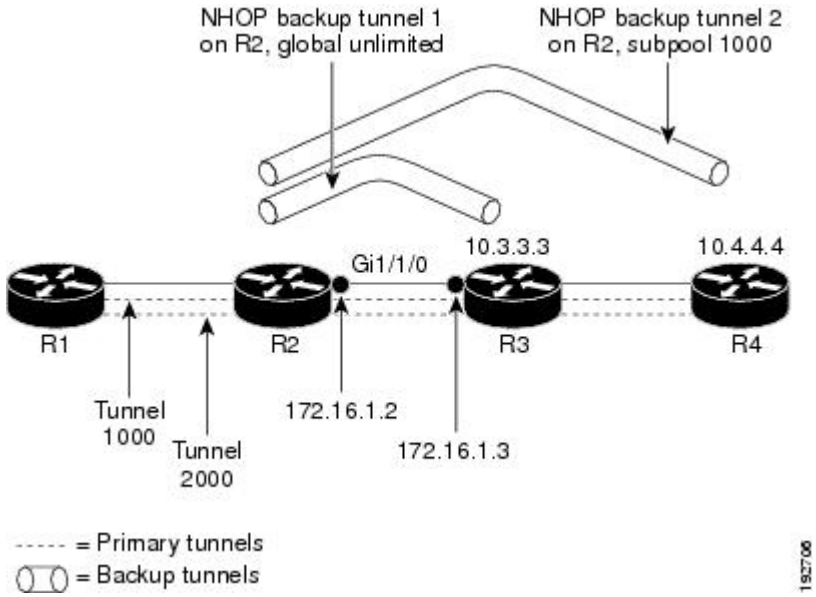
例：

```
Router# show ip rsvp hello bfd nbr summary

Client  Neighbor    I/F     State  LostCnt  LSPs
FRR     10.0.0.6   Gi2/1/1  Up     0        1
```

# MPLS トラフィック エンジニアリング BFD-triggered 高速リルートの設定例

このセクションの使用例は、次の図に示すバックアップ トンネルに基づいています。

図 *25*：バックアップ トンネル



# 例：ルータでの BFD サポートの有効化

次に、ルータで BFD プロトコルをイネーブルにする例を示します。

```
Router(config)# ip rsvp signalling hello bfd
```

# 例：LSP 上での高速リルートの有効化

上の図のルータ R1 上で、保護対象のトンネル（トンネル 1000 とトンネル 2000）ごとにインターフェイス コンフィギュレーション モードを開始します。パス上でリンクまたはノードの障害が発生した場合に、これらのトンネルがバックアップ トンネルを使用できるようにします。

トンネル 1000 は、サブプールから 10 ユニットの帯域幅を使用します。

トンネル 2000 は、グローバル プールから 5 ユニットの帯域幅を使用します。**tunnelmplstraffic-engfast-reroute** コマンド内でそれぞれ **bw-prot**、**node-prot** を指定することにより、「bandwidth protection desired」ビットと「node protection desired」ビットが設定されています。

```
Router(config)# interface tunnel 1000
Router(config-if)# tunnel mpls traffic-eng fast-reroute
Router(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 10
Router(config)# interface tunnel 2000
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect node-protect
Router(config-if)# tunnel mpls traffic-eng bandwidth 5
```

# 例：ネクスト ホップへのバックアップ トンネルの作成

上の図のルータ R2 上に、R3 への NHOP バックアップ トンネルを作成します。このバックアップ トンネルは、リンク 10.1.1.2 の使用を回避する必要があります。

```
Router(config)# ip explicit-path name avoid-protected-link
Router(cfg-ip-expl-path)# exclude-address 10.1.1.2

Explicit Path name avoid-protected-link:
____1: exclude-address 10.1.1.2
Router(cfg-ip_expl-path)# exit

Router(config)# interface tunnel 1

Router(config-if)# ip unnumbered loopback 0

Router(config-if)# tunnel destination 10.3.3.3
Router(config-if)# tunnel mode mpls traffic-eng

Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit avoid-protected-link
```

# 例：NNHOP バックアップ トンネルの作成

上の図のルータ R2 上に、R4 への NNHOP バックアップ トンネルを作成します。このバックアップ トンネルは R3 を回避する必要があります。

```
Router(config)# ip explicit-path name avoid-protected-node

Router(cfg-ip-expl-path)# exclude-address 10.3.3.3

Explicit Path name avoid-protected-node:
____1: exclude-address 10.3.3.3
Router(cfg-ip_expl-path)# end

Router(config)# interface tunnel2

Router(config-if)# ip unnumbered loopback0

Router(config-if)# tunnel destination 10.4.4.4

Router(config-if)# tunnel mode mpls traffic-eng0

Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit avoid-protected-node
```

# 例：保護インターフェイスへのバックアップ トンネルの割り当て

上の図のルータ R2 上では、両方のバックアップ トンネルがインターフェイス ギガビット イーサネット 0/1/0 に関連付けられています。

```
Router(config)# interface Gi0/1/0

Router(config-if)# mpls traffic-eng backup-path tunnel 1

Router(config-if)# mpls traffic-eng backup-path tunnel 2
```

# 例：保護インターフェイスでの BFD の有効化

上の図で、BFD はインターフェイス ギガビット イーサネット 2/1/1 で有効にされています。

```
Router(config)# interface Gi2/1/1

Router(config-if)# ip rsvp signalling hello bfd

Router(config-if)# bfd interval 100 min_rx 100 multiplier 4
```

# 例：バックアップ帯域幅およびプール タイプのバックアップ トンネルへの関連付け

上の図で、バックアップ トンネル 1 は、グローバル プールから帯域幅を取り込む LSP だけが使用します。バックアップ トンネル 1 は帯域幅保護を提供しません。バックアップ トンネル 2 は、

サブプールから帯域幅を取り込むLSPだけが使用します。バックアップ トンネル2は、最大1000ユニットの帯域幅保護を提供します。

```
Router(config)# interface tunnel 1
Router(config-if)# tunnel mpls traffic-eng backup-bw global-pool Unlimited
Router(config)# interface tunnel 2
Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000
```

## 例：バックアップ帯域幅保護の設定

（注） このグローバル設定が必要なのは、バックアップ保護プリエンプション アルゴリズムを、デモートされる LSP の数を最小限にするアルゴリズムから、無駄な帯域幅の大きさを最小限にするアルゴリズムに変更する場合だけです。

```
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect
Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw
```

# 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』 |
| リンクおよびノード保護 | 『MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)』 |
| マルチプロトコル ラベル スイッチング コマンド | 『*Cisco IOS Multiprotocol Label Switching Command Reference*』 |
| 双方向フォワーディング方向設定情報 | 『*Cisco IOS IP Routing Configuration Guide*』の「Bidirectional Forwarding Detection」の章 |

### 標準

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

### MIB

| MIB | MIB のリンク |
|---|---|
| この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。<br>http://www.cisco.com/go/mibs |

### RFC

| RFC | Title |
|---|---|
| この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC の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 | Link |
|---|---|
| ★枠で囲まれた Technical Assistance の場合★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 |

# MPLS トラフィック エンジニアリング BFD-triggered 高速リルートの機能情報

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 *9*：***MPLS*** トラフィック エンジニアリング：***BFD-triggered*** 高速リルートの機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| MPLS トラフィック エンジニアリング：BFD-triggered 高速リルート | Cisco IOS XE Release 2.3 | MPLS トラフィック エンジニアリング：BFD-triggered 高速リルート機能では、双方向フォワーディング検出（BFD）プロトコルを使用して、あらゆるメディア タイプ、カプセル化、トポロジ、およびルーティングプロトコルの高速転送パス障害検出回数を提供することによって、リンクおよびノード保護を取得できます。高速転送パス障害検出に加えて、BFD はネットワーク管理者に整合性のある障害検出方法を提供します。<br>Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。<br>次のコマンドが導入または変更されました: **clearipsvphellobfd**、**iprsvpsignallinghellobfd**（設定）、**iprsvpsignallinghellobfd**（インターフェイス）、**showiprsvphello**、**showiprsvphellobfdnbr**、**showiprsvphellobfdnbrdetail**、**showiprsvphellobfdnbrsummary**、および **showiprsvpinterfacedetail**。 |

# 用語集

**バックアップ帯域幅**：NHOP および NNHOP バックアップ トンネルを使用すると、リルートされた LSP の帯域幅保護を提供できます。

**バックアップトンネル**：リンクまたはノードの障害発生時に他の（プライマリ）トンネルのトラフィックを保護するために使用される MPLS TE トンネル。

**帯域幅**：リンクの使用可能なトラフィック容量。

**高速リルート**：ヘッドエンドで新しい LSP を確立しながら、障害のあるリンクまたはノード周囲の一時ルーティングをイネーブルにする手順。

**グローバルプール**：MPLS トラフィック エンジニアリングのリンクまたはノードに割り当てられた合計帯域幅。

**ヘッドエンド**：特定の LSP の起点となり、その LSP を管理するルータ。これは、LSP パス上の最初のルータです。

**ホップ**：2 つのネットワーク ノード間（たとえば、2 つのルータ間）のデータ パケットの通路。

**インスタンス**：Hello インスタンスは、特定のルータ インターフェイス アドレスおよびリモート IP アドレスに対して RSVP Hello 拡張機能を実装します。アクティブな Hello インスタンスは、定期的に Hello Request メッセージを送信し、応答として Hello ACK メッセージを予期します。予期されている Ack メッセージを受信できない場合、アクティブな Hello インスタンスは、そのネイバー（リモートの IP アドレス）が到達不能である（つまり失われている）ことを宣言します。これにより、このネイバーを通過する LSP の高速リルートが行われることがあります。

**インターフェイス**：ネットワーク接続。

**リンク**：隣接するノード間のポイントツーポイント接続。隣接するノード間に複数のリンクが存在することがあります。送信者と受信者の間の回線または伝送パスおよびすべての関連装置からなるネットワーク通信チャネル。回線または伝送リンクと呼ばれることもあります。

**LSP**：ラベルスイッチド パス。2 つのルータ間に設定された接続。この接続では、パケットを伝送するためにラベル スイッチングが使用されます。LSP の目的は、データ パケットを伝送することです。

**MPLS**：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ネットワーク コアにおいて使用されるパケット転送テクノロジー。これにより、スイッチング ノードにデータの転送方法を指示するためのデータ リンク層ラベルが適用されるため、ネットワーク層ルーティングで通常行われる転送よりも高速でスケーラブルな転送が行われます。

**NHOP**：ネクスト ホップ。LSP のパス上の次のダウンストリーム ノード。

**NHOPバックアップトンネル**：ネクストホップ バックアップ トンネル。障害ポイントの先にある LSP のネクスト ホップで終端し、障害ポイントのすぐアップストリームにあるホップを起点とするバックアップ トンネル。このバックアップ トンネルは、障害の発生したリンクをバイパスし、障害発生前にこのリンクを使用していたプライマリ LSP を保護するために使用されます。

**NNHOP**：Next-Next HOP（ネクストネクスト ホップ）。LSP のパス上の次のダウンストリーム ノードの後ろのノード。

**NNHOPバックアップトンネル**：ネクストホップから 1 つめのホップのバックアップ トンネル。障害ポイントの先にある LSP のネクストネクスト ホップで終端し、障害ポイントのすぐアップストリームにあるホップを起点とするバックアップ トンネル。このバックアップ トンネルは、障害の発生したリンクまたはノードをバイパスし、障害発生前にこのリンクまたはノードを使用していたプライマリ LSP を保護するために使用されます。

**ノード**：ネットワーク接続のエンドポイント、つまりネットワーク内の複数の回線に共通する接合部。複数のノードをリンクで相互接続することができます。これらのノードは、ネットワーク内のコントロール ポイントとなります。ネットワーク接続のエンドポイント、つまりネットワー

ク内の複数の回線に共通する接合部。ノードは、プロセッサ、コントローラ、またはワークステーションです。

**プライマリLSP**：当初、障害発生前に保護インターフェイスを介してシグナリングされていた最後の LSP。障害の前の LSP。

**プライマリトンネル**：障害が発生した場合に高速リルートされる LSP に割り当てられたトンネル。バックアップ トンネルをプライマリ トンネルにすることはできません。

**保護インターフェイス**：1 つ以上のバックアップ トンネルが関連付けられたインターフェイス。

**冗長性**：デバイス、サービス、または接続を重複させて、障害発生時に、冗長なデバイス、サービス、または接続が、障害が発生したこれらの作業を実行できるようにすること。

**RSVP**：Resource Reservation Protocol（リソース予約プロトコル）。カスタマーがインターネットサービスのために要求をシグナリング（予約をセットアップ）する際に使用する IETF プロトコル。これにより、カスタマーはそのネットワーク部分を経由してデータを伝送することを許可されます。

**ステート**：ルータが各 LSP に関して保守する必要のある情報。この情報は、トンネルをリルートする場合に使用されます。

**サブプール**：MPLS トラフィック エンジニアリングのリンクまたはノードにおける、より限定的な帯域幅。サブプールは、リンクまたはノードの全体的なグローバル プール帯域幅の一部です。

**テールエンド**：LSP が終端するルータ。これは、LSP のパス上の最後のルータです。

**トンネル**：2 つのピア間（2 台のルータ間など）のセキュアな通信パス。

第 7 章

# MPLS トラフィック エンジニアリング（TE）：IP 明示アドレス除外

MPLS トラフィック エンジニアリング（TE）- IP 明示アドレス除外機能は、マルチプロトコル ラベル スイッチング（MPLS）の TE ラベル スイッチド パス（LSP）のパスからリンクまたはノードを除外する手段を提供します。

この機能を有効にするには、**ipexplicit-path** コマンドを使用します。このコマンドにより、IP 明示パスを作成し、パスを指定するためのコンフィギュレーション サブモードを開始できます。この機能により、サブモード コマンドに、パスから除外するアドレスを指定するための **exclude-address** コマンドが追加されます。

MPLS TE LSP の除外アドレスが、フラッディングされたリンクを識別している場合、Constraint-based Shortest Path First（CSPF）ルーティング アルゴリズムでは、LSP のパスの計算時にそのリンクが考慮されません。除外アドレスが、フラッディングされた MPLS TE ルータ ID を指定している場合、CSPF ルーティング アルゴリズムでは、LSP のパスがルータ ID で識別されるノードを経由することが許可されません。

# 機能情報の確認

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

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、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。

# MPLS トラフィック エンジニアリング（TE）：IP 明示アドレス除外の前提条件

IP 明示アドレス除外をサポートするには、ネットワークで次の Cisco IOS XE 機能がサポートされている必要があります。

- MPLS
- IP シスコ エクスプレス フォワーディング
- Intermediate System-to-Intermediate System（IS-IS）または Open Shortest Path First（OSPF）

# MPLS トラフィック エンジニアリング（TE）：IP 明示アドレス除外の制約事項

MPLS TE は、**exclude-address** コマンドで設定されたすべての除外アドレスか、**next-address** コマンドで設定されたすべての包含アドレスのいずれか（両方の組み合わせではない）で構成された IP 明示パスを受け入れます。

# MPLS トラフィック エンジニアリング（TE）：IP 明示アドレス除外の概要

## MPLS トラフィック エンジニアリング

MPLSは、インターネット技術特別調査委員会（IETF）により指定されたフレームワークであり、ネットワークを介するトラフィック フローの効率的な指定、ルーティング、フォワーディング、

およびスイッチングを可能にします。MPLS はラベルを使用して IP トラフィックを転送する方法の 1 つです。このラベルによって、ネットワーク内のルータおよびスイッチが、事前に確立された IP ルーティング情報に基づくパケットの転送先を指示されます。

トラフィックエンジニアリング（TE）は、ハイプライオリティのトラフィックに常に十分な帯域幅が確保されるように、帯域割り当てを調整するプロセスです。

MPLS TE では、上流のルータが特定のトラフィック ストリームのネットワーク トンネルを作成してから、そのトンネルに使用可能な帯域幅を修正します。

## Cisco Express Forwarding; シスコ エクスプレス フォワーディング

シスコ エクスプレス フォワーディングは、ルータ内部の高度なレイヤ 3 スイッチング テクノロジーです。これにより、Cisco ルータが入力インターフェイスから出力インターフェイスにパケットを転送するときに使用する最速の方法が定義されます。**ip cef** コマンドを使用すると、Cisco Express Forwarding がグローバルに有効になります。**ip route-cache cef** コマンドを使用すると、インターフェイス上で Cisco Express Forwarding が有効になります。

# MPLS トラフィック エンジニアリング（TE）：IP 明示アドレス除外の設定方法

## IP 明示アドレス除外の設定

### 手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipexplicit-path** {**name** *path-name* | **identifier** *number*} [**enable** | **disable**]
4. **exclude-address***ip-address*
5. **exit**
6. **exit**
7. **showipexplicit-path**

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化 | 特権 EXEC モードをイネーブルにします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | 例：<br>`Router> enable` | • パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br>例：<br>`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 | **ipexplicit-path** {**name** *path-name* \| **identifier** *number*} [**enable** \| **disable**]<br>例：<br>`Router(config)# ip explicit-path name OmitR12` | 明示パスの名前または番号を指定し、パスをイネーブルにして、明示パス コンフィギュレーション モードに切り替えます。 |
| ステップ 4 | **exclude-address***ip-address*<br>例：<br>`Router(cfg-ip-expl-path)# exclude-address 10.12.12.12` | 指定したリンクまたはノードを、コンストレイントベースの SPF による考慮から除外します。<br>• *ip-address* は、ノードのリンク アドレスまたはルータ ID です。 |
| ステップ 5 | **exit**<br>例：<br>`Router(cfg-ip-expl-path)# exit` | 明示パス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 6 | **exit**<br>例：<br>`Router(config)# exit` | 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 7 | **showipexplicit-path**<br>例：<br>`Router# show ip explicit-path` | 設定した IP 明示パスの情報を表示します。 |

# MPLS トラフィック エンジニアリング トンネルの設定

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipunnumberedloopback0**
5. **tunneldestination***ip-address*
6. **tunnelmodemplstraffic-eng**
7. **tunnelmplstraffic-engbandwidth***bandwidth*
8. **tunnelmplstraffic-engpath-option***number* {**dynamic** | **explicit** {**name** *path-name* | **ID** *path-number*}} [*lockdown*]
9. **exit**
10. **exit**
11. **showmplstrafficengtunnels**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **interfacetunnel***number*<br><br>例：<br><br>`Router(config)# interface tunnel11` | インターフェイスタイプを設定し、インターフェイスコンフィギュレーション モードを開始します。 |
| ステップ 4 | **ipunnumberedloopback0**<br><br>例：<br><br>`Router(config-if)# ip unnumbered loopback0` | トンネルインターフェイスにIPアドレスを割り当てます。<br><br>• MPLS トラフィック エンジニアリング トンネル インターフェイスは単一方向リンクを表すため、番号なしにする必要があります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **tunneldestination***ip-address*<br><br>例：<br><br>`Router(config-if)# tunnel destination 10.11.11.11` | トンネルの宛先を指定します。<br><br>• トンネルの宛先は、宛先デバイスの MPLS トラフィック エンジニアリング ルータ ID にする必要があります。 |
| ステップ 6 | **tunnelmodemplstraffic-eng**<br><br>例：<br><br>`Router(config-if)# tunnel mode mpls traffic-eng` | トンネル カプセル化モードを MPLS トラフィック エンジニアリングに設定します。 |
| ステップ 7 | **tunnelmplstraffic-engbandwidth***bandwidth*<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng bandwidth 100` | MPLS トラフィック エンジニアリング トンネルの帯域幅を設定します。 |
| ステップ 8 | **tunnelmplstraffic-engpath-option***number* {**dynamic** \| **explicit** {**name** *path-name* \| **ID** *path-number*}} [*lockdown*]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 2 dynamic` | 指定した IP 明示パス、またはトラフィック エンジニアリング トポロジデータベースからダイナミックに計算されたパスを使用するように、トンネルを設定します。<br><br>• 明示パスが使用可能でない場合は、ダイナミック パスが使用されます。<br><br>（注） 除外アドレスを指定するパス オプションを設定するには、（**dynamic** キーワードではなく）**explicit** キーワードを指定し、「IP 明示アドレス除外の設定，（201 ページ）」の項の手順に従って設定した IP 明示パスを指定します。 |
| ステップ 9 | **exit**<br><br>例：<br><br>`Router(config-if)# exit` | インターフェイス 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 | **exit**<br><br>例：<br><br>`Router(config)# exit` | 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 11 | **showmplstrafficengtunnels**<br><br>例：<br><br>`Router# show mpls traffic eng tunnels` | トンネルの情報（トンネルが動作中であれば現在のトンネル パスを含む）を表示します。<br><br>• コマンド出力を参照すると、トンネルの構築に使用されたパスを判断できます。**exclude-address** コマンドを入力した場合、指定したリンクまたはノードは表示されません。 |

# MPLS トラフィック エンジニアリング（TE）：IP 明示アドレス除外の設定例

## 例：IP 明示アドレス除外の設定

次に、2 つのパス オプションを使用して MPLS TE トンネルを設定する例を示します。1 つは除外アドレスを使用した優先的な明示パスで、もう 1 つはバックアップのダイナミック パスです。

OmitR12 という名前の IP 明示パスを設定します。これにより、ルータ ID が 10.12.12.12 のルータが除外されます。

```
ip explicit-path name OmitR12
exclude-address 10.12.12.12
   Explicit Path name OmitR12:
   1: exclude-address 10.12.12.12
exit
```

明示パスの設定を確認するには、**show ip explicit-path** コマンドを使用します。

```
show ip explicit-paths name OmitR12
PATH OmitR12 (loose source route, path complete, generation 3)
 1: exclude-address 10.12.12.12
```

（注） ネットワーク内の LSR（ノード）のルータ ID がわかっている必要があります。この例では、その 10.12.12.12 がルータ ID です。この ID がわからない場合、指定したアドレスがリンク ID の IP アドレスかルータ ID の IP アドレスかが不明になります。

# 例：MPLS トラフィック エンジニアリング トンネルの設定

次の例では、トンネル 11 を 2 つのオプションで設定します。優先されるパスオプションは IP 明示パスである OmitR2 です。

```
interface tunnel11
ip unnumbered loopback0
tunnel destination 10.11.11.11
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name OmitR12
tunnel mpls traffic-eng path-option 2 dynamic
```

（注） この他にも、TE トンネルのプロパティ（帯域幅やプライオリティなど）を設定するためのコマンドがあります。これらのコマンドの説明は、『Cisco IOS Multiprotocol Label Switching Command Reference』を参照してください。

