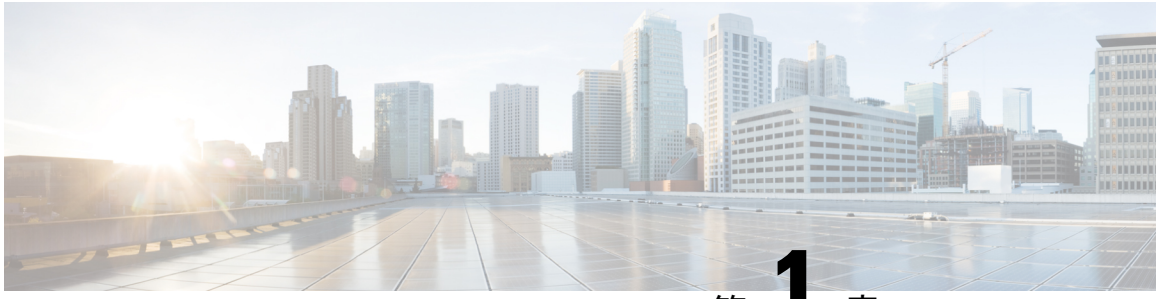
Cisco IOS XE Gibraltar 16.10.x セグメント ルーティング コンフィギュレーション ガイド

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

目 次



第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE Release 3.7.0E（Catalyst スイッチング用）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 つのリリースは、単一バージョンのコンバージドリリース Cisco IOS XE 16 に進化（マージ）しました。これにより、スイッチングおよびルーティング ポートフォリオにおける広範なアクセス製品およびエッジ製品を 1 つのリリースでカバーします。

機能情報

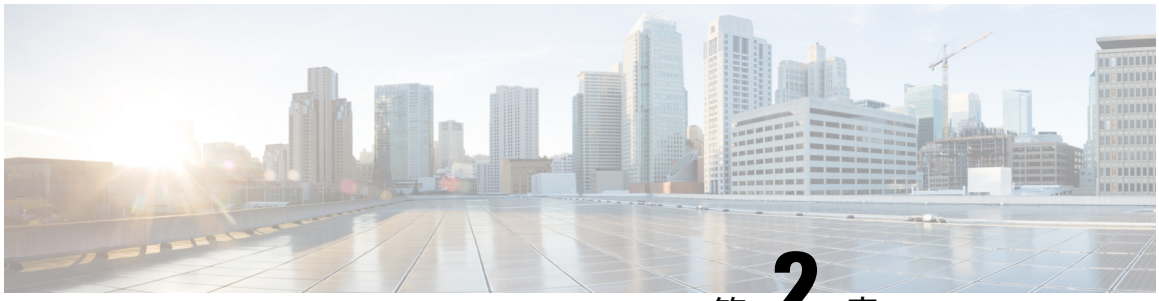
機能のサポート、プラットフォームのサポート、およびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco.com のアカウントは必要ありません。

参考資料

- 『Cisco IOS Command References, All Releases』

マニュアルの入手方法およびテクニカル サポート

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。



第 2 章

セグメント ルーティングの概要

この章では、セグメント ルーティング（SR）の概念を紹介します。

セグメント ルーティングの概要

セグメント ルーティング（SR）は、送信元ルーティングを実行するための柔軟でスケーラブルな方法です。送信元がパスを選択し、セグメントの番号付きリストとしてパケット ヘッダー内で暗号化します。セグメントは、すべてのタイプの命令の識別子です。各セグメントを識別するセグメント ID（SID）は、フラットな 32 ビットの符号なし整数で構成されます。次のようなセグメント命令があります。

- 最短パスを使用してノード N へ移動する
- ノード M への最短パスを介してノード N に移動した後にレイヤ 1、レイヤ 2、レイヤ 3 のリンクをたどる
- サービス S を適用する

セグメント ルーティングを使用すると、ネットワークでアプリケーションごとやフロー状態ごとに管理する必要がなくなります。代わりに、パケット内に指定されている転送命令に従います。

セグメント ルーティングは、シスコの Intermediate System-to-Intermediate System（IS-IS）および Open Shortest Path First（OSPF）プロトコルのいくつかの拡張機能に依存しています。MPLS（マルチプロトコル ラベル スイッチング）または IPv6 データ プレーンで動作でき、レイヤ 3 VPN（L3VPN）、仮想プライベート ワイヤ サービス（VPWS）、仮想プライベート LAN サー

ビス（VPLS）、イーサネット VPN（EVPN）などの、さまざまなマルチサービス機能と統合されます。

セグメント ルーティングは、転送プレーンを変更することなく、マルチプロトコル ラベル スイッチング（MPLS）アーキテクチャに直接適用できます。セグメント ルーティングは従来の MPLS ネットワークよりも効率的にネットワーク帯域幅を利用し、遅延を低減します。セグメントは MPLS ラベルとしてエンコードされます。セグメントの番号付きリストはラベルのスタックとしてエンコードされます。処理するセグメントは、スタックの一番上にあります。セグメントの完了後に関連するラベルがスタックからポップします。

セグメント ルーティングは、新しいタイプのルーティング拡張ヘッダーを使用して、IPv6 アーキテクチャに適用できます。セグメントは、IPv6 アドレスとしてエンコードされます。セグメントの順序付きリストは、ルーティング拡張ヘッダー内の IPv6 アドレスの順序付きリストとしてエンコードされます。処理するセグメントは、ルーティング拡張ヘッダー内のポインタによって示されます。ポインタは、セグメントの完了後にインクリメントされます。

セグメント ルーティングは自動トラフィック保護を提供しますが、トポロジ上の制約事項はありません。ネットワークがリンク障害やノード障害からトラフィックを保護し、ネットワーク内での追加シグナリングは必要ありません。既存の IP 高速再ルート（FRR）技術と、セグメント ルーティングの明示的なルーティング機能を組み合わせると、最適なバックアップ パスを備えた完全な保護適用範囲が保証されます。トラフィック保護には、他のシグナリング要件は適用されません。

セグメント ルーティングの仕組み

セグメント ルーティング ネットワーク内のルータは、明示的な最短パスか、または内部ゲートウェイ プロトコル（IGP）の最短パスかどうかにかかわらず、トラフィックを転送するパスを選択できます。セグメントは、ネットワークの宛先への完全なルートを形成するためにルータを組み合わせることができるサブパスを表しています。各セグメントには識別子（セグメント識別子）があり、新しい IGP 拡張機能を使用してネットワーク全体に配布されます。この拡張機能は IPv4 および IPv6 のコントロール プレーンに等しく適用されます。従来の MPLS ネットワークとは異なり、セグメント ルータ ネットワーク内のルータに Label Distribution Protocol（LDP）や Resource Reservation Protocol（RSVP）、つまり、セグメント識別子の割り当てや通知を行い、それらの転送情報をプログラミングするトラフィック エンジニアリング（RSVP-TE）は必要ありません。

各ルータ（ノード）と各リンク（隣接関係）には関連付けられたセグメント識別子（SID）があります。ノード セグメント識別子はグローバルに一意であり、IGP で決定されたルータへの最短パスを表します。ネットワーク管理者は各ルータに予約済みブロックからノード ID を割り当てます。一方、隣接関係セグメント ID はローカルで有効なものであり、出力インターフェイスなどの隣接ルータに固有の隣接関係を表します。ルータは、ノード ID の予約済みブロック外の隣接関係識別子を自動的に生成します。MPLS ネットワークでは、セグメント識別子は MPLS ラベル スタック エントリとしてエンコードされます。セグメント ID は指定したパスに沿ってデータを移動します。次の 2 種類のセグメント ID があります。

- **プレフィックス SID**：サービス プロバイダー コア ネットワーク内で IGP が計算した IP アドレス プレフィックスが含まれたセグメント ID。プレフィックス SID はグローバルに一

意です。プレフィックス セグメントは、特定のプレフィックスに到達する最短パス（IGP が計算）を表します。ノード セグメントは、ノードのループバック アドレスに結合された特殊なプレフィックス セグメントです。これは、インデックスとしてノード固有の SR グローバル ブロック（SRGB）にアドバタイズされます。

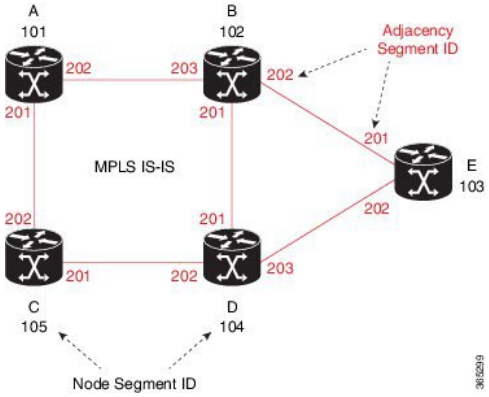
- **隣接関係 SID**：ネイバーへのアドバタイジング ルータの隣接関係が含まれたセグメント ID。隣接関係 SID は 2 つのルータ間のリンクです。隣接関係 SID は特定のルータに関連しているため、ローカルに一意となっています。

ノード セグメントはマルチホップ パスを使用できますが、隣接関係セグメントはワンホップ パスです。

セグメント ルーティングの例

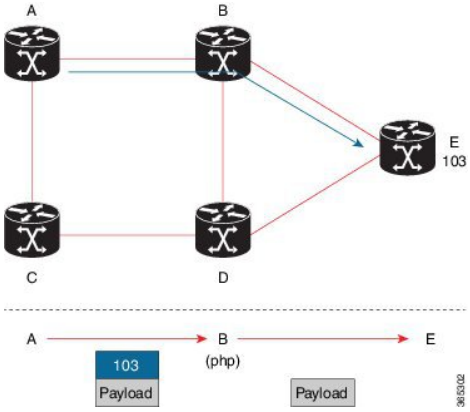
次の図は、セグメント ルーティング、IS-IS、ノード ID 用に 100 ～ 199 のラベル範囲、および 200 以上の隣接 ID を使用する、5 台のルータを含む MPLS ネットワークについて示しています。IS-IS は、ネットワーク全体にセグメント ID（MPLS ラベル）とともに IP プレフィックスの到達可能性を配布します。

図 *1*：セグメント ルーティングを使用する *5* 台のルータを含む *MPLS* ネットワーク



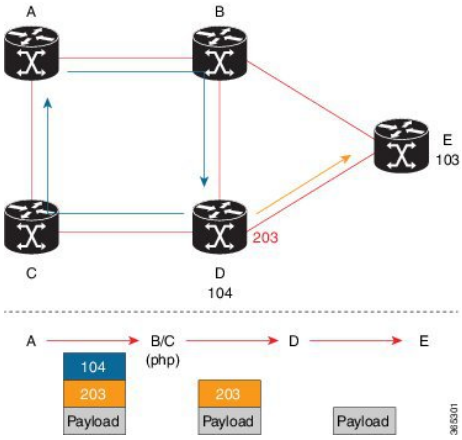
前の例では、ルータ E にトラフィックを送信しているルータは、ラベル 103（ルータ E ノード セグメント識別子）をプッシュし、IS-IS 最短パスを使用してトラフィックを転送します。各ホップでの MPLS ラベルスワッピング操作は、パケットが E に到着するまでラベル 103 を保持します（図 2）。一方、隣接関係セグメントの動作は異なります。たとえば、パケットが 203（D 対 E の隣接関係セグメント識別子）のスタック トップの MPLS ラベルを持つルータ D に到着する場合、ルータ D はラベルをポップし、ルータ E にトラフィックを転送します。

図 *2: MPLS* ラベルスワッピング操作



セグメント識別子は、トラフィック エンジニアリングを実行するための順序付きリストとして組み合わせることができます。セグメント リストには、転送要件に応じて複数の隣接関係セグメント、複数のノードセグメント、または両方の組み合わせを含めることができます。前の例では、ルータ A は、ラベル スタック（104、203）を代わりにプッシュし、最短パスとルータ D に該当するすべての ECMP を使用し、次に宛先への明示的なインターフェイスを通って、ルータ E に到達することができます（図 3）。ルータ A は新しいパスをシグナリングする必要がなく、状態情報はネットワーク内で一定に保たれます。ルータ A は、最終的に特定のパス経由でルータ E 宛てのどのフローを切り替えるかを決定する転送ポリシーを適用します。

図 *3:* ルータ *E* の宛先パス

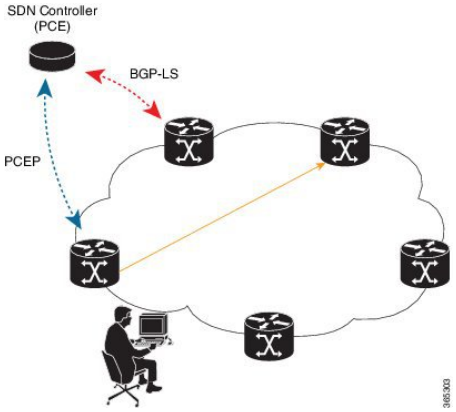


セグメント ルーティングの利点

- **SDN の準備**：セグメント ルーティングは、Software-Defined Network（SDN）の採用を構想した魅力的なアーキテクチャであり、アプリケーション対応ルーティング（AER）の基盤です。これは、自動リンクおよびノード保護などのネットワークベースの分散インテリジェンスと、トラフィック最適化などのコントローラベースの集中型インテリジェンスとの間のバランスをとります。厳格なネットワーク パフォーマンス保証、ネットワーク リ

ソースの効率的な使用、およびアプリケーションベースのトランザクションに対する非常に高いスケーラビリティを提供することができます。ネットワークは、これらの要件を満たすために最小限の状態情報を使用します。セグメント ルーティングは、コントローラベースの SDN アーキテクチャと簡単に統合できます。下図は、コントローラが帯域幅アドミッション コントロールなどの集中最適化を実行する SDN シナリオの例を示しています。このシナリオでは、コントローラがネットワーク トポロジとフローの全体像をもっています。ルータは、遅延、帯域幅、ダイバーシティなど、特定の特性を持つ宛先へのパスを要求できます。コントローラは最適なパスを計算し、MPLS ラベル スタックなどの対応するセグメント リストを要求元ルータに返します。その時点で、ルータはネットワークに追加のシグナリングなしでセグメント リストとともにトラフィックを注入できます。

図 *4 : SDN* コントローラ



- さらに、セグメント リストを使用すると、ネットワークにアプリケーションの状態を追加することなく、完全なネットワーク仮想化を実現できます。状態は、セグメントのリストとしてパケットにエンコードされます。ネットワークはセグメント状態を維持するだけなので、ネットワークに負荷をかけることなく、大量で高頻度のトランザクションベースのアプリケーション要求をサポートできます。

- **シンプル化**：
  - MPLS データ プレーンに適用された場合、セグメント ルーティングは、IGP（ISIS または OSPF）以外のプロトコルを使用せずに、入力プロバイダー エッジから出力プロバイダー エッジへの MPLS サービス（VPN、VPLS、および VPWS）をトンネリングする機能を提供します。
  - ラベル配布用に別のプロトコルを使用しない単純な動作です（たとえばLDPやRSVPが不要）。
  - トラブルシューティングを行うための複雑な LDP または IGP 同期はありません。
  - ECMP に対応した最短パス転送（ノード セグメント ID を使用）により、設置済みインフラストラクチャの使用率を向上し、設備投資（CapEx）を削減します。

- **Fast Reroute（FRR）をサポート**：任意のトポロジに対して自動化 FRR を提供します。ネットワーク内でリンクまたはノード障害が発生した場合、MPLS はFRR メカニズムを使

用してコンバージェンスを行います。セグメントルーティングでは、コンバージェンス時間は 50 ミリ秒以下です。

- **大規模データセンター**：
  - セグメント ルーティングでは、ボーダー ゲートウェイ プロトコル（BGP）RFC 3107（トップオブラック/リーフ/スパイン スイッチ間の IPv4 ラベル付きユニキャスト）を使用して、MPLS 対応のデータセンター設計を簡素化します。
  - BGP は、IGP ノード SID と同等のノード セグメント ID を配布します。
  - トポロジ内のノードは、同じスイッチに同じ BGP セグメントを割り当てます。
  - IGP ノード SID：ECMP および自動 FRR（BGP PIC（プレフィックス独立コンバージェンス））の場合と同じ利点が提供されます。
  - これは、トラフィック エンジニアリング（SR TE データセンター ファブリックの最適化）のためのビルディング ブロックです。
- **スケーラブル**：
  - LDP データベース内のラベルが何千にもなることを回避します。
  - ネットワーク内の MPLS トラフィック エンジニアリング LSP が何千にもなることを回避します。
  - 設定するトンネルが何千にもなることを回避します。
- **デュアルプレーン ネットワーク**：
  - セグメントルーティングは、プレーンがパーティション分割されていない限り、特定のプレーンからエッジ宛先へのルートがプレーン内に留まる、いわゆる「デュアルプレーン」ネットワーク内で独立であることを強制するための簡単なソリューションを提供します。
  - 追加の SID 「エニーキャスト」セグメント ID により、次のようなマクロ ポリシーの式が可能です。「ノード Z に向けてノード A に挿入されたフロー 1 は、プレーン 1 を経由しなければならない」および「ノード Z に向けてノード A に注入されたフロー 2 は、プレーン 2 を経由しなければならない」。
- **集中型トラフィック エンジニアリング**：
  - コントローラとオーケストレーション プラットフォームは、WAN 最適化などの集中型の最適化のために、セグメント ルーティング トラフィック エンジニアリングと対話することができます。
  - 輻輳などのネットワーク変更により、アプリケーションがセグメント ルーティング トラフィック エンジニアリング トンネルの配置を最適化（再計算）することをトリガーできます。
  - セグメント ルーティング トンネルは、PCE のようなサウスバウンド プロトコルを使用してオーケストレータからネットワーク上に動的にプログラムされます。

- セグメント ルーティング トンネルは中間点およびテール エンド ルータでのシグナリングおよびフローごとの状態を必要としないため、アジャイル ネットワーク プログラミングが可能です。

- **出力ピアリング トラフィック エンジニアリング（EPE）**：
  - セグメント ルーティングは集中型 EPE を可能にします。
  - コントローラは、特定の出力プロバイダーのエッジと特定の外部インターフェイスを使用して宛先に到達するように、入力プロバイダーのエッジとコンテンツ ソースに指示します。
  - BGP 「ピアリング」セグメント ID は、ソースルーティングされたドメイン間パスを表すために使用されます。
  - コントローラは、BGP リンクの状態（BGP-LS）EPE ルートを介して、BGP ピアリング SID と出力境界ルータの外部トポロジを学習します。
  - コントローラは、必要なパスを使用して入力ポイントをプログラムします。

- **プラグ アンド プレイ展開**：セグメント ルーティング トンネルは、既存の MPLS コントロール プレーンおよびデータ プレーンと相互運用可能で、既存の展開に実装できます。

セグメント ルーティング グローバル ブロック

セグメント ルーティング グローバル ブロック（SRGB）は、セグメント ルーティングに予約されたラベルの範囲のことです。SRGB は、セグメント ルーティング ノードのローカル プロパティです。MPLS アーキテクチャでは、SRGB はグローバル セグメントに予約済みの一連のローカル ラベルです。セグメント ルーティングでは、各ノードを異なる SRGB で設定できます。そのため、IGP プレフィックス セグメントに関連付けられた絶対 SID はノードごとに変更できます。

SRGB のデフォルト値は 16000 ～ 23999 です。SRGBは、次のように設定できます。

```
Device(config)# router isis 1
Device(config-isis)#segment-routing global-block 45000 55000
```

SRGB ラベル値は、次のように計算されます。

- プラットフォームが 100 万ラベル以上をサポートしている場合、SRGB 値は 90 万 ～ 90 万 + 2^16 です。
- プラットフォームでサポートされているラベルが 100 万未満の場合、SRGB 値は最後の 2^16 ラベルになります。

制約事項

- SRGB サイズは 2^16 より大きくすることはできません。
- SRGB の上限は、プラットフォームの能力を超えることはできません。

- SRGB は、デフォルトの SRGB と同じ値になるように設定することはできません。したがって、SRGB を 16000 ～ 23999 に設定することはできません。

セグメント ルーティング グローバル ブロック

この章では、セグメントルーティングを使用して、ルータ用に予約済みラベルのブロックを作成するという概念について説明します。この予約済みラベルのブロックは、セグメント ルーティング グローバル ブロック（SRGB）として知られています。

隣接関係セグメント識別子

隣接関係セグメント識別子（adj-SID）は、特定のインターフェイスとそのインターフェイスからの次のホップを指す、ローカル ラベルです。adj-SID を有効にするために必要な特定の設定はありません。アドレスファミリに対して IS-IS でセグメント ルーティングを有効にすると、IS-IS が実行されるあらゆるインターフェイスで、そのアドレスファミリは自動的にそのインターフェイスからのすべてのネイバーに adj-SID を割り当てます。

（注） IPV4 アドレスファミリのみが adj-SID の割り当てをサポートします。

プレフィックス セグメント識別子

プレフィックスセグメント識別子（SID）は、プレフィックスによって表される宛先につながるセグメント ルーティング トンネルを識別します。プレフィックス SID の最大値は 2^16 - 1 です。

プレフィックス SID は、セグメント ルーティング グローバル ブロック（SRGB）から割り当てられます。プレフィックス SID 値は、値が以下のように計算されるローカル MPLS ラベルに変換されます。

- プラットフォームが 100 万ラベル以上をサポートしている場合、プレフィックス SID 値に対応する MPLS ラベルは 90 万 + *SID* 値です。
- プラットフォームでサポートされるラベルが 100 万未満の場合、プレフィックス SID 値に対応する MPLS ラベルは最大サポート ラベル値 - 2^16 + *SID* 値です。

プレフィックス SID 値 *x* を設定すると、プレフィックス SID は、*x* + SRGB の下限境界に相当するラベル値に変換されます。たとえば、デフォルトの SRGB が使用される場合、100 万 MPLS ラベル以上をサポートするプラットフォームでは、IPv4 アドレス 1.0.0.1/32 を使用したインターフェイス ループバック 0 に対して 10 のプレフィックス SID を設定すると、ラベル 9000010 16010 がプレフィックス 1.0.0.1/32 に割り当てられます。

BGP プレフィックス セグメント識別子

BGP プレフィックスに関連付けられたセグメントは、BGP プレフィックス SID と呼ばれます。

- BGP プレフィックス SID は、セグメント ルーティングまたは BGP ドメイン内で常にグローバルです
- BGP プレフィックス SID は、所定のプレフィックスに対して BGP によって計算された ECMP 対応のベスト パス上のパケットを転送する命令を識別します

セグメント ルーティングでは、セグメント ルーティング グローバル ブロック（SRGB）を使用して BGP スピーカーを設定する必要があります。一般的に SRGB は、ラベルの範囲、SRGB = [SR_S, SR_E] として構成されます。

- SR_S = 範囲の開始
- SR_E = 範囲の終わり

各プレフィックスには、固有のラベル インデックスが割り当てられます。

次の例では、route-policy **name** コマンドを使用して、set label index という BGP ルート ポリシーが定義されます。

BGP でセグメント ルーティング グローバル ブロック（SRGB）を設定します。ルート ラベル パスにラベルインデックス属性があり、SRGB が設定されている場合、ローカル ラベル ルートは SRGB から割り当てられます。ルートポリシーを使用して再配布されたルートにラベルインデックスが追加されると、BGP はルートとともに属性としてラベルインデックスを提示します。

```
router bgp 100
 bgp log-neighbor-changes
 neighbor 192.0.2.1 remote-as 100
 neighbor 192.0.2.1 update-source Loopback0
 neighbor 192.0.23.3 remote-as 300
 !
 address-family ipv4
  segment-routing mpls
  neighbor 192.0.2.1 activate
  neighbor 192.0.2.1 send-label
  neighbor 192.0.23.3 activate
 exit-address-family
```

セグメント ルーティングに関する追加情報

関連資料

関連項目	マニュアル タイトル
動画	• シスコ セグメント ルーティングの概要（YouTube） • シスコセグメントルーティングの概要（CCO）

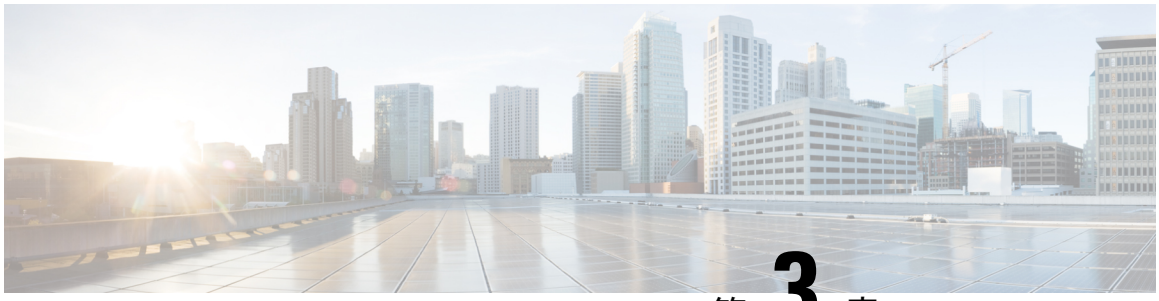
セグメント ルーティングの概要の機能情報

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

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

表 *1:* セグメント ルーティングの概要の機能情報

機能名	リリース	機能情報
セグメント ルーティングの概要	Cisco IOS XE Release 3.16S Cisco IOS XE Fuji 16.7.1	セグメントルーティング（SR）は、送信元ルーティングを実行するための柔軟でスケーラブルな方法です。 Cisco IOS XE Fuji 16.7.1 では、この機能は Cisco 4000 シリーズ サービス統合型ルータでサポートされています。



第 3 章

IS-IS v4 ノード SID のセグメント ルーティング

この章では、セグメント ルーティング（SR）が IS-IS でどのように機能するかについて説明します。

IS-IS v4 ノード SID のセグメント ルーティングの制限

- ルーティング プロトコルの構成をそのルータ構成のサブ モードで許可する前に、セグメント ルーティングを最上位レベルで設定する必要があります。
- IS-IS プロトコルの SR コマンドは、トポロジごと（IPv4 アドレス ファミリ）に基づいています。
- 有効な Cisco IOS-XE リリース 3.16 では、ISIS は IPv4 に対してのみセグメント ルーティングをサポートしています。

IS-IS v4 ノード SID のセグメント ルーティングに関する情報

セグメント ルーティング IS-IS v4 ノード SID

セグメント ルーティングは、シスコの Intermediate System-to-Intermediate System（IS-IS）および Open Shortest Path First（OSPF）プロトコルのいくつかの拡張機能に依存しています。ルー

ティング プロトコル インスタンスのセグメント ルーティングを有効にするには、2 つのレベルの構成が必要です。セグメント ルーティング インフラストラクチャ コンポーネントによって管理される最上位のセグメント ルーティング構成では、セグメント ルーティングが可能になり、一方、ルータ レベルでのセグメント ルーティング構成では、ルーティング プロトコル インスタンスの特定のアドレスファミリに対してセグメントルーティングが可能になります。セグメント ルーティングの状態には、次の 3 つがあります。

- SR_NOT_CONFIGURED
- SR_DISABLED
- SR_ENABLED

IGP 下のセグメント ルーティング構成は、SR の状態が SR_DISABLED または SR_ENABLED のいずれかである場合にのみ許可されます。SR_ENABLED 状態は、少なくとも MFI によって正常に予約済みの有効な SRGB 範囲にあることを示します。コマンドを使用して、ルータ設定サブ モードで IGP のセグメント ルーティングを有効にすることができます。ただし、IGP セグメント ルーティングは、グローバル SR が設定された後にのみ有効になります。

（注） IS-IS プロトコルの SR コマンドは、トポロジごと（IPv4 アドレス ファミリ）に基づいています。

SR_ENABLED は、SR を有効にするためにすべてのプロトコルに必要な状態ですが、プロトコル インスタンスの SR を有効にするには十分ではありません。その理由は、IS-IS にセグメント ルーティング グローバル ブロック（SRGB）情報に関する情報がまだないことです。SRGB に関する情報を受信する要求が正常に処理されると、IS-IS SR の動作状態が有効になります。

セグメントルーティングでは、各ルータが、セグメントルーティングデータプレーン機能と、グローバル SID が割り当てられている場合にセグメント ルーティングに使用される MPLS ラベル値の範囲をアドバタイズする必要があります。データプレーン機能とラベル範囲は、RFC4971 で定義されている、IS-IS ルータ機能 TLV-242 に挿入される SR 機能サブ TLV を使用してアドバタイズされます。

ISIS SR 機能サブ TLV には、すべての予約済み SRGB 範囲が含まれます。ただし、シスコの実装でサポートされる SRGB 範囲は 1 つだけです。サポートされている IPv4 プレフィックス SID サブ TLV は、TLV-135 および TLV-235 です。

リモートルータからのラベルスイッチドパスで受信されたプレフィックス SID

到達可能性 TLV（TLV 135 および 235）を使用してラベル スイッチド パス（LSP）で受信したプレフィックス SID は、次の条件が満たされている場合にのみ、プレフィックス VPN ラベルごとの BGP ダウンロードと同じ方法でルーティング情報ベース（RIB）にダウンロードされます。

- トポロジとアドレスファミリに対してセグメント ルーティングが有効。
- プレフィックス SID が有効。

• MFI へのローカル ラベルのバインドが成功している。

（注）
- 指定された SID 範囲に収まらない SID の場合、RIB の更新時にラベルは使用されません。SID が SID の範囲内には収まるが、ネクストホップのネイバー SID の範囲には収まらない場合は、そのパスに関連付けられているリモート ラベルはインストールされません。
- 到達可能性 TLV（TLV 135 および 235）を使用して LSP で受信されたノード SID は、対応するアドレスファミリでセグメント ルーティングが有効になっている場合にのみ RIB にダウンロードされます。
- 複数のベスト ネクスト ホップの場合は、すべてのネクスト ホップがセグメント ルーティングをサポートしていないと、ISIS は同じプレフィックスに割り当てられた一致しないラベルに類似したインスタンスを処理します。つまり、IS-IS がラベルを無視し、すべての ECMP パスについてラベルのないパスをグローバル RIB にインストールすることを意味します。

セグメント ルーティング隣接関係 SID アドバタイズメント

Cisco IOS XE リリース 3.17 では、IS-IS によるセグメント ルーティング隣接関係 SID のアドバタイズメントのサポートが有効です。隣接関係セグメント識別子（Adj-SID）は、セグメント ルーティングにおけるルータ隣接関係を表します。

セグメントルーティング対応ルータは、隣接関係ごとにAdj-SIDを割り当てることができ、この SID を隣接関係 TLV で伝送するように Adj-SID サブ TLV が定義されます。IS-IS 隣接関係は、次のいずれかのネイバー TLV を使用してアドバタイズされます。

- TLV-22 [RFC5305]
- TLV-23 [RFC5311]

IS-IS は、IS-IS 隣接関係状態がアップであり、IS-IS セグメント ルーティングの内部動作状態が有効になっている場合にのみ、IS-IS ネイバーごとに隣接関係 SID を割り当てます。ラベル リソースの不足が原因で隣接関係 SID の割り当てに失敗した場合、IS-IS は、デフォルトの間隔（30 秒）で定期的に Adj-SID の割り当てを再試行します。

複数の隣接関係 SID

Cisco IOS XE リリース 3.18 では、複数の隣接関係 SID がサポートされています。保護された P2P/LAN 隣接関係のそれぞれに対して、IS-IS は 2 つの Adj-SID を割り当てます。バックアップ Adj-SID は、インターフェイス上で FRR（ローカル LFA）が有効になっているときにのみ割り当てられ、アドバタイズされます。FRR が無効になっている場合は、バックアップ隣接関係 SID が解放されます。フォワーディング プレーンでの保護された adj-SID の永続化はサポートされます。プライマリ リンクがダウンしている場合、IS-IS は、遅延タイマーが期限切れになるまでバックアップ Adj-SID の解放を遅らせます。これにより、フォワーディング プレーンは、ルータがコンバージされるまで、バックアップ パスを経由してトラフィックを転送し続けることができます。

Cisco IOS XE リリース 3.18 では、フォワーディング プレーンがプロトコル固有のレベルを認識しないので、IS-IS Adj-SID はレベルごとに変更されます。割り当てられ、アドバタイズされたバックアップ Adj-SID は、**show isis neighbor detail** および **show isis data verbose** コマンドの出力で表示できます。

セグメント ルーティング マッピング サーバ（SRMS）

セグメントルーティングマッピングサーバ（SRMS）を使用すると、プレフィックスSIDマッピング ポリシー エントリの構成と保守を行うことができます。Cisco IOS XE リリース 3.17 では、IGP は SRMS のアクティブ ポリシーを使用して、フォワーディング プレーンのプログラミング時に SID 値を決定します。

SRMS は、ネットワークの SID/ラベル マッピング ポリシーにプレフィックスを提供します。一方、IGP は、プレフィックス SID/ラベル バインディング TLV を介して SID/ラベル マッピング ポリシーにプレフィックスをアドバタイズする役割を担います。アクティブ ポリシー情報と変更は、アクティブ ポリシー情報を使用して転送情報を更新する IGP に通知されます。

接続されたプレフィックス SID

場合によってはルータは、LSP にアドバタイズするものとは異なる SID を持つプレフィックスをインストールすることがあります。たとえば、複数のプロトコルまたは複数の IGP インスタンスが、異なる SID を持つ同じプレフィックスを SRMS にアナウンスしている場合、SRMS は競合を解決し、ローカルインスタンスと同じでない可能性がある競合に勝ったプレフィックスと SID をアナウンスします。その場合、IGP は、常にソース LSP から学習した内容をアドバタイズしますが、その LSP で学習したものとは異なる可能性がある SID のインストールを試みます。これは IGP が別のプロトコルまたは別のプロトコル インスタンスから SID を再配布することを防ぐために行われます。

SRGB 範囲の変更

IS-IS セグメント ルーティングが設定されている場合、IS-IS は、IS-IS SR の動作状態を有効にする前に SRGB とのインタラクションを要求する必要があります。SRGB 範囲が作成されていない場合、IS-IS は有効になりません。

SRGB 変更イベントが発生した場合、IS-IS は、そのサブブロック エントリで対応する変更を行います。また IS-IS は、SR 機能サブ TLV で新しく作成または拡張された SRGB 範囲をアドバタイズし、プレフィックス SID サブ TLV アドバタイズメントを更新します。

（注） Cisco IOS XE リリース 3.16 では、変更に対して 1 つの SRGB 範囲と SRGB 拡張機能のみがサポートされます。

SRGB の削除

IS-IS が SRGB 削除イベントを受信すると、IS-IS は、IS-IS SRGB キューのリストで SRGB エントリを検索します。SRGB エントリが存在しない場合、IS-IS は保留中の SRGB が作成されたイベントがないことを確認します。保留中の SRGB 作成イベントが見つかった場合、IS-IS は SRGB 作成イベントを削除し、SRGB の削除処理を完了します。

IS-IS SRGB キューで SRGB エントリが見つかった場合、IS-IS は SRGB をロックし、RIB を再配布し、保留中の削除 SRGB 範囲内の SID の値を持つすべてのプレフィックス SID をアドバタイズせず、SR 機能サブ TLV から SRGB 範囲をアドバタイズしません。IS-IS は SRGB の削除処理を完了すると、SRGB のロックを解除し、その SR サブブロック エントリから SRGB を削除します。

SRGB の削除後に有効な SRGB がない場合、IS-IS SR の動作状態が無効になります。

インターフェイスでの MPLS 転送

セグメント ルーティングがインターフェイスを使用する前に、MPLS 転送を有効にする必要があります。IS-IS は、インターフェイスでの MPLS 転送を有効にする役割を担います。

セグメント ルーティングが IS-IS トポロジに対して有効になっている場合、または IS-IS セグメント ルーティングの動作状態が有効になっている場合、IS-IS は、IS-IS トポロジがアクティブである任意のインターフェイスに対して MPLS を有効にします。同様に、IS-IS トポロジのセグメント ルーティングが無効になっている場合、IS-IS は、そのトポロジのすべてのインターフェイスで MPLS 転送を無効にします。

セグメント ルーティングと LDP の設定

コマンド **sr-label-preferred** により、転送インターフェイスは、トポロジ内のすべてのプレフィックスに対して、セグメント ルーティング ラベルを LDP ラベルより優先させることができます。

セグメント ルーティング トラフィック エンジニアリング アナウンス

IS-IS は、少なくとも 1 つのレベルに対して IS-IS SR と TE の両方が有効になっていることを検出した場合に、SR 情報を TE にアナウンスします。IS-IS は、TE が設定されているレベルから取得された情報のみをアナウンスします。

同様に、IS-IS は、SR が有効になっていないこと、または TE がどのレベルでも設定されていなくなったことを検出したときに、すべてのアナウンスを削除するように TE に指示します。

セグメント ルーティングの設定方法：IS-IS v4 ノード SID

セグメント ルーティングの設定

始める前に

セグメント ルーティングをサポートするように IS-IS を設定する前に、最初にグローバル コンフィギュレーション モードでセグメント ルーティング機能を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. segment-routing mpls
4. connected-prefix-sid-map
5. address-family ipv4
6. 1.1.1.1/32 index 100 range 1
7. exit-address-family

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	segment-routing mpls 例： `Device(config-sr)# segment-routing mpls`	mplsデータ プレーンを使用してセグメント機能を有効にします。
ステップ 4	connected-prefix-sid-map 例： `Device(config-srmpls)# connected-prefix-sid-map`	ローカル プレフィックスと SID のアドレス ファミリ固有のマッピングを設定できるサブモードを開始します。
ステップ 5	address-family ipv4 例：	IPv4 アドレス プレフィックスを指定します。

	コマンドまたはアクション	目的
	`Device(config-srmpls-conn)# address-family ipv4`	
ステップ 6	1.1.1.1/32 index 100 range 1 例： `Device(config-srmpls-conn-af)# 1.1.1.1/32 100 range 1`	SID 100 にアドレス 1.1.1.1/32 を関連付けます。
ステップ 7	exit-address-family 例： `Device(config-srmpls-conn-af)# exit-address-family`	アドレス ファミリを終了します。

IS-IS ネットワークでのセグメント ルーティングの設定

始める前に

IS-IS ネットワークでセグメント ルーティングを設定するには、その前にネットワークで IS-IS をイネーブルにする必要があります。

手順の概要

1. router isis
2. net network-entity-title
3. metric-style wide
4. **segment-routing** mpls
5. exit
6. show isis segment-routing

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	router isis 例： `Device(config-router)# router isis`	IS-IS ルーティング プロトコルをイネーブルにし、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 2	net network-entity-title 例： `Device(config-router)# net 49.0000.0000.0003.00`	ルーティング インスタンスの Network Entity Title（NET）を設定します。
ステップ 3	metric-style wide 例：	ワイド リンク

	コマンドまたはアクション	目的
	`Device(config-router)# metric-style wide`	メトリックだけを生成および受け入れるようにデバイスを設定します。
ステップ 4	**segment-routing** mpls 例： `Device(config-router)# segment-routing mpls`	セグメントルーティングの動作状態を設定します。
ステップ 5	exit 例： `Device(config-router)# exit`	セグメントルーティングモードを終了し、コンフィギュレーション端末モードに戻ります。
ステップ 6	show isis segment-routing 例： `Device# show is-is segment-routing`	（任意）IS-IS セグメント ルーティングの現在の状態を表示します。

例

次の例は、IS-IS のセグメント ルーティングに対する show isis segment-routing state コマンドからの出力を表しています。

```
Device# show isis segment-routing

ISIS protocol is registered with MFI
ISIS MFI Client ID:0x63
Tag 1 - Segment-Routing:
   SR State:SR_ENABLED
   Number of SRGB:1
   SRGB Start:16000, Range:8000, srgb_handle:0x4500AED0, srgb_state: created
   Address-family IPv4 unicast SR is configured
     Operational state:Enabled
```

IS-IS のプレフィックス SID の設定

ここでは、各インターフェイスでプレフィックスセグメント ID（SID）を設定する方法について説明します。

始める前に

セグメント ルーティングを対応するアドレス ファミリでイネーブルにする必要があります。

手順の概要

1. enable
2. configure terminal

3. segment-routing mpls
4. connected-prefix-sid-map
5. address-family ipv4
6. 1.1.1.1/32 index 100 range 1
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	enable 例： `Device# enable`	特権 EXEC モードをイネーブルにします。
ステップ 2	configure terminal 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	segment-routing mpls 例： `Device(config)# segment-routing mpls`	セグメント ルーティング MPLS モードを設定します。
ステップ 4	connected-prefix-sid-map 例： `Device(config-srmpls)# connected-prefix-sid-map`	ローカル プレフィックスと SID のアドレス ファミリ固有のマッピングを設定できるサブモードを開始します。
ステップ 5	address-family ipv4 例： `Device(config-srmpls-conn)# address-family ipv4`	IPv4 アドレス ファミリを指定し、ルータ アドレス ファミリ 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	1.1.1.1/32 index 100 range 1 例： `Device(config-srmpls-conn-af)# 1.1.1.1/32 100 range 1`	SID 100 にアドレス 1.1.1.1/32 を関連付けます。
ステップ 7	exit 例： `Device(config-router)# exit`	セグメント ルーティング モードを終了し、コンフィギュレーション端末モードに戻ります。

プレフィックス属性 N-flag-clear の設定

デフォルトでは、ループバック アドレスに関連付けられた SID をアドバタイズするときに、IS-IS によって N-flag と呼ばれるフラグが設定されます。このフラグをクリアするには、明示的な設定を追加します。

手順の概要

1. **enable**
2. **configure terminal**
3. interface loopback3
4. isis prefix n-flag-clear

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface loopback3 例： `Device(config)# interface loopback3`	インターフェイス ループバックを指定します。
ステップ 4	isis prefix n-flag-clear 例： `Device(config-if)# isis prefix n-flag-clear`	プレフィックス N-flag をクリアします。

明示的ヌル属性の設定

penultimate-hop-popping（PHP）を無効にし、明示的ヌル ラベルを追加するには、explicit-null オプションを指定する必要があります。オプションを指定すると、IS-IS は、プレフィックス SID サブ TLV に E フラグを設定します。

デフォルトでは、ループバック アドレスに関連付けられたプレフィックス SID をアドバタイズするときに、IS-IS によって E-flag（明示的ヌル フラグ）と呼ばれるフラグが 0 に設定されます。このフラグを設定するには、明示的な設定を追加します。

手順の概要

1. **enable**
2. **configure terminal**
3. segment-routing mpls
4. set-attributes
5. address-family ipv4
6. explicit-null
7. exit-address-family

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	segment-routing mpls 例： `Device(config)# segment-routing mpls`	セグメント ルーティング MPLS モードを設定します。
ステップ 4	set-attributes 例： `Device(config-srmpls)# set-attributes`	属性を設定します。
ステップ 5	address-family ipv4 例： `Device(config-srmpls-attr)# address-family ipv4`	IPv4 アドレス ファミリを指定し、ルータ アドレス ファミリ 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	explicit-null 例： `Device(config-srmpls-attr-af)# explicit-null`	明示的ヌルを指定します。
ステップ 7	exit-address-family 例： `Device(config-srmpls-attr-af)# exit-address-family`	アドレス ファミリを終了します。

セグメント ルーティング Label Distribution Protocol 優先順位の設定

手順の概要

1. **enable**
2. **configure terminal**
3. segment-routing mpls
4. set-attributes
5. address-family ipv4
6. sr-label-preferred
7. exit-address-family

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	segment-routing mpls 例： `Device(config)# segment-routing mpls`	セグメント ルーティング MPLS モードを設定します。
ステップ 4	set-attributes 例： `Device(config-srmpls)# set-attributes`	属性を設定します。
ステップ 5	address-family ipv4 例： `Device(config-srmpls-attr)# address-family ipv4`	IPv4 アドレス ファミリを指定し、ルータ アドレス ファミリ 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	sr-label-preferred 例： `Device(config-srmpls-attr-af)# sr-label-preferred`	LDP より優先される SR ラベルを指定します。

	コマンドまたはアクション	目的
ステップ 7	exit-address-family 例： `Device(config-srmpls-attr-af)# exit-address-family`	アドレス ファミリを終了します。

IS-IS SRMS の設定

次のコマンドは、IS-IS SRMS を有効にして、IS-IS がローカル マッピング エントリをアドバタイズできるようにします。IS-IS は、SRMS ライブラリにリモート エントリを送信しません。ただし、IS-IS は、ローカルに設定されたマッピング エントリのみに基づいて計算される SRMS アクティブ ポリシーを使用します。

```
[no] segment-routing prefix-sid-map advertise-local
```

IS-IS SRMS クライアントの設定

デフォルトでは、IS-IS SRMS クライアント モードが有効になっています。IS-IS は、常に SRMS に LSP を通じて受信したリモート プレフィックス SID マッピング エントリを送信します。SRMS アクティブ ポリシーは、ローカルおよびリモートのマッピング エントリに基づいて計算されます。

次のコマンドを実行すると、プレフィックス SID マッピング クライアント機能が無効になります。これは受信側で設定されます。

```
segment-routing prefix-sid-map receive [disable]
```

IS-IS SID バインド TLV ドメイン フラッディングの設定

デフォルトでは、IS-IS SRMS サーバは、ルーティング ドメイン内の SID バインディング エントリをフラッディングしません。Cisco IOS-XE リリース 3.18 から、IS-IS SRMS サーバ モード コマンドにオプションのキーワード **domain-wide** が追加され、SID およびラベル バインド TLV フラッディング機能が有効になります。

```
segment-routing prefix-sid-map advertise-local [domain-wide]
```

キーワード **domain-wide** を使用すると、IS-IS SRMS サーバは、ルーティング ドメイン全体で SID バインド TLV をアドバタイズできます。

（注） このオプションは、IS-IS SRMS が SRMS サーバ モードで実行する場合にのみ有効です。

セグメント ルーティングの設定例：IS-IS v4 ノード SID

例：IS-IS ネットワークでのセグメント ルーティングの設定

次の例では、各インターフェイスでプレフィックスセグメントID（SID）を設定する方法について説明します。

```
Device(config)#segment-routing mpls
 Device(config-srmpls)#connected-prefix-sid-map
  Device(config-srmpls-conn)#address-family ipv4
   Device(config-srmpls-conn-af)#10.1.2.2/32 index 2 range 1
  Device(config-srmpls-conn-af)#exit-address-family
 Device(config-srmpls-conn-af)#end
```

例：明示的ヌル属性の設定

明示的ヌル属性を設定する例を次に示します。

```
Device(config)# segment-routing mpls
Device(config-srmpls)# set-attributes
 Device(config-srmpls-attr)# address-family ipv4
  Device(config-srmpls-attr-af)# explicit-null
 Device (config-srmpls-attr-af)# exit-address-family
```

IS-IS v4 ノード SID のセグメント ルーティングに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』 http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html
IP ルーティング ISIS コマンド	『Cisco IOS IP Routing ISIS commands』 http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

RFC

RFC	タイトル
RFC4971	『Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information』

RFC	タイトル
RFC5305	『IS-IS Extensions for Traffic Engineering』。IPv4 用のルータ ID のアドバタイズメントを定義します。
RFC6119	『IPv6 Traffic Engineering in IS-IS』。IPv6 用のルータ ID のアドバタイズメントを定義します。

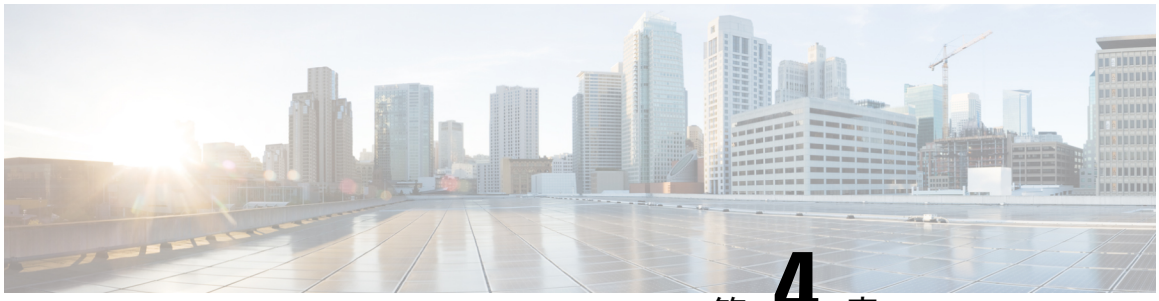
セグメント ルーティングの機能情報：IS-IS v4 ノード SID

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 *2*：セグメント ルーティングの機能情報：*IS-IS v4* ノード *SID*

機能名	リリース	機能情報
セグメント ルーティング：IS-IS v4 ノード SID	Cisco IOS XE Release 3.16S Cisco IOS XE Fuji 16.7.1	セグメント ルーティング：ISIS v4 ノード SID 機能は、IS-IS ネットワークでのセグメント ルーティングのサポートを提供します。 次のコマンドが導入または変更されました。**connected-prefix-sid-map**、 **show isis segment-routing**、**isis prefix n-flag-clear**、**explicit-null** Cisco IOS XE Fuji 16.7.1 では、この機能は Cisco 4000 シリーズ サービス統合型ルータでサポートされています。



第 4 章

IS-IS リンク保護のトポロジに依存しないループ フリー代替高速再ルーティング

このドキュメントでは、セグメントルーティング（SR）のトポロジに依存しないループフリー代替（TI-LFA）リンク保護を使用した IP 高速再ルーティング機能（IPFRR）の機能性と IS-IS の実装について説明します。

IS-ISリンク保護のトポロジに依存しないループフリー代替高速再ルーティングの前提条件

- すべてのノードで TI-LFA を有効にしてから、TI-LFA 用の SR-TE を設定してください。

```
mpls traffic-eng tunnels
!
segment-routing mpls
 connected-prefix-sid-map
  address-family ipv4
   1.1.1.1/32 index 11 range 1
  exit-address-family
 !
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
 ip router isis 1
!
```

```
interface Tunnel1
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 10 explicit name IP_PATH segment-routing
!
interface GigabitEthernet2
 ip address 192.168.1.1 255.255.255.0
 ip router isis 1
 negotiation auto
 mpls traffic-eng tunnels
 isis network point-to-point
!
interface GigabitEthernet3
 ip address 192.168.2.1 255.255.255.0
 ip router isis 1
 negotiation auto
 mpls traffic-eng tunnels
 isis network point-to-point
!
router isis 1
 net 49.0001.0010.0100.1001.00
 is-type level-1
 metric-style wide
 log-adjacency-changes
 segment-routing mpls
 fast-reroute per-prefix level-1 all
 fast-reroute ti-lfa level-1
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng level-1
!
ip explicit-path name IP_PATH enable
 next-address 4.4.4.4
 next-address 5.5.5.5
 next-address 6.6.6.6
```

- プライマリとセカンダリのパス切り替えの場合で、ルータ間でマイクロループが作成された場合は、コンバージェンス時間を減らす必要があります。**microloop avoidance rib-update-delay** コマンドを使用して、コンバージェンス時間を減らします。

```
router isis ipfrr
net 49.0001.0120.1201.2012.00
is-type level-2-only
metric-style wide
log-adjacency-changes
segment-routing mpls
segment-routing prefix-sid-map advertise-local
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
microloop avoidance rib-update-delay 10000
```

- 高可用性（HA）切り替え後のトラフィック損失を削減または最小化するために、MPLS-TE ノンストップ ルーティング（NSR）と IS-IS ノンストップ フォワーディング（NSF）を有効にします。グローバル EXEC モードで **mpls traffic-eng nsr** コマンドを使用します。

```
mpls traffic-eng nsr
```

IS-IS で **nsf** コマンドを使用します。

```
router isis
nsf cisco
nsf interval 0
```

IS-ISリンク保護のトポロジに依存しないループフリー代替高速再ルーティングについて

ローカル LFA およびリモート LFA が有効になっている場合、保護すべきプレフィックスのカバレッジは良好になります。ただし、PQ インターセクト ノードを持たないいくつかのまれなトポロジでは、ローカルおよびリモート LFA のどちらも、失敗したリンクを保護するために解放ノードを見つけることに失敗します。さらに、2 つのアルゴリズムには LFA のコンバージェンス後の特性についての知識がないため、コンバージェンス後の経路を優先する方法はありません。

上記の制限を克服するために、有効な Cisco IOS-XE リリース 3.18 では、トポロジに依存しない LFA（TI-LFA）が SR 対応ネットワークでサポートされます。

トポロジに依存しないループ フリー代替

TI-LFA は以下のためのサポートを提供します。

- リンク保護：LFA はリンクの障害のための修復パスを提供します。
- ローカル LFA：コンバージェンス後のパスのローカル LFA が利用可能であるときはいつでも、ローカル LFA は修復パスのための追加 SID を必要としないので、TI LFA より優先されます。つまり、PQ ノードのラベルは、リリース ノードには必要ありません。
- 拡張 P スペースのローカル LFA：拡張 P スペースのノードの場合、ローカル LFA は今でも修復パスのための最も経済的な方法です。この場合、TI-LFA は選択されません。
- PQ 交差ノードへのトンネル：これは、修復パスが TI-LFA を使用してコンバージェンス後のパスで保証されることを除いて、リモート LFA と類似しています。
- PQ 分離ノードへのトンネル：ローカルおよびリモート LFA が修復パスを見つけられない場合には、この機能は TI-LFA に固有です。
- プラットフォームのサポートされている最大ラベル数までの、複数の交差または分離 PQ ノードを通過するトンネル：TI-LFA は、すべてのプレフィックスの完全なカバレッジを提供します。
- 保護されたリンクのための P2P インターフェイス：TI-LFA は P2P インターフェイスを保護します。
- 非対称リンク：ネイバー間の ISIS メトリックは同じではありません。
- マルチホーム（エニーキャスト）プレフィックス保護：同じプレフィックスが複数のノードによって発信される場合があります。
- 保護されたプレフィックスのフィルタリング：ルートマップは、保護するプレフィックスのリストと、リリース ノードまでの最大修復距離を制限するオプションを含めるかまたは除外します。

- タイブレーカー：TI-LFA に適用可能な既存のタイブレーカーのサブセットがサポートされています。

トポロジに依存しないループ フリー代替タイブレーク

ローカルおよびリモート LFA は、プレフィックスを保護するために複数のパスがある場合、デフォルトまたはユーザ設定のヒューリスティックを使用してタイブレークします。この属性は、ロード バランシングの前に、TI-LFA リンク保護計算の終了時に修復パスの数を削減するために使用されます。ローカル LFA およびリモート LFA は次のタイブレーカーをサポートします。

- Linecard-disjoint：ライン カード分離修復パスを優先します
- Lowest-backup-path-metric：最小の合計メトリックを持つ修復パスを優先します
- Node-protecting：修復パスを保護するノードを優先します
- SRLG-disjoint：SRLG 分離修復パスを優先します
- Load-sharing：リンクとプレフィックスの間で均等に修復パスを分配します

特定のプレフィックスに対して 2 つの修復パスがある場合、プライマリ ポートのものとは異なるライン カードの出力ポートであるパスが、修復パスとして選択されます。TI-LFA リンク保護の場合、次のタイブレーカーがサポートされています。

- Linecard-disjoint：ライン カード分離修復パスを優先します。
- LC disjoint index：修復パスの両方がプライマリ パスのものと同じライン カード上にある場合、両方のパスが候補と見なされます。パスの 1 つが別のライン カード上にある場合は、そのパスが修復パスとして選択されます。
- SRLG index：両方の修復パスがプライマリ パスのものと同じ SRLG ID を持つ場合、両方のパスが候補と見なされます。パスの 1 つが異なる srlg id を持つ場合、そのパスが修復パスとして選択されます。
- Node-protecting：TI-LFA ノード保護の場合、コンバージェンス後の最短パスを計算するときに保護ノードが削除されます。修復パスは、保護されたノードの周囲のトラフィックを指示する必要があります。

SRLG ID は、各インターフェイスに対して構成できます。プレフィックスに対して 2 つの修復パスがある場合、修復パスに設定された SRLG ID は、プライマリ パス SRLG ID のものと比較されます。セカンダリ パスの SRLG ID がプライマリのものと異なる場合、そのパスが修復パスとして選択されます。このポリシーが有効になるのは、プライマリ パスが SRLG ID で構成されている場合のみです。同じインターフェイスまたは同じプロトコル インスタンスに対して、ノードと SRLG の両方の保護モードを設定することができます。その場合、追加の TI-LFA ノード SRLG の組み合わせ保護アルゴリズムが実行されます。TI-LFA ノード SRLG の組み合わせアルゴリズムは、コンバージェンス後の SPT を計算するときに、保護されたノードと、同じ SRLG グループを持つインターフェイスのすべてのメンバーを削除します。

インターフェイス高速再ルーティング タイブレーカー

インターフェイス高速再ルーティング（FRR）タイブレーカーは、TI-LFA ノードおよびSRLG保護にも必要です。インターフェイスおよびプロトコル インスタンス FRR タイブレーカーの両方が設定されている場合、インターフェイス FRR タイブレーカーはプロトコル インスタンスよりも優先されます。インターフェイス FRR タイブレーカーが設定されていない場合、インターフェイスは、プロトコル インスタンス FRR タイブレーカーを継承します。

以下のインターフェイス FRR タイブレーカー コマンドは、特定のインターフェイスにのみ適用されます。

```
isis fast-reroute tie-break
[level-1 | level-2] linecard-disjoint
priority
isis fast-reroute tie-break
[level-1 | level-2] lowest-backup-metric
priority
isis fast-reroute tie-break
[level-1 | level-2] node-protecting
priority
isis fast-reroute tie-break
[level-1 | level-2] srlg-disjoint
priority
isis fast-reroute tie-break
[level-1 | level-2] default
```

同じインターフェイス上のタイブレーカーのデフォルトと明示的なタイブレーカーは、相互に排他的です。

以下のタイブレーカーは、すべての LFA でデフォルトで有効になっています。

- linecard-disjoint
- lowest-backup-metric
- srlg-disjoint

Cisco IOS XE リリース 3.18 では、ノード保護タイブレーカーはデフォルトで無効になっています。

IS-ISリンク保護のトポロジに依存しないループフリー代替高速再ルーティングの設定方法

リンク保護のトポロジに依存しないループ フリー代替高速再ルーティングを設定するには、以下のステップを実行します。

トポロジに依存しないループ フリー代替高速再ルーティングの設定

次の 2 つの方法のいずれかを使用して、TI-LFA を有効にすることができます。

1. **プロトコルの有効化**：すべての IS-IS インターフェイスに対してルータ isis モードで TI-LFA を有効にします。必要に応じて、インターフェイス コマンドを使用して、TI-LFA を無効にするインターフェイスを除外します。

   たとえば、すべての IS-IS インインターフェイスに対して TI-LFA を有効にするには次を実行します。

```
router isis 1
fast-reroute per-prefix {level-1 | level-2}
fast-reroute ti-lfa {level-1 | level-2} [maximum-metric value]
```

（注） **isis fast-reroute protection level-x** コマンドはローカル LFA を有効にし、TI-LFA の有効化を要求されます。

2. **インターフェイスの有効化**：各インターフェイスで TI-LFA を選択的に有効にします。

```
interface interface-name
isis fast-reroute protection {level-1 | level-2}
isis fast-reroute ti-lfa protection {level-1 | level-2} [maximum-metric value]
```

   maximum-metric オプションは、ノードがリリース ノードとして適格であると見なされる最大修復距離を指定します。

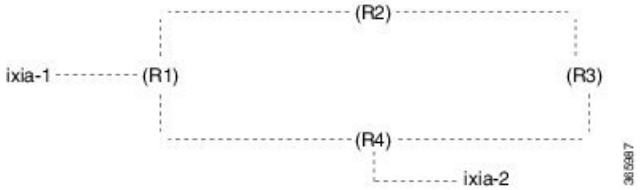
   インターフェイスとプロトコルの両方で TI-LFA が有効になっている場合、インターフェイス設定はプロトコル設定より優先されます。TI-LFA はデフォルトでは無効になっています。

   特定のインターフェイスで TI-LFA を無効にするには、次のコマンドを使用します。

```
interface interface-name
isis fast-reroute ti-lfa protection level-1 disable
```

マッピング サーバを使用したトポロジに依存しないループ フリー代替の設定

構成を理解するために、次のトポロジを検討してください。



- IXIA-2 は ISIS のプレフィックスを注入し、IXIA-1 は一方向のトラフィックを IXIA-2 に送ります

.

