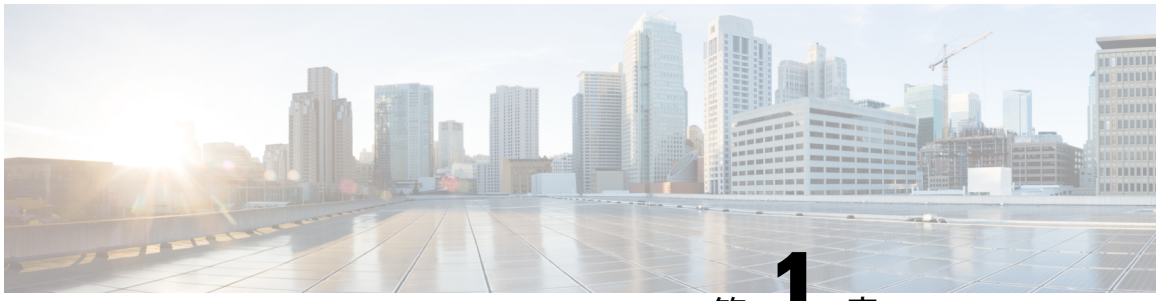
Cisco NCS 560 シリーズ ルータ（IOS XR リリース 7.1.x）セグメント ルーティング コンフィギュレーション ガイド

初版：2020 年 1 月 29 日

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

目 次



第 1 章

セグメント ルーティングについて

この章では、セグメント ルーティングの概念およびセグメント ルーティングを設定するためのワークフローについて説明します。

スコープ

セグメント ルーティングは、送信元のルーティング パラダイムに基づいてネットワーク上でパケットを転送する方法です。送信元はパスを選択し、パケット ヘッダーでセグメントの番号付きリストとしてエンコードします。セグメントは、任意のタイプの命令の識別子です。例えば、トポロジ セグメントは、宛先へのネクスト ホップを識別します。各セグメントを識別するセグメント ID（SID）は、フラットな 20 ビットの符号なし整数からなります。

セグメント

内部ゲートウェイ プロトコル（IGP）は、2 つのタイプのセグメント、プレフィックス セグメントと隣接関係セグメントを配布します。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。

- プレフィックス SID は、IP プレフィックスに関連付けられます。プレフィックス SID は、ラベルのセグメント ルーティング グローバル ブロック（SRGB）の範囲から手動で設定され、IS-IS または OSPF によって配布されます。プレフィックス セグメントは、その宛先への最短パスに沿ってトラフィックを誘導します。ノード SID は、特定のノードを識別する特別なタイプのプレフィックス SID です。ノードのループバック アドレスをプレフィックスとして使用して、ループバック インターフェイスの下に設定されます。

  プレフィックス セグメントはグローバル セグメントであるため、プレフィックス SID はセグメント ルーティング ドメイン内でグローバルに一意です。

- 隣接関係セグメントは、隣接ルータへの出力インターフェイスなどの特定の隣接関係を表す、隣接関係 SID と呼ばれるラベルによって識別されます。隣接関係 SID は、動的ラベル

の範囲から動的に割り当てることも、ラベルのセグメント ルーティング ローカル ブロック（SRLB）の範囲から手動で設定することもできます。隣接関係 SID は、IS-IS または OSPF によって配布されます。隣接関係セグメントは、トラフィックを特定の隣接関係に誘導します。

隣接関係セグメントはローカル セグメントであるため、隣接関係 SID は特定のルータに対してローカルに一意です。

番号付きリストでプレフィックス（ノード）と隣接関係セグメント ID を組み合わせることにより、ネットワーク内で任意のパスを構築できます。各ホップにおいて、先頭のセグメントがネクスト ホップを識別するために使用されます。セグメントはパケット ヘッダーの先頭に順番にスタックされます。先頭のセグメントに別のノードの ID が含まれている場合、受信ノードは等コスト マルチパス（ECMP）を使用してパケットをネクスト ホップに移動させます。ID が受信ノードの ID である場合、ノードは先頭のセグメントをポップし、次のセグメントに必要なタスクを実行します。

データ プレーン

セグメント ルーティングは、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することができ、フォワーディング プレーンは変更されません。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。

サービス

セグメント ルーティングは、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、MPLS の豊富なマルチサービス機能と統合されています。

トラフィック エンジニアリング用のセグメント ルーティング

トラフィック エンジニアリング用のセグメント ルーティング（SR-TE）は、送信元と宛先のペア間のポリシーを通じて行われます。トラフィック エンジニアリング用のセグメント ルーティングでは、送信元ルーティングの概念が使用されます。送信元はパスを計算し、パケット ヘッダーでセグメントとしてエンコードします。各セグメントは、送信元から宛先までのエンドツーエンドのパスであり、プロバイダー コア ネットワークのルータに、IGP によって計算された最短パスではなく指定されたパスに従うように指示します。宛先はポリシーの存在を認識しません。

必要性

トラフィック エンジニアリング用のセグメント ルーティング（SR-TE）では、ネットワークはアプリケーション単位およびフロー単位の状態を維持する必要はありません。代わりに、パケットで提供されている転送指示に従うだけです。

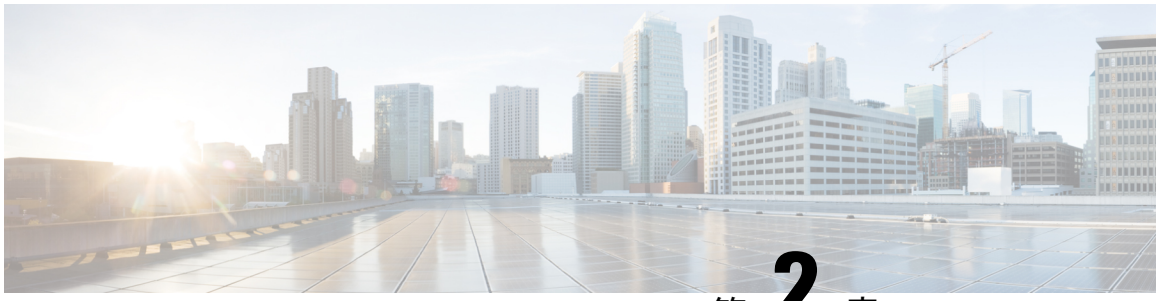
SR-TE は、すべてのセグメント レベルで ECMP を使用することにより、従来の MPLS-TE ネットワークよりも効果的にネットワーク帯域幅を利用します。単一のインテリジェント ソースを使用し、残りのルータをネットワーク経由で必要なパスを計算するタスクから解放します。

利点

- **SDN 対応**：セグメント ルーティングは SDN 向けに構築され、Application Engineered Routing（AER）の基礎となります。SR は、アプリケーションがネットワークの行動を指示できるビジネス モデル用のネットワークを準備します。SR は、分散されたインテリジェンスと集中化された最適化およびプログラミングの間の適切なバランスを提供します。
- **最小構成**：TE のセグメント ルーティングでは、送信元ルータで最小構成が必要です。
- **ロード バランシング**：RSVP-TE とは異なり、セグメント ルーティングのロード バランシングは、Equal Cost Multipath（ECMP; 等コスト マルチパス）の存在下で実行できます。
- **Fast Reroute（FRR）をサポート**：Fast Reroute により、パス障害の 50 ミリ秒以内に事前設定されたバックアップ パスの有効化が可能になります。
- **プラグアンドプレイ展開**：セグメント ルーティング ポリシーは、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を展開するためのワークフロー

セグメント ルーティングを展開するには、次のワークフローに従います。



第 2 章

セグメント ルーティング グローバル ブロックおよびセグメントルーティングローカル ブロックの設定

ローカル ラベルの割り当てはラベル スイッチング データベース（LSD）によって管理されます。セグメント ルーティング グローバル ブロック（SRGB）およびセグメント ルーティング ローカル ブロック（SRLB）は LSD のセグメント ルーティングに対して保持されるラベル値です。