# 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』 |
| MPLS コマンド | 『*Cisco IOS Multiprotocol Label Switching Command Reference*』 |
| MPLS 設定情報 | 『*Cisco IOS XE Multiprotocol Label Switching Configuration Guide*』 |

### 標準

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

### MIB

| MIB | MIB のリンク |
|---|---|
| この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。<br>http://www.cisco.com/go/mibs |

### RFC

| RFC | Title |
|---|---|
| この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC の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 | Link |
|---|---|
| ★枠で囲まれた Technical Assistance の場合★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 |

# MPLS トラフィック エンジニアリング（TE）：IP 明示アドレス除外の機能情報

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 *10*：*MPLS* トラフィック エンジニアリング（*TE*）：*IP* 明示アドレス除外の機能情報**

| 機能名 | リリース | 機能の設定情報 |
|---|---|---|
| MPLS トラフィック エンジニアリング（TE）：IP 明示アドレス除外 | Cisco IOS XE Release 2.3 | MPLS トラフィック エンジニアリング（TE）：IP 明示アドレス除外機能は、マルチプロトコル ラベル スイッチング（MPLS）の TE ラベル スイッチドパス（LSP）のパスからリンクまたはノードを除外する手段を提供します。<br>この機能は、Cisco IOS XE Release 2.3 に統合されました。<br>この機能により、コマンド **exclude-address** が導入されました。 |

# 用語集

**シスコエクスプレスフォワーディング**：ルート参照情報を 1 つのルート キャッシュではなく複数のデータ構造に分けて保存することにより、ルータ内のパケットの転送を短時間で行うための手段。

**IP明示パス**：IP アドレスのリスト。それぞれの IP アドレスは明示パス内のノードまたはリンクを表します。

**リンク**：送信者と受信者の間の回線または伝送パスおよびすべての関連装置からなるネットワーク通信チャネル。回線または伝送リンクと呼ばれることもあります。

**MPLS**：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ラベルを使用して IP トラフィックを転送するスイッチング方式。このラベルによって、ネットワーク内のルータおよびスイッチが、事前に確立された IP ルーティング情報に基づくパケットの転送先を指示されます。

**ノード**：ネットワーク接続のエンドポイント、つまりネットワーク内の複数の回線に共通する接合部。複数のノードをリンクで相互接続することができます。これらのノードは、ネットワーク内のコントロール ポイントとなります。

第 8 章

# MPLS トラフィック エンジニアリング：共有リスク リンク グループ

MPLS トラフィック エンジニアリング：共有リスク リンク グループ機能では、バックアップ トンネルが保護しているインターフェイスと同じ共有リスク リンク グループ（SRLG）にあるリンクの使用がバックアップ トンネルによって回避されるようにバックアップ トンネル パス選択が拡張されます。

SRLG は、ネットワーク内のリンクが共通のファイバ（または共通の物理属性）を共有する状況を意味します。1 つのリンクに障害が発生すると、グループ内の他のリンクでも障害が発生する可能性があります。グループ内のリンクには共有リスクがあります。



## 機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモ

ジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、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。

# MPLS トラフィック エンジニアリング：共有リスク リンク グループの前提条件

- Fast Reroute が可能なトンネルを設定する必要があります。
- 自動トンネル バックアップをイネーブルにする必要があります。

# MPLS トラフィック エンジニアリング：共有リスク リンク グループの制約事項

- バックアップ トンネルは単一エリア内にある必要があります。
- 手動で作成したバックアップ トンネルでは、保護インターフェイスの SRLG は自動的に回避されません。
- 指定した SRLG に属するリンクを回避するようにプライマリ トンネルを指定することはできません。

# MPLS トラフィック エンジニアリング：共有リスク リンク グループに関する情報

## MPLS トラフィック エンジニアリングの概要

マルチプロトコル ラベル スイッチング（MPLS）は、インターネット技術特別調査委員会（IETF）により指定されたフレームワークであり、ネットワークを介するトラフィック フローの効率的な指定、ルーティング、フォワーディング、およびスイッチングを可能にします。

トラフィック エンジニアリング（TE）は、ハイプライオリティのトラフィックに常に十分な帯域幅が確保されるように、帯域割り当てを調整するプロセスです。

MPLS TE では、上流のルータが特定のトラフィック ストリームのネットワーク トンネルを作成してから、そのトンネルに使用可能な帯域幅を修正します。

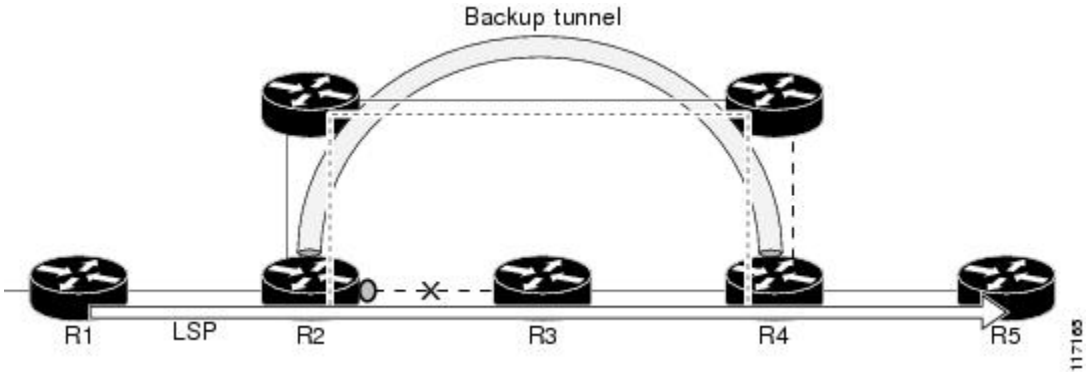
# MPLS トラフィック エンジニアリング：共有リスク リンク グループ

SRLG は、ネットワーク内のリンクが共通のファイバ（または共通の物理属性）を共有する状況を意味します。1 つのリンクに障害が発生すると、グループ内の他のリンクでも障害が発生する可能性があります。グループ内のリンクには共有リスクがあります。

バックアップ トンネルでは、保護しているインターフェイスと同じ SRLG 内のリンクの使用を回避する必要があります。そうしないと、保護対象のリンクに障害が発生した場合にバックアップ トンネルでも障害が発生します。

次の図に、ルータ R1 からルータ R5 へのプライマリ ラベル スイッチド パス（LSP）を示します。LSP により、R4 へのバックアップ トンネルを介して R2 の R2-R3 リンクの障害から保護されます。R2-R3 リンクに障害が発生した場合は、リンク保護によって LSP がバックアップ トンネルにリルートされます。ただし、R2-R3 リンクとバックアップ トンネル リンクの 1 つが同じ SRLG にあります。このため、R2-R3 リンクに障害が発生した場合は、バックアップ トンネルにも障害が発生する可能性があります。

**図 *26*：保護しているインターフェイスと同じ *SRLG* にあるバックアップ トンネル**




MPLS TE SRLG 機能では、バックアップ トンネルが保護しているインターフェイスと同じ SRLG にあるリンクの使用を回避できるようにバックアップ トンネル パス選択が拡張されます。

バックアップ トンネルが保護インターフェイスの SRLG を回避するには、次の 2 つの方法があります。

- 保護インターフェイスの SRLG を回避しないかぎり、ルータがバックアップ トンネルを作成しない。
- ルータは、保護インターフェイスの SRLG の回避を試みるが、それが可能でない場合はルータによってバックアップ トンネルが作成される。この場合は、2 つの明示パスがあります。最初のパスでは、保護インターフェイスの SRLG の回避が試行されます。回避できない場合は、バックアップ トンネルによって 2 番めのパス（これは SRLG を無視します）が使用されます。

（注） ルータが自動的に作成するバックアップ トンネル（自動トンネル バックアップと呼ばれます）だけが、保護インターフェイスの SRLG を回避できます。これらのバックアップ トンネルの詳細については、MPLS TE SRLG の自動トンネル バックアップ，（214 ページ）を参照してください。

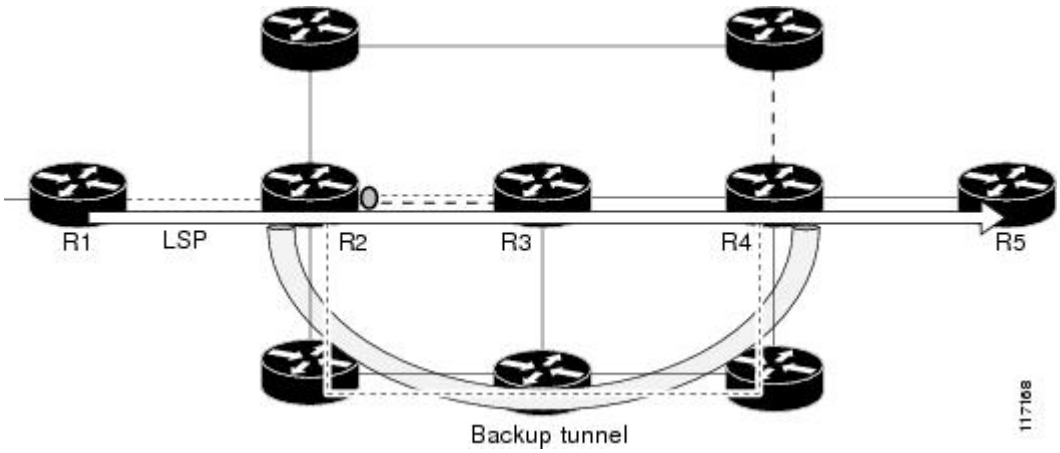
MPLS TE SRLG 機能をアクティブにするには、次の操作を実行する必要があります。

- 別のリンクとの共有リスクを持つ各リンクの SRLG メンバーシップを設定する。
- 保護インターフェイスの SRLG を回避するバックアップ トンネルを自動的に作成するようにルータを設定する。

設定手順の詳細な説明については、MPLS トラフィック エンジニアリング：共有リスク リンク グループの設定方法，（216 ページ）を参照してください。

Open Shortest Path First（OSPF）と Intermediate System-to-Intermediate System（IS-IS）は、SRLG メンバーシップ情報（帯域幅のアベイラビリティやアフィニティなどの他の TE リンク属性を含む）をフラッディングして、ネットワーク内のすべてのルータに各リンクの SRLG 情報があるようにします。このトポロジ情報を使用して、ルータは保護インターフェイスと共通の SRLG を持つリンクを除外するバックアップ トンネルパスを計算できます。次の図に示すように、バックアップ トンネルは、保護インターフェイスと SRLG を共有する R2 と R3 間のリンクを回避します。

**図 *27*：保護インターフェイスの *SRLG* を回避するバックアップ トンネル**



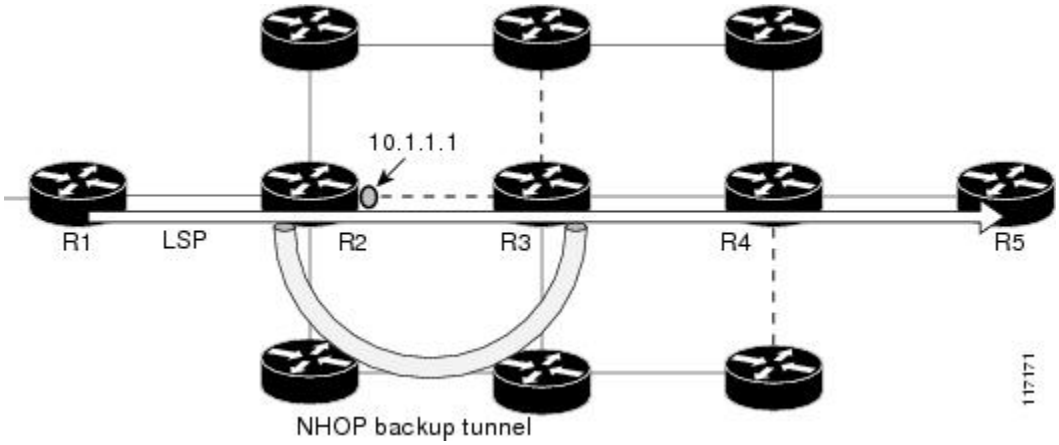

# MPLS TE SRLG の高速リルート保護

高速再ルーティング（FRR）は、障害ポイントで LSP をローカルに修復することにより、リンクとノードの障害から MPLS TE LSP を保護します。この保護により、ヘッドエンド ルータが自身を置換するための新しいエンドツーエンドの LSP を確立しようとしている間、LSP 上でのデータのフローを継続できます。FRR は、障害が発生したリンクまたはノードをバイパスするバックアッ

プ トンネルを介して再ルーティングすることによって、保護されている LSP をローカルに修復します。

LSP のパスの単一リンクだけをバイパスするバックアップ トンネルが、リンク保護を提供します。パス上のリンクに障害が発生した場合、バックアップ トンネルは、LSP のトラフィックをネクスト ホップにリルートする（障害の発生したリンクをバイパスする）ことによって LSP を保護します。これらは、障害ポイントの向こう側にある LSP のネクスト ホップで終端するため、ネクスト ホップ（NHOP）バックアップ トンネルと呼ばれます。次の図は、NHOP バックアップ トンネルを示しています。

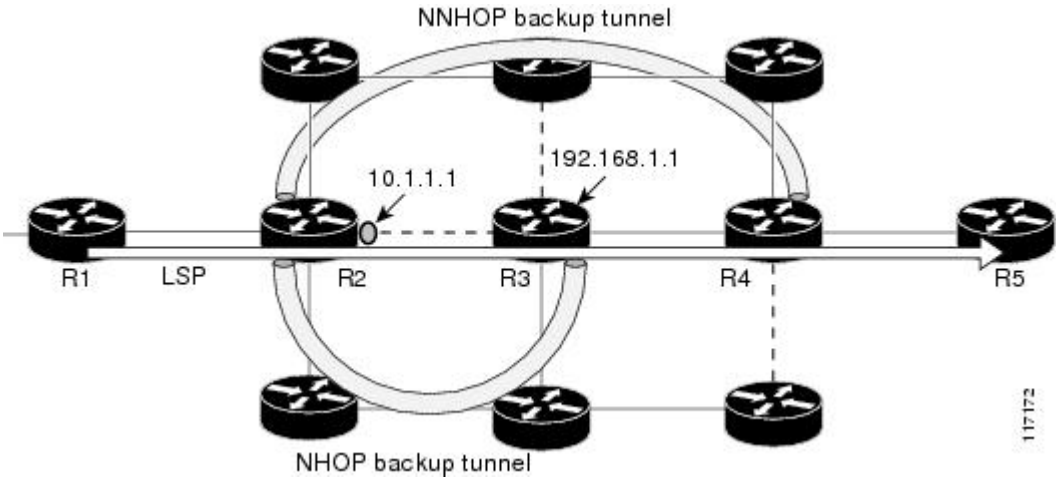
**図 *28*：*NHOP* バックアップ トンネル**




FRR により、LSP に対するノード保護が提供されます。LSP パス上のネクストホップ ノードをバイパスするバックアップ トンネルは、LSP パスのネクストホップ ノードの次のノードで終端して、結果としてネクストホップ ノードをバイパスするため、ネクストネクストホップ（NNHOP）バックアップ トンネルと呼ばれます。LSP パス上のノードに障害が発生した場合は、NNHOP バックアップ トンネルが LSP を保護します。具体的には、障害のアップストリームにあるノードをイネーブルにして、障害の発生したノードの周囲の LSP とそのトラフィックをネクストネクストホップにリルートします。FRR では、ノード障害を短時間で検出できるように、リソース予約プロトコル（RSVP）hello の使用がサポートされています。また、NNHOP バックアップ トンネルは、障害の発生したリンクおよびノードをバイパスするため、リンク障害からの保護も提供しています。

次の図は、NNHOP バックアップ トンネルを示しています。

**図 29：*NNHOP* バックアップ トンネル**




# MPLS TE SRLG の自動トンネル バックアップ

自動トンネルバックアップは、バックアップ トンネルを自動的に作成するルータの機能です。したがって、各バックアップ トンネルを事前に設定し、バックアップ トンネルを保護インターフェイスに割り当てる必要はありません。自動的に作成されたバックアップ トンネルだけが、SRLG または保護インターフェイスを回避できます。

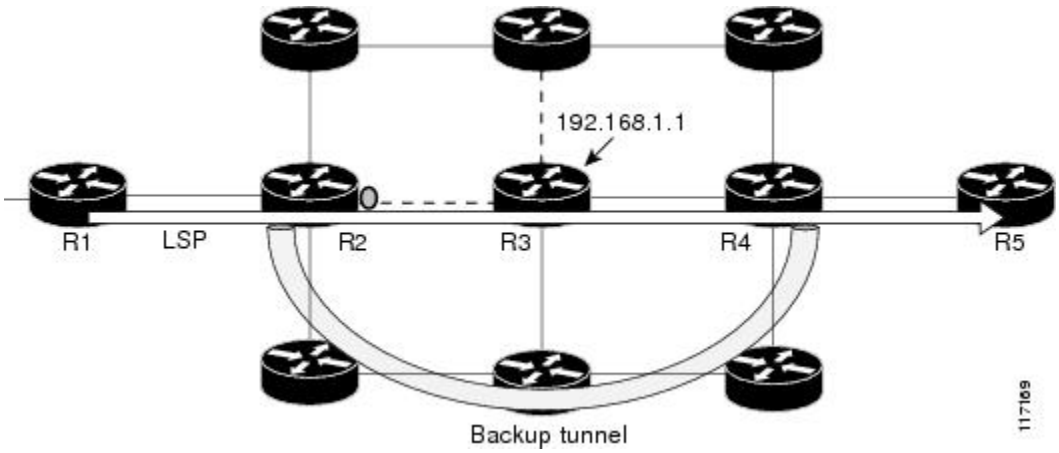
バックアップ トンネルの詳細については、MPLS TE SRLG の高速リルート保護，（212 ページ）を参照してください。

自動トンネルバックアップの詳細およびデフォルトのコマンド値の変更方法については、『MPLS Traffic Engineering (TE)--AutoTunnel Primary and Backup』を参照してください。

自動トンネル バックアップ機能をグローバルにアクティブにするには、**mplstraffic-engauto-tunnelbackup** コマンドを入力します。

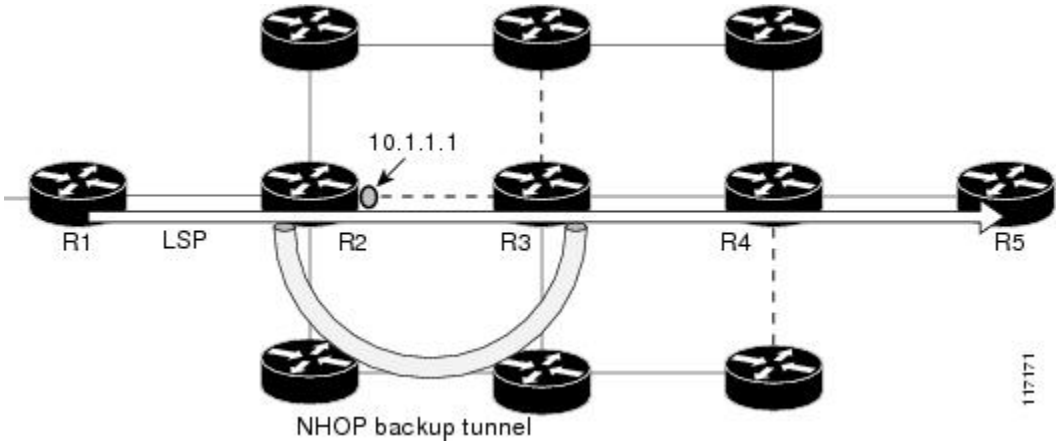
次の図に、ルータ 192.168.1.1 を除外し、ルータ R4 で終端する NNHOP 自動生成バックアップ トンネルを示します。バックアップ トンネルでは、192.168.1.1 のリンクへの接触を回避する必要があります。

**図 *30*：*NNHOP* の自動トンネル バックアップ**




次の図に、ルータ R3 で終端し、ノード全体ではなくリンク 10.1.1.1 を回避する NHOP 自動生成バックアップ トンネルを示します。

**図 *31*：*NHOP* の自動トンネル バックアップ**




（注） NNHOP では、ルータ ID が除外されます（ルータ全体を除外する必要があります。つまり、ルータのどのリンクもバックアップ トンネルのパスに含めることができません）。NHOP では、バックアップ トンネルのパスの計算時にだけリンクが除外されます。

# MPLS トラフィック エンジニアリング：共有リスク リンク グループの設定方法

## 別のリンクとの共有リスクを持つ各リンクの MPLS TE SRLG メンバーシップの設定

別のリンクとの共有リスクを持つ各リンクの MPLS TE SRLG メンバーシップを設定するには、次の作業を実行します。SRLG メンバーシップを設定することで、バックアップ トンネルが保護しているインターフェイスと同じ SRLG にあるリンクの使用がバックアップ トンネルによって回避されるようにバックアップ トンネル パス選択が拡張されます。

物理インターフェイスでコマンドを入力します。

### 手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typeslot/port*
4. **mpls traffic-eng srlg** [*number*] [
5. **mpls traffic-eng srlgend**

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• 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**<br><br>例：<br><br>`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***typeslot/port*<br><br>例：<br><br>`Router(config)# interface pos 1/1/1` | 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。<br><br>• *type* 引数で、設定するインターフェイスのタイプを指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • *slot* 引数はスロット番号です。スロット情報およびポート情報については、該当するハードウェア マニュアルを参照してください。<br>• **/Port***port* 引数はポート番号です。スロット情報およびポート情報については、該当するハードウェア マニュアルを参照してください。スラッシュ（/）が必要です。 |
| ステップ 4 | **mpls traffic-eng srlg** [*number*] [<br><br>例：<br><br>`Router(config-if)# mpls traffic-eng srlg 5` | リンク（インターフェイス）の SRLG メンバーシップを設定します。<br>• *number* 引数は SRLG ID です。有効な値は 0 ～ 4,294,967,295 です。<br><br>（注） リンクを複数の SRLG のメンバにするには、**mplstraffic-engsrlg** コマンドを複数回入力します。 |
| ステップ 5 | **mpls traffic-eng srlgend**<br><br>例：<br><br>`Router(config-if)# end` | 特権 EXEC モードに戻ります。 |