• R1 10,000 プレフィックスはセグメントルーティング マッピングサーバで設定されます。

R1 の設定は次のとおりです。

```
configure terminal
segment-routing mpls
global-block 16 20016
!
connected-prefix-sid-map
address-family ipv4
11.11.11.11/32 index 11 range 1
exit-address-family
!
!
mapping-server
!
prefix-sid-map
address-family ipv4
120.0.0.0/24 index 2 range 1 attach
200.0.0.0/24 index 1 range 1 attach
192.168.0.0/24 index 100 range 10000 attach
exit-address-family
!
!
!
!
interface Loopback0
ip address 11.11.11.11 255.255.255.255
ip router isis ipfrr
!
interface GigabitEthernet0/1/0
ip address 14.0.0.1 255.255.255.0
ip router isis ipfrr
negotiation auto
isis network point-to-point
!
interface GigabitEthernet0/1/2
ip address 11.0.0.1 255.255.255.0
ip router isis ipfrr
negotiation auto
isis network point-to-point
!
interface GigabitEthernet0/1/4
ip address 200.0.0.1 255.255.255.0
ip router isis ipfrr
negotiation auto
isis network point-to-point
!
router isis ipfrr
net 49.0001.0110.1101.1011.00
is-type level-2-only
metric-style wide
log-adjacency-changes
nsf cisco
segment-routing mpls
segment-routing prefix-sid-map advertise-local
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
microloop avoidance rib-update-delay 10000
```

R2 の設定は次のとおりです。

```
configure terminal
!
!
segment-routing mpls
!
connected-prefix-sid-map
address-family ipv4
12.12.12.12/32 index 12 range 1
exit-address-family
!
!
interface Loopback0
ip address 12.12.12.12 255.255.255.255
ip router isis ipfrr
!
interface GigabitEthernet0/1/0
ip address 12.0.0.1 255.255.255.0
ip router isis ipfrr
negotiation auto
isis network point-to-point
!
interface GigabitEthernet0/1/1
ip address 11.0.0.2 255.255.255.0
ip router isis ipfrr
negotiation auto
isis network point-to-point
!
router isis ipfrr
net 49.0001.0120.1201.2012.00
is-type level-2-only
metric-style wide
log-adjacency-changes
nsf cisco
segment-routing mpls
segment-routing prefix-sid-map advertise-local
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
microloop avoidance rib-update-delay 10000
!
```

R3 の設定は次のとおりです。

```
configure terminal
!
mpls traffic-eng tunnels
!
segment-routing mpls
!
connected-prefix-sid-map
address-family ipv4
13.13.13.13/32 index 13 range 1
exit-address-family
!
!
interface Loopback0
ip address 13.13.13.13 255.255.255.255
ip router isis ipfrr
!
interface GigabitEthernet0/0/4
ip address 13.0.0.1 255.255.255.0
ip router isis ipfrr
load-interval 30
speed 1000
```

```
no negotiation auto
isis network point-to-point
!
interface GigabitEthernet0/0/5
ip address 12.0.0.2 255.255.255.0
ip router isis ipfrr
negotiation auto
isis network point-to-point
!
router isis ipfrr
net 49.0001.0130.1301.3013.00
is-type level-2-only
metric-style wide
log-adjacency-changes
nsf cisco
segment-routing mpls
segment-routing prefix-sid-map advertise-local
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
microloop avoidance rib-update-delay 10000
!
```

R4 の設定は次のとおりです。

```
configure terminal
!
mpls traffic-eng tunnels
!
segment-routing mpls
!
connected-prefix-sid-map
address-family ipv4
14.14.14.14/32 index 14 range 1
exit-address-family
!
!
interface Loopback0
ip address 14.14.14.14 255.255.255.255
ip router isis ipfrr
!
interface GigabitEthernet0/0/0
ip address 14.0.0.2 255.255.255.0
ip router isis ipfrr
negotiation auto
isis network point-to-point
!
interface GigabitEthernet0/0/3
ip address 13.0.0.2 255.255.255.0
ip router isis ipfrr
speed 1000
no negotiation auto
isis network point-to-point
!
interface GigabitEthernet0/0/5
ip address 120.0.0.1 255.255.255.0
ip router isis ipfrr
speed 1000
no negotiation auto
isis network point-to-point
!
router isis ipfrr
net 49.0001.0140.1401.4014.00
is-type level-2-only
metric-style wide
```

```
log-adjacency-changes
nsf cisco
segment-routing mpls
segment-routing prefix-sid-map advertise-local
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
microloop avoidance rib-update-delay 10000
!
```

例：IS-IS リンク保護のトポロジに依存しないループ フリー代替高速再ルーティングの設定

例 1：次の例では、ローカル LFA が linecard-disjoint と srlg-disjoint タイブレーカーで設定されています。Linecard-disjoint は、srlg-disjoint（11）よりも低い優先順位値（10）で優先されます。

```
router isis access
 net 49.0001.2037.0685.b002.00
 metric-style wide
 fast-flood 10
 max-lsp-lifetime 65535
 lsp-refresh-interval 65000
 spf-interval 5 50 200
 prc-interval 5 50 200
 lsp-gen-interval 5 5 200
 log-adjacency-changes
 nsf ietf
 segment-routing mpls
 fast-reroute per-prefix level-1 all - configures the local LFA
 fast-reroute per-prefix level-2 all
 fast-reroute remote-lfa level-1 mpls-ldp - enables rLFA (optional)
 fast-reroute remote-lfa level-2 mpls-ldp
 fast-reroute ti-lfa level-1 - enables TI-LFA
 microloop avoidance rib-update-delay 10000
 bfd all-interfaces
```

例 2：優先度 100 のすべての ISIS レベル 2 インターフェイスで、TI-LFA node-protecting タイブレーカーを有効にします。その他のタイブレーカーはすべて無効になります。

```
router isis
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
fast-reroute tie-break level-2 node-protecting 100
```

例 3：すべての IS-IS レベル 2 インターフェイスで、優先度 100 の TI-LFA node-protecting タイブレーカーと、優先度 200 の TI-LFA SRLG 保護を有効にします。node-protecting タイブレーカーが設定されているため、他のすべてのタイブレーカーは無効になります。

```
router isis
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
fast-reroute tie-break level-2 node-protecting 100
fast-reroute tie-break level-2 srlg-disjoint 200
```

例 4：Ethernet0/0 を除くすべての ISIS レベル 2 インターフェイスで、優先度 100 の TI-LFA node-protecting タイブレーカーを有効にします。これらの IS-IS インターフェイスでは、他のす

べてのタイブレーカーは無効になります。Ethernet0/0 は継承を上書きし、linecard-disjoint、lowest-backup-path-metric、srlg-disjoint を有効にしたタイブレーカーのデフォルト セットを使用します。

```
router isis
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
fast-reroute tie-break level-2 node-protecting 100
!
interface ethernet0/0
ip router isis
isis fast-reroute tie-break level-2 default
```

例 5：Ethernet0/0 以外のすべての IS-IS インターフェイスで、デフォルトのタイブレーカーを使用して TI-LFA を有効にします。Ethernet0/0 で、優先度 100 の TI-LFA node-protecting を有効にし、他のすべてのタイブレーカーを無効にします。

```
router isis
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
!
interface ethernet0/0
ip router isis
isis fast-reroute tie-break level-2 node-protecting 100
```

例 6：すべての ISIS レベル 2 インターフェイスで、優先度 200 の TI-LFA node-protecting タイブレーカーおよび優先度 100 の linecard-disjoint tie-breaker タイブレーカーを有効にします。その他のタイブレーカーはすべて無効になります。

```
router isis
fast-reroute per-prefix level-2 all
fast-reroute ti-lfa level-2
fast-reroute tie-break level-2 linecard-disjoint 100
fast-reroute tie-break level-2 node-protecting 200
```

タイブレーカーの確認

インターフェイスで有効になっているタイブレーカーを表示するには、次のコマンドを使用します。

show running all | section interface *interface-name*

ルータ モードで有効になっているタイブレーカーを表示するには、次のコマンドを使用します。

show running all | section router isis

プライマリおよび修復パスの確認

この例では、1.1.1.1 は保護ネイバーであり、4.4.4.4 は保護リンク上のネイバーです。

```
Router#
show ip cef 1.1.1.1
1.1.1.1/32
```

```
  nexthop 1.1.1.1 GigabitEthernet0/2/0 label [explicit-null|explicit-null]() - slot 2
is primary interface
    repair: attached-nexthop 24.0.0.2 TenGigabitEthernet0/3/0 - slot 3 is repair interface

  nexthop 24.0.0.2 TenGigabitEthernet0/3/0 label [explicit-null|explicit-null]()
    repair: attached-nexthop 1.1.1.1 GigabitEthernet0/2/0
Router#
show ip cef 4.4.4.4
4.4.4.4/32
  nexthop 4.4.4.4 GigabitEthernet0/2/3 label [explicit-null|16004]() - slot 2 is primary
 interface
    repair: attached-nexthop 5.5.5.5 MPLS-SR-Tunnel2
Router# show ip cef 4.4.4.4 int
4.4.4.4/32, epoch 3, RIB[I], refcnt 6, per-destination sharing
  sources: RIB, Adj, LTE
  feature space:
    IPRM: 0x00028000
    Broker: linked, distributed at 4th priority
    LFD: 4.4.4.4/32 2 local labels
    dflt local label info: global/877 [0x3]
    sr local label info: global/16004 [0x1B]
        contains path extension list
        dflt disposition chain 0x46654200
          label implicit-null
          FRR Primary
            <primary: IP adj out of GigabitEthernet0/2/3, addr 4.4.4.4>
        dflt label switch chain 0x46654268
          label implicit-null
          TAG adj out of GigabitEthernet0/2/3, addr 4.4.4.4
        sr disposition chain 0x46654880
          label explicit-null
          FRR Primary
            <primary: TAG adj out of GigabitEthernet0/2/3, addr 4.4.4.4>
        sr label switch chain 0x46654880
          label explicit-null
          FRR Primary
            <primary: TAG adj out of GigabitEthernet0/2/3, addr 4.4.4.4>
  subblocks:
    Adj source: IP adj out of GigabitEthernet0/2/3, addr 4.4.4.4 464C6620
      Dependent covered prefix type adjfib, cover 0.0.0.0/0
  ifnums:
    GigabitEthernet0/2/3(11): 4.4.4.4
    MPLS-SR-Tunnel2(1022)
  path list 3B1FC930, 15 locks, per-destination, flags 0x4D [shble, hvsh, rif, hwcn]
    path 3C04D5E0, share 1/1, type attached nexthop, for IPv4, flags [has-rpr]
      MPLS short path extensions: [rib | lblmrg | srlbl] MOI flags = 0x21 label
explicit-null
      nexthop 4.4.4.4 GigabitEthernet0/2/3 label [explicit-null|16004](), IP adj out of
 GigabitEthernet0/2/3, addr 4.4.4.4 464C6620
        repair: attached-nexthop 5.5.5.5 MPLS-SR-Tunnel2 (3C04D6B0)
    path 3C04D6B0, share 1/1, type attached nexthop, for IPv4, flags [rpr, rpr-only]
      MPLS short path extensions: [rib | lblmrg | srlbl] MOI flags = 0x1 label 16004
      nexthop 5.5.5.5 MPLS-SR-Tunnel2 label 16004(), repair, IP midchain out of
MPLS-SR-Tunnel2 46CE2440
  output chain:
    label [explicit-null|16004]()
    FRR Primary (0x3B209220)
      <primary: TAG adj out of GigabitEthernet0/2/3, addr 4.4.4.4 464C6480> - primary
path
      <repair:  TAG midchain out of MPLS-SR-Tunnel2 46CE22A0
                label 16()
                label 16003()
               TAG adj out of TenGigabitEthernet0/3/0, addr 24.0.0.2 46CE25E0> - repair
 path
```

IS-IS セグメント ルーティングの設定の確認

```
Router# show isis segment-routing
 ISIS protocol is registered with MFI
 ISIS MFI Client ID:0x63
 Tag Null - Segment-Routing:
   SR State:SR_ENABLED
   Number of SRGB:1
   SRGB Start:14000, Range:1001, srgb_handle:0xE0934788, srgb_state: created
   Address-family IPv4 unicast SR is configured
     Operational state: Enabled
```

コマンドでキーワード **global-block** を指定すると、SRGB と、LSP の範囲を表示します。

```
Router# show isis segment-routing global-block
IS-IS Level-1 Segment-routing Global Blocks:
System ID             SRGB Base    SRGB Range
nevada                  20000        4001
arizona               * 16000        1000
utah                    40000        8000
```

show isis segment-routing prefix-sid-map コマンドでキーワード **advertise** を指定すると、ルータがアドバタイズするプレフィックス SID マップを表示します。

```
Roouter# show isis segment-routing prefix-sid-map adv
IS-IS Level-1 advertise prefix-sid maps:
Prefix               SID Index    Range        Flags
16.16.16.16/32       101          1
16.16.16.17/32       102          1            Attached
```

show isis segment-routing prefix-sid-map コマンドでキーワード **receive** を指定すると、ルータが受信するプレフィックス SID マップを表示します。

```
Router #sh isis segment-routing prefix-sid-map receive
IS-IS Level-1 receive prefix-sid maps:
Host                 Prefix              SID Index    Range        Flags
utah                 16.16.16.16/32      101          1
                     16.16.16.17/32      102          1            Attached
```

LSP で見つかった、マッピング サーバ コンポーネントに渡される接続 SID を表示するには、**show isis segment-routing connected-sid** コマンドを使用します。

```
Router# show isis segment-routing connected-sid
IS-IS Level-1 connected-sids
Host                  Prefix              SID Index    Range        Flags
nevada              * 1.1.1.2/32          1002         1
                      2.2.2.2/32          20           1
                      100.1.1.10/32       10           1
colorado              1.1.1.3/32          33           1
                      1.1.1.6/32          6            1
IS-IS Level-2 connected-sids
Host                 Prefix              SID Index    Range        Flags
```

IS-IS トポロジに依存しないループ フリー代替トンネルの確認

```
Router# show isis fast-reroute ti-lfa tunnel
Fast-Reroute TI-LFA Tunnels:
Tunnel  Interface  Next Hop         End Point        Label     End Point Host
MP1     Et1/0      30.1.1.4         1.1.1.2          41002     nevada
MP2     Et0/0      19.1.1.6         1.1.1.6          60006     colorado
                                    1.1.1.2          16        nevada
MP3     Et0/0      19.1.1.6         1.1.1.6          60006     colorado
                                    1.1.1.2          16        nevada
                                    1.1.1.5          70005     wyoming
```

トポロジに依存しないループ フリー代替構成によるセグメント ルーティング トラフィック エンジニアリングの確認

```
Router# show mpls traffic-eng tunnels tunnel1
Name: PE1                              (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, (SEGMENT-ROUTING) type explicit IP_PATH (Basis for Setup)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    Path Selection:
     Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 0 [0] bw-based
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: explicit path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  History:
    Tunnel:
      Time since created: 4 hours, 25 minutes
      Time since path change: 4 hours, 21 minutes
      Number of LSP IDs (Tun_Instances) used: 37
    Current LSP: [ID: 37]
      Uptime: 4 hours, 21 minutes
  Tun_Instance: 37
  Segment-Routing Path Info (isis  level-1)
    Segment0[Node]: 4.4.4.4, Label: 16014
    Segment1[Node]: 5.5.5.5, Label: 16015
    Segment2[Node]: 6.6.6.6, Label: 16016
Router# show isis fast-reroute ti-lfa tunnel

Tag 1:
Fast-Reroute TI-LFA Tunnels:
Tunnel  Interface  Next Hop         End Point        Label     End Point Host
MP1     Gi2        192.168.1.2      6.6.6.6          16016     SR_R6
MP2     Gi3        192.168.2.2      6.6.6.6          16016     SR_R6
Router# show frr-manager client client-name ISIS interfaces detail
TunnelI/F : MP1
  Type : SR
  Next-hop : 192.168.1.2
  End-point : 6.6.6.6
  OutI/F : Gi2
  Adjacency State : 1
```

```
  Prefix0 : 6.6.6.6(Label : 16016)
TunnelI/F : MP2
  Type : SR
  Next-hop : 192.168.2.2
  End-point : 6.6.6.6
  OutI/F : Gi3
  Adjacency State : 1
  Prefix0 : 6.6.6.6(Label : 16016)
Router# show ip cef 6.6.6.6 internal

6.6.6.6/32, epoch 2, RIB[I], refcnt 6, per-destination sharing
  sources: RIB, LTE
  feature space:
    IPRM: 0x00028000
    Broker: linked, distributed at 1st priority
    LFD: 6.6.6.6/32 1 local label
    sr local label info: global/16016 [0x1A]
        contains path extension list
        sr disposition chain 0x7FC6B0BF2AF0
          label implicit-null
          IP midchain out of Tunnel1
          label 16016
          FRR Primary
            <primary: label 16015
                      TAG adj out of GigabitEthernet3, addr 192.168.2.2>
        sr label switch chain 0x7FC6B0BF2B88
          label implicit-null
          TAG midchain out of Tunnel1
          label 16016
          FRR Primary
            <primary: label 16015
                      TAG adj out of GigabitEthernet3, addr 192.168.2.2>
  ifnums:
    Tunnel1(13)
  path list 7FC6B0BBDDE0, 3 locks, per-destination, flags 0x49 [shble, rif, hwcn]
    path 7FC7144D4300, share 1/1, type attached nexthop, for IPv4
      MPLS short path extensions: [rib | prfmfi | lblmrg | srlbl] MOI flags = 0x3 label
 implicit-null
      nexthop 6.6.6.6 Tunnel1, IP midchain out of Tunnel1 7FC6B0BBB440
  output chain:
    IP midchain out of Tunnel1 7FC6B0BBB440
    label [16016|16016]
    FRR Primary (0x7FC714515460)
      <primary: label 16015
                TAG adj out of GigabitEthernet3, addr 192.168.2.2 7FC6B0BBB630>
      <repair:  label 16015
                label 16014
                TAG midchain out of MPLS-SR-Tunnel1 7FC6B0BBAA90
                label 16016
                TAG adj out of GigabitEthernet2, addr 192.168.1.2 7FC6B0BBBA10>
```

（注） TI-LFA を使用して 50 ミリ秒未満のトラフィック保護を保証するには、ダイナミック パス オプションを指定した SR-TE でバックアップ隣接関係 SID を使用する必要があります。

ダイナミック パス オプションを指定して SR-TE を作成するには、トポロジ内のすべてのルータで次の設定を使用します。

```
router isis 1
fast-reroute per-prefix level-1 all
```

トンネルのヘッドエンド ルータ：

```
interface Tunnel1
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 6.6.6.6
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 1 dynamic segment-routing
tunnel mpls traffic-eng path-selection segment-routing adjacency protected
```

IS-ISリンク保護のトポロジに依存しないループフリー代替高速再ルーティングの追加情報

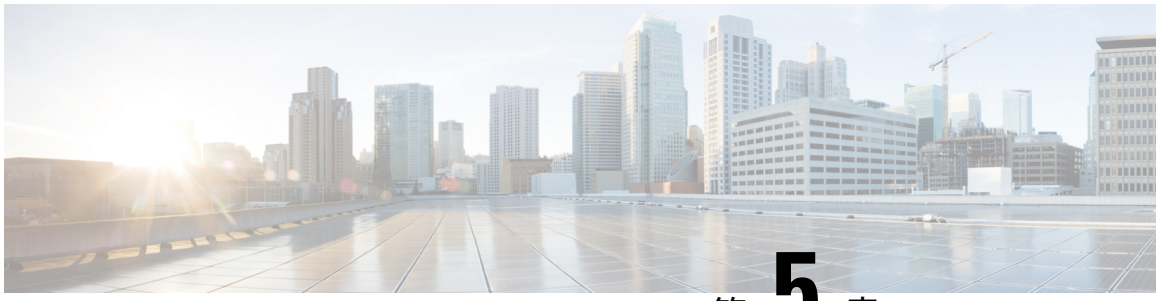
関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

IS-ISリンク保護のトポロジに依存しないループフリー代替高速再ルーティングの機能情報

表 *3 : IS-IS* リンク保護のトポロジに依存しないループ フリー代替高速再ルーティングの機能情報

機能名	リリース	機能情報
IS-IS リンク保護のトポロジに依存しないループ フリー代替高速再ルーティング	Cisco IOS XE Everest 16.4.1 Cisco IOS XE Fuji 16.7.1	次のコマンドが導入または変更されました。 **fast-reroute ti-lfa {level-1 | level-2} [maximum-metric value]**、isis fast-reroute ti-lfa protection level-1 disable、**isis fast-reroute ti-lfa protection {level-1 | level-2} [maximum-metric value]**、**show running all | section interface interface-name**、**show running all | section router isis**。 Cisco IOS XE Fuji 16.7.1 では、この機能は Cisco 4000 シリーズ サービス統合型ルータでサポートされています。



第 5 章

IS-IS のセグメント ルーティング トラフィック エンジニアリング

この章では、IS-IS を使用してセグメント ルーティング トラフィック エンジニアリング（SR-TE）を実装する方法について説明します。

IS-IS のセグメント ルーティング トラフィック エンジニアリングの制約事項

- SR-TE は、ブロードキャスト インターフェイスではサポートされていません。ポイントツーポイント インターフェイスのみサポートしています。
- Cisco ASR ルータは、発信パケットに課される特定の数のラベルのみをサポートします。ラベルの数が指定された数よりも大きい場合、SR-TE トンネルの作成は失敗します。Cisco ASR1000 ルータは、最大 16 個のラベルをサポートします。
- 特定の時点で、TE に対して有効にする必要があるプロトコルのインスタンスは 1 つだけです。
- verbatim キーワードは、明示パス オプションが設定されたラベル スイッチド パス（LSP）でだけ使用できます。
- verbatim LSP では、再最適化はサポートされていません。

IS-IS のセグメント ルーティング トラフィック エンジニアリングに関する情報

トラフィック エンジニアリング（TE）トンネルは、トンネルの入力とトンネルの宛先との間でインスタンス化された TE LSP のコンテナです。TE トンネルは、同じトンネルに関連付けられた 1 つ以上の SR-TE LSP をインスタンス化できます。SR-TE LSP パスが宛先ノードへの同じ IGP パスに必ずしも従うとは限りません。この場合、SR-TE パスは、プレフィックス SID のセット、またはノードの隣接関係 SID、あるいはその両方と、SR-TE LSP によってトラバースされるリンクによって指定することができます。

ヘッドエンドは、トンネルを通して伝送される発信パケットに、対応する MPLS ラベル スタックを課します。SR-TE LSP パスに沿った各通過ノードは、パケットが最終的な宛先に到達するまで、着信トップ ラベルを使用してネクストホップを選択し、ラベルをポップまたはスワップし、ラベル スタックの残りの部分を使用して次のノードにパケットを転送します。SR-TE LSP パスを定義するホップまたはセグメントのセットは、演算子によってプロビジョニングされます。

SR-TE LSP のインスタンス化

トラフィック エンジニアリング（TE）トンネルは、1 つ以上のインスタンス化された TE LSP のコンテナです。SR-TE LSP は、TE トンネルのパスオプションで「segment-routing」を設定することによってインスタンス化されます。トンネルにマップされたトラフィックは、プライマリ SR-TE のインスタンス化 LSP を介して転送されます。

同じトンネルの下で複数のパスオプションを設定することもできます。各パスオプションには、プリファレンス インデックスまたはパスオプション インデックスが割り当てられていて、プライマリ LSP をインスタンス化するためのより有利なパスオプションを決定するために使用されます。パスオプションのプリファレンス インデックスが低いほど、パスオプションがより有利になります。同じ TE トンネルにおける他のあまり有利ではないパスオプションは、セカンダリ パスオプションと見なされ、（たとえば、パス上の障害が原因で）現在使用されているパスオプションが無効になった場合に使用されることがあります。

（注） フォワーディング ステートは、プライマリ LSP に対してのみ維持されます。

SR-TE LSP の明示的ヌル

MPLS-TE トンネルのヘッドエンドは、スタックの最下部に明示的ヌルを課しません。penultimate hop popping（PHP）が SR プレフィックス SID に対して有効になっている場合、または隣接関係 SID が SR-TE LSP の最後のホップである場合、パケットはトランスポート ラベルなしでテールエンドに到着する可能性があります。ただし、場合によっては、パケットが明示的ヌル ラベルでテールエンドに到着することが望ましいため、このような場合、ヘッドエンドはラベル スタックの最上部に明示的ヌル ラベルを課すことになります。

SR TE LSP のパス検証

SR-TE トンネル機能では、ヘッドエンドがトンネルパスの初期検証と、その後のトンネルテールエンドおよび通過セグメントの到達可能性の追跡を実行する必要があります。

SR-TE LSP パスのパス検証は、トポロジの変更または SR SID の更新について MPLS-TE で通知されるたびにトリガーされます。

SR-TE LSP 検証手順は、以下のチェックで構成されています。

トポロジ パスの検証

ヘッドエンドは、TE トポロジに対する接続性について SR-TE LSP のパスを検証します。MPLS-TE ヘッドエンドは、隣接関係 SID に対応するリンクが TE トポロジで接続されているかどうかをチェックします。

新たにインスタンス化された SR-TE LSP の場合、ヘッドエンドが SR-TE パスの任意のリンクで不連続性を検出すると、そのパスは無効であると見なされ、使用されません。有効なパスを持つ他のパスオプションがトンネルにある場合、これらのパスを使用してトンネル LSP をインスタンス化します。

既存のインスタンス化された SR-TE LSP がある TE トンネルでは、ヘッドエンドがリンク上の不連続性を検出すると、ヘッドエンドはそのリンクで障害が発生したと見なします。この場合、IP FRR などのローカル修復保護が有効になります。隣接関係がしばらく失われた後、IGP は保護された隣接関係ラベルと関連付けられた転送を維持し続けます。これにより、同じ障害の影響を受けない別のパスにトンネルを再ルーティングするのに十分な時間が、ヘッドエンドで可能になります。ヘッドエンドは、リンク障害を検出した後、有効なパスを持つ他の使用可能パスオプションにトンネルの再ルーティングを試みるために、トンネル無効化タイマーを開始します。

TE トンネルが、障害の影響を受けない検証済みの他のパスオプションを使用して設定されている場合、ヘッドエンドは、これらのパスオプションの 1 つを使用して、影響を受けないパスを使用してトンネルの新しいプライマリ LSP をインスタンス化することによって、トンネルを再ルーティングします。

同じトンネルの下に他の有効なパスオプションが存在しない場合、または TE トンネルが障害の影響を受けるパスオプションを 1 つだけで設定されている場合、ヘッドエンドは無効タイマーを開始し、その後トンネルの状態を「ダウン」にします。このアクションは、影響を受ける SR-TE LSP 上を流れるトラフィックをブラックホール化することを回避し、トンネルを通過するサービスがヘッドエンドで利用可能な異なるパスを経由して再ルーティングすることを可能にします。無効化ドロップ構成は、トンネルを「アップ」のままにしますが、無効化タイマーが満了したときにトラフィックをドロップします。

エリア内 SR-TE LSP では、ヘッドエンドは LSP パス上で完全な可視性を持ち、最終的な LSP 宛先へのパスを検証します。ただし、エリア間 LSP の場合、ヘッドエンドには LSP パスに対する部分的な可視性があります（最初の ABR までのみ）。この場合、ヘッドエンドは、入力から最初の ABR へのパスのみを検証できます。最初の ABR ノードを超える LSP に沿った障害は、ヘッドエンドからは見えず、LSP を介した BFD など、そのような障害を検出するその他のメカニズムが想定されます。

SR SID の検証

SR-TE LSP の SID ホップは TE トンネルの SR-TE LSP を介して運ばれる発信パケットに課される発信 MPLS ラベル スタックを決定するために使用されます。グローバルおよびローカルの隣接関係 SID のデータベースは、IGP から受信した情報から取り込まれ、MPLS-TE で維持されます。MPLS TE データベースで利用できない SID を使用すると、明示的パスを使用するパスオプションが無効になります。この場合、パスオプションは、SR TE LSP のインスタンス化には使用されません。また、MPLS の SID データベースで SID を取り消す、追加する、または変更すると、MPLS-TE ヘッドエンドは、SR パスオプション（使用中またはセカンダリ）を持つすべてのトンネルを確認し、適切な処理を呼び出します。

LSP 出力インターフェイス

SR-TE LSP が最初のパス ホップの隣接関係の SID を使用するとき、TE は隣接関係 SID および SR-TE LSP が出力するノードに関連付けられているインターフェイス状態および IGP 隣接関係状態を監視します。インターフェイスまたは隣接関係がダウンした場合、TE は SR-TE LSP パスで障害が発生したと仮定し、前のセクションで説明したのと同じリアクティブ アクションを実行できます。

（注） SR-TE LSP が最初のホップのプレフィックス SID を使用するとき、TE はトンネルが出力するインターフェイスを直接推測できません。TE は、プレフィックスの IP 到達可能性情報に基づいて、最初のホップへの接続が維持されるかどうかを判断します。

IP 到達可能性の検証

MPLS-TE では、SR パスを有効と宣言する前に、プレフィックス SID に対応するノードが IP 到達可能であることを検証します。MPLS-TE は、SR-TE LSP パスの隣接関係またはプレフィックス SID に対応する IP プレフィックスのパス変更を検出します。リンクまたはノードの障害が原因で、特定の SID をアナウンスするノードが IP の到達可能性を失う場合、MPLS-TE はパス変更（パスなし）の通知を受けます。MPLS-TE は、現在の SR-TE LSP パスを無効にすることによって反応し、もしあれば有効なパスを持つ他のパスオプションを使用して新しい SR-TE LSP をインスタンス化する場合があります。

（注） IP-FRR は（SR-TE LSP パスに沿ったプレフィックス SID の失敗など）SR-TE LSP が通過しているノードの障害に対する保護を提供しないため、ヘッドエンドは、トンネル状態を「ダウン」に設定することによってプレフィックス SID ノードの IP ルートの到達可能性の損失にすぐに反応し、影響を受けるトンネルに対して有効なパスを持つパスオプションが他にない場合は、トンネル転送エントリを削除します。

トンネル パス アフィニティの検証

トンネル パスのアフィニティは、トンネル インターフェイスで **tunnel mpls traffic-eng affinity** コマンドを使用して指定することができます。

ヘッドエンドは、指定された SR パスが設定されたアフィニティに準拠していることを検証します。これにより、SR パスの各セグメントのパスは、指定された制約に照らして検証される必要があります。パスの少なくとも 1 つのセグメントが設定されているアフィニティを満たさない場合、そのパスは設定されているアフィニティ制約に対して無効として宣言されます。

トンネル パス リソース回避の検証

SR-TE トンネルパケットの通過から除外されたことを検証するアドレスのセットを指定できます。これを実現するために、ヘッドエンドはセグメントごとの検証チェックを実行し、指定されたノード、プレフィックス、またはリンク アドレスが SR パスのトンネルから実際に除外されていることを検証します。以下のコマンドを使用して、トンネル リソース回避チェックをパスごとに有効にすることができます。除外されるアドレスのリストが定義され、リストの名前がパスオプションで参照されます。

```
interface tunnel100
 tunnel mpls traffic-eng path-option 1 explicit name EXCLUDE segment-routing
ip explicit-path name EXCLUDE enable
 exclude-address 192.168.0.2
 exclude-address 192.168.0.4
 exclude-address 192.168.0.3
!
```

Verbatim パス サポート

通常、MPLS TE LSP を使用する場合は、ネットワーク内のすべてのノードで TE の IGP 拡張がサポートされていて、TE が認識されるように設定されている必要があります。ただし、TE の IGP 拡張をサポートしないが、TE の RSVP 拡張はサポートするノードを通過する TE LSP を構築する機能を必要とするネットワーク管理者もいます。Verbatim LSP は、ネットワーク内のすべてまたは一部の中間ノードで TE の IGP 拡張がサポートされていない場合に役立ちます。

この機能をイネーブルにすると、IP 明示パスの TE トポロジ データベースに対するチェックは行われません。TE トポロジ データベースの検証が行われないため、IP 明示パス情報を持つ Path メッセージは、IP ルーティング用の Shortest Path First（SPF）アルゴリズムを使用してルーティングされます。

SR-TE トラフィックのロード バランシング

SR-TE トンネルは、次のロードバランシング オプションをサポートします。

ポート チャネル TE リンクのロード バランシング

ポート チャネル インターフェイスは SR-TE LSP トラフィックを運びます。このトラフィック負荷は、ポート チャネル メンバー リンクと、SR-TE LSP の先頭または中間のバンドル インターフェイス上でバランスをとります。

単一トンネルでのロード バランシング

同じコストのマルチパス プロトコル（ECMP）を使用している間、特定のプレフィックス SID へのパスが複数のネクストホップを指す場合があります。さらに、SR-TE LSP パスが、ECMP を持つ 1 つ以上のプレフィックス SID を通過する場合、SR-TE LSP トラフィック負荷は、SR-TE

LSP パスに沿ってヘッドエンドまたは中間点の通過したノードから通過した各プレフィックス SID の ECMP パスでバランスをとります。

複数トンネルでのロード バランシング

スタティック ルートを設定するか、同じ宛先に対して複数の並列トンネルを自動ルート アナウンスをすると、複数の TE トンネルを特定の IP プレフィックスへのルーティングのためのネクストホップ パスとして使用することができます。このような場合、トンネルはトラフィック負荷を均等に共有するか、複数の並列トンネル上でトラフィックをロード バランシングします。トンネル ヘッドエンドでトンネルごとの明示的な設定を使用して不等なロード バランシング（UELB）を許可することも可能です。この場合、トンネルのロードシェアは MPLS-TE からフォワーディング プレーンに渡されます。

トンネルのロードシェア機能は、SR-TE LSP をインスタンス化する TE トンネルで引き続き機能します。

SR-TE トンネルの再最適化

TE トンネルの再最適化は、ヘッドエンドが、現在使用されているパスよりも利用可能な最適なパスがあると判断した場合に発生します。たとえば、SR-TE LSP パスに沿って障害が発生した場合、ヘッドエンドは再最適化をトリガーすることによって、より最適なパスを検出し復帰することができます。

SR-TE LSP をインスタンス化するトンネルは、トンネルを通して運ばれるトラフィックに影響を与えずに再最適化できます。

再最適化は、次の理由で発生します。

- プライマリ SR-TE LSP 明示的パスによって使用される明示的なパス ホップが変更された
- トポロジ パスが切断されているか、または明示的パスで指定されている SID データベースで SID が見つからないため、ヘッドエンドが現在使用されているパスオプションが無効であると判断した
- より有利なパスオプション（より低いインデックス）が利用可能になった

ヘッドエンドは、SR-TE LSP が通過する保護された SR 隣接関係 SID で障害を検出すると、無効化タイマーを開始します。タイマーが期限切れになり、別のパスで再ルーティングできないために失敗したパスをヘッドエンドがまだ使用している場合、トラフィックをブラックホール化しないようにトンネル状態が「ダウン」になります。トンネルがダウンすると、トンネル上のサービスは、異なるパスを使用するために収束します。

次に手動の再最適化の例で出力されるサンプルを示します。この例では、パスオプションが「10」から「20」に変更されます。

```
Router# mpls traffic-eng reoptimize tunnel 1 path-option 20
The targeted path-option is not in lock down mode. Continue? [no]: yes
Router# show mpls traffic-eng tunnels tunnel1
Name: R1_t1                           (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 20, (SEGMENT-ROUTING) type explicit IP_PATH (Basis for Setup)
    path option 10, (SEGMENT-ROUTING) type dynamic
  Config Parameters:
```

```
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
     Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: explicit path option 20 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  History:
    Tunnel:
      Time since created: 6 days, 19 hours, 9 minutes
      Time since path change: 14 seconds
      Number of LSP IDs (Tun_Instances) used: 1819
    Current LSP: [ID: 1819]
      Uptime: 17 seconds
      Selection: reoptimization
    Prior LSP: [ID: 1818]
      ID: path option unknown
      Removal Trigger: reoptimization completed
  Tun_Instance: 1819
  Segment-Routing Path Info (isis level-1)
    Segment0[Node]: 4.4.4.4, Label: 114
    Segment1[Node]: 5.5.5.5, Label: 115
    Segment2[Node]: 6.6.6.6, Label: 116
```

ロックダウン オプション付き SR-TE

lockdown オプションは、SR-TE がより良いパスに再最適化することを防ぎます。ただし、新しいパスの存在をシグナリングすることは防げません。

```
interface Tunnel1
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng path-option 10 segment-routing lockdown
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
Router# show mpls traffic-eng tunnels tunnel1
Name: csr551_t1                           (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, (LOCKDOWN) type segment-routing (Basis for Setup)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
     Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: enabled  Loadshare: 10 [200000000]
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: segment-routing path option 10 is active
    BandwidthOverride: disabled  LockDown: enabled   Verbatim: disabled
  History:
    Tunnel:
      Time since created: 6 days, 19 hours, 22 minutes
```

```
    Time since path change: 1 minutes, 26 seconds
    Number of LSP IDs (Tun_Instances) used: 1822
  Current LSP: [ID: 1822]
    Uptime: 1 minutes, 26 seconds
    Selection: reoptimization
  Prior LSP: [ID: 1821]
    ID: path option unknown
    Removal Trigger: configuration changed
Tun_Instance: 1822
Segment-Routing Path Info (isis  level-1)
  Segment0[Node]: 6.6.6.6, Label: 116
```

SR-TE トンネル保護

SR TE トンネルの保護は、次のいずれかの代替手段で行うことができます。

IP-FRR ローカル修復保護

SR-TE LSP ヘッドエンドまたはミッドポイント ノードでは、IP-FRR はプレフィックス SID または隣接関係 SID ラベルのためのバックアップ保護パスを計算し、プログラムするのに使用されます。

IP-FRR を使用すると、バックアップ修復パスは、リンクまたはノードの障害が発生する前に IGP によって事前に計算されプログラムされます。リンクが失敗すると、TE トポロジからの即時の取り消し（リンク アドバタイズメントの取り消し）がトリガーされます。これにより、ヘッドエンドは、失敗した隣接関係 SID を通過する SR-TE LSP の障害を検出することができます。

保護された隣接関係 SID が失敗した場合、失敗した隣接関係 SID ラベルとそれに関連する転送は、すべての SR TE トンネルのヘッドエンドが障害を検出して対応できるように、指定した時間（5 ～ 15 分）機能し続けます。隣接関係 SID ラベルを使用するトラフィックは、バックアップ修復パスを変更するその後のトポロジ更新がある場合でも、FRR 保護され続けます。この場合、IGP は FRR がアクティブになっている間にバックアップ修復パスを更新し、新しく計算されたバックアップ パス上のトラフィックを再ルーティングします。

保護されたプレフィックス SID のプライマリ パスが失敗すると、PLR はバックアップ パスに経路を再ルーティングします。ヘッドエンドは障害に対してトランスペアレントなままであり、引き続き SR-TE LSP を有効なパスとして使用します。

IP-FRR は、リンク障害に対してのみ隣接関係およびプレフィックス SID を保護します。

トンネル パス保護

パス保護とは、単一の TE トンネルのプライマリ LSP の障害から保護するために、1 つまたは複数のスタンバイ LSP をインスタンス化することです。

パス保護では、同じトンネルのプライマリ パスオプションによってさまざまな障害のセカンダリ パスを事前に計算し、事前プロビジョニングすることで、障害から保護します。この保護は、プライマリ LSP が通過するプレフィックス SID および隣接関係 SID を除外するパスを計算するか、またはプライマリ SR-TE LSP パスの SRLG を除外するパスを計算することによって実現します。

プライマリ SR-TE LSP に障害が発生した場合、トンネルには少なくとも 1 台のスタンバイ SR-TE LSP が使用されます。複数のセカンダリ パスオプションをスタンバイ SR-TE LSP パスとして使用するように設定できます。

アンナンバード サポート

アンナンバード リンクの IS-IS の説明には、リモート インターフェイス ID 情報は含まれません。アンナンバード リンクのリモート インターフェイス ID には、SR-TE トンネルの一部としてアンナンバード リンクを含める必要があります。

IS-IS のセグメント ルーティング トラフィック エンジニアリングの設定方法

次の手順を実行して、IS-IS でのセグメント ルーティング トラフィック エンジニアリング（SR-TE）を設定します。

TE トンネルのパス オプションの設定

キーワード **segment-routing** は、指定されたパスが SR パスとしてプログラムされることを示します。

```
Device(config)# interface tunnel 100
Device(config-if)# tunnel mpls traffic-eng path-option 1 explicit name foo segment-routing
Device(config-if)# tunnel mpls traffic-eng path-option 2 dynamic segment-routing
Device(config-if)# tunnel mpls traffic-eng path-option 3 segment-routing
```

（注） IP アンナンバード インターフェイスでは、動的パスはサポートされません。

稼働中の SR トンネルのパスオプション タイプが SR から非 SR（たとえば **dynamic**）に変更されると、トンネルの既存の転送エントリが削除されます。

セグメント ルーティングは、既存のセカンダリまたは使用中のパスオプションで有効または無効にすることができます。トンネルでシグナリングされた RSVP-TE の明示的パスオプションが使用され、そのトンネルでセグメント ルーティングが有効になっている場合、RSVP-TE LSP は切断され、SR-TE LSP が同じパスオプションを使用してインスタンス化されます。逆に、プライマリ LSP によって使用されているパスオプションでセグメント ルーティングが無効になっている場合、トンネルは断続的にダウンし、新しい RSVP-TE LSP は同じ明示的パスを使用してシグナリングされます。

セグメント ルーティング パスオプションがセカンダリ パスオプションで有効になっている（すなわち、トンネルのプライマリ LSP によって使用されていない）場合、新しく指定された SR-TE LSP パスオプションが有効で、トンネルのプライマリ LSP に使用するのがより有利であるかどうかを評価するためにトンネルがチェックされます。

SR 明示パス ホップの設定

次の SR-TE 明示的パス ホップがサポートされています。

- IP アドレス
- MPLS ラベル
- IP アドレスと MPLS ラベルの混在

エリア内 LSP では、明示的パスを IP アドレスのリストとして指定できます。

```
Device(config)# ip explicit-path name foo
Device(config-ip-expl-path)# index 10 next-address 1.1.1.1 node address
Device(config-ip-expl-path)# index 20 next-address 12.12.12.2 link address
```

（注） IP アンナンバード インターフェイスを使用する場合、ネクスト ホップ アドレスを明示的パスのインデックスとして指定することはできません。これは、ノードアドレスまたはラベルである必要があります。

明示的パスは、セグメントルーティング SID として指定することもできます。

```
Device(config)# ip explicit-path name foo
Device(config-ip-expl-path)# index 10 next-label 20
```

（注） IP アドレスは、MIXED_PATH でラベルを使用した後に使用することはできません。

インターフェイスのアフィニティの設定

インターフェイスでアフィニティを設定するには、次の手順を実行します。

```
interface GigabitEthernet2
 ip address 192.168.2.1 255.255.255.0
 ip router isis 1
 negotiation auto
 mpls traffic-eng tunnels
 mpls traffic-eng attribute-flags 0x1
 isis network point-to-point
 ip rsvp bandwidth
```

Verbatim パス サポートの有効化

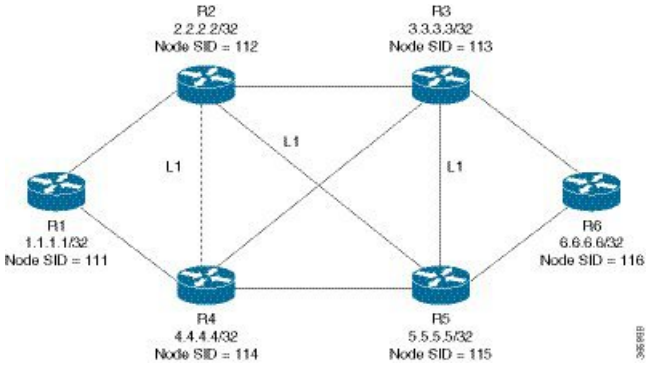
SR-TE で verbatim を有効にするには、次の例を使用します。この例では、トンネル宛先 11.11.11.11 が異なるエリアにあり、multihop という名前を持つ明示的パスが SR-TE パスオプションで定義されます。

```
R6#
interface Tunnel4
```

```
ip unnumbered Loopback66
tunnel mode mpls traffic-eng
tunnel destination 11.11.11.11
tunnel mpls traffic-eng path-option 1 explicit name multihop segment-routing verbatim
!
ip explicit-path name multihop enable
index 1 next-label 16003
index 2 next-label 16002
index 3 next-label 16001
!
End
```

使用例：セグメント ルーティング トラフィック エンジニアリングの基本設定

SR-TE の構成を理解するには、次のトポロジを検討してください。



ヘッドエンド ルータで設定するには、R1 で次を実行します。

```
!
mpls traffic-eng tunnels
!
segment-routing mpls
connected-prefix-sid-map
  address-family ipv4
   1.1.1.1/32 index 111  range 1
  exit-address-family
!
set-attributes
  address-family ipv4
  sr-label-preferred
exit-address-family
!
interface Loopback1
ip address 1.1.1.1 255.255.255.255
ip router isis 1
!
int gig0/0
ip address 11.11.11.1 255.255.255.0
ip router isis 1
mpls traffic-eng tunnels
isis network point-to-point
!
router isis 1
net 49.0001.0010.0100.1001.00
```

```
is-type level-1
metric-style wide
segment-routing mpls
segment-routing prefix-sid-map advertise-local
mpls traffic-eng router-id  Loopback1
mpls traffic-eng level-1
!
end
```

SR-TE の明示的パス（ノード SID ベース）を有効にするには、R1 で次の CLI を有効にします。

```
Head end SR-TE configuration R1#
!
interface tunnel1
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 6.6.6.6
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 6 6
tunnel mpls traffic-eng path-option 10 explicit name Node_PATH segment-routing
!
ip explicit-path name Node_PATH
 next-label  16114
next-label  16115
next-label  16116
```

R1 上の SR-TE トンネル 1 の正常な動作を確認するには、次の CLI を有効にします。

```
Tunnel verification on (R1)# show mpls traffic-eng tun tun 1 detail
Name: R1_t1                             (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, (SEGMENT-ROUTING) type explicit Node_PATH (Basis for Setup)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
Verbatim: disabled
Number of LSP IDs (Tun_Instances) used: 1815
    Current LSP: [ID: 1815]
      Uptime: 2 seconds
Removal Trigger: configuration changed
    Segment-Routing Path Info (isis  level-1)
    Segment0[Node]: 4.4.4.4, Label: 16114
    Segment1[Node]: 5.5.5.5, Label: 16115
    Segment2[Node]: 6.6.6.6, Label: 16116
```

テールエンド ルータで設定するには、R6 で次を実行します。

```
interface GigabitEthernet2
ip address 100.101.1.1 255.255.255.0
ip router isis 1
negotiation auto
mpls traffic-eng tunnels
router isis 1
 net 49.0001.0060.0600.6006.00
 ispf level-1
 metric-style wide
 log-adjacency-changes
 segment-routing mpls

segment-routing prefix-sid-map advertise-local
```

```
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng level-1
```

明示パス SR-TE トンネル 1

トンネル 1 を IP アドレスのみに基づいて考慮します。

```
ip explicit-path name IP_PATH1
 next-address 2.2.2.2
 next-address 3.3.3.3
 next-address 6.6.6.6
!
interface Tunnel1
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng path-option 10 explicit name IP_PATH1 segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
end
```

明示パス SR-TE トンネル 2

トンネル 2 をノードの SID に基づいて考慮します

```
ip explicit-path name IA_PATH
 next-label 114
 next-label 115
 next-label 116
!
interface Tunnel2
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng bandwidth 10000 class-type 1
 tunnel mpls traffic-eng path-option 10 explicit name NODE_PATH segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
end
```

明示パス SR-TE トンネル 3

トンネル 3 は IP アドレスとラベルの組み合わせに基づいていることを考慮します

```
ip explicit-path name MIXED_PATH enable
 next-address 2.2.2.2
 next-address 3.3.3.3
 next-label 115
 next-label 116
!
interface Tunnel3
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
```

```
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng path-option 10 explicit name MIXED_PATH segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
```

（注） パスが混在している場合、パスでノード SID を使用した後に IP ネクストホップを使用することはできません。次のパスは有効ではありません。

```
ip explicit-path name MIXED_PATH enable
next-label 115
next-label 116
next-address 2.2.2.2
```

動的パス SR-TE トンネル 4

トンネル 4is は隣接関係 SID に基づいていることを考慮します

```
interface Tunnel4
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng bandwidth 10000 class-type 1
 tunnel mpls traffic-eng path-option 10 dynamic segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
end
```

動的パス SR-TE トンネル 5

トンネル 5 はノード SID に基づいていることを考慮します

```
 interface Tunnel5
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng path-option 10 segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
```

SR-TE トンネルの構成の確認

show mpls traffic-eng tunnels *tunnel-number* コマンドを使用して、SR-TE トンネルの構成を確認します。

トンネル 1 の確認

```
Name: R1_t1                             (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
```

```
  path option 10, (SEGMENT-ROUTING) type explicit IP_PATH (Basis for Setup)
Config Parameters:
  Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
  Metric Type: IGP (interface)
  Path Selection:
   Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
  AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
History:
  Tunnel:
    Time since created: 6 days, 19 hours
    Time since path change: 2 seconds
    Number of LSP IDs (Tun_Instances) used: 1814
  Current LSP: [ID: 1814]
    Uptime: 2 seconds
    Selection: reoptimization
  Prior LSP: [ID: 1813]
    ID: path option unknown
    Removal Trigger: configuration changed
Tun_Instance: 1814
Segment-Routing Path Info (isis  level-1)
  Segment0[Node]: 4.4.4.4, Label: 114
  Segment1[Node]: 5.5.5.5, Label: 115
  Segment2[Node]: 6.6.6.6, Label: 116
```

トンネル 2 の確認

```
Name: R1_t2                             (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, (SEGMENT-ROUTING) type explicit IA_PATH (Basis for Setup)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
     Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: explicit path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  History:
    Tunnel:
      Time since created: 6 days, 19 hours, 1 minutes
      Time since path change: 1 seconds
      Number of LSP IDs (Tun_Instances) used: 1815
    Current LSP: [ID: 1815]
      Uptime: 1 seconds
    Prior LSP: [ID: 1814]
      ID: path option unknown
      Removal Trigger: configuration changed
  Tun_Instance: 1815
  Segment-Routing Path Info (isis  level-1)
    Segment0[ - ]: Label: 114
```

```
  Segment1[ - ]: Label: 115
  Segment2[ - ]: Label: 116
```

トンネル 3 の確認

```
Name: R1_t3                             (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, (SEGMENT-ROUTING) type explicit MIXED_PATH (Basis for Setup)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
     Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: explicit path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  History:
    Tunnel:
      Time since created: 6 days, 19 hours, 2 minutes
      Time since path change: 2 seconds
      Number of LSP IDs (Tun_Instances) used: 1816
    Current LSP: [ID: 1816]
      Uptime: 2 seconds
      Selection: reoptimization
    Prior LSP: [ID: 1815]
      ID: path option unknown
      Removal Trigger: configuration changed
  Tun_Instance: 1816
  Segment-Routing Path Info (isis  level-1)
    Segment0[Node]: 2.2.2.2, Label: 112
    Segment1[Node]: 3.3.3.3, Label: 113
    Segment2[ - ]: Label: 115
    Segment3[ - ]: Label: 116
```

トンネル 4 の確認

```
Name: R1_t4                             (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, (SEGMENT-ROUTING) type dynamic (Basis for Setup, path weight 30)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
     Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: dynamic path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  History:
    Tunnel:
      Time since created: 6 days, 19 hours
      Time since path change: 2 seconds
```

```
    Number of LSP IDs (Tun_Instances) used: 1813
  Current LSP: [ID: 1813]
    Uptime: 2 seconds
  Prior LSP: [ID: 1806]
    ID: path option unknown
    Removal Trigger: configuration changed
Tun_Instance: 1813
Segment-Routing Path Info (isis  level-1)
  Segment0[Link]: 192.168.2.1 - 192.168.2.2, Label: 17
  Segment1[Link]: 192.168.4.2 - 192.168.4.1, Label: 25
  Segment2[Link]: 192.168.8.1 - 192.168.8.2, Label: 300
```

トンネル 5 の確認

```
Name: R1_t5                              (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, type segment-routing (Basis for Setup)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
     Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: segment-routing path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  History:
    Tunnel:
      Time since created: 6 days, 19 hours, 4 minutes
      Time since path change: 14 seconds
      Number of LSP IDs (Tun_Instances) used: 1817
    Current LSP: [ID: 1817]
      Uptime: 14 seconds
      Selection: reoptimization
    Prior LSP: [ID: 1816]
      ID: path option unknown
      Removal Trigger: configuration changed
  Tun_Instance: 1817
  Segment-Routing Path Info (isis  level-1)
    Segment0[Node]: 6.6.6.6, Label: 116
```

Verbatim パス サポートの確認

適切な動作と SR-TE トンネル状態を確認するには、次の CLI を使用します。

```
R6#sh mpl traffic-eng tunnels tunnel 4

Name: R6_t4                                (Tunnel4) Destination: 11.11.11.11
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 1, (SEGMENT-ROUTING) type explicit (verbatim) multihop (Basis for Setup)


  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
```

```
  Path Selection:
   Protection: any (default)
  Path-selection Tiebreaker:
    Global: not set   Tunnel Specific: not set   Effective: min-fill (default)
  Hop Limit: disabled [ignore: Verbatim Path Option]
  Cost Limit: disabled
  Path-invalidation timeout: 10000 msec (default), Action: Tear
  AutoRoute: disabled LockDown: disabled Loadshare: 0 [0] bw-based
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: explicit path option 1 is active
  BandwidthOverride: disabled  LockDown: disabled  Verbatim: enabled

History:
  Tunnel:
    Time since created: 16 minutes, 40 seconds
    Time since path change: 13 minutes, 6 seconds
    Number of LSP IDs (Tun_Instances) used: 13
  Current LSP: [ID: 13]
    Uptime: 13 minutes, 6 seconds
    Selection: reoptimization
  Prior LSP: [ID: 12]
    ID: path option unknown
    Removal Trigger: configuration changed (severe)
Tun_Instance: 13
Segment-Routing Path Info (IGP information is not used)
  Segment0[First Hop]: 0.0.0.0, Label: 16003
  Segment1[ - ]: Label: 16002
  Segment2[ - ]: Label: 16001
```

IS-IS のセグメント ルーティング トラフィック エンジニアリングの追加情報

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 Command List, All Releases』

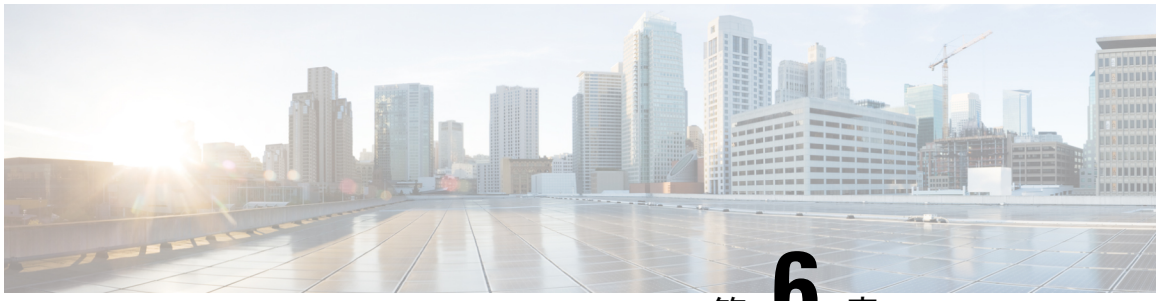
IS-IS のセグメント ルーティング トラフィック エンジニアリングの機能情報

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 *4 : IS-IS* のセグメント ルーティング トラフィック エンジニアリングの機能情報

機能名	リリース	機能情報
IS-IS のセグメント ルーティングトラフィック エンジニアリング	Cisco IOS XE Everest 16.4.1 Cisco IOS XE Fuji 16.7.1	次のコマンドが導入または変更されました。 **mpls traffic-eng nsr**、**show mpls traffic-eng tunnels tunnel1**、**show isis fast-reroute ti-lfa tunnel**、**show frr-manager client client-name ISIS interfaces detail**、**show ip cef 6.6.6.6 internal** Cisco IOS XE Fuji 16.7.1 では、この機能は Cisco 4000 シリーズ サービス統合型ルータでサポートされています。



第 6 章

OSPFv2 ノード SID のセグメント ルーティング

この章では、セグメント ルーティングが OSPFv2 ノード SID でどのように機能するかについて説明します。

OSPFv2 ノード SID のセグメント ルーティングに関する情報

セグメント ルーティングは、Open Shortest Path First（OSPF）プロトコルのいくつかの拡張機能に依存しています。ルーティング プロトコル インスタンスのセグメント ルーティングを有効にするには、2 つのレベルの構成が必要です。セグメント ルーティング インフラストラクチャ コンポーネントによって管理される最上位のセグメント ルーティング構成では、セグメント ルーティングが可能になり、一方、ルータ ospf レベルでのセグメント ルーティング構成では、ospfインスタンスに対してセグメントルーティングが可能になります。セグメントルーティングの状態には、次の 3 つがあります。

- SR_NOT_CONFIGURED
- SR_DISABLED
- SR_ENABLED

IGP 下のセグメント ルーティング構成は、SR の状態が SR_DISABLED または SR_ENABLED のいずれかである場合にのみ許可されます。SR_ENABLED 状態は、少なくとも予約済みの有効な SRGB 範囲にあることを示します。コマンドを使用して、ルータ設定サブ モードで IGP のセグメント ルーティングを有効にすることができます。ただし、IGP セグメント ルーティングは、グローバル SR が設定された後にのみ有効になります。

SR_ENABLEDは、SRを有効にするためにすべてのプロトコルに必要な状態ですが、プロトコル インスタンスの SR を有効にするには十分ではありません。その理由は、OSPF にセグメント ルーティング グローバル ブロック（SRGB）情報に関する情報がまだないことです。SRGB に関する情報を受信する要求が正常に処理されると、OSPF SR の動作状態が有効になります。

セグメント ルーティングでは、各ルータが、セグメント ルーティング データプレーン機能と、グローバル SID が割り当てられている場合にセグメント ルーティングに使用される MPLS ラベル値の範囲をアドバタイズする必要があります。データプレーン機能とラベル範囲は、OSPF ルータ情報不透明 LSA に挿入される SR 機能サブ TLV を使用してアドバタイズされます。

OSPF SR 機能サブ TLV には、すべての予約済み SRGB 範囲が含まれます。ただし、シスコの実装でサポートされる SRGB 範囲は 1 つだけです。

リモート ルータからのラベル スイッチド パスで受信されたプレフィックス SID

OSPF は、その不透明な拡張プレフィックス LSA 内の拡張プレフィックス サブ TLV を使用して、接続されたプレフィックスに関連付けられたプレフィックス SID を送信します。到達可能性がある LSA で受信したプレフィックス SID は、次の条件が満たされている場合にのみ、プレフィックス VPN ラベルごとの BGP ダウンロードと同じ方法でルーティング情報ベース（RIB）にダウンロードされます。

- トポロジとアドレスファミリに対してセグメント ルーティングが有効。
- プレフィックス SID が有効。
- MFI へのローカル ラベルのバインドが成功している。

（注） 指定された SID 範囲に収まらない SID の場合、RIB の更新時にラベルは使用されません。SID が SID の範囲内には収まるが、ネクストホップのネイバー SID の範囲には収まらない場合は、そのパスに関連付けられているリモート ラベルはインストールされません。

セグメント ルーティング隣接関係 SID アドバタイズメント

Cisco IOS XE リリース 3.17 では、OSPF によるセグメント ルーティング隣接関係 SID のアドバタイズメントのサポートが有効です。隣接関係セグメント識別子（Adj-SID）は、セグメント ルーティングにおけるルータ隣接関係を表します。

セグメント ルーティング対応ルータは、隣接関係ごとに Adj-SID を割り当てることができ、この SID を拡張不透明リンク LSA で伝送するように Adj-SID サブ TLV が定義されます。

OSPF は、OSPF 隣接関係が 2 つの方法または完全な状態にある場合、各 OSPF ネイバーに隣接関係 SID を割り当てます。OSPF は、セグメント ルーティングが有効になっている場合にのみ隣接関係 SID を割り当てます。隣接関係 SID のラベルは、システムによって動的に割り当てられます。これにより、ローカルでしか有効でないため、設定ミスの可能性がなくなります。

複数の隣接関係 SID

Cisco IOS XE リリース 16.3 では、複数の隣接関係 SID がサポートされています。OSPF の隣接関係ごとに、OSPF は拡張リンク LSA で伝送される隣接関係 SID、非保護および保護された Adj-SID を割り当てます。保護された隣接関係 SID（またはバックアップ Adj-SID）は、ルータで FRR が有効になっている場合のみ、また SR がシステムで有効になっているインターフェイスでのみ、割り当てられてアドバタイズされます。FRR または SR が無効になっている場合、保護された Adj-SID は解放されます。

フォワーディング プレーンでの保護された adj-SID の永続化はサポートされます。プライマリリンクがダウンしている場合、OSPF は、遅延タイマー（30 秒）が期限切れになるまでバックアップ Adj-SID の解放を遅らせます。これにより、フォワーディング プレーンは、ルータがコンバージされるまで、バックアップ パスを経由してトラフィックを転送し続けることができます。

割り当てられ、アドバタイズされたバックアップ Adj-SID は、 **show ip ospf neighbor detail** および **show ip ospf segment-routing protected-adjacencies command** の出力で表示できます。

セグメント ルーティング マッピング サーバ

セグメント ルーティング マッピング サーバ（SRMS）を使用すると、プレフィックス SID マッピング ポリシー エントリの構成と保守を行うことができます。Cisco IOS XE リリース 3.17 では、IGP は SRMS のアクティブ ポリシーを使用して、フォワーディング プレーンのプログラミング時に SID 値を決定します。

SRMS は、ネットワークの SID/ラベル マッピング ポリシーにプレフィックスを提供します。一方、IGP は、プレフィックス SID/ラベル バインディング TLV を介して SID/ラベル マッピング ポリシーにプレフィックスをアドバタイズする役割を担います。

アクティブ ポリシー情報と変更は、アクティブ ポリシー情報を使用して転送情報を更新する IGP に通知されます。

接続されたプレフィックス SID

ルータが LSP にアドバタイズしたものとは異なる SID を持つプレフィックスをインストールする場合、たとえば、複数のプロトコルまたは複数の IGP インスタンスが、異なる SID を持つ同じプレフィックスを SRMS にアナウンスしている場合、SRMS は競合を解決し、ローカル インスタンスと同じでない可能性がある競合に勝ったプレフィックスと SID をアナウンスします。その場合、IGP は、常にソース LSP から学習した内容をアドバタイズしますが、その LSP で学習したものとは異なる可能性がある SID のインストールを試みます。これは IGP が別のプロトコルまたは別のプロトコル インスタンスから SID を再配布することを防ぐために行われます。