セグメント ルーティング グローバル ブロックについて

SRGB ラベル値は SR 対応ノードへのプレフィックス セグメント識別子（SID）として割り当てられ、ドメイン全体でグローバルな意味を持ちます。

（注） 範囲から割り当てられた値はドメイン全体で重要な意味を持つため、ドメイン内のすべてのルータに同じ値の範囲を設定することをお勧めします。

デフォルトの SRGB の範囲は 16000 ～ 23999 です。

（注） SR 対応ルータでは、実行中のシステムで SR が有効になっているときにデフォルトの SRGB ラベル値（16000 ～ 23999）を使用できるように、動的ラベル範囲のデフォルトの開始値が 16000 ～ 24000 に増加します。動的ラベルの範囲が開始値 16000 で設定されている場合、実行中のシステムで SR が有効になっている場合は、デフォルトの SRGB ラベル値がすでに使用されている可能性があります。したがって、SR を有効にした後にルータをリロードして、現在割り当てられているラベルを解放し、SRGB を割り当てる必要があります。

また、SR を有効にした後で SRGB の範囲を増やす必要がある場合は、ルータをリロードして、現在割り当てられているラベルを解放し、新しい SRGB を割り当てる必要があります。

セグメント ルーティングの設定を簡易に保ち、セグメント ルーティングの問題のトラブルシューティングを容易にするため、ドメイン内の各ノードではデフォルトの SRGB 範囲を使用することをお勧めします。ただし、異なる範囲を定義する必要がある場合があります。次に例を示します。

- 別のベンダーのノードがデフォルトの SRGB とは異なるラベル範囲をサポートしていて、すべてのノードで同じ SRGB を使用したい場合。
- デフォルトの範囲が小さすぎる場合。
- 範囲が重複しない限り、IS-IS および OSPF プロトコルに別々の SRGB を指定する場合。

制約事項

- Cisco IOS XR リリース 6.2.x 以前では、LSD ラベル値 0 ～ 15999 が予約されています。Cisco IOS XR リリース 6.3.1 以降では、LSD ラベル値 0 ～ 14999 が予約されています。
- Cisco IOS XR リリース 6.2.x 以前では、最大 SRGB サイズは 65536 です。Cisco IOS XR リリース 6.3.1 以降では、最大 SRGB サイズは 262,143 です。
- 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。

（注） 事前に予約されていないラベル値は、動的割り当てに使用できます。

SR を使用しない場合は、SRGB を無効にできます。

セグメント ルーティング ローカル ブロックについて

セグメントルーティング ローカルブロック（SRLB）は、隣接関係セグメント識別子（adj-SID）の手動割り当てのために保存されているラベル値の範囲です。これらのラベルはローカルで重要であり、ラベルを割り当てるノードでのみ有効です。デフォルトの SRLB の範囲は 15000 ～ 15999 です。

（注） SRLB を使用して手動で割り当てられない隣接関係 SIDは、動的ラベルの範囲から動的に割り当てられます。

セグメント ルーティングの設定を簡易に保ち、セグメント ルーティングの問題のトラブルシューティングを容易にするため、デフォルトのSRLB範囲を使用することをお勧めします。ただし、異なる範囲を定義する必要がある場合があります。次に例を示します。

- 別のベンダーのノードがデフォルトのSRLBとは異なるラベル範囲をサポートしていて、すべてのノードで同じ SRLB を使用したい場合。
- デフォルトの範囲が小さすぎる場合。

新しいSRLB範囲を定義すると、ラベルの競合が発生する可能性があります（たとえば、新しいSRLB範囲でラベルがすでに静的または動的に割り当てられている場合など）。この場合、新しい SRLB 範囲は受け入れられますが、適用はされません（保留中）。以前の SRLB 範囲（アクティブ）は、次のいずれかを行うまで引き続き使用されます。

- ルータをリロードして、現在割り当てられているラベルを解放し、新しいSRLBを割り当てる。
- **clear segment-routing local-block discrepancy all** コマンドを使用してラベルの競合をクリアする。

制約事項

- LSD ラベル値 0 ～ 14999 は予約されています。
- SRLB のサイズは 262,143 を超えることはできません。
- SRLB 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。

（注） SRLB（セグメントルーティング ローカルブロック）の不整合および割り当て失敗エラーは、SRLB および SRGB（セグメント ルーティング グローバル ブロック）にデフォルト以外の値が設定され、commit-replaceの後に設定の再適用が続く場合に発生します。SR ラベルが適切にプログラムされていないため、この問題はデータ転送に影響を及ぼします。

この問題を回避するには、**clear segment-routing local-block discrepancy all** コマンドを使用してラベルの競合をクリアします。

SR を使用しない場合は、SRLB を無効にできます。

非デフォルトセグメントルーティンググローバルブロック範囲の設定

このタスクでは、デフォルト以外の SRGB 範囲を設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	[**router** { **isis** *instance-id* | **ospf** *process_name*}] 例： `RP/0/RP0/cpu 0: router(config)# router isis 1`	（任意）IS-IS および OSPF プロトコル用に個別の SRGB を設定する場合は、**router isis** *instance-id* または **router ospf** *process_name* コマンドを入力します。
ステップ 3	**segment-routing global-block** *starting_value ending_value* 例： `RP/0/RP0/cpu 0: router(config-isis)# segment-routing global-block 18000 19999`	SRGB範囲に開始値として含める最小値を入力します。SRGB範囲に終了値として含める最大値を入力します。
ステップ 4	**commit**	

SRGB 設定を確認します。

```
RP/0/RP0/cpu 0: router# show mpls label table detail
Table Label   Owner                              State  Rewrite
----- ------- ---------------------------------- ------ -------

<...snip...>

0     18000   ISIS(A):1                          InUse  No
   Lbl-blk SRGB, vers:0, (start_label=18000, size=2000)
0     24000   ISIS(A):1                          InUse  Yes
   (SR Adj Segment IPv4, vers:0, index=1, type=0, intf=Gi0/0/0/0, nh=10.0.0.2)
```

次のタスク

プレフィックス SID を設定し、セグメント ルーティングを有効にします。

非デフォルト セグメント ルーティング ローカル ブロック範囲の設定

このタスクでは、デフォルト以外の SRLB 範囲を設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**segment-routing local-block** *starting_value ending_value* **例：** `RP/0/RP0/cpu 0: router(config)# segment-routing local-block 30000 30999`	SRLB 範囲に開始値として含める最小値を入力します。SRLB 範囲に終了値として含める最大値を入力します。
ステップ 3	**commit**	

SRLB 設定を確認します。

```
RP/0/RP0/cpu 0: router# show mpls label table detail
Table Label   Owner                              State  Rewrite
----- ------- -------------------------------- ------ -------

<...snip...>

0     13      LSD(A)                           InUse  Yes
0     30000   LSD(A)                           InUse  No
  (Lbl-blk SRLB, vers:0, (start_label=30000, size=1000, app_notify=0)
0     30002   Static(A)                        InUse  Yes
```

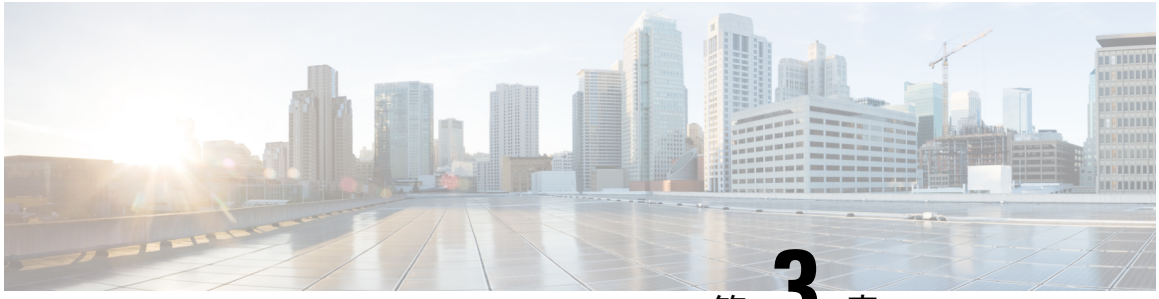
SRLB の不一致を表示し解決します。

```
RP/0/RP0/cpu 0: router# show segment-routing local-block inconsistencies
Tue Aug 15 13:53:30.555 EDT
SRLB inconsistencies range: Start/End: 30000/30009

RP/0/RP0/cpu 0: router# show mpls lsd private | i SRLB
Tue Aug 15 13:53:50.874 EDT
SRLB Lbl Mgr:
   Current Active SRLB block      = [15000, 15999]
   Configured Pending SRLB block  = [30000, 30009]

RP/0/RP0/cpu 0: router# clear segment-routing local-block discrepancy all
Tue Aug 15 13:59:46.897 EDT

RP/0/RP0/cpu 0: router# show mpls lsd private | i SRLB
```

```
Tue Aug 15 13:59:55.370 EDT
SRLB Lbl Mgr:
   Current Active SRLB block      = [30000, 30009]
   Configured Pending SRLB block  = [0, 0]

RP/0/RP0/cpu 0: router# show mpls label table detail private
Tue Aug 15 14:00:26.023 EDT
Table Label   Owner                              State  Rewrite
----- ------- -------------------------------- ------ -------
0     0       LSD(A)                           InUse  Yes
0     1       LSD(A)                           InUse  Yes
0     2       LSD(A)                           InUse  Yes
0     13      LSD(A)                           InUse  Yes
0     30000   LSD(A)                           InUse  No
  (Lbl-blk SRLB, vers:0, (start_label=30000, size=1000, app_notify=0)
```