# MPLS TE SRLG を回避するためにバックアップ トンネルを自動的に作成するルータを設定

保護インターフェイスの MPLS TE SRLG を回避するためにバックアップ トンネルを自動的に作成するルータを設定するには、次の作業を実行します。バックアップ トンネルは、ネクストホップにトラフィックをリルートして障害のあるリンクをバイパスするか、この例のように SRLG を回避することにより、リンク保護を提供します。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplstraffic-engauto-tunnelbackupsrlgexclude** [**force** | **preferred**]
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 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **mplstraffic-engauto-tunnelbackupsrlgexclude** [**force** \| **preferred**]<br><br>例：<br><br>`Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude force` | 自動作成されたバックアップ トンネルが保護インターフェイスの SRLG を回避する必要があることを指定します。<br><br>• **force** キーワードでは、バックアップ トンネルに対して、1 つまたは複数の保護インターフェイスの SRLG を回避するよう強制します。<br><br>• **preferred** キーワードを指定すると、バックアップ トンネルは、1 つまたは複数の保護インターフェイスの SRLG の回避を試みますが、SRLG を回避できない場合はバックアップ トンネルを作成できます。 |
| ステップ 4 | **end**<br><br>例：<br><br>`Router(config)# end` | 特権 EXEC モードに戻ります。 |

# MPLS トラフィック エンジニアリング共有リスク リンク グループの設定の検証

## 手順の概要

1. イネーブル化
2. **show running-config**
3. **show mpls traffic-eng link-management interfaces***interfaceslot*/*port*
4. **show mpls traffic-eng topology**
5. **show mpls traffic-eng topology srlg**
6. **show mpls traffic-eng topology brief**
7. **show mpls traffic-eng link-management advertisements**
8. **show ip rsvp fast-reroute**
9. **mpls traffic-eng auto-tunnel backup srlg exclude force**
10. **show ip explicit-paths**
11. **show mpls traffic-eng tunnels tunnel***num*
12. **mpls traffic-eng auto-tunnel backup srlg exclude preferred**
13. **show ip explicit-paths**
14. **show ip rsvp fast-reroute**
15. **exit**

## 手順の詳細

**ステップ 1** イネーブル化

このコマンドを使用して、特権EXECモードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。次に例を示します。

例：

```
Router> enable
Router#
```

**ステップ 2** **show running-config**

次のコマンドを使用して、インターフェイス pos 1/3/1 の SRLG メンバーシップを設定し、設定が想定どおりであることを確認します。次に例を示します。

例：

```
Router# configure terminal
Router(config)# interface pos 1/3/1
Router(config-if)# mpls traffic-eng srlg 1
Router(config-if)# mpls traffic-eng srlg 2
Router(config-if)# end
Router# show running-config
```

```
interface POS 1/3/1
 ip address 10.0.0.33 255.255.255.255
 no ip directed-broadcast
 ip router isis
 encapsulation ppp
 no ip mroute-cache
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel5000
 mpls traffic-eng srlg 1
 mpls traffic-eng srlg 2
 tag-switching ip
 crc 32
 clock source internal
 pos ais-shut
 pos report rdool
 pos report lais
 pos report lrdi
 pos report pais
 pos report prdi
 pos report sd-ber
 isis circuit-type level-2-only
 ip rsvp bandwidth 20000 20000 sub-pool 5000
```

これにより、Packet over SONET（POS）インターフェイス pos 1/3/1 に SRLG 1 および SRLG 2 が関連付けられていることを検証します。

**ステップ 3** **show mpls traffic-eng link-management interfaces***interfaceslot/port*

このコマンドを使用して、インターフェイス pos 1/3/1 に設定されている SRLG メンバーシップを表示します。次に例を示します。

例：

```
Router# show mpls traffic-eng link-management interfaces pos 1/3/1
System Information::
    Links Count:         11
Link ID:: PO1/3/1 (10.0.0.33)
    Link Status:
      SRLGs:               1 2
      Physical Bandwidth:  2488000 kbits/sec
      Max Res Global BW:   20000 kbits/sec (reserved:0% in, 0% out)
      Max Res Sub BW:      5000 kbits/sec (reserved:0% in, 0% out)
      MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
      Inbound Admission:   allow-all
      Outbound Admission:  allow-if-room
      Admin. Weight:       10 (IGP)
      IGP Neighbor Count:  1
      IGP Neighbor:        ID 0000.0000.0004.00, IP 10.0.0.34 (Up)
    Flooding Status for each configured area [1]:
      IGP Area[1]: isis  level-2: flooded
```

**ステップ 4** **show mpls traffic-eng topology**

このコマンドを使用して、Interior Gateway Protocol（IGP）を介してフラッディングされる SRLG リンクメンバーシップを表示します。次に例を示します。

例：

```
Router# show mpls traffic-eng topology

My_System_id:0000.0000.0003.00 (isis  level-2)
Signalling error holddown:10 sec Global Link Generation 9
IGP Id:0000.0000.0003.00, MPLS TE Id:10.0.3.1 Router Node  (isis
level-2)
```

```
      link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0004.00,
nbr_node_id:2, gen:9
          frag_id 0, Intf Address:10.0.0.33, Nbr Intf Address:10.0.0.34
          TE metric:10, IGP metric:10, attribute_flags:0x0
          SRLGs:1 2
          physical_bw:2488000 (kbps), max_reservable_bw_global:20000
(kbps)
          max_reservable_bw_sub:5000 (kbps)
                                Global Pool       Sub Pool
               Total Allocated  Reservable        Reservable
               BW (kbps)        BW (kbps)         BW (kbps)
               ---------------  -----------       ----------
        bw[0]:           0            20000             5000
        bw[1]:           0            20000             5000
        bw[2]:           0            20000             5000
        bw[3]:           0            20000             5000
        bw[4]:           0            20000             5000
        bw[5]:           0            20000             5000
```

**ステップ 5** **show mpls traffic-eng topology srlg**

このコマンドを使用して、指定されたSRLGのメンバであるネットワーク内のすべてのリンクを表示します。次に例を示します。

例：

```
Router# show mpls traffic-eng topology srlg
MPLS TE Id:0000.0000.0003.00 (isis  level-2)
  SRLG:1
     10.0.0.33
  SRLG:2
     10.0.0.33
```

次のコマンドでは、SRLG 1 に 2 つのリンクがあることが表示されます。

例：

```
Router# show mpls traffic-eng topology srlg
MPLS TE Id:0000.0000.0003.00 (isis  level-2)
  SRLG:1
     10.0.0.33
     10.0.0.49
```

**ステップ 6** **show mpls traffic-eng topology brief**

このコマンドを使用して、短いトポロジ情報を表示します。

例：

```
Router# show mpls traffic-eng topology brief
My_System_id:0000.0000.0003.00 (isis  level-2)
Signalling error holddown:10 sec Global Link Generation 9
IGP Id:0000.0000.0003.00, MPLS TE Id:10.0.3.1 Router Node  (isis
level-2)
      link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0004.00,
nbr_node_id:2, gen:9
          frag_id 0, Intf Address:10.0.0.33, Nbr Intf Address:10.0.0.34
          TE metric:10, IGP metric:10, attribute_flags:0x0
          SRLGs:1 2
```

**ステップ 7** **show mpls traffic-eng link-management advertisements**

このコマンドで、MPLS-TE リンク管理によってグローバル TE トポロジに現在フラッディングされているローカル リンク情報を表示します。次に例を示します。

例：

```
Router# show mpls traffic-eng link-management advertisements

Flooding Status:      ready
Configured Areas:     1
IGP Area[1] ID::  isis  level-2
  System Information::
    Flooding Protocol:    ISIS
  Header Information::
    IGP System ID:        0000.0000.0003.00
    MPLS TE Router ID:    10.0.3.1
    Flooded Links:        2
  Link ID::  0
    Link Subnet Type:     Point-to-Point
    Link IP Address:      10.0.0.49
    IGP Neighbor:         ID 0000.0000.0007.00, IP 10.0.0.50
    TE metric:            80000
    IGP metric:           80000
    SRLGs:                None
    Physical Bandwidth:   622000 kbits/sec
    Res. Global BW:       20000 kbits/sec
    Res. Sub BW:          5000 kbits/sec
    Downstream::
                                 Global Pool   Sub Pool
                                 -----------   --------------
      Reservable Bandwidth[0]:  20000         5000 kbits/sec
      Reservable Bandwidth[1]:  20000         5000 kbits/sec
      Reservable Bandwidth[2]:  20000         5000 kbits/sec
      Reservable Bandwidth[3]:  20000         5000 kbits/sec
      Reservable Bandwidth[4]:  20000         5000 kbits/sec
      Reservable Bandwidth[5]:  20000         5000 kbits/sec
      Reservable Bandwidth[6]:  20000         5000 kbits/sec
      Reservable Bandwidth[7]:  20000         5000 kbits/sec
    Attribute Flags:      0x00000000
  Link ID::  1
    Link Subnet Type:     Point-to-Point
    Link IP Address:      10.0.0.33
    IGP Neighbor:         ID 0000.0000.0004.00, IP 10.0.0.34
    TE metric:            10
    IGP metric:           10
    SRLGs:                1
    Physical Bandwidth:   2488000 kbits/sec
    Res. Global BW:       20000 kbits/sec
    Res. Sub BW:          5000 kbits/sec
    Downstream::
                                 Global Pool   Sub Pool
                                 -----------   --------------
      Reservable Bandwidth[0]:  20000         5000 kbits/sec
      Reservable Bandwidth[1]:  20000         5000 kbits/sec
      Reservable Bandwidth[2]:  20000         5000 kbits/sec
      Reservable Bandwidth[3]:  20000         5000 kbits/sec
      Reservable Bandwidth[4]:  20000         5000 kbits/sec
      Reservable Bandwidth[5]:  20000         5000 kbits/sec
      Reservable Bandwidth[6]:  20000         5000 kbits/sec
      Reservable Bandwidth[7]:  20000         5000 kbits/sec
    Attribute Flags:      0x00000000
```

**ステップ 8** **show ip rsvp fast-reroute**

このコマンドを使用して、プライマリ トンネルが、SLRG 1 が設定されている R3 上の Pos1/3/1 を経由することを表示します。次に例を示します。

例：

```
Router# show ip rsvp fast-reroute
```

```
Primary    Protect      BW      Backup
Tunnel     I/F        BPS:Type  Tunnel:Label  State   Level   Type
-------    -------    --------  ------------  -----   -----   ----
R3-PRP_t0  PO1/3/1 0:G  None      None          None    None    None
```

**ステップ 9** **mpls traffic-eng auto-tunnel backup srlg exclude force**

次のコマンドを使用して、**force** キーワードで自動トンネル バックアップを設定します。次に例を示します。

例：

```
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude force
Router(config)# exit
```

**ステップ 10** **show ip explicit-paths**

次のコマンドを使用して、**force** キーワードが IP 明示パスから除外された pos1/3/1 リンクで設定されていることを確認します。次に例を示します。

例：

```
Router# show ip explicit-paths

PATH __dynamic_tunnel65436 (loose source route, path complete,
generation 24, status non-configured)
    1:exclude-address 10.0.0.33
    2:exclude-srlg    10.0.0.33
```

**ステップ 11** **show mpls traffic-eng tunnels tunnel***num*

次のコマンドを使用して、自動トンネルは設定されているがダウンしていることを表示します。ヘッドエンドルータにシグナリングする他のパスがなく、pos1/2/1 は同じ SRLG（SRLG 1）に属しているため使用できないことがダウンしている理由です。次に例を示します。

例：

```
Router# show mpls traffic-eng tunnels tunnel 65436
Name:R3-PRP_t65436                        (Tunnel65436) Destination:
10.0.4.1
  Status:
    Admin:up         Oper:down   Path:not valid   Signalling:Down
    path option 1, type explicit __dynamic_tunnel65436
  Config Parameters:
    Bandwidth:0        kbps (Global)  Priority:7  7   Affinity:
0x0/0xFFFF
    Metric Type:TE (default)
    AutoRoute: disabled  LockDown:disabled  Loadshare:0
bw-based
    auto-bw:disabled
  Shortest Unconstrained Path Info:
    Path Weight:10 (TE)
    Explicit Route:10.0.0.34 10.0.4.1
  History:
    Tunnel:
      Time since created:5 minutes, 29 seconds
    Path Option 1:
      Last Error:PCALC::No path to destination, 0000.0000.0004.00
```

**ステップ 12** **mpls traffic-eng auto-tunnel backup srlg exclude preferred**

次のコマンドでは、**preferred** キーワードを指定して自動トンネル バックアップを設定します。次に例を示します。

例：

```
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude preferred
Router(config)# exit
```

**ステップ 13 show ip explicit-paths**

次のコマンドでは、2 つの明示パスが表示されます。最初のパスでは、保護インターフェイスの SRLG が回避されます。2 番めのパスでは SRLG は回避されません。次に例を示します。

例：

```
Router# show ip explicit-paths

PATH __dynamic_tunnel65436 (loose source route, path complete,
generation 30, status non-configured)
    1:exclude-address 10.0.0.33
    2:exclude-srlg    10.0.0.33
PATH __dynamic_tunnel65436_pathopt2 (loose source route, path complete,
generation 33, status non-configured)
    1:exclude-address 10.0.0.33
```

**ステップ 14 show ip rsvp fast-reroute**

次のコマンドでは、SRLG を回避しない 2 番めのパス オプション（ステップ 10 を参照）を使用してプライマリ トンネルが自動トンネルバックアップで保護されていることが表示されます。次に例を示します。

例：

```
Router# show ip rsvp fast-reroute
Primary    Protect      BW      Backup
Tunnel     I/F        BPS:Type  Tunnel:Label  State   Level   Type
-------    -------    --------  ------------  -----   -----   ----
R3-PRP_t0  PO1/3/1 0:G  0:G       Tu65436:0     Ready   any-unl nhop
```

次のコマンドは、トンネル Tu65436 のパス オプションを表示します。

例：

```
Router# show mpls traffic-eng tunnels tunnel 65436
Name:R3-PRP_t65436                        (Tunnel65436) Destination:
10.0.4.1
  Status:
    Admin:up         Oper:up     Path:valid       Signalling:connected
    path option 2, type explicit __dynamic_tunnel65436_pathopt2 (Basis
for Setup, path weight 80020)
    path option 1, type explicit __dynamic_tunnel65436
  Config Parameters:
    Bandwidth:0        kbps (Global)  Priority:7  7   Affinity:
0x0/0xFFFF
    Metric Type:TE (default)
    AutoRoute: disabled  LockDown:disabled  Loadshare:0
bw-based
    auto-bw:disabled
  Active Path Option Parameters:
    State:explicit path option 2 is active
```

```
    BandwidthOverride:disabled  LockDown:disabled  Verbatim:disabled
InLabel  : -
  OutLabel :POS1/2/1, 23
  RSVP Signalling Info:
       Src 10.0.3.1, Dst 10.0.4.1, Tun_Id 65436, Tun_Instance 3
    RSVP Path Info:
      My Address:10.0.3.1
      Explicit Route:10.0.0.50 10.0.0.66 10.0.0.113 10.0.4.1
      Record   Route:  NONE
      Tspec:ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
    RSVP Resv Info:
      Record   Route:  NONE
      Fspec:ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
  Shortest Unconstrained Path Info:
    Path Weight:10 (TE)
    Explicit Route:10.0.0.34 10.0.4.1
```

**ステップ 15** **exit**

このコマンドを使用して、ユーザ EXEC モードに戻ります。次に例を示します。

**例：**

```
Router# exit
Router>
```

# MPLS トラフィック エンジニアリング：共有リスク リンク グループの設定例

## 別のリンクとの共有リスクを持つ各リンクの SRLG メンバーシップの設定例

次の例では、各リンクの SRLG メンバーシップが別のリンクとの共有リスクを持つことを指定する方法を示します。

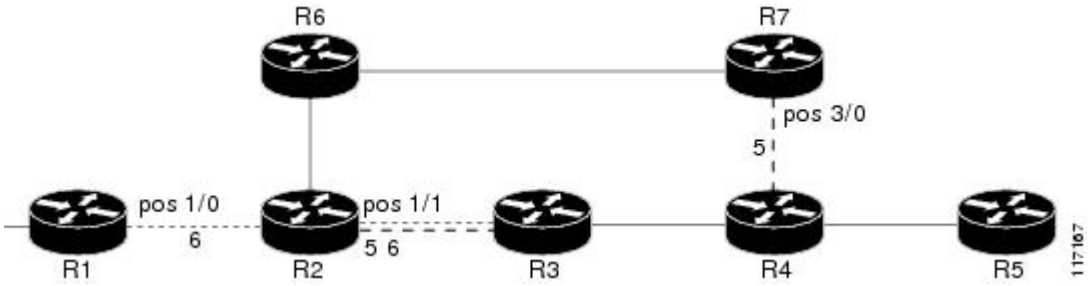
次の図と次のコマンドで示します。

- link R2-R3 = SRLG5
- link R2-R3 = SRLG6
- link R7-R4 = SRLG5
- link R1-R2 = SRLG6

```
Router1# configure terminal
Router1# interface pos 1/0
Router1(config-if)# mpls traffic-eng srlg 6

Router2# configure terminal
Router2# interface pos 1/1
```

```
Router2(config-if)# mpls traffic-eng srlg 5
Router2(config-if)# mpls traffic-eng srlg 6
Router7# configure terminal
Router7# interface pos 3/0
Router7(config-if)# mpls traffic-eng srlg 5
```

図 *32*：*SRLG* メンバーシップ




# SRLGを回避するためにバックアップトンネルを自動的に作成するルータを設定：例

次の例では、自動的に作成されるバックアップ トンネルに保護インターフェイスの SRLG の回避を強制することを指定する方法を示します。

```
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude force
```

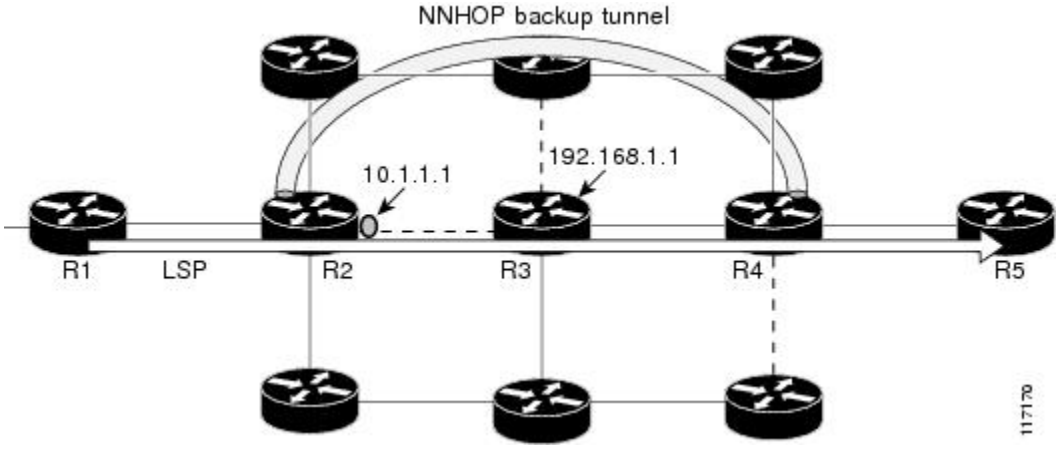
次の図は、以下の状態で保護インターフェイスの SRLG を防止するために自動作成される NNHOP バックアップトンネルを示します。

除外アドレスは 192.168.1.1 です。

R2 のリンクには IP アドレス 10.1.1.1 があります。

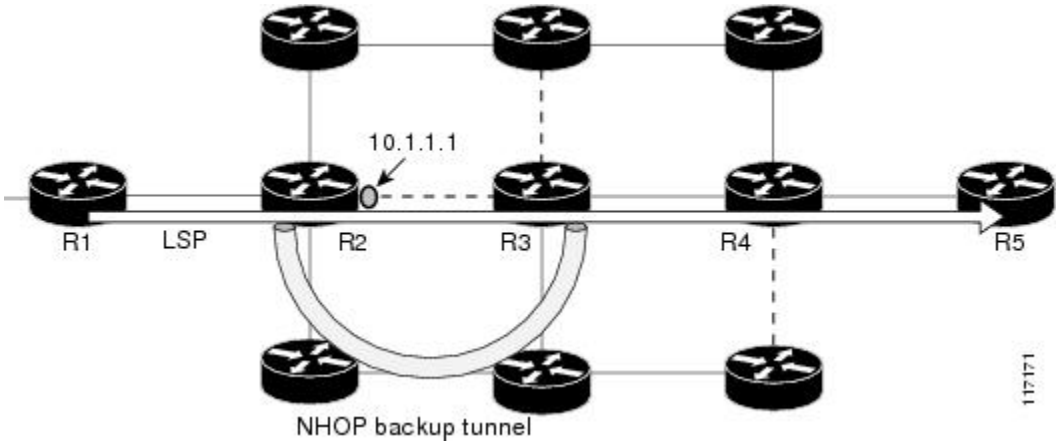
バックアップ トンネルの明示的なパスは、IP アドレスが 10.1.1.1 であるリンクなどとと同一の SRLG にメンバーシップをもつリンクを回避します。

**図 *33*：*srlg exclude force*：*NNHOP* 自動バックアップ トンネル**




次の図は、自動作成される NHOP バックアップトンネルを示しています。

**図 *34*：*srlg exclude force*：*NHOP* 自動バックアップ トンネル**




# 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 |
|---|---|
| 高速再ルーティング | 『MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)』 |

| 関連項目 | マニュアル タイトル |
|---|---|
| IS-IS | 『Integrated IS-IS Routing Protocol Overview』 |
| OSPF | 『Configuring OSPF』 |
| 自動トンネル バックアップ | 『MPLS Traffic Engineering AutoTunnel Primary and Backup』 |

### 標準

| 規格 | Title |
|---|---|
| なし | -- |

### MIB

| MIB | MIB のリンク |
|---|---|
| なし | 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。<br>http://www.cisco.com/go/mibs |

### RFC

| RFC | Title |
|---|---|
| draft-ietf-isis-gmpls-extensions-16.txt | *IS-IS Extensions in Support of Generalized MPLS* |

### シスコのテクニカル サポート

| 説明 | Link |
|---|---|
| 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。<br>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。<br>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/en/US/support/index.html |