SRGB 範囲の変更

OSPF セグメント ルーティングが設定されている場合、OSPF は、OSPF SR の動作状態を有効にする前に SRGB とのインタラクションを要求する必要があります。SRGB 範囲が作成されていない場合、OSPF は有効になりません。

SRGB 変更イベントが発生した場合、OSPF は、そのサブブロック エントリで対応する変更を行います。また OSPF は、SR 機能サブ TLV で新しく作成または拡張された SRGB 範囲をアドバタイズし、プレフィックス SID サブ TLV アドバタイズメントを更新します。

インターフェイスでの MPLS 転送

セグメントルーティングがインターフェイスを使用する前に、MPLS転送を有効にする必要があります。OSPF は、インターフェイスでの MPLS 転送を有効にする役割を担います。

セグメントルーティングが OSPF トポロジに対して有効になっている場合、またはOSPF セグメントルーティングの動作状態が有効になっている場合、OSPFは、OSPF トポロジがアクティブである任意のインターフェイスに対して MPLS を有効にします。同様に、OSPF トポロジのセグメント ルーティングが無効になっている場合、OSPF は、そのトポロジのすべてのインターフェイスで MPLS 転送を無効にします。

SID エントリの競合処理

SIDエントリと関連付けられているプレフィックスエントリの間に競合がある場合は、次のいずれかの方法を使用して競合を解決します。

- システムが同じプレフィックスに対して2つのSIDエントリを受信すると、より高いルータ ID で受信したプレフィックスが、プレフィックスに対応する SID として扱われます。プレフィックスは、上位のルータ ID によってアドバタイズされた SID エントリを使用してインストールされます。
- システムが、1 つは OSPF プロトコル、他方は IS-IS プロトコルによる 2 つの SID エントリを受信すると、OSPF プロトコルによって受信した SID エントリが有効な SID として扱われます。プレフィックスは、OSPF プロトコルによって受信した SID エントリを使用してインストールされます。
- 2 つのプレフィックスが同じ SID エントリでアドバタイズされると、上位のルータ ID によってアドバタイズされたプレフィックスがSIDエントリを使用してインストールされ、もう一方のプレフィックスは SID エントリなしでインストールされます。

理想的な状況では、各プレフィックスに一意のSIDエントリが割り当てられている必要があります。

OSPFv2 ノード SID のセグメント ルーティングの設定方法

OSPFv2 ノード SID を使用してセグメント ルーティングを設定するには、次の手順を実行します。

OSPF のセグメント ルーティングの設定

始める前に

セグメント ルーティングをサポートするように OSPF を設定する前に、最初にグローバル コンフィギュレーション モードでセグメント ルーティング機能を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. segment-routing mpls
4. connected-prefix-sid-map
5. address-family ipv4
6. 1.1.1.1/32 index 100 range 1
7. exit-address-family

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	segment-routing mpls 例： `Device(config-sr)# segment-routing mpls`	mplsデータ プレーンを使用してセグメント機能を有効にします。
ステップ 4	connected-prefix-sid-map 例： `Device(config-srmpls)# connected-prefix-sid-map`	ローカル プレフィックスと SID のアドレス ファミリ固有のマッピングを設定できるサブモードを開始します。

	コマンドまたはアクション	目的
ステップ 5	address-family ipv4 例： `Device(config-srmpls-conn)# address-family ipv4`	IPv4 アドレス プレフィックスを指定します。
ステップ 6	1.1.1.1/32 index 100 range 1 例： `Device(config-srmpls-conn-af)# 1.1.1.1/32 100 range 1`	SID 100 にアドレス 1.1.1.1/32 を関連付けます。
ステップ 7	exit-address-family 例： `Device(config-srmpls-conn-af)# exit-address-family`	アドレス ファミリを終了します。

OSPF ネットワークでのセグメント ルーティングの設定

始める前に

OSPF ネットワークでセグメント ルーティングを設定する前に、ネットワーク上で OSPF を有効にする必要があります。

手順の概要

1. **router ospf 10**
2. **router-id**<*id*>
3. **segment-routing mpls**
4. **segment-routing area** <*area id*> **mpls**
5. **show ip ospf 10 segment-routing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**router ospf 10** 例： `Device(config)# router ospf 10`	OSPF モードを有効にします。
ステップ 2	**router-id**<*id*> 例： `Device(config-router)# router-id 1.0.0.0`	OSPF ルートを設定します。

	コマンドまたはアクション	目的
ステップ 3	**segment-routing mpls** 例： `Device(config-router)# segment-routing mpls`	セグメント ルーティング MPLS モードを設定します。
ステップ 4	**segment-routing area** <*area id*> **mpls** 例： `Device(config-router) # segment-routing area 0 mpls`	特定の領域にセグメントルーティングMPLSモードを設定します。

ステップ 5	**show ip ospf 10 segment-routing**
	例：
	`Device# show ip ospf 10 segment-routing`
		OSPFの下でSRを設定するための出力を示します。
		次の例は、OSPF のセグメント ルーティングに対する show ip ospf segment-routing state コマンドからの出力を表しています。
		`Device#show ip ospf 10 segment-routing`
		`OSPF Router with ID (0.0.0.1) (Process ID 10)`
		`Global segment-routing state: Enabled`
		`Segment Routing enabled:`
		`Area Topology name Forwarding`
		`0 Base MPLS`
		`1 Base MPLS`
		`SR Attributes`
		`Prefer non-SR (LDP) Labels`
		`Do not advertise Explicit Null`
		`Local MPLS label block (SRGB):`
		`Range: 16000 - 23999`
		`State: Created`
		`Registered with SR App, client handle: 3`
		`Connected map notifications active (handle 0x4), bitmask 0x1`
		`Active policy map notifications active (handle 0x5), bitmask 0xC`
		`Registered with MPLS, client-id: 100`
		`Bind Retry timer not running`
		`Adj Label Bind Retry timer not running`

OSPF のプレフィックス SID の設定

ここでは、各インターフェイスでプレフィックスセグメントID（SID）を設定する方法について説明します。

始める前に

セグメント ルーティングを対応するアドレス ファミリでイネーブルにする必要があります。

手順の概要

1. イネーブル化
2. configure terminal
3. segment-routing mpls
4. connected-prefix-sid-map
5. address-family ipv4
6. 1.1.1.1/32 index 100 range 1
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 例： `Device# enable`	特権 EXEC モードをイネーブルにします。
ステップ 2	configure terminal 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	segment-routing mpls 例： `Device(config)# segment-routing mpls`	セグメント ルーティング MPLS モードを設定します。
ステップ 4	connected-prefix-sid-map 例： `Device(config-srmpls)# connected-prefix-sid-map`	ローカル プレフィックスと SID のアドレス ファミリ固有のマッピングを設定できるサブモードを開始します。
ステップ 5	address-family ipv4 例： `Device(config-srmpls-conn)# address-family ipv4`	IPv4 アドレス ファミリを指定し、ルータ アドレス ファミリ 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	1.1.1.1/32 index 100 range 1 例： `Device(config-srmpls-conn-af)# 1.1.1.1/32 100 range 1`	SID 100 にアドレス 1.1.1.1/32 を関連付けます。

	コマンドまたはアクション	目的
ステップ 7	exit 例： `Device(config-router)# exit`	セグメントルーティングモードを終了し、コンフィギュレーション端末モードに戻ります。

プレフィックス属性 N-flag-clear の設定

OSPF は、その不透明 LSA に拡張プレフィックス TLV を介してプレフィックス SID をアドバタイズします。これはプレフィックスのフラグを伝送します。そのうちの1つはNフラグ（ノード）で、プレフィックスに沿って送信されたトラフィックが、LSAを発信するルータ宛てであることを示します。このフラグは通常、ルータのループバックのホスト ルートをマークします。

手順の概要

1. **enable**
2. **configure terminal**
3. interface loopback3
4. ip ospf prefix-attributes n-flag-clear

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface loopback3 例： `Device(config)# interface loopback3`	インターフェイス ループバックを指定します。
ステップ 4	ip ospf prefix-attributes n-flag-clear 例： `Device(config-if)# ip ospf prefix-attributes n-flag-clear`	プレフィックス N-flag をクリアします。

OSPF での明示的ヌル属性の設定

penultimate-hop-popping（PHP）を無効にし、明示的ヌル ラベルを追加するには、explicit-null オプションを指定する必要があります。このオプションを指定すると、OSPF は、拡張プレフィックス SID TLV の E フラグをその LSA に設定します。

デフォルトでは、ループバック アドレスに関連付けられたプレフィックス SID をアドバタイズするときに、OSPF によって E-flag（明示的ヌル フラグ）と呼ばれるフラグが 0 に設定されます。このフラグを設定するには、明示的な設定を追加します。

手順の概要

1. **enable**
2. **configure terminal**
3. segment-routing mpls
4. set-attributes
5. address-family ipv4
6. explicit-null
7. exit-address-family

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	segment-routing mpls 例： `Device(config)# segment-routing mpls`	セグメント ルーティング MPLS モードを設定します。
ステップ 4	set-attributes 例： `Device(config-srmpls)# set-attributes`	属性を設定します。
ステップ 5	address-family ipv4 例： `Device(config-srmpls-attr)# address-family ipv4`	IPv4 アドレス ファミリを指定し、ルータ アドレス ファミリ 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	explicit-null 例： `Device(config-srmpls-attr-af)# explicit-null`	明示的ヌルを指定します。
ステップ 7	exit-address-family 例： `Device(config-srmpls-attr-af)# exit-address-family`	アドレス ファミリを終了します。

OSPF のセグメント ルーティング Label Distribution Protocol 優先順位の設定

手順の概要

1. **enable**
2. **configure terminal**
3. segment-routing mpls
4. set-attributes
5. address-family ipv4
6. sr-label-preferred
7. exit-address-family

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	segment-routing mpls 例： `Device(config)# segment-routing mpls`	セグメント ルーティング MPLS モードを設定します。

	コマンドまたはアクション	目的
ステップ 4	set-attributes 例： `Device(config-srmpls)# set-attributes`	属性を設定します。
ステップ 5	address-family ipv4 例： `Device(config-srmpls-attr)# address-family ipv4`	IPv4 アドレス ファミリを指定し、ルータ アドレス ファミリ 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	sr-label-preferred 例： `Device(config-srmpls-attr-af)# sr-label-preferred`	LDP より優先される SR ラベルを指定します。
ステップ 7	exit-address-family 例： `Device(config-srmpls-attr-af)# exit-address-family`	アドレス ファミリを終了します。

OSPF SRMS の設定

次のコマンドは、OSPF SRMS を有効にして、OSPF がローカル マッピング エントリをアドバタイズできるようにします。OSPF は、SRMS ライブラリにリモート エントリを送信しません。ただし、OSPF は、ローカルに設定されたマッピング エントリのみに基づいて計算される SRMS アクティブ ポリシーを使用します。

```
[no] segment-routing prefix-sid-map advertise-local
```

OSPF SRMS クライアントの設定

デフォルトでは、OSPF SRMS クライアント モードが有効になっています。OSPF は、常に SRMS に LSA を通じて受信したリモート プレフィックス SID マッピング エントリを送信します。SRMS アクティブ ポリシーは、ローカルおよびリモートの両方のマッピング エントリに基づいて計算されます。

次のコマンドを実行すると、プレフィックス SID マッピング クライアント機能が無効になります。これは受信側で設定されます。

```
segment-routing prefix-sid-map receive [disable]
```

OSPFv2 ノード SID のセグメント ルーティングに関する追加情報

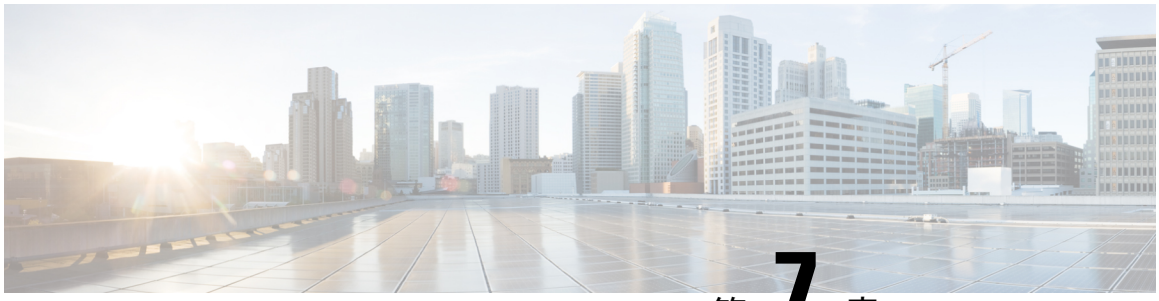
関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』 http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html
IP ルーティング ISIS コマンド	『Cisco IOS IP Routing ISIS commands』 http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

OSPFv2 ノード SID のセグメント ルーティングに関する機能情報

表 *5 : OSPFv2* ノード *SID* のセグメント ルーティングに関する機能情報

機能名	リリース	機能情報
OSPF によるセグメント ルーティング	Cisco IOS XE Release 3.16S Cisco IOS XE Fuji 16.7.1	セグメント ルーティング OSPFv2 ノード SID 機能は、OSPF ネットワークでのセグメント ルーティングのサポートを提供します。 次のコマンドが導入または変更されました。 **connected-prefix-sid-map**、 **show ip ospf 10 segment-routing**、 **sr-label-preferred**、 **ip ospf prefix-attributes n-flag-clear** Cisco IOS XE Fuji 16.7.1 では、この機能は Cisco 4000 シリーズ サービス統合型ルータでサポートされています。



第 7 章

OSPFv2 リンク保護のトポロジに依存しないループ フリー代替高速再ルーティング

このドキュメントでは、TI -LFA（トポロジに依存しないループ フリー代替）を使用した IP 高速再ルーティング機能（IP FRR）の OSPFv2 の実装について説明します。

トポロジに依存しないループフリー代替高速再ルーティングの制約事項

- TI-LFA は OSPFv2 でのみサポートされています。
- TI-LFA トンネルは、ルータが SR をサポートし、プレフィックス SID を使用して設定されている場合だけ作成されます。プレフィックス（または）ノード SID は、接続された SID として設定（または）SRMS（セグメント ルーティング マッピング サーバ）を使用してアドバタイズできます。
- TI-LFA は、マルチ ポイント インターフェイスへの OSPF ポイントではサポートされません。
- TI-LFA は、マルチ トポロジ ルーティング（MTR）をサポートしません。

- TI-LFA は、仮想リンク、シャム リンク（または）TE トンネルを使用して修復パスを作成しません。
- TI-LFA トンネルは、トンネルが通過する必要があるノード（または）修復ノードのセットを明示的に指定することによって構築され、プログラムされます。

OSPFv2リンク保護のトポロジに依存しないループフリー代替高速再ルーティングについて

トポロジに依存しないループフリー代替（TI-LFA）は、セグメントルーティングを使用して、RLFA（リモートループフリー代替）などの他の高速再ルーティング技術が保護を提供できないトポロジでリンク、ノード、および共有リスク リンク グループ（SRLG）保護を提供します。TI-LFA の目的は、リンク障害によるトポロジ変更後にルータがコンバージェンスする間に結果として生じるパケット損失を減らすことです。急速な障害修復（50 ミリ秒未満）は、分散ネットワーク コンバージェンス プロセスが完了するまで、ループフリーで安全に使用できる事前計算済みのバックアップ パスを使用することによって達成されます。

TI-LFA を使用する主な利点を次に示します。

- すべてのプレフィックスの 100% のカバレッジと 50 ミリ秒以内のリンクおよびノードの保護を提供します。
- コンバージェンス後のパスを活用することで、一時的な輻輳と最適でないルーティングを防ぎます。
- ラベル配布プロトコル（LDP）と IP トラフィックも保護します。

IP 高速再ルーティングおよびリモート ループ フリー代替

IP 高速再ルーティング（FRR）は、ネットワーク内の障害が発生したリンクまたは障害が発生したノードの周囲の IP トラフィックを、非常に短時間（50 ミリ秒未満）で再ルーティングできるようにする一連の手法です。使用される手法の 1 つは、OSPF プロトコルを使用して実装されるループ フリー代替（LFA）です。OSPF は現在、プレフィックスごとの直接接続された LFA およびリモート LFA（RLFA）をサポートします。これらの LFA アルゴリズムの問題はトポロジ依存性です。LFA アルゴリズムはすべてのトポロジに対してネットワークを通してループ フリー代替パスを見つけることはできません。

プレフィックスごとの直接接続された LFA（DLFA としても知られています）はほとんどの三角形のトポロジに対してループフリー代替パスを提供しますが、長方形または円形のトポロジに対しては優れたカバレッジを提供しません。再ルーティングされたトラフィックを中間ノードにトンネリングするために LDP シグナリングとともに MPLS フォワーディングを使用するリモート LFA 実装（RLFA）は、リングまたは長方形トポロジの IPFRR カバレッジを拡張します。各リンクについて、RLFA は P スペース（保護対象リンクを横断せずに計算ノードから到達可能なノードのセット）と Q スペース（保護対象リンク自体を横断せずに保護されたリンク上のネイバーに到達できるノードのセット）を定義します。P および Q スペースの両方に属す

るノードは、PQ ノードと呼ばれ、保護対象トラフィックの中間ノードとして使用できます。RLFA は、PQ ノードを対象にした LDP セッションを形成し、RLFA トンネルを構成します。ただし、P スペースと Q スペースが分離されているトポロジでは、R-LFA はそれらのプレフィックスを保護しません。

トポロジに依存しない高速再ルーティング

トポロジに依存しない高速再ルーティング（TI-FRR）は、トポロジ内のリンクのメトリックが対称であると仮定して、セグメントルーティングを使用して任意のトポロジでリンク保護を提供する技法です。TI-LFA は、単一リンクの帯域幅が非対称である場合のバックアップを保証しません。TI-LFA は、コンバージェンス後のパス上にあるループフリー修復パスのみを考慮します。これは、ネットワークのより優れたキャパシティ計画を行うのに役立ちます。

TI-LFA アルゴリズムは、ネットワークを通して完全な明示的パスを作成することを可能にします。完全に指定されたパスを使用すると、パスに沿ったセグメントの数が原因で、大きなトポロジで問題が発生する可能性があります。ただし、パス全体を指定する必要はなく、トラフィックを保護ノードにループバックしない中間ノード（リリース ノード）にトラフィックを伝送するために必要なのはパスのサブセットのみです。TI-LFA アルゴリズムは、修復パスとして SR トンネルを構築します。TI-LFA トンネルは、トンネルが通過する必要があるノード（または）修復ノードのセットを明示的に指定することによって構築され、プログラムされます。トラフィックは（プライマリ パスが失敗した場合）トンネルで伝送され、コンバージェンス後パスでも伝送されます。

トポロジに依存しないループ フリー代替

ローカル LFA およびリモート LFA が有効になっている場合、保護すべきプレフィックスのカバレッジは良好になります。ただし、PQ インターセクト ノードを持たないいくつかのまれなトポロジでは、ローカルおよびリモート LFA のどちらも、失敗したリンクを保護するために解放ノードを見つけることに失敗します。さらに、2 つのアルゴリズムには LFA のコンバージェンス後の特性についての知識がないため、コンバージェンス後の経路を優先する方法はありません。

上記の制限を克服するために、トポロジに依存しない LFA（TI-LFA）が SR 対応ネットワークでサポートされ、次のサポートを提供します。

- **リンク保護**：LFA はリンクの障害のための修復パスを提供します。
- **ローカル LFA**：コンバージェンス後のパスのローカル LFA が利用可能であるときはいつでも、ローカル LFA は修復パスのための追加 SID を必要としないので、TI LFA より優先されます。つまり、PQ ノードのラベルは、リリース ノードには必要ありません。
- **拡張 P スペースのローカル LFA**：拡張 P スペースのノードの場合、ローカル LFA は今でも修復パスのための最も経済的な方法です。この場合、TI-LFA は選択されません。
- **PQ 交差ノードへのトンネル**：これは、修復パスが TI-LFA を使用してコンバージェンス後のパスで保証されることを除いて、リモート LFA と類似しています。
- **PQ 分離ノードへのトンネル**：ローカルおよびリモート LFA が修復パスを見つけられない場合には、この機能は TI-LFA に固有です。

- **複数の交差または分離 PQ ノードを通過するトンネル**：TI-LFA は、プラットフォームのサポートされている最大ラベル数まで、すべてのプレフィックスの完全なカバレッジを提供します。
- **保護対象リンクのための P2P およびブロードキャスト インターフェイス**：TI-LFA は P2P およびブロードキャスト インターフェイスを保護します。
- **非対称リンク**：ネイバー間の OSPF メトリックは同じではありません。
- **マルチホーム（エニーキャスト）プレフィックス保護**：同じプレフィックスが複数のノードによって発信される可能性があり、TI-LFA はコンバージェンス後の修復パスを提供することによってエニーキャスト プレフィックスも保護します。
- **保護されたプレフィックスのフィルタリング**：ルートマップは、保護するプレフィックスのリストと、リリース ノードまでの最大修復距離を制限するオプションを含めるかまたは除外します。
- **タイブレーカー**：TI-LFA に適用可能な既存のタイブレーカーのサブセットがサポートされています。

トポロジに依存しないループ フリー代替タイブレーク

ローカルおよびリモート LFA は、プレフィックスを保護するために複数のパスがある場合、デフォルトまたはユーザ設定のヒューリスティックを使用してタイブレークします。この属性は、ロード バランシングの前に、TI-LFA リンク保護計算の終了時に修復パスの数を削減するために使用されます。

ローカル LFA およびリモート LFA は次のタイブレーカーをサポートします。

- **Linecard-disjoint**：ライン カード分離修復パスを優先します。
- **Node-protecting**：修復パスを保護するノードを優先します。
- **SRLG-disjoint**：SRLG 分離修復パスを優先します。
- **Load-sharing**：リンクとプレフィックスの間で均等に修復パスを分配します。

特定のプレフィックスに対して 2 つの修復パスがある場合、プライマリ ポートのものとは異なるライン カードの出力ポートであるパスが、修復パスとして選択されます。

- **LC-disjoint-index**：修復パスの両方がプライマリ パスのものと同じライン カード上にある場合、両方のパスが候補と見なされます。パスの 1 つが別のライン カード上にある場合は、そのパスが修復パスとして選択されます。

- **SRLG-disjoint**：SRLG 分離修復パスを優先します。

SRLG ID は、各インターフェイスに対して構成できます。プレフィックスに対して 2 つの修復パスがある場合、修復パスに設定された SRLG ID は、プライマリ パス SRLG ID のものと比較されます。セカンダリ パスの SRLG ID がプライマリのものと異なる場合、そのパスが修復パスとして選択されます。

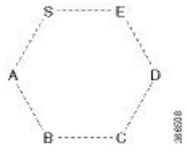
Cisco IOS XE リリース 3.18 では、ノード保護タイブレーカーはデフォルトで無効になっています。同じインターフェイス上のタイブレーカーのデフォルトと明示的なタイブレーカーは、相互に排他的です。以下のタイブレーカーは、すべての LFA でデフォルトで有効になっています。

- linecard-disjoint
- lowest-backup-metric
- SRLG-disjoint

P スペース

S-E を通過せずに最短パス ツリー上の S から到達できるルータのセットは、リンク S-E に関して、S の P スペースと呼ばれます。

図 *5 :* 単純なリング トポロジ



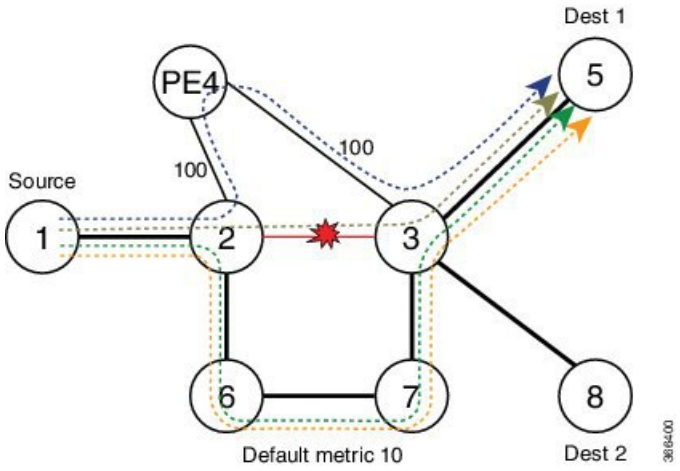
Q スペース

リンク S-E を通過することなく通常のフォワーディングによってノード E に到達できるルータのセットは、リンク S-E に関して、E の Q スペースと呼ばれます。

コンバージェンス後のパス

コンバージェンス後のパスは、OSPF がリンク障害の後に使用するパスです。TI-LFA は常に、コンバージェンス後のパスである修復パスを計算します。障害発生時にトラフィックを伝送するために、コンバージェンス後のパスを計画してサイズを合わせることができます。TI-LFA は、コンバージェンス後のパスをセグメントのリストとしてエンコーディングすることによって適用します。次の図は、コンバージェンス後のパスを使用した TI-LFA の例を示しています。

図 *6 :* コンバージェンス後のパスを使用した *TI-LFA*



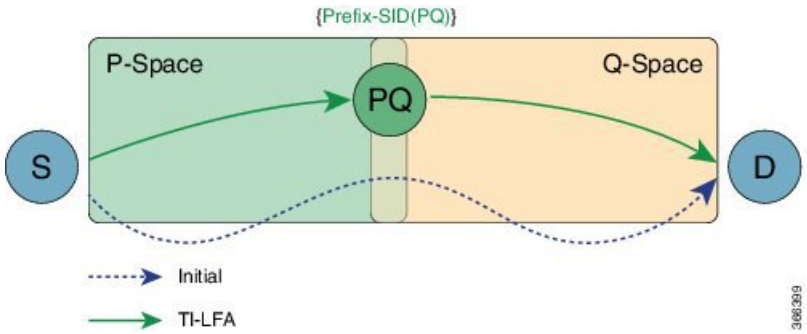
- これは、リンク 2-3 の障害に対してノード 2 の宛先ノード 5 を保護します。

- ノード 2 は、コア リンクを介してノード 5 宛てのすべてのトラフィックをスイッチします。

宛先ごとのリンク保護

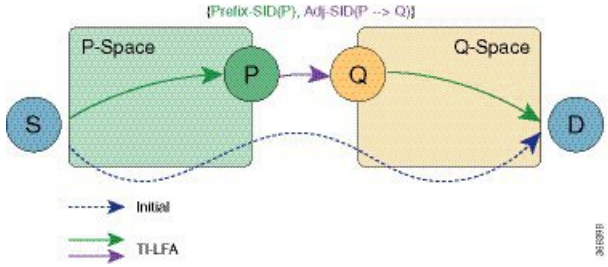
TI-LFA の実装は、基盤となるハードウェアによってサポートされるセグメント（ラベル）の数で宛先ごとのリンク保護を提供します。次の図は、TI-LFA の実装を示しています。

図 *7 : TI-LFA* : *{プレフィックス SID（PQ）}*



PQ が S の直接ネイバーである場合、追加セグメントをプッシュする必要はありません。

図 *8 : TI-LFA* : *{プレフィックス SID（P）、隣接関係 SID（P -> Q）}*



インターフェイスごとのループ フリー代替の使用可能性

- TI-LFA は、エリアごとに有効にすることができます。
- TI-LFA バックアップ パスが計算されるのは、保護対象のプライマリ インターフェイスで TI-LFA 保護が有効になっている場合だけです。デフォルトでは、すべてのインターフェイスで保護が有効です。
- TI-LFA 修復パスは、ハードウェアによってサポートされるラベルの数によって制限されます。ハードウェアが 2 つのラベルだけをサポートする場合、TI-LFA 修復パスは、2 つ以下のセグメントによって保護できるそれらのプレフィックスだけを保護できます。2 つ以上のセグメントを必要とするそれらのプレフィックスは、未保護のままになります。

プレフィックス処理

すべてのリンクについて TI-LFA パスが計算されると、プレフィックス処理が開始されます。デフォルトでは、エリア内およびエリア間のプレフィックスのみが保護されます。外部プレフィックスを保護するには、OSPF レベルでグローバルにセグメント ルーティングを有効にする必要があります。

プライマリ パスと修復パスは、保護されているプレフィックスと同じルート タイプである必要があります。つまり、エリア内を保護する必要がある場合、TI-LFA 修復パスは、プレフィックスが一意であっても（または）エニーキャストプレフィックスであっても、同じエリア内プレフィックスについても計算します。

エニーキャスト プレフィックス処理

またOSPF TI-LFAは、エニーキャストプレフィックスのための修復パスを計算します。エニーキャストプレフィックス（または）デュアルホームのプレフィックスは、複数のルータによってアドバタイズされたプレフィックスです。エリア内、エリア間、またはエリア外プレフィックスである可能性があります。エニーキャスト プレフィックスのための TI-LFA 修復パスの計算は以下のとおりです。

- プレフィックス P1 がルータ R1 および R2 によってアドバタイズされると仮定します。両方のルータによってアドバタイズされたプレフィックスは、同じルート タイプである必要があります。つまり、R1 と R2 の両方で、プレフィックスをエリア内プレフィックス（またはエリア内もしくはエリア外）としてアドバタイズする必要があります。
- プライマリ パスは、コストが低いため R1 に向けて計算されます。
- TI-LFAがバックアップパスを計算するときに、コンバージェンス後のパスを計算します。したがって、コンバージェンス後のパスは R1 向けである必要はありません。R2（コンバージェンス後）に到達するためのコストがより短い場合、TI-LFA アルゴリズムは R2 向けのコンバージェンス後パスを選択します。TI-LFA トンネルは R2 に向けて形成されます。
- R2 がプレフィックスをアドバタイズしない場合、TI-LFA アルゴリズムは R1 向けの修復パスについて再計算されます。

プレフィックスごとのループ フリー代替タイブレーク

IP FRR には、以下に示す順序で下記のタイ ブレーク ルールがあります。最適なパスを選択できる複数の修復パスがある場合は、次のタイブレーク ルールが適用されます。複数のパスがすべてのタイブレーク ルールに一致する場合、すべてのパスが修復パスとして使用されます。

- **Post Convergence**：コンバージェンス後のパスであるバックアップ パスを優先します。これはデフォルトで有効になっていて、ユーザはこれを変更できません。
- **Primary-path**：ECMP セットからのバックアップ パスを優先します。
- **Interface-disjoint**：ポイントツーポイントインターフェイスには、プライマリ ゲートウェイで障害が発生した場合、再ルーティングのための代替のネクストホップはありません。

interface-disjoint 属性を設定すると、このような修復パスの選択を防ぐことができるため、インターフェイスが保護されます。

- **Lowest-backup-metric**：最小の合計メトリックを持つバックアップ パスを優先します。TI-LFA は常に最低のコストであるバックアップ パスを選択するので、これは TI-LFA には適用されません。
- **LC-disjoint**：プライマリ パスとは異なるライン カードにあるバックアップ パスを優先します。
- **Broadcast-interface-disjoint**：LFA 修復パスは、修復パスと保護されたプライマリ パスが異なるネクストホップインターフェイスを使用するときにリンクを保護します。ただし、ブロードキャストインターフェイスでは、LFA修復パスがプライマリ パスと同じインターフェイスを介して計算され、ネクストホップ ゲートウェイが異なる場合、ノードは保護されますがリンクは保護されないことがあります。broadcast-interface-disjoint 属性を設定すると、プライマリ パスがポイントするブロードキャスト ネットワークを修復パスが経由しない（つまり、インターフェイスと、これに接続されるブロードキャスト ネットワークを使用できない）ように指定することができます。
- **Load Sharing**：上記のルールに一致する修復パスが複数ある場合は、バックアップ パスをロード シェアします。このルールは、ユーザが変更することもできます。

（注） ユーザは、要件に応じてタイブレーク ルールを変更および定義できます。このようにして、ユーザはシーケンスの優先順位を変更したり、必要のないタイ ブレーク インデックスの一部を削除したりすることができます。

（注） TI-LFA は常に最低コストのバックアップ パスのみを選択するので、Lowest-backup-metric ポリシーは TI-LFA には適用されません。

上記のルールは、次のコマンドを使用して確認できます。

```
R2#show ip ospf fast-reroute

            OSPF Router with ID (2.2.2.200) (Process ID 10)

Microloop avoidance is enabled for protected prefixes, delay 5000 msec

Loop-free Fast Reroute protected prefixes:

           Area        Topology name   Priority   Remote LFA Enabled     TI-LFA Enabled
              0                Base        Low                  No                Yes
    AS external                Base        Low                  No                Yes

  Repair path selection policy tiebreaks (built-in default policy):
      0  post-convergence
     10  primary-path
     20  interface-disjoint
     30  lowest-metric
```

```
     40  linecard-disjoint
     50  broadcast-interface-disjoint
    256  load-sharing

OSPF/RIB notifications:
 Topology Base: Notification Enabled, Callback Registered

Last SPF calculation started 17:25:51 ago and was running for 3 ms.
```

TI-LFA の導入によって、次の 2 つのタイブレーク ルールが拡張されます。

- node-protection
- srlg-protection

上記の2つのタイブレーク ルールは、デフォルトでは有効になっていません。ユーザは、前述のタイブレーク ポリシーを設定する必要があります。

ノード保護

TI-LFA ノード保護は、ノード障害からの保護を提供します。ノードを保護する TI-LFA は、特定のネクストホップへのリンクだけでなく、特定のネクストホップの障害に対して保護するコンバージョン後の修復パスの計算を試みます。

ノード保護は、ローカル LFA の実装でもタイブレーカーとして使用されます。ただし、これが TI-LFA と組み合わされると、バックアップ パスはノード保護パスとのコンバージェンス後に計算されます。プレフィックスごとの TI-LFA ノード保護はデフォルトで無効になっています。IPFRR TI-LFA ノード保護機能は、対応するタイブレークが TI-LFA 機能とともに有効になると有効になります。つまり、

```
router ospf 10
   [no] fast-reroute per-prefix ti-lfa [area <area> [disable]]
   [no] fast-reroute per-prefix tie-break node-protecting index <index>
   [no] fast-reroute per-prefix tie-break node-protecting required index <index>
```

ノード保護を有効にする場合、他のすべてのタイ ブレーク ルールも手動で設定する必要があります。ノード保護はリンク保護上に構築されます。

node-protecting と **node-protecting required** の違いは、バックアップ パスの選択です。**node-protecting required** を設定すると、選択されたバックアップは、ノード（保護しているリンクの一部）を通過しないパスでなければなりません。このようなパスが使用できない場合は、バックアップ パスとしてパスが選択されません。

共有リスク リンク グループ保護

共有リスク リンク グループ（SRLG）は、同時に障害が発生する可能性が高い修復パスおよび保護されたプライマリ パスのネクストホップ インターフェイスのグループです。OSPFv2 ループフリー Fast Reroute 機能では、コンピューティング ルータでローカルに設定された SRLG のみがサポートされます。TI LFA の導入によって、SRLG グループ ID をプライマリ パス インターフェイスと共有しないコンバージェンス後のパスが選択されます。このようにして、プライマリ リンクが失敗するたびに、ユーザは SRLG 保護を確認します。

IPFRR TI-LFA SRLG 保護機能は、対応するタイブレークが Ti-LFA 機能とともに有効になると有効になります。つまり、

```
router ospf 10
   [no] fast-reroute per-prefix ti-lfa [area <area> [disable]]
   [no] fast-reroute per-prefix tie-break srlg index <index>
   [no] fast-reroute per-prefix tie-break srlg required index <index>
```

SRLG 保護を有効にすると、他のすべてのタイ ブレーク ルールを手動で設定する必要があります。**srlg-protecting** と **srlg-protecting required** の違いは、バックアップ パスの選択です。**srlg-protecting required** を設定すると、選択されたバックアップは、保護されているプライマリ リンクと SRLG ID を共有しないパスでなければなりません。このようなパスが使用できない場合は、バックアップ パスとしてパスが選択されません。

一方、**srlg-protecting** を単独で設定すると、SRLG 保護パスが使用できない場合は、リンク保護パスがバックアップ パスとして選択されます。SRLG 保護パスが使用可能な場合、SRLG 保護パスへのスイッチオーバーが行われます。

ノード共有リスク リンク グループ保護

ノードと SRLG の保護タイ ブレークの両方を一緒に設定できます。これは、バックアップ パスがノード保護と SRLG 保護の両方の基準を満たす必要があることを意味します。その場合、追加の TI-LFA ノード SRLG の組み合わせ保護アルゴリズムが実行されます。TI-LFA ノード SRLG の組み合わせアルゴリズムは、コンバージェンス後の最短パスツリー（SPT）を計算するときに、保護されたノードと、同じ SRLG グループを持つインターフェイスのすべてのメンバーを削除します。

ノードおよび SRLG の保護タイ ブレークを一緒に有効にするには、次のコマンドを使用します。

```
router ospf 10
   [no] fast-reroute per-prefix ti-lfa [area <area> [disable]]
   [no] fast-reroute per-prefix tie-break node-protecting index <index>
   [no] fast-reroute per-prefix tie-break srlg index <index>
```

次の show コマンドは、タイ ブレーク ポリシーを表示するために使用されます。

```
R3#show ip ospf fast-reroute

            OSPF Router with ID (3.3.3.33) (Process ID 10)

Loop-free Fast Reroute protected prefixes:

           Area        Topology name   Priority   Remote LFA Enabled     TI-LFA Enabled
              0                Base        Low                   No                 No
              1                Base        Low                   No                 No
           1000                Base        Low                   No                 No
    AS external                Base        Low                   No                 No

  Repair path selection policy tiebreaks:
      0  post-convergence
     60  node-protecting
     70  srlg
    256  load-sharing
```

```
OSPF/RIB notifications:
 Topology Base: Notification Disabled, Callback Not Registered

Last SPF calculation started 00:00:06 ago and was running for 2 ms.
```

トポロジに依存しないループフリー代替高速再ルーティングの設定方法

トポロジに依存しないループフリー代替高速再ルーティングの有効化

デフォルトでは、TI-LFA は無効になっています。プロトコルの有効化を使用して、TI-LFA を有効にすることができます。

プロトコルの有効化：すべての OSPF エリアに対して、ルータ OSPF モードで TI-LFA を有効にします。TI-LFA FRR を有効にするには、次の手順を実行します。

```
[no] fast-reroute per-prefix ti-lfa [ area <area> disable]
```

```
router ospf <process>
fast-reroute per-prefix enable area <area> prefix-priority {low | high}
fast-reroute per-prefix ti-lfa [ area <area> disable]
```

また、インターフェイス コマンドを使用して、特定のインターフェイスで IP FRR を有効または無効にすることもできます。

```
interface <interface>
ip ospf fast-reroute per-prefix protection disable
ip ospf fast-reroute per-prefix candidate disable
ip ospf fast-reroute per-prefix protection ti-lfa [disable]
```

（注）
- TI-LFA が OSPF ルータおよび広域で設定されるとき、エリア特定の設定が優先します。
- 外部プレフィックスを保護するには、TI-LFA はグローバルに有効にする必要があります。

トポロジに依存しないループ フリー代替高速再ルーティングの設定

このタスクでは、リンク、ノード、および SRLG の障害に関するトラフィック フローを収束させるために、プレフィックスごとのトポロジに依存しないループフリー代替（TI-LFA）の計算を有効にする方法について説明します。TI-LFA は、より低いレベルによって継承されたインスタンスまたはエリア レベルで設定することができます。TI-LFA にも適用されるインターフェイス レベルごとのプレフィックス FRR ごとに有効または無効にできます。

設定を開始する前に、次のトポロジ要件を満たしていることを確認してください。

- ルータ インターフェイスがトポロジごとに設定されている。

- ルータが OSPF で設定されている。
- セグメント ルーティングが OSPF レベルでもグローバルでも有効である。

1. 指定されたルーティング プロセスの OSPF ルーティングを有効にして、ルータ コンフィギュレーション モードを開始します。

```
Device(config)# router ospf 10
```

2. FRR を有効にします。

```
Device(config-router)# fast-reroute per-prefix enable prefix-priority low
```

3. TI-LFA を有効にします。

```
Device(config-router)# fast-reroute per-prefix ti-lfa
```

4. 特定のエリアで TI-LFA を有効にします。

```
Device(config-router)# fast-reroute per-prefix ti-lfa area 0
```

5. TI-LFA モードを終了します。

```
Device(config-router)# exit
```

6. インターフェイス モードに入ります。

```
Device(config)#interface ethernet 0/0
```

7. 特定のインターフェイスで FRR を有効にしたくない場合は、protection disable コマンドを使用します。

```
Device(config-if)#ip ospf fast-reroute per-prefix protection disable
```

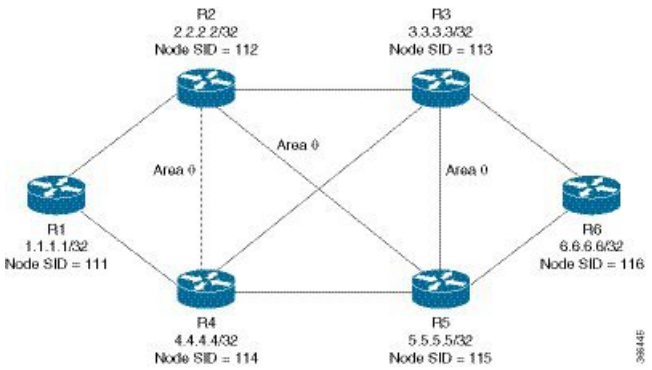
8. 特定のインターフェイスを修復パスとして有効にしたくない場合は、candidate disable コマンドを使用します。

```
Device(config-if)#ip ospf fast-reroute per-prefix candidate disable
```

トポロジに依存しない高速再ルーティング タイブレーカーの設定

すべてのノードのプレフィックス SID が設定されているすべてのルータで、セグメント ルーティングを有効にする必要があります。構成を理解するには、次のトポロジを参照として使用してください。

図 *9* : 設定例



R2 と R3 の間のリンクを保護するデバイス R2 を考えます。R2 での設定：

```
router ospf 10
fast-reroute per-prefix enable prefix-priority low
fast-reroute per-prefix ti-lfa
segment-routing mpls
segment-routing area 0 mpls
fast-reroute per-prefix enable prefix-priority low
fast-reroute per-prefix ti-lfa
fast-reroute per-prefix ti-lfa area 0
fast-reroute per-prefix tie-break node-protecting index 60
fast-reroute per-prefix tie-break srlg index 70
mpls traffic-eng router-id Loopback1
mpls traffic-eng area 0

interface GigabitEthernet4   //interface connecting to the router 4
ip address 100.101.4.4 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
srlg gid 10
negotiation auto

interface GigabitEthernet3  //interface connecting to the router 3
ip address 100.101.3.3 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
srlg gid 10
negotiation auto

interface GigabitEthernet5   //interface connecting to the router 2
ip address 100.101.5.5 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
srlg gid 20
negotiation auto



interface loopback2
ip address 2.2.2.2/32
ip ospf 10 area 0
```

（注） 他のすべてのデバイスでは、セグメント ルーティングの構成と、接続されたプレフィックス SID の割り当てを行う必要があります。

ノード保護の仕組み：例として同じトポロジを使用し、R2 と R3 の間のリンクと R6 からのプレフィックスも保護している場合を考えてみましょう。その場合、プレフィックスのプライマリ パスが R2-R3 経由であると想定してみましょう。したがってプライマリ パスは R2---R3---R6 であり、リンク R2---R3 を保護しています。

このシナリオでは、リンク保護のみが設定され、有効になっています。OSPF プロセスの下で TI-LFA を有効にすると、すべてのパスのコストが等しいという条件で次のパスが得られます。

R2----R4----R5---R6

R2---R5----R3---R6

R2----R5---R6

リンク保護のみを設定している場合は、3 つのパスがすべて選択され、それらの間で負荷が共有されます。

ノード保護を構成する場合は、バックアップ パスに保護対象のノードが含まれないようにバックアップが計算されます。この例では、バックアップのノード R3 は必要ありません。その結果、次の 2 つのパスのみがバックアップ パスとして選択されます。

R2----R4----R5---R6

R2----R5---R6

R2---R5---R3---R6 のコストは上記の 2 つのパスよりも小さい可能性があります。しかし、ノード保護が設定されているため、上記の 2 つのパスのみが考慮されます。

SRLG 保護の仕組み：SRLG 保護は、プライマリ パスとバックアップが同じ SRLG ID を共有しないような方法で、バックアップ パスをさらに排除します。次のバックアップ パスが使用可能であるとします。

R2----R4----R5---R6

R2----R5---R6

次に、（R2----R4）と（R2----R5）の SRLG ID が、10 であるプライマリ インターフェイス（R2----R3）と比較されます。インターフェイス R2----R5 のみが、異なる SRLG ID である 20 を持つことに注意します。したがって、バックアップ パス R2---R5---R6 のみが選択されます。

トポロジに依存しない高速再ルーティング トンネルの確認

次のコマンドを使用して、TI LFA トンネルを確認することができます。

```
Device#show ip ospf fast-reroute ti-lfa tunnels

                OSPF Router with ID (2.2.2.200) (Process ID 10)
```

```
                          Area with ID (0)

                    Base Topology (MTID 0)

Tunnel                Interface         Next Hop         Mid/End Point    Label
------------------------------------------------------------------------------
MPLS-SR-Tunnel2       Et1/1             2.7.0.7          1.1.1.1          16020
MPLS-SR-Tunnel6       Et0/3             2.8.0.0          3.3.3.3          16003
MPLS-SR-Tunnel7       Et1/1             2.7.0.7          1.1.1.1          16020
                                                         5.5.5.5          16005
                                                         3.3.3.3          16003
MPLS-SR-Tunnel5       Et0/3             2.8.0.0          5.5.5.5          16005
MPLS-SR-Tunnel1       Et1/1             2.7.0.7          1.1.1.1          16020
                                                         5.5.5.5          16005
MPLS-SR-Tunnel3       Et1/1             2.7.0.7          6.6.6.6          16006
```

次のコマンドを使用して、プライマリおよび修復パスを持つOSPFルーティングテーブル内のルートを確認できます。

```
Device#show ip ospf rib 6.6.6.6

            OSPF Router with ID (2.2.2.200) (Process ID 10)

                Base Topology (MTID 0)

OSPF local RIB
Codes: * - Best, > - Installed in global RIB
LSA: type/LSID/originator

*>  6.6.6.6/32, Intra, cost 31, area 0
     SPF Instance 19, age 02:12:11
      contributing LSA: 10/7.0.0.0/6.6.6.6 (area 0)
     SID: 6
     CSTR Local label: 0
     Properties: Sid, LblRegd, SidIndex, N-Flag, TeAnn
     Flags: RIB, HiPrio
      via 2.7.0.7, Ethernet1/1 label 16006
       Flags: RIB
       LSA: 1/6.6.6.6/6.6.6.6
      PostConvrg repair path via 3.3.3.3, MPLS-SR-Tunnel6 label 16006, cost 81, Lbl cnt
 1
       Flags: RIB, Repair, PostConvrg, IntfDj, LC Dj
       LSA: 1/6.6.6.6/6.6.6.6
```

次のコマンドを使用して、IP ルーティング テーブルにルートを表示できます。

```
Device#show ip route 6.6.6.6
Routing entry for 6.6.6.6/32
  Known via "ospf 10", distance 110, metric 31, type intra area
  Last update from 2.7.0.7 on Ethernet1/1, 00:25:14 ago
 SR Incoming Label: 16006
  Routing Descriptor Blocks:
  * 2.7.0.7, from 6.6.6.6, 00:25:14 ago, via Ethernet1/1, merge-labels
      Route metric is 31, traffic share count is 1
      MPLS label: 16006
      MPLS Flags: NSF
      Repair Path: 3.3.3.3, via MPLS-SR-Tunnel6
```

トポロジに依存しないループフリー代替高速再ルーティングのデバッグ

次のコマンドを使用して、TI-LFA FRR をデバッグすることができます。

```
debug ip ospf fast-reroute spf
debug ip ospf fast-reroute spf detail
debug ip ospf fast-reroute rib
debug ip ospf fast-reroute rib [<access-list>]
```

例：OSPFv2リンク保護のトポロジに依存しないループフリー代替高速再ルーティング

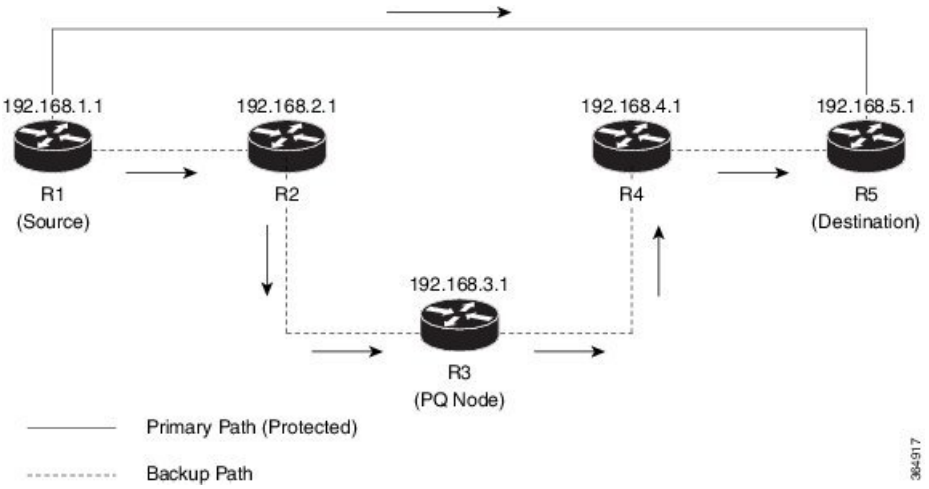
OSPFv2 リンク保護 TI-LFA FRR の例を次に示します。

例：トポロジに依存しないループフリー代替高速再ルーティングの設定

この例では、単一またはディスジョイントの PQ ノードを使用してセグメント ルーティング TE トンネルに TI-LFA を設定する方法を示します。次に、使用される 2 つのトポロジを示します。

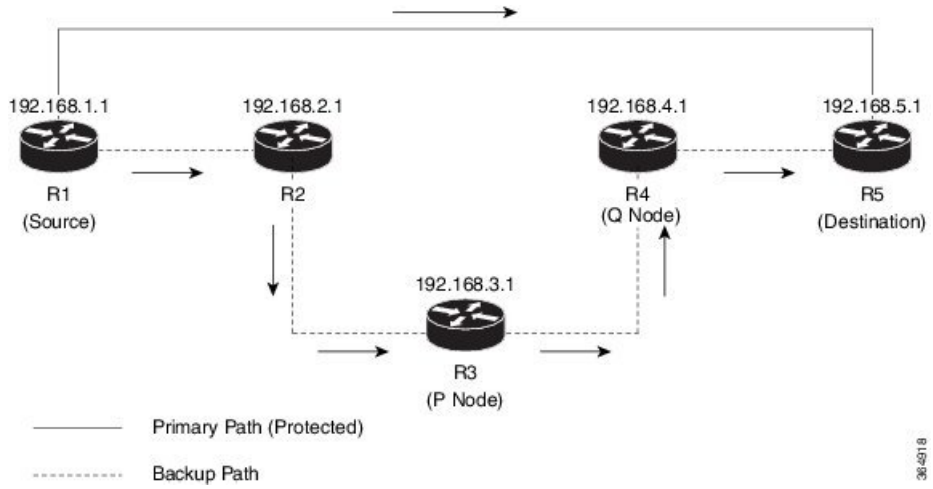
- トポロジ 1：単一の PQ ノードであり、2 つの SID を持ちます。送信元ルータ R1 から PQ ノードを経由して宛先ルータ R5 に送信されます。

図 *10*：トポロジ *1*：単一の *PQ* ノード



- トポロジ2：ディスジョイントPQノードであり、3つのSIDで構成されます。送信元ルータR1からPノードおよびQノードを介して宛先ルータR5に送信されます。

図 *11*：トポロジ *2*：ディスジョイント *PQ* ノード



宛先ルータ（R5）に接続する送信元ルータ（R1）インターフェイスでOSPF用にTI-LFAを設定します。

```
Device(config)# router ospf 10
Device(config-router)# fast-reroute per-prefix enable prefix-priority low
Device(config-router)# fast-reroute per-prefix ti-lfa
Device(config-router)# fast-reroute per-prefix ti-lfa area 0
Device(config-router)# exit
```

OSPFv2リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの追加情報

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 Command List, All Releases』

OSPFv2リンク保護のトポロジに依存しないループフリー代替高速再ルーティングの機能情報

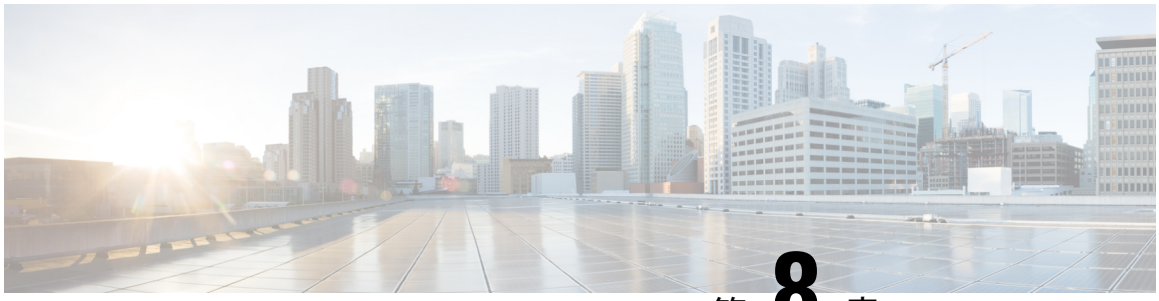
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

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 *6 : OSPFv2* リンク保護のトポロジに依存しないループ フリー代替高速再ルーティングの機能情報

機能名	リリース	機能情報
OSPFv2 リンク保護のトポロジに依存しないループ フリー代替高速再ルーティング	Cisco IOS XE Everest 16.4.1 Cisco IOS XE Fuji 16.7.1	トポロジに依存しないループ フリー代替（TI-LFA）は、セグメント ルーティングを使用して、他の高速再ルーティング技術が保護を提供できないトポロジでリンク、ノード、および共有リスク リンク グループ（SRLG）保護を提供します。TI-LFA の目的は、リンク障害によるトポロジ変更後にルータがコンバージェンスする間に結果として生じるパケット損失を減らすことです。 次のコマンドが導入または変更されました。 **fast-reroute per-prefix ti-lfa [area <area> [disable]]、fast-reroute per-prefix tie-break node-protecting index <index>、fast-reroute per-prefix tie-break node-protecting required index <index>、fast-reroute per-prefix tie-break srlg index <index>、fast-reroute per-prefix tie-break srlg required index <index>、ip ospf fast-reroute per-prefix protection disable、ip ospf fast-reroute per-prefix candidate disable、show ip ospf fast-reroute ti-lfa tunnels**。 Cisco IOS XE Fuji 16.7.1 では、この機能は Cisco 4000 シリーズ サービス統合型ルータでサポートされています。



第 8 章

OSPF のセグメント ルーティング トラフィック エンジニアリング

この章では、OSPF を使用してセグメント ルーティング トラフィック エンジニアリングを実装する方法について説明します。

OSPF のセグメント ルーティング トラフィック エンジニアリングの制約事項

- セグメント ルーティング トラフィック エンジニアリングは、OSPFv2 でのみサポートされています。
- SR-TE は、ブロードキャスト インターフェイスではサポートされていません。ポイントツーポイント インターフェイスのみサポートしています。
- Cisco ASR ルータは、発信パケットに課される特定の数のラベルのみをサポートします。ラベルの数が指定された数よりも大きい場合、SR-TE トンネルの作成は失敗します。Cisco ASR1000 ルータは、最大 16 個のラベルをサポートします。
- 特定の時点で、TE に対して有効にする必要があるプロトコルのインスタンスは 1 つだけです。

OSPF のセグメント ルーティング トラフィック エンジニアリングに関する情報

トラフィック エンジニアリング（TE）トンネルは、トンネルの入力とトンネルの宛先との間でインスタンス化された TE LSP のコンテナです。TE トンネルは、同じトンネルに関連付けられた 1 つ以上の SR-TE LSP をインスタンス化できます。SR-TE LSP パスが宛先ノードへの同じ IGP パスに必ずしも従うとは限りません。この場合、SR-TE パスには、SR-TE LSP が通過するノードおよび/またはリンクのプレフィックス SID および/または隣接関係 SID のセットを指定することができます。

ヘッドエンドは、トンネルを通して伝送される発信パケットに、対応する MPLS ラベル スタックを課します。SR-TE LSP パスに沿った各通過ノードは、パケットが最終的な宛先に到達するまで、着信トップ ラベルを使用してネクストホップを選択し、ラベルをポップまたはスワップし、ラベル スタックの残りの部分を使用して次のノードにパケットを転送します。OSPF は、トポロジおよび SR に関連する情報を TE に提供します。SR 関連情報には、ネットワーク内で SR が有効になっているすべてのノード/リンクの SRGB/プレフィックス/隣接関係 SID が含まれます。

OSPF のセグメント ルーティング トラフィック エンジニアリングを使用する利点

セグメント ルーティング トラフィック エンジニアリングは、次のような役に立つすべての最適化と制約を包括的にサポートしています。

- 遅延
- 帯域幅
- ディスジョイントネス
- リソース回避

OSPFv2 は、SR-TE に以下の機能を提供します。

- OSPFv2 は、TE モジュールに SR 情報とともに TE トポロジ情報を提供します。
- TE では、この情報を使用し、プレフィックスおよび/または隣接関係セグメントの組み合わせを使用して、1 つ以上のセグメントで構成される SR TE パス/トンネルを構築します。
- TE が関連するプレフィックスの場合、OSPF はフォワーディング プレーンをセットアップするためのファースト ホップの解決策を提供します。
- また、SR TE トンネルは、SR-TE トンネル上のトラフィックを即転送するために OSPF（RSVP TE トンネルなど）に再度アドバタイズされます。

OSPFv2 セグメント ルーティング トラフィック エンジニアリング機能

OSPFv2 は、SR-TE のために以下の機能を実行します。

- OSPFv2 は、TE モジュールに SR 情報とともに TE トポロジ情報を提供します。
- TE では、この情報を使用し、プレフィックスおよび/または隣接関係セグメントの組み合わせを使用して、1 つ以上のセグメントで構成される SR TE パス/トンネルを構築します。
- TE が関連するプレフィックスの場合、OSPF はフォワーディング プレーンをセットアップするためのファースト ホップの解決策を提供します。
- また、SR TE トンネルは、SR-TE トンネル上のトラフィックを即転送するために OSPF（RSVP TE トンネルなど）に再度アドバタイズされます。

保護された隣接関係 SID

セグメント ルーティングは、ポイント ツー ポイント インターフェイスおよびブロードキャスト インターフェイスに対して保護された隣接関係 SID を作成します。セグメント ルーティングは、それらを保護されていない隣接関係 SID とともに、拡張リンク ステート アドバタイズメント（LSA）にアドバタイズします。保護された隣接関係 SID は修復パスを持つことができますが、修復パスを持つことが保証されるわけではありません。

トラフィック エンジニアリング インターフェイス

SR-TE 機能をサポートするため、TE は、TE トポロジに関する情報を配布および受信するためのさまざまなコンポーネントや IGP（OSPF および ISIS）と連携します。SR-TE サポートの場合、OSPF は、さまざまな LSA を通じて受信した SR 情報を TE に追加で提供する必要があります。

- ルータ情報 LSA
- 拡張プレフィックス LSA
- 拡張リンク LSA

TE インターフェイスは、TE 用に設定されたリンクに関連付けられた、帯域幅リソース、制約、機能、その他の属性などの情報を配布します。リンク情報は、不透明な LSA を使用して他のルータに配布され、TE によってローカル トポロジ データベースを作成するために使用されます。トポロジ データベースは、TE が LSP を確立するための適切な制約ベースのパスを計算できるようにするための鍵となる要素です。TE は IGP とも連携し、ルーティング パケット用に TE ヘッドエンド インターフェイスを考慮できる場合に通知します。

アンナンバード サポート

アンナンバード リンクの IS-IS の説明には、リモート インターフェイス ID 情報は含まれません。アンナンバード リンクのリモート インターフェイス ID には、SR-TE トンネルの一部としてアンナンバード リンクを含める必要があります。

隣接関係転送のためのセグメント ルーティング トラフィック エンジニアリング サポート

MPLS TE 転送隣接機能は、OSPF でサポートされます。この場合、TE トンネルは IGP ネットワーク内のリンクと見なされます。TE トンネル インターフェイスは、他のリンクと同様に、IGP ネットワーク内にアドバタイズされます。その後、ルータはこれらのリンクを使用して最短パス ツリー（SPT）を計算できます。

（注） この機能は、SR-TE トンネルではサポートされていません。

自動ルート アナウンスのためのセグメント ルーティング トラフィック エンジニアリング サポート

MPLS TE 自動ルート アナウンス機能は、TE トンネルをファーストホップとして使用する OSPF によって、ノードがそのトンネル経由で到達可能な場合にサポートされます。これにより、TE トンネルのテールエンドへ向かう下流方向のノードへのトラフィックがトンネルを通って流れます。OSPF では、RSVP を使用した MPLS TE トンネル設定と同様に、SR-TE トンネル上での自動ルートをサポートします。