次のタスク

隣接関係 SID を設定し、セグメント ルーティングを有効にします。



第 3 章

IS-IS プロトコル用のセグメント ルーティングの設定

Integrated Intermediate System-to-Intermediate System（IS-IS）、インターネット プロトコル バージョン 4（IPv4）は、標準ベースの内部ゲートウェイ プロトコル（IGP）です。Cisco IOS XR ソフトウェアは、国際標準化機構（ISO）/International Engineering Consortium（IEC）10589 および RFC 1995 に記載されている IP ルーティング機能を実装し、IP バージョン 6（IPv6）向けに標準拡張のシングル トポロジおよびマルチトポロジ IS-IS を追加しています。

このモジュールは、IS-IS のセグメント ルーティングを有効にするために使用される設定情報を提供します。

IS-IS プロトコル用のセグメント ルーティングの有効化

IS-IS コントロール プレーン上のセグメント ルーティングは、次をサポートしています。

- レベル 1、レベル 2、およびマルチレベルのルーティング
- ループバック インターフェイス上のホスト プレフィックスのプレフィックス SID
- 隣接関係用の隣接関係 SID
- MPLS penultimate hop popping（PHP）と明示的な NULL シグナリング

ここでは、IS-IS 用のセグメント ルーティングを有効にする方法について説明します。

始める前に

ルータで IS-IS のセグメント ルーティングを有効にする前に、ネットワークで MPLS Cisco IOS XR ソフトウェア機能をサポートする必要があります。

（注） ネットワークのトラフィック エンジニアリング部分にあるすべての IS-IS ルータ上で、次のタスク リストのコマンドを入力する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**router isis** *instance-id* 例： `RP/0/RP0/cpu 0: router(config)# router isis isp`	指定したルーティング インスタンスの IS-IS ルーティングを有効にし、ルータをルータ コンフィギュレーション モードにします。 （注） **is-type** ルータ コンフィギュレーション コマンドを使用して、特定のルーティング インスタンスによって実行されるルーティングのレベルを変更できます。
ステップ 3	**metric-style wide** ［ **level** ｛ **1** ｜ **2** ｝］ 例： `RP/0/RP0/cpu 0: router(config-isis-af)# metric-style wide level 1`	レベル 1 エリアでワイド リンク メトリックのみを生成して受け入れるようにルータを設定します。
ステップ 4	**segment-routing mpls** 例： `RP/0/RP0/cpu 0: router(config-isis-af)# segment-routing mpls`	セグメント ルーティングは、次の操作で有効になります。 • IS-IS がアクティブなすべてのインターフェイスで MPLS 転送が有効化される。 • 転送プレーン内のすべての既知プレフィックス SID が、リモート ルータによってアドバタイズされた、またはローカルまたはリモート マッピング サーバを介して学習されたプレフィックス SID を使用してプログラミングされる。

	コマンドまたはアクション	目的
		• ローカルで設定されたプレフィックス SID がアドバタイズされる。

ステップ 5	**exit**
	例：
	`RP/0/RP0/cpu 0: router(config-isis-af)# exit`
	`RP/0/RP0/cpu 0: router(config-isis)# exit`	

ステップ 6	**commit**	

次のタスク

プレフィックス SID を設定します。

IS-IS対応ループバックインターフェイスでのプレフィックス SID の設定

プレフィックスセグメント識別子（SID）は、IP プレフィックスに関連付けられます。プレフィックス SID は、ラベルのセグメント ルーティング グローバル ブロック（SRGB）の範囲から手動で設定されます。プレフィックスSIDは、ノードのループバックアドレスをプレフィックスとして使用して、ループバック インターフェイスの下に設定されます。プレフィックスセグメントは、その宛先への最短パスに沿ってトラフィックを誘導します。

プレフィックスSIDは、ノードSIDであることもエニーキャストSIDであることもあります。ノード SID は、特定のノードを識別するタイプのプレフィックス SID です。エニーキャスト SID は、一連のノードを識別するタイプのプレフィックス SID であり、n-flag-clear を使用して設定されます。一連のノード（エニーキャストグループ）は、共有プレフィックスアドレスとプレフィックスSIDをアドバタイズするように設定されます。エニーキャストルーティングにより、複数のアドバタイズノードへのトラフィックのステアリングが可能になります。エニーキャストアドレス宛てのパケットは、トポロジ的に最も近いノードに転送されます。

プレフィックス SID は、セグメント ルーティング ドメイン内でグローバルに一意です。

このタスクでは、IS-IS 対応ループバック インターフェイスでプレフィックス セグメント識別子（SID）のインデックスまたは絶対値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が対応するアドレス ファミリで有効になっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**router isis** *instance-id* 例： `RP/0/RP0/cpu 0: router(config)# router isis 1`	指定したルーティング インスタンスの IS-IS ルーティングを有効にし、ルータをルータ コンフィギュレーション モードにします。 • **is-type** ルータ コンフィギュレーション コマンドを使用して、特定のルーティング インスタンスによって実行されるルーティングのレベルを変更できます。
ステップ 3	**interface Loopback** *instance* 例： `RP/0/RP0/cpu 0: router(config-isis)# interface Loopback0`	ループバック インターフェイスとインスタンスを指定します。
ステップ 4	**commit**	

プレフィックス SID 設定を確認します。

隣接関係 SID の設定

隣接関係 SID（Adj-SID）は、隣接ノードへの隣接関係に関連付けられています。隣接関係 SID は、トラフィックを特定の隣接関係に誘導します。隣接関係 SID はローカルな意味を持ち、それらを割り当てるノードでのみ有効です。

隣接関係 SID は、動的ラベルの範囲から動的に割り当てることも、ラベルのセグメント ルーティング ローカル ブロック（SRLB）の範囲から手動で設定することもできます。

動的に割り当てられる隣接関係 SID には特別な構成は必要ありませんが、いくつかの制限があります。

- 動的に割り当てられた Adj-SID 値は、割り当てられるまで認識されず、情報が IGP によってフラッディングされるまでコントローラは Adj-SID 値を認識しません。
- 動的に割り当てられた Adj-SID は永続的ではなく、リロードまたはプロセスの再起動後に再割り当てすることができます。
- 各リンクには一意の Adj-SID 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。

手動で割り当てられた Adj-SID は、リロードおよび再起動後も永続的です。同じネイバーまたは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できます。Adj-SID が保護されることを指定できます。Adj-SID がプライマリ インターフェイスで保護されていて、バックアップ パスが利用可能な場合、バックアップ パスがインストールされます。デフォルトでは、手動 Adj-SID は保護されていません。

隣接関係 SID は、既存の IS-IS Adj-SID サブ TLV を使用してアドバタイズされます。S フラグと P フラグは、手動で割り当てられた Adj-SID に対して定義されています。

```
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|F|B|V|L|S|P|   |
+-+-+-+-+-+-+-+-+
```

表 *1*：隣接関係セグメント識別子（*Adj-SID*）のフラグ サブ *TLV* フィールド

フィールド	説明
S（セット）	このフラグは、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設定されます。
P（永続的）	このフラグは、Adj-SID が永続的（手動割り当て）の場合に設定されます。