# MPLS トラフィック エンジニアリング共有リスク リンク グループの機能情報

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 *11*：*MPLS* トラフィック エンジニアリング共有リスク リンク グループの機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| 『MPLS Traffic Engineering: Shared Risk Link Groups』 | 12.0(28)S<br>12.0(29)S<br>12.2(33)SRA<br>12.2(33)SXH<br>12.4(20)T<br>Cisco IOS XE Release 3.5S | |

| 機能名 | リリース | 機能情報 |
|---|---|---|
| | | MPLS トラフィック エンジニアリング：共有リスク リンク グループ機能では、バックアップ トンネルが保護しているインターフェイスと同じ共有リスク リンク グループ（SRLG）にあるリンクの使用がバックアップ トンネルによって回避されるようにバックアップ トンネル パス選択が拡張されます。<br><br>SRLG は、ネットワーク内のリンクが共通のファイバ（または共通の物理属性）を共有する状況を意味します。1 つのリンクに障害が発生すると、グループ内の他のリンクでも障害が発生する可能性があります。グループ内のリンクには共有リスクがあります。<br><br>このドキュメントでは、MPLS トラフィック エンジニアリング リスク共有リンクグループ機能の設定を説明します。<br><br>この機能は、12.0(28)S で導入されました。<br><br>12.0(29)S では、Open Shortest Path First（OSPF）のサポートが追加されました。<br><br>この機能は、12.2(33)SRA で Cisco IOS 12.2SRA リリースに統合されました。<br><br>この機能は、12.2(33)SXH で Cisco IOS 12.2SXH リリースに統合されました。<br><br>この機能は、12.4(20)T で Cisco IOS 12.4T リリースに統合されました。<br><br>この機能は、Cisco IOS XE リリース 3.5S で Cisco IOS XE リリース 3.5S に統合されました。 |

| 機能名 | リリース | 機能情報 |
|---|---|---|
| | | 次のコマンドが導入または変更されました。**mpls traffic-eng auto-tunnel backup srlg exclude**、**mpls traffic-eng srlg**、**show ip explicit-paths**、**show mpls traffic-eng link-management advertisements**、**show mpls traffic-eng link-management interfaces**、および **show mpls traffic-eng topology**。 |

# 用語集

**高速リルート**：障害ポイントで LSP をローカルに修復することにより、リンクとノードの障害から MPLS トラフィック エンジニアリング（TE）LSP を保護するメカニズム。この保護により、ヘッドエンド ルータがエンドツーエンド LSP を確立してそれらを置き換えようとしたときにデータのフローを継続できるようになります。FRR は、障害が発生したリンクまたはノードをバイパスするバックアップ トンネルを介して再ルーティングすることによって、保護されている LSP をローカルに修復します。

**ホップ**：2 つのネットワーク ノード間（たとえば、2 つのルータ間）のデータ パケットの通路。

**IGP**：Interior Gateway Protocol（内部ゲートウェイ プロトコル）。自律システム内でルーティング情報の交換に使用するインターネット プロトコル。

**インターフェイス**：ネットワーク接続。

**IPアドレス**：TCP/IP を使用するホストに割り当てられている 32 ビット アドレス。IP アドレスは、5 つのクラス（A、B、C、D、または E）の 1 つに属し、ピリオドで区切った 4 オクテットとして記述されます（ドット付き 10進表記）。各アドレスはネットワーク番号、オプションのサブネットワーク番号、およびホスト番号で構成されます。ルーティングにはネットワーク番号とサブネットワーク番号を組み合わせて使用し、ネットワーク内またはサブネットワーク内の個別のホストのアドレス指定にはホスト番号を使用します。IP アドレスからのネットワーク情報とサブネットワーク情報の抽出には、サブネット マスクを使用します。

**IP明示パス**：IP アドレスのリスト。それぞれの IP アドレスは明示パス内のノードまたはリンクを表します。

**IS-IS**：Intermediate System-to-Intermediate System。DECnet Phase V ルーティングに基づいた OSI リンクステート階層型ルーティング プロトコル。Intermediate System（IS）ルータが、単一のメトリックに基づいてルーティング情報を交換して、ネットワーク トポロジを決定します。

**LDP**：Label Distribution Protocol（ラベル配布プロトコル）。パケットの転送に使用されるラベル（アドレス）をネゴシエーションするための、MPLS 対応ルータ間の標準プロトコル。

**リンク**：隣接するノード間のポイントツーポイント接続。

**LSP**：ラベルスイッチド パス。ラベル付きパケットが複数のホップを介して通過するパス。このパスは、入力 LSR から開始し、出力 LSR で終了します。

**LSR**：ラベル スイッチング ルータ。パケット内のラベル カプセル化の値に基づいて、パケットを転送するレイヤ 3 ルータ。

**MPLS**：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ネットワークを介してパケット（フレーム）を転送する方式。ネットワークのエッジにあるルータがパケットにラベルを適用できるようにします。ネットワーク コア内の ATM スイッチまたは既存のルータは、最小限のルックアップ オーバーヘッドでラベルに従ってパケットを切り替えることができます。

**ノード**：ネットワーク接続のエンドポイント、つまりネットワーク内の複数の回線に共通する接合部。複数のノードをリンクで相互接続することができます。これらのノードは、ネットワーク内のコントロール ポイントとなります。

**OSPF**：Open Shortest Path First。IS-IS プロトコルから派生した、リンクステート階層型の Interior Gateway Protocol（IGP）ルーティング アルゴリズム。OSPF 機能には、最小コストによるルーティング、マルチパスのルーティング、およびロード バランシングが含まれます。

**ルータ**：1 つ以上のメトリックを使用して、ネットワーク トラフィックを転送すべき最適のパスを決定するネットワーク層装置。ルータは、ネットワーク層情報に基づいて、ネットワーク間でパケットを転送します。

**ルータ ID**：パケットを発信するルータを他のすべてのルータと一意に区別するために使用できる ID。たとえば、ルータのインターフェイスの 1 つの IP アドレスです。

**トラフィックエンジニアリング**：ネットワーク上で、標準的なルーティング方法が使用された場合に選択されるパスとは異なるパスを経由してトラフィックがルーティングされるようにするために使用する技術やプロセス。

**トンネル**：2 つのピア間（2 台のルータ間など）のセキュアな通信パス。トラフィック エンジニアリング トンネルは、トラフィック エンジニアリングに使用されるラベル スイッチド トンネルです。このようなトンネルは、通常のレイヤ 3 ルーティング以外の方法で設定します。レイヤ 3 ルーティングでトンネルが使用するパス以外のパスでトラフィックを転送するために使用します。

第 9 章

# MPLS トラフィック エンジニアリングにおける Inter-AS TE

MPLS トラフィック エンジニアリング - Inter-AS TE 機能は、自律システム境界ルータ（ASBR）ノード保護、ルーズ パス再最適化、ルーズ ホップが含まれるラベル スイッチド パス（LSP）のステートフル スイッチオーバー（SSO）回復、ASBR 強制リンク フラッディング、相互自律システム（Inter-AS）用の Cisco IOS リソース予約プロトコル（RSVP）ローカル ポリシー拡張機能、およびネイバー単位のキーを提供します。

- ASBR ノード保護：エリア間および Inter-AS TE ラベル スイッチド パス（LSP）をエリア境界ルータ（ABR）または ASBR の障害から保護します。
- ルーズ パス再最適化：マルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）トンネルの LSP が、トンネル ヘッドエンド ルータのトポロジ データベース内にないホップ、つまり、同じ Open Shortest Path First（OSPF）エリア、Intermediate System-to-Intermediate System（IS-IS）レベル、またはトンネルのヘッドエンド ルータとしての自律システムのいずれにもないホップを通過できるようにします。
- ルーズ ホップ回復：ルーズ ホップが含まれる LSP の SSO 回復をサポートします。
- ASBR 強制リンク フラッディング：他のドメイン内の情報がヘッドエンド ルータに使用可能でないときに、LSP が境界を越えて別のドメインに入れるようにします。
- Inter-AS 用の Cisco IOS RSVP ローカル ポリシー拡張機能：ネットワーク管理者は、複数の自律システムにわたって機能する TE トンネルに対して、管理されたポリシーを作成できます。
- ネイバー単位のキー：ネイバー単位で暗号化認証を実施できます。

# 機能情報の確認

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

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、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。

# MPLS トラフィック エンジニアリング - Inter-AS TE の前提条件

- MPLS をイネーブルにします。
- ルータ上で TE を設定する。
- ネットワークが次の Cisco 機能をサポートしていることを確認します。
  - MPLS
  - Cisco Express Forwarding; シスコ エクスプレス フォワーディング
  - IS-IS または OSPF
- ルーズ パス再最適化を行う場合、次の設定方法を知っておく。
  - MPLS TE トンネルの IP 明示パス
  - ルーズ ホップ
  - エリア間トンネルおよび Inter-AS トンネル

# MPLS トラフィック エンジニアリング - Inter-AS TE の制約事項

### ルーズ パス再最適化

- ミッドポイント再最適化はサポートされない。

### ASBR 強制リンク フラッディング

- ヘッドエンドルータで認識されている（および、LSP のパスの計算時に制約として使用される）TE メトリックおよびアフィニティ属性は、現在シグナリングされない。このため、Explicit Router（ERO）展開では、これらの制約が考慮されません。
- 自律システム内の各ノードには、それぞれ固有のルータ ID が必要である。
- リンク上に設定されたルータ ID は、自律システム内のルータ ID と競合できない。
- リンクの強制リンク フラッディングが設定されている場合、リンクのネイバーは通常の Interior Gateway Protocol（IGP）アップデートからの情報を学習しない。リンクがリンク上の IGP によってネイバーの情報をすでに学習している場合、そのリンクをパッシブとして設定することはできません。このため、リンクの強制フラッディングを設定する場合は、ノードでそのリンク上にネイバーが存在していないことを確認してください。

# MPLS トラフィック エンジニアリング - Inter-AS TE の概要

## MPLS トラフィック エンジニアリング トンネル

MPLS TE を使用すると、ネットワーク全体にわたる LSP を構築し、そのネットワークを介してトラフィックを転送できます。

（TE トンネルとも呼ばれる）MPLS TE LSP を使用すると、TE トンネルのヘッドエンドによって、そのトラフィックが特定の宛先に到達するために使用するパスを制御できます。この方式は、宛先アドレスだけに基づいてトラフィックを転送する方式よりも柔軟性が高くなります。

エリア間トンネルを使用すると、次の操作を実行できます。

- エリア間に TE トンネルを構築する（エリア間トンネル）。
- 1 台のルータ上で、同じエリア内に起点と終点を持つ TE トンネルを複数のエリアに構築する（エリア内トンネル）。

トンネルの重要性には差があります。たとえば、Voice over IP（VoIP）トラフィックを伝送するトンネルと、データ トラフィックを伝送するトンネルが、同じリソースに対して競合する場合があります。または、単に、データ トンネル自体の重要性に差がある場合もあります。MPLS TE を使

用すると、一部のトンネルが他のトンネルをプリエンプトするように設定できます。各トンネルにはプライオリティがあり、重要性の高いトンネルが重要性の低いトンネルよりも優先されます。

# マルチエリア ネットワーク設計

複数の IGP エリアおよびレベルにわたって MPLS TE トンネルを確立できます。トンネルのヘッドエンド ルータとテールエンド ルータを同じエリアに配置する必要はありません。IGP には、IS-IS または OSPF が使用できます。

エリア間トンネルを設定するには、**next-address loose** コマンドを使用して、ヘッドエンド ルータ上に、LSP が通過する各 ABR を識別する、LSP のルーズにルーティングされた明示パスを指定します。指定した明示パス上のヘッドエンド ルータと ABR は、ルーズ ホップを展開し、それぞれが次の ABR またはトンネル宛先へのパス セグメントを計算します。

# 高速再ルーティング

MPLS 高速再ルーティング（FRR）は、リンク、共有リスク リンク グループ（SRLG）、およびノードの障害から TE LSP を保護するための、高速回復ローカル保護の手法です。リンク、ノード、または SRLG の障害から保護するために、（バックアップ LSP と呼ばれる）1 つ以上の TE LSP を事前に設定しておきます。障害が発生した場合、障害が発生したリソースを通過する保護対象の TE LSP が、それぞれ適切なバックアップ トンネルにリルートされます。

バックアップ トンネルは、次の要件を満たしている必要があります。

- バックアップ トンネルは、その保護対象の要素を通過することはできない。
- バックアップ トンネルは、少なくとも 2 つのノード（ローカル修復ポイント（PLR）とマージ ポイント（MP））でプライマリ トンネルと交差する必要がある。PLR は、バックアップ トンネルのヘッドエンド LSR にする必要があります。MP は、バックアップ トンネルのテールエンド LSR にする必要があります。PLR は、リンク、ノード、または SRLG の障害が発生したときに FRR がトリガーされるポイントです。
- Inter-AS トンネルに対して FRR 保護を実行できるのは、バックアップ トンネルのマージ ポイントがパケットを PLR のバックアップ トンネルの出力インターフェイスにルーティングできる場合だけです。スタティック ルートを設定することも、ボーダー ゲートウェイ プロトコル（BGP）を設定して、バックアップ トンネルの出力インターフェイスを他の自律システムにエクスポートすることもできます。
- 優先リンクがパッシブ リンクの場合は、アドミニストレイティブウェイトを割り当てる必要があります。管理上の重みを割り当てるには、インターフェイス コンフィギュレーション モードで **mpls traffic-eng administrative-weight** コマンドを使用します。
- 各ルータを、グローバル コンフィギュレーション モードで **mpls traffic-eng reoptimize events link-up** コマンドを使用して設定する必要があります。

# ASBR ノード保護

MP と PLR は異なる IGP を持つ別々の自律システム内に配置されるため、ASBR を通過する TE LSP には、特殊な保護メカニズム（ASBR ノード保護）が必要です。

PLR は、プライマリ トンネルの Record Route Object（RRO）を検証して、RRO 内に指定されているアドレスのいずれかがバックアップ トンネルの宛先と一致しているかどうかを調べます。これにより、確実にバックアップ トンネルが MP でプライマリ トンネルと交差するようにしています。

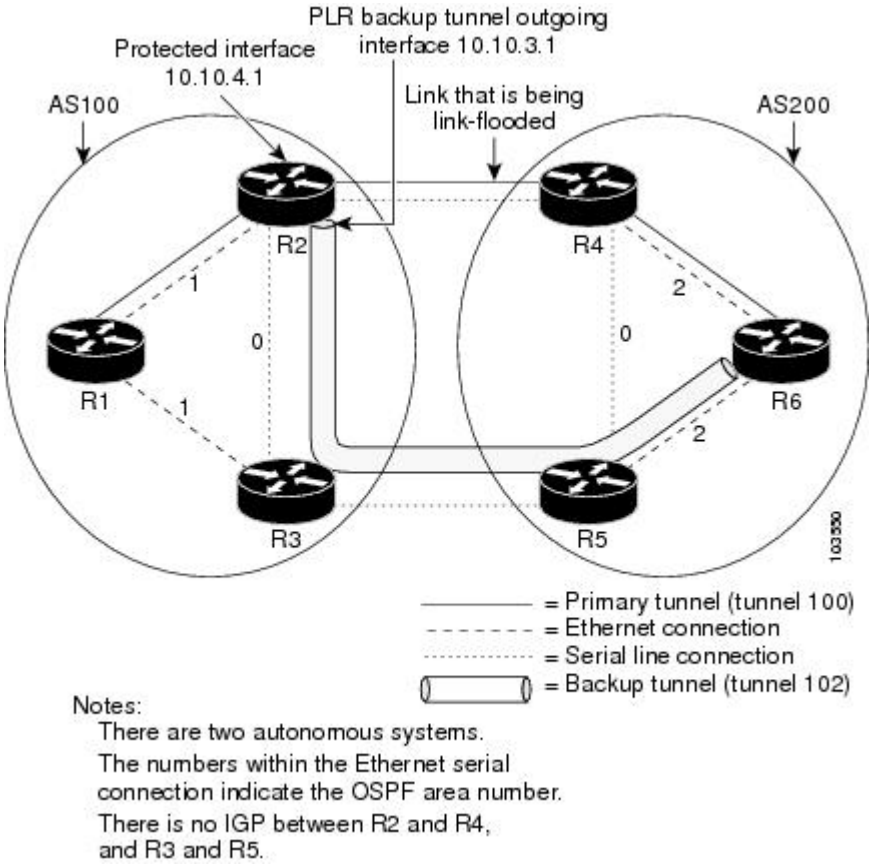
RRO IPv4 および IPv6 サブオブジェクト内に指定するアドレスは、ノード ID およびインターフェイスのアドレスにできます。トラフィック エンジニアリング RFC 3209 では、ルータ アドレスまたはインターフェイスアドレスを使用できることを規定していますが、発信パスメッセージのインターフェイス アドレスの使用を推奨しています。このため、次の図では、ルータ R2 は、プライマリ トンネル（T1）とバックアップ トンネルの resv メッセージとともに伝送される RRO オブジェクト内におそらくインターフェイス アドレスを指定しています。

ノード ID を使用すると、PLR は、resv RRO 内のノード ID をバックアップ トンネルの宛先と比較することにより、適切なバックアップ トンネルを選択できます。

RSVP メッセージを適切なピア（たとえば、resv メッセージ）にルーティングして転送する必要がある場合、その RSVP メッセージを送達するために MP から PLR に戻るためのルートが必要です。resv メッセージを送達するために、MP に、PLR バックアップ トンネルの発信インターフェイスへのルートが必要です。このため、MP から PLR へのスタティック ルートを設定する必要があります。設定手順については、MP から PLR へのスタティック ルートの設定, （251 ページ）を参照してください。

次の図は、ASBR ノード保護を示しています。ルータ R4 は、R2-R3-R5-R6 からのバックアップ トンネルを使用してノード保護が設定されています。

**図 *35*：*ASBR* ノード保護**




この設定では、IP アドレスは次のようになっています。

- R1：Loopback0 10.10.0.1
  - イーサネット 0：IP アドレス 10.10.1.1 が R2 イーサネット 0 に接続されています。
  - イーサネット 1：IP アドレス 10.10.2.1 が R3 イーサネット 1 に接続されています。
- R2：Loopback0 10.10.0.2
  - イーサネット 0：IP アドレス 10.10.1.2 が R1 イーサネット 0 に接続されています。
  - イーサネット 1：IP アドレス 10.10.3.1 が R3 イーサネット 1 に接続されています。
  - シリアル 2：IP アドレス 10.10.4.1 が R4 シリアル 2 に接続されています。
- R3：Loopback0 10.10.0.3
  - イーサネット 0：IP アドレス 10.10.2.2 が R1 イーサネット 1 に接続されています。

- イーサネット 1：IP アドレス 10.10.3.2 が R2 イーサネット 1 に接続されています。
- シリアル 2：IP アドレス 10.10.5.1 が R5 シリアル 2 に接続されています。

- R4：Loopback0 10.10.0.4
  - イーサネット 0：IP アドレス 10.10.7.1 が R6 イーサネット 0 に接続されています。
  - イーサネット 1：IP アドレス 10.10.6.1 が R5 イーサネット 1 に接続されています。
  - シリアル 2：IP アドレス 10.10.4.2 が R2 シリアル 2 に接続されています。

- R5：Loopback0 10.10.0.5
  - イーサネット 0：IP アドレス 10.10.8.1 が R6 イーサネット 0 に接続されています。
  - イーサネット 1：IP アドレス 10.10.6.2 が R4 イーサネット 1 に接続されています。
  - シリアル 2：IP アドレス 10.10.5.2 が R3 シリアル 2 に接続されています。

- R6：Loopback0 10.10.0.6
  - イーサネット 0：IP アドレス 10.10.7.2 が R4 イーサネット 0 に接続されています。
  - イーサネット 1：IP アドレス 10.10.8.2 が R5 イーサネット 1 に接続されています。

上の図では、次のような状況になっています。

- ルータ R1、R2、および R3 は、AS 100 内にある。R1-R2 リンクと R1-R3 リンクは、OSPF エリア 1 内にある。
- ルータ R4、R5、および R6 は、AS200 内にある。R4-R6 リンクと R5-R6 リンクは、OSPF エリア 2 内にある。
- リンク R2-R3 は AS100 内にあり、リンク R4-R5 は AS200 内にある。リンク R2-R3 とリンク R4-R5 は、OSPF エリア 0 内にある。
- リンク R2-R4 とリンク R3-R5 は、AS100 と AS200 の間の Inter-AS 境界を越えるため、IGP を実行していない。これらのリンクでは IGP が実行されていないため、FRR が機能するには、パッシブ インターフェイスごとに管理上の重みを設定する必要があります。インターフェイス コンフィギュレーション モードで **mpls traffic-eng administrative-weight** コマンドを使用してください。
- R1-R2-R4-R6 を通過するプライマリ トンネル（トンネル 100）が存在する。
- R2-R3-R5-R6 を通過するバックアップ トンネル（トンネル 102）が存在する。
- R6-R5-R3-R1 を通過する、トンネル 100 のデータ トラフィックを戻すための TE トンネル（トンネル 101）が存在する。
- R6-R5-R3-R2 を通過する、トンネル 102 のデータ トラフィックを戻すための TE トンネル（トンネル 103）が存在する。
- すべてのトンネルの明示パスがルーズ ホップを使用する。

- R2-R4 リンクは、R2 と R4 の両方の IGP でリンク フラッディングするように設定されている。R3-R5 リンクは、R3 と R5 の両方の IGP でリンク フラッディングするように設定されている。

ルータ R2 は、次のことが確実になるように設定する必要があります。

- バックアップ トンネルが MP でプライマリ トンネルと交差し、有効な MP アドレスを持つ。上の図では、R2 が、トンネル 100 とバックアップ トンネル 102 が MP ノード R6 を共有することを決定する必要があります。
- バックアップ トンネルが帯域幅保護のためのプライマリ LSP の要求を満たしている。たとえば、障害発生時にプライマリ トンネルに対して保証される帯域幅の大きさや、保護のタイプ（リンク障害よりもノード障害に対して保護することが推奨される）などです。

### RRO でのノード ID シグナリング

ASBR ノード保護には、ノード ID フラグ（0x20）が含まれます。これは、ノード ID サブオブジェクトとも呼ばれます。このフラグが設定されている場合、resv メッセージ内の RRO オブジェクトの中に指定されているアドレスがノード ID アドレスであることを示します。ノード ID アドレスは、トラフィック エンジニアリング ルータ ID を参照します。