SR-TE LSP をインスタンス化する TE トンネルは、IGP のショートカットとして IGP（OSPF および ISIS）に自動ルート アナウンス（AA）することができます。IGP はネクスト ホップとして TE トンネルを使用し、最短パスが TE トンネルの宛先よりも遅くなるすべての IP プレフィックスに対して RIB にルートをインストールします。TE トンネルの自動ルート アナウンスは、IPV4 プレフィックスを運ぶためにサポートされています。

自動ルート アナウンス IP2MPLS

SR トンネルのための自動ルート IP2MPLS 機能は、SR-TE トンネルのヘッドエンド/入力と、ヘッドエンド/入力にパケットを指定/ルーティングして戻すノードとの間で、潜在的なパケットが無限にループするのを回避するために導入されました。

このソリューションは、SR-TE トンネルにマッピングされるプレフィックスに対して 2 セットのパスを転送するヘッドエンドプログラミングで構成されています。1 つ目は、発信インターフェイスをトンネルインターフェイスとして持ち、マッピングされているプレフィックスの純粋な IP ルートです。これにより、IP トラフィックをトンネル経由で直接マッピングできます。2 つ目は、トンネルにマップされたプレフィックスの MPLS パスです。この場合プレフィック

スSIDラベルはIGPの最短パス発信インターフェイス、つまり非トンネル出力インターフェイスでプログラムされます。

SR-TE LSP のインスタンス化

トラフィック エンジニアリング（TE）トンネルは、1 つ以上のインスタンス化された TE LSP のコンテナです。SR-TE LSP は、TE トンネルのパスオプションで「segment-routing」を設定することによってインスタンス化されます。トンネルにマップされたトラフィックは、プライマリ SR-TE のインスタンス化 LSP を介して転送されます。

同じトンネルの下で複数のパスオプションを設定することもできます。各パスオプションには、プリファレンスインデックスまたはパスオプションインデックスが割り当てられていて、プライマリ LSP をインスタンス化するためのより有利なパスオプションを決定するために使用されます。パスオプションのプリファレンスインデックスが低いほど、パスオプションがより有利になります。同じ TE トンネルにおける他のあまり有利ではないパスオプションは、セカンダリ パスオプションと見なされ、（たとえば、パス上の障害が原因で）現在使用されているパスオプションが無効になった場合に使用されることがあります。

（注） フォワーディング ステートは、プライマリ LSP に対してのみ維持されます。

トンネル パス アフィニティの検証

トンネル パスのアフィニティは、トンネル インターフェイスで **tunnel mpls traffic-eng affinity** コマンドを使用して指定することができます。

ヘッドエンドは、指定された SR パスが設定されたアフィニティに準拠していることを検証します。これにより、SR パスの各セグメントのパスは、指定された制約に照らして検証される必要があります。パスの少なくとも 1 つのセグメントが設定されているアフィニティを満たさない場合、そのパスは設定されているアフィニティ制約に対して無効として宣言されます。

SR-TE トラフィックのロード バランシング

SR-TE トンネルは、次のロードバランシング オプションをサポートします。

ポート チャネル TE リンクのロード バランシング

ポート チャネル インターフェイスは SR-TE LSP トラフィックを運びます。このトラフィック負荷は、ポート チャネル メンバー リンクと、SR-TE LSP の先頭または中間のバンドル インターフェイス上でバランスをとります。

単一トンネルでのロード バランシング

同じコストのマルチパス プロトコル（ECMP）を使用している間、特定のプレフィックス SID へのパスが複数のネクストホップを指す場合があります。さらに、SR-TE LSP パスが、ECMP

を持つ1つ以上のプレフィックス SID を通過する場合、SR-TE LSP トラフィック負荷は、SR-TE LSP パスに沿ってヘッドエンドまたは中間点の通過したノードから通過した各プレフィックス SID の ECMP パスでバランスをとります。

複数トンネルでのロード バランシング

スタティック ルートを設定するか、同じ宛先に対して複数の並列トンネルを自動ルート アナウンスをすると、複数の TE トンネルを特定の IP プレフィックスへのルーティングのためのネクストホップ パスとして使用することができます。このような場合、トンネルはトラフィック負荷を均等に共有するか、複数の並列トンネル上でトラフィックをロード バランシングします。トンネル ヘッドエンドでトンネルごとの明示的な設定を使用して不等なロード バランシング（UELB）を許可することも可能です。この場合、トンネルのロードシェアは MPLS-TE からフォワーディング プレーンに渡されます。

トンネルのロードシェア機能は、SR-TE LSP をインスタンス化する TE トンネルで引き続き機能します。

SR-TE トンネルの再最適化

TE トンネルの再最適化は、ヘッドエンドが、現在使用されているパスよりも利用可能な最適なパスがあると判断した場合に発生します。たとえば、SR-TE LSP パスに沿って障害が発生した場合、ヘッドエンドは再最適化をトリガーすることによって、より最適なパスを検出し復帰することができます。

SR-TE LSP をインスタンス化するトンネルは、トンネルを通して運ばれるトラフィックに影響を与えずに再最適化できます。

再最適化は、次の理由で発生します。

- プライマリ SR-TE LSP 明示的パスによって使用される明示的なパス ホップが変更された
- トポロジ パスが切断されているか、または明示的パスで指定されている SID データベースで SID が見つからないため、ヘッドエンドが現在使用されているパスオプションが無効であると判断した
- より有利なパスオプション（より低いインデックス）が利用可能になった

ヘッドエンドは、SR-TE LSP が通過する保護された SR 隣接関係 SID で障害を検出すると、無効化タイマーを開始します。タイマーが期限切れになり、別のパスで再ルーティングできないために失敗したパスをヘッドエンドがまだ使用している場合、トラフィックをブラックホール化しないようにトンネル状態が「ダウン」になります。トンネルがダウンすると、トンネル上のサービスは、異なるパスを使用するために収束します。

次に手動の再最適化の例で出力されるサンプルを示します。この例では、パスオプションが「10」から「20」に変更されます。

```
Router# mpls traffic-eng reoptimize tunnel 1 path-option 20
The targeted path-option is not in lock down mode. Continue? [no]: yes
Router# show mpls traffic-eng tunnels tunnel1
Name: R1_t1                           (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
```

```
    path option 20, (SEGMENT-ROUTING) type explicit IP_PATH (Basis for Setup)
    path option 10, (SEGMENT-ROUTING) type dynamic
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
     Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: explicit path option 20 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  History:
    Tunnel:
      Time since created: 6 days, 19 hours, 9 minutes
      Time since path change: 14 seconds
      Number of LSP IDs (Tun_Instances) used: 1819
    Current LSP: [ID: 1819]
      Uptime: 17 seconds
      Selection: reoptimization
    Prior LSP: [ID: 1818]
      ID: path option unknown
      Removal Trigger: reoptimization completed
  Tun_Instance: 1819
  Segment-Routing Path Info (isis level-1)
    Segment0[Node]: 4.4.4.4, Label: 114
    Segment1[Node]: 5.5.5.5, Label: 115
    Segment2[Node]: 6.6.6.6, Label: 116
```

ロックダウン オプション付き SR-TE

lockdown オプションは、SR-TE がより良いパスに再最適化することを防ぎます。ただし、新しいパスの存在をシグナリングすることは防げません。

```
interface Tunnel1
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng path-option 10 segment-routing lockdown
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
Router# show mpls traffic-eng tunnels tunnel1
Name: csr551_t1                           (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, (LOCKDOWN) type segment-routing (Basis for Setup)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
     Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: enabled  Loadshare: 10 [200000000]
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: segment-routing path option 10 is active
    BandwidthOverride: disabled  LockDown: enabled   Verbatim: disabled
```

```
History:
  Tunnel:
    Time since created: 6 days, 19 hours, 22 minutes
    Time since path change: 1 minutes, 26 seconds
    Number of LSP IDs (Tun_Instances) used: 1822
  Current LSP: [ID: 1822]
    Uptime: 1 minutes, 26 seconds
    Selection: reoptimization
  Prior LSP: [ID: 1821]
    ID: path option unknown
    Removal Trigger: configuration changed
Tun_Instance: 1822
Segment-Routing Path Info (isis  level-1)
  Segment0[Node]: 6.6.6.6, Label: 116
```

SR-TE トンネル保護

SR TE トンネルの保護は、次のいずれかの代替手段で行うことができます。

IP-FRR ローカル修復保護

SR-TE LSP ヘッドエンドまたはミッドポイント ノードでは、IP-FRR はプレフィックス SID または隣接関係 SID ラベルのためのバックアップ保護パスを計算し、プログラムするのに使用されます。

IP-FRR を使用すると、バックアップ修復パスは、リンクまたはノードの障害が発生する前に IGP によって事前に計算されプログラムされます。リンクが失敗すると、TE トポロジからの即時の取り消し（リンク アドバタイズメントの取り消し）がトリガーされます。これにより、ヘッドエンドは、失敗した隣接関係 SID を通過する SR-TE LSP の障害を検出することができます。

保護された隣接関係 SID が失敗した場合、失敗した隣接関係 SID ラベルとそれに関連する転送は、すべての SR TE トンネルのヘッドエンドが障害を検出して対応できるように、指定した時間（5 ～ 15 分）機能し続けます。隣接関係 SID ラベルを使用するトラフィックは、バックアップ修復パスを変更するその後のトポロジ更新がある場合でも、FRR 保護され続けます。この場合、IGP は FRR がアクティブになっている間にバックアップ修復パスを更新し、新しく計算されたバックアップ パス上のトラフィックを再ルーティングします。

保護されたプレフィックス SID のプライマリ パスが失敗すると、PLR はバックアップ パスに経路を再ルーティングします。ヘッドエンドは障害に対してトランスペアレントなままであり、引き続き SR-TE LSP を有効なパスとして使用します。

IP-FRR は、リンク障害に対してのみ隣接関係およびプレフィックス SID を保護します。

トンネル パス保護

パス保護とは、単一の TE トンネルのプライマリ LSP の障害から保護するために、1 つまたは複数のスタンバイ LSP をインスタンス化することです。

パス保護では、同じトンネルのプライマリ パスオプションによってさまざまな障害のセカンダリ パスを事前に計算し、事前プロビジョニングすることで、障害から保護します。この保護は、プライマリ LSP が通過するプレフィックス SID および隣接関係 SID を除外するパスを計

算するか、またはプライマリ SR-TE LSP パスの SRLG を除外するパスを計算することによって実現します。

プライマリ SR-TE LSP に障害が発生した場合、トンネルには少なくとも 1 台のスタンバイ SR-TE LSP が使用されます。複数のセカンダリ パスオプションをスタンバイ SR-TE LSP パスとして使用するように設定できます。

SR TE LSP のパス検証

SR-TE トンネル機能では、ヘッドエンドがトンネルパスの初期検証と、その後のトンネルテールエンドおよび通過セグメントの到達可能性の追跡を実行する必要があります。

SR-TE LSP パスのパス検証は、トポロジの変更または SR SID の更新について MPLS-TE で通知されるたびにトリガーされます。

SR-TE LSP 検証手順は、以下のチェックで構成されています。

トポロジ パスの検証

ヘッドエンドは、TE トポロジに対する接続性について SR-TE LSP のパスを検証します。MPLS-TE ヘッドエンドは、隣接関係 SID に対応するリンクが TE トポロジで接続されているかどうかをチェックします。

新たにインスタンス化された SR-TE LSP の場合、ヘッドエンドが SR-TE パスの任意のリンクで不連続性を検出すると、そのパスは無効であると見なされ、使用されません。有効なパスを持つ他のパスオプションがトンネルにある場合、これらのパスを使用してトンネル LSP をインスタンス化します。

既存のインスタンス化された SR-TE LSP がある TE トンネルでは、ヘッドエンドがリンク上の不連続性を検出すると、ヘッドエンドはそのリンクで障害が発生したと見なします。この場合、IP FRR などのローカル修復保護が有効になります。隣接関係がしばらく失われた後、IGP は保護された隣接関係ラベルと関連付けられた転送を維持し続けます。これにより、同じ障害の影響を受けない別のパスにトンネルを再ルーティングするのに十分な時間が、ヘッドエンドで可能になります。ヘッドエンドは、リンク障害を検出した後、有効なパスを持つ他の使用可能パスオプションにトンネルの再ルーティングを試みるために、トンネル無効化タイマーを開始します。

TE トンネルが、障害の影響を受けない検証済みの他のパスオプションを使用して設定されている場合、ヘッドエンドは、これらのパスオプションの 1 つを使用して、影響を受けないパスを使用してトンネルの新しいプライマリ LSP をインスタンス化することによって、トンネルを再ルーティングします。

同じトンネルの下に他の有効なパスオプションが存在しない場合、または TE トンネルが障害の影響を受けるパスオプションを 1 つだけで設定されている場合、ヘッドエンドは無効タイマーを開始し、その後トンネルの状態を「ダウン」にします。このアクションは、影響を受ける SR-TE LSP 上を流れるトラフィックをブラックホール化することを回避し、トンネルを通過するサービスがヘッドエンドで利用可能な異なるパスを経由して再ルーティングすることを可能にします。無効化ドロップ構成は、トンネルを「アップ」のままにしますが、無効化タイマーが満了したときにトラフィックをドロップします。

エリア内 SR-TE LSP では、ヘッドエンドは LSP パス上で完全な可視性を持ち、最終的な LSP 宛先へのパスを検証します。ただし、エリア間 LSP の場合、ヘッドエンドには LSP パスに対する部分的な可視性があります（最初の ABR までのみ）。この場合、ヘッドエンドは、入力から最初の ABR へのパスのみを検証できます。最初の ABR ノードを超える LSP に沿った障害は、ヘッドエンドからは見えず、LSP を介した BFD など、そのような障害を検出するその他のメカニズムが想定されます。

SR SID の検証

SR-TE LSP の SID ホップは TE トンネルの SR-TE LSP を介して運ばれる発信パケットに課される発信 MPLS ラベル スタックを決定するために使用されます。グローバルおよびローカルの隣接関係 SID のデータベースは、IGP から受信した情報から取り込まれ、MPLS-TE で維持されます。MPLS TE データベースで利用できない SID を使用すると、明示的パスを使用するパスオプションが無効になります。この場合、パスオプションは、SR TE LSP のインスタンス化には使用されません。また、MPLS の SID データベースで SID を取り消す、追加する、または変更すると、MPLS-TE ヘッドエンドは、SR パスオプション（使用中またはセカンダリ）を持つすべてのトンネルを確認し、適切な処理を呼び出します。

LSP 出力インターフェイス

SR-TE LSP が最初のパス ホップの隣接関係の SID を使用するとき、TE は隣接関係 SID および SR-TE LSP が出力するノードに関連付けられているインターフェイス状態および IGP 隣接関係状態を監視します。インターフェイスまたは隣接関係がダウンした場合、TE は SR-TE LSP パスで障害が発生したと仮定し、前のセクションで説明したのと同じリアクティブ アクションを実行できます。

（注） SR-TE LSP が最初のホップのプレフィックス SID を使用するとき、TE はトンネルが出力するインターフェイスを直接推測できません。TE は、プレフィックスの IP 到達可能性情報に基づいて、最初のホップへの接続が維持されるかどうかを判断します。

IP 到達可能性の検証

MPLS-TE では、SR パスを有効と宣言する前に、プレフィックス SID に対応するノードが IP 到達可能であることを検証します。MPLS-TE は、SR-TE LSP パスの隣接関係またはプレフィックス SID に対応する IP プレフィックスのパス変更を検出します。リンクまたはノードの障害が原因で、特定の SID をアナウンスするノードが IP の到達可能性を失う場合、MPLS-TE はパス変更（パスなし）の通知を受けます。MPLS-TE は、現在の SR-TE LSP パスを無効にすることによって反応し、もしあれば有効なパスを持つ他のパスオプションを使用して新しい SR-TE LSP をインスタンス化する場合があります。

（注） IP-FRR は（SR-TE LSP パスに沿ったプレフィックス SID の失敗など）SR-TE LSP が通過しているノードの障害に対する保護を提供しないため、ヘッドエンドは、トンネル状態を「ダウン」に設定することによってプレフィックス SID ノードの IP ルートの到達可能性の損失にすぐに反応し、影響を受けるトンネルに対して有効なパスを持つパスオプションが他にない場合は、トンネル転送エントリを削除します。

トンネル パス リソース回避の検証

SR-TE トンネルパケットの通過から除外されたことを検証するアドレスのセットを指定できます。これを実現するために、ヘッドエンドはセグメントごとの検証チェックを実行し、指定されたノード、プレフィックス、またはリンク アドレスが SR パスのトンネルから実際に除外されていることを検証します。以下のコマンドを使用して、トンネル リソース回避チェックをパスごとに有効にすることができます。除外されるアドレスのリストが定義され、リストの名前がパスオプションで参照されます。

```
interface tunnel100
 tunnel mpls traffic-eng path-option 1 explicit name EXCLUDE segment-routing
ip explicit-path name EXCLUDE enable
 exclude-address 192.168.0.2
 exclude-address 192.168.0.4
 exclude-address 192.168.0.3
!
```

SR-TE LSP の明示的ヌル

MPLS-TE トンネルのヘッドエンドは、スタックの最下部に明示的ヌルを課しません。penultimate hop popping（PHP）が SR プレフィックス SID に対して有効になっている場合、または隣接関係 SID が SR-TE LSP の最後のホップである場合、パケットはトランスポート ラベルなしでテールエンドに到着する可能性があります。ただし、場合によっては、パケットが明示的ヌル ラベルでテールエンドに到着することが望ましいため、このような場合、ヘッドエンドはラベル スタックの最上部に明示的ヌル ラベルを課すことになります。

Verbatim パス サポート

通常、MPLS TE LSP を使用する場合は、ネットワーク内のすべてのノードで TE の IGP 拡張がサポートされていて、TE が認識されるように設定されている必要があります。ただし、TE の IGP 拡張をサポートしないが、TE の RSVP 拡張はサポートするノードを通過する TE LSP を構築する機能を必要とするネットワーク管理者もいます。Verbatim LSP は、ネットワーク内のすべてまたは一部の中間ノードで TE の IGP 拡張がサポートされていない場合に役立ちます。

この機能をイネーブルにすると、IP 明示パスの TE トポロジ データベースに対するチェックは行われません。TE トポロジ データベースの検証が行われないため、IP 明示パス情報を持つ Path メッセージは、IP ルーティング用の Shortest Path First（SPF）アルゴリズムを使用してルーティングされます。

OSPF のセグメント ルーティング トラフィック エンジニアリングの設定方法

次の手順を実行して、OSPF でのセグメント ルーティング トラフィック エンジニアリングを設定します。

OSPF のセグメント ルーティング トラフィック エンジニアリングの有効化

OSPF セグメント ルーティング トラフィック エンジニアリングは、mpls トラフィック エンジニアリングとともにセグメントルーティングが有効になっている場合に有効になります。エリア内で SR と MPLS TE を有効にした場合、そのエリア内で SR-TE のサポートがオンになります。

```
router ospf 10
 router-id 10.10.10.2
 segment-routing mpls
  mpls traffic-eng area 0
```

TE トンネルのパス オプションの設定

キーワード **segment-routing** は、指定されたパスが SR パスとしてプログラムされることを示します。

```
Device(config)# interface tunnel 100
Device(config-if)# tunnel mpls traffic-eng path-option 1 explicit name foo segment-routing
Device(config-if)# tunnel mpls traffic-eng path-option 2 dynamic segment-routing
Device(config-if)# tunnel mpls traffic-eng path-option 3 segment-routing
```

（注） IP アンナンバード インターフェイスでは、動的パスはサポートされません。

稼働中の SR トンネルのパスオプション タイプが SR から非 SR（たとえば **dynamic**）に変更されると、トンネルの既存の転送エントリが削除されます。

セグメントルーティングは、既存のセカンダリまたは使用中のパスオプションで有効または無効にすることができます。トンネルでシグナリングされた RSVP-TE の明示的パスオプションが使用され、そのトンネルでセグメントルーティングが有効になっている場合、RSVP-TE LSP は切断され、SR-TE LSP が同じパスオプションを使用してインスタンス化されます。逆に、プライマリ LSP によって使用されているパスオプションでセグメントルーティングが無効になっている場合、トンネルは断続的にダウンし、新しい RSVP-TE LSP は同じ明示的パスを使用してシグナリングされます。

セグメントルーティング パスオプションがセカンダリ パスオプションで有効になっている（すなわち、トンネルのプライマリ LSP によって使用されていない）場合、新しく指定された

SR-TE LSP パスオプションが有効で、トンネルのプライマリ LSP に使用するのがより有利であるかどうかを評価するためにトンネルがチェックされます。

SR 明示パス ホップの設定

次の SR-TE 明示的パス ホップがサポートされています。

- IP アドレス
- MPLS ラベル
- IP アドレスと MPLS ラベルの混在

エリア内 LSP では、明示的パスを IP アドレスのリストとして指定できます。

```
Device(config)# ip explicit-path name foo
Device(config-ip-expl-path)# index 10 next-address 1.1.1.1 node address
Device(config-ip-expl-path)# index 20 next-address 12.12.12.2 link address
```

（注） IP アンナンバード インターフェイスを使用する場合、ネクスト ホップ アドレスを明示的パスのインデックスとして指定することはできません。これは、ノードアドレスまたはラベルである必要があります。

明示的パスは、セグメントルーティング SID として指定することもできます。

```
Device(config)# ip explicit-path name foo
Device(config-ip-expl-path)# index 10 next-label 20
```

（注） IP アドレスは、MIXED_PATH でラベルを使用した後に使用することはできません。

トンネル パス アフィニティの検証の設定

トンネル パスのアフィニティは、トンネル インターフェイスで **tunnel mpls traffic-eng affinity** コマンドを使用して指定することができます。

ヘッドエンドは、指定された SR パスが設定されたアフィニティに準拠していることを検証します。これにより、SR パスの各セグメントのパスは、指定された制約に照らして検証される必要があります。パスの少なくとも 1 つのセグメントが設定されているアフィニティを満たさない場合、そのパスは設定されているアフィニティ制約に対して無効として宣言されます。

```
interface Tunnel1
 no ip address
 tunnel mode mpls traffic-eng
 tunnel destination 5.5.5.5
 tunnel mpls traffic-eng priority 5 5
 tunnel mpls traffic-eng bandwidth 100
 tunnel mpls traffic-eng affinity 0x1 mask 0xFFFF
        tunnel mpls traffic-eng path-option 10 dynamic segment-routing
```

```
Router# show tunnel ??
Name: R1_t1                             (Tunnel1) Destination: 5.5.5.5
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, (SEGMENT-ROUTING) type dynamic (Basis for Setup, path weight 20)
  Config Parameters:
    Bandwidth: 100      kbps (Global)  Priority: 5  5   Affinity: 0x1/0xFFFF
    Metric Type: TE (default)
    Path Selection:
     Protection: any (default)
    Path-selection Tiebreaker:
      Global: not set   Tunnel Specific: not set   Effective: min-fill (default)
    Hop Limit: disabled
    Cost Limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear
    AutoRoute: disabled LockDown: disabled Loadshare: 100 [0] bw-based
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: dynamic path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  Node Hop Count: 2
  History:
    Tunnel:
      Time since created: 10 minutes, 54 seconds
      Time since path change: 34 seconds
      Number of LSP IDs (Tun_Instances) used: 55
    Current LSP: [ID: 55]
      Uptime: 34 seconds
    Prior LSP: [ID: 49]
      ID: path option unknown
      Removal Trigger: tunnel shutdown
  Tun_Instance: 55
  Segment-Routing Path Info (isis  level-1)
    Segment0[Link]: 192.168.2.1 - 192.168.2.2, Label: 46
    Segment1[Link]: 192.168.4.2 - 192.168.4.1, Label: 49
```

インターフェイスのアフィニティの設定

インターフェイスでアフィニティを設定するには、次の手順を実行します。

```
interface GigabitEthernet2
 ip address 192.168.2.1 255.255.255.0
 ip router isis 1
 negotiation auto
 mpls traffic-eng tunnels
 mpls traffic-eng attribute-flags 0x1
 isis network point-to-point
 ip rsvp bandwidth
```

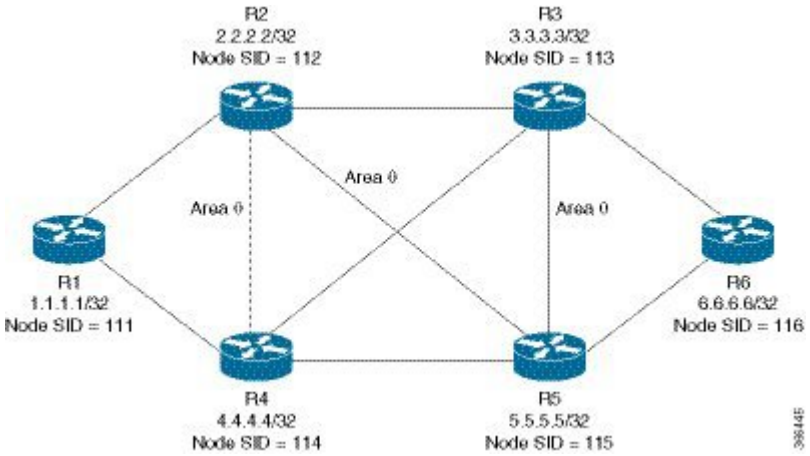
OSPF のセグメント ルーティング トラフィック エンジニアリングの設定

OSPF で SR-TE を設定するには、次のエリア間およびエリア内の使用例を考慮してください。

エリア内トンネルの設定

エリア内トンネルを設定するには、次のトポロジを検討してください。

図 *12 :* エリア内トンネル



すべてのルータは、同じエリアである、エリア 0 内で設定されています。

ヘッドエンド ルータ R1 の構成

```
router ospf 10
fast-reroute per-prefix enable prefix-priority low
fast-reroute per-prefix ti-lfa
segment-routing mpls
mpls traffic-eng router-id Loopback1
mpls traffic-eng area 0

interface GigabitEthernet2   //interface connecting to the router 2
ip address 100.101.1.1 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface GigabitEthernet4  //interface connecting to the router 4
ip address 100.101.1.1 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface loopback1
ip address 1.1.1.1/32
ip ospf 10 area 0
```

テールエンド ルータ R6 の構成

```
router ospf 10
fast-reroute per-prefix enable prefix-priority low
fast-reroute per-prefix ti-lfa
segment-routing mpls
mpls traffic-eng area 0
mpls traffic-eng router-id Loopback1
interface GigabitEthernet2   //interface connecting to the router 3
ip address 100.101.2.1 255.255.255.0
```

```
ip ospf 10 area 0
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface GigabitEthernet4  //interface connecting to the router 5
ip address 100.101.2.1 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface loopback1
ip address 6.6.6.6/32
ip ospf 10 area 0
```

明示パス SR-TE トンネル 1

トンネル 1 を IP アドレスのみに基づいて考慮します。

```
ip explicit-path name IP_PATH1
 next-address 2.2.2.2
 next-address 3.3.3.3
 next-address 6.6.6.6
!
interface Tunnel1
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng path-option 10 explicit name IP_PATH1 segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
end
```

明示パス SR-TE トンネル 2

トンネル 2 をノードの SID に基づいて考慮します

```
ip explicit-path name IA_PATH
 next-label 114
 next-label 115
 next-label 116
!
interface Tunnel2
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng bandwidth 10000 class-type 1
 tunnel mpls traffic-eng path-option 10 explicit name NODE_PATH segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
end
```

明示パス SR-TE トンネル 3

トンネル 3 は IP アドレスとラベルの組み合わせに基づいていることを考慮します

```
ip explicit-path name MIXED_PATH enable
 next-address 2.2.2.2
 next-address 3.3.3.3
 next-label 115
 next-label 116
!
interface Tunnel3
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng path-option 10 explicit name MIXED_PATH segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
```

（注） パスが混在している場合、パスでノード SID を使用した後に IP ネクストホップを使用することはできません。次のパスは有効ではありません。

```
ip explicit-path name MIXED_PATH enable
next-label 115
next-label 116
next-address 2.2.2.2
```

動的パス SR-TE トンネル 4

トンネル 4is は隣接関係 SID に基づいていることを考慮します

```
interface Tunnel4
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng bandwidth 10000 class-type 1
 tunnel mpls traffic-eng path-option 10 dynamic segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
end
```

動的パス SR-TE トンネル 5

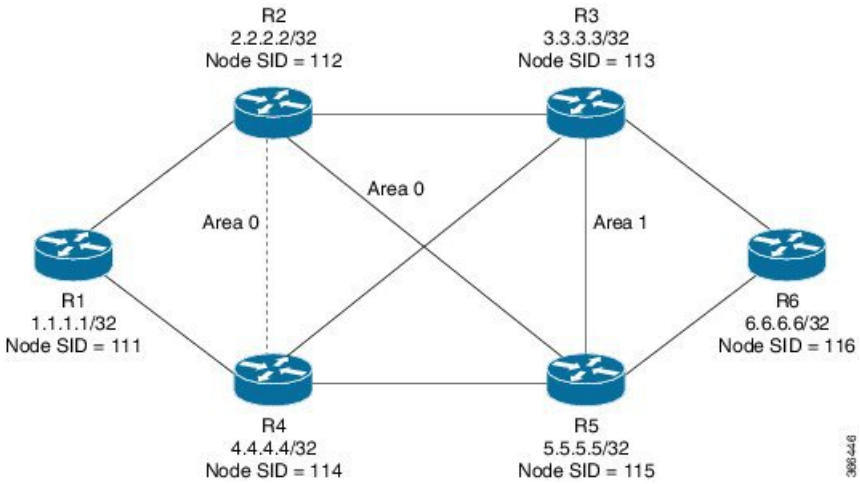
トンネル 5 はノード SID に基づいていることを考慮します

```
 interface Tunnel5
 ip unnumbered Loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng path-option 10 segment-routing
 tunnel mpls traffic-eng path-selection metric igp
 tunnel mpls traffic-eng load-share 10
```

エリア間トンネルの設定

エリア間トンネルを設定するには、次のトポロジを検討してください。

図 *13 :* エリア間トンネル



エリア 1 内で設定されている R6 を除き、すべてのルータは同じエリアであるエリア 0 内で設定されています。

ヘッドエンド ルータ R1 の構成

```
router ospf 10
fast-reroute per-prefix enable prefix-priority low
fast-reroute per-prefix ti-lfa
segment-routing mpls
mpls traffic-eng router-id Loopback1
mpls traffic-eng area 0

interface GigabitEthernet2   //interface connecting to the router 2
ip address 100.101.1.1 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface GigabitEthernet4  //interface connecting to the router 4
ip address 100.101.1.1 255.255.255.0
ip ospf 10 area 0
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface loopback1
ip address 1.1.1.1/32
ip ospf 10 area 0
```

テールエンド ルータ R6 の構成

```
router ospf 10
fast-reroute per-prefix enable prefix-priority low
fast-reroute per-prefix ti-lfa
segment-routing mpls
```

```
mpls traffic-eng area 1
mpls traffic-eng router-id Loopback1
interface GigabitEthernet2   //interface connecting to the router 3
ip address 100.101.2.1 255.255.255.0
ip ospf 10 area 1
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface GigabitEthernet4  //interface connecting to the router 5
ip address 100.101.2.1 255.255.255.0
ip ospf 10 area 1
ip ospf network point-to-point
negotiation auto
mpls traffic-eng tunnels

interface loopback1
ip address 6.6.6.6/32
ip ospf 10 area 1
```

エリア間トンネルの設定に関する制約事項

エリア間トンネルの設定に関する制約事項は次のとおりです。

- ノードおよび隣接関係 SID を持つ動的オプションはサポートされていません。
- ラベルのみおよび/または IP アドレスとラベルを含む明示的パスを使用して、エリア間トンネルを設定できます。

（注） IPアドレスは、エリア境界ルータ（ABR）までのみ使用でき、その後はラベルのみを指定する必要があります。

明示パス SR-TE トンネル 1

トンネル 2 はノード SID に基づいていることを考慮します。

```
ip explicit-path name IA_PATH
next-label 114
next-label 115
next-label 116
!
interface Tunnel2
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 6.6.6.6
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 6 6
tunnel mpls traffic-eng bandwidth 10000 class-type 1
tunnel mpls traffic-eng path-option 10 explicit name NODE_PATH segment-routing
tunnel mpls traffic-eng path-selection metric igp
tunnel mpls traffic-eng load-share 10
end
```

明示パス SR-TE トンネル 2

トンネル 3 は IP アドレスとラベルの組み合わせに基づいていることを考慮します。

```
ip explicit-path name MIXED_PATH enable
next-address 2.2.2.2
next-address 3.3.3.3
next-label 115
next-label 116
!

interface Tunnel3
ip unnumbered Loopback1
tunnel mode mpls traffic-eng
tunnel destination 6.6.6.6
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 6 6
tunnel mpls traffic-eng path-option 10 explicit name MIXED_PATH segment-routing
tunnel mpls traffic-eng path-selection metric igp
tunnel mpls traffic-eng load-share 10
```

SR-TE トンネルの構成の確認

show mpls traffic-eng tunnels *tunnel-number* コマンドを使用して、SR-TE トンネルの構成を確認します。

トンネル 1 の確認

```
Name: R1_t1                             (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, (SEGMENT-ROUTING) type explicit IP_PATH (Basis for Setup)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
     Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: explicit path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  History:
    Tunnel:
      Time since created: 6 days, 19 hours
      Time since path change: 2 seconds
      Number of LSP IDs (Tun_Instances) used: 1814
    Current LSP: [ID: 1814]
      Uptime: 2 seconds
      Selection: reoptimization
    Prior LSP: [ID: 1813]
      ID: path option unknown
      Removal Trigger: configuration changed
  Tun_Instance: 1814
  Segment-Routing Path Info (ospf 10  area 0)
    Segment0[Node]: 4.4.4.4, Label: 114
    Segment1[Node]: 5.5.5.5, Label: 115
    Segment2[Node]: 6.6.6.6, Label: 116
```

-

トンネル 2 の確認

```
Name: R1_t2                             (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, (SEGMENT-ROUTING) type explicit IA_PATH (Basis for Setup)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
     Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: explicit path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  History:
    Tunnel:
      Time since created: 6 days, 19 hours, 1 minutes
      Time since path change: 1 seconds
      Number of LSP IDs (Tun_Instances) used: 1815
    Current LSP: [ID: 1815]
      Uptime: 1 seconds
    Prior LSP: [ID: 1814]
      ID: path option unknown
      Removal Trigger: configuration changed
  Tun_Instance: 1815
  Segment-Routing Path Info (ospf 10  area 0)
    Segment0[ - ]: Label: 114
    Segment1[ - ]: Label: 115
    Segment2[ - ]: Label: 116
```

トンネル 3 の確認

```
Name: R1_t3                             (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, (SEGMENT-ROUTING) type explicit MIXED_PATH (Basis for Setup)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
     Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: explicit path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  History:
    Tunnel:
      Time since created: 6 days, 19 hours, 2 minutes
      Time since path change: 2 seconds
```

```
    Number of LSP IDs (Tun_Instances) used: 1816
  Current LSP: [ID: 1816]
    Uptime: 2 seconds
    Selection: reoptimization
  Prior LSP: [ID: 1815]
    ID: path option unknown
    Removal Trigger: configuration changed
Tun_Instance: 1816
Segment-Routing Path Info (ospf 10  area 0)
  Segment0[Node]: 2.2.2.2, Label: 112
  Segment1[Node]: 3.3.3.3, Label: 113
  Segment2[ - ]: Label: 115
  Segment3[ - ]: Label: 116
```

トンネル 4 の確認

```
Name: R1_t4                             (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, (SEGMENT-ROUTING) type dynamic (Basis for Setup, path weight 30)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
     Protection: any (default)
    Path-invalidation timeout: 45000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: dynamic path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  History:
    Tunnel:
      Time since created: 6 days, 19 hours
      Time since path change: 2 seconds
      Number of LSP IDs (Tun_Instances) used: 1813
    Current LSP: [ID: 1813]
      Uptime: 2 seconds
    Prior LSP: [ID: 1806]
      ID: path option unknown
      Removal Trigger: configuration changed
  Tun_Instance: 1813
  Segment-Routing Path Info (ospf 10  area 0)
    Segment0[Link]: 192.168.2.1 - 192.168.2.2, Label: 17
    Segment1[Link]: 192.168.4.2 - 192.168.4.1, Label: 25
    Segment2[Link]: 192.168.8.1 - 192.168.8.2, Label: 300
```

トンネル 5 の確認

```
Name: R1_t5                             (Tunnel1) Destination: 6.6.6.6
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, type segment-routing (Basis for Setup)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 6  6   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
```

```
   Protection: any (default)
  Path-invalidation timeout: 45000 msec (default), Action: Tear
  AutoRoute: enabled  LockDown: disabled Loadshare: 10 [200000000]
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: segment-routing path option 10 is active
  BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
History:
  Tunnel:
    Time since created: 6 days, 19 hours, 4 minutes
    Time since path change: 14 seconds
    Number of LSP IDs (Tun_Instances) used: 1817
  Current LSP: [ID: 1817]
    Uptime: 14 seconds
    Selection: reoptimization
  Prior LSP: [ID: 1816]
    ID: path option unknown
    Removal Trigger: configuration changed
Tun_Instance: 1817
Segment-Routing Path Info (ospf 10  area 0)
  Segment0[Node]: 6.6.6.6, Label: 116
```

OSPF のセグメント ルーティング トラフィック エンジニアリングの追加情報

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』

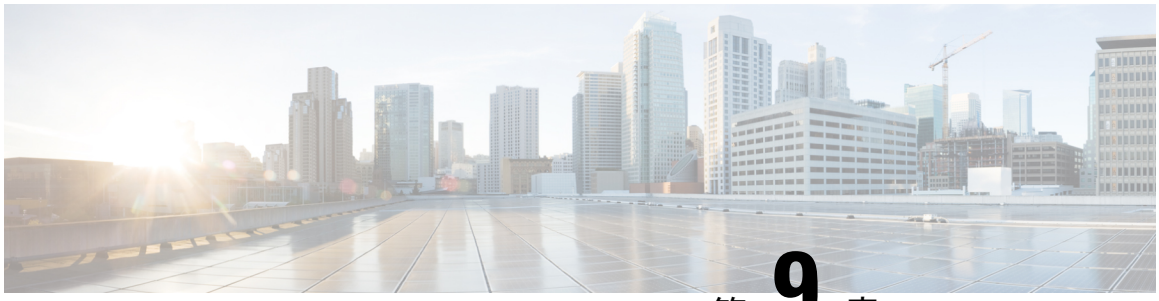
OSPF のセグメント ルーティング トラフィック エンジニアリングの機能情報

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 *7: OSPF* のセグメント ルーティング トラフィック エンジニアリングの機能情報

機能名	リリース	機能情報
OSPF のセグメント ルーティング トラフィック エンジニアリング	Cisco IOS XE リリース 3.17S Cisco IOS XE Fuji 16.7.1	トラフィック エンジニアリング（TE）トンネルは、トンネルの入力とトンネルの宛先との間でインスタンス化された TE LSP のコンテナです。TE トンネルは、同じトンネルに関連付けられた 1 つ以上の SR-TE LSP をインスタンス化できます。 次のコマンドが追加または修正されました。 **show mpls traffic-eng tunnels**、**tunnel mpls traffic-eng path-option 10 dynamic segment-routing**、**tunnel mpls traffic-eng path-option 10 segment-routing**、**tunnel mpls traffic-eng path-option 10 explicit name MIXED_PATH segment-routingtunnel mpls traffic-eng path-option 10 explicit name IP_PATH1 segment-routingtunnel mpls traffic-eng path-option 10 explicit name NODE_PATH segment-routing**。 Cisco IOS XE Fuji 16.7.1 では、この機能は Cisco 4000 シリーズ サービス統合型ルータでサポートされています。



第 9 章

BGP ダイナミック セグメント ルーティング トラフィック エンジニアリング

ボーダー ゲートウェイ プロトコル（BGP）はデータセンター（DC）ネットワークのルーティングプロトコルとして一般的な選択となっています。BGPによって開始されるセグメント ルーティング トラフィック エンジニアリング（SR-TE）パスを設定する機能により、DC ネットワークの動作が簡素化されます。

セグメントルーティングの制約事項：トラフィックエンジニアリング ダイナミック BGP

- エニーキャストの場合、BGP-TE を動作させるために SID サポートで前に付加（Prepend）機能を設定する必要があります。
- BGP ダイナミック SR-TE では、SR-TE で障害が発生した場合、フォワーディングが中断されます。

セグメントルーティングに関する情報：トラフィックエンジニアリング ダイナミック BGP

BGP ダイナミック SR-TE では、定義済みの基準とポリシーが満たされ、それが手動で有効になっている SR-TE と BGP ダイナミック SR-TE 間の主な違いである場合、ラベル スイッチド パス（LSP）がオンデマンドで有効になります。たとえば、低遅延パス、最小コストパスなどのポリシーは、BGPによって伝送され、特定の顧客プレフィックスで一致します。自動検出とシグナリングのためにBGPを使用するL3VPNまたは仮想プライベートLANサービス（VPLS）に使用される SR-TE トンネルは、BGP-TE ダイナミックと呼ばれます。

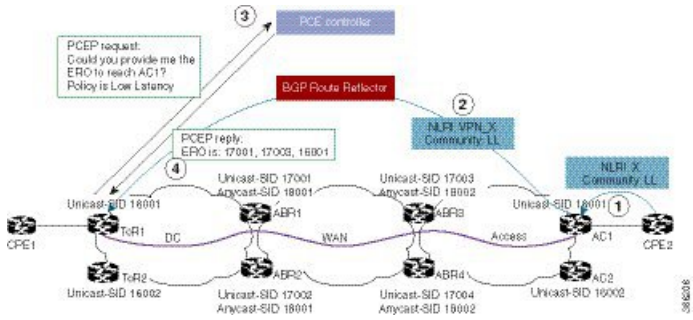
BGP SR-TE ダイナミックは、オンデマンドの自動トンネルが単一の IGP ドメインに存在することを前提としています。この場合、パスの計算は IGP を介して行われます。BGP からの要求に基づいて作成された SR-TE 自動トンネルはダイナミック SR-TE トンネルです。つまり、トンネルパス情報またはラベル スタックが、BGP ネクストホップおよびTE属性設定に基づいて計算されます。BGP ダイナミック SR-TEは、オンデマンドLSP（自動トンネル）をトリガーする機能を備えています。機能は次のとおりです。

- ルート マップ設定を介してコミュニティ（コミュニティ リスト）を使用して、顧客プレフィックス（IPv4 または L3VPN VRF）にタグを付けます。
- 各コミュニティを TE の属性セットまたはプロファイルに関連付けます。

SR-TE プロファイルは、遅延、分離パスなどの特定の SR-TE パラメータを定義するために、属性設定でローカルに設定されます。BGP 顧客プレフィックスが SR-TE プロファイルにマップされると、プレフィックスと関連付けられている指定された各 BGP ネクストホップおよび属性セットのペアに対して、属性セットで定義されたパラメータを使用してトンネルが動的に作成されます（自動トンネルまたはオン デマンド ラベル スイッチド パス（LSP））。バインディング SID は、各 SR-TE 自動トンネルに関連付けられていて、BGP に渡されます。バインディング SID またはバインディング ラベルは、ルーティング情報ベース（RIB）および転送情報ベース（FIB）にインストールされます。FIB は、オン デマンド SR-TE 自動トンネルを経由して転送するバインディング SID またはバインディング ラベルによって BGP パスを解決します。バインディング SID は、SR-TE LSP 上の顧客トラフィックを制御するためにも使用されます。

BGP はこの場合は SR-TE ポリシーのみを伝送し、パスの計算は単一の IGP ドメインで IGP を介して行われることに注意する必要があります。単一のIGPドメインでは、ヘッドエンドノードはエンド ツー エンド パスとトポロジ エンジニアリング データベース（トラフィック エンジニアリング データベースまたは TED）の完全な可視性を持っています。また、BGP 動的 SR-TE ですべてのノードが単一の AS と単一の IGP ドメイン内に存在することを前提とします。

図 *14 : BGP-TE* ダイナミック ワークフロー



上の図は、複数のルーティング ドメインを使用した BGP-TE ダイナミック ワークフローの使用例を示しています。

1. 顧客宅内機器 2（CPE）は、プレフィックス X に対して BGP アップデートを送信し、LL コミュニティ（100:333 など）を追加します。
2. AC1 は LL コミュニティを持つプレフィックス X のための VPN ルートをアナウンスします。
3. VPN ルート マッチング コミュニティ LL の BGP アップデートを受信した後、ToR1 は低遅延の TE ポリシーを使用して AC1 に向かう LSP パスに対して PCE コントローラに要求を送信します。
4. パス計算要素（PCE）コントローラは、ラベル スタックで応答します（たとえば、17003、1600）。
5. ToR1 は SR-TE 自動トンネルを作成し、この VPN の VRF のプレフィックス X のためのルートをインストールします。

TE ラベル スイッチド パス属性セット

TE-LSP 属性セットは、LSP のプロパティを設定するために使用されます。これは、オートトンネルを作成するために使用される、帯域幅、アフィニティの包含と除外、リンク/ノード/SRLG の包含と除外、メトリック、パスの分離度、グループなどの TE プロファイルまたはポリシーについて記述します。

TE ラベル スイッチド パス属性セットの設定方法

TE ラベル スイッチド パス属性セットの設定

コマンド **mpls traffic-eng lsp attribute** <*name*> を使用して、TE-LSP 属性を設定することができます。次のオプションを使用できます。

```
Mpls traffic-eng lsp attribute name
```

```
   affinity      Specify attribute flags for links comprising LSP
   lockdown      Lockdown the LSP--disable reoptimization
   priority      Specify LSP priority
```

TE-LSP 属性コマンドは、拡張して 2 つのオプション **pce** と **path-selection** の設定をサポートすることができます。次のように設定できます。

```
mpls traffic-eng lsp attribute name <test>
    path-selection
       metric <te/igp>
       invalidation <time-out> <drop/tear>
       segment-routing adjacency <protected/unprotected>
```

- pce オプションが TE 属性で設定されている場合、ダイナミック パスは pce によって計算されます。それ以外の場合、パスは TE PCALC（パス計算）エンティティによってローカルに計算されます。後者の場合、IGP を設定する必要があり、BGP ネクストホップが IGP によってアドバタイズされ、IGP ルートを経由してローカル ノードから到達可能である必要があります。
- オプションの path-selection メトリックは、パスの計算が TE のメトリックまたは IGP メトリックに基づいているかどうかを示します。このオプションが設定されていない場合は、mpls traffic-eng path-selection メトリックで設定されたグローバル値が使われます。
- オプションの **path-selection invalidation** は、LSP がネットワークからのソフト障害にどのように反応するかの動作を設定します。LSP パスにリンクまたはノード障害に対する IGP からの保護パスがある場合、リンクまたはノードへの障害はソフト障害と見なされます。
- オプション **path-selection segment-routing adjacency** は、LSP ラベル スタックを計算する際に、IGP 保護の有無にかかわらず隣接関係 SID を選択するかどうかを示します。
- オプション **pce disjoint-path** は、トンネル LSP が disjoint-path グループのメンバーであることを示します。同じ disjoint-path グループ内の LSP は、そのパス内のリンク、ノード、または SRLG などの同じリソースを通過しません。これは、分離パスを持つ 2 つ以上のトンネル LSP を作成するために使用されます。

BGP-TE ダイナミックの場合、TE 属性名は次のように BGP ルートマップ セット拡張に関連付けられます。

```
route-map <name>
    match community <name>
         set attribute-set  <name>
```

BGP は文字列 **attribute-set** <*name*> をその BGP ネクストホップとともに使用して、SR-TE 自動トンネルを要求します。

BGP ダイナミック セグメント ルーティング トラフィック エンジニアリングの追加情報

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 Command List, All Releases』

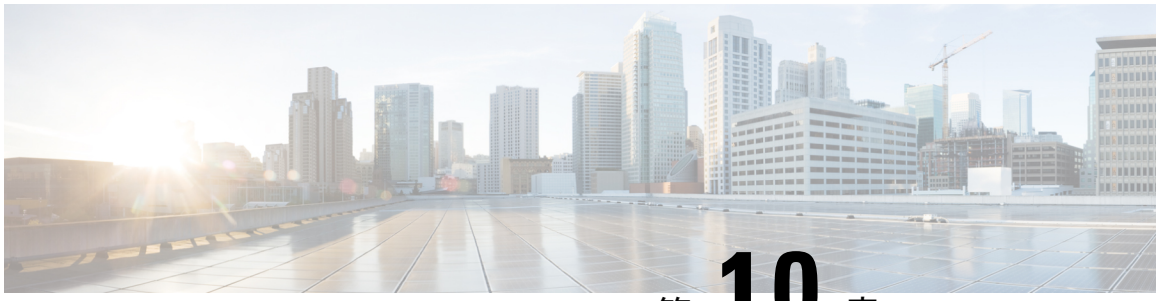
BGP ダイナミック セグメント ルーティング トラフィック エンジニアリングの機能情報

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 : BGP* ダイナミック セグメント ルーティング トラフィック エンジニアリングの機能情報

機能名	リリース	機能情報
BGP ダイナミック セグメント ルーティング トラフィック エンジニアリング	Cisco IOS XE Everest 16.5.1b	BGP ダイナミック SR-TE では、定義済みの基準とポリシーが満たされると、ラベル スイッチド パス（LSP）がオン デマンドで有効になります。 次のコマンドが導入または変更されました。 **mpls traffic-eng lsp attribute** *name*



第 10 章

L3/L3VPN 用のセグメント ルーティング オン デマンド ネクスト ホップ

ドメイン全体にルーティング情報を再配布すると、マルチドメイン サービス（L2VPN と L3VPN）のプロビジョニングにそれ自体の複雑性と拡張性の問題が発生します。オン デマンド ネクスト ホップ（ODN）は、再配布を行わずに制約やポリシーなど、PCE コントローラへのエンドツーエンド LSP の計算の委任をトリガーします。次に、サービスが Forwarding Information Base（FIB）へ移行する間に応答されたマルチドメイン LSP をインストールします。

L3/L3VPN のセグメント ルーティング オン デマンド ネクスト ホップの制約事項

- オン デマンド ネクスト ホップ（ODN）エニーキャスト SID はサポートされていません。
- IPv6 の ODN はサポートされていません。
- SR ODN トンネルは、BGP ノンストップ ルーティング（NSR）ではサポートされていません。BGP ノンストップ フォワーディング（NSF）でのみサポートされています。

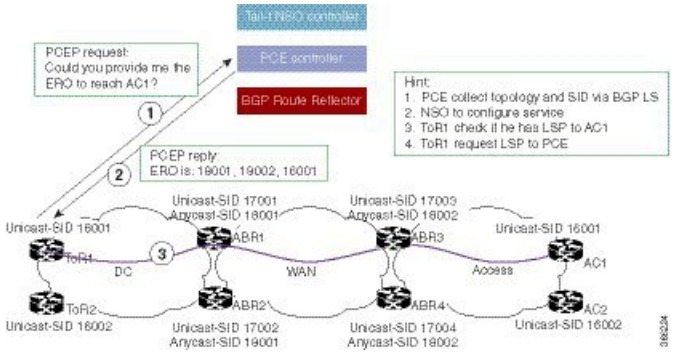
  BGP NSF を有効にするには、次のコマンドを使用します。

```
bgp grace-full restart
neighbor 10.0.0.2 ha-mode graceful-restart
```

L3/L3VPN のセグメント ルーティング オン デマンド ネクスト ホップに関する情報

オンデマンド ネクスト ホップは、BGP ダイナミック SR-TE 機能を活用し、要件に基づいてエンドツーエンドパスを検索してダウンロードするためのパス計算（PCE）機能を追加します。ODN は定義された BGP ポリシーに基づいて SR-TE 自動トンネルをトリガーします。下の図に示すように、ToR1 と AC1 間のエンド ツー エンドパスは、低遅延あるいは VRF（L3VPN）または IPv4 サービスの他の基準に基づいて両端から確立できます。ODN のワークフローは次のようにまとめられます。

図 *15 : ODN* 操作



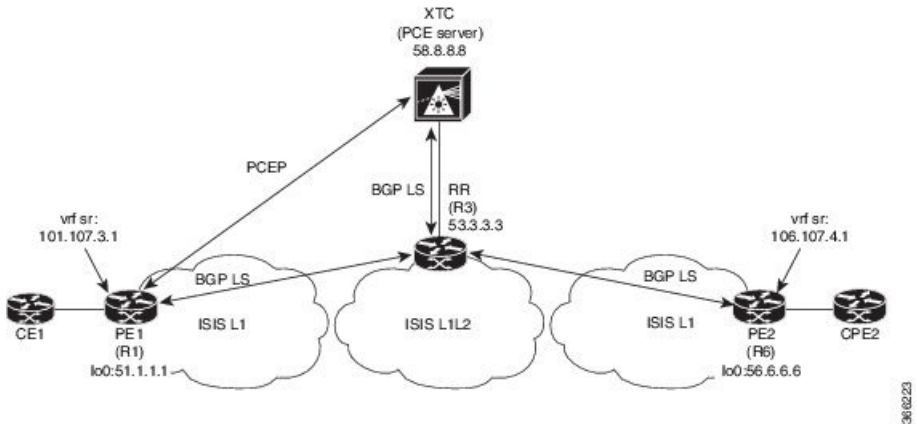
1. PCE コントローラは、BGP リンク ステート（BGP-LS）を介してトポロジと SID の情報を収集します。BGP-LS の詳細については、「BGP Link-State」を参照してください。
2. NSO コントローラが有効になっている場合、L3VPN VRF または IPv4 プレフィックスが設定され、要求が ToR1 および AC1 に送信されます。
3. ToR1 と AC1 は、お互いに対する LSP が存在するかどうかをチェックします。ない場合は、PCE コントローラに要求が送信され、BGP 経由で伝送される SR-TE ポリシーに一致する SR-TE パスが計算されます。
4. PCE コントローラはパスを計算し、ラベル スタック（ToR1 の例では 18001、18002、16001）で応答します。
5. ToR1 と AC1 は、SR-TE の自動トンネルを作成し、VRF または IPv4 用の LSP がアップであり稼働中であることを示す返信を NSO コントローラに返します。

L3/L3VPN のセグメント ルーティング オン デマンド ネクスト ホップの設定方法

L3/L3VPN のセグメント ルーティング オン デマンド ネクスト ホップの設定

SR-TE のオンデマンド ネクスト ホップを設定するには、次のステップを実行します。設定ステップを説明するため、次の図を参考として使用します。

図 *16 : ODN* 自動トンネル セットアップ



1. VRF インターフェイスを使用してルータ（R6 テール エンド）を設定します。

```
interface GigabitEthernet0/2/2
 vrf forwarding sr
 ip address 10.0.0.1 255.0.0.0
 negotiation auto

interface Loopback0
 ip address 192.168.0.1 255.255.0.0
 ip router isis 1
```

2. R6（テール エンド）での BGP コミュニティを持つ VRF プレフィックスをタグ付けします。

```
route-map BGP_TE_MAP permit 9
 match ip address traffic
 set community 3276850

ip access-list extended traffic
 permit ip 10.0.0.1 255.255.0.0 any
```

3. R6（テールエンド）およびR1（ヘッドエンド）上のBGPを有効にしてVRF SRプレフィックスをアドバタイズおよび受信し、R6（テールエンド）上のコミュニティ設定で一致させます。

```
 router bgp 100
 bgp router-id 172.16.0.1
 bgp log-neighbor-changes
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 10.0.0.2 remote-as 100
 neighbor 10.0.0.2 update-source Loopback0

 address-family ipv4
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.2 send-community both
  neighbor 10.0.0.2 next-hop-self
 exit-address-family

 address-family vpnv4
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.2 send-community both
  neighbor 10.0.0.2 route-map BGP_TE_MAP out
 exit-address-family

 address-family link-state link-state
  neighbor 10.0.0.2 activate
 exit-address-family

 address-family ipv4 vrf sr
  redistribute connected
 exit-address-family

route-map BGP_TE_MAP permit 9
 match ip address traffic
 set community 3276850

ip access-list extended traffic
 permit ip 10.0.0.1 255.255.0.0 any


router bgp 100
 bgp router-id 192.168.0.2
 bgp log-neighbor-changes
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 10.0.0.2 remote-as 100
 neighbor 10.0.0.2 update-source Loopback0


address-family ipv4
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.2 send-community both
  neighbor 10.0.0.2 next-hop-self
 exit-address-family

 address-family vpnv4
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.2 send-community both
  neighbor 10.0.0.2 route-map BGP_TE_MAP in
 exit-address-family

 address-family link-state link-state
  neighbor 10.0.0.2 activate
 exit-address-family

 address-family ipv4 vrf sr
  redistribute connected
```

```
 exit-address-family

route-map BGP_TE_MAP permit 9
 match community 1
 set attribute-set BGP_TE5555

ip community-list 1 permit 3276850

mpls traffic-eng lsp attributes BGP_TE5555
 path-selection metric igp
 pce
```

4. ヘッドエンド（R1）上のルートマップ/属性設定を有効にします。

```
route-map BGP_TE_MAP permit 9
 match community 1
 set attribute-set BGP_TE5555

ip community-list 1 permit 3276850

mpls traffic-eng lsp attributes BGP_TE5555
 path-selection metric igp
 pce

end
```

5. R1 で PCE および自動トンネル設定を有効にします。

```
mpls traffic-eng tunnels
mpls traffic-eng pcc peer 10.0.0.3 source 10.0.0.4 precedence 255
mpls traffic-eng auto-tunnel p2p tunnel-num min 2000 max 5000
```

6. SR-TE 構成ですべてのコア リンクを有効にし、ポイント ツー ポイント インターフェイスとして有効になっていることを確認します。

```
mpls traffic-eng tunnels

interface GigabitEthernet0/2/0
 ip address 101.102.6.1 255.255.255.0
 ip router isis 1
 mpls traffic-eng tunnels
 isis network point-to-point

interface GigabitEthernet0/3/1
 vrf forwarding sr
 ip address 101.107.3.1 255.255.255.0
 negotiation auto

end
```

7. R3（RR）を有効にして、BGP-LS によって TED を PCE サーバにアドバタイズします。

```
router isis 1
 net 49.0002.0000.0000.0003.00
 ispf level-1-2
 metric-style wide
 nsf cisco
 nsf interval 0
 distribute link-state
 segment-routing mpls
 segment-routing prefix-sid-map advertise-local
 redistribute static ip level-1-2
```

```
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1
 mpls traffic-eng level-2

router bgp 100
 bgp router-id 10.0.0.2
 bgp log-neighbor-changes
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 10.0.0.3 remote-as 100
 neighbor 10.0.0.3 update-source Loopback0

 address-family ipv4
 neighbor 10.0.0.3 activate
 exit-address-family
```

8. PCE サーバの設定を有効にし、RR によって BGP-LS セッションが正しく確立されていることを確認します。

```
Device# sh bgp li li summary
BGP router identifier 10.0.0.3, local AS number 100
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 1436
BGP main routing table version 1436
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs
BGP is operating in STANDALONE mode.
Process       RcvTblVer   bRIB/RIB   LabelVer  ImportVer  SendTblVer  StandbyVer
Speaker            1436       1436          1436       1436           1436
           0

Neighbor        Spk    AS MsgRcvd   MsgSent   TblVer  InQ  OutQ  Up/Down  St/PfxRcd
10.0.0.2          0      100   19923       17437        1436       0     0
  1w2d        103

Device# sh pce ipv4 topo | b Node 3
Node 3
  TE router ID: 10.0.0.2
  Host name: R3
  ISIS system ID: 0000.0000.0003 level-1

  ISIS system ID: 0000.0000.0003 level-2
  Prefix SID:
    Prefix 10.0.0.2, label 20011 (regular)
```

L3/L3VPN のセグメント ルーティング オン デマンド ネクスト ホップの確認

ODN の検証は、L3VPN VRF プレフィックスに基づいています。

1. R1（ヘッドエンドと PCE サーバ）間の PCEP セッションが確立されていることを確認します。

```
Device# sh pce client peer
PCC's peer database:
```

```
--------------------
Peer address: 10.0.0.3 (best PCE)
  State up
  Capabilities: Stateful, Update, Segment-Routing
```

2. すべてのピア間（PCC）で PCEP セッションが確立されていることを確認します。

```
Device# sh pce ipv4 peer
PCE's peer database:
--------------------
Peer address: 10.0.0.4
  State: Up
  Capabilities: Stateful, Segment-Routing, Update
Peer address: 172.16.0.5
  State: Up
  Capabilities: Stateful, Segment-Routing, Update
```

3. R1（ヘッドエンド）に、R6ループバック アドレスへの可視性がないことを確認します。

```
Device# sh ip route 192.168.0.1
% Network not in table
```

4. VRF プレフィックスが R1 VRF SR ルーティング テーブルの MP-BGP によって注入されることを確認します。

```
Device# sh ip route vrf sr
Routing Table: sr
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set
     10.0.0.6/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.0.7/24 is directly connected, GigabitEthernet0/3/1
L        10.0.0.7/32 is directly connected, GigabitEthernet0/3/1
      10.0.0.8/24 is subnetted, 1 subnets
B        10.0.0.9 [200/0] via binding label: 865, 4d21h
```