手動で割り当てられた Adj-SID は、ポイントツーポイント（P2P）インターフェイスでサポートされています。

ここでは、インターフェイスに Adj-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が対応するアドレス ファミリで有効になっていることを確認します。

show mpls label table detail コマンドを使用して、SRLB の範囲を確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**router isis** *instance-id* 例： `RP/0/RP0/cpu 0: router(config)# router isis 1`	指定したルーティング インスタンスの IS-IS ルーティングを有効にし、ルータをルータ コンフィギュレーション モードにします。 • **is-type** ルータ コンフィギュレーション コマンドを使用して、特定のルーティング インスタンスによって実行されるルーティングのレベルを変更できます。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type interface-path-id* 例： `RP/0/RP0/cpu 0: router(config-isis)# interface GigabitEthernet0/0/0/7`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**point-to-point** 例： `RP/0/RP0/cpu 0: router(config-isis-if)# point-to-point`	インターフェイスがポイントツーポイント インターフェイスになるように指定します。

ステップ 5	**adjacency-sid** {**index** *adj-SID-index* | **absolute** *adj-SID-value* } [**protected**]
	例：
	`RP/0/RP0/cpu 0: router(config-isis-if-af)# adjacency-sid index 10`
	`RP/0/RP0/cpu 0: router(config-isis-if-af)# adjacency-sid absolute 15010`
		インターフェイスの Adj-SID インデックスまたは絶対値を設定します。
		SRLB + インデックスの下限に基づいて Ajd-SID を作成するには、各リンクに **index** *adj-SID-index* を指定します。
		SRLB 内に特定の Ajd-SID を作成するには、各リンクに **absolute** *adj-SID-value* を指定します。
		Adj-SID が **protected** であるかを指定します。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ていて、バックアップ パスが利用可能な場合、バックアップ パスがインストールされます。デフォルトでは、手動 Adj-SID は保護されていません。

ステップ 6	**commit**	

Adj-SID 設定を確認します。

ラベルが MPLS Forwarding Information Base（LFIB）に追加されていることを確認します。

```
RP/0/RP0/cpu 0: router# show mpls forwarding labels 15010
Mon Jun 12 02:50:12.172 PDT
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
15010  Pop         SRLB (idx 10)      Gi0/0/0/3    10.0.3.3        0
       Pop         SRLB (idx 10)      Gi0/0/0/7    10.1.0.5        0
       16004       SRLB (idx 10)      Gi0/0/0/7    10.1.0.5        0           (!)
       16004       SRLB (idx 10)      Gi0/0/0/3    10.0.3.3        0           (!)
```

レイヤ 2 隣接関係 SID の設定

通常、隣接関係 SID（Adj-SID）はネイバー ノードへのレイヤ 3 隣接に関連付けられ、トラフィックを特定の隣接関係に誘導します。複数の物理インターフェイスがバンドル インターフェイスを形成するレイヤ 2 バンドル インターフェイスを使用する場合、個々のレイヤ 2 バンドル メンバーは IGP には表示されません。バンドル インターフェイスのみが表示されます。

個々のレイヤ 2 バンドル インターフェイスにレイヤ 2 Adj-SID を設定できます。この設定により、個々のバンドル メンバー リンクの可用性を追跡し、運用管理および保守（OAM）のために個々のバンドル メンバー リンクを介してセグメント ルーティング転送を確認することができます。

レイヤ 2 Adj-SID は動的に割り当てることも、手動で設定することもできます。

- IGP は、レイヤ 2 バンドル メンバーごとに動的ラベル範囲からレイヤ 2 Adj-SID を動的に割り当てます。動的レイヤ 2 Adj-SID は永続的ではなく、レイヤ 2 バンドル リンクが稼働および停止したときに再割り当てできます。
- 手動で設定されたレイヤ 2 Adj-SID は、レイヤ 2 バンドル リンクが稼働および停止している場合は永続的です。レイヤ 2 Adj-SID は、ラベルのセグメント ルーティング ローカル ブロック（SRLB）から割り当てられます。ただし、レイヤ 2 Adj-SID の設定値が利用可能な SRLB 内に収まらない場合、レイヤ 2 Adj-SID は転送情報ベース（FIB）にはプログラムされません。

制約事項

- Adj-SID 転送にはネクストホップが必要です。これは IPv4 アドレスまたは IPv6 アドレスのいずれかで指定できますが、両方を指定することはできません。そのため、手動で設定されたレイヤ 2 Adj-SID は address-family ごとに設定されます。
- 手動で設定されたレイヤ 2 Adj-SID は、1 つのレイヤ 2 バンドル メンバー リンクにのみ関連付けることができます。
- レイヤ 2 Adj-SID に使用される SID 値はレイヤ 3 Adj-SID と共有することはできません。
- レイヤ 2 Adj-SID を使用した SR-TE はサポートされていません。

ここでは、インターフェイスにレイヤ 2 Adj-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 ルーティングが対応するアドレス ファミリで有効になっていることを確認します。

show mpls label table detail コマンドを使用して、SRLB の範囲を確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	

	コマンドまたはアクション	目的
ステップ 2	**segment-routing** 例： `RP/0/RP0/CPU0:Router(config)# segment-routing`	セグメントルーティング 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	**adjacency-sid** 例： `RP/0/RP0/CPU0:Router(config-sr)# adjacency-sid`	隣接関係 SID コンフィギュレーション モードを開始します。
ステップ 4	**interface** *type interface-path-id* 例： `RP/0/RP0/CPU0:Router(config-sr-adj)# interface GigabitEthernet0/0/0/3`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**address-family** { **ipv4** | **ipv6** } [**unicast**] 例： `RP/0/RP0/CPU0:Router(config-sr-adj-intf)# address-family ipv4 unicast`	IPv4 または IPv6 アドレス ファミリを指定して、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	**l2-adjacency sid** {**index** *adj-SID-index* | **absolute** *adj-SID-value* } [**next-hop** {*ipv4_address* | *ipv6_address* }] 例： `RP/0/RP0/CPU0:Router(config-sr-adj-intf-af)# l2-adjacency sid absolute 15015 next-hop 10.1.1.4`	インターフェイスの Adj-SID インデックスまたは絶対値を設定します。 SRLB+インデックスの下限に基づいて Ajd-SID を作成するには、各リンクに **index** *adj-SID-index* を指定します。 SRLB 内に特定の Ajd-SID を作成するには、各リンクに **absolute** *adj-SID-value* を指定します。 ポイントツーポイントインターフェイスの場合は、ネクストホップを指定する必要はありません。ただし、ネクストホップを指定した場合は、指定されたネクストホップがネイバーアドレスと一致する場合にのみ、レイヤ 2 Adj-SID が使用されます。 LAN インターフェイスの場合は、ネクストホップ IPv4 または IPv6 アドレスを設定する必要があります。ネクストホップを設定しない場合、レイヤ 2

	コマンドまたはアクション	目的
		Adj-SID は LAN インターフェイスには使用されません。
ステップ 7	**commit**	
ステップ 8	**end**	
ステップ 9	**router isis** *instance-id* 例： `RP/0/RP0/CPU0:Router(config)# router isis isp`	指定したルーティング インスタンスの IS-IS ルーティングを有効にし、ルータをルータ コンフィギュレーション モードにします。
ステップ 10	**address-family** { **ipv4** | **ipv6** } [**unicast**] 例： `RP/0/RP0/CPU0:Router(config-isis)# address-family ipv4 unicast`	IPv4 または IPv6 アドレス ファミリを指定して、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 11	**segment-routing bundle-member-adj-sid** 例： `RP/0/RP0/CPU0:Router(config-isis-af)# segment-routing bundle-member-adj-sid`	動的レイヤ 2 Adj-SID をプログラムし、手動と動的の両方のレイヤ 2 Adj-SID をアドバタイズします。 （注） このコマンドは、手動 L2 Adj-SID のプログラミングには必要ありませんが、動的レイヤ 2 Adj-SID のプログラミングには必要で、手動と動的の両方のレイヤ 2 Adj-SID をアドバタイズする必要があります。

設定を確認します。

```
Router# show mpls forwarding detail | i "Pop|Outgoing Interface|Physical Interface"
Tue Jun 20 06:53:51.876 PDT
. . .
15001  Pop         SRLB (idx 1)       BE1          10.1.1.4        0
     Outgoing Interface: Bundle-Ether1 (ifhandle 0x000000b0)
     Physical Interface: GigabitEthernet0/0/0/3 (ifhandle 0x000000b0)


Router# show running-config segment-routing
Tue Jun 20 07:14:25.815 PDT
segment-routing
 adjacency-sid
  interface GigabitEthernet0/0/0/3
   address-family ipv4 unicast
```

```
    l2-adjacency-sid absolute 15001
   !
  !
 !
!
```