1 つのノードは、常に RRO 内の同じアドレスを使用する必要があります（つまり、IPv4 と IPv6 のいずれか一方だけを使用する必要があります）。

すべてのホップを表示するには、ヘッドエンド ルータ上で次のコマンドを入力します。サンプル コマンド出力は次のとおりです。

```
Router(config)# show ip rsvp reservations detail
Reservation:
 Tun Dest:   10.10.0.6  Tun ID: 100  Ext Tun ID: 10.10.0.1
 Tun Sender: 10.10.0.1  LSP ID: 31
 Next Hop: 10.10.1.2 on Ethernet0/0
 Label: 17 (outgoing)
 Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
 Average Bitrate is 10K bits/sec, Maximum Burst is 1K bytes
 Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
 RRO:
   10.10.0.2/32, Flags:0x29 (Local Prot Avail/to NNHOP, Is Node-id)
   10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP)
     Label subobject: Flags 0x1, C-Type 1, Label 17
   10.10.0.4/32, Flags:0x20 (No Local Protection, Is Node-id)
   10.10.7.1/32, Flags:0x0 (No Local Protection)
     Label subobject: Flags 0x1, C-Type 1, Label 17
   10.10.0.6/32, Flags:0x20 (No Local Protection, Is Node-id)
   10.10.7.2/32, Flags:0x0 (No Local Protection)
     Label subobject: Flags 0x1, C-Type 1, Label 0
 Resv ID handle: 0100040E.
 Status:
 Policy: Accepted. Policy source(s): MPLS/TE
```

フィールドの説明については、『Cisco IOS Quality of Service Solutions Command Reference』を参照してください。

### ノード ID サブオブジェクトの追加

高速リルート可能な LSP がシグナリングされると、次の処理が行われます。

- LSR で、resv メッセージ内にノード ID サブオブジェクトと着信ラベル サブオブジェクトが追加される。
- path メッセージ内に RRO オブジェクトがある場合、LSR で、resv メッセージ内に、ノード ID サブオブジェクト、インターフェイス アドレスを記録する RRO IPv4 サブオブジェクト、および着信ラベル サブオブジェクトが追加される。

ヘッドエンド LSR 上で record-route をイネーブルにすると、LSP のインターフェイス アドレスが、resv メッセージ内の RRO オブジェクトに追加されます。

record-route を有効にするには、**record-route** キーワードを使用して次のコマンドを入力します。

```
tunnel mpls traffic-eng record-route
```

### ノード ID サブオブジェクトを使用した RRO の処理

ノード ID サブオブジェクトは、RECORD_ROUTE オブジェクトのラベル ルート サブオブジェクトの前に追加されます。RECORD_ROUTE がオンになっている場合、RRO オブジェクトには、ノード ID、インターフェイス アドレス、ラベルがこの順に含まれます。

### マージ ポイント ロケーション

バックアップ トンネルの宛先は、MP のノード ID です。PLR は、バックアップ トンネルの宛先アドレスと、プライマリ トンネルの resv RRO に含まれているノード ID サブオブジェクトを比較することにより、MP および適切なバックアップ トンネルを検出できます。

IPv4 ノード ID サブオブジェクトと IPv6 ノード ID サブオブジェクトの両方が存在する場合、PLR は、そのいずれかまたは両方を使用して MP アドレスを検出できます。

### 下位互換性の決定

IPv4 ノード ID サブオブジェクトまたは RRO IPv6 ノード ID サブオブジェクトがサポートされていないノードとの互換性を保つために、ノードでは、これらのオブジェクトを無視できます。これらのノードを、エリア間トラフィック エンジニアリングまたは Inter-AS トラフィック エンジニアリングを使用したネットワーク内の MP にすることはできません。

## ルーズ パス再最適化

### エリア間 LSP および Inter-AS LSP

MPLS TE トンネルの LSP がヘッドエンド ルータのトポロジ データベース内にない（つまり、別の OSPF エリアまたは IS-IS レベルにある）ホップを通過する場合、LSP はエリア間 *TE LSP* と呼ばれます。

トンネルの LSP がトンネルのヘッドエンド ルータとは別の自律システム（AS）内にあるホップを通過する場合、LSP は *Inter-AS TE LSP* と呼ばれます。

エリア間 TE LSP と Inter-AS TE LSP は、ERO 内のルーズ ホップ サブオブジェクトを使用してシグナリングできます。ヘッドエンドではエリアの外側にあるホップについての「厳格（ストリク

ト）な」情報を持たないため、LSP のパスはヘッドエンドで「ルーズに」指定されます。これらのルーズホップ サブオブジェクトは、これらのサブオブジェクトを処理する、（情報を持つ）ダウンストリーム ルータに基づいて、ストリクト ホップに展開されます。

### ルーズ ホップ設定

ヘッドエンド エリアの外側では、ホップをルーズ ホップとして設定します。通常、ABR および トンネルのテールエンド ルータだけを指定しますが、他にも任意の組み合わせを指定できます。

### ルーズ ホップ展開

ルーズ ホップ展開とは、1 つの ERO ルーズ ホップ サブジェクトを 1 つ以上のストリクト ホップ サブオブジェクトに変換することです。

エリア間 TE LSP と Inter-AS TE LSP は、ERO 内のルーズ ホップ サブオブジェクトを使用してシグナリングできます。次のアドレスとしてルーズ ホップを持つ ERO が含まれる path メッセージをルータが受信すると、このルータでは、通常、1 つのルーズ ホップ サブオブジェクトを 1 つ以上のストリクト ホップ サブオブジェクトに変換することによって、ERO を展開します。通常、ルータのトポロジデータベース内には、ルーズホップに到達するための最良の方法に関する情報があり、Constraint-based Shortest Path First（CSPF）を使用してこのパスを計算します。このため、ルータでは、ERO 内に見つかったルーズ ホップ サブオブジェクトを、より詳細なこの情報に置き換えます。このプロセスは、ルーズ ホップ展開または ERO 展開と呼ばれます。

ルーズ ホップ展開は、LSP のパス上の 1 つ以上のホップで実行できます。このプロセスは、ルーズ パス再最適化と呼ばれます。

### トンネル再最適化手順

トンネル再最適化は、TE トンネルが現在使用している LSP よりも適切な LSP（たとえば、長さが短い、コストが低いなど）をシグナリングし、この新しい LSP を使用するようにトンネルのデータを切り替えることです。

常に、より適切な新しい TE LSP が確立され、元の LSP が切断される前に、データがその LSP に移動されます（このため、これは「make before break」手順と呼ばれます）。これにより、新しい LSP に移行するときに、データ パケットが失われないようにできます。

トンネル再最適化を行うために必要な条件は、次のとおりです。

- 各ルータが **mpls traffic-eng reoptimize events link-up** コマンドを使用して設定されている。
- 各パッシブ リンクに管理上の重みが割り当てられている。管理上の重みを設定するには、インターフェイス コンフィギュレーション モードで **mpls traffic-eng administrative-weight** コマンドを使用します。

TE LSP 再最適化プロセスは、次の場合にトリガーされます。

- 定期的に（タイマーに基づく）
- ユーザが再最適化を要求するコマンド（**mpls traffic-eng reoptimize**）を入力した。
- リンクアップなどのネットワーク イベントが発生した。

再最適化がトリガーされる方法に関係なく、ヘッドエンド ルータによってトンネルが再最適化されるのは、トンネルが現在使用しているパスよりも適切なパスが見つかった場合だけです。より適切なパスがローカル トポロジ データベース内に存在しない場合、新しい LSP はシグナリングされず、再最適化は行われません。

ルーズパス再最適化が追加される前は、ヘッドエンドエリアの外側のエリアにより適切なパスがあっても、エリア間 TE LSP は再最適化されませんでした。これは、より適切なパスが、ヘッドエンド ルータによって認識される範囲外に存在する（つまり、ローカル トポロジ データベース内にない）場合に、そのパスを検出する機能がヘッドエンド ルータになかったためです。

ルーズ パス再最適化が追加されたため、トンネルのヘッドエンドは、LSP が複数のエリア、レベル、または自律システムにわたっていても、LSP を再最適化できます。このことは、*draft-vasseur-mpls-loose-path-reopt-02.txt* で定義されているクエリーおよび応答を実装することによって行われます。このドラフトには、トンネルのヘッドエンドがダウンストリーム ルータを照会してこのトンネルの LSP の ERO 展開を実行するときに使用するプロトコルが定義されています。これらのダウンストリーム ルータでは、使用されているパスよりも適切なパスが見つかると、肯定応答を返します（このことは、新しい ERO 展開を介して行われます。）ヘッドエンドは、クエリーに対する肯定応答を受信すると、トンネルの新しい LSP をシグナリングします。新しい LSP では、より適切なパスを使用して新しい ERO 展開を実行することによるメリットを得ることができます。

ルーズ パス再最適化はデフォルトで有効になっており、ディセーブルにできません。LSP 再最適化を試行しても、ヘッドエンドがより適切なパスを見つけることができず、かつ、LSP にルーズな ERO サブオブジェクトが含まれている場合は、ダウンストリーム ルータがより適切なパスを見つけることができるかどうかを判別するためのクエリーがダウンストリーム送信されます。肯定応答が返された場合、LSP は再最適化されます。つまり、（より適切なパスを通過する）新しい LSP がシグナリングされると、トンネルのデータ パケットが、この新しい LSP を使用するように切り替えられ、元の LSP は切断されます。

このクエリーおよび応答のプロトコルの詳細については、*draft-vasseur-mpls-loose-path-reopt-02.txt.* を参照してください。

# ASBR 強制リンク フラッディング

インターフェイス上に強制リンク フラッディングを設定すると、MPLS TE リンク管理モジュールによって、そのリンクがすべてのノードにアドバタイズされます。このアドバタイズメントの結果、Inter-AS 内のすべてのノード上の TE トポロジ データベースが、この情報でアップデートされます。

ASBR 強制リンク フラッディングを使用すると、これらのリンク上で IGP 隣接が実行されていなくても、リンクをアドバタイズできます。IP 明示パス内に exit ASBR がなくても、TE LSP は、BGP（またはスタティック ルート）を実行している 2 つのノード間のこれらのリンクを、ネットワークのエッジで通過できます。このため、ヘッドエンド LSR は、TE LSP パスを計算する際に、そのリンクを考慮できます。

### ASBR 強制リンク フラッディングの設定

ASBR 強制リンク フラッディングをアクティブにするには、リンクをパッシブとして設定し、ネイバー情報（つまり、ネイバー IGP ID およびネイバー TE ID）を指定します。必要な設定タスクについては、MP から PLR へのスタティック ルートの設定, （251 ページ）で説明します。

### リンク フラッディング

ASBR のインターフェイス上には、パッシブ リンクが設定されています。このリンクは、ASBR の IGP でフラッディングされます。すべてのリンクは、ポイントツーポイント リンクとしてフラッディングされます。

フラッディング通知は、リンクのプロパティが変更された場合にも送信されます。

### OSPF フラッディング

OSPF は、不透明なリンクステート アドバタイズメント（LSA）タイプ 10 リンク情報をフラッディングします。

マルチアクセス リンクに複数のネイバーが存在する場合、ネイバーごとにタイプ 10 LSA がアドバタイズされます。トポロジ データベース内では、ネイバーはポイントツーポイントのネイバー関係で表されています。

#### Link TLV

Link TLV は単一のリンクを記述するもので、複数のサブ TLV を含みます。

不透明 LSA には、単一の Link TLV が含まれます。

ASBR から ASBR へのリンクごとに、ASBR は、リンクの属性を持つ 1 つの Link TLV が含まれる不透明 LSA をフラッディングする必要があります。

Link TLV は、次のサブ TLV で構成されます。

- リンク タイプ（1 オクテット）：（必須）リンクのタイプを定義します。パッシブ インターフェイスのリンク タイプは、常に 1（ポイントツーポイント）となります。マルチアクセス サブネットワークの場合も同様です。
- リンク ID（4 オクテット）：（必須）ポイントツーポイント リンクのもう一方のリンクのエンドを識別します。ネイバーのシステム ID が含まれます。マルチアクセスの ASBR から ASBR へのリンクの場合は、スタティック設定が必要となります。ネイバーのシステム ID が含まれます。
- ローカル インターフェイス IP アドレス（4 オクテット）：このリンクに対応するネイバーのインターフェイスの IP アドレスを指定します。
- リモート インターフェイス IP アドレス（4 オクテット）：このリンクに対応するネイバーのインターフェイスの IP アドレスを指定します。リモート インターフェイス IP アドレスは、ネクストホップのルータ ID に設定されます。ASBR から ASBR へのリンクには、スタティック設定が存在する必要があります。
- トラフィック エンジニアリング メトリック（4 オクテット）
- 最大帯域幅（4 オクテット）

- 最大予約可能帯域幅（4 オクテット）
- 非予約帯域幅（32 オクテット）
- 管理グループ（4 オクテット）

### IS-IS TLV

IS-IS では、自律システム A1 でその LSP がフラッディングされると、A1 にシステム ID と疑似ノード番号が組み込まれます。

3 つの自律システムがマルチアクセス ネットワーク LAN に接続されている場合、各リンクはポイントツーポイント リンクであると見なされます。inter-ASBR リンクが Shortest Path First（SPF）ではなく CSPF によって考慮されるように、リンクは最大メトリック値でマーキングされます。

TE では、プロトコル TLV タイプ 22 が使用されます。そのデータ構造は次のとおりです。

- システム ID および疑似ノード番号ノード（7 オクテット）
- デフォルト メトリック（3 オクテット）
- サブ TLV の長さ（1 オクテット）
- サブ TLV（0 ～ 244 オクテット）。各サブ TLV は、サブタイプ（1 オクテット）、サブ TLV の値フィールドの長さ（1 オクテット）、値（0～242 オクテット）がこの順に含まれます。

次の表は、サブ TLV を定義しています。

**表 *12* : サブ *TLV***

| サブ TLV | 長さ（オクテット） | 名前 |
|---|---|---|
| 3 | 4 | 管理グループ（カラー）。 |
| 6 | 4 | メイン TLV により記述されたインターフェイスの IPv4 アドレス。 |
| 8 | 4 | このリンク上のネイバー ルータの IPv4 アドレス。これは、ネクスト ホップのルータ ID に設定されます。 |
| 9 | 4 | 最大リンク帯域幅。 |
| 10 | 4 | 予約可能リンク帯域幅。 |
| 11 | 32 | 非予約帯域幅。 |
| 18 | 3 | TE デフォルト メトリック。 |

| サブ TLV | 長さ（オクテット） | 名前 |
|---|---|---|
| 250 ～ 254 | -- | シスコ固有の拡張機能用に予約済み。 |
| 255 | -- | 将来の展開用に予約済み。 |

（注） TE ルータ ID は、TLV タイプ 134 です。

### トポロジ データベース

トポロジ データベース モジュールは、リンクステート アドバタイズメント（LSA）を受信すると、LSA をスキャンしてリンクのネイバーを検索します。ASBR リンクは同じ LSA の一部であり、他のリンクと同様に TE トポロジ データベースにインストールされます。

CSPF の動作中、TE ヘッドエンド モジュールは、TE トポロジ データベースを使用して宛先へのパスを検索します。Inter-AS リンクは TE トポロジ データベースの一部であるため、CSPF の動作では、LSP パスを計算するためにこれらのリンクが使用されます。

## リンク フラッディング

IGP は、次のような場合にリンクの情報をフラッディングします。

- リンクが停止した。
- リンクの設定が変更された（たとえば、リンク コストが変更された）。
- ルータの IGP 情報を定期的に再フラッディングするタイミングになった。
- リンク帯域幅が大幅に変更された。

フラッディングは、IS-IS と OSPF で少し異なります。Type 10 LSA には単一のリンク アドバタイズメントが含まれているため、OSPF では、変更されたリンクの情報だけがフラッディングされます。IS-IS では、Type 22 TLV にルータ上のすべてのリンクのリストが含まれるため、ノード上のリンクの 1 つしか変更されていなくても、すべてのリンクの情報がフラッディングされます。

# MPLS トラフィック エンジニアリング - Inter-AS TE の設定方法

（注） ルーズ パス再最適化の設定手順はありません。

## ルーズ ホップの設定

ここでは、ルーズ ホップを設定するための次の手順について説明します。

### Inter-AS リンクを通過するトンネルでの明示パスの設定

1 つのトンネルを複数のネットワークにまたがって設定する場合、次の手順を実行して、Inter-AS リンクを通過するトンネル上に明示パスを設定します。

#### 手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip explicit-path** {**name***path-name* | **identifier***number*} [**enable** | **disable**]
4. **next-address loose***A.B.C.D*
5. **interface tunnel***number*
6. **tunnel mpls traffic-eng fast-reroute**
7. **mpls traffic-eng reoptimize events link-up**

#### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• 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**<br><br>例：<br>`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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **ip explicit-path** {**name***path-name* \| **identifier***number*} [**enable** \| **disable**]<br><br>例：<br><br>`Router(config)# ip explicit-path identifier 2 enable` | IP 明示パス用のサブコマンド モードを開始し、明示パスを作成または変更します。このコマンドによって、ルータは IP 明示パス コンフィギュレーション モードになります。 |
| ステップ 4 | **next-address loose***A.B.C.D*<br><br>例：<br><br>`Router(cfg-ip-expl-path)# next-address loose 10.10.0.2` | 明示パス内の次のルーズな IP アドレスを指定します。<br>**next-address loose** コマンド内で、パスが通過する各エリア境界ルータ（ABR）を指定する必要があります。このコマンドによって、ルータはグローバル コンフィギュレーション モードになります。 |
| ステップ 5 | **interface tunnel***number*<br><br>例：<br><br>`Router(config)# interface tunnel 100` | トンネル インターフェイスを設定します。このコマンドによって、ルータはインターフェイス コンフィギュレーション モードになります。 |
| ステップ 6 | **tunnel mpls traffic-eng fast-reroute**<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng fast-reroute` | MPLS トラフィック エンジニアリング トンネルが、リンク障害発生時に、確立されたバックアップ トンネルを使用できるようにします。 |
| ステップ 7 | **mpls traffic-eng reoptimize events link-up**<br><br>例：<br><br>`Router(config)# mpls traffic-eng reoptimize events link-up` | インターフェイスが動作を開始した時点でMPLS トラフィック エンジニアリングの自動再最適化をイネーブルにします。 |

## リモート ASBR に到達するルートの設定

### 手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip route***prefixmask* {*ip-address* | *interface-typeinterface-number*}

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• 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**<br><br>例：<br><br>`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 | **ip route***prefixmask* {*ip-address* \| *interface-typeinterface-number*}<br><br>例：<br><br>`Router(config)# ip route 10.10.0.1 255.255.255.255 tunnel 101` | スタティック ルートを確立します。 |

## MP から PLR へのスタティック ルートの設定

異なる自律システムにわたって高速リルート保護をイネーブルにするには、次の手順を実行して、MP から PLR へのスタティック ルートを設定します。

### 手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip route***prefixmaskip-addressoutgoing-interface*

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configure terminal**<br><br>例：<br><br>`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 | **ip route***prefixmaskip-addressoutgoing-interface*<br><br>例：<br><br>`Router(config)# ip route 10.10.3.1 255.255.255.255 10.0.0.0 FastEthernet0/0` | スタティック ルートを確立します。インターフェイス情報については、該当するハードウェア マニュアルを参照してください。<br><br>（注） このコマンドは、MP 上で入力してください。宛先は PLR です。 |

# ASBR 強制リンク フラッディングの設定

ここでは、ASBR 強制リンク フラッディングを設定するための次の手順について説明します。

## 2 つの ASBR 間のパッシブ インターフェイスとしての Inter-AS リンクの設定

### 手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typeslot/port*
4. **ip address***ip-addressmask* [**secondary**]
5. **mpls traffic-eng passive-interface nbr-te-id***te-router-id* [**nbr-if-addr***if-addr*] [**nbr-igp-id** {**isis***sysid* | **ospf***sysid*}]
6. **mpls traffic-eng administrative-weight***weight*

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configure terminal**<br><br>例：<br><br>`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***typeslot/port*<br><br>例：<br><br>`Router(config)# interface serial 2/0` | 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。インターフェイス情報については、該当するハードウェア マニュアルを参照してください。 |
| ステップ 4 | **ip address***ip-addressmask* [**secondary**]<br><br>例：<br><br>`Router(config-if)# ip address 10.10.4.1 255.255.255.0` | インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。 |
| ステップ 5 | **mpls traffic-eng passive-interface nbr-te-id***te-router-id* [**nbr-if-addr***if-addr*] [**nbr-igp-id** {**isis***sysid* \| **ospf***sysid*}]<br><br>例：<br><br>`Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.11.12 nbr-igp-id ospf 10.10.15.18` | 2 つの ASBR 間にパッシブ インターフェイスとしてリンクを設定します。<br><br>（注） Inter-AS リンク上に RSVP Hello を設定する場合、すべてのフィールドが必須です。 |
| ステップ 6 | **mpls traffic-eng administrative-weight***weight*<br><br>例：<br><br>`Router(config-if)# mpls traffic-eng administrative-weight 20` | リンクの内部ゲートウェイ プロトコル（IGP）管理上の重みを上書きし、リンクに特定のウェイトを割り当てます。 |

## ASBR を通過する LSP の作成

ASBR を通過する LSP を作成するには、次の手順を実行します。

（注） プライマリ LSP に対してステップ 3 ～ 7 を実行してから、バックアップ LSP に対して同様の手順を実行してください。

## 手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip explicit path***name***enable**
4. **next-address loose***A.B.C.D*
5. **interface tunnel***number*
6. **tunnel mpls traffic-eng fast-reroute**
7. **tunnel mpls traffic-eng path-option***number* {**dynamic** | **explicit** | {**name***path-name* | *path-number*}} [**lockdown**]

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• 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**<br><br>例：<br><br>`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 | **ip explicit path***name***enable**<br><br>例：<br><br>`Router(config)# ip explicit path route1 enable` | 明示パスの名前を指定し、パスをイネーブルにします。 |
| ステップ 4 | **next-address loose***A.B.C.D*<br><br>例：<br><br>`Router(config)# next-address loose 10.10.10.2` | ルーズ ホップを設定します。 |
| ステップ 5 | **interface tunnel***number*<br><br>例：<br><br>`Router(config)# interface tunnel 100` | トンネルインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **tunnel mpls traffic-eng fast-reroute**<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng fast-reroute` | MPLS トラフィック エンジニアリング トンネルが、リンク障害発生時に、確立されたバックアップ トンネルを使用できるようにします。 |
| ステップ 7 | **tunnel mpls traffic-eng path-option***number* {**dynamic** \| **explicit** \| {**name***path-name* \| *path-number*}} [**lockdown**]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 1 route1` | MPLS トラフィック エンジニアリング トンネルのパス オプションを設定します。 |