5. BGP がポリシーとバインディング SID を VRF プレフィックスと正しく関連付けていることを確認します。

```
Device# sh ip bgp vpnv4 vrf sr 106.107.4.0
BGP routing table entry for 100:100:106.107.4.0/24, version 3011
Paths: (1 available, best #1, table sr)
  Not advertised to any peer
  Refresh Epoch 4
  Local
    192.168.0.1 (metric 10) (via default) from 10.0.0.2 (10.0.0.2)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Community: 3276850
      Extended Community: RT:100:100
      Originator: 192.168.0.1, Cluster list: 10.0.0.2
      mpls labels in/out nolabel/1085
      binding SID: 865 (BGP_TE5555)
      rx pathid: 0, tx pathid: 0x0
```

6. バインディング ラベルの VRF プレフィックスとの関連付けを確認します。

```
Device# sh ip route vrf sr 106.107.4.0
Routing Table: sr
Routing entry for 106.107.4.0/24
  Known via "bgp 100", distance 200, metric 0, type internal
  Routing Descriptor Blocks:
  *  Binding Label: 865, from 10.0.0.2, 4d22h ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: 1085
      MPLS Flags: NSF
```

7. VRF プレフィックスが ODN 自動トンネルによって転送されることを確認します。

```
Device# sh ip cef label-table
Label               Next Hop             Interface
0                    no route
865                  attached             Tunnel2000

     Device# sh ip cef vrf sr 106.107.4.0 detail
10.0.0.8/24, epoch 15, flags [rib defined all labels]
  recursive via 865 label 1085
    attached to Tunnel2000
```

8. ODN 自動トンネルの状態を確認します。

```
Device# sh mpls traffic-eng tunnels
P2P TUNNELS/LSPs:
Name: R1_t2000                 (Tunnel2000) Destination: 192.168.0.1 Ifhandle:
0x6F5 (auto-tunnel for BGP TE)
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected---□
auto-tunnel 2000
    path option 1, (SEGMENT-ROUTING) (PCE) type dynamic (Basis for Setup, path
weight 10)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
    Metric Type: IGP (interface)
    Path Selection:
     Protection: any (default)
    Path-selection Tiebreaker:
      Global: not set   Tunnel Specific: not set   Effective: min-fill (default)
    Hop Limit: disabled
    Cost Limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear
    AutoRoute: disabled LockDown: disabled Loadshare: 0 [0] bw-based
    auto-bw: disabled
    Attribute-set: BGP_TE5555---□ attribute-set
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: dynamic path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  PCEP Info:
    Delegation state: Working: yes   Protect: no
    Working Path Info:
      Request status: processed
      Created via PCRep message from PCE server: 10.0.0.3--□ via PCE server
      PCE metric: 30, type: IGP
    Reported paths:
      Tunnel Name: Tunnel2000_w
       LSPs:
        LSP[0]:
         source 10.0.0.4, destination 192.168.0.1, tunnel ID 2000, LSP ID 1
         State: Admin up, Operation active
         Binding SID: 865
         Setup type: SR
```

```
        Bandwidth: requested 0, used 0
        LSP object:
          PLSP-ID 0x807D0, flags: D:0 S:0 R:0 A:1 O:2
        Metric type: IGP, Accumulated Metric 0
        ERO:
          SID[0]: Adj, Label 2377, NAI: local 101.102.6.1 remote 10.0.0.10
          SID[1]: Unspecified, Label 17, NAI: n/a
          SID[2]: Unspecified, Label 20, NAI: n/a
  History:
    Tunnel:
      Time since created: 4 days, 22 hours, 21 minutes
      Time since path change: 4 days, 22 hours, 21 minutes
      Number of LSP IDs (Tun_Instances) used: 1
    Current LSP: [ID: 1]
      Uptime: 4 days, 22 hours, 21 minutes
  Tun_Instance: 1
  Segment-Routing Path Info (isis  level-1)
    Segment0[Link]: 101.102.6.1 - 10.0.0.10, Label: 2377
    Segment1[ - ]: Label: 17
    Segment2[ - ]: Label: 20
```

9. R1（ヘッドエンド）で ODN 自動トンネル LSP の状態を確認します。

```
Device# sh pce client lsp brief
PCC's tunnel database:
----------------------
 Tunnel Name: Tunnel2000_w
   LSP ID 1
 Tunnel Name: Tunnel2000_p

R1# sh pce client lsp detail
PCC's tunnel database:
----------------------
Tunnel Name: Tunnel2000_w
 LSPs:
  LSP[0]:
   source 10.0.0.4, destination 192.168.0.1, tunnel ID 2000, LSP ID 1
   State: Admin up, Operation active
   Binding SID: 865
   Setup type: SR
   Bandwidth: requested 0, used 0
   LSP object:
     PLSP-ID 0x807D0, flags: D:0 S:0 R:0 A:1 O:2
   Metric type: IGP, Accumulated Metric 0
   ERO:
     SID[0]: Adj, Label 2377, NAI: local 101.102.6.1 remote 10.0.0.10
     SID[1]: Unspecified, Label 17, NAI: n/a
     SID[2]: Unspecified, Label 20, NAI: n/a
```

10. PCE サーバで ODN LSP の状態を確認します。

```
Device# sh pce lsp summ

PCE's LSP database summary:
--------------------------------
All peers:
 Number of LSPs:         1
  Operational: Up:       1 Down:                 0
  Admin state: Up:       1 Down:                 0
  Setup type: RSVP:      0 Segment routing:      1


Peer 10.0.0.4:
 Number of LSPs:         1
  Operational: Up:       1 Down:                 0
```

```
  Admin state: Up:       1  Down:                0
  Setup type: RSVP:       0 Segment routing:     1
```

11. PCE サーバで詳細な LSP 情報を確認します。

```
Device# sh pce lsp det
PCE's tunnel database:
----------------------
PCC 10.0.0.4:
Tunnel Name: Tunnel2000_w
 LSPs:
  LSP[0]:
   source 10.0.0.4, destination 192.168.0.1, tunnel ID 2000, LSP ID 48
   State: Admin up, Operation active
   Binding SID: 872
   PCEP information:
     plsp-id 526288, flags: D:1 S:0 R:0 A:1 O:2
   Reported path:
     Metric type: IGP, Accumulated Metric 0
      SID[0]: Adj, Label 885, Address: local 10.0.0.9 remote 10.0.0.10
      SID[1]: Unknown, Label 17,
      SID[2]: Unknown, Label 20,
   Computed path:
     Computed Time: Tue Dec 20 13:12:57 2016 (00:11:53 ago)
     Metric type: IGP, Accumulated Metric 30
      SID[0]: Adj, Label 885, Address: local 10.0.0.9 remote 10.0.0.10
      SID[1]: Adj, Label 17, Address: local 10.0.0.12 remote 10.0.0.13
      SID[2]: Adj, Label 20, Address: local 10.0.0.14 remote 10.0.0.14
   Recorded path:
     None
```

12. VRF SR に接続されているインターフェイスをシャットダウンして、プレフィックスが MP-BGP によってアドバタイズされなくなるようにします。

```
Device# int gig0/2/2
Device(config-if)#shut
```

13. VRF プレフィックスが R6（テールエンド）を介して R1（ヘッドエンド）にアドバタイズされなくなったことを確認します。

```
Device# sh ip route vrf sr
Routing Table: sr
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set
      10.0.0.6/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.0.7/24 is directly connected, GigabitEthernet0/3/1
L        10.0.0.8/32 is directly connected, GigabitEthernet0/3/1
```

14. ODN 自動トンネルが存在しないことを確認します。

```
Device# sh mpls traffic-eng tunnels
P2P TUNNELS/LSPs:
P2MP TUNNELS:
P2MP SUB-LSPS:
```

L3/L3VPN のセグメント ルーティング オン デマンド ネクスト ホップの追加情報

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 Command List, All Releases』

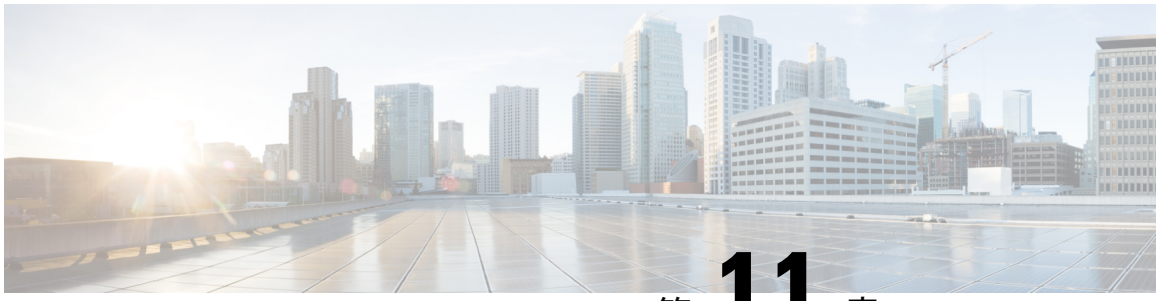
L3/L3VPN のセグメント ルーティング オン デマンド ネクスト ホップに関する機能情報

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 *9 : L3/L3VPN* のセグメント ルーティング オン デマンド ネクスト ホップに関する機能情報

機能名	リリース	機能情報
L3/L3VPN 用のセグメント ルーティング オン デマンド ネクスト ホップ	Cisco IOS XE Everest 16.5.1b	オンデマンドネクストホップ（ODN）は、再配布を行わずに制約やポリシーなど、PCE コントローラへのエンドツーエンド LSP の計算の委任をトリガーします。 次のコマンドが導入または変更されました。 **route-map BGP_TE_MAP permit**、**mpls traffic-eng tunnels**、**sh bgp li li summary**、**sh pce client peer**、**sh pce ipv4 peer**、**sh ip route vrf sr**、**sh ip bgp vpnv4 vrf sr**、**sh ip cef label-table**、**sh mpls traffic-eng tunnels**、**sh pce client lsp brief**、**sh pce lsp summ**、**sh pce lsp det**、**routing-default-optimize**



第 11 章

L2VPN/VPWS のセグメント ルーティング オン デマンド

レイヤ 2 VPN（L2VPN）のためのオンデマンド ネクスト ホップ（ODN）は、セグメント ルーティング（SR）トラフィック エンジニアリング（TE）自動トンネルを作成し、擬似回線データプレーンのために自動トンネルを使用します。

L2VPN/VPWS のセグメント ルーティング オン デマンド ネクスト ホップの制約事項

- レイヤ 2 VPN/VPWS（仮想プライベート ワイヤ サービス）オン デマンド ネクスト ホップ（ODN）は擬似回線（PW）クラスではサポートされません。

- L2VPN または VPWS のためのオン デマンドのセグメント ルーティングは、BGP シグナル/ADVPWS または仮想プライベート LAN サービス（VPLS）ではサポートされません。
- 属性セットを使用して L2VPN 用にサポートおよび作成されるのは、セグメント ルーティング TE トンネルのみです。
- TE の属性セットが設定されている場合、L2VPN 優先パス帯域幅関連の設定は有効になりません。
- LDP シグナリングを使用した L2-VPN ODN VPWS のみがサポートされています。

L2VPN/VPWS のセグメント ルーティング オン デマンド ネクスト ホップに関する情報

L2VPN のオン デマンド ネクスト ホップ（ODN）は SR TE 自動トンネルを作成し、擬似回線データプレーンの自動トンネルを使用します。ピア IP アドレスはトンネルの宛先であり、TE LSP 属性によってトンネルのパスが決定されます。場合によっては、擬似回線接続は複数の内部ゲートウェイ プロトコル（IGP）エリアにまたがる必要がありますが、LDP はシグナリング プロトコルとして使用されます。擬似回線エンドポイント プロバイダー エッジ（PE）のループバック アドレスは、IGP エリアの境界を越えて配布されません。この場合、ある PE がその RIB 内に擬似回線接続のピア PE に到達するためのデフォルト ルート（または完全一致ルート）を持たない可能性があります。したがって、擬似回線接続は LDP によってシグナルを受けることができません。この問題に対処するために、LSP 属性の下に新しいオプション **autoroute destination** が導入されました。この **autoroute destination** コマンドを使用して LSP 属性が設定されている場合、自動トンネルは LSP 属性を使用して、自動トンネル インターフェイスをネクスト ホップとしてトンネル宛先のスタティック ルートを自動的に作成します。このスタティック ルートにより、LDP は LDP セッションを確立し、2 つの擬似回線エンドポイント間でラベル マッピング メッセージを交換することができます。

（注） LDP シグナリング L2VPN によって使用される LSP 属性の設定にのみ autoroute destination コマンドを使用します。これは BGP シグナリング レイヤ 3 VPN ODN には必要ありません。

AToM マネージャ

Any Transport over MPLS（AToM）マネージャは、属性セットとピア IP アドレスのペアで自動トンネルのデータベースを維持します。AToM マネージャは擬似回線インターフェイス（VC）の SR TE 自動トンネルを追加または削除できます。

同じ属性セットまたはピアで設定された VC は、同じ自動トンネルを使用します。すべての擬似回線インターフェイスで属性セットまたはピアのペアが使用されなくなった場合、TE サービスを使用して自動トンネルをデータベースから削除できます。

エリア間 L2VPN ODN

LDP がシグナリング プロトコルとして使用され、擬似回線接続が複数の内部ゲートウェイ プロトコル（IGP）にまたがる場合、擬似回線エンドポイント PE のループバック アドレスは IGP エリア境界を越えて配布されません。この場合、ある PE がその RIB 内に擬似回線接続のピア PE に到達するためのデフォルト ルート（または完全一致ルート）を持たない可能性があります。したがって、擬似回線接続は LDP によってシグナルを受けることができません。

L2VPN/VPWS のセグメント ルーティング オン デマンド ネクスト ホップの設定方法

L2VPN/VPWS を設定するには、擬似回線インターフェイス コマンドまたはテンプレート メソッドのいずれかを使用できます。

Pesudowire インターフェイス コマンドを使用した、L2VPN/VPWS のオン デマンド ネクスト ホップでのセグメント ルーティングの設定

1. ヘッドエンド ノード（R1）で次のコマンドを実行します。

```
R1#
!
mpls traffic-eng auto-tunnel p2p tunnel-num min 2000 max 2002
!
interface GigabitEthernet0/3/1
 no ip address
 negotiation auto
 service instance 300 ethernet
  encapsulation dot1q 300
!
interface pseudowire4243
 encapsulation mpls
 neighbor 56.6.6.6 300
 preferred-path segment-routing traffic-eng attribute-set L2VPNODN
!
l2vpn xconnect context foobar
 member GigabitEthernet0/3/1 service-instance 300
 member pseudowire4243
!
mpls traffic-eng lsp attributes L2VPNODN
 priority 7 7
 path-selection metric te
!
end
```

2. テール エンド（R2）で次のコマンドを実行します。

```
R2#
!
mpls traffic-eng auto-tunnel p2p tunnel-num min 2000 max 2002

interface pseudowire4243
```

```
 encapsulation mpls
 neighbor 51.1.1.1 300
 preferred-path segment-routing traffic-eng attribute-set L2VPNODN
!
interface GigabitEthernet0/2/2
 no ip address
 negotiation auto
 service instance 300 ethernet
  encapsulation dot1q 300
!
l2vpn xconnect context foobar
 member GigabitEthernet0/3/1 service-instance 300
 member pseudowire4243
!
mpls traffic-eng lsp attributes L2VPNODN
 priority 7 7
 path-selection metric te
!
end
```

テンプレートコマンドを使用したL2VPN/VPWSのセグメントルーティング オン デマンド ネクスト ホップの設定

1. ヘッドエンド ノード（R1）で次のコマンドを実行します。

```
R1#
template type pseudowire test
 encapsulation mpls
 preferred-path segment-routing traffic-eng attribute-set L2VPNODN
!
interface GigabitEthernet0/3/1
 no ip address
 negotiation auto
 service instance 400 ethernet
  encapsulation dot1q 400
!
l2vpn xconnect context foobar2
 member 56.6.6.6 400 template test
 member GigabitEthernet0/3/1 service-instance 400
```

2. テール エンド（R2）で次のコマンドを実行します。

```
R2#
!
template type pseudowire test
 encapsulation mpls
 preferred-path segment-routing traffic-eng attribute-set L2VPNODN
!
interface GigabitEthernet0/2/2
 no ip address
 negotiation auto
 service instance 400 ethernet
  encapsulation dot1q 400
!
l2vpn xconnect context foobar2
 member 51.1.1.1 400 template test
 member GigabitEthernet0/2/2 service-instance 400
!
```

```
end
```

前に付加オプションを使用した L2VPN/VPWS のセグメント ルーティング オン デマンド ネクスト ホップの設定

LSP のパスを制御するために前に付加（Prepend）オプションを有効にすることができます。前に付加オプションは、エリア内でのみサポートされ、ラベル付きパスのみをサポートします。前に付加オプションを有効にするには、次の CLI を使用します。

```
R1(config-lsp-attr)#path-selection segment-routing prepend
R1(config-lsp-attr-sr-prepend)#?
Segment-routing label prepend commands:
  exit   Exist from segment-routing prepend config mode
  index  Specify the next entry index to add, edit or delete
  list   List all prepend entries
  no     Delete a specific entry index
R1(config-lsp-attr-sr-prepend)#index ?
  <1-10>  Entry index number
  last-hop    Indicates the end of label list
  next-label  Specify the next MPLS label in the path
```

（注） ラストホップ オプションがテール エンド ノードを示している場合。このオプションを使用する場合は、LSP パスの制御を行うことはできません。

L2VPN/VPWS のセグメント ルーティング オン デマンド ネクスト ホップの優先パスの設定

パスが失敗したか、コマンドが削除されたことが原因である、LSP に障害が発生した場合に仮想回線（VC）をダウンさせるには、フォールバック モードを無効にします。

```
preferred-path segment-routing traffic-eng attribute-set L2VPNODN
disable-fallback  disable fall back to alternative route
```

L2VPN/VPWS のセグメント ルーティング オン デマンド ネクスト ホップの自動ルート宛先の設定

エリア間宛先の場合、IP アドレスがヘッドエンドにインストールされていない可能性があります。L2-VPN VPWS の対象となる LDP セッションを有効にするには、宛先 IP アドレスがイン

ストールされている必要があります。L2VPN VPWS の対象となる LDP セッションを有効にするには、属性セットの下に自動ルートの宛先を設定します。

```
Device#
mpls traffic-eng lsp attributes L2VPNODN
 priority 7 7
 path-selection metric te
 pce
 autoroute destination
!
end
```

宛先アドレスはスタティック ルートとして L2-VPN ODN LSP によってインストールされます。

次のコマンドを実行して、自動ルート宛先の設定を確認します。

```
Device#sh ip route 56.6.6.6
Routing entry for 56.6.6.6/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via Tunnel2000------------------------ L2-VPN ODN LSP
      Route metric is 0, traffic share count is 1


Device#sh mpls for 56.6.6.6
Local      Outgoing             Prefix          Bytes Label      Outgoing   Next Hop

Label      Label               or Tunnel Id     Switched          interface

25          [T]  Pop Label    56.6.6.6/32      0                 Tu2000     point2point
```

L2VPN/VPWS のセグメント ルーティング オン デマンド ネクスト ホップの確認

1. **sh mpls l2 vc**

```
Device#sh mpls l2 vc
Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Gi0/3/1        Eth VLAN 300               56.6.6.6        300        UP
```

2. **sh mpls l2 vc detail**

```
Device# sh mpls l2 vc detail
Local interface: Gi0/3/1 up, line protocol up, Eth VLAN 300 up
  Interworking type is Ethernet
  Destination address: 56.6.6.6, VC ID: 300, VC status: up
    Output interface: Tu2000, imposed label stack {23 17 20}----- 20 is the VC label
 assigned by R6
    Preferred path: Tunnel2000,  active
    Default path: ready
    Next hop: point2point
  Create time: 00:15:48, last status change time: 00:15:38
    Last label FSM state change time: 00:15:38
  Signaling protocol: LDP, peer 56.6.6.6:0 up
```

```
    Targeted Hello: 51.1.1.1(LDP Id) -> 56.6.6.6, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 2032, remote 20
    Group ID: local 20, remote 25
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  SSO Descriptor: 56.6.6.6/300, local label: 2032
  Dataplane:
    SSM segment/switch IDs: 10198/6097 (used), PWID: 1001
  VC statistics:
    transit packet totals: receive 0, send 0
    transit byte totals:   receive 0, send 0
    transit packet drops:  receive 0, seq error 0, send 0
```

3. sh l2vpn atom preferred-path

```
Device#  sh l2vpn atom preferred-path
Tunnel interface    Bandwidth Tot/Avail/Resv         Peer ID         VC ID
------------------       ---------------------------------          ---------------
     ----------
Tunnel2000                                                             56.6.6.6
     300
!
end
```

4. sh l2vpn atom vc

```
Device# sh l2vpn atom vc
Interface Peer ID         VC ID      Type   Name                       Status
--------- --------------      ----------     ------ -------------------------
----------
pw4243    56.6.6.6        300        p2p    foobar                        UP
!
end
```

5. sh mpl traffic-eng tun tun 2000

```
Device# sh mpl traffic-eng tun tun 2000
Name: R1_t2000                 (Tunnel2000) Destination: 56.6.6.6 Ifhandle: 0x7EE
(auto-tunnel for atom)
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
   path option 1, (SEGMENT-ROUTING) (PCE) type dynamic (Basis for Setup, path weight
 30)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
```

```
    Metric Type: TE (interface)
    Path Selection:
     Protection: any (default)
    Path-selection Tiebreaker:
      Global: not set   Tunnel Specific: not set   Effective: min-fill (default)
    Hop Limit: disabled
    Cost Limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear
    AutoRoute: disabled LockDown: disabled Loadshare: 0 [0] bw-based
    auto-bw: disabled
    Attribute-set: L2VPNODN
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: dynamic path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
PCEP Info:
    Delegation state: Working: yes   Protect: no
    Delegation peer: 58.8.8.8
    Working Path Info:
      Request status: processed
      Created via PCRep message from PCE server: 58.8.8.8
      PCE metric: 30, type: TE
    Reported paths:
      Tunnel Name: Tunnel2000_w
       LSPs:
        LSP[0]:
         source 51.1.1.1, destination 56.6.6.6, tunnel ID 2000, LSP ID 4
         State: Admin up, Operation active
         Binding SID: 20
         Setup type: SR
         Bandwidth: requested 0, used 0
         LSP object:
           PLSP-ID 0x807D0, flags: D:0 S:0 R:0 A:1 O:2
         Metric type: TE, Accumulated Metric 30
         ERO:
           SID[0]: Adj, Label 19, NAI: local 101.104.1.1 remote 101.104.1.2
           SID[1]: Adj, Label 23, NAI: local 103.104.12.2 remote 103.104.12.1
           SID[2]: Adj, Label 17, NAI: local 103.106.13.1 remote 103.106.13.2
       PLSP Event History (most recent first):
         Tue Jun 20 10:04:48.514: PCRpt create LSP-ID:4, SRP-ID:0, PST:1,
METRIC_TYPE:2, REQ_BW:0, USED_BW:0
         Tue Jun 20 10:04:48.511: PCRep RP-ID:9
         Tue Jun 20 10:04:48.505: PCReq RP-ID:9, LSP-ID:4, REQ_BW:0
  History:
    Tunnel:
      Time since created: 18 minutes, 26 seconds
      Time since path change: 17 minutes, 9 seconds
      Number of LSP IDs (Tun_Instances) used: 4
    Current LSP: [ID: 4]
      Uptime: 17 minutes, 9 seconds
  Tun_Instance: 4
  Segment-Routing Path Info (isis  level-2)
    Segment0[Link]: 101.104.1.1 - 101.104.1.2, Label:  19--------□ will not be shown
 in sh mpls l2 vc output
    Segment1[Link]: 103.104.12.2 - 103.104.12.1, Label: 23
    Segment2[Link]: 103.106.13.1 - 103.106.13.2, Label: 17
!
end
```

6. sh mpls ldp discovery

```
Device# sh mpls ldp discovery
Local LDP Identifier:
```

```
    51.1.1.1:0
    Discovery Sources:
    Targeted Hellos:
        51.1.1.1 -> 56.6.6.6 (ldp): active/passive, xmit/recv
            LDP Id: 56.6.6.6:0
```

7. **sh mpl ldp nei**

```
Device# sh mpl ldp nei
Peer LDP Ident: 56.6.6.6:0; Local LDP Ident 51.1.1.1:0
        TCP connection: 56.6.6.6.38574 - 51.1.1.1.646
        State: Oper; Msgs sent/rcvd: 43/42; Downstream
        Up time: 00:19:33
        LDP discovery sources:
          Targeted Hello 51.1.1.1 -> 56.6.6.6, active, passive
        Addresses bound to peer LDP Ident:
          105.106.2.2     103.106.13.2    56.6.6.6
!
```

8. **sh int pseudowire 4243**

```
Device# sh int pseudowire 4243
pseudowire4243 is up
    MTU 1500 bytes, BW not configured
    Encapsulation mpls
    Peer IP 56.6.6.6, VC ID 300
    RX    0 packets 0 bytes 0 drops
    TX    0 packets 0 bytes 0 drops
!
```

9. **sh xconnect all**

```
Device# sh xconnect all
Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware

XC ST  Segment 1                                    S1 Segment 2
      S2
------+---------------------------------+--+---------------------------------+--
UP pri   ac Gi0/3/1:300(Eth VLAN)        UP mpls 56.6.6.6:300                  UP
```

L2VPN/VPWS のセグメント ルーティング オン デマンド ネクスト ホップの追加情報

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 Command List, All Releases』

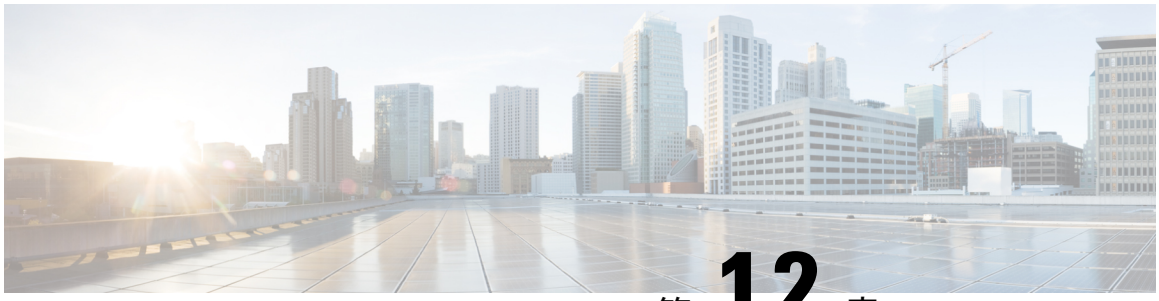
L2VPN/VPWS のセグメント ルーティング オン デマンド ネクスト ホップに関する機能情報

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 *10 : L2VPN/VPWS* のセグメント ルーティング オン デマンド ネクスト ホップに関する機能情報

機能名	リリース	機能情報
L2VPN/VPWS のセグメント ルーティング オン デマンド ネクスト ホップ	Cisco IOS XE Fuji 16.7.1	L2VPN の ODN は、SR TE 自動トンネルを作成し、擬似回線データプレーンの自動トンネルを使用します。ピア IP アドレスはトンネルの宛先であり、TE LSP 属性によってトンネルのパスが決定されます。 次のコマンドが追加または修正されました。 **sh mpls l2 vc**、**sh mpls l2 vc detail**、**sh l2vpn atom preferred-path**、**sh l2vpn atom vc**、**sh mpl traffic-eng tun tun 2000**、**sh mpls ldp discovery**、**sh mpl ldp nei**、**sh int pseudowire 4243**、**sh xconnect all**。



第 12 章

高速コンバージェンスのデフォルト最適化

高速コンバージェンスのデフォルトの最適化機能は、すべてのプロトコルのデフォルトの設定を、高速コンバージェンスの推奨されるデフォルト値に変更します。

高速コンバージェンスのデフォルト最適化に関する情報

高速コンバージェンスのデフォルトの最適化機能は、すべてのプロトコルのデフォルトの設定を、高速コンバージェンスの推奨されるデフォルト値に変更します。IS-IS および OSPF の両方についてデフォルトを事前の高速コンバージェンス設定に戻すには、**no routing-default-optimize** コマンドを使用します。このコマンドは、信号をその IS-IS および OSPF に送信し、これらのプロトコルのデフォルト設定を変更します。

デフォルトでは、高速コンバージェンス設定が有効になっているため、ソフトウェアをアップグレードすると、新しい動作が自動的に表示されます。これにより、マルチベンダー展開でのデバイスの統合が容易になり、コンバージェンスの低下によるサポートケースが減少します。

デフォルトの最適化を無効にすると、既存のプロトコルのデフォルト設定が使用されます。デフォルトの最適化を有効にすると、新しいプロトコルのデフォルト値が使用されます。show running configurations は、デフォルト設定が使用されている場合でも、デフォルト設定の設定行を表示しません。

プロトコルの設定はデフォルトよりも優先されますが、デフォルトの最適化への変更は設定を上書きしません。

次に、IS-IS での **spf-interval** コマンドの出力例を示します。

```
Device(config-if)# router isis
Device(config-router)# spf-interval 10 5500 5500
```

デフォルト値以外が設定されている場合は、show running configuration の出力に表示されます。

```
Device(config-router)# spf-interval 5 50 200
Device(config-router)# do show run | inc spf-interval
 spf-interval 5 50 200
```

デフォルト値を設定するか、デフォルト以外の設定を削除することによって、デフォルト値に戻すことができます。

IS-IS のデフォルト最適化値

次の表は、デフォルト最適化の影響を受ける設定の概要を示します。

IS-IS コマンド	パラメータ	デフォルト最適化が無効	デフォルト最適化が有効
fast-flood			
	# of lsps flooded back-back	無効	10
spf-interval			
	初期（ミリ秒）	5500	50
	セカンダリ（ミリ秒）	5500	200
	最大（秒）	10	5
prc-interval			
	初期（ミリ秒）	2000	50
	セカンダリ（ミリ秒）	5000	200
	最大（秒）	5	5
lsp-gen-interval			
	初期（ミリ秒）	50	50
	セカンダリ（ミリ秒）	5000	200
	最大（秒）	5	5
log-adjacency-changes		無効	有効

OSPF のデフォルト最適化値

次の表は、OSPFv2/v3 のデフォルト最適化の影響を受ける設定の概要を示します。

OSPF コマンド	パラメータ	デフォルト最適化が無効	デフォルト最適化が有効
timers throttle spf			
	初期（ミリ秒）	5000	50
	セカンダリ（ミリ秒）	10000	200
	最大（ミリ秒）	10	5
timers throttle lsa all			
	初期（ミリ秒）	0	50
	セカンダリ（ミリ秒）	5000	200
	最大（ミリ秒）	5	5
timers lsa arrival			
	milliseconds	1000	100

以下は、デフォルト最適化値を使用した OSPFv2 の **show ip ospf** コマンドの出力例です。

```
Device# show ip ospf
 Routing Process "ospf 10" with ID 1.1.1.1
 Start time: 00:00:01.471, Time elapsed: 03:00:34.706
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Supports NSSA (compatible with RFC 3101)
 Supports Database Exchange Summary List Optimization (RFC 5243)
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 50 msecs
 Minimum hold time between two consecutive SPFs 200 msecs
 Maximum wait time between two consecutive SPFs 5000 msecs
 Incremental-SPF disabled
 Initial LSA throttle delay 50 msecs
 Minimum hold time for LSA throttle 200 msecs
 Maximum wait time for LSA throttle 5000 msecs
Minimum LSA arrival 100 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
EXCHANGE/LOADING adjacency limit: initial 300, process maximum 300
Number of external LSA 18. Checksum Sum 0x075EB2
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
```

```
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 4 (2 loopback)
        Area has RRR enabled
        Area has no authentication
        SPF algorithm last executed 02:27:23.736 ago
        SPF algorithm executed 20 times
        Area ranges are
        Number of LSA 94. Checksum Sum 0x321DCF
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

以下は、デフォルト最適化値を使用した OSPFv3 の **show ospf** コマンドの出力例です。

```
Device# show ospfv3
 OSPFv3 10 address-family ipv6
 Router ID 11.11.11.11
 Supports NSSA (compatible with RFC 3101)
Supports Database Exchange Summary List Optimization (RFC 5243)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 50 msecs
Minimum hold time between two consecutive SPFs 200 msecs
Maximum wait time between two consecutive SPFs 5000 msecs
Initial LSA throttle delay 50 msecs
Minimum hold time for LSA throttle 200 msecs
Maximum wait time for LSA throttle 5000 msecs
Minimum LSA arrival 100 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Retransmission limit dc 24 non-dc 24
EXCHANGE/LOADING adjacency limit: initial 300, process maximum 300
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        SPF algorithm executed 7 times
        Number of LSA 3. Checksum Sum 0x012426
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

高速コンバージェンスのデフォルト最適化の追加情報

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 Command List, All Releases』

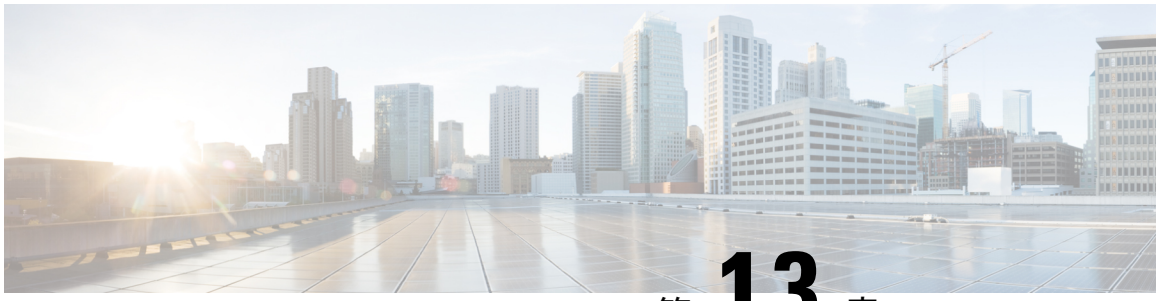
高速コンバージェンスのデフォルト最適化の機能情報

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* : 高速コンバージェンスのデフォルト最適化の機能情報

機能名	リリース	機能情報
高速コンバージェンスのデフォルト最適化	Cisco IOS XE Everest 16.5.1b	高速コンバージェンスのデフォルトの最適化機能は、すべてのプロトコルのデフォルトの設定を、高速コンバージェンスの推奨されるデフォルト値に変更します。 新しく追加または変更されたコマンドはありません。



第 13 章

ルーティング情報ベースのサポート

ルーティング情報ベース（RIB）拡張は、ルート再配布およびオンデマンドネクストホップ要件をサポートします。

ルート再配布のためのルーティング情報ベースのサポート

Cisco IOS XE Everest 16.5.1 では、プレフィックスに関連付けられたラベルを再配布するための要件が導入されています。再配布の要件をサポートするために、プレフィックスごとのローカル ラベルのストレージが RIB でサポートされます。

異なる SRGB を使用する可能性のあるさまざまなプロトコルでの使用を容易にするために、SID の代わりにローカル ラベルが保存されます。宛先プロトコルによって割り当てられた SID は、送信元プロトコルに関連付けられた SID と同じではない場合があります。

プレフィックス到達可能性アドバタイズメントまたは SRMS アドバタイズメントは、SID のソースです。SRMS アドバタイズでは、再配布の宛先プロトコルは、アドバタイズメントのソースが SRMS ではないことを他のネットワーク ノードで示すことによって競合の解決を変更するため、そのプレフィックス到達可能性アドバタイズメントで SID をアドバタイズしません。

OSPF ノード SID 再配布のサポート

Cisco IOS XE 16.7.1 では以前のケースとは異なり、OSPF が他の IGP から再配布されたプレフィックスを受信し、その逆にプレフィックス セグメント識別子（SID）もアドバタイズされ

ます。IGP ドメイン間で SID を学習するには、BGP LS（または）セグメント ルーティング マッピング サーバ（SRMS）のサポートが必要でした。

ユーザがOSPFで再配布を有効にすると、プレフィックスエントリに関連付けられたプレフィックス SID エントリが OSPF に提供されます。これは OSPF によってそのすべてのネイバーにアドバタイズされます。OSPF のアドバタイズ方法は、ネットワーク内の OSPF の役割によって異なります。

OSPF ノード SID 再配布のサポートに関する情報

NSSA ASBR

Not-So-Stubby Area 自律システム境界ルータ（NSSA ASBR）の OSPF で **redistribute ISIS** *instance* **ip** を有効にすると、SID エントリとともに IS-IS で学習された IP ルーティング情報ベース（RIB）からのすべてのプレフィックスを取得します。OSPF は、エリアとして範囲と、プレフィックスのRTYPE_NSSA1またはRTYPE_NSSA2としてルートタイプを持つ拡張プレフィックスLSA（EPL）を生成し、そのすべてのネイバーにアドバタイズします。同様に、再配布が設定されていない場合（または）プレフィックスが使用できなくなったときに、OSPF は EPL を取り消します。再配布されたルートが非接続ルートである場合、OSPF は No-PHP フラグを設定しますが、明示的なNULLフラグは設定されません。ただし、再配布されたルートが接続済みルートである場合、OSPF は、SR ポリシーで行われた設定に従って明示的な NULL および No-PHP フラグを設定します。

NSSA ABR が EPL を受信すると、ABR は LSA を不透明 AS EPL に変換し、そのすべてのネイバーにフラッディングします。

ABR でも ASBR でもないNSSAルータがEPLを受信すると、SIDエントリとともにプレフィックスを学習し、同じエリア内のすべてのネイバーにフラッディングします。

非 NSSA ASBR

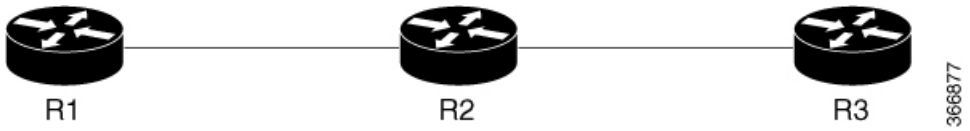
通常の ASBR ルータである OSPF でユーザが **redistribute ISIS** *instance* **ip** を有効にすると、SID エントリとともに IS-IS によって学習された IP RIB からのすべてのプレフィックスを取得します。OSPF は、自律システム（AS）として範囲と、プレフィックスの RTYPE_EXTERN1 または RTYPE_EXTERN2 としてルートタイプを持つ EPL を生成し、そのすべてのネイバーにアドバタイズします。同様に、再配布が設定されていない場合（または）プレフィックスが使用できなくなったときに、OSPF は再び EPL を AS 範囲とともに取り消します。再配布されたルートが非接続ルートである場合、OSPF は No-PHP フラグを設定しますが、明示的な NULL フラグは設定されません。ただし、再配布されたルートが接続済みルートである場合、OSPF は、SR ポリシーで行われた設定に従って明示的なNULLおよびNo-PHPフラグを設定します。ルータは AS 範囲を持つ EPL を受信すると、SID エントリとともにプレフィックスを学習し、すべてのエリアのすべてのネイバーにフラッディングします。

プレフィックスの再配布

IS-IS で OSPF ルートの再配布が有効になっている場合、プレフィックスが SID 情報とともに与えられ、プレフィックスがSID値を持つ他のドメインに到達するようになります。他のドメ

インへの OSPF プレフィックスの再配布を理解するには、以下のトポロジを参照してください。

図 *17 : OSPF* プレフィックスの再配布



R1 および R2 は OSPF が有効になっています。R2 および R3 は IS-IS が有効になっています。IS-IS および OSPF の両方ともセグメント ルーティングが有効になっています。R2 では、IS-IS および OSPF の両方とも設定されています。設定されているプレフィックスは次のとおりです。

1. R1：1.1.1/32（SID 1 で OSPF が有効）
2. R2：2.2.2/32（SID 2 で OSPF が有効）
3. R3：3.3.3/32（ISIS SID 3 が対応）

R2 で SID 再配布を有効にすると、プレフィックス 3.3.3.3/32is が R1 に再配布されます。したがって、R1 はプレフィックス R3 に到達する SID を知っています。

```
conf t
router isis 10
 net 49.0001.0000.0000.0001.00
 metric-style wide
distribute link-state
 segment-routing mpls
router ospf 10
router-id 2.2.2.2
segment-routing mpls
distribute link-state
```

OSPF ルートへの ISIS の再配布を有効にするには次を実行します。

```
conf t
router ospf 10
redistribute isis 10 ip
```

OSPF ノード SID 再配布の確認

show ip ospf rib redistribution detail コマンドを使用して、OSPF が IS-IS からプレフィックスを再配布しているかどうかを確認します。

```
Device# show ip ospf rib redistribution  detail
OSPF Router with ID (2.2.2.2) (Process ID 10)

                Base Topology (MTID 0)

OSPF Redistribution
3.3.3.3/32, type 2, metric 20, tag 0, from IS-IS Router
  Attributes 0x1000000, event 1, PDB Index 4, PDB Mask 0x0
  Source route metric 20, tag 0
  SID 1003, SID Flags NP-bit, EPX Flags None
   via 7.9.0.9, Ethernet0/0
```

show ip ospf segment-routing local-prefix コマンドを使用して、SID エントリがそのネイバーにアドバタイズされているかどうかを確認します。

```
Device# show ip ospf segment-routing local-prefix

           OSPF Router with ID (2.2.2.2) (Process ID 10)
Area 0:
 Prefix:            Sid:   Index:          Type:      Source:
2.2.2.2/32         2      0.0.0.0         Intra      Loopback0
AS external:
Prefix:            Sid:   Index:          Type:      Source:
 3.3.3.3/32        3     0.0.0.1         External   Redist
```

show ip ospf segment-routing sid-database コマンドを使用して、SID が受信されているかどうかを確認します。

```
Device# show ip ospf segment-routing sid-database

           OSPF Router with ID (1.1.1.1) (Process ID 10)
OSPF Segment Routing SIDs

Codes: L - local, N - label not programmed,
       M - mapping-server

SID             Prefix              Adv-Rtr-Id       Area-Id  Type
--------------  ------------------  ---------------  -------  ----------
1               1.1.1.1/32          1.1.1.1          0        Intra
2               2.2.2.2/32          2.2.2.2          0        Intra
3               3.3.3.3/32          2.2.2.2          -        External
```

show ip route 3.3.3.3 コマンドを使用して、再配送されたルートに対して IP ルーティング エントリが設定されているかどうかを確認します。

```
Device# show ip route 3.3.3.3
Routing entry for 3.3.3.3/32
  Known via "ospf 10", distance 110, metric 20, type extern 2, forward metric 20
  Last update from 1.2.0.2 on Ethernet0/1, 00:00:01 ago
 SR Incoming Label: 16003
  Routing Descriptor Blocks:
  * 1.3.1.3, from 2.2.2.2, 00:00:01 ago, via Ethernet1/1, merge-labels
      Route metric is 20, traffic share count is 1
      MPLS label: 16003
      MPLS Flags: NSF
```

オンデマンドネクストホップのためのルーティング情報ベースのサポート

オンデマンドネクストホップ（ODN）要件の場合、RIBは、ルーティングプロトコル（BGP）をサポートすることによって提供されるバインディング ラベルと呼ばれるネクスト ホップをサポートします。FIB は、バインディング ラベルを使用してネクスト ホップを動的に解決します。

ルートプロデューサは、ネクストホップに関連付けられたODNトンネルパスを識別するローカル バインディング ラベルをインストールします。ラベル付きトラフィックは、トンネルを介して送信され、ラベルは既存のアウトラベルとは区別されます。

次に、各ネクスト ホップがバインディング ラベルを表示するように更新される **show ip route** コマンドの出力例を示します。

```
Device# show ip route 10.10.10.2

Routing entry for 10.10.10.2/32
  Known via "isis", distance 115, metric 10, type level-1
  Redistributing via isis
  Last update from 200.200.200.2 on Ethernet0/0, 00:00:14 ago
  Incoming Label: 16100
  Routing Descriptor Blocks:
  * 200.200.200.2, from 10.10.10.2, 00:00:14 ago, via Ethernet0/0
      Route metric is 10, traffic share count is 1
      * Binding Label 4020, from 2.2.2.2, 00:00:14 ago,
      Route metric is 10, traffic share count is 1
```

（注） 受信ラベルは、SIDの再配布が有効になった後にのみ表示されます。

ルーティング情報ベースの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 Command List, All Releases』

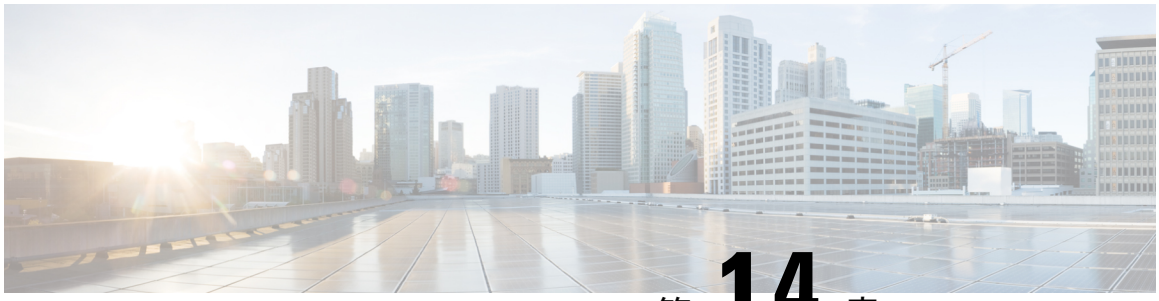
ルーティング情報ベースのサポートの機能情報

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 *12 :* ルーティング情報ベースのサポートの機能情報

機能名	リリース	機能情報
ルーティング情報ベースのサポート	Cisco IOS XE Everest 16.5.1b	ルーティング情報ベース（RIB）拡張は、ルート再配布およびオンデマンドネクストホップ要件をサポートします。 新しく追加または変更されたコマンドはありません。
OSPF ノード SID 再配布のサポート	Cisco IOS XE Fuji 16.7.1	Cisco IOS XE Fuji 16.7.1 リリースでは以前のケースとは異なり、OSPF が他の IGP から再配布されたプレフィックスを受信し、その逆にプレフィックスセグメント識別子（SID）もアドバタイズされます。IGP ドメイン間で SID を学習するには、BGP LS（または）セグメントルーティング マッピング サーバ（SRMS）のサポートが必要です。 この機能のために、**show ip ospf rib redistribution detail**、**show ip ospf segment-routing local-prefix**、**show ip ospf segment-routing sid-database**、**show ip route 3.3.3.3** コマンドが導入または変更されました。



第 14 章

SR-TE オン デマンド LSP

SR TE オン デマンド LSP 機能は、宛先へのスタティック ルートを経由してメトロ アクセス リングを接続する機能を提供します。スタティック ルートは明示的なパスにマップされ、宛先へのオン デマンド LSP をトリガーします。SR TE オン デマンド LSP 機能は、メトロ アクセス リング間の VPN サービスの転送に使用されます。

SR-TE オン デマンド LSP の制約事項

- セグメントルーティング自動トンネル スタティック ルートは ECMP をサポートしていません。
- IP 明示的パスのメトリクスおよび自動トンネル SRTE スタティック ルートのアドミニストレーティブ ディスタンスの変更はサポートされていません。
- MPLS トラフィック エンジニアリング（TE）ノンストップ ルーティング（NSR）は、ステートフル スイッチオーバー（SSO）のためにアクティブ ルート プロセッサ（RP）で設定する必要があります。これは、スタティック ルート自動トンネル設定を削除して再設定しない限り、SSO の後に SR スタティック自動トンネルが起動しなくなるためです。
- IP アンナンバード インターフェイスは動的パスをサポートしません。
- IP アンナンバード インターフェイスを使用する場合、ネクスト ホップ アドレスを明示的パスのインデックスとして指定することはできません。これは、ノードアドレスまたはラベルである必要があります。

SR-TE オン デマンド LSP に関する情報

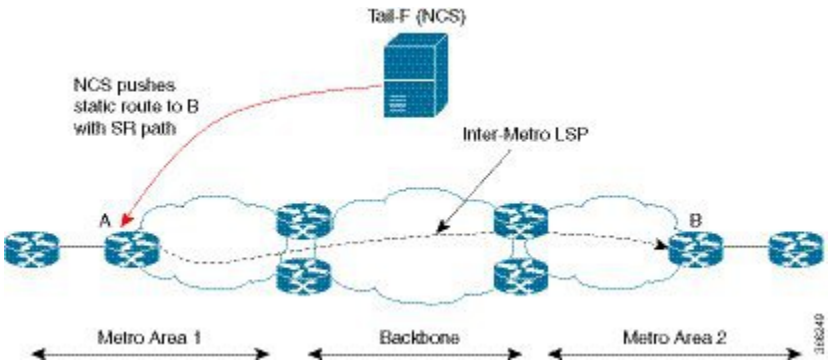
SR TE オン デマンド LSP 機能は、宛先へのスタティック ルートを経由してメトロ アクセス リングを接続する機能を提供します。

SR-TE：スタティック ルートとして LSP をセットアップする

アジャイル キャリア イーサネット（ACE）ソリューションは、統合 VPN サービスのためにセグメント ルーティングベースのトランスポートを活用します。メトロ リング アーキテクチャでは、アクセス リングはルーティング トポロジを互いに共有しません。

SR TE オン デマンド LSP 機能は、宛先へのスタティック ルートを経由してメトロ アクセス リングを接続する機能を提供します。スタティック ルートは明示的なパスにマップされ、宛先へのオン デマンド LSP をトリガーします。SR TE オン デマンド LSP 機能は、メトロ アクセス リング間の VPN サービスの転送に使用されます。

図 *18 : ACE* ソリューションにおけるメトロ間 *LSP*



メトロ間 LSP には、次のような側面があります。

- 送信元パケットが宛先デバイスの IP アドレスを知らない可能性があります。
- 既存のセグメント ルーティング機能を LSP に適用できます。

バインディング SID は、SR-TE トンネル内のトラフィックをステアリングするのに役立ちます。つまり、バインディング SID を持つ入力 MPLS パケットは、特定の SR-TE トンネルを介して転送されます。

アンナンバード インターフェイス上のスタティック SRTE

前のセクションで説明したように、LSP をスタティック ルートとして設定して、IP 明示的パスを指定することで自動トンネルを作成できます。

明示パスとは、IP アドレス（または）IP アドレスとラベルの組み合わせです。また、アンナンバードインターフェイス上でスタティック SRTE トンネルを設定することもできます。ナン

バード インターフェイスに対するアンナンバード インターフェイスの制限はほとんどありません。

- IP 明示パス オプションでネクスト ホップ インターフェイス アドレスではなく、ノードの IP アドレスを指定する必要があります。
- 明示パス オプションで隣接関係 SID を指定することはできません。つまり、明示パス オプションには、ノードの IP アドレス（/32 マスク）とプレフィックス SID ラベルのみが含まれている必要があります。

SR-TE オン デマンド LSP の設定方法

SR-TE のオン デマンド LSP を設定するには、次のステップを実行します。

スタティック ルートとしての LSP の設定

SR TE による RP スイッチオーバー後のパケット ドロップを回避するには、次のコマンドを使用することをお勧めします。

```
mpls traffic-eng nsr
```

ISIS が設定されている場合は、次のコマンドを使用します。

```
router isis
 nsf cisco
 nsf interval 0
```

セグメント ルーティング自動トンネル スタティック ルートの有効化

このタスクを実行して、次のように自動トンネル スタティック ルートを設定します。

- IP 明示パスを設定します
- IP 明示パスを持つ自動トンネルをスタティック ルートに関連付けます
- ピアツーピア（P2P）自動トンネルサービスを有効にします

```
ip explicit-path name path1
 index 1 next-label 16002
 index 2 next-label 16006
 exit
ip route 172.16.0.1 255.240.0.0 segment-routing mpls path name path1
mpls traffic-eng auto-tunnel p2p
mpls traffic-eng auto-tunnel p2p config unnumbered-interface loopback0
mpls traffic-eng auto-tunnel p2p tunnel-num min 10 max 100
```

セグメント ルーティング自動トンネル スタティック ルートの確認

コマンド **show mpls traffic-eng service summary** は、TE 自動トンネルを使用するすべての登録済み TE サービス クライアントおよび統計を表示します。

```
Device# show mpls traffic-eng service summary

Service Clients Summary:
  Client: BGP TE
    Client ID                 :0
    Total P2P tunnels         :1
    P2P add requests          :6
    P2P delete requests       :5
    P2P add falis             :0
    P2P delete falis          :0
    P2P notify falis          :0
    P2P notify succs          :12
    P2P replays               :0
  Client: ipv4static
    Client ID                 :1
    Total P2P tunnels         :1
    P2P add requests          :6
    P2P delete requests       :5
    P2P add falis             :0
    P2P delete falis          :0
    P2P notify falis          :0
    P2P notify succs          :85
    P2P replays               :0
```

コマンド **show mpls traffic-eng auto-tunnel p2p** は、ピアツーピア（P2P）自動トンネルの設定と操作状態を表示します。

```
Device# show mpls traffic-eng auto-tunnel p2p

State: Enabled
  p2p auto-tunnels: 2 (up: 2, down: 0)
  Default Tunnel ID Range: 62336 - 64335
  Config:
   unnumbered-interface: Loopback0
   Tunnel ID range: 1000 - 2000
```

コマンド **show mpls traffic-eng tunnel summary** は、P2P 自動トンネルの状態を表示します。

```
Device# show mpls traffic-eng tunnel summmary

Signalling Summary:
    LSP Tunnels Process:            running
    Passive LSP Listener:           running
    RSVP Process:                   running
    Forwarding:                     enabled
    auto-tunnel:
        p2p    Enabled  (1), id-range:1000-2000
    Periodic reoptimization:        every 3600 seconds, next in 1265 seconds
    Periodic FRR Promotion:         Not Running
    Periodic auto-bw collection:    every 300 seconds, next in 66 seconds
    SR tunnel max label push:       13 labels
    P2P:
      Head: 11 interfaces,   5234 active signalling attempts, 1 established
            5440 activations,  206 deactivations
            1821 failed activations
            0 SSO recovery attempts, 0 SSO recovered
      Midpoints: 0, Tails: 0
    P2MP:
      Head: 0 interfaces,   0 active signalling attempts, 0 established
            0 sub-LSP activations,  0 sub-LSP deactivations
            0 LSP successful activations,  0 LSP deactivations
            0 SSO recovery attempts, LSP recovered: 0 full, 0 partial, 0 fail
```

```
      Midpoints: 0, Tails: 0
Bidirectional Tunnel Summary:
    Tunnel Head: 0 total, 0 connected, 0 associated, 0 co-routed
    LSPs Head:   0 established, 0 proceeding, 0 associated, 0 standby
    LSPs Mid:    0 established, 0 proceeding, 0 associated, 0 standby
    LSPs Tail:   0 established, 0 proceeding, 0 associated, 0 standby

AutoTunnel P2P Summary:
    ipv4static:
        Tunnels: 1 created, 1 up, 0 down
    Total:
        Tunnels: 1 created, 1 up, 0 down
```

コマンド **show mpls traffic-eng tunnel auto-tunnel** は、TE サービス自動トンネルのみを表示します。

```
Device# show mpls traffic-eng tunnel auto-tunnel detail

 P2P TUNNELS/LSPs:

Name: R1_t1000                             (Tunnel1000) Destination: 0.0.0.0 Ifhandle:
0x17 (auto-tunnel for ipv4static)
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 1, (SEGMENT-ROUTING) type explicit (verbatim) path202 (Basis for Setup)

  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    Path Selection:
     Protection: any (default)
    Path-selection Tiebreaker:
      Global: not set   Tunnel Specific: not set   Effective: min-fill (default)
    Hop Limit: disabled [ignore: Verbatim Path Option]
    Cost Limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear
    AutoRoute: disabled LockDown: disabled Loadshare: 0 [0] bw-based
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: explicit path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: enabled

  History:
    Tunnel:
      Time since created: 33 days, 20 hours, 29 minutes
      Time since path change: 10 days, 19 hours, 45 minutes
      Number of LSP IDs (Tun_Instances) used: 1646
    Current LSP: [ID: 1646]
      Uptime: 10 days, 19 hours, 45 minutes
    Prior LSP: [ID: 1645]
      ID: path option unknown
      Removal Trigger: signalling shutdown
  Tun_Instance: 1646
  Segment-Routing Path Info (IGP information is not used)
    Segment0[First Hop]: 0.0.0.0, Label: 16002
    Segment1[ - ]: Label: 16006
```

コマンド **show mpls traffic-eng tunnel brief** は、自動トンネルの情報を表示します。

```
Device# show mpls traffic-eng tunnel brief

Signalling Summary:
    LSP Tunnels Process:            running
    Passive LSP Listener:           running
    RSVP Process:                   running
    Forwarding:                     enabled
    auto-tunnel:
        p2p    Enabled  (2), id-range:1000-2000

    Periodic reoptimization:        every 3600 seconds, next in 406 seconds
    Periodic FRR Promotion:         Not Running
    Periodic auto-bw collection:    every 300 seconds, next in 107 seconds
    SR tunnel max label push:       13 labels

P2P TUNNELS/LSPs:
TUNNEL NAME                       DESTINATION      UP IF     DOWN IF   STATE/PROT
R1_t1                             66.66.66.66      -         -         up/down
R1_t2                             66.66.66.66      -         -         up/up
R1_t3                             66.66.66.66      -         -         up/up
R1_t10                            66.66.66.66      -         -         up/up
SBFD tunnel                       33.33.33.33      -         -         up/up
SBFD Session configured: 1        SBFD sessions UP: 1
```

SR-TE オン デマンド LSP 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 Command List, All Releases』

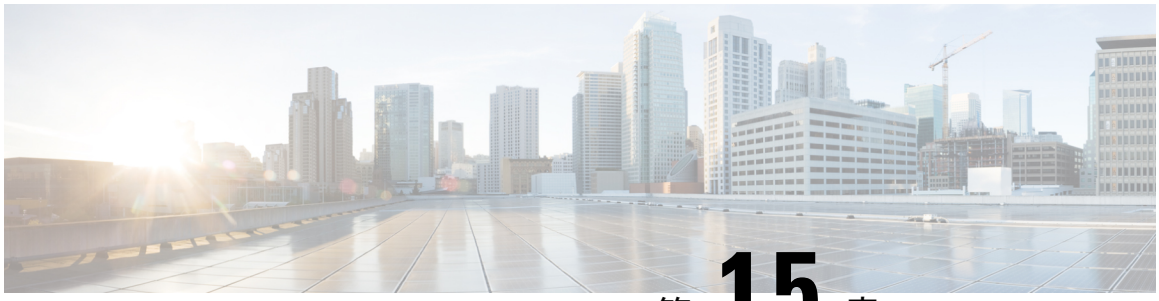
SR-TE オン デマンド LSP の機能情報

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 : SR-TE* オン デマンド *LSP* の機能情報

機能名	リリース	機能情報
SR-TE オン デマンド LSP	Cisco IOS XE Everest 16.5.1b	SR TE オン デマンド LSP 機能は、宛先へのスタティック ルートを経由してメトロ アクセス リングを接続する機能を提供します。スタティック ルートは明示的なパスにマップされ、宛先へのオン デマンド LSP をトリガーします。SR TE オン デマンド LSP 機能は、メトロ アクセス リング間の VPN サービスの転送に使用されます。 **mpls traffic-eng auto-tunnel** コマンドが変更されました。



第 15 章

セグメント ルーティング MPLS OAM のサポート

セグメントルーティング保守運用管理（OAM）は、ネットワークの障害検出とトラブルシューティングに役立ちます。これを使用することで、サービス プロバイダーはラベル スイッチド パス（LSP）をモニタしてフォワーディングの問題を迅速に隔離できます。セグメント ルーティング OAM 機能では、Nil-FEC（フォワーディング等価クラス）LSP Ping および Traceroute、IGP プレフィックス SID FEC タイプ、および SR-TE 機能のための部分的な IGP 隣接関係 SID FEC タイプのサポートを提供します。

セグメントルーティング OAM MPLS サポートの制約事項

- Ping と traceroute は、SR-TE スタティック自動トンネル、BGP ダイナミック TE、およびオンデマンド ネクスト ホップ自動トンネルではサポートされていません。
- Strict-SID オプションは、OSPF によってインストールされたパスではサポートされません。
- MPLS traceroute は、1 つのノードで 2 つの明示的ヌル ラベルのポップをサポートしません。

- IP ルーティングの宛先が MPLS FEC ではないため、レイヤ 3 VPN を使用せずに、MPLS セグメント経由で IP へのパスを再ルーティングすることはサポートされていません。

セグメント ルーティング MPLS OAM サポートに関する情報

セグメント ルーティング OAM サポート

Nil-FEC LSP ping および traceroute の操作は、通常の MPLS ping および traceroute の拡張機能です。Nil-FEC LSP Ping/Trace 機能は、セグメント ルーティングと MPLS スタティックをサポートしています。また、他のすべての LSP タイプに対する追加の診断ツールとしても機能します。この機能は、オペレータがラベル スタックをテストして以下を指定できるようにします。

- ラベル スタック
- 発信インターフェイス
- ネクストホップ アドレス

セグメント ルーティングの場合、ルーティング パスに沿った各セグメント ノード ラベルおよび隣接関係ラベルは、イニシエータのラベル スイッチ ルータ（LSR）からのエコー要求メッセージのラベル スタックに入れられます。MPLS データ プレーンは、このパケットをラベル スタック ターゲットに転送し、ラベル スタック ターゲットはエコー メッセージを送り返します。