帯域幅ベースのローカル UCMP の設定

帯域幅ベースのローカル非等コスト マルチパス（UCMP）を使用すると、ローカル リンクの帯域幅に基づいて、等コスト マルチパス（ECMP）のパス間で UCMP 機能をローカルで有効にできます。

帯域幅ベースのローカル UCMP は、IS-IS によってインストールされたプレフィックス、セグメント ルーティング隣接関係 SID、およびセグメント ルーティング ラベル クロスコネクトに対して実行され、有効な帯域幅を持つ物理インターフェイスまたは仮想インターフェイスでサポートされます。

たとえば、リンクまたはライン カードのアップ/ダウン イベントのためにバンドル インターフェイスの容量が変化した場合、利用可能なプロビジョニング済みバンドル メンバーに関係なく、トラフィックは引き続き影響を受けるバンドルインターフェイスを使用します。障害により一部のバンドル メンバーが利用できなかった場合、この動作によりトラフィックでバンドル インターフェイスが過負荷状態になる可能性があります。バンドル容量の変更に対処するために、帯域幅ベースのローカル UCMP は、バンドル容量が変更されたときにローカル リンクの帯域幅を使用してトラフィックの負荷を分散します。

始める前に

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**router isis** *instance-id* 例： `RP/0/RP0/cpu 0: router(config)# router isis 1`	指定したルーティング インスタンスの IS-IS ルーティングを有効にし、ルータをルータ コンフィギュレーション モードにします。 **is-type** ルータ コンフィギュレーション コマンドを使用して、特定のルーティング インスタンスによって実行されるルーティングのレベルを変更できます。
ステップ 3	**apply-weight ecmp-only bandwidth** 例： `RP/0/RP0/cpu 0: router(config-isis-af)# apply-weight ecmp-only bandwidth`	ローカル リンクの帯域幅に基づいて、ECMP パス間で UCMP 機能をローカルで有効にします。

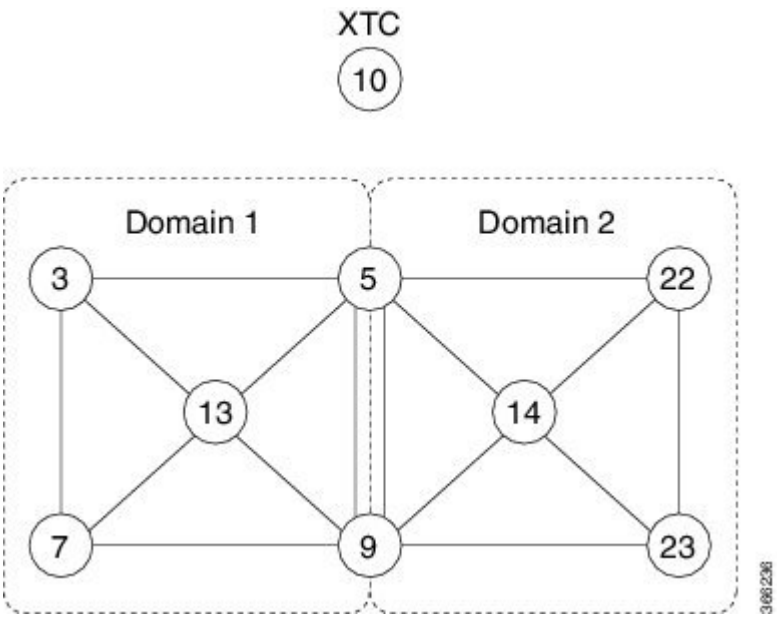
	コマンドまたはアクション	目的
ステップ 4	**commit**	

IS-IS マルチドメイン プレフィックス SID とドメイン ステッチング：例

IS-IS マルチドメイン プレフィックス SID とドメイン ステッチングでは、ドメイン ボーダー ノード用に同じループバック インターフェイス上に複数の IS-IS インスタンスを設定できます。複数の IS-IS インスタンスの下にループバック インターフェイスとプレフィックス SID を指定すると、プレフィックスとプレフィックス SID が異なるドメインに到達できるようになります。

この例では、次のトポロジを使用しています。ノード 5 とノード 9 は、2 つの IS-IS ドメイン（Domain1 と Domain2）の間のボーダー ノードです。ノード 10 は、セグメントルーティング パス計算要素（SR-PCE）として設定されています）。

図 *1 :* マルチドメイン トポロジ



IS-IS マルチドメイン プレフィックス SID の設定

各ボーダー ノードで複数の IS-IS インスタンスの下にループバック インターフェイスとプレフィックス SID を指定します。

Example: Border Node 5

```
router isis Domain1
 interface Loopback0
```

```
  address-family ipv4 unicast
   prefix-sid absolute 16005

router isis Domain2
 interface Loopback0
  address-family ipv4 unicast
   prefix-sid absolute 16005


Example: Border Node 9
router isis Domain1
 interface Loopback0
  address-family ipv4 unicast
   prefix-sid absolute 16009

router isis Domain2
 interface Loopback0
  address-family ipv4 unicast
   prefix-sid absolute 16009
```

ボーダー ノード 5 および 9 はそれぞれ 2 つの IS-IS インスタンス（Domain1 および Domain2）を実行し、両方のドメインで Loopback0 プレフィックスとプレフィックス SID をアドバタイズします。

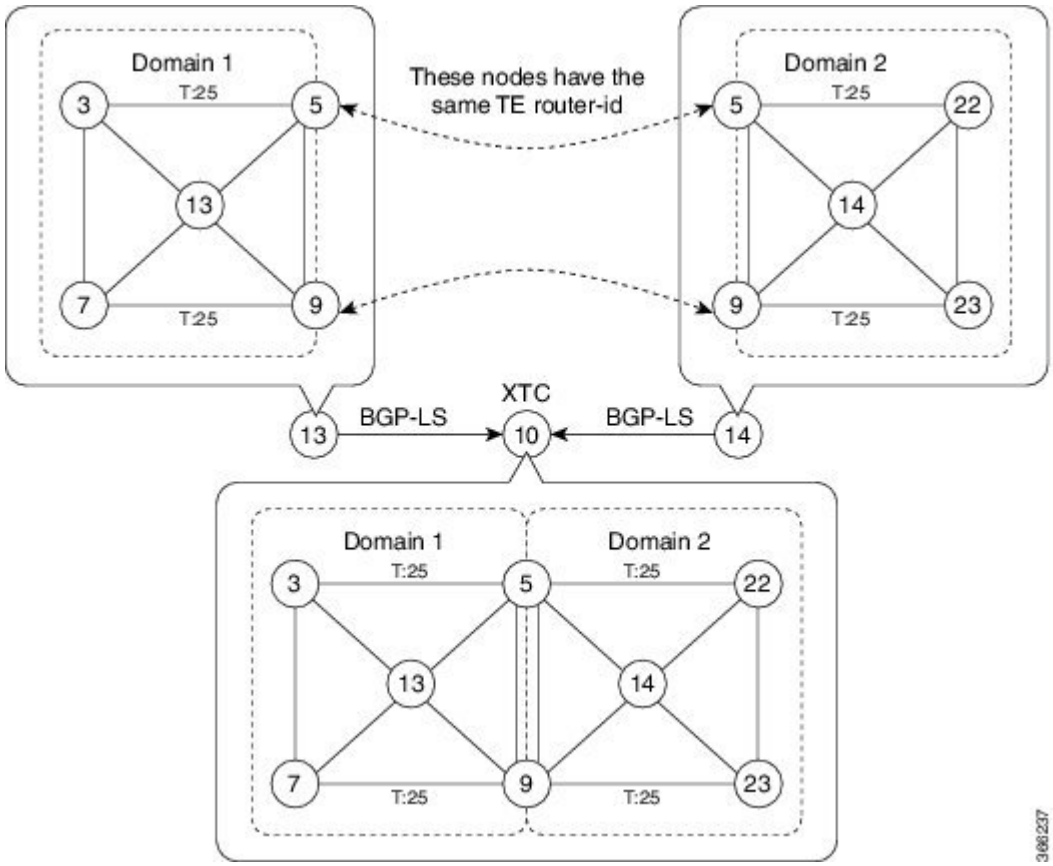
両方のドメイン内のノードは、同じプレフィックスとプレフィックス SID を使用してボーダー ノードに到達できます。例えば、ノード 3 およびノード 22 は、プレフィックス SID 16005 を使用してノード 5 に到達できます。