## リンクでの複数のネイバーの設定

### 手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typeslot/port*
4. **mpls traffic-eng passive-interface** [**nbr-te-id**] [*router-id* | *te-id*] [**nbr-igp-id**] [**isis***sysid* | **ospf***sysid*]
5. **mpls traffic-eng administrative-weight***weight*

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• 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**<br><br>例：<br><br>`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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **interface***typeslot/port*<br><br>例：<br><br>`Router(config)# interface serial 2/0` | 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。インターフェイス情報については、該当するハードウェア マニュアルを参照してください。 |
| ステップ 4 | **mpls traffic-eng passive-interface** [**nbr-te-id**] [*router-id* \| *te-id*] [**nbr-igp-id**] [**isis***sysid* \| **ospf***sysid*]<br><br>例：<br><br>`Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf 10.10.0.4` | リンクをパッシブ リンクとして設定します。 |
| ステップ 5 | **mpls traffic-eng administrative-weight***weight*<br><br>例：<br><br>`Router(config-if)# mpls traffic-eng administrative-weight 20` | リンクの内部ゲートウェイ プロトコル（IGP）管理上の重みを上書きし、リンクに特定のウェイトを割り当てます。 |

### トラブルシューティングのヒント

MPLS トラフィック エンジニアリング - Inter-AS TE に関する問題のトラブルシューティングには、次の debug コマンドが役立ちます。

#### TE LSP のヘッドエンドのデバッグ

```
debug mpls traffic-eng path lookup
debug mpls traffic-eng path verify
debug mpls traffic-eng path spf
```

#### ヘッドおよびミッドポイントのデバッグ（リンク関連のデバッグ）

```
debug mpls traffic-eng link-management igp-neighbors
debug mpls traffic-eng link-management advertisements
debug mpls traffic-eng link-management bandwidth-allocation
debug mpls traffic-eng link-management routing
```

## Inter-AS TE 設定の確認

Inter-AS TE 設定を確認するには、次の手順を実行します。

（注） 高速リルートの準備ができているかどうかを確認する場合はステップ1を、高速リルートがアクティブかどうかを確認する場合はステップ 2 を実行します。

## 手順の概要

1. **show ip rsvp sender detail**
2. **show ip rsvp sender detail**
3. **show mpls traffic-eng link-management advertisements**

## 手順の詳細

**ステップ 1** **show ip rsvp sender detail**

このコマンドを使用すると、プライマリ トンネルの高速リルートの準備ができている場合、MP 送信者が表示されます。

例：

```
Router# show ip rsvp sender detail
PATH:
 Tun Dest:   10.10.0.6  Tun ID: 100  Ext Tun ID: 10.10.0.1
 Tun Sender: 10.10.0.1  LSP ID: 31
 Path refreshes:
  arriving: from PHOP 10.10.7.1 on Et0/0 every 30000 msecs
 Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0x7) Local Prot desired, Label Recording, SE Style
  session Name: R1_t100
 ERO: (incoming)
  10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
  10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
 RRO:
   10.10.7.1/32, Flags:0x0 (No Local Protection)
   10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP) !Available to NNHOP
   10.10.1.1/32, Flags:0x0 (No Local Protection)
 Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
   Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
 Fast-Reroute Backup info:
   Inbound  FRR: Not active
   Outbound FRR: No backup tunnel selected
 Path ID handle: 50000416.
 Incoming policy: Accepted. Policy source(s): MPLS/TE
 Status: Proxy-terminated
```

**ステップ 2** **show ip rsvp sender detail**

このコマンドを使用すると、プライマリ トンネルの高速リルートがアクティブになっている場合、MP 送信者が表示されます。

例：

```
Router# show ip rsvp sender detail
PATH:
 Tun Dest:   10.10.0.6  Tun ID: 100  Ext Tun ID: 10.10.0.1
 Tun Sender: 10.10.0.1  LSP ID: 31
 Path refreshes:
```

```
  arriving: from PHOP 10.10.3.1 on Et1/0 every 30000 msecs
 Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0x7) Local Prot desired, Label Recording, SE Style
  Session Name: R1_t100
 ERO: (incoming)
  10.10.0.4 (Strict IPv4 Prefix, 8 bytes, /32)
  10.10.0.6 (Loose IPv4 Prefix, 8 bytes, /32)
 RRO:
  10.10.3.1/32, Flags:0xB (Local Prot Avail/In Use/to NNHOP) !Ready
  10.10.1.1/32, Flags:0x0 (No Local Protection)
 Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
 Fast-Reroute Backup info:
  Inbound  FRR: Active
   Orig Input I/F: Et0/0
   Orig PHOP: 10.10.7.1
   Now using Bkup Filterspec w/ sender: 10.10.3.1 LSP ID: 31
  Outbound FRR: No backup tunnel selected
 Path ID handle: 50000416.
 Incoming policy: Accepted. Policy source(s): MPLS/TE
 Status: Proxy-terminated
```

**ステップ 3** **show mpls traffic-eng link-management advertisements**

このコマンドを使用すると、パッシブ リンクの影響が表示されます。R2 では、R4 へのパッシブ リンクは、リンク ID:: 1 セクション内にあります。

例：

```
Router# show mpls traffic-eng link-management advertisements

Flooding Status: ready
Configured Areas: 2
IGP Area[1] ID:: ospf 1 area 0
 System Information::
  Flooding Protocol: OSPF
 Header Information::
  IGP System ID: 10.10.0.2
  MPLS TE Router ID: 10.10.0.2
  Flooded Links: 2
 Link ID:: 1
  Link Subnet Type: Point-to-Point
  Link IP Address: 10.10.4.1
  IGP Neighbor: ID 0-0-0-0-0-0-0, IP 10.10.0.4
  Physical Bandwidth: 1544 kbits/sec
  Res. Global BW: 1158 kbits/sec
  Res. Sub BW: 0 kbits/sec
  Downstream::
                           Global Pool Sub Pool
                           ----------- ---------
   Reservable Bandwidth[0]: 1158        0 kbits/sec
   Reservable Bandwidth[1]: 1158        0 kbits/sec
   Reservable Bandwidth[2]: 1158        0 kbits/sec
   Reservable Bandwidth[3]: 1158        0 kbits/sec
   Reservable Bandwidth[4]: 1158        0 kbits/sec
   Reservable Bandwidth[5]: 1158        0 kbits/sec
   Reservable Bandwidth[6]: 1158        0 kbits/sec
   Reservable Bandwidth[7]: 1148        0 kbits/sec
  Attribute Flags: 0x00000000
 IGP Area[1] ID:: ospf 1 area 1
  System Information::
   Flooding Protocol: OSPF
  Header Information::
   IGP System ID: 10.10.0.2
   MPLS TE Router ID: 10.10.0.2
   Flooded Links: 2
  Link ID:: 1
   Link Subnet Type: Point-to-Point
```

```
Link IP Address: 10.10.4.1
IGP Neighbor: ID 0-0-0-0-0-0-0, IP 10.10.0.4
Physical Bandwidth: 1544 kbits/sec
Res. Global BW: 1158 kbits/sec
Res. Sub BW: 0 kbits/sec
Downstream::
                          Global Pool Sub Pool
                          ----------- -----------
 Reservable Bandwidth[0]: 1158        0 kbits/sec
 Reservable Bandwidth[1]: 1158        0 kbits/sec
 Reservable Bandwidth[2]: 1158        0 kbits/sec
 Reservable Bandwidth[3]: 1158        0 kbits/sec
 Reservable Bandwidth[4]: 1158        0 kbits/sec
 Reservable Bandwidth[5]: 1158        0 kbits/sec
 Reservable Bandwidth[6]: 1158        0 kbits/sec
 Reservable Bandwidth[7]: 1148        0 kbits/sec
Attribute Flags: 0x00000000
```

# MPLS トラフィック エンジニアリング Inter-AS TE の設定例

## ルーズ ホップの設定：例

### Inter-AS リンクを通過するトンネルでの明示パスの設定：例

次のコマンドでは、Inter-AS TE を使用して ABR 10.10.0.2 および 10.10.0.4 を通過して宛先 10.10.10.6 に到達する場合のパス オプションとして適した、route1 という名前のルーズな IP 明示パスを設定しています。トンネル ヘッドエンドおよび指定された ABR は、送信元 AS100 から AS200 内の宛先 10.10.0.6 へのパスを検索します。上の図を参照してください。

```
Router(config)# ip explicit-path name route1 enable
Router(cfg-ip-expl-path)# next-address loose 10.10.0.2
Router(cfg-ip-expl-path)# next-address loose 10.10.0.4
Router(cfg-ip-expl-path)# next-address loose 10.10.0.6
```

エリア間 TE トンネルの明示パスが宛先ルータを指定する必要はありません。トンネル設定で、トンネル宛先コマンド内にそれが指定されているためです。次のコマンドでは、前の例で作成したエリア間トンネルに対して同様に機能する、path-without-tailend という名前の明示パスを設定しています。

```
Router(config)# ip explicit-path name path-without-tailend
Router(cfg-ip-expl-path)# next-address loose 10.10.0.2
Router(cfg-ip-expl-path)# next-address loose 10.10.0.4
```

### IP ルーティング テーブル内のリモート ASBR に到達するルートの設定：例

次の例では、ルータ ID が 10.10.0.1 である ASBR のパケットが、トンネル 101 を経由して転送されます。

```
Router> enable
Router# configure terminal
Router(config)# ip route 10.10.0.1 255.255.255.255 tunnel 101
```

## MP から PLR へのスタティック ルートの設定：例

次の例では、MP から PLR へのスタティック ルートが設定されます。発信インターフェイスは、トンネル 103 です。

```
Router> enable
Router# configure terminal
Router(config)# ip route 10.10.3.1 255.255.255.255 tunnel 103
```

## ASBR 強制リンク フラッディングの設定：例

### パッシブ インターフェイスとしての Inter-AS リンクの設定：例

この例では、上の図を参照してください。

ルータ R2 と R4 のルータ ID は、次のとおりです。

- ルータ R2：10.100.2
- ルータ R4：10.10.0.4

```
Router> enable
Router# configure terminal
Router(config)# interface serial 2/0
```

**ネイバーも OSPF を実行している場合にルータ R2 で OSPF を設定する**

```
Router(config-if)# mpls traffic-end passive-interface nbr-te-id 10.10.0.4
```

（注） 両方のルータが OSPF を実行しているため、**nbr-igp-id** キーワードは指定していません。

ルータ R2 とそのネイバーの両方が OSPF を実行していることを指定する（nbr-igp-id キーワードが指定されている）

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf
10.10.0.4
```

ルータ R1 で IS-IS を設定する

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id isis
40.0000.0002.0001.00
```

リンク上に複数のネイバーが指定されているときにネイバー IGP ID（nbr-igp-id）を設定する

```
Router(config-if)# mpls traffic-end passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf
10.10.0.4
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.7 nbr-igp-id ospf
10.10.0.7
```

リンクの Interior Gateway Protocol（IGP）管理上の重みを上書きし、特定のウェイトを割り当てる

```
Router(config-if)# mpls traffic-eng administrative-weight 20
```

（注） ID は、各ネイバーで固有です。

パッシブ インターフェイスとしてリンクを設定する（グローバル TE コマンドを含む）

```
interface serial 2/0
ip address 10.10.4.1.255.255.255.0
 mpls traffic-eng tunnels
 mpls traffic-eng administrative-weight 10
 mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf 10.10.0.4
 ip rsvp bandwidth 1000
 mpls traffic-eng administrative-weight 20
```

## ASBR を通過する LSP の作成：例

次の例では、プライマリ LSP が作成されます。

```
Router> enable
Router# configure terminal
Router(config)# ip explicit path route1 enable
Router(config)# next-address loose 10.10.0.2
Router(config)# next-address loose 10.10.0.4
Router(config)# next-address loose 10.10.0.6
Router(config)# interface tunnel 100
Router(config-if)# tunnel mpls traffic-eng fast reroute
Router(config-if)# tunnel mpls traffic-eng path-option 1 route1
```

次の例では、バックアップ LSP が作成されます。

```
Router> enable
Router# configure terminal
```

```
Router(config)# ip explicit path backpath1 enable
Router(config)# next-address loose 10.10.0.3
Router(config)# next-address loose 10.10.0.5
Router(config)# next-address loose 10.10.0.6
Router(config)# interface tunnel 102
Router(config)# mpls traffic-eng backup path tunnel 102
Router(config-if)# tunnel mpls traffic-eng path-option 1 backpath1
```