セグメント ルーティング OAM サポートの利点

- この機能により、トラフィックが SR-TE トンネルまたはネイティブ SR フォワーディングを介してエンジニアリングされるセグメント ルーティング ネットワークの MPLS OAM 機能が有効になります。
- 従来の MPLS ネットワークでは、ソース ノードは、LDP または RSVP-TE のようなホップ バイ ホップ シグナリング プロトコルに基づいてパスを選択します。セグメント ルーティング ネットワークでは、パスは IGP プロトコル（現在は OSPF および ISIS）によってアドバタイズされるセグメントのセットによって指定されます。
- SR を使用して提供されるサービスの量が増加するため、オペレータが本質的に SR アーキテクチャの接続検証と障害分離を行うことができることが重要です。
- セグメントの割り当ては、従来の MPLS ネットワークのようにホップ バイ ホップ プロトコルに基づいていないため、切断された中継ノードがトラフィックのブラックホール化を引き起こし、望ましくない動作を引き起こす可能性があります。
- SR と SR-TE はどちらもロード バランシングをサポートしていて、ソース ルータとターゲット ルータの間で利用可能なすべての ECMP パスをトレースすることが重要です。こ

の機能は、TE とネイティブ SR パスの両方に対してマルチパスの traceroute をサポートします。

- セグメント ルーティング OAM サポートの主な利点は次のとおりです。
  - **運用**：ネットワークのモニタリングおよび障害管理。
  - **管理**：ネットワークの検出と計画。
  - **メンテナンス**：訂正および予防のアクティビティにより、障害の発生と影響を最小限に抑えます。

セグメント ルーティング MPLS Ping

MPLS ping および traceroute は設計によって拡張可能です。SR サポートを追加するには、新しい FEC および/または追加の検証手順を定義します。MPLS ping は MPLS データ パスを検証し、次を実行します。

- エコー要求パケットを MPLS ラベルにカプセル化します。
- 低密度ラウンド トリップ時間を測定します。
- 低密度ラウンド トリップ遅延を測定します。

セグメント ルーティング MPLS Traceroute

MPLS ping および traceroute は設計によって拡張可能です。SR サポートを追加するには、新しい転送等価クラス（FEC）および/または追加の検証手順を定義します。MPLS traceroute は、LSP の各ホップでフォワーディング プレーンおよびコントロール プレーンを検証して、障害を切り分けます。traceroute は、TTL 1 から始まり単調増加する存続可能時間（TTL）で MPLS エコー要求を送信します。TTL の有効期限が過ぎると、中継ノードはソフトウェアで要求を処理し、ターゲット FEC と目的の中継ノードへの LSP があるかどうかを確認します。中継ノードは、検証が成功した場合、ネクストホップに到達するための上記の検証とラベルスタックの結果を指定するリターンコードと、宛先に向かうネクストホップの ID を含むエコー応答を送信します。発信元は、TTL + 1 を含む次のエコー要求をビルドするためにエコー応答を処理します。宛先が FEC の出力であると応答するまで、プロセスが繰り返されます。

Nil FEC ターゲットに対する LSP Ping 操作

LSP Ping/Traceroute は LSP 破損の識別に使用されます。nil-fec ターゲット型は、既知のラベル スタックの接続性をテストするために使用できます。既存の LSP ping 手順に従います（詳細については、「MPLS Lsp ping/Traceroute」を参照してください）。ただし以下を変更します。

- 指定されたラベル スタックを使用してエコー要求パケットをビルドします。
- ラベル スタックの下部に明示的 null ラベルを追加します。

- ターゲットの FEC Nil FEC とラベルの値が明示的 null であるラベル スタックの下部のラベルに設定されているエコー要求 FTS TLV をビルドします。

LSP Ping およびトレース ルート Nil FEC ターゲットを使用してセグメント ルーティングを診断する方法

Nil FEC ターゲットに対する LSP Ping の使用

Nil FEC LSP ping および traceroute の操作は、単に通常の MPLS ping および traceroute の拡張機能です。**nil-fec labels <label, label…>** が ping mpls コマンドに追加されます。このコマンドは、指定に応じて MPLS ラベル スタックを使用してエコー要求メッセージを送信し、スタックの最下部に別の明示的ヌルを追加します。

```
ping mpls nil-fec labels <comma separated labels> output interface <tx-interface> nexthop
 <nexthop ip addr>
[repeat <count>]
[size <size> | sweep <min_size> <max_size> <increment>]
[timeout <seconds>]
[interval <milliseconds>]
[destination <addr_start> [<addr_end> [<addr_incr_mask> | <addr_incr>]]]
[source <addr>]
[exp <exp-value>]
[pad <pattern>]
[ttl <ttl>]
[reply [mode [ipv4 | router-alert | no-reply]]
[dscp <dscp-bits>]
[pad-tlv]]
[verbose]
[force-disposition ra-label]
{dsmap | ddmap [l2ecmp]} [hashkey {none | {ipv4 | ipv4-label-set {bitmap <bitmap_size>}}]
```

詳細については、「ping mpls」を参照してください。

Nil FEC ターゲットに対する LSP Traceroute の使用

```
trace mpls nil-fec labels <comma separated labels> output interface <tx-interface>}
nexthop <nexthop ip addr>
[timeout <seconds>]
[destination <addr_start> [<addr_end> [<addr_incr_mask> | <addr_incr>]]]
[source <addr> ]
[exp <exp-value>]
[ttl <ttl-max>]
[reply [mode [ipv4 | router-alert | no-reply]]
[dscp <dscp-bits>]
[pad-tlv]]
[flags {fec | ttl}]
[hashkey ipv4 | ipv4-label-set {bitmap <bitmap_size>}]
```

詳細については、「traceroute mpls」を参照してください。

LSP Ping Nil FEC ターゲットのサポートの例

```
Node loopback IP address: 1.1.1.3              1.1.1.4                1.1.1.5
       1.1.1.7
Node label:                                     16004                   16005
        16007
Nodes:                    Arizona ---------------- Utah  ---------------- Wyoming
---------------- Texas
Interface:                      Eth1/0        Eth1/0
Interface IP address:          30.1.1.3      30.1.1.4

Device#sh mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  3333.3333.0000-Et1/0-30.1.1.3   \
                                       0             Et1/0      30.1.1.3
17         Pop Label  5555.5555.5555-Et1/1-90.1.1.5   \
                                       0             Et1/1      90.1.1.5
18         Pop Label  3333.3333.0253-Et0/2-102.102.102.2   \
                                       0             Et0/2      102.102.102.2
19         Pop Label  9.9.9.4/32       0             Et0/2      102.102.102.2
20         Pop Label  1.1.1.5/32       0             Et1/1      90.1.1.5
21         Pop Label  1.1.1.3/32       0             Et1/0      30.1.1.3
22         Pop Label  16.16.16.16/32   0             Et1/0      30.1.1.3
23         Pop Label  16.16.16.17/32   0             Et1/0      30.1.1.3
24         Pop Label  17.17.17.17/32   0             Et1/0      30.1.1.3
25         20         9.9.9.3/32       0             Et1/0      30.1.1.3
26         21         1.1.1.6/32       0             Et1/0      30.1.1.3
27         24         1.1.1.2/32       0             Et1/0      30.1.1.3
           28         1.1.1.2/32       0             Et1/1      90.1.1.5
28         18         1.1.1.7/32       0             Et1/1      90.1.1.5
29         27         9.9.9.7/32       0             Et1/1      90.1.1.5
30         Pop Label  55.1.1.0/24      0             Et1/1      90.1.1.5
31         Pop Label  19.1.1.0/24      0             Et1/0      30.1.1.3
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
32         Pop Label  100.1.1.0/24     0             Et1/0      30.1.1.3
33         Pop Label  100.100.100.0/24 0             Et1/0      30.1.1.3
34         Pop Label  110.1.1.0/24     0             Et1/0      30.1.1.3
35         28         10.1.1.0/24      0             Et1/0      30.1.1.3
36         29         101.101.101.0/24 0             Et1/0      30.1.1.3
37         29         65.1.1.0/24      0             Et1/1      90.1.1.5
38         33         104.104.104.0/24 0             Et1/0      30.1.1.3
           39         104.104.104.0/24 0             Et1/1      90.1.1.5
39         30         103.103.103.0/24 0             Et1/1      90.1.1.5
16005      Pop Label  1.1.1.5/32       1782          Et1/1      90.1.1.5
16006      16006      1.1.1.6/32       0             Et1/0      30.1.1.3
16007      16007      1.1.1.7/32       0             Et1/1      90.1.1.5
16017      16017      17.17.17.17/32   0             Et1/0      30.1.1.3
16250      16250      9.9.9.3/32       0             Et1/0      30.1.1.3
16252      16252      9.9.9.7/32       0             Et1/1      90.1.1.5
16253      Pop Label  9.9.9.4/32       0             Et0/2      102.102.102.2
17000      17000      16.16.16.16/32   0             Et1/0      30.1.1.3
17002      17002      1.1.1.2/32       0             Et1/0      30.1.1.3
           17002      1.1.1.2/32       0             Et1/1      90.1.1.5

Device#ping mpls nil-fec labels 16005,16007 output interface ethernet 1/0 nexthop 30.1.1.4
 repeat 1
Sending 1, 72-byte MPLS Echos with Nil FEC labels 16005,16007,
     timeout is 2 seconds, send interval is 0 msec:
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms
 Total Time Elapsed 0 ms


Device#traceroute mpls nil-fec labels 16005,16007 output interface ethernet 1/0 nexthop
 30.1.1.4
Tracing MPLS Label Switched Path with Nil FEC labels 16005,16007, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
  0 30.1.1.3 MRU 1500 [Labels: 16005/16007/explicit-null Exp: 0/0/0]
L 1 30.1.1.4 MRU 1500 [Labels: implicit-null/16007/explicit-null Exp: 0/0/0] 1 ms
L 2 90.1.1.5 MRU 1500 [Labels: implicit-null/explicit-null Exp: 0/0] 1 ms
! 3 55.1.1.7 1 ms
```

セグメント ルーティング ネットワークのパス検証

MPLS OAM メカニズムは、MPLS エコー要求パケットで運ばれて FEC 検証のためにレスポンダによって使用されるさまざまなターゲット FEC スタックサブ TLV の使用によって、MPLS データプレーン パスのための障害検出および分離に役立ちます。新しいサブ TLV をセグメント ルーティングに割り当てる必要があることは明らかですが、セグメント ルーティング アーキテクチャの固有の性質により、パスの検証に関して追加の運用上の考慮が必要になります。

隣接関係セグメント ID の転送セマンティックは、セグメント ID をポップし、特定のリンクを介して特定のネイバーにパケットを送信することです。誤動作しているノードは、隣接関係セグメント ID を使用して、誤ったネイバーへまたは誤ったリンク上でパケットを転送することがあります。（誤って転送された隣接関係セグメント ID の）リスクにさらされているセグメント ID では、目的の厳格なトラバーサルが壊れているにもかかわらず、パケットが目的の宛先に到達できる可能性があります。MPLS traceroute はそのような逸脱の検出の役に立つ場合があります。

次のセグメント ID サブ TLV の形式は、ラベル スタック内の各ラベルに対応する FEC を運ぶターゲット FEC スタック TLV の原理に従います。これにより、ターゲット FEC スタック TLV に要求先ノードで受信したラベル スタックよりも多くの FEC が含まれている場合に LSP ping/traceroute 操作を機能させることができます。ターゲット FEC スタック TLV（タイプ 1）、

リバースパス ターゲット FEC スタック TLV（タイプ 16）、および応答パス TLV（タイプ 21）には、3 つの新しいサブ TLV が定義されています。

sub-Type	Value Field
34	IPv4 IGP-Prefix Segment ID
35	IPv6 IGP-Prefix Segment ID
36	IGP-Adjacency Segment ID

IGP プレフィックス SID FEC タイプ用の MPLS Ping および Traceroute

プレフィックス SID 用の MPLS ping および traceroute の操作は、次のようなさまざまな IGP シナリオでサポートされています。

- IS-IS レベルまたは OSPF エリア内
- IS-IS レベルまたは OSPF エリア間
- IS-IS から OSPF へ、および OSPF から IS-IS へのルート再配布

MPLS LSP ping 機能を使用して、LSP に沿った入力ラベル スイッチ ルータ（LSR）と出力 LSR 間の接続を確認します。MPLS LSP ping は、Internet Control Message Protocol（ICMP）のエコー要求メッセージと応答メッセージと同様に、LSP の検証に MPLS エコーの要求メッセージと応答メッセージを使用します。MPLS エコー要求パケットの宛先 IP アドレスは、ラベル スタックの選択に使用されるアドレスとは異なります。

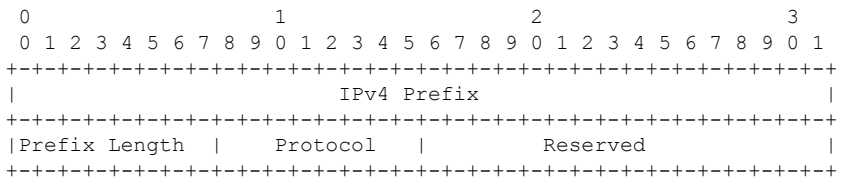
MPLS LSP traceroute 機能を使用して、LSP の障害ポイントを隔離します。これはホップバイホップ エラーのローカリゼーションとパス トレースに使用されます。MPLS LSP traceroute 機能は、エコー要求を伝送するパケットの存続可能時間（TTL）値の期限切れに依存します。MPLS エコー要求メッセージが中継ノードを見つけると TTL 値をチェックし、期限が切れている場合はコントロールプレーンにパケットが渡されます。それ以外の場合は、メッセージが転送されます。エコー メッセージがコントロール プレーンに渡されると、要求メッセージの内容に基づいて応答メッセージが生成されます。

MPLS LSP ツリー トレース（traceroute マルチパス）操作は、IGP プレフィックス SID でもサポートされています。MPLS LSP ツリー トレースでは、LSP のすべての可能な等コスト マルチパス（ECMP）ルーティング パスを検出して宛先プレフィックス SID に到達する手段が提供されます。エコー要求パケットにエンコードされたマルチパス データを使用して、ロードバランシング情報が照会されます。これにより、発信者は各 ECMP の実行を許可される場合があります。パケット TTL が応答ノードで期限切れになると、ノードはダウンストリーム パスのリストとマルチパス情報を返します。これにより、オペレータは MPLS エコー応答内の各パスを実行できるようになります。この操作は、すべての ECMP が検出されて検証されるまで、TTL 値が増加しながら各パスのホップごとに繰り返し実行されます。

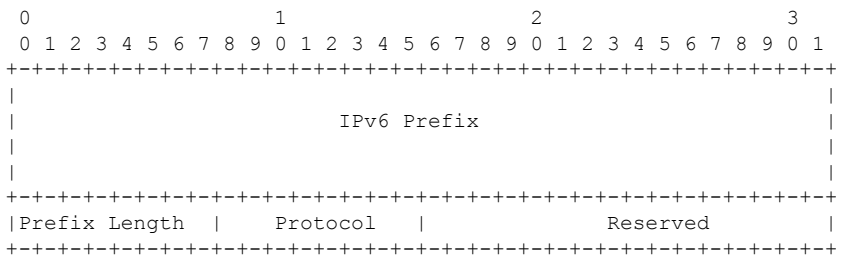
MPLS エコー要求パケットは、ターゲット FEC スタック サブ TLV を伝送します。ターゲット FEC サブ TLV は、レスポンダによって FEC 検証のために使用されます。IGPIPv4 プレフィックス サブ TLV がターゲット FEC スタック サブ TLV に追加されました。IGP IPv4 プレフィックス サブ TLV には、プレフィックス SID、プレフィックス長、およびプロトコル（IS-IS または OSPF）が含まれています。

ノード セグメント ID をアドバタイズしたネットワーク ノードは、PHP（Penultimate Hop Popping）が有効かどうかに関係なく、ノード セグメント ID の pop 操作タイプを持つ FEC スタック変更サブ TLV を生成します。

IPv4 IGP プレフィックス セグメント ID の形式は次のとおりです。



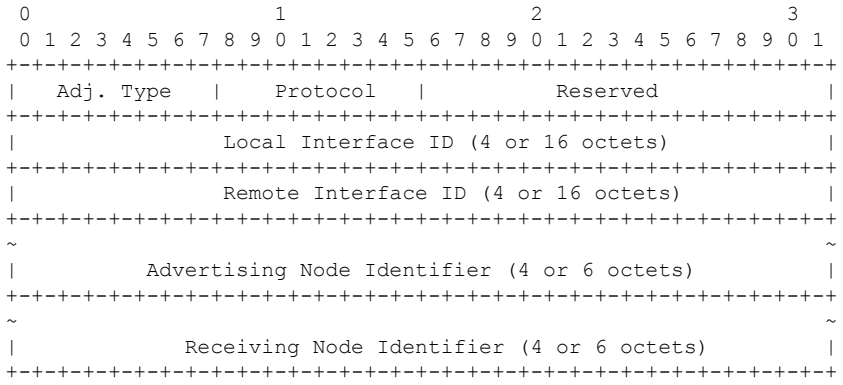
IPv6 IGP プレフィックス セグメント ID の形式は次のとおりです。



IGP 隣接セグメント ID 用の MPLS Ping および Traceroute

隣接関係セグメント ID をアドバタイズしたノードのすぐ下流にあるネットワーク ノードは、隣接関係セグメント ID の「POP」操作のための FEC スタック変更サブ TLV を生成します。

IGP 隣接関係 SID の形式は次のとおりです。



MPLS Ping および Traceroute 用のセグメント ルーティング MPLS トラフィック エンジニアリングの設定

```
ping mpls traffic-eng tunnel <tun-id>
[repeat <count>]
[size <size> | sweep <min_size> <max_size> <increment>]
[timeout <seconds>]
[interval <milliseconds>]
[destination <addr_start> [<addr_end> [<addr_incr_mask> | <addr_incr>]]]
[source <addr>]
[exp <exp-value>]
[pad <pattern>]
[ttl <ttl>]
[reply [mode [ipv4 | router-alert | no-reply]]
[dscp <dscp-bits>]
[pad-tlv]]
[verbose]
[output {interface <tx-interface>} [nexthop <nexthop ip addr>]]
[{dsmap | ddmap [l2ecmp]} [hashkey {none | {ipv4 | ipv4-label-set {bitmap <bitmap_size>}}]

traceroute mpls [multipath] traffic-eng <tunnel-interface>
[timeout <seconds>]
[destination <addr_start> [<addr_end> [<addr_incr_mask> | <addr_incr>]]]
[source <addr> ]
[exp <exp-value>]
[ttl <ttl-max>]
[reply [mode [ipv4 | router-alert | no-reply]]
[pad-tlv]]
[output {interface <tx-interface>} [nexthop <nexthop ip addr>]]
[flags {fec | ttl}]
[hashkey ipv4 | ipv4-label-set {bitmap <bitmap_size>}]
```

MPLS Ping および Traceroute 用のセグメント ルーティング MPLS IGP の設定

```
ping mpls ipv4 <prefix/prefix_length> [fec-type [ldp | bgp | generic | isis | ospf]]
[sr-path-type [ip | sid | strict-sid]]
[destination <addr_start> [<addr_end> [<addr_incr_mask> | <addr_incr>]]]
[source <addr>]
[exp <exp-value>]
[pad <pattern>]
[ttl <ttl>]
[reply [mode [ipv4 | router-alert | no-reply]]
[dscp <dscp-bits>]
[pad-tlv]]
[verbose]
[output {interface <tx-interface>} [nexthop <nexthop ip addr>]]
[{dsmap | ddmap [l2ecmp]} [hashkey {none | {ipv4 | ipv4-label-set {bitmap <bitmap_size>}}]

traceroute mpls [multipath] ipv4 <prefix/prefix_length> [fec-type [ldp | bgp | generic
| isis | ospf]] [sr-path-type [ip | sid | strict-sid]]
[timeout <seconds>]
[destination <addr_start> [<addr_end> [<addr_incr_mask> | <addr_incr>]]]
```

```
[source <addr> ]
[exp <exp-value>]
[ttl <ttl-max>]
[reply [mode [ipv4 | router-alert | no-reply]]
[pad-tlv]]
[output {interface <tx-interface>} [nexthop <nexthop ip addr>]]
[flags {fec | ttl}]
[hashkey ipv4 | ipv4-label-set {bitmap <bitmap_size>}]
```

- fec-type：IPv4 ターゲット FEC タイプ。デフォルトでヘッド エンド自動検出 FEC タイプを使用します。
- sr-path-type：セグメント ルーティング パスのタイプの選択アルゴリズム。オプションが指定されている場合は、IP インポジション パスを使用します。

Cisco IOS CLI を使用したセグメント ルーティング OAM の確認

このセクションでは、セグメント ルーティング OAM 機能を検証するために必要な、主要なコマンド ライン インターフェイス（CLI）についての要約を示します。ping および traceroute コマンドは IGP（OSPF SR）、ISIS SR および SR-TE での操作および出力を示します。実際のトンネル番号と IP アドレスは、設定で必要とされる有効な実際の値に基づいて変更します。

セグメント ルーティング トラフィック エンジニアリング OAM オペレーションの確認

次の **traceroute** コマンドは、SR-TE OAM 操作を表示します。

```
SR_Device#traceroute mpls traffic-eng tunnel 1005 verbose
Tracing MPLS TE Label Switched Path on Tunnel1005 Active LSP, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
  0 100.103.1.1 100.103.1.2 MRU 1500 [Labels: implicit-null/22/22 Exp: 0/0/0], RSC 0
l 1 100.103.1.2 103.104.1.2 MRU 1500 [Labels: implicit-null/22 Exp: 0/0] 3 ms, ret code
 15, RSC 0
l 2 103.104.1.2 104.105.1.2 MRU 1500 [Labels: implicit-null Exp: 0] 3 ms, ret code 15,
RSC 0
! 3 104.105.1.2 2 ms, ret code 3


SR_Device#traceroute mpls ipv4 55.5.5.5/32 output interface tunnel1 force-explicit-null
```

```
Tracing MPLS Label Switched Path to 55.5.5.5/32, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
  0 100.101.1.1 MRU 1500 [Labels: 26000/explicit-null Exp: 0/0]
L 1 100.101.1.2 MRU 1500 [Labels: 26000/explicit-null Exp: 0/0] 3 ms
L 2 101.104.1.2 MRU 1500 [Labels: implicit-null/explicit-null Exp: 0/0] 6 ms
! 3 104.105.1.2 3 ms
```

次の **tree traceroute** コマンドは、ECMP シナリオでの SR-TE OAM 操作を表示します。

```
SR_Device#traceroute mpls multi traffic-eng tunnel 1 verbose
Starting LSP Multipath Traceroute for Tunnel1
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
LL!
Path 0 found,
output interface Gi2 nexthop 100.101.1.2
source 50.0.0.0 destination 127.0.0.0
0 100.101.1.1 100.101.1.2 MRU 1500 [Labels: 26000 Exp: 0] multipaths 0
L 1 100.101.1.2 101.102.1.2 MRU 1500 [Labels: 26000 Exp: 0] ret code 8, RSC 0 multipaths
 2
L 2 101.102.1.2 102.105.1.2 MRU 1500 [Labels: implicit-null Exp: 0] ret code 8, RSC 0
multipaths 1
! 3 102.105.1.2, ret code 3 multipaths 0
L!
Path 1 found,
output interface Gi2 nexthop 100.101.1.2
source 50.0.0.0 destination 127.0.0.1
0 100.101.1.1 100.101.1.2 MRU 1500 [Labels: 26000 Exp: 0] multipaths 0
L 1 100.101.1.2 101.104.1.2 MRU 1500 [Labels: 26000 Exp: 0] ret code 8, RSC 0 multipaths
 2
L 2 101.104.1.2 104.105.1.2 MRU 1500 [Labels: implicit-null Exp: 0] ret code 8, RSC 0
multipaths 1
! 3 104.105.1.2, ret code 3 multipaths 0
LL!
Path 2 found,
output interface Gi3 nexthop 100.103.1.2
source 50.0.0.0 destination 127.0.0.0
0 100.103.1.1 100.103.1.2 MRU 1500 [Labels: 26000 Exp: 0] multipaths 0
L 1 100.103.1.2 102.103.1.1 MRU 1500 [Labels: 26000 Exp: 0] ret code 8, RSC 0 multipaths
 2
L 2 102.103.1.1 102.105.1.2 MRU 1500 [Labels: implicit-null Exp: 0] ret code 8, RSC 0
multipaths 1
! 3 102.105.1.2, ret code 3 multipaths 0
L!
Path 3 found,
output interface Gi3 nexthop 100.103.1.2
source 50.0.0.0 destination 127.0.0.1
```

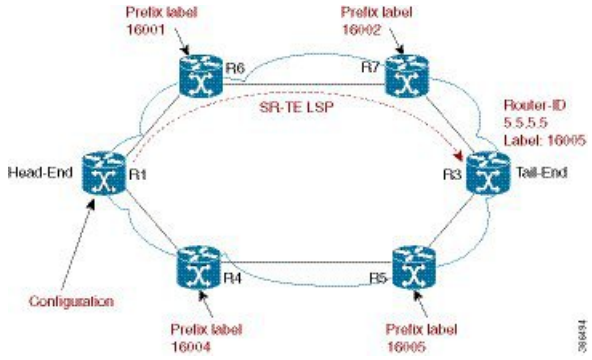
```
0 100.103.1.1 100.103.1.2 MRU 1500 [Labels: 26000 Exp: 0] multipaths 0
L 1 100.103.1.2 103.104.1.2 MRU 1500 [Labels: 26000 Exp: 0] ret code 8, RSC 0 multipaths
 2
L 2 103.104.1.2 104.105.1.2 MRU 1500 [Labels: implicit-null Exp: 0] ret code 8, RSC 0
multipaths 1
! 3 104.105.1.2, ret code 3 multipaths 0
Paths (found/broken/unexplored) (4/0/0)
Echo Request (sent/fail) (10/0)
Echo Reply (received/timeout)
```

CLI を使用したセグメント ルーティング OAM OSPF の確認

IGP 境界にまたがるプレフィックスに対して ping または traceroute を実行する場合は、特に fec タイプを指定する必要があります。たとえば、プレフィックスが ISIS ドメインから OSPF に再配布されるときは、fec タイプ ISIS を指定します。ping または traceroute が IGP ドメイン内で実行されるときは、明示的に fec タイプを言及する必要はありません。ユーザが宛先ノードで IGP プロトコルを知らない場合に汎用の fec タイプ ジェネリックを提供します。SR パスのタイプが記載されていない場合、デフォルトの SR パスのタイプ IP が採用されます。

次のトポロジは、SR パスのタイプの例です。

図 *19 :*



以下の ping コマンドは、基盤となるネットワークが OSPF の場合の SR OAM を説明するために使用されます。

上記のトポロジの例に従って、ヘッド エンド R1 では、SR-TE トンネルは宛先を R3 として作成されます。SR-TE トンネルは、R6 および R7 を通過するための明示的パス オプションを使用して作成されます。IP トラフィックが R1 で入力された場合、SR-TE パスは R1---R6----R7----R3 です。

```
Device#ping mpls ipv4 4.4.4.4/32 fec-type ospf sr-path-type ip verbose
Sending 2, 72-byte MPLS Echos to IGP Prefix SID(OSPF) FEC 5.5.5.5/32,
     timeout is 2 seconds, send interval is 0 msec:
Select segment routing IP imposition path.

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
```

```
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
!    size 72, reply addr 2.4.0.4, return code 3
!    size 72, reply addr 2.4.0.4, return code 3

Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
 Total Time Elapsed 4 ms
```

同じトポロジで、着信トラフィックにトラフィックのラベルが付いている場合、次の 2 つの ECMP パスが転送用に選択されます。

- R1---R6----R7----R3
- R1---R4----R5----R3

（注） マルチパス オプションを使用して、両方のパスを宛先に対してトレースすることができます。

```
Device# ping mpls ipv4 4.4.4.4/32 fec-type ospf sr-path-type sid verbose
Sending 1, 72-byte MPLS Echos to IGP Prefix SID(OSPF) FEC 5.5.5.5/32,
     timeout is 2 seconds, send interval is 0 msec:
Select segment routing prefix SID path.

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
!    size 72, reply addr 2.4.0.4, return code 3

Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms
 Total Time Elapsed 3 ms
```

次の **traceroute** コマンドは、基盤となるネットワークが OSPF の場合の SR OAM を表示します。

R1 への着信トラフィックがネイティブ IP である場合に IP ルート パスをトレースするために、R1 の終わりで以下のコマンドが使用されます。

```
Device#traceroute mpls ipv4 4.4.4.4/32 fec-type ospf sr-path-type ip verbose
Tracing MPLS Label Switched Path to IGP Prefix SID(OSPF) FEC 4.4.4.4/32, timeout is 2
seconds
Select segment routing IP imposition path.

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
 0 1.2.0.1 1.2.0.2 MRU 1500 [Labels: 16002/16005 Exp: 0/0], RSC 0

L 1 1.2.0.2 3.3.3.3 MRU 1500 [Labels: 16005 Exp: 0] 2 ms, ret code 8, RSC 0

L 2 3.3.3.3 3.4.0.4 MRU 1500 [Labels: implicit-null Exp: 0] 1 ms, ret code 8, RSC 0

! 3 3.4.0.4 1 ms, ret code 3


Device#traceroute mpls ipv4 4.4.4.4/32 fec-type ospf sr-path-type sid  verbose


Device#traceroute mpls multipath ipv4 4.4.4.4/32  fec-type ospf sr-path-type ip verbose
Type escape sequence to abort.
LL!
Path 0 found,
 output interface Et0/1 nexthop 1.2.0.2                              //path R1-R6-R7-R3
 source 1.1.1.1 destination 127.0.0.0
  0 1.2.0.1 1.2.0.2 MRU 1500 [Labels: 16666 Exp: 0] multipaths 0
L 1 1.2.0.2 2.4.0.4 MRU 1500 [Labels: 16666 Exp: 0] ret code 8, RSC 0 multipaths 1
L 2 2.4.0.4 4.6.0.6 MRU 1500 [Labels: implicit-null Exp: 0] ret code 8, RSC 0 multipaths
 1
! 3 4.6.0.6, ret code 3 multipaths 0
LL!
Path 1 found,
 output interface Et0/2 nexthop 1.3.0.3                              //path R1-R4-R5-R3

 source 1.1.1.1 destination 127.0.0.0
  0 1.3.0.1 1.3.0.3 MRU 1500 [Labels: 16666 Exp: 0] multipaths 0
L 1 1.3.0.3 3.4.0.4 MRU 1500 [Labels: 16666 Exp: 0] ret code 8, RSC 0 multipaths 1
L 2 3.4.0.4 4.6.0.6 MRU 1500 [Labels: implicit-null Exp: 0] ret code 8, RSC 0 multipaths
 1
! 3 4.6.0.6, ret code 3 multipaths 0

Paths (found/broken/unexplored) (2/0/0)
 Echo Request (sent/fail) (6/0)
 Echo Reply (received/timeout) (6/0)
 Total Time Elapsed 23 ms


Device#traceroute mpls multipath ipv4 4.4.4.4/32 fec-type ospf sr-path-type sid verbose
```

CLI を使用したセグメント ルーティング OAM IS-IS の確認

次の **ping** コマンドは、基盤となるネットワークが IS-IS の場合の SR OAM を表示するために使用されます。

```
Device# ping mpls ipv4 4.4.4.4/32 fec-type isis sr-path-type ip verbose

Device# ping mpls ipv4 4.4.4.4/32 fec-type isis sr-path-type sid verbose

Device# ping mpls ipv4 4.4.4.4/32 fec-type isis sr-path-type strict-sid verbose

Device# ping mpls ipv4 4.4.4.4/32 sr-path-type ip verbose

Device# ping mpls ipv4 4.4.4.4/32 sr-path-type sid verbose
```

```
Device# ping mpls ipv4 4.4.4.4/32 sr-path-type strict-sid verbose
```

次の **traceroute** コマンドは、基盤となるネットワークが IS-IS の場合の SR OAM を表示します。マルチパス オプションを有効にすると、すべての ECMP パスが返されます。

```
Device# traceroute mpls ipv4 4.4.4.4/32 fec-type isis sr-path-type ip verbose

Device# traceroute mpls ipv4 4.4.4.4/32 fec-type isis sr-path-type sid  verbose

Device# traceroute mpls ipv4 4.4.4.4/32 fec-type isis sr-path-type strict-sid verbose

Device# traceroute mpls multipath ipv4 4.4.4.4/32  fec-type isis sr-path-type ip verbose


Device# traceroute mpls multipath ipv4 4.4.4.4/32 fec-type isis sr-path-type sid verbose


Device# traceroute mpls multipath ipv4 4.4.4.4/32 fec-type isis sr-path-type strict-sid
 verbose
```

IGP セグメント ID の MPLS Ping および Traceroute の確認

IGP の検証で次のコマンド SR ネットワークを使用します。

```
ping|traceroute mpls [multipath] ipv4 <prefix> [fec-type bgp |generic|ldp|isis|ospf]
[sr-path-type ip|sid|strict-sid]
```

トンネル LSP が SR-TE LSP である場合は次のコマンドを使用して MPLS TE トンネル OAM を確認します。

```
ping|traceroute mpls traffic-eng tunnel <tunnelid>
```

セグメント ルーティング OAM 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』

セグメント ルーティング OAM サポートの機能情報

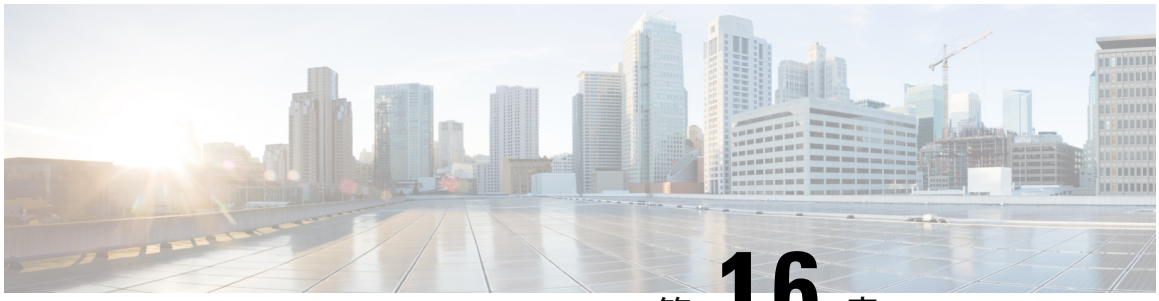
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

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* : セグメント ルーティング *OAM* サポートの機能情報

機能名	リリース	機能情報
セグメント ルーティング OAM サポート	Cisco IOS XE Release 3.17 S	セグメント ルーティング OAM 機能では、Nil-FEC（転送等価クラス）LSP Ping および Traceroute 機能のサポートを提供します。 Nil-FEC LSP ping および traceroute の操作は、単に通常の MPLS ping および traceroute の拡張機能です。
CLI を使用したセグメント ルーティング OAM の確認	Cisco IOS XE Everest 16.6.1 Cisco IOS XE Fuji 16.7.1	この機能は、セグメント ルーティング OAM 機能を検証するために必要なコマンド ライン インターフェイス（CLI）を提供します。ping および traceroute コマンドは IGP（OSPF SR、IS-IS SR）および SR-TE での操作および出力を表示します。 次のコマンドが導入または変更されました。 **ping mpls ipv4 4.4.4.4/32 fec-type isis sr-path-type ip verbose**、**ping mpls ipv4 4.4.4.4/32 fec-type isis sr-path-type sid verbose**、**ping mpls ipv4 4.4.4.4/32 fec-type isis sr-path-type strict-sid verbose**、**ping mpls ipv4 4.4.4.4/32 fec-type ospf sr-path-type ip verbose**、**ping mpls ipv4 4.4.4.4/32 fec-type ospf sr-path-type sid verbose**、**traceroute mpls traffic-eng tunnel 1005 verbose**、**traceroute mpls ipv4 55.5.5.5/32 output interface tunnel1 force-explicit-null**、**traceroute mpls ipv4 4.4.4.4/32 fec-type ospf sr-path-type ip verbose**、**traceroute mpls ipv4 4.4.4.4/32 fec-type ospf sr-path-type sid verbose**、**traceroute mpls multipath ipv4 4.4.4.4/32 fec-type ospf sr-path-type sid verbose**。 Cisco IOS XE Fuji 16.7.1 では、この機能は Cisco 4000 シリーズ サービス統合型ルータでサポートされています。



第 16 章

セグメント ルーティングでのシームレス BFD の使用

セグメント ルーティング TE 機能は、シームレスな双方向フォワーディング検出（S-BFD）のための情報サポートを提供します。

セグメントルーティングでのシームレス BFD 使用の制約事項

シームレス双方向フォワーディング（S-BFD）の制約事項

- シームレス双方向フォワーディング（S-BFD）は、セグメント ルーティング トラフィック エンジニアリング（SR-TE）では IPv4 のみをサポートしています。IPv6 はサポートされていません。
- シングル ホップの S-BFD セッションのみサポートされています。
- RSVP-TE は、S-BFD をサポートしていません。

セグメントルーティングでのシームレスBFDに関する情報

双方向フォワーディング検出とシームレス双方向フォワーディング検出（S-BFD）

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。

BFDは高速転送パス障害検出に加えて、ネットワーク管理者向けの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。

シームレス双方向フォワーディング検出（S-BFD）は、ネゴシエーションの側面の大部分が排除されたBFDを使用する単純化されたメカニズムであり、迅速なプロビジョニング、ネットワーク ノードが開始するパスの監視の制御と柔軟性の向上などの利点を提供します。

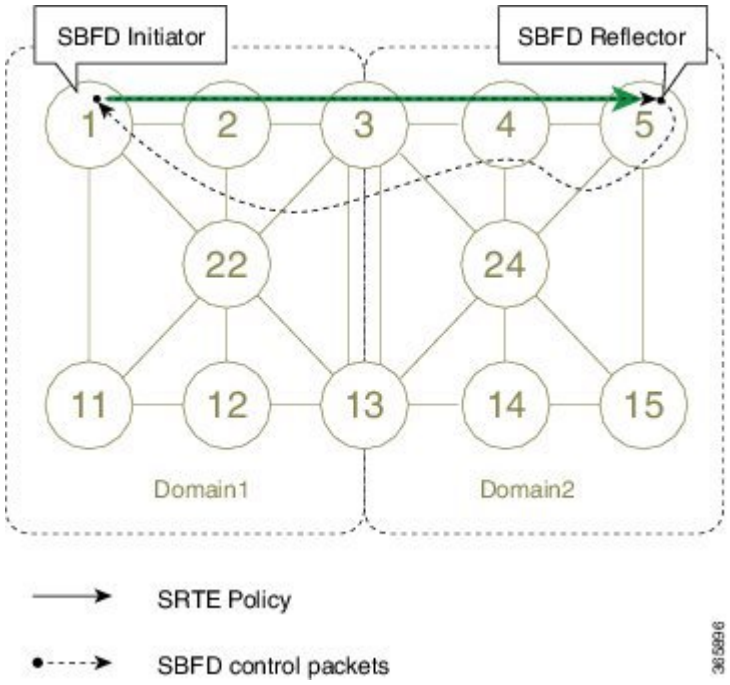
SBFDセッションが失敗した場合、S-BFDはSR-TEセッションをダウンさせます。また、S-BFDは、制御パケットの交換が少ないため、より高速なセッションの起動を提供します。S-BFDはSR-TE と関連付けられ、セッションを迅速に起動します。BFD 状態はヘッド エンドでのみ維持され、それによってオーバーヘッドが減少します。

S-BFD は、セグメント ルーティングで RFC 7880、RFC 7881 のサポートを実装しています。

イニシエータとリフレクタ

SBFD はイニシエータとリフレクタを使用して非対称的な動作をします。次の図は、SBFD イニシエータとリフレクタの役割を示しています。

図 *20 : SBFD* イニシエータとリフレクタ



イニシエータは、ネットワーク ノード上の SBFD セッションであり、SBFD パケットを送信することによってリモートエンティティへの連続性テストを実行します。イニシエータは、SBFD パケットをセグメントルーティング トラフィックエンジニアリング（SRTE）ポリシーに挿入します。イニシエータは、SBFDセッションをトリガーし、BFD状態およびクライアントコンテキストを維持します。

リフレクタは、ローカル エンティティへの着信 SBFD 制御パケットをリッスンし、応答 SBFD 制御パケットを生成するネットワーク ノード上の SBFD セッションです。リフレクタはステートレスで、SBFD パケットのみをイニシエータに反映します。

ノードはイニシエータとリフレクタの両方になることができるため、異なる SBFD セッションを設定できます。

S-BFD は SR-TE IPv4 で有効でありサポート対象ですが、IPv6 はサポートされていません。
SR-TE の場合、S-BFD 制御パケットは、前方向および逆方向にラベル スイッチされます。
S-BFD の場合、テール エンドはリフレクタ ノードです。その他のノードをリフレクタにすることはできません。SR-TE で S-BFD を使用するとき、フォワードとリターンの方向がラベル スイッチド パスである場合は、S-BFD をリフレクタ ノードで設定する必要はありません。

セグメントルーティングでのシームレスBFDの設定方法

セグメント ルーティングのシームレス双方向フォワーディング検出（S-BFD）の設定

S-BFD は、イニシエータとリフレクタの両方のノードで有効にする必要があります。

（注） SR-TE で S-BFD を使用するとき、フォワードとリターンの方向がラベル スイッチド パスである場合は、S-BFD をリフレクタ ノードで設定する必要はありません。

リフレクタ ノードでのシームレス双方向フォワーディング検出（S-BFD）の有効化

リフレクタ ノードで S-BFD を設定するには、このタスクを実行します。

```
sbfd local-discriminator 55.55.55.55
```

イニシエータ ノードでのシームレス双方向フォワーディング検出（S-BFD）の有効化

イニシエータ ノードで S-BFD を設定するには、このタスクを実行します。

```
bfd-template single-hop ABC
 interval min-tx 300 min-rx 300 multiplier 10
```

シームレス双方向フォワーディング（S-BFD）でのセグメント ルーティング トラフィック エンジニアリング トンネルの有効化

```
interface Tunnel56
 ip unnumbered Loopback11
 tunnel mode mpls traffic-eng
 tunnel destination 55.55.55.55 */IP address of Reflector node/*
 tunnel mpls traffic-eng path-option 1 dynamic segment-routing
 tunnel mpls traffic-eng bfd sbfd ABC
!
end
```

S-BFD 設定の確認

手順の概要

1. **show mpls traffic-engineering tunnel** *tunnel-name*
2. **show bfd neighbors**

手順の詳細

ステップ 1 **show mpls traffic-engineering tunnel** *tunnel-name*

SR TE の状態と、S-BFD セッションの状態を確認します。

例：

```
Router# sh mpls traffic-eng tunnel tunnel 56

    Name: R1_t56                              (Tunnel56) Destination: 55.55.55.55
      Status:
        Admin: up         Oper: up     Path: valid       Signalling: connected
        path option 1, (SEGMENT-ROUTING) type dynamic (Basis for Setup, path weight 12)

      Config Parameters:
        Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
        Metric Type: TE (default)
        Path Selection:
         Protection: any (default)
        Path-selection Tiebreaker:
          Global: not set   Tunnel Specific: not set   Effective: min-fill (default)
        Hop Limit: disabled
        Cost Limit: disabled
        Path-invalidation timeout: 10000 msec (default), Action: Tear
        AutoRoute: disabled LockDown: disabled Loadshare: 0 [0] bw-based
        auto-bw: disabled
        Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No

      SBFD configured with template: ABC
        Session type: CURRENT        State: UP       SBFD handle: 0x3
        LSP ID: 1
        Last uptime duration: 3 minutes, 35 seconds
        Last downtime duration: --
          Active Path Option Parameters:
        State: dynamic path option 1 is active
        BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
      Node Hop Count: 2
          History:
        Tunnel:
          Time since created: 4 minutes, 3 seconds
          Number of LSP IDs (Tun_Instances) used: 1
        Current LSP: [ID: 1]
          Uptime: 3 minutes, 36 seconds
      Tun_Instance: 1
      Segment-Routing Path Info (isis  level-2)
        Segment0[Link]: 12.12.12.1 - 12.12.12.2, Label: 48
        Segment1[Link]: 25.25.25.2 - 25.25.25.5, Label: 35 !
```

ステップ 2 show bfd neighbors

BFD ネイバーが正しく確立されていることを確認します。

例：

```
Router# show bfd neighbors

    MPLS-TE SR Sessions
    Interface      LSP ID(Type)                  LD/RD         RH/RS     State
    Tunnel56          1 (SR)                  4097/926365495  Up        Up
```

セグメントルーティングでのシームレスBFDに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セグメント ルーティング トラフィック エンジニアリングの設定	セグメント ルーティング - トラフィック エンジニアリング

表 *15* : 標準および *RFC*

標準/RFC	タイトル
draft-akiya-bfd-seamless-base-03	シームレス双方向フォワーディング検出（S-BFD）
draft-ietf-isis-segment-routing-extensions-07	セグメント ルーティング対応の IS-IS 拡張
draft-ietf-spring-segment-routing-09	セグメント ルーティング アーキテクチャ
RFC 7880	シームレス双方向フォワーディング検出（S-BFD）
RFC 7881	IPv4、IPv6、および MPLS 用のシームレス双方向フォワーディング検出（S-BFD）

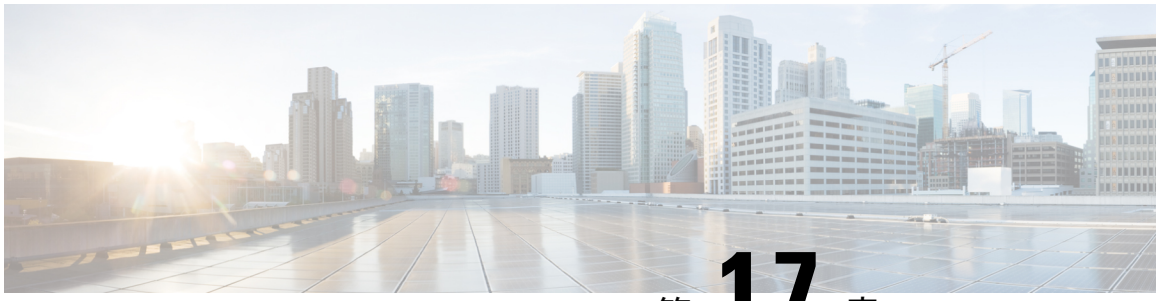
セグメントルーティングでのシームレスBFDに関する機能情報

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 *16* : セグメント ルーティング *TE* 機能の機能情報

機能名	リリース	機能情報
セグメント ルーティング TE の機能	Cisco IOS XE Denali 16.4.1	シームレス双方向フォワーディング検出（S-BFD）は、ネゴシエーションの側面の大部分が排除された BFD を使用する単純化されたメカニズムであり、迅速なプロビジョニング、ネットワーク ノードが開始するパスの監視の制御と柔軟性の向上などの利点を提供します。 次のコマンドが導入または変更されました。**address-family ipv4 strict-spf**、**bfd-template single-hop**、**index range**、**sbfd local-discriminator**、**show bfd neighbor**、**show isis segment-routing**、**show mpls forwarding-table**、**show mpls traffic tunnel**、**show mpls traffic-engineering**。



第 17 章

セグメント ルーティングでの SSPF の使用

セグメント ルーティング TE 機能は、厳格な最短パス優先（SPF）の情報サポートを提供します。

セグメント ルーティングでの SSPF に関する情報

厳格な最短パス優先

セグメント ルーティングは、次の 2 つのアルゴリズムをサポートします。

- アルゴリズム 0：これは、リンク メトリックに基づく最短パス優先（SPF）アルゴリズムです。この最短パス アルゴリズムは、内部ゲートウェイ プロトコル（IGP）によって計算されます。
- アルゴリズム 1：これは、リンク メトリックに基づく厳格な最短パス優先（SSPF）アルゴリズムです。アルゴリズム 1 はアルゴリズム 0 と同じですが、パスに沿ったすべてのノードが SPF ルーティングの決定を遵守することを必要とします。ローカル ポリシーは、転送の決定を変更しません。たとえば、パケットはローカルに設計されたパスを通じて転送されません。

アルゴリズムごとに異なる SID が同じプレフィックスに関連付けられます。

厳格な最短パス優先はデフォルトでサポートされていますが、厳格な SID を、セグメント ルーティングをサポートする各ノードで少なくとも 1 つのノード アドレスに対して設定する必要があります。

厳格な最短パス優先を設定するためのアプローチ

厳格な SFP を設定するには、次の 2 つの方法があります。

- **connect-prefix-sid-map** コマンドを使用する：厳格な SFP はすべてのノードでグローバルに設定されます。ネットワークを厳格な SFP 対応にする（つまり、ISIS で厳格な SPF を入力するため）場合、すべてのノードをローカルの厳格な SFP SID で設定する必要があります。
- セグメント ルーティング マッピング サーバを使用する：ネットワーク内の 1 つのノードがマッピング サーバとして設定され、残りのノードはクライアントとして機能します。

セグメント ルーティングでの SSPF の設定方法

厳格な最短パス優先（SPF）の設定

connect-prefix-sid-map コマンドを使用した厳格な最短パス優先の有効化

プロバイダーエッジ デバイスでの最短パス優先の有効化

connect-prefix-sid-map コマンドを使用して厳格な最短パス優先を有効にする場合は、最初にプロバイダーエッジデバイスで、次にノードデバイスで、厳格な最短パス優先（SPF）を設定する必要があります。次に示すのは、プロバイダーエッジデバイスで厳格な最短パス優先を有効にするための設定コード スニペットのサンプルです。

```
segment-routing mpls
connected-prefix-sid-map
  address-family ipv4
   10.10.10.10/32 index 100 range 1
  exit-address-family
  address-family ipv4 strict-spf
   10.10.10.10/32 index 1000 range 1 ------------------configure strict SPF locally
  exit-address-family
```

ノード デバイスでの最短パス優先の有効化

次に示すのは、ネットワーク内のノードで厳格な最短パス優先を有効にするための設定コード スニペットのサンプルで、ネットワーク内のすべてのノードで有効にする必要があります。

```
segment-routing mpls
connected-prefix-sid-map
  address-family ipv4
   20.20.20.20/32 index 110 range 1
  exit-address-family
  address-family ipv4 strict-spf
   20.20.20.20/32 index 1100 range 1
  exit-address-family
```

セグメント ルーティング マッピング サーバを使用した厳格な最短パス優先の有効化

セグメント ルーティング マッピング サーバとしてのノードの設定

次に示すのは、ノードをセグメント ルーティング マッピング サーバとして設定するための設定コード スニペットのサンプルです。

```
segment-routing mpls
mapping-server
  prefix-sid-map
   address-family ipv4
    10.10.10.10/32 index 100 range 1
    20.20.20.20/32 index 110 range 1
    30.30.30.30/32 index 120 range 1
    40.40.40.40/32 index 130 range 1
    50.50.50.50/32 index 140 range 1
   exit-address-family
   address-family ipv4 strict-spf
    10.10.10.10/32 index 1000 range 1
    20.20.20.20/32 index 1100 range 1
    30.30.30.30/32 index 1200 range 1
    40.40.40.40/32 index 1300 range 1
    50.50.50.50/32 index 1400 range 1
    100.100.100.100/32 index 2000 range 1
   exit-address-family
```

ローカル プレフィックスをアドバタイズおよび受信するようにセグメント ルーティング マッピング サーバの設定

次に示すのは、ローカルプレフィックスをアドバタイズおよび受信するようにセグメント ルーティング マッピング サーバを設定するための設定コード スニペットのサンプルです。

```
router isis SR
segment-routing mpls
 segment-routing prefix-sid-map advertise-local
 segment-routing prefix-sid-map receive
```

ISIS の SID のアドバタイズの確認

次に示すのは、ISIS が SID をアドバタイズしていることを確認するための設定コード スニペットのサンプルです。

```
Router# show isis segment-routing prefix-sid-map advertise strict-spf
Tag SR:
IS-IS Level-1 advertise prefix-sid maps:
Prefix               SID Index    Range        Flags
10.10.10.10/32       1000         1
20.20.20.20/32       1100         1
30.30.30.30/32       1200         1
40.40.40.40/32       1300         1
50.50.50.50/32       1400         1
100.100.100.100/32   2000         1
Tag SR:
IS-IS Level-2 advertise prefix-sid maps:
Prefix               SID Index    Range        Flags
10.10.10.10/32       1000         1
20.20.20.20/32       1100         1
30.30.30.30/32       1200         1
40.40.40.40/32       1300         1
50.50.50.50/32       1400         1
100.100.100.100/32   2000         1
```

次に示すのは、プロバイダーエッジ デバイスが SRMS サーバから厳格な最短パス優先の SID を受信することを確認するための設定コード スニペットのサンプルです。

```
Router# show isis segment-routing prefix-sid-map receive strict-spf

Tag SR:
IS-IS Level-1 receive prefix-sid maps:
Host                    Prefix               SID Index    Range        Flags
P1                      10.10.10.10/32       1000         1
                        20.20.20.20/32       1100         1
                        30.30.30.30/32       1200         1
                        40.40.40.40/32       1300         1
                        50.50.50.50/32       1400         1
                        100.100.100.100/32   2000         1
Tag SR:
IS-IS Level-2 receive prefix-sid maps:
Host                    Prefix               SID Index    Range        Flags
P1                      10.10.10.10/32       1000         1
                        20.20.20.20/32       1100         1
                        30.30.30.30/32       1200         1
                        40.40.40.40/32       1300         1
                        50.50.50.50/32       1400         1
                        100.100.100.100/32   2000         1
```

セグメント ルーティングでの SSPF 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 Command List, All Releases』
セグメント ルーティング トラフィック エンジニアリングの設定	セグメント ルーティング - トラフィック エンジニアリング

セグメント ルーティングでの SSPF 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 *17* : セグメント ルーティング *SSPF* 機能の機能情報

機能名	リリース	機能情報
セグメント ルーティング TE の機能	Cisco IOS XE Denali 16.4.1	セグメントルーティングTE機能は、厳格な最短パス優先（SPF）の情報サポートを提供します。 次のコマンドが導入または変更されました。**address-family ipv4 strict-spf**、**bfd-template single-hop**、**index range**、**sbfd local-discriminator**、**show bfd neighbor**、**show isis segment-routing**、**show mpls forwarding-table**、**show mpls traffic tunnel**、**show mpls traffic-engineering**。

第 18 章

ダイナミック PCC

ステートフル パス計算要素プロトコル（PCEP）により、ルータはステートフル パス計算要素（PCE）に対して、Resource Reservation Protocol（RSVP）プロトコルまたはセグメント ルーティング トラフィック エンジニアリング（SR-TE）のいずれかを使用して確立されたラベル スイッチド パス（LSP）をレポートし、必要に応じて委任することができます。

PCE に委任された LSP は、PCE によって更新でき、ステートフル PCE はパス計算クライアント（PCC）に LSP のパスを計算して提供することができます。

SR-TE および RSVP-TE LSP では、OSPF や ISIS などのリンクステート ルーティング プロトコルによって、トラフィック エンジニアリング トポロジを配布および学習する必要があります。ステートフル PCE では、BGP リンクステート プロトコルを使用してトラフィック エンジニアリング トポロジを学習できます。ネットワーク内のすべてまたは一部の中間ノードで TE の IGP 拡張がサポートされていない場合は、verbatim パス オプションを使用できます。

ダイナミック PCC に関する情報

パス計算要素プロトコル関数

パス計算要素プロトコル（PCEP）セッションは、プロトコル メッセージを使用した PCC と PCE の間の TCP セッションです。PCEP 関数は PCC 関数に基づいて検証されます。構成と検証により、要求が受け入れられ、クライアントからの PCReq メッセージに基づいてパスの計算が提供されることが示されます。パッシブ レポートでは、ルータは PCE に委任するのではなく、トンネルをレポートすることができます。PCEは、トンネルを変更できなくてもトンネルを認識しています。

PCEP 関数は、ルータが制御するトンネルと PCE 委任トンネルの両方ともネットワークにある場合に便利です。PCEは両方のトンネルを認識し、パス計算の正確な決定を行うことができます。

冗長パス計算要素

冗長性のために、冗長 PCE サーバの展開が必要になる場合があります。PCC は、LSP を委任するためにステートフルなPCE を選択するのに優先順位を使用します。優先順位は0から255の間の任意の値を取ることができます。デフォルトの優先順位は255です。アクティブなPCEPセッションを持つ複数のステートフルPCEがある場合、PCCは最も低い優先順位値を持つPCEを選択します。プライマリ PCE サーバ セッションがダウンした場合、PCC ルータは次に利用可能な PCE サーバにすべてのトンネルを再委任します。冗長 PCE の場合は、以下の CLI を使用できます。

```
R2(config)#mpls traffic-eng pcc peer 77.77.77.77 source 22.22.22.22 precedence 255
R2(config)#mpls traffic-eng pcc peer 88.88.88.88  source 22.22.22.22 precedence 100
!
end
```

上記の例では、IP アドレス 88.88.88.88 を持つ PCE サーバは、優先順位値が低いため、プライマリ PCE サーバです。

ダイナミック PCC の設定方法

ダイナミック PCC のグローバルな設定

ダイナミック PCC をグローバルに設定するには、次のタスクを実行します

```
enable
configure terminal
mpls traffic-eng tunnels
mpls traffic-eng pcc peer 10.0.0.1    ----□(10.0.0.1 is the PCE server address)
mpls traffic-eng pcc report-all
end
```

（注） **mpls traffic-eng pcc report-all** は、PCE/PCC 基本運用委任トンネルに必須ではありません。ローカルで計算された LSP を PCE サーバにレポートする必要があります。

インターフェイスでのダイナミック PCC の設定

インターフェイス上でダイナミック PCC を設定するには、次のタスクを実行します

```
interface Tunnel1
 ip unnumbered Loopback0
```

```
 tunnel mode mpls traffic-eng
 tunnel destination 7.7.7.7
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 5 5
 tunnel mpls traffic-eng bandwidth 200
 tunnel mpls traffic-eng path-option 10 dynamic pce segment-routing
end
```

Verbatim パス オプションを使用したダイナミック PCC の設定

verbatim パス オプションを使用してダイナミック PCC を有効にするには、SR-TE トンネル インターフェイスの下で次の CLI を使用します。

```
R1#
interface Tunnel2
ip unnumbered Loopback11
tunnel mode mpls traffic-eng
tunnel destination 66.66.66.66
tunnel mpls traffic-eng autoroute destination
tunnel mpls traffic-eng path-option 1 dynamic segment-routing pce verbatim
```

ダイナミック PCC の確認

次に、**show pce client peer detail** コマンドの出力例を示します。

```
Device# show pce client peer detail

PCC's peer database:
--------------------

Peer address: 1.1.1.1
  State up
  Capabilities: Stateful, Update, Segment-Routing
  PCEP has been up for: 23:44:58
  PCEP session ID: local 1, remote: 0
  Sending KA every 30 seconds
  Minimum acceptable KA interval: 20 seconds
  Peer timeout after 120 seconds
  Statistics:
    Keepalive messages: rx    2798 tx    2112
    Request messages:   rx       0 tx      32
    Reply messages:     rx      32 tx       0
    Error messages:     rx       0 tx       0
    Open messages:      rx       1 tx       1
    Report messages:    rx       0 tx      57
    Update messages:    rx      72 tx       0
```

次に、LSP の詳細を表示する **show mpls traffic-eng tunnels tunnel 1** コマンドの出力例を示します。

```
Device# show mpls traffic-eng tunnels tunnel 1

Name: d1_t1                           (Tunnel1) Destination: 7.7.7.7
  Status:
```

```
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, (SEGMENT-ROUTING) (PCE) type dynamic (Basis for Setup, path weight
0)

  Config Parameters:
    Bandwidth: 200      kbps (Global)  Priority: 5  5   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    Path Selection:
     Protection: any (default)
    Path-selection Tiebreaker:
      Global: not set   Tunnel Specific: not set   Effective: min-fill (default)
    Hop Limit: disabled
    Cost Limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 200 [10000000] bw-based
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: dynamic path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled

  PCEP Info:
    Delegation state: Working: yes   Protect: no
    Current Path Info:
      Request status: processed
      Created via PCRep message from PCE server: 1.1.1.1
    Reported paths:
      Tunnel Name: csr551_t2001
       LSPs:
        LSP[0]:
         source 2.2.2.2, destination 7.7.7.7, tunnel ID 1, LSP ID 5
         State: Admin up, Operation active
         Setup type: SR
         Bandwidth: signaled 0
         LSP object:
           PLSP-ID 0x807D1, flags: D:0 S:0 R:0 A:1 O:2
         Reported path:
           Metric type: TE, Accumulated Metric 0

  History:
    Tunnel:
      Time since created: 34 minutes, 3 seconds
      Time since path change: 1 minutes, 44 seconds
      Number of LSP IDs (Tun_Instances) used: 5
    Current LSP: [ID: 5]
      Uptime: 1 minutes, 44 seconds
    Prior LSP: [ID: 3]
      ID: path option unknown
      Removal Trigger: path verification failed
  Tun_Instance: 5
  Segment-Routing Path Info (isis  level-1)
    Segment0[Node]: 3.3.3.3, Label: 20270
    Segment1[Node]: 6.6.6.6, Label: 20120
    Segment2[Node]: 7.7.7.7, Label: 20210
```

次に、**show pce client lsp detail** コマンドの出力例を示します。

```
Device# show pce client lsp detail

PCC's tunnel database:
----------------------
Tunnel Name: d1_t1
 LSPs:
```

```
  LSP[0]:
   source 2.2.2.2, destination 7.7.7.7, tunnel ID 1, LSP ID 5
   State: Admin up, Operation active
   Setup type: SR
   Bandwidth: signaled 0
   LSP object:
     PLSP-ID 0x807D1, flags: D:0 S:0 R:0 A:1 O:2
   Reported path:
     Metric type: TE, Accumulated Metric 0
```