共通ルータ ID の設定

各ボーダー ノードで、各 IS-IS インスタンスの下に共通の TE ルータ ID を設定します。

```
Example: Border Node 5
router isis Domain1
 address-family ipv4 unicast
  router-id loopback0

router isis Domain2
 address-family ipv4 unicast
  router-id loopback0


Example: Border Node 9
router isis Domain1
 address-family ipv4 unicast
  router-id loopback0

router isis Domain2
 address-family ipv4 unicast
  router-id loopback0
```

IS-IS リンクステート データの配布



ノード 13 およびノード 14 で BGP リンクステート（BGP-LS）を設定して、ローカル ドメインをノード 10 に報告します。

```
Example: Node 13
router isis Domain1
 distribute link-state id


Example: Node 14
router isis Domain2
 distribute link-state id
```

Link-state ID は 32 から始まります。IGP ドメインごとに 1 つの ID が必要です。SR-TE TED が特定の IGP ドメインに属していることを識別するために、異なるドメイン ID が必要です。

ノード 13 とノード 14 はそれぞれ、BGP-LS のローカル ドメインをノード 10 に報告します。

ノード 10 は、共通のアドバタイズされた TE ルータの ID によってボーダー ノード（ノード 5 および9）を識別してから、これらのボーダー ノード上のドメインを結合（ステッチ）してエンドツーエンドのパス計算を行います。

セグメントルーティング ECMP-FEC の最適化

ECMP-FEC は、ラベル付けされていない ECMP、MPLS LSP ECMP、VPN マルチパス、EVPN マルチホーミングなどのシステム上のあらゆる ECMP プログラミングに使用されます。

SR の ECMP-FEC の最適化ソリューションは、SR-MPLS ネットワークのアンダーレイプログラミング時の ECMP-FEC リソースの消費を最小限に抑えます。この機能は、同じ一連のネクストホップを持つすべての /32 IPv4 セグメントルーティングプレフィックスの同じ ECMP-FEC、通常の FEC、および出力カプセル化 DB（EEDB）エントリの共有をサポートします。指定されたプレフィックスの ECMP パスに関連付けられているすべての out_label が同じ値である場合に、ECMP-FEC の最適化がトリガーされます。このルールは、LFA/TI-LFA が有効になっている場合に、プライマリパスとバックアップパスの両方に適用されます。このルールが満たされていない場合、プレフィックスは専用の ECMP-FEC を使用してプログラミングされます。ルールを満たすその他のプレフィックスが最適化の候補です。

セグメント ルーティング ラベル エッジ ルータ（FEC）ECMP-FEC の最適化により、最初はラベルスイッチドルータ（LSR）ノード（MPLS P）用に開発された ECMP-FEC の最適化が、LER（レイヤ 3 MPLS PE）のルータで有効になります。

機能と制限事項

SR ECMP-FEC の最適化は、次に適用されます。

- ラベルスイッチドルータ（LSR）ノード（MPLS P）
- ラベルエッジルータ（LER）L3VPN

SR ECMP-FEC の最適化は、次のインスタンスでは有効にしないでください。

- L2VPN サービスの LER。
- 転送チェーンがセグメントルーティングを介した BGP-LU 経由の VPN が含まれている場合の L2VPN/L3VPN サービス。
- プレフィックスごとのラベル割り当てモードまたは BGP PIC が必要な場合。

SR ECMP-FEC 最適化の有効化

SR ECMP-FEC の最適化を有効にするには、グローバル コンフィギュレーション モードで **hw-module fib mpls label lsr-optimized** コマンドを使用します。この機能を有効にした後、ラインカードをリロードします。

```
Router(config)# hw-module fib mpls label lsr-optimized
Router(config)# commit

LC/0/0/CPU0:Oct 11 20:19:12.540 UTC: fia_driver[185]:
%FABRIC-FIA_DRVR-4-MPLS_HW_PROFILE_MISMATCH :
    Mismatch found, reload LC to activate the new mpls profile


Router# reload location 0/0/CPU0
```

```
Proceed with reload? [confirm]
Reloading node 0/0/CPU0
```

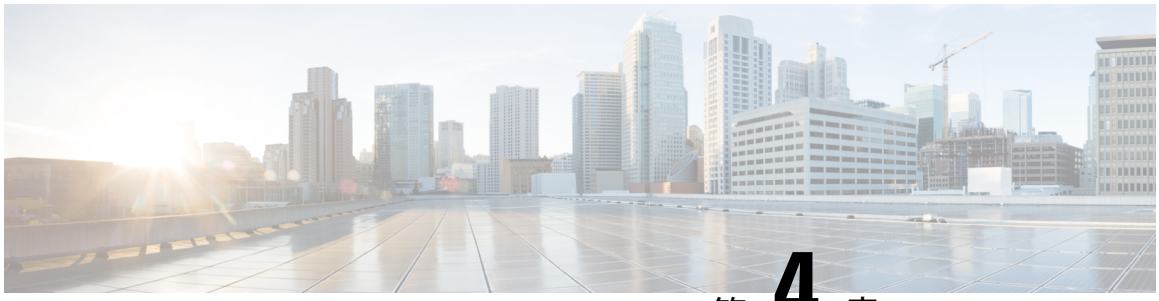
確認

次に、SR ECMP-FEC の最適化を有効にする前の NPU の使用例を示します。

```
Router# show controllers npu resources ecmpfec location all
HW Resource Information For Location: 0/0/CPU0
HW Resource Information
    Name                            : ecmp_fec

OOR Information
    NPU-0
        Estimated Max Entries       : 4096
        Red Threshold               : 95
        Yellow Threshold            : 80
        OOR State                   : Green

Current Usage
    NPU-0
        Total In-Use                : 1001      (24 %)
        ipnhgroup                   : 1001      (24 %)
        ip6nhgroup                  : 0         (0 %)
```

次に、SR ECMP-FEC の最適化を有効にした後の NPU の使用例を示します。

```
Router# show controllers npu resources ecmpfec location all
HW Resource Information For Location: 0/0/CPU0
HW Resource Information
    Name                            : ecmp_fec

OOR Information
    NPU-0
        Estimated Max Entries       : 4096
        Red Threshold               : 95
        Yellow Threshold            : 80
        OOR State                   : Green

Current Usage
    NPU-0
        Total In-Use                : 7         (0 %)
        ipnhgroup                   : 7         (0 %)
        ip6nhgroup                  : 0         (0 %)
```



第 4 章

OSPF プロトコル用のセグメント ルーティングの設定

Open Shortest Path First（OSPF）は、Internet Engineering Task Force（IETF）の OSPF ワーキング グループによって開発された内部ゲートウェイ プロトコル（IGP）です。OSPF は特に IP ネットワーク向けに設計されており、IP サブネット化、および外部から取得したルーティング情報のタギングをサポートしています。OSPF を使用するとパケット認証も可能になり、パケットを送受信するときに IP マルチキャストが使用されます。

このモジュールは、OSPF のセグメント ルーティングを有効にするための設定情報を提供します。

（注） でOSPF を実装する場合の詳細については、『』の「*Implementing OSPF*」モジュールを参照してください。

OSPF プロトコル用のセグメント ルーティングの有効化

OSPF コントロール プレーン上のセグメント ルーティングは、次をサポートしています。

- OSPFv2 のコントロール プレーン
- マルチエリア
- ループバック インターフェイス上のホスト プレフィックスの IPv4 プレフィックス SID
- 隣接関係用の隣接関係 SID
- MPLS penultimate hop popping（PHP）と明示的な NULL シグナリング

ここでは、OSPF でセグメント ルーティング MPLS および MPLS 転送を有効にする方法について説明します。セグメント ルーティングは、インスタンス、エリア、またはインターフェイス レベルで設定できます。

始める前に

ルータで OSPF のセグメント ルーティングを有効にする前に、ネットワークで MPLS Cisco IOS XR ソフトウェア機能をサポートする必要があります。