### リンクでの複数のネイバーの設定：例

次の例では、1 つのリンク上に複数のネイバーが存在します。

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 2/0
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf
10.10.0.4
Router(config-if)# mpls traffic-eng administrative-weight 20
```

# 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 |
|---|---|
| MPLS トラフィック エンジニアリング コマンド：コマンド構文、コマンドモード、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 Multiprotocol Label Switching Command Reference*』 |
| 高速再ルーティング | 『MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)』 |
| リンク フラッディングおよびノード保護 | 『MPLS Traffic Engineering: Interarea Tunnels』 |
| IS-IS の設定作業 | 『Configuring a Basic IS-IS Network』 |
| OSPF の設定タスク | 『Configuring OSPF』 |
| IS-IS および OSPF 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 IP Routing Protocols Command Reference*』 |
| RSVP | RSVP メッセージ認証 |

### 標準

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

### MIB

| MIB | MIB のリンク |
|---|---|
| この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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。<br>http://www.cisco.com/go/mibs |

### RFC

| RFC | Title |
|---|---|
| RFC 3209 | 『Extensions to RSVP for LSP Tunnels』 |
| draft-ietf-mpls-rsvp-lsp-fastreroute-02.txt | 『*Fast Reroute Extensions to RSVP-TE for LSP Tunnels*』 |
| draft-vasseur-mpls-loose-path-reopt-02.txt | 『*Reoptimization of an Explicitly Loosely Routed MPLS TE Path*』 |
| draft-vasseur-mpls-inter-as-te-00.txt | 『*MPLS Inter-AS Traffic Engineering*』 |
| draft-ietf-mpls-soft-preemption-00.txt | 『*MPLS Traffic Engineering Soft Preemption*』 |

シスコのテクニカル サポート

| 説明 | Link |
|---|---|
| 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。<br>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。<br>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/en/US/support/index.html |

# MPLS トラフィック エンジニアリング - Inter-AS TE 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 *13*：*MPLS* トラフィック エンジニアリング - *Inter-AS TE* の機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| 『MPLS Traffic Engineering: Inter-AS TE』 | 12.0(29)S<br>12.2(33)SRA<br>12.2(33)SRB<br>12.2(33)SXH<br>12.4(20)T<br>Cisco IOS XE Release 3.5S | MPLS トラフィック エンジニアリング - Inter-AS TE 機能は、ASBR ノード保護、ルーズ パス再最適化、ルーズ ホップが含まれる LSP の SSO 回復、ASBR 強制リンク フラッディング、Inter-AS 用の Cisco IOS RSVP ローカル ポリシー拡張機能、およびネイバー単位のキーの機能を提供します。<br>この機能は、12.0(29)S で導入されました。<br>12.2(33)SRA で、**mpls traffic-eng passive-interface** コマンドに **nbr-if-addr** キーワードが追加されました。<br>ルーズ ホップを含む LSP の SSO 回復のためのサポートは、12.2(33)SRB で追加されました。<br>この機能は、12.2(33)SXH で Cisco IOS リリース 12.2(33)SXH に統合されました。<br>この機能は、12.4(20)T で Cisco IOS リリース 12.4(20)T に統合されました。<br>この機能は、Cisco IOS XE リリース 3.5S で Cisco IOS XE リリース 3.5S に統合されました。 |

# 用語集

**ABR**：Area Border Router（エリア境界ルータ）。2 つのエリアを接続するルータ。

**隣接**：MPLS-TE 転送隣接機能により、ネットワーク管理者は、トラフィック エンジニアリング、ラベルスイッチド パス（LSP）トンネルを、Shortest Path First（SPF）アルゴリズムに基づいて、Interior Gateway Protocol（IGP）ネットワーク内のリンクとして処理できます。転送隣接は、ネッ

トワーク内でのルータのロケーションに関係なく、ルータとルータの間に作成できます。ルータとルータは、間に何個かホップを入れて配置できます。

**エリア**：ネットワーク セグメント（たとえば、OSPF ベースのセグメント）とそれに接続されたデバイスの論理セット。エリアは通常、ルータによって他のエリアに接続されて、1 つの自律システムを構成します。OSPF と IS-IS では、エリアの定義方法が異なります。OSPF エリアの境界は、ルータによってマーキングされます。異なるエリアに、別々のインターフェイスが含まれます。IS-IS では、すべてのルータが完全に 1 つのエリア内にあり、エリア境界はルータ上でなくリンク上にあります。エリア同士を接続するルータは、レベル 2 のルータであり、別のエリアに直接接続されていないルータは、レベル 1 のルータです。

**ASBR**：Autonomous System Boundary Router（自律システム境界ルータ）。ルータは、OSPF 自律システムと非 OSPF ネットワークの間に配置されます。ASBR は、OSPF と、RIP などの別のルーティング プロトコルの両方を実行します。ASBR は、非スタブ OSPF エリアに存在する必要があります。

**自律システム**：共通のルーティング戦略を共有する、共通の管理の下にあるネットワークの集合。自律システムは、エリアで分割されます。

**バックアップトンネル**：リンクまたはノードの障害発生時に他の（プライマリ）トンネルのトラフィックを保護するために使用される MPLS トラフィック エンジニアリング トンネル。

**BGP**：Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。EGP に置き換わるドメイン間ルーティング プロトコル。BGP は、別の BGP システムと到着可能性情報を交換します。

**境界ルータ**：プロバイダー ネットワークのエッジにあるルータ。拡張された BGP 手順を使用して、別のプロバイダーの境界ルータに接続されます。

**シスコエクスプレスフォワーディング**：ルート参照情報を 1 つのルート キャッシュではなく複数のデータ構造に分けて保存することにより、ルータ内のパケットの転送を短時間で行うための手段。

**高速リルート**：リンク障害およびノード障害から MPLS トラフィック エンジニアリング（TE）LSP を保護するためのメカニズム。障害ポイントで LSP をローカルに修復することによって、ヘッドエンド ルータがエンドツーエンド LSP を確立してそれらを置き換えようとしたときにデータのフローを継続できるようになります。FRR は、障害が発生したリンクまたはノードをバイパスするバックアップ トンネルを介して再ルーティングすることによって、保護されている LSP をローカルに修復します。

**フラッディング**：スイッチおよびブリッジにより使用されるトラフィック通過手法。インターフェイス上で受信されたトラフィックは、最初に情報を受信したインターフェイスを除き、そのデバイスのすべてのインターフェイスから送信されます。

**転送隣接**：IS-IS または OSPF ネットワークへのトラフィック エンジニアリング リンク（または LSP）。

**ヘッドエンド**：特定の LSP の起点となり、その LSP を管理するルータ。これは、LSP パス上の最初のルータです。

**ホップ**：2 つのネットワーク ノード間（たとえば、2 つのルータ間）のデータ パケットの通路。

**IGP**：Interior Gateway Protocol（内部ゲートウェイ プロトコル）。自律システム内でルーティング情報を交換するために使用されるインターネット プロトコルです。一般的な IGP には、Interior

Gateway Routing Protocol（IGRP）、Open Shortest Path First（OSPF）、Routing Information Protocol（RIP）などがあります。

**Inter-ASLSP**：ヘッドエンドのトポロジデータベース内にないホップを通過するMPLSトラフィック エンジニアリング ラベル スイッチド パス（LSP）（つまり、このLSPは、ヘッドエンドと同じOSPFエリア、IS-ISエリア、または自律システムのいずれにも存在しません）。

**インターフェイス**：ネットワーク接続。

**IP明示パス**：IPアドレスのリスト。それぞれのIPアドレスは明示パス内のノードまたはリンクを表します。

**IS-IS**：（Intermediate System-to-Intermediate System）DECnet Phase V ルーティングに基づいたOSIリンクステート階層型ルーティング プロトコル。Intermediate System（IS）ルータが、単一のメトリックに基づいてルーティング情報を交換して、ネットワーク トポロジを決定します。

**リンク**：隣接するノード間のポイントツーポイント接続。

**LSA**：Link-State Advertisement（リンクステート アドバタイズメント）。ネイバーおよびパスのコストに関する情報が含まれる、リンクステートプロトコルにより使用されるブロードキャストパケット。受信側ルータは、LSAを使用してルーティング テーブルのメンテナンスを行います。

**LSP**：ラベルスイッチド パス。パケットの伝送にMPLSが使用される、2台のルータ間に設定された接続。LSPは、1つ以上のラベル スイッチド ホップを連結して作成されたパスです。これにより、MPLSノードからのラベルを別のMPLSノードにスワップして、パケットを転送できます。

**ミッドポイント**：特定のLSPの中継ルータ。

**ミッドポイント再最適化**：ヘッドエンドの再最適化をトリガーする、ミッドポイントがもつ機能。

**MP**：Merge Point（マージ点）。1つ以上のバックアップ トンネルが、障害が発生する可能性のあるダウンストリームにある保護対象LSPのパスと再結合するLSR。1つのLSRをMPとPLRの両方にできます。

**MPLS**：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ネットワークコアにおいて使用されるパケット転送テクノロジー。これにより、スイッチング ノードにデータの転送方法を指示するためのデータ リンク層ラベルが適用されるため、ネットワーク層ルーティングで通常行われる転送よりも高速でスケーラブルな転送が行われます。

**マルチキャスト**：個別のパケットがネットワークによりコピーされ、ネットワーク アドレスの特定のサブセットに送信されます。これらのアドレスは、Destinationアドレス フィールド内で指定します。（マルチキャストは、そのグループ アドレスという概念のために、同じデータを複数の受信者に送信するための効率的なパラダイムとなっています。これにより、受信者のグループがその単一アドレスをリッスンできます。）

**ノード**：ネットワーク接続のエンドポイント、つまりネットワーク内の複数の回線に共通する接合部。複数のノードをリンクで相互接続することができます。これらのノードは、ネットワーク内のコントロール ポイントとなります。

**OSPF**：Open Shortest Path First。IS-ISプロトコルから派生した、リンクステート階層型の内部ゲートウェイ プロトコル ルーティング アルゴリズム。OSPF機能には、最小コストによるルーティング、マルチパスのルーティング、およびロード バランシングが含まれます。

**不透明な LSA**：ルータは、LSA Type 10 リンク情報を認識している場合、ネットワークにわたってリンクのフラッディングを続行します。

**パッシブリンク**：2 つの ASBR 間のリンク上で IGP が実行されていない場合、トラフィック エンジニアリングでは、そのリンクに代わってリンク情報をフラッディングするように IGP に通知されます（つまり、そのリンクがアドバタイズされます）。

**PLR**：Point of Local Repair（ローカル修復点）。バックアップ トンネルのヘッドエンド LSR。

**ルータ**：1 つ以上のメトリックを使用して、ネットワーク トラフィックを転送すべき最適のパスを決定するネットワーク層装置。ルータは、ネットワーク層情報に基づいて、ネットワーク間でパケットを転送します。

**RSVP**：Resource Reservation Protocol（リソース予約プロトコル）。カスタマーがインターネットサービスのために要求をシグナリング（予約をセットアップ）する際に使用する IETF プロトコル。これにより、カスタマーはそのネットワーク部分を経由してデータを伝送することを許可されます。

**SPF**：Shortest Path First。OSPF 操作の基礎として使用されるルーティング アルゴリズム。SPF ルータは、電源が投入されると、ルーティングプロトコル データ構造を初期化し、そのインターフェイスが動作している下位レイヤ プロトコルからの指示を待機します。

**SRLG**：Shared Risk Link Group（共有リスク リンク グループ）。（たとえば、基礎となるファイバが同じであるために）一緒に停止する可能性の高いリンクのセット。

**テールエンド**：LSP が終端するルータ。これは、LSP のパス上の最後のルータです。

**TE**：トラフィック エンジニアリング。標準のルーティング方式が使用されていた場合に選択されたであろうパス以外のパス上のネットワーク経由でトラフィックを転送するために使用されるテクニックとプロセス。

**TLV**：Type, Length, Value（タイプ、長さ、値）。Cisco Discovery Protocol アドバタイズメントに埋め込まれた情報のブロック。

第 10 章

# MPLS トラフィック エンジニアリング over GRE トンネル サポートの設定

MPLS トラフィック エンジニアリング over Generic Routing Encapsulation（GRE）トンネル サポート機能により、アプリケーションは仮想インターフェイス上に TE トンネルを確立できます。



## 機能情報の確認

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

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、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。

# MPLS TE over GRE トンネル サポートの設定の要件

ネットワークで次のものがサポートされている必要があります。

- Cisco Express Forwarding; シスコ エクスプレス フォワーディング
- 外部データ暗号化
- Intermediate System-to-Intermediate System（IS-IS）または Open Shortest Path First（OSPF）
- GRE トラフィックの暗号化を実装するために GRE ノードで有効になっている IPsec
- インターフェイス上および GRE トンネル上に設定されている MPLS TE
- MPLS TE トンネル

同一のルーティング ドメインに GRE トンネルと TE トンネルが共存すると、ルーティング ループが発生します。GRE パケットのスタティック ルーティングを行う GRE オーバーレイを設定するか、2 つのルーティングプロセス（GRE オーバーレイ用と TE トンネル用）を使用し、別々のルーティング ドメインを作成します。

# MPLS TE over GRE トンネル サポートの設定の制約事項

- 次の TE 機能は GRE トンネルをサポートしていないため、GRE トンネルを通過する可能性がある TE トンネルには設定できません。
  - 自動ルート接続先
  - 自動帯域幅調整
  - プライマリ 1 ホップ自動トンネル
  - 双方向フォワーディング検出（BFD）- triggered FRR
  - Diff-Serve 認識型 TE (DS-TE)
  - 除外したノードを特定する明示パス オプション
  - エリア間/自律システム MPLS TE
  - ポイント ツー マルチポイント TE
  - 共有リスク リンク グループ（SRLG）
  - トンネル ベース アドミッション コントロール (TBAC)
- GRE トンネルは、ステートフル スイッチオーバー付き Cisco Nonstop Forwarding（SSO を備えた NSF）をサポートしていません。スイッチオーバーが発生すると、TE over GRE でトラフィックの損失が発生し、TE トンネルは再びシグナリングされます。

# MPLS TE over GRE トンネル サポートの設定に関する情報

## MPLS TE over GRE トンネル サポートの概要

MPLS TE トンネルは、制約ベースであって、IGP の最短コストのパスに限定されないパスを使った MPLS ネットワークを通じたラベル スイッチングデータの転送を実現します。TE トンネルは通常、隣接ルータ間の物理リンク上に確立されます。ただし、一部のアプリケーションでは、GRE トンネルのような仮想インターフェイス上に TE トンネルを構築することが要求されます。連邦情報処理標準（FIPS）140-2 のコンプライアンスには、ネットワーク インフラストラクチャ上で連邦政府の顧客のトラフィックを暗号化することが要求されます。この暗号化は、暗号化セキュリティレベル Type-I と呼ばれるものです。Type-I の暗号化環境は、暗号化ネットワークと平文ネットワークに分別されます。暗号化ネットワークは暗号化を必要としない、セキュアな施設にある、ネットワークの安全な部分です。非暗号化ネットワークはネットワークの中でも安全ではない部分で、トラフィックの暗号化が必要です。

トラフィックの暗号化の一般的な方法は 2 つあり、次のとおりです。

- 外部 crypto デバイス
- 暗号化機能が組み込まれた Cisco IOS ソフトウェアである、Cisco IOS IPsec

外部 crypto デバイスは、レイヤ 2（L2）で作動し、ATM、SONET のトラフィックのリンク層の暗号化を提供します。L2 ネットワークの IP ネットワークへの移行により、IP ネットワーク向け crypto デバイスや IPsec の採用が増えています。この移行には、トラフィックの暗号化を IP レイヤで行う必要があります。IP トラフィックやレイヤ 3（L3）/L2 VPN MPLS トラフィックなど、IP ベースのトラフィック伝送サービスは GRE トンネルを介してのみ実装されます。

## MPLS TE over GRE トンネル サポートの利点

MPLS TE over GRE トンネル サポート機能により、GRE トンネル トランスポートのレイヤ 2 、レイヤ 3 VPN のような MPLS セグメンテーション機能を向上できます。この機能により、明示パスによる転送、FRR と GRE トンネルのトラフィックの帯域幅制御を実装するための MPLS TE の導入が可能となります。また、この機能は、現在 ATM レガシー ネットワークでサポートされている TE 機能の維持に役立ちます。

# MPLS TE over GRE トンネル サポートの設定方法

## Resource Reservation Protocol の帯域幅の設定

### 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **bandwidth***kbps*
5. **ipaddress***ip-addressmask*
6. **mplstraffic-engtunnels**
7. **tunnelsource***typenumber*
8. **tunneldestination** {*host-name* | *ip-address* | *ipv6-address*}
9. **iprsvpbandwidth**
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 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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***typenumber*<br><br>例：<br>`Router(config)# interface tunnel 0` | 指定のトンネルインターフェイスについて、トンネルインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **bandwidth***kbps*<br><br>例：<br>`Router(config-if)# bandwidth 100000` | 帯域幅プールの全帯域幅を指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **ipaddress***ip-addressmask*<br><br>例：<br><br>`Router(config-if)# ip address 172.16.0.0 255.255.255.254` | インターフェイスのプライマリ IP アドレスを設定します。 |
| ステップ 6 | **mplstraffic-engtunnels**<br><br>例：<br><br>`Router(config-if)# mpls traffic-eng tunnels` | インターフェイスでトラフィック エンジニアリング トンネル シグナリングを有効にします。 |
| ステップ 7 | **tunnelsource***typenumber*<br><br>例：<br><br>`Router(config-if)# tunnel source loopback 1` | トンネルインターフェイスの送信元アドレスを設定します。 |
| ステップ 8 | **tunneldestination** {*host-name* \| *ip-address* \| *ipv6-address*}<br><br>例：<br><br>`Router(config-if)# tunnel destination 192.168.1.1` | トンネルの宛先を指定します。<br>• *ip-address*：宛先ホストの IP アドレス（ドット付き 10 進表記）。 |
| ステップ 9 | **iprsvpbandwidth**<br><br>例：<br><br>`Router(config-if)# ip rsvp bandwidth` | インターフェイスで IP 用のリソース予約プロトコル（RSVP）をイネーブルにします。 |
| ステップ 10 | **end**<br><br>例：<br><br>`Router(config-if)# end` | （任意）インターフェイス 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。 |

# MPLS TE トンネルの設定

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***tunnelnumber*
4. **ipunnumbered***typenumber*
5. **tunneldestination** {*host-name* | *ip-address* | *ipv6-address*}
6. **mplstraffic-engtunnels**
7. **tunnelmplstraffic-engpriority***setup-priority* [*hold-priority*]
8. **tunnelmplstraffic-engbandwidth***kbps*
9. **tunnelmplstraffic-engpath-option***number***dynamic**
10. **tunnelmplstraffic-engfast-reroute**
11. **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 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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***tunnelnumber*<br><br>例：<br>`Router(config)# interface tunnel 10` | 指定のトンネルインターフェイスについて、トンネル インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **ipunnumbered***typenumber*<br><br>例：<br>`Router(config-if)# ip unnumbered loopback 0` | トンネル インターフェイスに IP アドレスを割り当てます。<br>• MPLS TE トンネル インターフェイスは単一方向リンクを表すため、番号なしにする必要があります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **tunneldestination** {*host-name* \| *ip-address* \| *ipv6-address*}<br><br>例：<br><br>`Router(config-if)# tunnel destination 192.168.2.2` | トンネルの宛先を指定します。<br><br>• *ip-address*：宛先ホストの IP アドレス（ドット付き 10 進表記）。 |
| ステップ 6 | **mplstraffic-engtunnels**<br><br>例：<br><br>`Router(config-if)# mpls traffic-eng tunnels` | インターフェイスでトラフィックエンジニアリングトンネル シグナリングを有効にします。 |
| ステップ 7 | **tunnelmplstraffic-engpriority***setup-priority* [*hold-priority*]<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng priority 7 7` | トンネルの設定および予約プライオリティを設定します。 |
| ステップ 8 | **tunnelmplstraffic-engbandwidth***kbps*<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng bandwidth 10` | トンネルに必要な帯域幅を設定します。 |
| ステップ 9 | **tunnelmplstraffic-engpath-option***number***dynamic**<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 10 dynamic` | トンネルのパス オプションを設定します。 |
| ステップ 10 | **tunnelmplstraffic-engfast-reroute**<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng fast-reroute` | MPLS TE トンネルが、リンクまたはノードの障害発生時に、確立されたバックアップ トンネルを使用できるようにします。 |
| ステップ 11 | **end**<br><br>例：<br><br>`Router(config-if)# end` | （任意）インターフェイス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。 |

# MPLS TE トンネル over GRE の設定

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***tunnel***number**
4. **ipunnumberedloopback***number*
5. **tunneldestination***ip-address*
6. **tunnelmplstraffic-engautorouteannounce**
7. **tunnel mpls traffic-eng**
8. **tunnelmplstraffic-engpath-option***number***dynamic**
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 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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***tunnel***number**<br><br>例：<br>`Router(config)# interface tunnel 100` | インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **ipunnumberedloopback***number*<br><br>例：<br>`Router(config-if)# ip unnumbered loopback 0` | トンネル インターフェイスに IP アドレスを割り当てます。<br>• MPLS TE トンネル インターフェイスは単一方向リンクを表すため、番号なしにする必要があります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **tunneldestination***ip-address*<br><br>例：<br><br>`Router(config-if)# tunnel destination 10.255.1.2` | トンネルの宛先を指定します。<br><br>• *ip-address*：宛先ホストの IP アドレス（ドット付き 10 進表記）。 |
| ステップ 6 | **tunnelmplstraffic-engautorouteannounce**<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng autoroute announce` | IGP における拡張最短パス優先（SPF）の計算において、トンネルを使用する必要があることを指定します。 |
| ステップ 7 | **tunnel mpls traffic-eng**<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng` | トンネルのカプセル化モードを MPLS TE に設定します。 |
| ステップ 8 | **tunnelmplstraffic-engpath-option***number***dynamic**<br><br>例：<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 10 dynamic` | MPLS TE トンネルのパス オプションを設定します。<br><br>• **dynamic** キーワードを指定すると、Cisco IOS ソフトウェアは必要な帯域幅がいずれかのリンクの物理的な帯域幅を超えないよう、インターフェイスの物理帯域幅と使用可能な TE 帯域幅の両方をチェックします。 |
| ステップ 9 | **end**<br><br>例：<br><br>`Router(config-if)# end` | （任意）インターフェイス 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。 |

# MPLS TE over GRE トンネル サポートの設定の例

## 例：MPLS TE over GRE トンネル サポートの設定

次に、2 台のルータ（ルータ 1、ルータ 2）間に MPLS TE over a GRE トンネルを設定例を示します。最初のループバック インターフェイスは、ルータの識別に使用され、もう 1 つは到達可能性の検出に使用されます。OSPF の 1 つは TE 用に使用され、もう 1 つは到達可能性の検出に使用されます。

### ルータ 1

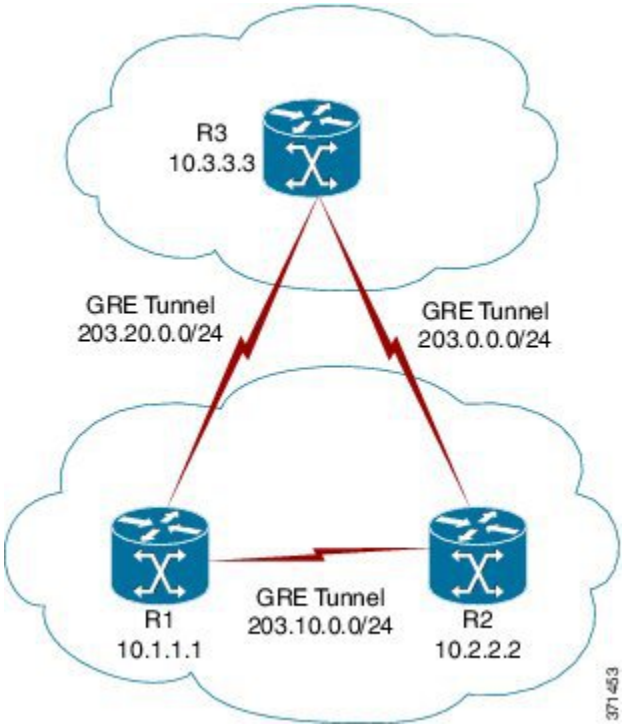
```
configure terminal
no logging console
mpls traffic-eng tunnels
interface Loopback 0
 ip address 172.16.1.1 255.255.255.255
 no shutdown
!
interface Loopback 1
 ip address 10.255.1.1 255.255.255.0
 no shutdown
!
interface gigabitethernet 1/1
 ip address 172.16.1.1 255.255.255.255
 ip rsvp bandwidth 100000
 no shutdown
!
router ospf 172
 router-id 172.16.1.1
 network 172.16.0.0 0.0.255.255 area 0
 mpls traffic-eng router-id Loopback 0
 mpls traffic-eng area 0
 no shutdown
!
router ospf 10
 router-id 10.255.1.1
 network 10.255.0.0 0.0.255.255 area 0
 no shutdown
!
interface Tunnel 10
bandwidth 20000
 ip address 172.16.0.1 255.255.255.252
 mpls traffic-eng tunnels
 keepalive 10 3
 tunnel source Loopback 1
 tunnel destination 10.255.1.2
 ip rsvp bandwidth 15000 sub-pool 5000
!
!
interface tunnel 100
ip unnumbered loopback 0
tunnel mode mpls traffic-eng
tunnel destination 192.168.10.10
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 10 dynamic
!
end
Router 2
configure terminal
no logging console
mpls traffic-eng tunnels
interface Loopback 0
 ip address 172.16.1.2 255.255.255.255
 no shutdown
!
interface Loopback 1
 ip address 10.255.1.2 255.255.255.255
 no shutdown
!
interface gigabitethernet 1/1
 ip address 10.255.0.2 255.255.255.252
 ip rsvp bandwidth 100000
 no shutdown
!
router ospf 172
 router-id 172.16.1.2
 network 172.16.0.0 0.0.255.255 area 0
 mpls traffic-eng router-id Loopback 0
 mpls traffic-eng area 0
 no shutdown
!
```

```
router ospf 10
 router-id 10.255.1.2
 network 10.255.0.0 0.0.255.255 area 0
 no shutdown
!
!
interface Tunnel0
bandwidth 20000
 ip address 172.16.0.2 255.255.255.252
 mpls traffic-eng tunnels
 keepalive 10 3
 tunnel source Loopback 1
 tunnel destination 10.255.1.1
 ip rsvp bandwidth 15000 sub-pool 5000
!
!
interface tunnel 100
ip unnumbered loopback 0
tunnel mode mpls traffic-eng
tunnel destination 172.16.1.1
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 10 dynamic
!
end
```

# 例：MPLS over GRE での CBTS 設定

次の例では、MPLS トラフィック エンジニアリング（TE）over GRE でクラスベース トンネル選択（CBTS）を設定する方法を示します。

図 *36*：*MPLS over GRE* での *CBTS* のネットワーク構造



### ミッドポイント ルータ（R1）の設定

```
mpls traffic-eng tunnels
!
interface Tunnel 102
ip address 203.20.0.1 255.255.255.0
mpls ip
mpls traffic-eng tunnels
tunnel source GigabitEthernet 0/0/0
tunnel destination 192.168.0.1
tunnel key 22
tunnel checksum
ip rsvp bandwidth 500000
!
interface Tunnel 103
ip address 203.10.0.1 255.255.255.0
mpls ip
mpls traffic-eng tunnels
tunnel source GigabitEthernet 0/0/0
tunnel destination 192.168.10.1
tunnel key 33
tunnel checksum
ip rsvp bandwidth 500000
mpls traffic-eng tunnels
!
router ospf 1
router-id 10.1.1.1
network 10.1.1.1 0.0.0.0 area 1
network 203.20.0.1 0.0.0.0 area 1
network 203.10.0.1 0.0.0.0 area 1
mpls traffic-eng router-id Loopback 0
mpls traffic-eng area 1
```

### ヘッド ルータ（R2）の設定

```
mpls traffic-eng tunnels
!
interface Tunnel 203
 ip address 203.0.0.1 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
 tunnel source GigabitEthernet 0/0/0
 tunnel destination 192.168.10.1
 tunnel key 6
 tunnel checksum
 ip rsvp bandwidth 500000
!
interface Tunnel 211
 ip address 172.16.0.2 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
 tunnel source GigabitEthernet 0/0/0
 tunnel destination 192.168.20.1
 tunnel key 22
 tunnel checksum
 ip rsvp bandwidth 500000
!
interface Tunnel 2300
 ip unnumbered Loopback 0
 tunnel mode mpls traffic-eng
 tunnel destination 10.3.3.3
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng autoroute metric relative -5
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 10 dynamic
 tunnel mpls traffic-eng exp-bundle master
 tunnel mpls traffic-eng exp-bundle member Tunnel 2301
 tunnel mpls traffic-eng exp-bundle member Tunnel 2302
!
```

```
interface Tunnel 2301
 ip unnumbered Loopback 0
 tunnel mode mpls traffic-eng
 tunnel destination 10.3.3.3
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng autoroute metric relative -5
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 10 explicit name TE2301
 tunnel mpls traffic-eng exp 6 7
!
interface Tunnel 2302
 ip unnumbered Loopback 0
 tunnel mode mpls traffic-eng
 tunnel destination 10.3.3.3
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng autoroute metric relative -5
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 10 explicit name TE2302
 tunnel mpls traffic-eng exp default
!
router ospf 1
 router-id 10.2.2.2
 network 10.2.2.2 0.0.0.0 area 1
 network 203.20.0.2 0.0.0.0 area 1
 network 172.16.0.2 0.0.0.0 area 1
 network 203.0.0.1 0.0.0.0 area 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 1
!
ip explicit-path name TE2301 enable
 next-address 203.0.0.2
ip explicit-path name TE2302 enable
 next-address 172.16.0.1
 next-address 172.26.0.2
```

### テール ルータ（R3）の設定