次に、トンネルの委任を示す **show pce lsp detail** コマンドの出力例を示します。

```
Device# show pce lsp detail

Thu Jul  7 10:24:30.836 EDT

PCE's tunnel database:
----------------------
PCC 102.103.2.1:

Tunnel Name: d1_t1
 LSPs:
  LSP[0]:
   source 2.2.2.2, destination 7.7.7.7, tunnel ID 1, LSP ID 5
   State: Admin up, Operation active
   Binding SID: 0
   PCEP information:
     plsp-id 526289, flags: D:1 S:0 R:0 A:1 O:2
   Reported path:
     Metric type: TE, Accumulated Metric 0
      SID[0]: Node, Label 20270, Address 3.3.3.3
      SID[1]: Node, Label 20120, Address 6.6.6.6
      SID[2]: Node, Label 20210, Address 7.7.7.7
   Computed path:
     Metric type: TE, Accumulated Metric 30
      SID[0]: Node, Label 20270, Address 3.3.3.3
      SID[1]: Node, Label 20120, Address 6.6.6.6
      SID[2]: Node, Label 20210, Address 7.7.7.7
   Recorded path:
     None
```

次に、レポートされたトンネルについての **show pce client lsp detail** コマンドの出力例を示します。

```
Device# show pce client lsp detail

PCC's tunnel database:
----------------------
Tunnel Name: d1_t2
 LSPs:
  LSP[0]:
   source 2.2.2.2, destination 7.7.7.7, tunnel ID 2, LSP ID 1
   State: Admin up, Operation active
   Setup type: SR
   Bandwidth: signaled 0
   LSP object:
     PLSP-ID 0x807D2, flags: D:0 S:0 R:0 A:1 O:2
   Reported path:
     Metric type: TE, Accumulated Metric 30
```

次に、トンネルが委任されていないことを示す **show pce lsp detail** コマンドの出力例を示します。

```
Device# show pce lsp detail

Thu Jul  7 10:29:48.754 EDT

PCE's tunnel database:
----------------------
PCC 10.0.0.1:

Tunnel Name: d1_t2
 LSPs:
  LSP[0]:
   source 2.2.2.2, destination 7.7.7.7, tunnel ID 2, LSP ID 1
   State: Admin up, Operation active
   Binding SID: 0
   PCEP information:
     plsp-id 526290, flags: D:0 S:0 R:0 A:1 O:2
   Reported path:
     Metric type: TE, Accumulated Metric 30
      SID[0]: Adj, Label 74, Address: local 172.16.0.1 remote 172.16.0.2
      SID[1]: Adj, Label 63, Address: local 173.17.0.1 remote 173.17.0.2
      SID[2]: Adj, Label 67, Address: local 174.18.0.1 remote 174.18.0.2
      SID[3]: Node, Label unknownAddress 7.7.7.7
   Computed path:
     None
   Recorded path:
     None
```

ダイナミック PCC を使用した Verbatim パス オプションの確認

verbatim パス オプションを使用して適切な操作を確認するには、次のコマンドを使用します。

```
R1#sh mpl tr tun tun 2
Name: R1_t2                                (Tunnel2) Destination: 66.66.66.66
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 1, (SEGMENT-ROUTING) (PCE) type dynamic (verbatim) (Basis for Setup)

  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
    Metric Type: TE (interface)
    Path Selection:
     Protection: any (default)
    Path-selection Tiebreaker:
      Global: not set   Tunnel Specific: not set   Effective: min-fill (default)
    Hop Limit: disabled [ignore: Verbatim Path Option]
    Cost Limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear
    AutoRoute: disabled LockDown: disabled Loadshare: 0 [0] bw-based
    AutoRoute destination: enabled
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
```

```
    State: dynamic path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: enabled

  PCEP Info:
    Delegation state: Working: yes   Protect: no
    Delegation peer: 77.77.77.77
    Working Path Info:
      Request status: processed
      Created via PCRep message from PCE server: 77.77.77.77
      PCE metric: 4, type: TE
    Reported paths:
      Tunnel Name: Tunnel2_w
       LSPs:
        LSP[0]:
         source 11.11.11.11, destination 66.66.66.66, tunnel ID 2, LSP ID 1
         State: Admin up, Operation active
         Binding SID: 17
         Setup type: SR
         Bandwidth: requested 0, used 0
         LSP object:
           PLSP-ID 0x80002, flags: D:0 S:0 R:0 A:1 O:2
         ERO:
           SID[0]: Adj, Label 24, NAI: local 12.12.12.1 remote 12.12.12.2
           SID[1]: Adj, Label 26, NAI: local 25.25.25.2 remote 25.25.25.5
           SID[2]: Adj, Label 22, NAI: local 56.56.56.5 remote 56.56.56.6

  History:
    Tunnel:
      Time since created: 39 days, 19 hours, 9 minutes
      Time since path change: 1 minutes, 3 seconds
      Number of LSP IDs (Tun_Instances) used: 1
    Current LSP: [ID: 1]
      Uptime: 1 minutes, 3 seconds
  Tun_Instance: 1
  Segment-Routing Path Info (IGP information is not used)
    Segment0[Link]: 12.12.12.1 - 12.12.12.2, Label: 24
    Segment1[Link]: 25.25.25.2 - 25.25.25.5, Label: 26
    Segment2[Link]: 56.56.56.5 - 56.56.56.6, Label: 22
!
end
```

ダイナミック PCC に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

ダイナミック PCC の機能情報

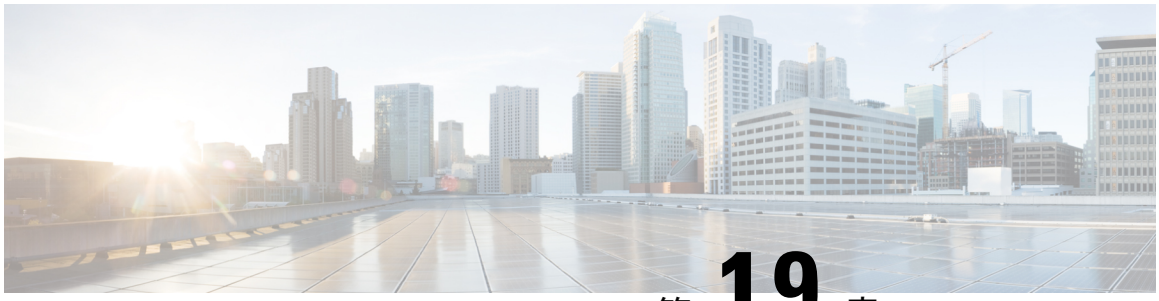
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

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 *18* : ダイナミック *PCC* の機能情報

機能名	リリース	機能情報
ダイナミック PCC	Cisco IOS XE Everest 16.6.1	動的パス計算クライアント（PCC）機能は、パス計算要素（PCE）に委任された LSP をサポートします。ダイナミック PCC は、RSVP-TE と SR-TE の両方をサポートします。 次のコマンドが追加または修正されました。 **show pce client peer detail**、 **show mpls traffic-eng tunnels tunnel 1**、 **show pce client lsp detail**、**show pce lsp detail**。



第 19 章

SR：PCE 開始の LSP

SR：PCE 開始の LSP 機能は、セグメント ルーティング ネットワーク上のステートフル PCE モデルで PCE によって開始される LSP をサポートします。

SR の前提条件：PCE 開始の LSP

- ダイナミック PCC 機能を設定する必要があります。
- 自動トンネルを PCC で有効にする必要があります。

SR の制約事項：PCE 開始の LSP

- SR：PCE 開始 LSP 機能は、基本的な LSP の生成のみをサポートし、TE の属性をサポートしていません。

SR に関する情報：PCE 開始の LSP

パス計算要素プロトコルの概要

draft-ietf-pce-stateful-pce-21 で説明されているステートフル パス計算要素プロトコル（PCEP）により、ルータはステートフル パス計算要素（PCE）に対して、Resource Reservation Protocol（RSVP）プロトコルまたはセグメントルーティング トラフィック エンジニアリング（SR-TE）のいずれかを使用して確立されたラベル スイッチド パス（LSP）をレポートし、必要に応じて

SR：PCE 開始の LSP

委任することができます。PCE に委任された LSP は、PCE によって更新でき、ステートフル PCE はパス計算クライアント（PCC）に LSP のパスを計算して提供することができます。

ステートフル PCE モデル（draft-ietf-pce-pce-initiated-lsp-11）において PCE 開始 LSP 設定のための PCEP 拡張は、RFC4657 に準拠した PCEP セッション全体で TE LSP のステートフルな制御を可能にするために、PCEP に対する一連の拡張を規定しています。**ステートフル PCE モデルで PCE 開始 LSP 設定のための PCEP 拡張は**、次の情報を提供します。

- PCC での LSP の設定
- PCE への LSP の制御の委任

SR：PCE 開始の LSP

SR：PCE 開始 LSP 機能を使用すると、クライアントは PCE サーバから LSP を作成、セットアップ、制御、削除することができます。これは PCE 開始メッセージを介して PCC 上で LSP の作成と削除を制御します。PCE 開始 LSP は、LSP を開始した PCE サーバに自動的に委任されます。PCE クライアントは LSP 開始メッセージを処理します。LSP 開始メッセージを使用することにより、PCE クライアントは LSP を作成または削除することができます。

ルートプロセッサ（RP）でフェールオーバーが発生すると、フェールオーバーによって RP がネットワークから切断されます。接続を再確立するには、PCE サーバは、クライアント上で PCE 開始 LSP を回収するために LSP 開始メッセージを再送する必要があり、そうしないとクライアントが作成した PCE 開始 LSP が自動的に削除されます。

PCC との PCEP セッションを確立するために **pce** コマンドを使用する必要があります。**force auto-route** コマンドは、自動ルート アナウンス メッセージを介してエリア内で、および自動ルート宛先メッセージを介してエリア間で LSP をアドバタイズするために使用されます。自動ルート アナウンスを使用するかまたは自動ルート宛先を使用するかの決定は、宛先 IP アドレスに応じてデバイスによって実行されます。開始された LSP に対して **force auto-route** コマンドを有効にすると、スタティック ルートを手動で設定してトラフィックをルーティングするのではなく、TE トンネル経由でトラフィックを自動的にルーティングできます。自動ルート アナウンス メッセージは、宛先ルータおよびダウンストリーム ルータによってアナウンスされたルートを、トンネルを介して到達可能なヘッドエンド デバイスのルーティング テーブルにインストールします。

PCC 構成には、各 PCE の IP アドレス（プライマリとスタンバイの両方、またはさらにその他）が含まれます。各 PCE の優先順位を明示的に指定することができます。2 つの PCE の優先順位が同じである場合、小さい IP アドレスを持つ PCE の方が優先順位が高くなります。

単一および冗長 PCE 操作

SR：PCE 開始 LSP 機能は、単一および冗長 PCE 操作をサポートしています。単一 PCE 操作では、PCE が失敗すると、PCC は状態がタイムアウト（60 秒）するまで待ち、LSP を削除します。

冗長 PCE 操作では、タイマーの満了前に Representational state transfer（REST）呼び出しがスタンバイ PCE に対して開始された場合は、開始された LSP が保持され、そうでない場合は LSP が削除されます。

（注） プライマリ PCE が失敗した場合は、スタンバイ PCE に対して REST コールをもう一度開始する必要があり、コールにスタンバイ PCE の IP アドレスが含まれる必要があります。

冗長 PCE 操作では、PCC 構成は LSP のためのプライマリおよびスタンバイ IP アドレスの両方を含み、より低い優先順位の IP アドレスがプライマリ PCE になります。同じ優先順位の場合は IP アドレスが比較されます。

SR の設定方法：PCE 開始の LSP

PCC との PCEP セッションの確立

このタスクを実行して、PCEP セッション PCE サーバ XR ベースの XTC サーバを設定します。

```
configure terminal
pce
 address ipv4 192.0.2.1
end
```

IP アドレス 192.0.2.1 は、トランスポート コントローラの IP アドレスです。

ネットワークでの LSP のアドバタイジング

```
configure terminal
 mpls traffic-eng pcc peer 192.0.2.1 source 203.0.113.1 force-autoroute
 end
```

上のコード スニペットでは、192.0.2.1 は PCE IP アドレスで、203.0.113.1 は PCEP セッションを確立するための PCC 送信元アドレスです。

PCC に対する PCE の優先順位の指定

```
configure terminal
mpls traffic-eng pcc peer 192.0.2.1 source 203.0.113.1 force autoroute precedence 255
mpls traffic-eng pcc peer 192.0.2.2 source 203.0.113.1 force-autoroute precedence 100
end
```

上記のコード スニペットでは、100 はデフォルトの優先順位である 255 よりも低い優先順位です。したがって、IP アドレス 192.0.2.2 を持つデバイスがプライマリ PCE になり、192.0.2.1 を持つデバイスがスタンバイ PCE になります。

PCE サーバ優先順位の再評価のトリガー

PCE サーバの優先順位の変更は、PCE サーバの障害とは見なされません。したがって、優先順位の変更によって、再委託タイムアウトが発生したり、または PCC で PCE サーバへの LSP 委任の再評価がトリガーされることはありません。

CLI 再構成後の PCE サーバへの LSP 委任の再評価は、TE 再最適化タイマーによって制御されます。デフォルトでは、TE 再最適化タイマーは 3600 秒に設定されています。

PCE サーバの優先順位を変更した後、または新しい PCE サーバを追加した後で、PCC から PCE サーバへの LSP 委任の再評価を高速化することができます。これを行うには、特権 EXEC モードで次のコマンドを使用して、TE 再最適化を手動でトリガーします。

```
mpls traffic-eng reoptimize
```

LSP 構成の確認

手順の概要

1. **show pce ipv4 peer detail**
2. **show pce lsp detail**
3. **show pce client peer**
4. **show mpls traffic-eng tunnel tunnel** *number*

手順の詳細

ステップ 1 show pce ipv4 peer detail

このコマンドを使用して、PCE で PCEP セッションの詳細を確認します。この例では、インスタンス化という用語は、PCE が開始された LSP をサポートすることを示します。

```
Device# show pce ipv4 peer detail


PCE's peer database:

--------------------

Peer address: 52.2.2.2----' PCC IP address

               State: Up

  Capabilities: Stateful, Segment-Routing, Update, Instantiation
```

ステップ 2 show pce lsp detail

このコマンドを使用して、PCE で開始された LSP を確認します。

```
Device# show pce lsp detail


PCE's tunnel database:

----------------------

PCC 52.2.2.2 ----' PCC IP address


Tunnel Name: Test1--------' tunnel name set by REST Call

LSPs:

  LSP[0]:

   source 52.2.2.2, destination 57.7.7.7, tunnel ID 2000, LSP ID 1

   State: Admin up, Operation active

   Binding SID: 26

   PCEP information:

     plsp-id 526288, flags: D:1 S:0 R:0 A:1 O:2 C:1

   LSP Role: Single LSP

   State-sync PCE: None

   PCC: 52.2.2.2

   LSP is subdelegated to: None

   Reported path:

     Metric type: TE, Accumulated Metric 2

      SID[0]: Adj, Label 25, Address: local 102.105.3.1 remote 102.105.3.2

      SID[1]: Adj, Label 24, Address: local 104.105.8.2 remote 104.105.8.1

      SID[2]: Adj, Label 38, Address: local 104.107.10.1 remote 104.107.10.2

   Computed path: (Local PCE)

     None
```

```
    Computed Time: Not computed yet

  Recorded path:

    None

  Disjoint Group Information:

    None
```

ステップ 3 **show pce client peer**

このコマンドを使用して、PCC での PCEP セッション出力を確認し、**force-autoroute** コマンドが有効かどうかを確認します。

```
Device# show pce client peer


PCC's peer database:

------------------------------

Peer address: 51.1.1.1, Precedence: 255

  State up

  Capabilities: Stateful, Update, Segment-Routing,Force-autoroute
```

ステップ 4 **show mpls traffic-eng tunnel tunnel** *number*

このコマンドを使用して、PCC で開始された LSP トンネルの出力を確認します。

```
Device# show mpls traffic-eng tunnel tunnel 2000


Name: Test1                               (Tunnel2000) Destination: 57.7.7.7 Ifhandle: 0x11E
(auto-tunnel for pce client)

  Status:

    Admin: up         Oper: up     Path: valid       Signalling: connected

    path option 1, (SEGMENT-ROUTING) (PCE) type dynamic (Basis for Setup)


  Config Parameters:
```

```
  Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  Path Selection:
   Protection: any (default)
  Path-selection Tiebreaker:
    Global: not set   Tunnel Specific: not set   Effective: min-fill (default)
  Hop Limit: disabled
  Cost Limit: disabled
  Path-invalidation timeout: 10000 msec (default), Action: Tear
  AutoRoute: enabled  LockDown: disabled Loadshare: 0 [0] bw-based
  auto-bw: disabled
  Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
Active Path Option Parameters:
  State: dynamic path option 1 is active
  BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled


PCEP Info:
  Delegation state: Working: yes   Protect: no
  Delegation peer: 51.1.1.1
  Working Path Info:
    Request status: delegated
    SRP-ID: 1
    Created via PCInitiate message from PCE server: 51.1.1.1-----' IP address
    PCE metric: 2, type: TE
  Reported paths:
```

```
     Tunnel Name: Test1
      LSPs:
       LSP[0]:
        source 52.2.2.2, destination 57.7.7.7, tunnel ID 2000, LSP ID 1
        State: Admin up, Operation active
       Binding SID: 26
        Setup type: SR
        Bandwidth: requested 0, used 0
        LSP object:
          PLSP-ID 0x807D0, flags: D:0 S:0 R:0 A:1 O:2
        Metric type: TE, Accumulated Metric 2
        ERO:
          SID[0]: Adj, Label 25, NAI: local 102.105.3.1 remote 102.105.3.2
          SID[1]: Adj, Label 24, NAI: local 104.105.8.2 remote 104.105.8.1
          SID[2]: Adj, Label 38, NAI: local 104.107.10.1 remote 104.107.10.2
      PLSP Event History (most recent first):
        Mon Jul 17 08:55:04.448: PCRpt update LSP-ID:1, SRP-ID:1, PST:1, METRIC_TYPE:2, REQ_BW:0,
USED_BW:0
        Mon Jul 17 08:55:04.436: PCRpt create LSP-ID:1, SRP-ID:1, PST:1, METRIC_TYPE:2, REQ_BW:0,
USED_BW:0
 History:
   Tunnel:
     Time since created: 2 hours, 42 minutes
     Time since path change: 2 hours, 42 minutes
     Number of LSP IDs (Tun_Instances) used: 1
   Current LSP: [ID: 1]
```

```
    Uptime: 2 hours, 42 minutes

Tun_Instance: 1

Segment-Routing Path Info (isis  level-2)

  Segment0[Link]: 102.105.3.1 - 102.105.3.2, Label: 25

  Segment1[Link]: 104.105.8.2 - 104.105.8.1, Label: 24

  Segment2[Link]: 104.107.10.1 - 104.107.10.2, Label: 38
```

SR の追加情報：PCE 開始の LSP

標準および RFC

標準/RFC	タイトル
draft-ietf-pce-pce-initiated-lsp-11	ステートフル *PCE* モデルでの *PCE* 開始 *LSP* 設定の *PCEP* 拡張機能
RFC 5440	パス計算要素（*PCE*）通信プロトコル（*PCEP*）
RFC 8231	パス計算要素（*PCE*）通信プロトコルの一般要件

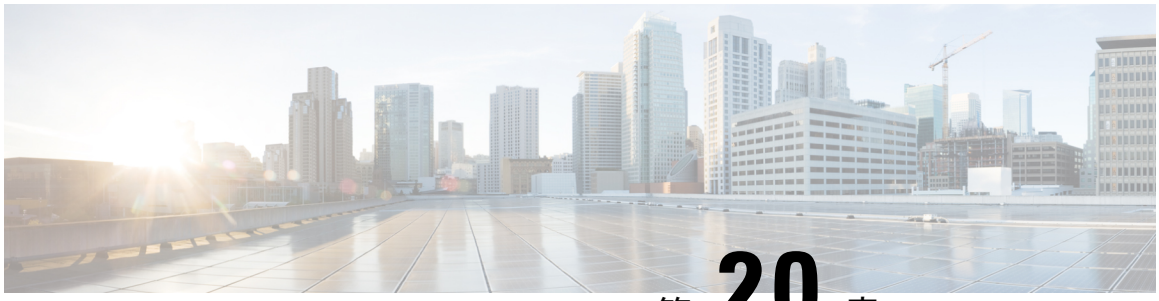
SR の機能情報：PCE 開始の LSP

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 *19 : SR* の機能情報：*PCE* 開始の *LSP*

機能名	リリース	機能情報
SR：PCE 開始の LSP	Cisco IOS XE Fuji 16.7.1	SR：PCE 開始 LSP は、セグメント ルーティング ネットワーク上のステートフル PCE モデルで PCE によって開始される LSP をサポートします。 次のコマンドが導入または変更されました。**mpls traffic-eng pcc**、**pce**、**show mpls traffic-eng tunnel**、**show pce client peer**、**show pce ipv4 peer**、**show pce lsp**



第 20 章

ISIS - SR：uLoop 回避

ISIS - SR：uLoop 回避機能により、ISIS ローカル マイクロループ保護機能が拡張され、リンクダウン イベントまたはリンクアップ イベント後のネットワーク コンバージェンス時にマイクロループが発生するのを防ぐことができます。

ISIS - SR の前提条件：uLoop 回避

- ISIS - SR：uLoop 回避機能はデフォルトで無効になっています。トポロジに依存しないループフリー代替（TI-LFA）機能が設定されている場合、この機能は自動的に有効になります。詳細については、IS-IS モジュールでのセグメント ルーティングの使用の「トポロジに依存しない LFA」のセクションを参照してください。

ISIS - SR の制約事項：uLoop 回避

- ISIS - SR：uLoop 回避機能は LAN ネットワークで同じサブネットの 2 ノードをサポートします。

ISIS - SR に関する情報：uLoop 回避

マイクロループ

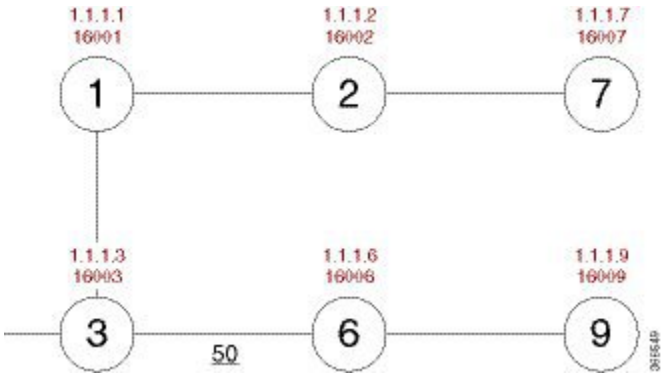
リンクまたはネットワーク デバイスで発生した障害や復旧のためにネットワーク トポロジに変更が生じると、IP Fast Reroute によって迅速なネットワーク コンバージェンスが行われます。このとき、定期的なコンバージェンス機能によってトラフィックが新しく計算されたベストパス（別名、ポスト コンバージェンス パス）へ移動されるまで、事前に計算されていたバックアップ パスにトラフィックが移動されます。このネットワーク コンバージェンスにより、トポロジ内で直接または間接的に接続された2台のデバイス間で、マイクロループが短期間発生する可能性があります。マイクロループは、ネットワーク内の異なるノードが異なるタイミングで互いに別々に代替パスを計算したときに発生します。たとえば、あるノードがコンバージェンスを実行し、ネイバー ノードにトラフィックを送信したときに、そのネイバー ノードでまだコンバージョンが完了していないと、その2つのノードでトラフィックがループする可能性があります。

マイクロループによってトラフィックが損失する場合も、損失しない場合もあります。マイクロループが発生している期間が短ければ、つまりネットワークのコンバージェンスが迅速に行われれば、存続可能時間（TTL）が期限切れになるまでの短い期間、パケットがループする可能性があります。最終的には、パケットは宛先に転送されます。マイクロループの期間が長くなる、つまりネットワーク内のいずれかのルータでコンバージェンスに時間がかかっていると、パケットで TTL が期限切れになったり、パケット レートが帯域幅を超過したり、パケットの順番が狂ったり、パケットがドロップされたりする場合があります。

障害が発生したデバイスとそのネイバーとの間で形成されたマイクロループはローカル ユーループと呼ばれます。また複数ホップ離れたデバイスとの間で形成されるマイクロループはリモート ユーループと呼ばれます。ローカル ユーループは、通常はローカルのループフリー代替（LFA）パスが使用できないネットワークで見られます。このようなネットワークでは、リモート LFA によってネットワークのバックアップ パスが提供されます。

上で説明した情報は、次の図に示すようにトポロジ例を参考にして示すことができます。

図 *21* : マイクロループのトポロジの例



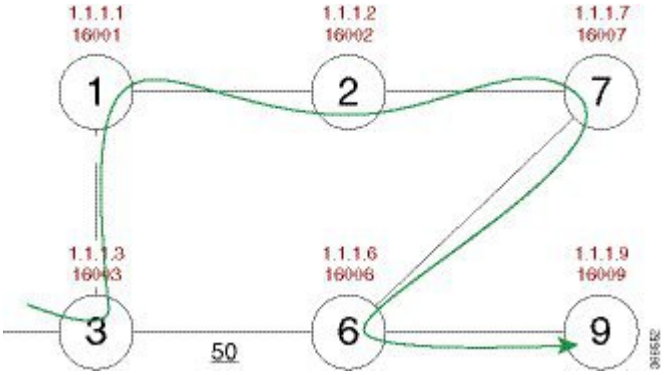
この例の前提条件は次のとおりです。

- デフォルトのメトリックは、メトリックが 50 であるノード 3 とノード 6 間のリンクを除き、各リンクごとに 10 です。各ノードでの SPF バックオフ遅延の収束順序は次のとおりです。
  - ノード 3：50 ミリ秒
  - ノード 1：500 ミリ秒
  - ノード 2：1 秒
  - ノード 2：1.5 秒

ノード 3 からノード 9（宛先）に送信されたパケットは、ノード 6 経由で通過します。

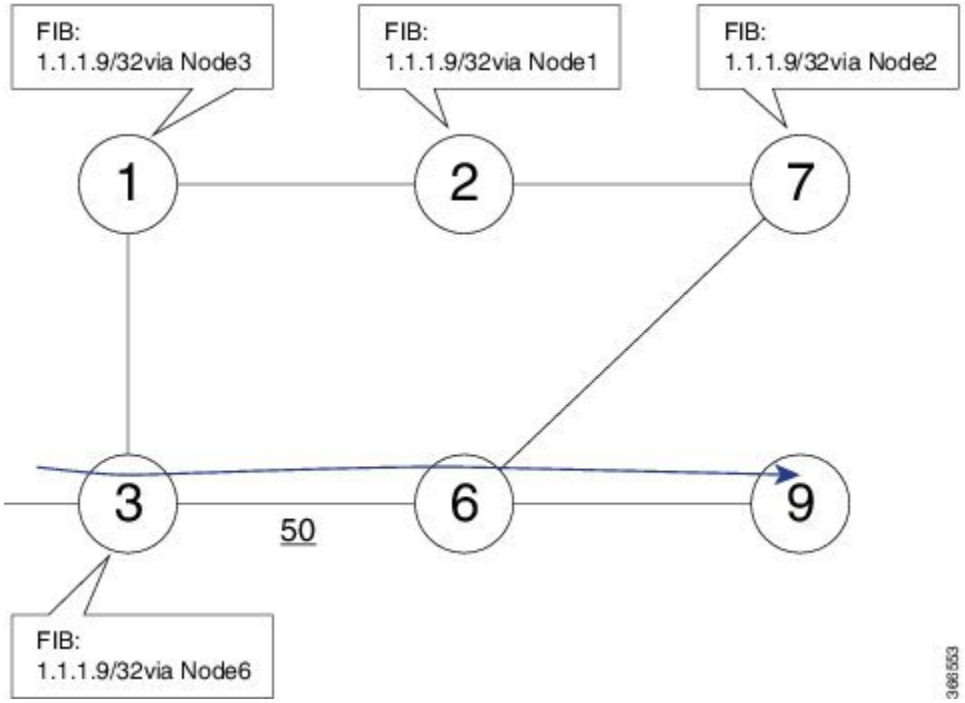
ノード 6 とノード 7 の間でリンクが確立されている場合、パケットが宛先であるノード 9 に到達する前のノード 3 からノード 9 へのパケットの最短パスは、ノード 1、ノード 2、ノード 7、およびノード 6 になります。

図 *22*：マイクロループのトポロジの例：最短パス



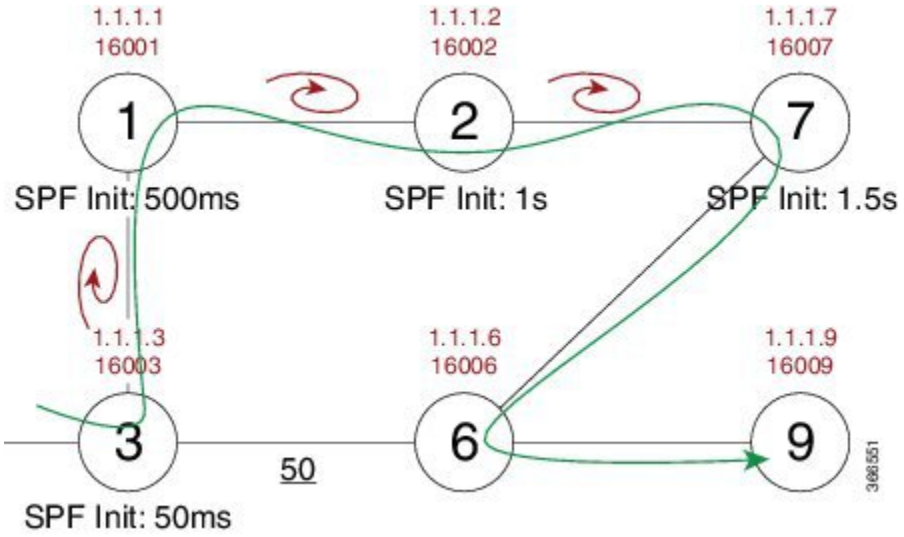
次の図は、ノード 6 とノード 7 間のリンクが確立される前の各ノードの転送情報ベース（FIB）テーブルを示しています。FIB エントリには、宛先ノード（ノード 9）のプレフィックスとネクスト ホップが含まれます。

図 *23 :* マイクロループのトポロジの例：*FIB* エントリ



ノード6とノード7間のリンクがアップすると、各ノードのコンバージェンスの順序に基づいて、マイクロループがリンクに対して発生します。この例では、ノード3は最初にノード1で収束し、その結果ノード3とノード1の間にマイクロループが発生します。その後、ノード1が次に収束し、その結果ノード1とノード2の間にマイクロループが発生します。次に、ノード2が次に収束し、その結果ノード2とノード7の間にマイクロループが発生します。最後に、次の図に示すように、ノード7はマイクロループの解決を収束し、パケットが宛先ノード9に到達します。

図 *24 :* マイクロループのトポロジの例：マイクロループ



SPF コンバージェンス遅延を追加すると、マイクロループは 1.5 秒間（ノード 7 に指定されたコンバージェンス期間）接続を失うことになります。

セグメント ルーティングとマイクロループ

ISIS - SR：uLoop 回避機能は次のシナリオをサポートします。

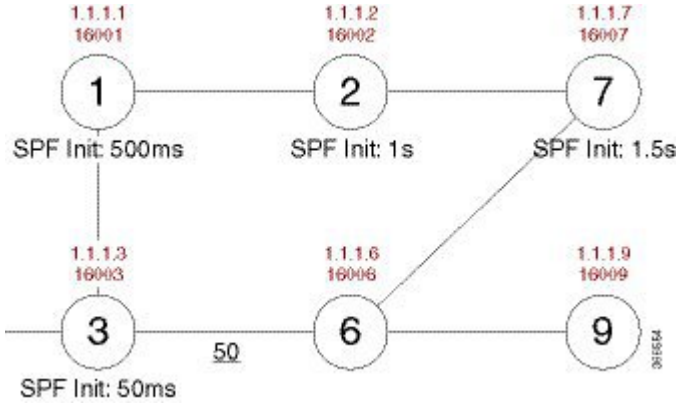
- ポイントツーポイント リンクのリンクアップまたはリンクダウンと 2 つのノードを持つ LAN セグメント
- オーバーロード ビットが設定または設定解除されているためにノードがアップまたはダウンした場合のリンク コストの減少または増加

マイクロループを防ぐために、ノードで **microloop avoidance segment-routing** コマンドを有効にする必要があります。

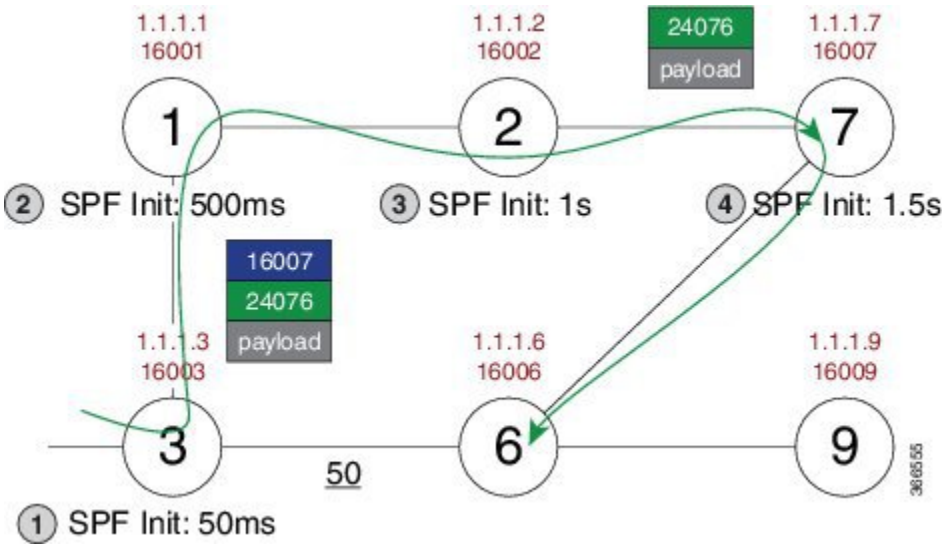
セグメント ルーティングがマイクロループを防ぐ仕組み

このセクションでは、マイクロループの説明に使用した例を使用して、セグメント ルーティングがマイクロループを防ぐ方法について説明します。この例のノード 3 は、**microloop avoidance segment-routing** コマンドで有効になっています。ノード 6 とノード 7 間のリンクがアップした後、ノード 3 はネットワーク上の新しいマイクロループを計算します。

図 *25*：マイクロループのトポロジの例：セグメント ルーティング



FIB テーブルを更新する代わりに、ノード 3 は、ノード 7 のプレフィックス セグメント ID（SID）である 16007 を含むセグメント ID のリストと、ノード 6 の隣接関係セグメント ID（SID）である 24076 を使用して、宛先（ノード 9）のダイナミック ループフリー代替（LFA）SR TE ポリシーを構築します。



したがって、SR TE ポリシーにより、ノード 3 からのパケットが宛先ノード 9 に到達することが可能になり、ネットワークが収束するまでマイクロループのリスクがなくなります。最後に、ノード 3 は新しいパスの FIB を更新します。

microloop avoidance segment-routing コマンドで protected キーワードを使用すると、保護するプレフィックスに対してのみマイクロループ回避が有効化されます。**microloop avoidance rib-update-delay** *milliseconds* コマンドを使用して、ノードのフォワーディング テーブルを更新する前にノードが待機する遅延時間をミリ秒単位で設定し、マイクロループ回避ポリシーの使用を停止することができます。RIB 遅延のデフォルト値は 5000 ミリ秒です。

ISIS - SR を有効にする方法：uLoop 回避

マイクロループ回避の有効化

マイクロループ回避を有効にするための構成コード スニペットの例を次に示します。

```
router isis
 fast-reroute per-prefix level-2 all
 microloop avoidance segment-routing
 microloop avoidance rib-update-delay 3000
```

マイクロループ回避の確認

修復パスが存在するかどうかを確認するには、**show isis rib** および **show ip route**コマンドを使用します。

```
Router# show isis rib 20.20.20.0 255.255.255.0

IPv4 local RIB for IS-IS process sr

IPV4 unicast topology base (TID 0, TOPOID 0x0) ==================
Repair path attributes:
```

```
 DS - Downstream, LC - Linecard-Disjoint, NP - Node-Protecting
 PP - Primary-Path, SR - SRLG-Disjoint


20.20.20.0/24 prefix attr X:0 R:0 N:0 prefix SID index 2 - Bound (ULOOP EP)
 [115/L2/130] via 77.77.77.77(MPLS-SR-Tunnel5), from 44.44.44.44, tag 0,
LSP[2/5/29]
 prefix attr: X:0 R:0 N:0
 SRGB: 16000, range: 8000 prefix-SID index: None
 (ULOOP_EP)(installed)
 - - - - - -
 [115/L2/130] via 16.16.16.6(Ethernet2/0), from 44.44.44.44, tag 0, LSP[2/5/29]
 prefix attr: X:0 R:0 N:0
 SRGB: 16000, range: 8000 prefix-SID index: None
 (ALT)
```

```
Router# show ip route 20.20.20.0

Routing entry for 20.20.20.0/24
 Known via "isis", distance 115, metric 130, type level-2
 Redistributing via isis sr
 Last update from 77.77.77.77 on MPLS-SR-Tunnel5, 00:00:43 ago
 SR Incoming Label: 16002 via SRMS
 Routing Descriptor Blocks:
 * 77.77.77.77, from 44.44.44.44, 00:00:43 ago, via MPLS-SR-Tunnel5,
 * prefer-non-rib-labels, merge-labels
 Route metric is 130, traffic share count is 1
 MPLS label: 16002
 MPLS Flags: NSF
```

ISIS - SR の追加情報：uLoop 回避

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 Command List, All Releases』
「Segment Routing and IS-IS」	『*Using Segment Routing with IS-IS*』
IS-IS の概念の概要	『"IS-IS Overview and Basic Configuration" module in the *IP Routing: ISIS Configuration Guide*』
ISIS でのローカル マイクロループからの保護	『"ISIS Local Microloop Protection" module in the *IP Routing: ISIS Configuration Guide*』

標準/RFC

標準/RFC	タイトル
draft-francois-rtgwg-segment-routing-uloop-00	*Loop avoidance using Segment Routing*

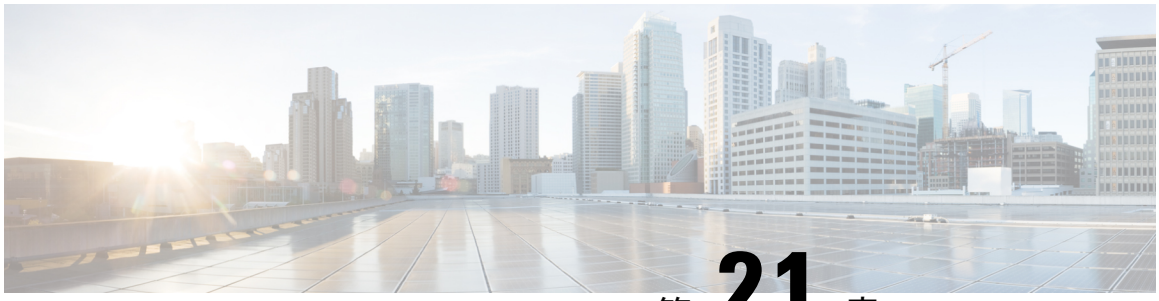
ISIS - SR の機能情報：uLoop 回避

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 *20 : ISIS - SR* の機能情報：*uLoop* 回避

機能名	リリース	機能情報
ISIS - SR：uLoop 回避	Cisco IOS XE Everest 16.6.1	ISIS - SR：uLoop 回避機能により、ISIS ローカル マイクロループ保護機能が拡張され、リンクダウン イベントまたはリンクアップ イベント後のネットワーク コンバージェンス時にマイクロループが発生するのを防ぐことができます。 次のコマンドが導入または変更されました。**microloop avoidance**、**microloop avoidance rib-update-delay**、**show mpls traffic tunnel**。



第 21 章

BGP-SR：BGP プレフィックス SID の再配布

BGP - SR：BGP プレフィックス SID 再配布機能は、セグメント ルーティング — BGP ネットワークにおいて IPv4 プレフィックスで BGP プレフィックス SID をサポートします。

BGP - SR の前提条件：BGP プレフィックス SID の再配布

- マルチプロトコル ラベル スイッチング（MPLS）が設定されている必要があります。

BGP - SR に関する情報：BGP プレフィックス SID の再配布

セグメント ルーティングと BGP

セグメント ルーティングでは、マルチプロトコル ラベル スイッチング（MPLS）ラベルを使用して、ネットワーク内のパケットをガイドするパスを作成します。セグメントルーティングを使用すると、MPLS ラベル範囲はMPLS転送インフラストラクチャ（MFI）で予約されます。このラベル範囲は、セグメント ルーティング グローバル ブロック（SRGB）と呼ばれます。プレフィックスに割り当てられたプレフィックス SID は、SRGB の拡張機能です。

セグメント ルーティングをサポートするためには、Border Gateway Protocol（BGP）が BGP プレフィックスのセグメントID（SID）をアドバタイズできなければなりません。BGPプレフィックス SID は、BGP ネットワークを使用したセグメント ルーティングにおける BGP プレフィッ

クス セグメントのセグメント識別子です。また BGP プレフィックス SID は、BGP によって計算された ECMP 対応のベストパス上のパケットを関連するプレフィックスに転送する命令でもあります。BGP ノードがネットワーク内のネイバーノードと通信するとき、BGP アップデート（ネイバーノードに送信されるメッセージ）には、ラベル付きユニキャスト NLRI のプレフィックス SID ラベルと、プレフィックス SID 属性と呼ばれる新しい属性のプレフィックス SID インデックスが含まれます。

トラフィック エンジニアリングの転送パスをサポートするには、転送パスが最適パスと異なっていることが必要な場合があります。したがって、各 BGP ノードはネイバーにローカル ラベルを割り当て、BGP -- リンク ステート アップデートによってローカルラベルを隣接関係 SID としてアドバタイズします。

BGP - SR：BGP プレフィックス SID 再配布機能は、セグメント ルーティング MPLS コンフィギュレーション モードで **connected-prefix-sid-map** コマンドを使用して有効にすることができます。さらに、各アドレス ファミリに対してルータ コンフィギュレーション モードでも **segment-routing mpls** コマンドを有効にする必要があります。

（注） Cisco IOS XE Everest 16.6.1 では、IPv4 プレフィックスのみサポートされています。

ローカル ソース ルートのセグメント ルーティング

ローカル ノードで設定されたインターフェイス ホスト ルートは、ローカル ソース ルートとして知られています。セグメント ルーティングが有効になっている場合、BGP ノードは、プレフィックス SID ラベルおよびプレフィックス SID 属性として明示的または暗黙的 null を含み、プレフィックスをネイバー ノードにアドバタイズします。

ネイバーに明示的 null が設定されていない場合、MPLS 暗黙的 Null ラベル（3）がネイバー ノードにアドバタイズされます。ネイバーに明示的 null が設定されている場合、プレフィックスのアドレス ファミリに対応する MPLS 明示的 Null ラベルがネイバー ノードにアドバタイズされます（IPv4 の場合は 0）。

受信したプレフィックスのセグメント ルーティング

通信を介してネイバー ノードからプレフィックス SID 属性を受信する BGP ノードは、ルートが RIB に追加されたときに、プレフィックスとして発信ラベルにラベルを追加します。ローカル ラベルおよびプレフィックス SID インデックスは RIB に含まれます。

再配布ルートのセグメント ルーティング

BGP ノード上のソース プロトコルは、受信したプレフィックス SID インデックスおよびローカル ノードで使用可能な SRGB に応じて、ローカル ラベルを割り当てます。ソース プロトコルは、プレフィックス SID インデックスと派生したローカル ラベルを RIB に提供します。BGP は、ネイバー ノードに送信されるラベル付きユニキャスト更新のラベルとして RIB からのローカル ラベルを使用します。

BGP--MFI インタラクション

BGP はクライアントとして MFI に登録し、プレフィックスのローカル ラベル（これを使用してトラフィックが到着することが予期される）としてSIDインデックスおよびSRGBから派生したラベルをバインドします。

BGP - SR を有効にする方法：BGP プレフィックス SID の再配布

BGP-Prefix-SID の有効化

```
segment-routing mpls
 connected-prefix-sid-map */--------> Configures Prefix to SIDIndex Map that can be
queried by BGP/IGP /*
 address-family ipv4
 10.0.0.1/255.0.0.0 index 10 range 11.0.0.1
```

セグメント ルーティング用の BGP の有効化

```
router bgp 2
 address-family-ipv4
  segment-routing mpls
```

BGP - SR の確認：BGP プレフィックス SID の再配布

このセクションでは、ネットワーク例の助けを借りて、BGP - SR：BGP プレフィックス SID 再配布機能を確認する方法を示します。セグメント ルーティングを使用して設定されているデバイスは、ボーダー ゲートウェイ プロトコル（BGP）を使用して設定されている 2 つのデバイスに接続されます。各デバイスで、**show segment-routing mpls** コマンドを使用して設定を表示します。

次に、セグメント ルーティングを使用して設定されているデバイスの構成を示します。

```
segment-routing mpls
global-block 10000 13000
!
connected-prefix-sid-map
  address-family ipv4
   12.1.1.1/32 index 3 range 1
  exit-address-family
!
  segment-routing mpls


interface Loopback0
ip address 12.1.1.1 255.255.255.255

router bgp 1
neighbor 10.1.1.2 remote-as 2
!
```

```
address-family ipv4
  redistribute connected
  segment-routing mpls
  neighbor 10.1.1.2 activate
  neighbor 10.1.1.2 send-label
exit-address-family
```

次に、BGP を使用して設定されている最初のデバイスの設定を示します。

```
segment-routing mpls

router bgp 2
neighbor 10.1.1.1 remote-as 1
neighbor 11.1.1.2 remote-as 3
!
address-family ipv4
  redistribute connected
  neighbor 10.1.1.1 activate
  neighbor 10.1.1.1 send-label
  neighbor 11.1.1.2 activate
  neighbor 11.1.1.2 send-label
exit-address-family
```

次に、BGP を使用して設定されている 2 台目のデバイスの設定を示します。

```
segment-routing mpls

router bgp 3
neighbor 11.1.1.1 remote-as 2
!
address-family ipv4
  redistribute connected
  neighbor 11.1.1.1 activate
  neighbor 11.1.1.1 send-label
exit-address-family
```

BGP - SR の追加情報：BGP プレフィックス SID の再配布

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 Command List, All Releases』

標準および RFC

標準/RFC	タイトル
RFC3107	『*Carrying Label Information in BGP-4*』

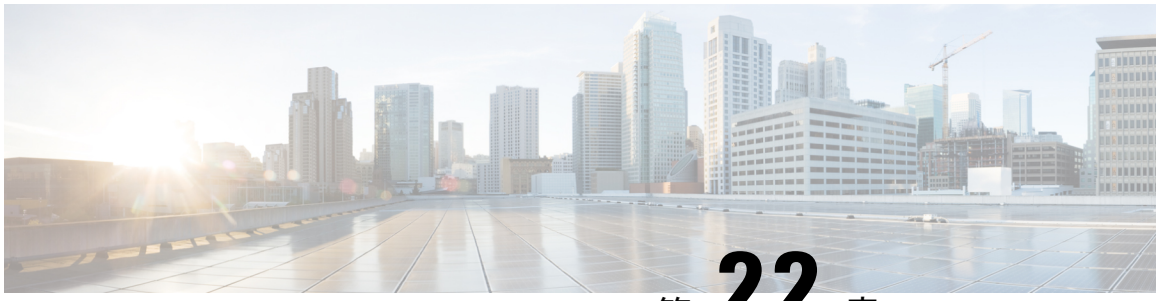
BGP - SR の機能情報：BGP プレフィックス SID の再配布

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 *21 : BGP - SR* の機能情報：*BGP* プレフィックス *SID* の再配布

機能名	リリース	機能情報
BGP-SR：BGP プレフィックス SID の再配布	Cisco IOS XE Everest 16.6.1	BGP - SR：BGP プレフィックス SID 再配布機能は、セグメント ルーティング — BGP ネットワークにおいて IPv4 プレフィックスで BGP プレフィックス SID をサポートします。 次のコマンドが導入または変更されました。**connected-prefix-sid-map**、**segment-routing**。



第 22 章

IS-IS および OSPF によって最大 SID 深度を BGP-LS にアドバタイズする

セグメント ルーティング（SR）が有効になっているネットワークでは、SR トンネルをプログラムする集中型コントローラが、適切な深度の SID スタックをプッシュするために、ノードのヘッドエンドでサポートされる最大セグメント識別子（SID）の深度（MSD）および/またはリンクの細分性を認識する必要があります。MSD は、SR トンネルまたはバインディング SID アンカー ノードのヘッドエンドに関連していて、バインディング SID の拡張によって新しい SID スタックが作成される可能性があります。

IS-IS および OSPF による最大 SID 深度の BGP-LS へのアドバタイズに関する制約事項

- IOS-XE ではライン カードがないため、リンク MSD はアドバタイズされません。

IS-IS および OSPF による最大 SID 深度の BGP-LS へのアドバタイズに関する情報

（注） この機能は、デフォルトで有効に設定されています。この機能を有効にするために固有の設定は不要です。

最大 SID 深度

次の方法により、IGP を使用して、ノードの MSD または集中型コントローラへのリンクをシグナリングすることができます。

- ノード - MSD をそのピアにアドバタイズする。
- MSD 情報を BGP-LS に提供する。

パス計算要素プロトコル（PCEP）SR 拡張は、SR PCE 能力 TLV の MSD およびメトリック オブジェクトをシグナリングします。ただし、PCEP が SR トンネルのヘッドエンドでサポート/設定されていないか、またはバインディング SID アンカー ノードとコントローラが IGP ルーティングに参加しない場合、ノードの MSD を学習する方法はありません。BGP-LS は、トポロジならびにそのトポロジ内のノードの関連する属性および機能を、集中型コントローラに公開する方法を定義します。通常、BGP-LS は、必ずしもヘッドエンドとして機能するとは限らない少数のノードで設定されます。ネットワーク内のすべての SR 対応ノードについて BGP-LS から MSD をシグナリングするために、MSD 機能をネットワーク内のすべての IGP ルータによってアドバタイズする必要があります。

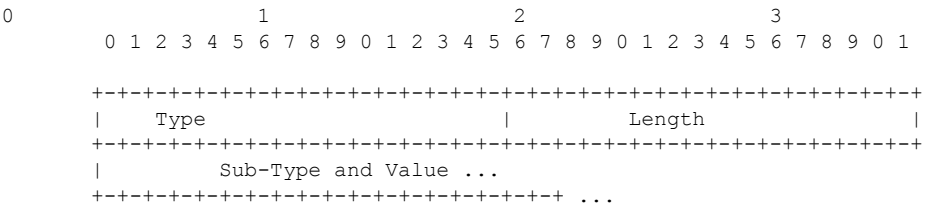
判読可能なラベル深度機能（RLDC）は、適切な深度でエントロピーラベル（EL）を挿入するためにヘッドエンドによって使用され、このためトランジット ノードで読むことができます。MSD は逆に、特定の深度の SID のスタックをプッシュするために機能を通知します。

タイプ 1 の MSD（IANA レジストリ）は、ノードがパス計算要素/コントローラによって使用されるように課すことができる SID の数を通知するために使用されます。これは、計算の結果として作成されたスタックの一部にのみ関係します。MSD は、サービス ラベルの数に関係なく、ノードが課すことができるラベルの合計数をアドバタイズします。

ノードの最大 SID 深度のアドバタイズメント

ノード MSD TLV と呼ばれる本文内の新しいタイプ/長さ/値（TLV）は、ルータ情報（RI）リンク状態アドバタイズメント（LSA）を発信するルータのプロビジョニングされた SID 深度を伝送するために定義されます。ノード MSD は、ノードがサポートする最も低い MSD です。

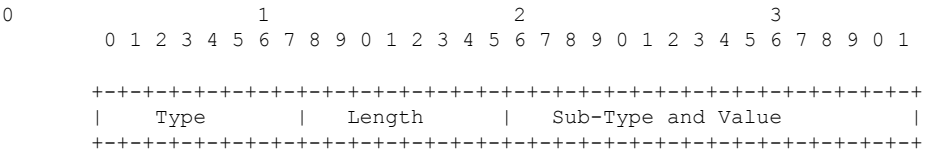
OSPF のノードの最大 SID 深度のアドバタイズメント



この TLV のタイプ（2 バイト）は 12 です（これは IANA によって割り当てられることが推奨されている値です）。長さは可変（最小 2、2 オクテットの倍数）であり、値フィールドの合計長を表します。値フィールドは 1 オクテットのサブタイプ（IANA レジストリ）と 1 オクテット値で構成されます。

サブタイプ 1、MSD、および値フィールドには、RI LSA を発信するデバイスの最大 MSD が含まれます。ノードの最大 MSD は、0 ～ 254 の範囲内です。0 は、任意の深度の MSD をプッシュする能力がないことを表します。その他の値は、ノードのその能力を表します。この値は、ノードによってサポートされる最小値を表す必要があります。

IS-IS のノードの最大 SID 深度のアドバタイズメント



ノード MSD は、TLV 242 のサブ TLV です。このサブ TLV のタイプは 23 です。長さは可変です（最小値は 2、2 オクテットの倍数）。

サブタイプ 1、MSD、および値フィールドには、RI LSA を発信するデバイスの最大 MSD が含まれます。ノードの最大 MSD は、0 ～ 254 の範囲内です。0 は、任意の深度の MSD をプッシュする能力がないことを表します。その他の値は、ノードのその能力を表します。この値は、ノードによってサポートされる最小値を表す必要があります。

ハードウェアからのノード MSD の取得

IS-IS および OSPF は、基盤となるハードウェアからのノードの最大 SID 深度について更新されます。IS-IS と OSPF はこれに基づいて、その TLV の値を更新します。

BGP LS への MSD のアドバタイジング

lGP は LSLIB に情報を送信して、MSD 情報を BGP-LS で使用できるようにします。これはノード MSD 情報またはリンク MSD 情報の可能性があります。また、MSD を動作させるためには、IS-IS で **distribute linkstate** を設定する必要があります。配布リンクの状態を設定するには、次の手順を実行します。

```
Device# configure terminal
```

```
Device(config)# router isis
Device(config-router)# distribute link-state
```

IS-IS および OSPF による最大 SID 深度の BGP-LS へのアドバタイズの確認

IS-IS を使用した最大 SID 深度のアドバタイズの確認

次の show コマンドはノード MSD TLV を確認するのに使用されます。

```
Device# show isis database verbose
Router CAP:   10.10.10.1, D:0, S:0
    Segment Routing: I:1 V:0, SRGB Base: 16000 Range: 8000
       Segment Routing Algorithms: SPF, Strict-SPF
      Router CAP:   2.2.2.2, D:0, S:0
    Segment Routing: I:1 V:0, SRGB Base: 16000 Range: 8000
    Segment Routing Algorithms: SPF, Strict-SPF
    Node-MSD
      MSD: 16
```

OSPF を使用した最大 SID 深度のアドバタイズの確認

次の show コマンドはノード MSD TLV を確認するのに使用されます。

```
Device# show ip ospf database opaque-area type router-information
TLV Type: Segment Routing Node MSD
   Length: 2
     Sub-type: Node Max Sid Depth, Value: 16
```

IS-IS および OSPF による最大 SID 深度の BGP-LS へのアドバタイズに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

IS-IS および OSPF による最大 SID 深度の BGP-LS へのアドバタイズに関する機能情報

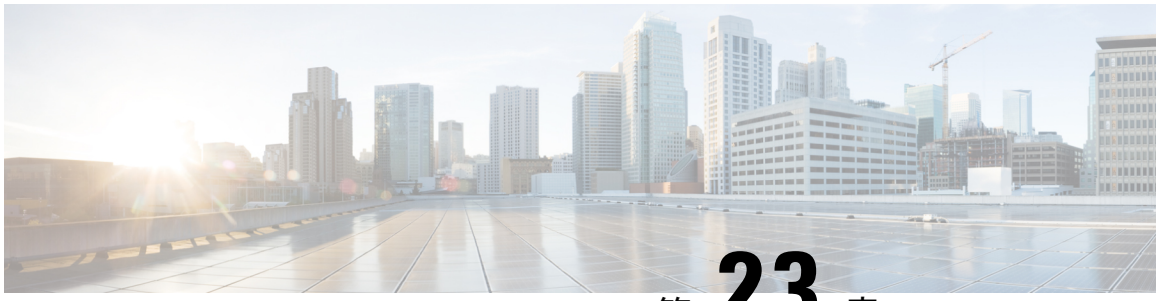
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

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 *22 : IS-IS* および *OSPF* による最大 *SID* 深度の *BGP-LS* へのアドバタイズに関する機能情報

機能名	リリース	機能情報
IS-IS および OSPF によって最大 SID 深度を BGP-LS にアドバタイズする	Cisco IOS XE Fuji 16.7.1	セグメント ルーティング（SR）が有効になっているネットワークでは、SR トンネルをプログラムする集中型コントローラが、適切な深度の SID スタックをプッシュするために、ノードのヘッドエンドでサポートされる最大セグメント識別子（SID）の深度（MSD）および/またはリンクの細分性を認識する必要があります。MSD は、SR トンネルまたはバインディング SID アンカー ノードのヘッドエンドに関連していて、バインディング SID の拡張によって新しい SID スタックが作成される可能性があります。 この機能により、次のコマンドが導入または変更されました。**distribute link-state**、**show isis database verbose**、**show ip ospf database opaque-area type router-information**



第 23 章

セグメント ルーティング トラフィック エンジニアリング AutoTunnel を使用した RSVP-TE の保護

このドキュメントでは、バックアップ セグメントルーティング トラフィック エンジニアリング（SR-TE）自動トンネルを使用した、ネクストホップ（NHOP）保護とも呼ばれるリンク保護のサポートについて説明します。これはRSVP トラフィック エンジニアリング（RSVP-TE）トンネルが通過するリンクを保護します。

セグメント ルーティング トラフィック エンジニアリング AutoTunnel を使用した RSVP-TE の保護に関する前提条件

SR-TEバックアップ自動トンネルを有効にする前に、セットアップで次のテクノロジーが構成されていることを確認してください。

- IS-IS ネットワーク ポイント ツー ポイント インターフェイス
- セグメント ルーティング

さらに、次のテクノロジーに関する事前知識が必要です。

- MPLS トラフィックエンジニアリング
- RSVP トラフィックエンジニアリング
- Fast Reroute

セグメント ルーティング トラフィック エンジニアリング AutoTunnel を使用した RSVP-TE の保護に関する制約事項

- SR-TE バックアップ自動トンネルは、帯域幅保護のために使用することはできません。
- SR-TE バックアップ自動トンネルは、RSVP-TE トンネル保護のバックアップとしてのみ使用できます。

セグメント ルーティング トラフィック エンジニアリング AutoTunnel を使用した RSVP-TE の保護に関する情報

セグメント ルーティング トラフィック エンジニアリング AutoTunnel を使用した RSVP-TE の保護の利点

ネットワークの複雑さが増すにつれて、複雑なシグナリングを伴う RSVP-TE トンネルのメンテナンスや、ネットワーク内のルータでの高いオーバーヘッドにより、スケーラビリティが問題になります。バックアップ自動トンネル機能は、セグメントルーティング（SR）ネットワー

クの複雑さを軽減するのに役立ちます。自動トンネルバックアップ機能には、次の利点があります。

- 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。
- バックアップ トンネルを設定すると、保護エリアが拡張されます。高速再ルーティング（FRR）は、TE トンネルを使用しない IP トラフィックや LDP ラベルの保護は行いません。
- バックアップ SR-TE 自動トンネルでは、RSVP-TE トンネルを通過する既存のトラフィックを中断することなく、SR ネットワークへの追加の移行手段が可能になります。

バックアップ AutoTunnel

ルータでのバックアップ 自動トンネルは、必要に応じて動的バックアップ トンネルを構築するのに役立ちます。これにより、静的 SR-TE トンネルの作成が防止されます。

静的SR-TEトンネルが存在しない場合にラベルスイッチドパス（LSP）を保護するには、次の手順を実行する必要があります。

- 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後、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ります。バックアップ トンネルが利用できない理由には、次のようなものがあります。

- 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。
- 静的バックアップトンネルは設定されているが、使用可能な帯域幅が不足しているか、トンネルが別のプールを保護しているか、またはトンネルが利用できないため、LSPを保護できない可能性があります。