（注） ネットワークのトラフィック エンジニアリング部分にあるすべての OSPF ルータ上で、次のタスク リストのコマンドを入力する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**router ospf** *process-name* 例： `RP/0/RP0/cpu 0: router(config)# router ospf 1`	指定したルーティング プロセスに OSPF ルーティングを有効にし、ルータ コンフィギュレーション モードでルータを配置します。
ステップ 3	**segment-routing mpls** 例： `RP/0/RP0/cpu 0: router(config-ospf)# segment-routing mpls`	ルーティング プロセス上の MPLS データ プレーンと、ルーティング プロセスのすべてのエリアとインターフェイスを使用して、セグメント ルーティングを有効にします。 ルーティング プロセスのすべてのインターフェイスでセグメント ルーティングの転送を有効にし、OSPF が受信した SID を転送テーブルにインストールします。
ステップ 4	**area 0** 例： `RP/0/RP0/cpu 0: router(config-ospf)# area 0`	エリア コンフィギュレーション モードを開始します。
ステップ 5	**segment-routing mpls** 例： `RP/0/RP0/cpu 0: router(config-ospf-ar)# segment-routing mpls`	（任意）エリア上の MPLS データ プレーンとそのエリア内のすべてのインターフェイスを使用して、セグメント ルーティングを有効にします。エリアのすべてのインターフェイスでセグメント ルーティングの転送を有効にし、OSPF が受

	コマンドまたはアクション	目的
		信した SID を転送テーブルにインストールします。

ステップ 6	**exit**
	例：
	`RP/0/RP0/cpu 0: router(config-ospf-ar)# exit`
	`RP/0/RP0/cpu 0: router(config-ospf)# exit`	

ステップ 7	**commit**	

次のタスク

プレフィックス SID を設定します。

OSPF対応ループバックインターフェイスでのプレフィックス SID の設定

プレフィックスセグメント識別子（SID）は、IP プレフィックスに関連付けられます。プレフィックス SID は、ラベルのセグメント ルーティング グローバル ブロック（SRGB）の範囲から手動で設定されます。プレフィックス SID は、ノードのループバックアドレスをプレフィックスとして使用して、ループバック インターフェイスの下に設定されます。プレフィックスセグメントは、その宛先への最短パスに沿ってトラフィックを誘導します。

プレフィックス SID は、ノード SID であることもエニーキャスト SID であることもあります。ノード SID は、特定のノードを識別するタイプのプレフィックス SID です。エニーキャスト SID は、一連のノードを識別するタイプのプレフィックス SID であり、n-flag-clear を使用して設定されます。一連のノード（エニーキャストグループ）は、共有プレフィックスアドレスとプレフィックス SID をアドバタイズするように設定されます。エニーキャストルーティングにより、複数のアドバタイズノードへのトラフィックのステアリングが可能になります。エニーキャストアドレス宛てのパケットは、トポロジ的に最も近いノードに転送されます。

プレフィックス SID は、セグメント ルーティング ドメイン内でグローバルに一意です。

このタスクでは、OSPF 対応ループバック インターフェイスでプレフィックスセグメント識別子（SID）のインデックスまたは絶対値を設定する方法について説明します。

始める前に

インスタンス、エリア、またはインターフェイスでセグメントルーティングが有効になっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**router ospf** *process-name* 例： `RP/0/RP0/cpu 0: router(config)# router ospf 1`	指定したルーティング プロセスに OSPF ルーティングを有効にし、ルータ コンフィギュレーション モードでルータを配置します。
ステップ 3	**area** *value* 例： `RP/0/RP0/cpu 0: router(config-ospf)# area 0`	エリア コンフィギュレーション モードを開始します。
ステップ 4	**interface Loopback** *interface-instance* 例： `RP/0/RP0/cpu 0: router(config-ospf-ar)# interface Loopback0 passive`	ループバック インターフェイスとインスタンスを指定します。
ステップ 5	**commit**	

プレフィックス SID 設定を確認します。

```
RP/0/RP0/cpu 0: router# show ospf database opaque-area 7.0.0.1 self-originate
 OSPF Router with ID (10.0.0.1) (Process ID 1)
                Type-10 Opaque Link Area Link States (Area 0)
<...>
    Extended Prefix TLV: Length: 20
      Route-type: 1
      AF        : 0
      Flags     : 0x40
      Prefix    : 10.0.0.1/32

      SID sub-TLV: Length: 8
        Flags     : 0x0
        MTID      : 0
        Algo      : 0
        SID Index : 1001
```

セグメントルーティング ECMP-FEC の最適化

ECMP-FEC は、ラベル付けされていない ECMP、MPLS LSP ECMP、VPN マルチパス、EVPN マルチホーミングなどのシステム上のあらゆる ECMP プログラミングに使用されます。

SR の ECMP-FEC の最適化ソリューションは、SR-MPLS ネットワークのアンダーレイプログラミング時の ECMP-FEC リソースの消費を最小限に抑えます。この機能は、同じ一連のネクストホップを持つすべての /32 IPv4 セグメントルーティングプレフィックスの同じ ECMP-FEC、通常の FEC、および出力カプセル化 DB（EEDB）エントリの共有をサポートします。指定されたプレフィックスの ECMP パスに関連付けられているすべての out_label が同じ値である場合に、ECMP-FEC の最適化がトリガーされます。このルールは、LFA/TI-LFA が有効になっている場合に、プライマリパスとバックアップパスの両方に適用されます。このルールが満たされていない場合、プレフィックスは専用の ECMP-FEC を使用してプログラミングされます。ルールを満たすその他のプレフィックスが最適化の候補です。

セグメント ルーティング ラベル エッジ ルータ（FEC）ECMP-FEC の最適化により、最初はラベルスイッチドルータ（LSR）ノード（MPLS P）用に開発された ECMP-FEC の最適化が、LER（レイヤ 3 MPLS PE）のルータで有効になります。

機能と制限事項

SR ECMP-FEC の最適化は、次に適用されます。

- ラベルスイッチドルータ（LSR）ノード（MPLS P）
- ラベルエッジルータ（LER）L3VPN

SR ECMP-FEC の最適化は、次のインスタンスでは有効にしないでください。

- L2VPN サービスの LER。
- 転送チェーンがセグメントルーティングを介した BGP-LU 経由の VPN が含まれている場合の L2VPN/L3VPN サービス。
- プレフィックスごとのラベル割り当てモードまたは BGP PIC が必要な場合。

SR ECMP-FEC 最適化の有効化

SR ECMP-FEC の最適化を有効にするには、グローバル コンフィギュレーション モードで **hw-module fib mpls label lsr-optimized** コマンドを使用します。この機能を有効にした後、ラインカードをリロードします。

```
Router(config)# hw-module fib mpls label lsr-optimized
Router(config)# commit

LC/0/0/CPU0:Oct 11 20:19:12.540 UTC: fia_driver[185]:
%FABRIC-FIA_DRVR-4-MPLS_HW_PROFILE_MISMATCH :
    Mismatch found, reload LC to activate the new mpls profile


Router# reload location 0/0/CPU0

Proceed with reload? [confirm]
Reloading node 0/0/CPU0
```

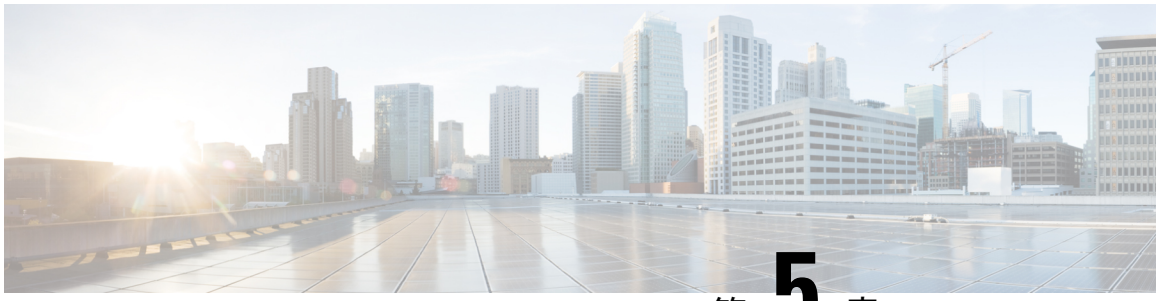
確認

次に、SR ECMP-FEC の最適化を有効にする前の NPU の使用例を示します。

```
Router# show controllers npu resources ecmpfec location all
HW Resource Information For Location: 0/0/CPU0
HW Resource Information
    Name                            : ecmp_fec

OOR Information
    NPU-0
        Estimated Max Entries       : 4096
        Red Threshold               : 95
        Yellow Threshold            : 80
        OOR State                   : Green

Current Usage
    NPU-0
        Total In-Use                : 1001      (24 %)
        ipnhgroup                   : 1001      (24 %)
        ip6nhgroup                  : 0         (0 %)
```