```
mpls traffic-eng tunnels
!
interface Tunnel 302
 ip address 203.0.0.2 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
 tunnel source GigabitEthernet 0/0/0
 tunnel destination 192.168.0.1
 tunnel key 6
 tunnel checksum
 ip rsvp bandwidth 500000
!
interface Tunnel 311
 ip address 172.26.0.2 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
 tunnel source GigabitEthernet 0/0/0
 tunnel destination 192.168.20.1
 tunnel key 33
 tunnel checksum
 ip rsvp bandwidth 500000
 !
router ospf 1
 router-id 10.3.3.3
 network 10.3.3.3 0.0.0.0 area 1
 network 203.10.0.2 0.0.0.0 area 1
 network 172.26.0.2 0.0.0.0 area 1
 network 203.0.0.2 0.0.0.0 area 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 1
```

!

# MPLS TE over GRE トンネル サポートの追加情報

### 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』 |
| MPLS コマンド | 『Cisco IOS Multiprotocol Label Switching Command Reference』 |

### 標準

| 規格 | Title |
|---|---|
| FIPS 140-2 | 暗号モジュールのセキュリティ要件 |

### MIB

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

### RFC

| RFC | Title |
|---|---|
| RFC 3812 | MPLS TE 管理情報ベース（MIB） |

### シスコのテクニカル サポート

| 説明 | Link |
|---|---|
| ★枠で囲まれた Technical Assistance の場合★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 |

# MPLS TE over GRE トンネル サポートの機能情報

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 *14* : ***MPLS TE over GRE*** トンネル サポートの機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| MPLS TE over GRE トンネル サポート | Cisco IOS XE Release 3.3S<br>15.2(1)T<br>Cisco IOS XE リリース 3.12S | MPLS TE over GRE トンネル サポート機能により、アプリケーションは仮想インターフェイス上にトラフィック エンジニアリング トンネルを確立できます。<br>次のコマンドが導入または変更されました。<br>**mplstraffic-engtunnels**、**tunnelmplstraffic-engautorouteannounce**。**tunnelmplstraffic-engbandwidth**、**tunnelmplstraffic-engfast-reroute**、**tunnelmplstraffic-engpath-option**、**tunnelmplstraffic-engpriority**。<br>Cisco IOS XE 3.12S リリースでは、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの GRE インターフェイスタイプに CBTS サポートが追加されました。 |

第 11 章

# MPLS トラフィック エンジニアリング-RSVP グレースフル リスタート

MPLS トラフィック エンジニアリング - RSVP グレースフル リスタート機能を使用すると、隣接するルートプロセッサ（RP）が、マルチプロトコルラベルスイッチング（MPLS）フォワーディング ステートを失うことなく、コントロール プレーン サービス（具体的には、ラベル配布プロトコル（LDP）コンポーネント）の中断から回復できます。この機能には、次の利点があります。

- グレースフル リスタートを使用すると、RP障害が発生した場合や、デバイスのステートフル スイッチオーバー（SSO）が行われた場合に、ステート情報をネイバーから回復できます。
- グレースフル リスタートを使用すると、ネットワークの中断を最小限に抑えながら、セッション情報を回復できます。
- ノードは、グレースフル リスタートを実行してラベル バインディング情報とステート情報とを保持することにより、ネイバーのステート回復を支援します。その結果、障害の発生したノードは短時間で回復し、その時点で転送されていたトラフィックには影響が出ません。

• 用語集，299 ページ

# 機能情報の確認

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

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、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。

# MPLS TE：RSVP グレースフル リスタートの前提条件

MPLS トラフィック エンジニアリング - RSVP グレースフル リスタート機能を設定する前に、ルータに対して次の作業を実行します。

- Resource Reservation Protocol（RSVP）を設定します。
- MPLS をイネーブルにします。
- トラフィック エンジニアリング（TE）を設定する。
- グレースフル リスタートを有効にします。

# MPLS TE：RSVP グレースフル リスタートの制約事項

- グレースフル リスタートはノード障害のみをサポートします。
- ネイバー ルータがノード Hello をサポートしていない場合のみインターフェイス Hello を設定することを推奨します。
- 番号が付いていないインターフェイスはサポートされない。
- 同じインターフェイス上で、グレースフル リスタート用にインターフェイス Hello を設定し、同時に高速リルートまたは Hello State Timeout（HST）用にインターフェイス Hello を設定することはできない。

# MPLS TE：RSVP グレースフル リスタートの設定に関する情報

## グレースフル リスタートの動作

RSVP グレースフル リスタートを使用すると、ネットワークのノード障害発生後、RSVP TE-enabled ノードを正常に回復できます。つまり、障害発生後の RSVP ステートが、可能な限り短時間で復元されます。ノード障害がネットワーク内の他のノードに完全に透過的な場があります。

RSVP グレースフル リスタートでは、ラベル値もフォワーディング情報も保持されます。また、サードパーティ製ルータ、Cisco ルータともシームレスに機能します。

RSVP グレースフル リスタートは、RSVP Hello メッセージを利用して、ネイバーのダウンを検出します。Hello メッセージには、2 つのネイバー間の Hello Request オブジェクトまたは Hello Acknowledgment（ACK）オブジェクトが含まれます。

グレースフル リスタートがグローバルに設定されており、ネイバーへの最初の LSP が作成されるときに、ノード Hello が送信されます。

インターフェイス Hello はオプション設定の 1 つです。インターフェイス上でグレースフル リスタート Hello コマンドを設定した場合、そのインターフェイス Hello は、当該ネイバーを相手とする追加の Hello インスタンスと見なされます。

ルータは、次の条件がすべて満たされるとグレースフル リスタートのためのインターフェイス Hello を送信します。

- グレースフル リスタートがグローバルに設定してあること。
- グレースフル リスタートがインターフェイス上で設定してあること。
- 隣接ルータへの LSP が作成され、その LSP がインターフェイスを通過すること。

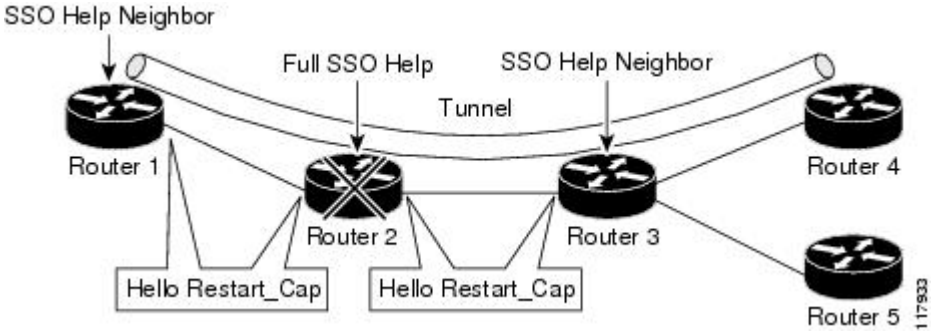
ネイバーがノード Hello をサポートしている場合は、ノード Hello を使用すること、またネイバールータがノード Hello をサポートしていない場合のみインターフェイス Hello を設定することを推奨します。

インターフェイス Hello とノード Hello の違いは次のとおりです。

- **インターフェイス hello**：Hello メッセージの IP ヘッダー内にある送信元アドレスには、Hello メッセージが送信されるインターフェイスと一致する IP アドレスが含まれます。IP ヘッダー内の宛先アドレスは、リンクのもう一方の側にあるネイバーのインターフェイスアドレスです。インターフェイス単位の Hello では TTL の 1 が使用され、直接接続されたネイバーに向かいます。
- **ノード hello**：Hello メッセージの IP ヘッダー内にある送信元アドレスには、送信側ルータの TE ルータ ID が含まれます。IP ヘッダーの宛先アドレスには、このメッセージの送信先であるネイバーのルータ ID が含まれます。1 より大きな TTL が使用されます。

次の図に、これらのメッセージに対するグレースフル リスタート拡張機能を示します。障害が発生すると、Restart_Cap という名前のオブジェクトによって、再起動可能なノードがネイバーに通知されます。2 つのネイバー間のリンクが停止しても、代替パスを介して隣接を維持できるように、これらのメッセージ内の存続可能時間（TTL）は、255 に設定されています。

**図 *37*：グレースフル リスタートの機能**




Restart_Cap オブジェクトには 2 つの値があります。1 つは再起動期間であり、障害発生後に送信側が RSVP_TE コンポーネントを再起動して Hello メッセージを交換するための時間です。もう 1 つは回復期間であり、送信者によって要求される、受信者が RSVP と MPLS データベースを同期化するための時間です。

上の図では、ルータ 1、ルータ 2、ルータ 3、およびルータ 4 でグレースフル リスタートが有効になっています。簡単に説明するため、すべてのルータが再起動可能であると仮定します。TE ラベル スイッチド パス（LSP）がルータ 1 からルータ 4 へシグナリングされます。

ルータ 2 とルータ 3 は、10,000 ミリ秒（10 秒）ごとに定期的なグレースフル リスタート Hello メッセージを交換します。また、ルータ 2 とルータ 1、およびルータ 3 とルータ 4 でも同様の処理が実行されます。次の例に示すように、ルータ 2 がその再起動期間を 60,000 ミリ秒（60 秒）、その回復期間を 60,000 ミリ秒（60 秒）としてアドバタイズするとします。

```
23:33:36: Outgoing Hello:
23:33:36:   version:1 flags:0000 cksum:883C ttl:255 reserved:0 length:32
23:33:36:   HELLO                type HELLO REQUEST length 12:
23:33:36:   Src_Instance: 0x6EDA8BD7, Dst_Instance: 0x00000000
23:33:36:   RESTART_CAP          type 1 length 12:
23:33:36:   Restart_Time: 0x0000EA60
, Recovery_Time: 0x0000EA60
```

（注） 再起動とリカバリの時間は、最後のエントリに**太字**で示されています。

このことは、ルータ 3 によってデータベースに記録されます。また、両方のネイバーで、ネイバー ステータスが UP に保たれます。ただし、ルータ 3 のコントロール プレーンには、ある時点で障害が発生します（たとえば、プライマリ ルート プロセッサ障害など）。その結果、RSVP と TE のシグナリング情報およびステートは失われます。一方、ラインカードによってデータ パケットの転送が続行されます。

ルータ 2 からの ACK メッセージの受け取りに 4 回失敗した（40 秒）時点で、ルータ 3 はルータ 2 との通信が失われたことを宣言し（「LOST」で示される）、再起動期間を開始して、前にルー

タ 2 でアドバタイズされて記録されている時間（60 秒）だけ待機します。ルータ 1 とルータ 2 は、Hello を除く、ルータ 3 へのすべての RSVP メッセージを抑制します。ルータ 3 は、LSP のステートが期限切れにならないように、RSVP Path メッセージおよび Resv リフレッシュ メッセージをルータ 4 およびルータ 5 に送信し続けます。ただし、ルータ 3 は、ルータ 2 に対してはこれらのメッセージを抑制します。

（注） ノードで ACK の受け取りに 4 回失敗した場合、またはその Hello src_instance（そのネイバーに送信された最後の送信元インスタンス）が変更されてその再起動期間が 0 になった場合、ノードは再起動されます。

再起動期間が満了する前に、ルータ 2 はその設定を再起動してロードします。ルータ 2 の設定により、グレースフル リスタートが行われ、新しい送信元インスタンスを持つ Hello メッセージが、接続されているすべてのデータ リンクに送信されます。ただし、ルータ 2 では、ネイバー ステートを失っているため、これらのメッセージ内に使用する必要のある宛先インスタンスを認識できません。このため、すべての宛先インスタンスは 0 に設定されます。

ルータ 3 は、ルータ 2 からの Hello を確認すると、ルータ 2 の再起動期間を停止し、ACK メッセージを戻します。ルータ 3 がルータ 2 からの Hello メッセージに新しいソースのインスタンス値を発見した場合に、ルータ 3 はルータ 2 のコントロール プレーンに障害が発生していることを把握します。ルータ 2 はルータ 3 の送信元インスタンス値を取得し、それを宛先インスタンスとして使用します。

また、ルータ 3 は、ルータ 2 からの Hello メッセージ内にある回復期間の値も確認します。回復期間が 0 の場合、ルータ 3 は、ルータ 2 がその転送情報を保持できなかったと認識し、ルータ 2 に関連するすべての RSVP ステートを削除します。

回復期間が 0 より多い場合、ルータ 1 は、以前にルータ 2 経由で送信した LSP ごとに、ルータ 2 に Path メッセージを送信します。これらのメッセージは、以前にサマリー メッセージ内でリフレッシュされていなければ、回復期間中に個別に送信されます。こうした Path メッセージのそれぞれには、障害発生前にルータ 2 から受信されたラベル値を含んだ Recovery_Label オブジェクトが含まれます。

ルータ 3 は、ルータ 2 から Path メッセージを受信すると、Resv メッセージをアップストリームに送信します。ただし、ルータ 3 は、Path メッセージを受信するまでは Resv メッセージを抑制します。

# MPLS TE：RSVP グレースフル リスタートの設定方法

## グレースフル リスタートのイネーブル化

（注） インターフェイスでのグレースフル リスタートの設定は、任意です。

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **iprsvpsignallinghellograceful-restartmodehelp-neighbor**
4. **interface***typenumber*
5. **iprsvpsignallinghellograceful-restart**
6. **exit**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **iprsvpsignallinghellograceful-restartmodehelp-neighbor**<br><br>例：<br><br>`Router(config)# ip rsvp signalling hello graceful-restart mode help-neighbor` | 再起動機能を持つネイバー ルータで、DSCP Hello メッセージの数を設定します。 |
| ステップ 4 | **interface***typenumber*<br><br>例：<br><br>`Router(config)# interface POS 1/0/0` | （任意）インターフェイスのタイプおよび番号を設定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 5 | **iprsvpsignallinghellograceful-restart**<br><br>例：<br><br>`Router(config-if)# ip rsvp signalling hello graceful-restart` | （任意）ネイバー ルータで RSVP TE グレースフル リスタート機能をイネーブルにします。 |
| ステップ 6 | **exit**<br><br>例：<br><br>`Router(config)# exit` | 特権 EXEC モードに戻ります。 |

# DSCP 値の設定

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **iprsvpsignallinghellograceful-restartdscp***num*
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 | イネーブル化<br><br>例：<br><br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br><br>`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 | **iprsvpsignallinghellograceful-restartdscp***num*<br><br>例：<br><br>`Router(config)# ip rsvp signalling hello graceful-restart dscp 30` | グレースフル リスタート対応のルータで、DSCP Hello メッセージの数を設定します。 |
| ステップ 4 | **end**<br><br>例：<br><br>`Router(config)# end` | 特権 EXEC モードに戻ります。 |

# Hello リフレッシュ間隔の設定

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **iprsvpsignallinghellograceful-restartrefreshinterval***interval-value*
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 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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 | **iprsvpsignallinghellograceful-restartrefreshinterval***interval-value*<br><br>例：<br>`Router(config)# ip rsvp signalling hello graceful-restart refresh interval 5000` | グレースフル リスタートがイネーブルになっているルータで、Hello リフレッシュ間隔を設定します。 |
| ステップ 4 | **end**<br><br>例：<br>`Router(config)# end` | 特権 EXEC モードに戻ります。 |

# リフレッシュ失敗制限の設定

## 手順の概要

1. イネーブル化
2. **configureterminal**
3. **iprsvpsignallinghellograceful-restartrefreshmisses***msg-count*
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 | イネーブル化<br><br>例：<br>`Router> enable` | 特権EXECモードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configureterminal**<br><br>例：<br>`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 | **iprsvpsignallinghellograceful-restartrefreshmisses***msg-count*<br><br>例：<br>`Router(config)# ip rsvp signalling hello graceful-restart refresh misses 5` | グレースフル リスタートがイネーブルになっているルータで、リフレッシュ制限を設定します。 |
| ステップ 4 | **end**<br><br>例：<br>`Router(config)# end` | 特権 EXEC モードに戻ります。 |

# グレースフル リスタート設定の確認

### 手順の概要

1. イネーブル化
2. **showiprsvphellograceful-restart**
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 | イネーブル化<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **showiprsvphellograceful-restart**<br><br>例：<br>`Router#` **show ip rsvp hello graceful-restart** | グレースフル リスタートのステータスおよび関連パラメータの情報を表示します。 |
| ステップ 3 | **end**<br><br>例：<br>`Router# end` | ユーザ EXEC モードに戻ります。 |

# MPLS TE：RSVP グレースフル リスタートの設定例

## MPLS TE - RSVP グレースフル リスタート：例

次の例では、グレースフルリスタートをイネーブルにし、DSCP値、リフレッシュ間隔、リフレッシュ失敗制限などの関連パラメータを設定しています。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp signalling hello graceful-restart mode help-neighbor
Router(config)# ip rsvp signalling hello graceful-restart dscp 30
Router(config)# ip rsvp signalling hello graceful-restart refresh interval 10000
Router(config)# ip rsvp signalling hello graceful-restart refresh misses 4
Router(config)# end
```

次の例では、グレースフル リスタートのステータスおよび設定されているパラメータを確認しています。

```
Router# show ip rsvp hello graceful-restart
Graceful Restart:Enabled (help-neighbor only)
  Refresh interval:10000 msecs
  Refresh misses:4
  DSCP:0x30
  Advertised restart time:0 secs
  Advertised recovery time:0 secs
  Maximum wait for recovery:3600000 secs
```

# 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 |
|---|---|
| RSVP コマンド：完全なコマンドの構文、コマンドモード、デフォルト、使用上の注意事項、および例 | 『Cisco IOS Quality of Service Solutions Command Reference』 |
| Quality of Service（QoS）分類 | 『Classification Overview』 |
| QoS シグナリング | 『Signalling Overview』 |
| QoS 輻輳管理 | 『Congestion Management Overview』 |
| ステートフル スイッチオーバー | 『Stateful Switchover』 |
| MPLS ラベル配布プロトコル | MPLS ラベル配布プロトコル（LDP） |
| ステートフル スイッチオーバー、Cisco ノンストップ フォワーディング、グレースフル リスタートに関する情報 | NSF/SSO：MPLS TE および RSVP グレースフル リスタート |
| RSVP Hello ステート タイマー | 『MPLS Traffic Engineering: RSVP Hello State Timer』 |

### 標準

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

### MIB

| MIB | MIB のリンク |
|---|---|
| この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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。<br>http://www.cisco.com/go/mibs |

### RFC

| RFC | Title |
|---|---|
| RFC 3209 | 『*RSVP-TE: Extensions to RSVP for LSP Tunnels*』 |
| RFC 3473 | 『*Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*』 |
| RFC 3478 | 『*Graceful Restart Mechanism for Label Distribution*』 |

### シスコのテクニカル サポート

| 説明 | Link |
|---|---|
| ★枠で囲まれた Technical Assistance の場合★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 |

# MPLS トラフィック エンジニアリング：RSVP グレースフル リスタートの機能情報

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 *15*：*MPLS* トラフィック エンジニアリング：*RSVP* グレースフル リスタートの機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| MPLS トラフィック エンジニアリング - RSVP グレースフル リスタート | 12.0(29)S<br>12.2(33)SRE<br>12.4(20)T<br>Cisco IOS XE Release 2.3 | MPLS TE - RSVP グレースフル リスタート機能を使用すると、隣接するルート プロセッサ（RP）が、MPLS フォワーディング ステートを失うことなく、コントロール プレーン サービス（具体的には、ラベル配布プロトコル（LDP）コンポーネント）の中断から回復できます。<br>この機能は、Cisco IOS Release 12.0(29)S で導入されました。<br>この機能は、Cisco IOS Release 12.4(20)T で統合されました。<br>次のコマンドが導入または変更されました: **ip rsvp signalling hello graceful-restart dscp**、**ip rsvp signalling hello graceful-restart mode help-neighbor**、**ip rsvp signalling hello graceful-restart refresh interval**、**ip rsvp signalling hello graceful-restart refresh misses**、**show ip rsvp counters**、**show ip rsvp counters state teardown**、**show ip rsvp hello**、**show ip rsvp hello client lsp detail**、**show ip rsvp hello client lsp summary**、**show ip rsvp hello client neighbor detail**、**show ip rsvp hello client neighbor summary**、**show ip rsvp hello graceful-restart**、**show ip rsvp hello instance detail**、および **show ip rsvp hello instance summary**。<br>Cisco IOS リリース 12.2(33)SRE では、ノード単位の Hello により、Cisco IOS リリース 12.0S との相互運用性がサポートされています。 |

# 用語集

**自律システム**：同じルーティング プロトコルを共有し、同じシステム管理者の管理下にあるネットワークの集合。

**ASBR**：Autonomous System Boundary Router（自律システム境界ルータ）。複数の自律システムを接続し、これらの間で情報を交換するルータ。

**バックアップ トンネル**：リンクまたはノードの障害発生時に他の（プライマリ）トンネルのトラフィックを保護するために使用される MPLS トラフィック エンジニアリング トンネル。

**DSCP**：Differentiated Services Code Point（DiffServ コード ポイント）。IETF によって定義された IP ヘッダー内の 6 ビット。これらのビットにより、IP パケットに提供されるサービス クラスが決まります。

**高速リルート**：リンク障害およびノード障害から MPLS トラフィック エンジニアリング（TE）LSP を保護するためのメカニズム。障害ポイントで LSP をローカルに修復することによって、ヘッドエンド ルータがエンドツーエンド LSP を確立してそれらを置き換えようとしたときにデータのフローを継続できるようになります。FRR は、障害が発生したリンクまたはノードをバイパスするバックアップ トンネルを介して再ルーティングすることによって、保護されている LSP をローカルに修復します。

**グレースフル リスタート**：ノード障害の発生後にネイバー ルート プロセッサを再起動するためのプロセス。

**ヘッドエンド**：特定の LSP の起点となり、その LSP を管理するルータ。これは、LSP パス上の最初のルータです。

**IGP**：Interior Gateway Protocol（内部ゲートウェイ プロトコル）。自律システム内でルーティング情報を交換するために使用されるインターネット プロトコルです。一般的なインターネット IGP の例として、IGRP、OSPF、および RIP を挙げることができます。

**インスタンス**：特定のルータ インターフェイス アドレスおよびリモート IP アドレスに対して RSVP Hello 拡張機能を実装するメカニズム。アクティブな Hello インスタンスは、定期的に Hello Request メッセージを送信し、応答として Hello ACK メッセージを予期します。予期されている ACK メッセージを受信できない場合、アクティブな Hello インスタンスは、そのネイバー（リモートの IP アドレス）が到達不能である（つまり失われている）ことを宣言します。これにより、このネイバーを通過する LSP の高速リルートが行われることがあります。

**ラベル**：スイッチング ノードに対してデータの転送方法（パケットまたはセル）を指示する短い固定長のデータ ID。

**LDP**：ラベル配布プロトコル（LDP）。ラベルとネットワーク プレフィックスの間のバインディングを配布することによって、MPLS ホップバイホップ転送をサポートするプロトコル。このプロトコルのシスコ独自のバージョンは、タグ配布プロトコル（TDP）です。

**LSP**：ラベル スイッチド パス。パケットの伝送に MPLS が使用される、2 台のルータ間に設定された接続。1 つ以上のラベル スイッチド ホップを連結して作成されたパスです。これにより、MPLS ノードからのラベルを別の MPLS ノードにスワップして、パケットを転送できます。

**マージ ポイント**：バックアップ トンネルの終端。

**MPLS**：マルチプロトコル ラベル スイッチング。ネットワークを介してパケット（フレーム）を転送する方式。MPLS により、ネットワークのエッジにあるルータはラベルをパケット（フレーム）に適用できます。ネットワーク コア内の ATM スイッチまたは既存のルータは、ラベルに従ってパケットを切り替えることができます。

**PLR**：Point of Local Repair（ローカル修復点）。バックアップ トンネルのヘッドエンド。

**RSVP**：Resource Reservation Protocol（リソース予約プロトコル）。IP ネットワーク上でリソースの予約をサポートするためのプロトコル。IP エンド システム上で動作しているアプリケーションは、RSVP を使用して、受信するパケット ストリームの特性（帯域幅、ジッタ、最大バーストなど）を他のノードに示すことができます。

**RP**：ルート プロセッサ。ルータのプロセッサ モジュールで、CPU、システム ソフトウェア、およびルータで使用されるメモリ コンポーネントの大半が含まれます。監視プロセッサと呼ばれることもあります。

**ステート**：ルータが各 LSP に関して保守する必要のある情報。この情報は、トンネルをリルートする場合に使用されます。

**テールエンド**：LSP が終端するルータ。これは、LSP のパス上の最後のルータです。

**TE**：トラフィック エンジニアリング。標準のルーティング方式が使用されていた場合に選択されたであろうパス以外のパス上のネットワーク経由でトラフィックを転送するために使用されるテクニックとプロセス。

**トポロジ**：企業ネットワーキング構造内のネットワーク ノードおよびメディアの物理的な配置。

**トンネル**：2 つのピア（2 つのルータなど）の間のセキュアな通信パス。