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

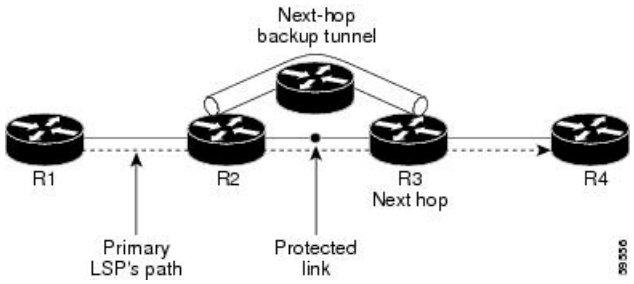
- NNHOP：ノード障害から保護

（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。

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、NHOP バックアップ トンネルと呼ばれます。

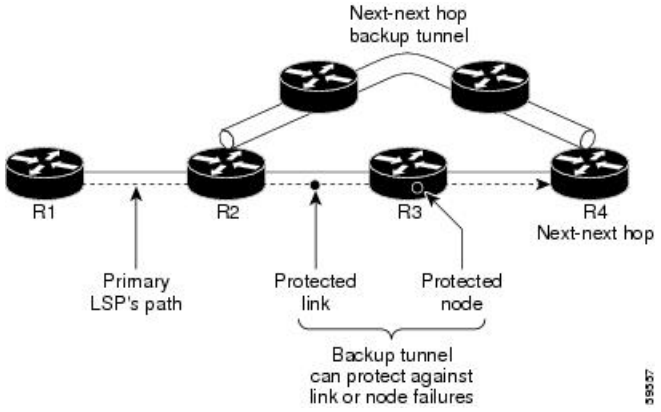
図 *26 :* ネクストホップ バックアップ トンネル



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。

図 *27 :* 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。

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。自動トンネルは、割り当てられている最も小さい番号で始まるトンネル ID を検出します。

たとえば、1000 ～ 1100 の範囲内でトンネルを設定するとします。また、静的に設定された TE トンネルも同じ範囲に入るため、ルータはこれらの ID を使用しません。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。

セグメント ルーティング トラフィック エンジニアリング AutoTunnel を使用した RSVP-TE の保護の設定方法

ポイントツーポイント ネットワーク タイプの明示パスの設定

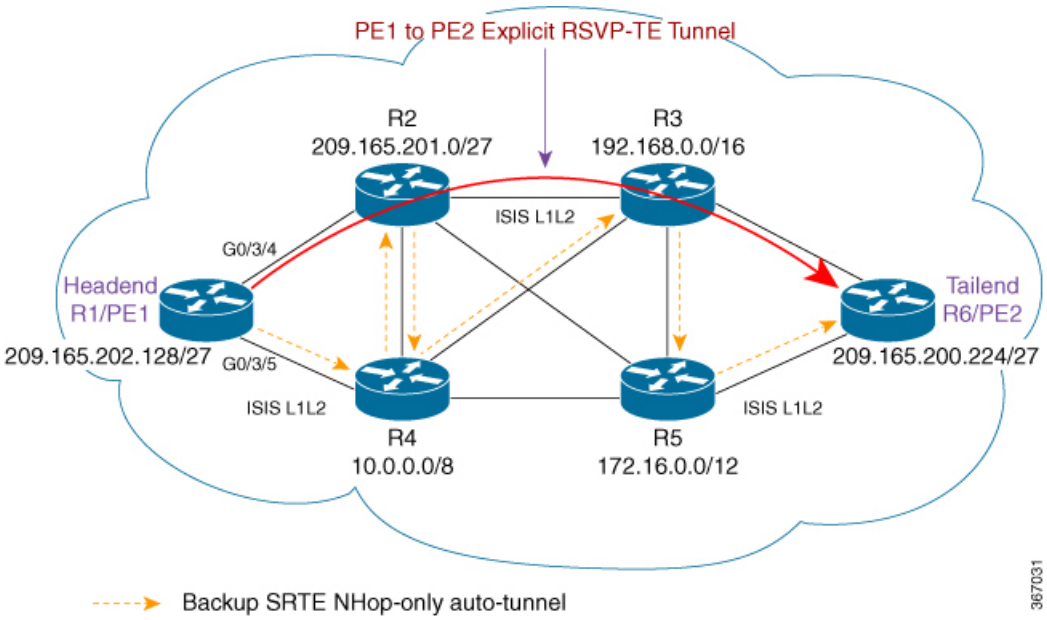
SR-TE 自動トンネル バックアップ機能を動作させるには、インターフェイスがポイントツーポイント ネットワーク タイプである必要があります。

```
interface Loopback0
```

```
 ip address 51.1.1.1 255.255.255.255
 ip router isis 1
end
!
interface GigabitEthernet0/2/0
 ip address 101.102.6.1 255.255.255.0
 ip router isis 1
 negotiation auto
 mpls traffic-eng tunnels
 isis network point-to-point
 ip rsvp bandwidth
end
!
interface GigabitEthernet0/2/4
 ip address 101.104.1.1 255.255.255.0
 ip router isis 1
 negotiation auto
 mpls traffic-eng tunnels
 isis network point-to-point
 ip rsvp bandwidth
end
```

FRR での明示的 RSVP-TE トンネルの設定

図 *28* : 明示的 *RSVP-TE* トンネル



1. ルータ R2 と R3 を通過する R1/PE1 から R6/PE2 への明示的パスを設定します。

```
ip explicit-path name path1 enable
 index 1 next-address 209.165.202.128
 index 2 next-address 209.165.201.0
 index 3 next-address 192.168.0.0
 index 4 next-address 209.165.200.224
```

2. 明示的 RSVP-TE トンネルを設定します。

```
interface Tunnel1
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 209.165.200.224
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 10 explicit name path1
 tunnel mpls traffic-eng record-route
end
```

3. プライマリ RSVP-TE トンネル 1 を FRR で設定して、保護プロセスをアクティブにします。

```
interface tunnel 1
 tunnel mpls traffic-eng fast-reroute
```

4. SR-TE 自動トンネルを使用してリンク保護を有効にするには、グローバル コマンドを設定します。

```
mpls traffic-eng auto-tunnel backup segment-routing nhop-only
```

（注） このコマンドは、リンク保護を必要とするすべてのノードで使用可能である必要があります。

プライマリ RSVP/TE トンネルは、ヘッドエンド R1/PE1 から宛先 R6/PE2 に初期化され、次のノード R2 などを通過するように保護する必要があります。この場合、R1/PE1 はローカル修復点（PLR）であり、R2 は中間点（MP）です。リンク保護によって、SR-TE バックアップ自動トンネルは、パス R1/PE1 -> R4 および R4 -> R2 を通過することによって R1/PE1 から R2 へのリンクに保護を提供するため、MP に収束します。

セグメント ルーティング トラフィック エンジニアリング AutoTunnel を使用した RSVP-TE の保護の確認

show interfaces Tunnel コマンドを使用して、SR-TE 自動トンネルが生成され、アップになっているかどうかを確認します。

```
Device#show interfaces Tunnel65436
Tunnel65436 is up, line protocol is up
```

show mpls traffic-eng tunnels コマンドを使用して、バックアップ自動トンネルが SR-TE トンネルであるかどうかを確認します。

```
Device#show mpls traffic-eng tunnels tunnel 65436
Name: R1_t65436 (Tunnel65436) Destination: 209.165.201.0
 Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 1, (SEGMENT-ROUTING) type explicit __dynamic_tunnel65436 (Basis for
Setup, path weight 20)
```

show ip explicit-paths コマンドを使用して、SR-TE バックアップ トンネルがノードに到達するためにセカンダリ パスを使用しているかどうかを確認します。

```
Device#show ip explicit-paths
PATH __dynamic_tunnel65436 (strict source route, path complete, generation 49, status
non-configured)
1: exclude-address 101.102.5.1
```

show mpls traffic-eng tunnels tunnel 65436 | s Segment-Routing Path Info コマンドを使用して、バックアップ トンネルがパス R1/PE1 から R4 へ、および最終的に中間点である宛先 R2 を通過しているかどうかを確認します。

```
Device#show mpls traffic-eng tunnels tunnel 65436 | s Segment-Routing Path Info
Segment-Routing Path Info (isis level-1)
 Segment0[Link]: 101.104.1.1 - 101.104.1.2, Label: 19
 Segment1[Link]: 102.104.6.2 - 102.104.6.1, Label: 18
```

show mpls traffic-eng auto-tunnel backup コマンドを使用して、自動トンネル バックアップの状態が正しいかどうかを確認します。

```
Device#show mpls traffic-eng auto-tunnel backup
State: Enabled
 Auto backup tunnels: 1 (up: 1, down: 0)
 Tunnel ID Range: 65436 - 65535
 Create Nhop Only: Yes
 Check for deletion of unused tunnels every: 3600 Sec
 SRLG: Not configured

Config:
 unnumbered-interface: Loopback0
  Affinity/Mask: 0x0/0xFFFF
```

show mpls traffic-eng fast-reroute database コマンドを使用して、RSVP-TE LSP が通過するプライマリ リンクが保護されているかどうかを確認します。

```
Device#show mpls traffic-eng fast-reroute database
P2P Headend FRR information:
Protected tunnel In-label Out intf/label FRR intf/label Status
-------------------------- -------- -------------- -------------- ------
Tunnel1 Tun hd Gi0/3/4:30 Tu65436:30 ready

Device#show ip rsvp fast-reroute
P2P Protect BW Backup
Protected LSP I/F BPS:Type Tunnel:Label State Level Type
------------ ------- -------- ------------ ------ ----- ------
R1_t1 Gi0/3/4 0:G Tu65436:28 Ready any-unl Nhop
```

セグメント ルーティング トラフィック エンジニアリング AutoTunnel を使用した RSVP-TE の保護に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

セグメント ルーティング トラフィック エンジニアリング AutoTunnel を使用した RSVP-TE の保護に関する機能情報

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 *23:* セグメント ルーティング トラフィック エンジニアリング *AutoTunnel* を使用した *RSVP-TE* の保護に関する機能情報

機能名	リリース	機能情報
セグメントルーティング トラフィック エンジニアリング AutoTunnel を使用した RSVP-TE の保護	Cisco IOS XE Fuji 16.8.1	この機能は、バックアップ セグメントルーティング トラフィック エンジニアリング（SR-TE）自動トンネルを使用した、ネクストホップ（NHOP）保護とも呼ばれるリンク保護をサポートします。これはRSVP トラフィック エンジニアリング（RSVP-TE）トンネルが通過するリンクを保護します。 この機能により、次のコマンドが導入されました。**ip explicit-path name path1 enable**、**show mpls traffic-eng tunnels tunnel 65436**、**show ip explicit-paths**、**show mpls traffic-eng tunnels tunnel 65436 | show Segment-Routing Path Info**、**show mpls traffic-eng fast-reroute database**、**show ip rsvp fast-reroute sh mpls traffic-eng auto-tunnel backup**。

第 24 章

ISIS 手動隣接関係 SID

統合された Intermediate System-to-Intermediate System（IS-IS）の手動隣接関係 SID 機能は、手動でプロビジョニングされた隣接関係 SID に関する情報を提供します。

ISIS 手動隣接関係 SID に関する情報

セグメント ルーティング（SR）ネットワークでは、多くの場合、ネットワーク上で特定のトラフィックが通過するパスに影響を与えるためにSR トラフィック エンジニアリング（SR-TE）を使用します。SR-TE トンネルはトンネル ヘッドで手動でプロビジョニングできますが、多くの場合、中央コントローラによって計算およびプロビジョニングされます。多くの場合ネットワークのオペレータは、トラフィックに特定のノードやリンクを経由させたいと考えます。

SR ネットワーク オペレータの特定のノードをトラフィックに経由させるために、ノードによってアドバタイズされるプレフィックス SID を使用できます。多くの場合、複数のノードが同じプレフィックス SID を共有する特定の場所を通過するようにトラフィックに強制するエニーキャスト プレフィックス SID が使用されます。

トラフィックに特定のリンク上を通過させるためには、隣接関係 SID（Adj-SID）が使用されます。既存の Adj-SID の実装の問題は、手動でプロビジョニングされたプレフィックス SID とは対照的に、動的に割り当てられた値であるということです。Adj-SID が動的に割り当てられているということは、一連の問題をもたらします。

- この値は、リロードまたはプロセスの再起動に対して永続的ではありません。
- この値は事前にわからないので、IGP によってフラッディングされた情報（ネイティブまたは BGP-LS）にアクセスしない限り、コントローラが使用することはできません。
- 各リンクには一意の Adj-SID 値が割り当てられているため、複数のリンクで同じ Adj-SID を共有することはできません。

上記の問題に対処するために、adj-SID が拡張され、以下が可能になりました。

- リロードと再起動に対して永続的な、手動でプロビジョニングされた adj-SID をサポートします。
- 同じネイバーへの複数の隣接関係に対してプロビジョニングされる同じ adj-SID をサポートします。
- 異なるネイバーへの複数の隣接関係にプロビジョニングされる同じ adj-SID をサポートします。
- 1 つの隣接関係に対して複数の手動 Adj-SID を設定できます。

手動隣接関係 SID

新しい永続的な Adj-SID の要件をサポートするために、動的に割り当てられた Adj-SID に使用されている既存の IS-IS Adj-SID インフラストラクチャが拡張されます。新しい CLI コマンドも導入され、ポイントツーポイントリンクのために Adj-SID 値を手動で割り当てることができます。単一のポイントツーポイントインターフェイスで複数の Adj-SID をプロビジョニングできます。同じ Adj-SID を、同じまたは異なるネイバーにつながる複数のポイントツーポイントインターフェイスでプロビジョニングできます。

すべての手動 Adj-SID は、セグメント ルーティング ローカル ブロック（SRLB）と呼ばれるラベルの範囲から割り当てられます。デフォルトの SRLB の範囲は 15000 ～ 15999 です。

手動の Adj-SID は、インデックスまたは絶対値として設定できます。インデックスとして設定されている場合、絶対ラベルはインデックス + SRLB 開始ラベルとして計算されます。たとえば、56 を手動 Adj-SID のインデックスとして設定した場合、絶対ラベルは 15000 + 56 = 15056 になります。絶対値として設定されている場合、ラベル自体が絶対値になります。たとえば、56 を絶対手動 Adj-SID として設定した場合、絶対ラベルは 56 のみになります。ラベル（インデックスと絶対の両方）は、保護または非保護として設定できます。デフォルトでは、すべてのラベルは非保護です。

隣接関係 SID のアドバタイズメント

手動で設定された adj-SID は、ISIS SR 拡張機能の草案で定義される既存の ISIS adj-SID サブ TLV を使用してアドバタイズされます。S フラグは、同じ Adj-SID 値が複数のインターフェイスにプロビジョニングされている場合に adj-SID サブ TLV に設定されます。手動で設定された SID の場合、P フラグは常に設定されます。

プロビジョニングされた adj-SID がプロテクトとして設定済みの場合は、B フラグも設定されます。

隣接関係 SID は常にラベル値としてアドバタイズされます。adj-SID の設定にインデックスが使用されている場合でも、インデックスとしてはアドバタイズされません。

隣接関係 SID のフォワーディング

adj-SID の値が 1 つのインターフェイスでのみ設定される場合、ISIS は手動で割り当てられた adj-SID のフォワーディング エントリをインストールします。任意の Adj-SID のプライマリ パスは、Adj-SID が割り当てられているポイントツーポイント インターフェイス上の POP 操作です。割り当てられた adj-SID がバックアップの対象となり、バックアップ パスが利用可能であれば、IS-IS はバックアップ パスもプログラムします。Adj-SID のバックアップ パスは、ネイバー ルータ ID アドレスに対して計算されたバックアップ パスと同じです。

複数のリンクで同じ adj-SID 値が設定されている場合、次のような転送が発生します。

- この値を使用して adj-SID が設定されている各リンクを経由して、POP 操作を含むプライマリ パスがインストールされます。
- 各プライマリ パスについて、Adj-SID がプライマリ インターフェイスで保護されるように設定されていて、バックアップが利用可能な場合、バックアップ パスがインストールされます。バックアップ パスは、ネイバー ルータ ID アドレスに関連付けられたバックアップ パスとして表されます。

設定要件

- セグメント ルーティングがグローバルに設定されていることを確認します。
- セグメント ルーティングが IS-IS を使用して設定されていることを確認します。

手動隣接関係 SID の設定

```
Device#configure terminal
Device(config)#interface ethernet0/1
Device(config-if)#isis adjacency-sid [absolute | index] <value> [protected]
```

[index]：（オプション）隣接関係 SID が SRLB 範囲のインデックスとして設定されている場合に使用されます。index キーワードが使用されていない場合、値はラベルの絶対値を表すことが期待されます。

[absolute]：（オプション）隣接関係 SID が絶対値として設定されている場合に使用されます。

<*value*>：adj-SID ラベルの値またはインデックスを表します。プログラムおよびアドバタイズされる adj-SID では、値/インデックスは有効な SRLB の範囲である必要があります。

[protected]：（オプション）手動の adj-SID を保護するために使用されます。デフォルトでは、手動 Adj-SID は保護されていません。

セグメント ルーティング ローカル ブロック（SRLB）範囲の変更

```
Device#configure terminal
Device(config)#segment-routing mpls
Device(config-srmpls)#local-block 7000 7999
```

手動隣接関係 SID の確認

SR アプリ データベースでのラベルの確認

```
Device#show segment-routing mpls lb assigned-sids
Adjacency SID Database
 C=> In conflict
 S=> Shared
 R=> In range
SID  STATE       PROTOCOL     TOPOID      LAN      PRO NEIGHBOR    INTERFACE
15378 R
                 ISIS         0           N        N   10.0.0.3     Ethernet0/1
```

MPLS 転送でのラベルの確認

```
      Device# show mpls forwarding-table
      Local      Outgoing        Prefix               Bytes Label      Outgoing
 Next Hop
      Label      Label           or Tunnel Id         Switched         interface
      15378      Pop Label       0.0.60.18-A          0                Et0/0
   10.0.0.2 □== Configured only for interface e0/0
```

共有ラベルの確認

```
      Device# show mpls forwarding-table
      Local      Outgoing        Prefix               Bytes Label      Outgoing
Next Hop
      Label      Label           or Tunnel Id         Switched         interface
      15378      Pop Label       0.0.60.18-A          0                Et0/0
  10.0.0.2  □== Same Label is configured for 2 interfaces
                 Pop Label       0.0.60.18-A          0                Et0/1
  10.0.0.3  □==
```

ISIS LSP の確認

```
      Device# sh isis database verbose R1.00-00
      xxxxxx
      xxxxxx
      Adjacency SID Value:15378 F:0 B:0 V:1 L:1 S:1 P:1 Weight:0 □== P (Persistent)
flag is always 1 if it is Manual Adj-SID
      xxxxxx

      P -> Persistent Flag (0 for Dynamic Adj-SID and 1 for Manual Adj-SID)
      S -> Shared Flag (1 if label is shared by multiple adjacencies)
```

ISIS 手動隣接関係 SID 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』

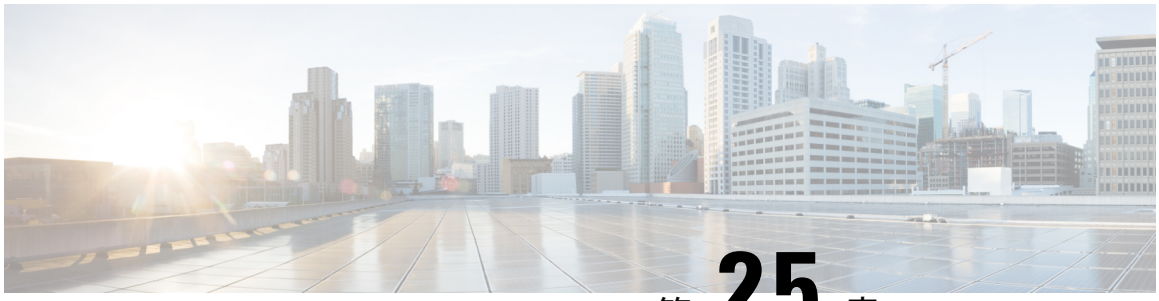
ISIS 手動隣接関係 SID の機能情報

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 *24 : ISIS* 手動隣接関係 *SID* の機能情報

機能名	リリース	機能情報
ISIS 手動隣接関係 SID	Cisco IOS XE Fuji 16.9.1	統合された Intermediate System-to-Intermediate System（IS-IS）の手動隣接関係 SID 機能は、手動でプロビジョニングされた隣接関係 SID に関する情報を提供します。 この機能により、次のコマンドが追加されました。 **adjacency-sid [absolute | index]**<*value*> **[protected]**。 .



第 25 章

OSPFv2 セグメント ルーティングの厳格な SPF

OSPFv2 セグメント ルーティングの厳格な最短パス優先（SPF）機能では、厳格な SPF セグメント識別子（SID）に関する情報を提供します。

OSPFv2 セグメント ルーティングの厳格な SPF の制約事項

- OSPF エリア内のすべてのノードが厳格な SPF に対応していなければならず、セグメント ルーティング トラフィック エンジニアリング（SR-TE）と連携する厳格な SPF ソリューションのために各ノードに少なくとも 1 つの厳格な SPF SID が必要です。
- 厳格な SPF SID の再配布はサポートされていません。

OSPFv2 セグメント ルーティングの厳格な SPF に関する情報

セグメント ルーティング（SR）アーキテクチャは、複数のプレフィックス SID アルゴリズムをサポートするためのプロビジョニングを提供します。現在、2 つのアルゴリズムが定義されています。

- **アルゴリズム 0**：これは最短パス アルゴリズムであり、デフォルトでサポートされています。

- **アルゴリズム 1**：これは厳格な最短パス アルゴリズムです。パケットが SPF アルゴリズムに従って転送されることを強制し、SPF 決定を上書きする可能性のあるローカル ポリシーを無視するようにパス内のルータに指示します。厳格な最短パス アルゴリズムでアドバタイズされた SID により、パケットが取得しようとしているパスは、変更後の SPF パスではなく、予期したパスになります。セグメント ルーティングをサポートする各ノードで、厳格な SPF SID を構成する必要があります。

  アルゴリズム 1 はアルゴリズム 0 と同じですが、パスに沿ったすべてのノードが SPF ルーティングの決定を遵守することを必要とします。ローカル ポリシーは、転送の決定を変更しません。たとえば、パケットはローカルに設計されたパスを通じて転送されません。

厳格な SPF を使用する理由

トンネル パスでリンクまたはノード障害が発生した場合、トラフィックが修復パスに即転送されると、SR-TE トンネルを介してルーティングされた MPLS トラフィックが中間チェーンからトンネル ヘッド エンドに再ルーティングされる可能性があります。ヘッドエンドが SR-TE トンネル経由でこの MPLS トラフィックを再びルーティングした場合は、利用可能な宛先への代替 IGP 最短パスが存在する場合でも、同じ MPLS トラフィックが、TTL が満了するまでトンネルに沿ってループすることがあります。

厳格な SPF SID を使用すると、SR-TE トンネルを介したトラフィックのループを防ぐことができます。厳格な SPF のサポートにより、すべてのルータは、デフォルト SID、つまり SID0 と厳格な SPF SID、つまり SID1 の両方を持つように設定されます。トンネル トラフィックがヘッドエンドにルーティングされ戻された場合、アクティブ ラベルとして厳格な SPF SID を持つヘッドエンドに到着して非トンネル IGP 最短パス（ネイティブ パス）経由で転送されるため、SR-TE トンネルに沿ってループを壊します。エリア/トンネル パス内のすべてのノードが厳格な SPF に対応している場合は、SRTE トンネルのデフォルトのプレフィックス SID よりも、厳格な SPF プレフィックス SID が優先されます。

厳格な SPF 機能のアドバタイズメント

OSPF は、セグメント ルーティングがグローバルまたは特定のエリアで有効になっている場合に、ルータ情報（RI）Opaque リンク状態アドバタイズメント（LSA）の SR アルゴリズム TLV で厳格な SPF 機能をアドバタイズします。OSPF には、SR アルゴリズム TLV のアルゴリズム 0（SPF）とアルゴリズム 1（厳格な SPF SID）の両方が含まれています。

受信されると、OSPF はルータ情報 Opaque LSA を解析して、SR アルゴリズム TLV を検出します。TLV が見つからないか、またはアルゴリズム 1 が TLV に含まれていない場合、OSPF はアドバタイズメント ルータからのすべての厳格な SPF SID アドバタイズを無視します。

OSPF は引き続き単一の SRGB のみをサポートします。同じ SRGB が、通常の SID と厳格な SPF SID の両方に使用されます。通常の SID と同様に、OSPF では、SRGB 範囲の厳格な SPF SID を使用しないでください。

拡張プレフィックス LSA での厳格な SPF SID アドバタイズメント

OSPF は、拡張プレフィックス Opaque LSA の OSPF 拡張プレフィックス TLV で 1 に設定されたアルゴリズムを使用して、プレフィックス SID サブ TLV の厳格な SPF SID 接続マップをアドバタイズします。同じプレフィックスに対してデフォルト SID と厳格な SPF SID の両方が同じ LSA でアドバタイズされます。OSPF は、通常の SID と厳格な SPF SID に対して、個別の明示的 NULL をアドバタイズします。両方の SID は、同じアタッチ フラグを共有します。

OSPF は、拡張プレフィックス Opaque LSA の OSPF 拡張プレフィックス範囲 TLV で、1 に設定されたアルゴリズムを使用して、プレフィックス SID サブ TLV の厳格な SPF SID マッピング サーバ エントリをアドバタイズします。同じプレフィックスに対して、デフォルト SID と厳格な SPF SID の両方がアドバタイズされる場合があります。同じプレフィックスに対して同じアルゴリズムの複数の SID がアドバタイズされている場合、受信側のルータは最初のエンコード済み SID を使用します。OSPF は、通常の SID と厳格な SPF SID に対して、個別の明示的 NULL をアドバタイズします。両方の SID は、同じアタッチ フラグを共有します。通常の SID では、アタッチ フラグの設定が異なる場合に優先順位を引き継ぎます。

SR アルゴリズム TLV が見つからないか、またはアルゴリズム 1 が TLV に含まれていない場合、OSPF はアドバタイズメント ルータからのすべての厳格な SPF SID アドバタイズを無視します。同じプレフィックスに対して同じアルゴリズムの複数の SID を受信した場合、受信側のルータは最初のエンコード済み SID を使用します。明示的 NULL およびアタッチ フラグがプレフィックスの受信 SID0 および SID1 と異なる場合、SID0 のフラグが優先順位を引き継ぎます。

SR-TE およびルータ情報ベースとのインタラクション

デフォルトの SID と同様に、厳格な SPF SID も、SR と TE の両方がそのエリアに対して有効になっている場合にのみ SR-TE と通信します。厳格な SPF SID に関連する SR-TE では、次の 3 つの形式の通信が発生する可能性があります。

- OSPF は、そのエリアが厳格な SPF に対応しているかどうかを SR-TE にアナウンスします。エリア内のすべてのノードが厳格な SPF に対応しているいて、各ノードに少なくとも 1 つの厳格 SPF SID が設定されている場合、そのエリアは厳格な SPF に対応しています。
- OSPF は、すべてのプレフィックスおよび登録されたプレフィックス パスについての厳格な SPF SID を SR-TE にアナウンスします。
- SR-TE は、ラベル スタックに対して厳格な SPF SID を優先します。OSPF は、自動ルート アナウンス トンネル リストのリストが変更されたときに、SR-TE からトンネル リストを受信します。各トンネルについて、SR-TE は、トンネルが厳格な SPF の SID またはデフォルトの SID を使用して作成されているかどうかを示します。OSPF は、更新されたトンネル リストが SR-TE から受信されるたびにフル SPF を実行し、トンネル エンドポイント経由で到達可能なプレフィックスの RIB パスをトンネルのネクストホップに置き換えます。

厳格な SPF SID は、ルータ情報ベース（RIB）にはインストールされていません。RIB にインストールされているプレフィックスの発信ラベルとしてインストールされるのは、デフォルトの SID のみです。SR-TE トンネル タイプは両方とも RIB にインストールされています。

OSPFv2セグメントルーティングの厳格なSPFの有効化および無効化

セグメントルーティング mpls が OSPF およびグローバル モードの下で設定される場合、厳格な SPF 機能はデフォルトで有効になっています。これを有効または無効にする個別の CLI はありません。

OSPFv2 セグメント ルーティングの厳格な SPF SID の設定

OSPFv2 セグメント ルーティングの厳格な SPF を設定するには、次の手順を実行します。

```
segment-routing mpls
 connected-prefix-sid-map
  address-family ipv4
   10.0.0.0/8 2
   172.16.0.0/8 3
  address-family ipv4 strict-spf
   10.0.0.0/8 22
   172.16.0.0/8 23
  exit-address-family
```

OSPFv2 セグメント ルーティングの厳格な SPF の確認

次のコマンドを使用して、OSPFv2 セグメント ルーティングの厳格な SPF を確認します。

OSPFv2 セグメント ルーティングの厳格な SPF SID の確認

```
Device#show ip ospf database opaque-area type ext-prefix

            OSPF Router with ID (10.0.0.4) (Process ID 10)

                Type-10 Opaque Area Link States (Area 0)

  LS age: 40
  Options: (No TOS-capability, DC)
  LS Type: Opaque Area Link
  Link State ID: 7.0.0.3
  Opaque Type: 7 (Extended Prefix)
  Opaque ID: 3
  Advertising Router: 10.0.0.2
  LS Seq Number: 80000003
  Checksum: 0xFB42
  Length: 56

    TLV Type: Extended Prefix
    Length: 32
      Prefix    : 10.0.0.6/32
      AF        : 0
      Route-type: Intra
      Flags     : N-bit
```

```
      Sub-TLV Type: Prefix SID
      Length: 8
        Flags : None
        MTID  : 0
        Algo  : SPF
        SID   : 100

      Sub-TLV Type: Prefix SID
      Length: 8
        Flags : None
        MTID  : 0
        Algo  : Strict SPF
        SID   : 101
```

```
Device#show ip ospf segment-routing sid-database


            OSPF Router with ID (10.0.0.4) (Process ID 10)

OSPF Segment Routing SIDs

Codes: L - local, N - label not programmed,
       M - mapping-server

SID             Prefix              Adv-Rtr-Id       Area-Id  Type      Algo
--------------  ------------------  ---------------  -------  --------  ----
2               10.0.0.2/32          10.0.0.2          0        Intra     0
4       (L)     10.0.0.4/32          10.0.0.4          0        Intra     0
7               10.0.0.7/32          10.0.0.5          0        Intra     0
9               10.0.0.8/32          10.0.0.2          0        Intra     0
20              2.0.2.20/32         2.2.2.2          0        Intra     0
21              22.0.22.21/32       2.2.2.2          0        Intra     1
22      (M)     2.0.2.22/32                                   Unknown   0
29      (M)     22.0.22.29/32                                 Unknown   1
33              33.0.33.33/32       3.3.3.3          0        Intra     1
38      (M)     3.0.3.38/32                                   Unknown   0
39      (M)     33.0.33.39/32                                 Unknown   1
77              77.77.77.77/32      5.5.5.5          0        Inter     0
92      (M)     2.1.2.92/32                                   Unknown   0
99              99.99.99.99/32      9.9.9.9          0        Intra     0
100             2.0.2.100/32        2.2.2.2          0        Intra     0
101             2.0.2.100/32        2.2.2.2          0        Intra     1
120             3.3.3.120/32        3.3.3.3          0        Intra     0
121             3.3.3.120/32        3.3.3.3          0        Intra     1
```

```
Device#show ip ospf segment-routing mapping-server

            OSPF Router with ID (10.0.0.4) (Process ID 10)

Advertise local: Enabled
Receive remote: Enabled

Flags: i - sent to mapping-server, u - unreachable,
       s - self-originated

2.0.2.22/32 (R), range size 1
   Adv-rtr        Area          LSID          SID    Type    Algo
i  2.2.2.2        0             7.0.0.4       22     Intra   0
s  4.4.4.4        24            7.0.0.1       22     Inter   0

2.1.2.92/32 (R), range size 1
   Adv-rtr        Area          LSID          SID    Type    Algo
```

```
i  2.2.2.2        0             7.0.0.5       92     Intra   0
s  4.4.4.4        24            7.0.0.2       92     Inter   0

3.0.3.38/32 (R), range size 1
   Adv-rtr        Area          LSID          SID    Type    Algo
i  3.3.3.3        0             7.0.0.2       38     Intra   0
s  4.4.4.4        24            7.0.0.3       38     Inter   0

3.3.3.48/32 (R), range size 1
   Adv-rtr        Area          LSID          SID    Type    Algo
i  3.3.3.3        0             7.0.0.3       48     Intra   0
s  4.4.4.4        24            7.0.0.4       48     Inter   0

22.0.22.29/32 (R), range size 1
   Adv-rtr        Area          LSID          SID    Type    Algo
i  2.2.2.2        0             7.0.0.6       29     Intra   1
s  4.4.4.4        24            7.0.0.5       29     Inter   1

22.1.22.99/32 (R), range size 1
   Adv-rtr        Area          LSID          SID    Type    Algo
i  2.2.2.2        0             7.0.0.7       99     Intra   1
s  4.4.4.4        24            7.0.0.6       99     Inter   1

33.0.33.39/32 (R), range size 1
   Adv-rtr        Area          LSID          SID    Type    Algo
i  3.3.3.3        0             7.0.0.4       39     Intra   1
s  4.4.4.4        24            7.0.0.7       39     Inter   1

33.3.33.49/32 (R), range size 1
   Adv-rtr        Area          LSID          SID    Type    Algo
i  3.3.3.3        0             7.0.0.5       49     Intra   1
s  4.4.4.4        24            7.0.0.8       49     Inter   1
```

```
Device#show ip ospf segment-routing local-prefix
            OSPF Router with ID (10.0.0.7) (Process ID 10)
Area 0:
 Prefix:            Sid:   Index:          Type:      Algo: Source:
 2.2.2.2/32         2      0.0.0.0         Intra      0     Loopback0
                         22     0.0.0.0         Intra      1     Loopback0
 23.23.23.4/32      233    0.0.0.1         Intra      1     Loopback3
```

OSPFv2 セグメント ルーティングの厳格な SPF 機能の確認

```
Device#show ip ospf database opaque-area type router-information self

            OSPF Router with ID (10.0.0.4) (Process ID 10)

                Type-10 Opaque Area Link States (Area 0)

  LS age: 1692
  Options: (No TOS-capability, DC)
  LS Type: Opaque Area Link
  Link State ID: 4.0.0.0
  Opaque Type: 4 (Router Information)
  Opaque ID: 0
  Advertising Router: 4.4.4.4
  LS Seq Number: 80000002
  Checksum: 0x72B
  Length: 60

    TLV Type: Router Information
    Length: 4
```

```
    Capabilities:
      Graceful Restart Helper
      Stub Router Support
      Traffic Engineering Support

    TLV Type: Segment Routing Algorithm
    Length: 2
      Algorithm: SPF
      Algorithm: Strict SPF

    TLV Type: Segment Routing Range
    Length: 12
      Range Size: 8000

      Sub-TLV Type: SID/Label
      Length: 3
        Label: 16000

    TLV Type: Segment Routing Node MSD
    Length: 2
      Sub-type: Node Max Sid Depth, Value: 10
```

OSPF ローカル RIB データベースで使用される厳格な SPF ラベルの確認

```
Device#show ip ospf rib 10.0.0.8

            OSPF Router with ID (10.0.0.6) (Process ID 10)


                Base Topology (MTID 0)

OSPF local RIB
Codes: * - Best, > - Installed in global RIB
LSA: type/LSID/originator

*>  2.0.2.100/32, Intra, cost 21, area 0
     SPF Instance 28, age 00:01:19
      contributing LSA: 10/7.0.0.3/2.2.2.2 (area 0)
     SID: 100, Properties: Sid, LblRegd, SidIndex, N-Flag, TeAnn
     Strict SPF SID: 101, Properties: Force, Sid, LblRegd, SidIndex, N-Flag
     Flags: RIB, HiPrio
      via 3.6.0.3, Ethernet0/1, label 16100, strict label 16101
       Flags: RIB
       LSA: 1/2.2.2.2/2.2.2.2
      PostConvrg repair path via 5.6.0.5, Ethernet0/3, label 16100, strict label 16100,
 cost 31
       Flags: RIB, Repair, PostConvrg, IntfDj, BcastDj
       LSA: 1/2.2.2.2/2.2.2.2
```

厳格な SPF TILFA トンネルの確認

```
Device#show ip ospf fast-reroute ti-lfa tunnels internal

            OSPF Router with ID (10.0.0.2) (Process ID 10)

                        Area with ID (0)

                    Base Topology (MTID 0)


TI-LFA Release Node Tree:
```

```
TI-LFA Release Node 4.4.4.4 via 1.2.0.1 Ethernet0/0, instance 12, metric 20
  Interface MPLS-SR-Tunnel2
    Tunnel type: MPLS-SR (strict spf)
    Tailend router ID: 4.4.4.4
    Termination IP address: 4.4.4.4
    Outgoing interface: Ethernet0/0
    First hop gateway: 1.2.0.1
    instance 12, refcount 1
      rn-1: rtrid 4.4.4.4, addr 4.4.4.4, strict node-sid label 16044

TI-LFA Release Node 4.4.4.4 via 2.3.0.3 Ethernet0/1, instance 12, metric 20
  Interface MPLS-SR-Tunnel1
    Tunnel type: MPLS-SR (strict spf)
    Tailend router ID: 4.4.4.4
    Termination IP address: 4.4.4.4
    Outgoing interface: Ethernet0/1
    First hop gateway: 2.3.0.3
    instance 12, refcount 1
      rn-1: rtrid 4.4.4.4, addr 4.4.4.4, strict node-sid label 16044


TI-LFA Node Tree:

TI-LFA Node 1.1.1.1 via 1.2.0.1 Ethernet0/0, abr, instance 12, rspt dist 0
  not-in-ext-p-space, in-q-space, interesting node 1
  Link Protect strict Path-1: via 2.3.0.3 Et0/1, parent 1/4.4.4.4, metric:30,
rls-pt:4.4.4.4 at dist:20
  repair:y, rn-cnt:1, first-q:4.4.4.4, rtp-flags:Repair, PostConvrg, IntfDj
    rn-1: rtrid 4.4.4.4, addr 4.4.4.4, strict node-sid label 16044
    Protected by: MPLS-SR-Tunnel1, tailend 4.4.4.4, rls node 4.4.4.4
    instance 12, metric 20, refcount 1


TI-LFA Node 3.3.3.3 via 2.3.0.3 Ethernet0/1, instance 12, rspt dist 0
  not-in-ext-p-space, in-q-space, interesting node 1
  Link Protect strict Path-1: via 1.2.0.1 Et0/0, parent 1/4.4.4.4, metric:30,
rls-pt:4.4.4.4 at dist:20
  repair:y, rn-cnt:1, first-q:4.4.4.4, rtp-flags:Repair, PostConvrg, IntfDj
    rn-1: rtrid 4.4.4.4, addr 4.4.4.4, strict node-sid label 16044
    Protected by: MPLS-SR-Tunnel2, tailend 4.4.4.4, rls node 4.4.4.4
    instance 12, metric 20, refcount 1

TI-LFA Node 4.4.4.4 via 1.2.0.1 Ethernet0/0, abr, instance 12, rspt dist 10
  in-ext-p-space, in-q-space, interesting node 1
  Link Protect strict Path-1: via 2.3.0.3 Et0/1, parent 1/3.3.3.3, metric:20,
rls-pt:3.3.3.3 at dist:10
  repair:y, rn-cnt:0, first-q:4.4.4.4, rtp-flags:Repair, PostConvrg, IntfDj, PrimPath
    Protected by: directly connected TI-LFA

TI-LFA Node 4.4.4.4 via 2.3.0.3 Ethernet0/1, abr, instance 12, rspt dist 10
  in-ext-p-space, in-q-space, interesting node 1
  Link Protect strict Path-1: via 1.2.0.1 Et0/0, parent 1/1.1.1.1, metric:20,
rls-pt:1.1.1.1 at dist:10
  repair:y, rn-cnt:0, first-q:4.4.4.4, rtp-flags:Repair, PostConvrg, IntfDj, PrimPath
    Protected by: directly connected TI-LFA


TI-LFA Protected neighbors:

  Neighbor 1.2.0.1 Ethernet0/0, ID 1.1.1.1, Dist 10, instance 12
    TI-LFA Required, TI-LFA Computed, RLFA not Required
```

```
    TI-LFA protection Required: link

  Neighbor 2.3.0.3 Ethernet0/1, ID 3.3.3.3, Dist 10, instance 12
    TI-LFA Required, TI-LFA Computed, RLFA not Required
    TI-LFA protection Required: link
```

厳格な SPF SR-TE トンネルの確認

```
Device#show mpls traffic-eng segment-routing ospf summary
IGP Area[1]:  ospf 10  area 0, Strict SPF Enabled:
Nodes:
IGP Id: 1.1.1.20, MPLS TE Id: 1.1.1.1, OSPF area 0
   2 links with segment-routing adjacency SID
IGP Id: 2.0.0.0, MPLS TE Id: 2.2.2.2, OSPF area 0
   2 links with segment-routing adjacency SID
IGP Id: 3.0.0.0, MPLS TE Id: 3.3.3.3, OSPF area 0
   3 links with segment-routing adjacency SID
IGP Id: 4.4.4.4, MPLS TE Id: 4.4.4.4, OSPF area 0
   3 links with segment-routing adjacency SID
IGP Id: 5.0.0.0, MPLS TE Id: 5.5.5.5, OSPF area 0
   2 links with segment-routing adjacency SID
Prefixes:
1.1.1.1/32, SID index: 1, Strict SID index: 11
1.2.0.2/32
2.2.2.2/32, SID index: 2, Strict SID index: 22
2.2.2.22/32, SID index: 222, Strict SID index: 2222
3.3.3.3/32, SID index: 3, Strict SID index: 34
3.3.3.33/32, SID index: 333, Strict SID index: 1333
4.4.4.4/32, SID index: 4, Strict SID index: 444
5.5.5.5/32, SID index: 5, Strict SID index: 555
6.6.6.6/32, SID index: 6
7.7.7.7/32, SID index: 7
Total:
  Node Count          : 5
  Adjacency-SID Count: 17
  Prefix-SID Count    : 10
Grand Total:
  Node Count          : 5
  Adjacency-SID Count: 17
  Prefix-SID Count    : 10
  IGP Areas Count     : 1
```

厳格な SPF 修復パスを使用して保護された adj-SID の確認

```
Device#sh ip ospf segment-routing protected-adjacencies detail

            OSPF Router with ID (10.0.0.0) (Process ID 10)

                        Area with ID (0)

Nbr id 10.0.0.1, via 10.0.0.2 on Ethernet0/1, Label 26
  Primary path: via 10.0.0.2 on Et0/1, out-label 3
  Repair path: via 10.0.0.3 on Et0/2, out-label 13222, cost 31, labels 0
  Nbr Prefix 10.0.0.4, Strict
Nbr id 10.0.0.5, via 10.0.0.3 on Ethernet0/2, Label 25
  Primary path: via 10.0.0.3 on Et0/2, out-label 3
  Repair path: via 10.0.0.2 on Et0/1, out-label 12333, cost 21, labels 0
  Nbr Prefix 10.0.0.5, Strict
```

セグメント ルーティング グローバル ブロックの確認

```
Device#show ip ospf segment-routing global-block

            OSPF Router with ID (10.0.0.0) (Process ID 10)

OSPF Segment Routing Global Blocks in Area 0

  Router ID:      SR Capable: SR Algorithm: SRGB Base: SRGB Range:  SID/Label:

 *10.0.0.0         Yes         SPF,StrictSPF 16000      8000         Label
  10.0.0.1         Yes         SPF,StrictSPF 16000      8000         Label
  10.0.0.2         Yes         SPF,StrictSPF 16000      8000         Label
  10.0.0.3         Yes         SPF           16000      8000         Label
  10.0.0.4         Yes         SPF,StrictSPF 16000      8000         Label
  10.0.0.5         No
  10.0.0.6         Yes         SPF           16000      8000         Label
Device#
```

OSPFv2セグメントルーティングの厳格なSPFに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

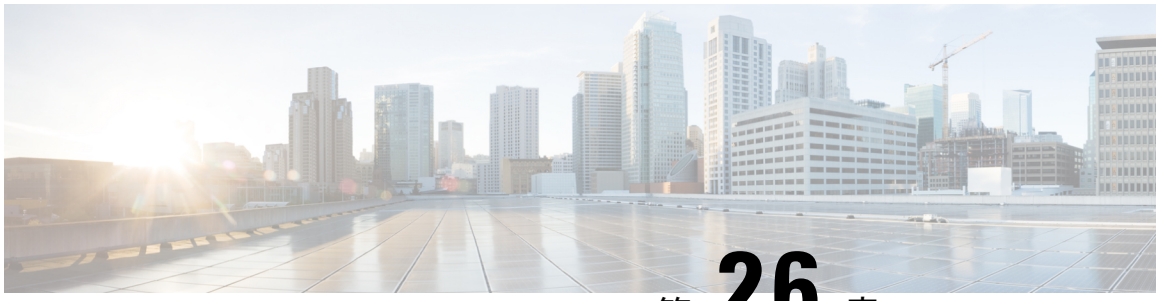
OSPFv2セグメントルーティングの厳格なSPFに関する機能情報

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 *25 : OSPFv2* セグメント ルーティングの厳格な *SPF* に関する機能情報

機能名	リリース	機能情報
OSPFv2 セグメント ルーティングの厳格な SPF	Cisco IOS XE Fuji 16.9.1	OSPFv2 セグメント ルーティングの厳格な SPF 機能は、厳格な最短パス アルゴリズムをサポートするためのプロビジョニングを提供します。パケットが SPF アルゴリズムに従って転送されることを強制し、SPF 決定を上書きする可能性のあるローカル ポリシーを無視するようにパス内のルータに指示します。 次のコマンドが追加または修正されました。 **address-family ipv4 strict-spf**。



第 26 章

セグメント ルーティング OSPFv2 マイクロループ回避

この機能により、IS-IS や OSPF などのリンクステート ルーティング プロトコルを使用して、トポロジ変更後のネットワーク コンバージェンス中に発生するマイクロループを防止または回避することができます。

セグメント ルーティング OSPFv2 マイクロループ回避に関する機能情報

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 *26 :* セグメント ルーティング *OSPFv2* マイクロループ回避に関する機能情報

機能名	リリース	機能情報
セグメント ルーティング OSPFv2 マイクロループ回避	Cisco IOS XE ジブラルタル 16.10.1	セグメント ルーティング マイクロループ回避により、IS-IS や OSPF などのリンクステート ルーティング プロトコルを使用して、トポロジ変更後のネットワーク コンバージェンス中に発生するマイクロループを防止または回避することができます。 この機能により、次のコマンドが導入または変更されました。**microloop avoidance segment-routing**。

セグメント ルーティング OSPFv2 マイクロループ回避に関する情報

マイクロループは、トポロジの変更（リンク ダウン、リンク アップ、またはメトリック変更イベント）後にネットワークで発生する短いパケットループです。マイクロループは、ネットワーク内の異なるノードの非同時コンバージェンスによって引き起こされます。ノードが収束し、収束していないネイバー ノードにトラフィックを送信すると、これら2つのノード間でトラフィックがループし、パケット損失、ジッター、および順不同パケットが発生する可能性があります。

セグメント ルーティング マイクロループ回避機能によってトポロジの変更が検出されると、セグメントのリストを使用して宛先へのループフリー パスが作成されます。

マイクロループ

リンクまたはネットワーク デバイスで発生した障害や復旧のためにネットワーク トポロジに変更が生じると、IP Fast Reroute によって迅速なネットワーク コンバージェンスが行われます。このとき、定期的なコンバージェンス機能によってトラフィックが新しく計算されたベストパス（別名、ポスト コンバージェンス パス）へ移動されるまで、事前に計算されていたバックアップ パスにトラフィックが移動されます。このネットワーク コンバージェンスにより、トポロジ内で直接または間接的に接続された2台のデバイス間で、マイクロループが短期間発生する可能性があります。マイクロループは、ネットワーク内の異なるノードが異なるタイミングで互いに別々に代替パスを計算したときに発生します。たとえば、あるノードがコンバージェンスを実行し、ネイバー ノードにトラフィックを送信したときに、そのネイバー ノードでまだコンバージョンが完了していないと、その2つのノードでトラフィックがループする可能性があります。

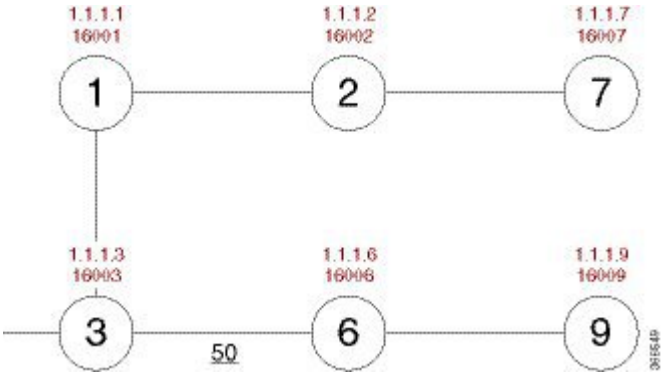
マイクロループによってトラフィックが損失する場合も、損失しない場合もあります。マイクロループが発生している期間が短ければ、つまりネットワークのコンバージェンスが迅速に行われれば、存続可能時間（TTL）が期限切れになるまでの短い期間、パケットがループする可能性があります。最終的には、パケットは宛先に転送されます。マイクロループの期間が長く

なる、つまりネットワーク内のいずれかのルータでコンバージェンスに時間がかかっていると、パケットで TTL が期限切れになったり、パケット レートが帯域幅を超過したり、パケットの順番が狂ったり、パケットがドロップされたりする場合があります。

障害が発生したデバイスとそのネイバーとの間で形成されたマイクロループはローカル ユーループと呼ばれます。また複数ホップ離れたデバイスとの間で形成されるマイクロループはリモート ユーループと呼ばれます。ローカル ユーループは、通常はローカルのループフリー代替（LFA）パスが使用できないネットワークで見られます。このようなネットワークでは、リモート LFA によってネットワークのバックアップ パスが提供されます。

上で説明した情報は、トポロジ例を参考にして示すことができます。

図 *29 :* マイクロループのトポロジの例



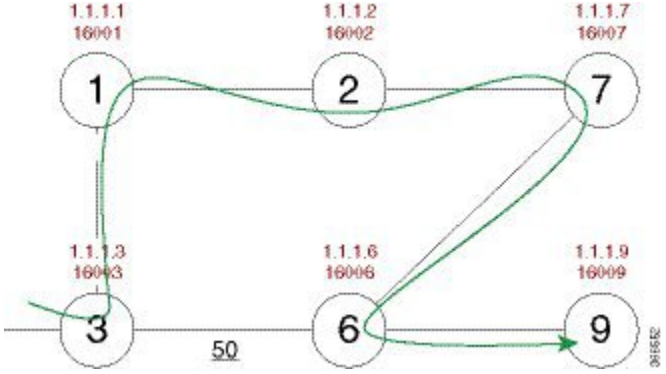
この例の前提条件は次のとおりです。

- デフォルトのメトリックは、メトリックが 50 であるノード 3 とノード 6 間のリンクを除き、各リンクごとに 10 です。各ノードでの SPF バックオフ遅延の収束順序は次のとおりです。
  - ノード 3 : 50 ミリ秒
  - ノード 1 : 500 ミリ秒
  - ノード 2 : 1 秒
  - ノード 7 : 1.5 秒

ノード 3 からノード 9（宛先）に送信されたパケットは、ノード 6 経由で通過します。

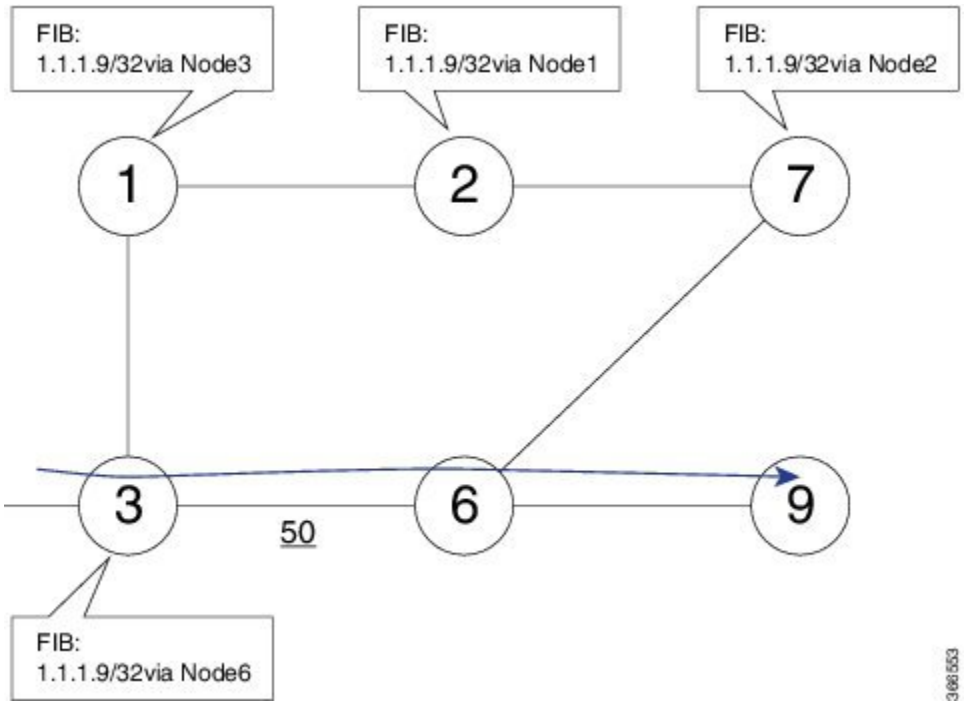
ノード 6 とノード 7 の間でリンクが確立されている場合、パケットが宛先であるノード 9 に到達する前のノード 3 からノード 9 へのパケットの最短パスは、ノード 1、ノード 2、ノード 7、およびノード 6 になります。

図 *30 :* マイクロループのトポロジの例：最短パス



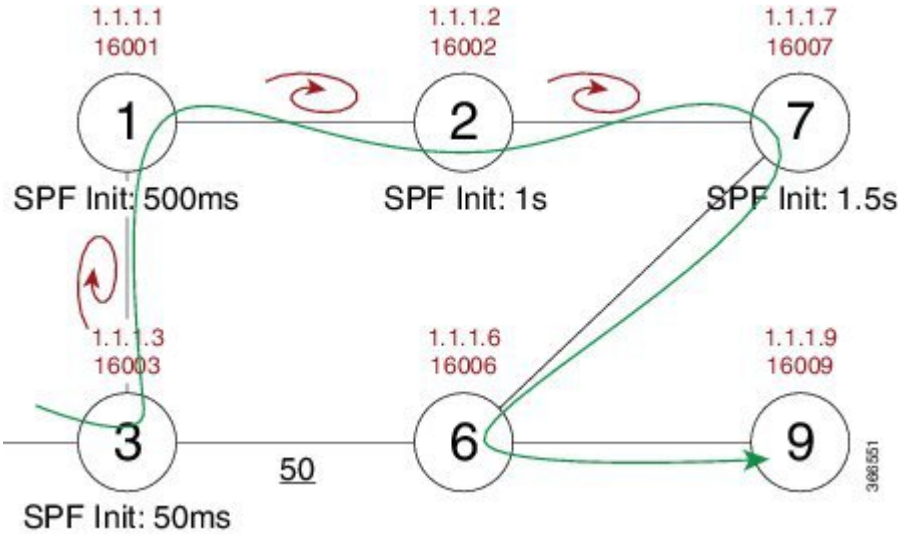
次の図は、ノード6とノード7間のリンクが確立される前の各ノードの転送情報ベース（FIB）テーブルを示しています。FIB エントリには、宛先ノード（ノード 9）のプレフィックスとネクスト ホップが含まれます。

図 *31 :* マイクロループのトポロジの例：*FIB* エントリ



ノード6とノード7間のリンクがアップすると、各ノードのコンバージェンスの順序に基づいて、マイクロループがリンクに対して発生します。この例では、ノード3は最初にノード1で収束し、その結果ノード3とノード1の間にマイクロループが発生します。その後、ノード1が次に収束し、その結果ノード1とノード2の間にマイクロループが発生します。次に、ノード2が次に収束し、その結果ノード2とノード7の間にマイクロループが発生します。最後に、次の図に示すように、ノード7はマイクロループの解決を収束し、パケットが宛先ノード9に到達します。

図 *32 :* マイクロループのトポロジの例：マイクロループ

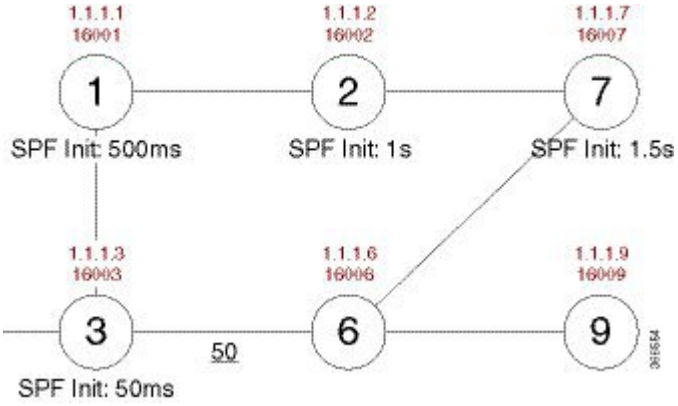


SPF コンバージェンス遅延を追加すると、マイクロループは 1.5 秒間（ノード 7 に指定されたコンバージェンス期間）接続を失うことになります。

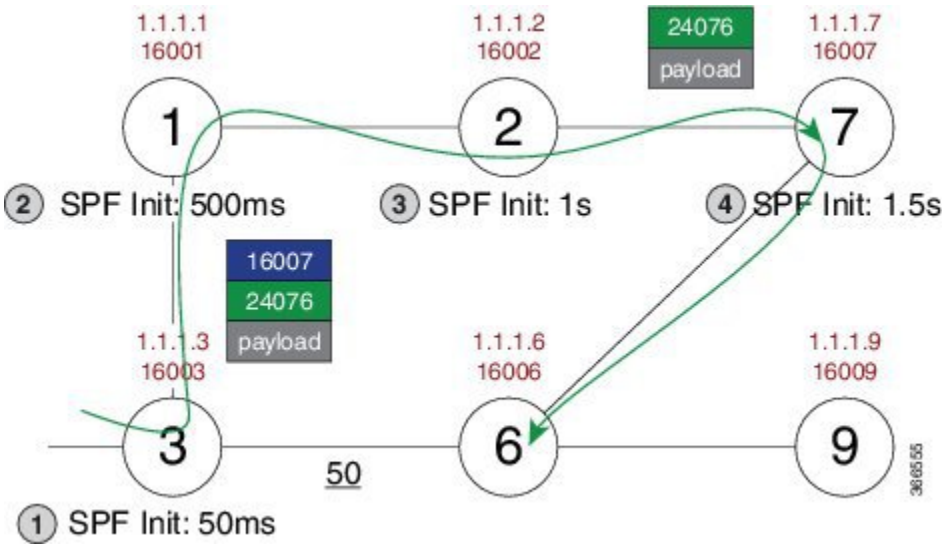
セグメント ルーティングを使用したマイクロループの防止

このセクションでは、例を使用して、セグメント ルーティングがマイクロループを防ぐ方法について説明します。この例のノード 3 は、**microloop avoidance segment-routing** コマンドで有効になっています。

図 *33 :* マイクロループのトポロジの例：セグメント ルーティング



FIB テーブルを更新する代わりに、ノード 3 は、ノード 7 のプレフィックス セグメント ID（SID）である 16007 を含むセグメント ID のリストと、ノード 6 の隣接関係セグメント ID（SID）である 24076 を使用して、宛先（ノード 9）のダイナミック ループフリー パスを構築します。



したがって、ノード 3 からのパケットが宛先ノード 9 に到達することが可能になり、ネットワークが収束するまでマイクロループのリスクがなくなります。最後に、ノード 3 は新しいパスで FIB を更新します。

セグメント ルーティング OSPFv2 マイクロループ回避の前提条件

SR マイクロループ回避を設定する前に、セグメント ルーティングが OSPF ルータ モードでグローバルに設定されていることを確認してください。

```
router ospf process
segment-routing mpls
```

セグメント ルーティング OSPFv2 マイクロループ回避の制約事項

- セグメント ルーティング OSPFv2 マイクロループ回避は、マルチ トポロジ ルーティング（MTR）をサポートしていません。MTID 0 のみをサポートしています。
- コンバージェンス後のパスに沿ったセグメント ID のリストは、リスト内のノードが SR に対応していて、ノード SID が少なくとも 1 つある場合にのみ使用されます。それ以外の場合、OSPF はコンバージェンス後のパスをただちにインストールします。
- SR マイクロループ回避は、ポイントツーポイント インターフェイスと 2 つのネイバーのみのブロードキャスト インターフェイスのリンク アップ、リンク ダウン、およびリンク メトリック変更イベントに使用されます。

- SR マイクロループ回避は、1 つのトポロジ変更に対してのみ使用できます。複数のトポロジ変更が発生すると、OSPF はコンバージェンス後のパスをすぐにインストールします。

セグメント ルーティング OSPFv2 マイクロループ回避の設定

すべてのプレフィックスのセグメント ルーティング マイクロループ回避を有効にします。

```
router ospf
 microloop avoidance segment-routing
 microloop avoidance rib-update-delay delay-time
```

microloop avoidance rib-update-delay *delay-time* コマンドを使用して、ノードのフォワーディングテーブルを更新する前にノードが待機する遅延時間をミリ秒単位で設定し、マイクロループ回避の使用を停止します。RIB 遅延のデフォルト値は 5000 ミリ秒です。

セグメント ルーティング OSPFv2 マイクロループ回避の確認

show ip ospf segment-routing microloop avoidance コマンドを使用して、SR マイクロループ回避が有効かどうかを確認します。

セグメント ルーティング OSPFv2 マイクロループ回避の追加情報

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』