次に、SR ECMP-FEC の最適化を有効にした後の NPU の使用例を示します。

```
Router# show controllers npu resources ecmpfec location all
HW Resource Information For Location: 0/0/CPU0
HW Resource Information
    Name                            : ecmp_fec

OOR Information
    NPU-0
        Estimated Max Entries       : 4096
        Red Threshold               : 95
        Yellow Threshold            : 80
        OOR State                   : Green

Current Usage
    NPU-0
        Total In-Use                : 7         (0 %)
        ipnhgroup                   : 7         (0 %)
        ip6nhgroup                  : 0         (0 %)
```



第 5 章

BGP 用のセグメント ルーティングの設定

ボーダー ゲートウェイ プロトコル（BGP）は、自律システム間にループフリーのドメイン間ルーティングを作成可能な外部ゲートウェイ プロトコル（EGP）です。自律システムは、単一の技術管理に基づくルータのまとまりです。自律システム内のルータは、複数の内部ゲートウェイ プロトコル（IGP）を使用して自律システム内のルーティング情報を交換し、EGP を使用して自律システム外でパケットをルーティングします。

このモジュールでは、BGP のセグメントルーティングを有効にするために使用される設定情報を示します。

（注） ルータで BGP を実装する場合の詳細については、『*Routing Configuration Guide for Cisco NCS 560 Series Routers*』の「*Implementing BGP*」モジュールを参照してください。

BGP 用のセグメント ルーティング

従来の BGP ベースのデータセンター（DC）ファブリックでは、パケットは自律システムの各ノードにホップバイホップで転送されます。トラフィックは、外部 BGP（eBGP）マルチパス ECMP に沿ってのみ送信されます。トラフィック エンジニアリングを行うことはできません。

MPLS ベースの DC ファブリックでは、ノード間の eBGP セッションは、BGP ラベル付きユニキャスト（BGP-LU）ネットワーク層到達可能性情報（NLRI）を交換します。MPLS ベースの DC ファブリックを使用すると、ファブリック内の任意のリーフ（トップオブラックまたは境界ルータ）が単一のラベルを使用して他のリーフと通信できるため、従来の BGP ベースの DC ファブリックよりもパケット転送パフォーマンスが高くなり、カプセル化のオーバーヘッドが少なくなります。ただし、各ラベル値はホップごとに異なる可能性があるため、MPLS ベースの DC ファブリックはトラブルシューティングが難しく、構成が複雑です。

BGP は、セグメント ルーティング プレフィックス SID インデックスを伝送するように拡張されました。BGP-LU は、各ノードが他のリーフ ノードの BGP プレフィックス SID を学習するのに役立ち、送信元と宛先の間で ECMP を使用できます。BGP のセグメント ルーティングによって、ファブリックの構成、操作、およびトラブルシューティングが簡素化されます。BGP のセグメント ルーティングでは、BGP プレフィックス SID を使用してデータセンターでトラフィック ステアリング機能を有効にできます。

BGP プレフィックス セグメント識別子の設定

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 ドメイン内でグローバルです。これは、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を識別します。BGP プレフィックス SID は、ラベルのセグメント ルーティング グローバル ブロック（SRGB）の範囲から手動で設定されます。

各 BGP スピーカーは、**segment-routing global-block** コマンドを使用して SRGB で設定する必要があります。SRGB の詳細については、「セグメント ルーティング グローバル ブロックについて」の項を参照してください。

（注） 範囲から割り当てられた値はドメイン全体で重要な意味を持つため、ドメイン内のすべてのルータに同じ値の範囲を設定することをお勧めします。

BGP プレフィックス SID を割り当てるには、最初に **set label-index** *index* 属性を使用してルーティング ポリシーを作成し、次にそのインデックスをノードに関連付けます。

例

次の例に、SRGB を設定し、$SID パラメータと **set label-index** 属性を使用して BGP ルート ポリシーを作成し、プレフィックス SID インデックスをノードに関連付ける方法を示します。

```
RP/0/RP0/CPU0:router(config)# segment-routing global-block 16000 23999

RP/0/RP0/CPU0:router(config)# route-policy SID($SID)
RP/0/RP0/CPU0:router(config-rpl)# set label-index $SID
RP/0/RP0/CPU0:router(config-rpl)# end policy

RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# bgp router-id 1.1.1.1
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-af)# network 1.1.1.3/32 route-policy SID(3)
RP/0/RP0/CPU0:router(config-bgp-af)# allocate-label all
RP/0/RP0/CPU0:router(config-bgp-af)# commit
RP/0/RP0/CPU0:router(config-bgp-af)# end


RP/0/RP0/CPU0:router# show bgp 1.1.1.3/32
BGP routing table entry for 1.1.1.3/32
Versions:
  Process           bRIB/RIB  SendTblVer
```

```
  Speaker                 74          74
    Local Label: 16003
Last Modified: Sep 29 19:52:18.155 for 00:07:22
Paths: (1 available, best #1)
  Advertised to update-groups (with more than one peer):
    0.2
  Path #1: Received by speaker 0
  Advertised to update-groups (with more than one peer):
    0.2
  3
    99.3.21.3 from 99.3.21.3 (1.1.1.3)
      Received Label 3
      Origin IGP, metric 0, localpref 100, valid, external, best, group-best
      Received Path ID 0, Local Path ID 1, version 74
      Origin-AS validity: not-found
      Label Index: 3
```

セグメントルーティング出力ピアエンジニアリングの設定

セグメント ルーティング出力ピア エンジニアリング（EPE）はコントローラを使用して、セグメント ルーティング ドメイン内の入力プロバイダー エッジまたはコンテンツ ソース（ノード）に、特定の出口プロバイダーエッジ（ノード）および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指示します。BGP ピア SID 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-LS EPE ルートを介して、BGP ピア 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、BGP ラベル付きユニキャスト（BGP-LU）を使用して出口ノードとピア ノードを経由して宛先にトラフィックを誘導するように入力ノードをプログラミングできます。

EPE 機能は、EPE 出力境界ルータおよび EPE コントローラでのみ必要です。

このタスクでは、EPE 出口ノードでセグメント ルーティング EPE を設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**router bgp** *as-number* 例： `RP/0/RP0/CPU0:router(config)# router bgp 1`	BGP AS 番号を指定し、BGP コンフィギュレーション モードを開始します。このモードでは、BGP ルーティング プロセスを設定できます。
ステップ 2	**neighbor** *ip-address* 例：	BGP ルーティングのためにルータをネイバー コンフィギュレーション モード

	コマンドまたはアクション	目的
	`RP/0/RP0/CPU0:router(config-bgp)# neighbor 192.168.1.3`	にして、ネイバーの IP アドレスを BGP ピアとして設定します。
ステップ 3	**remote-as** *as-number* 例： `RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 3`	ネイバーを作成し、リモート自律システム番号を割り当てます。
ステップ 4	**egress-engineering** 例： `RP/0/RP0/CPU0:router(config-bgp-nbr)# egress-engineering`	eBGP ピア用に EPE を使用して出力ノードを設定します。

BGP リンク ステートの設定

BGP リンクステート（LS）は、BGP を介して内部ゲートウェイ プロトコル（IGP）リンクステートデータベースを伝えるために定義されたアドレス ファミリ識別子（AFI）およびサブアドレス ファミリ識別子（SAFI）です。BGP LS は、ネットワーク トポロジ情報をトポロジ サーバおよびアプリケーション層トラフィック最適化（ALTO）サーバに提供します。BGP LS では、集約、情報の非表示、および抽象化に対するポリシー ベースの制御が可能です。BGP LS は、IS-IS および OSPFv2 をサポートしています。

（注） IGP は、リモート ピアからの BGP LS データを使用しません。BGP は、ルータの他のコンポーネントに受信した BGP LS データをダウンロードしません。

セグメント ルーティングの場合、次の属性が BGP LS に追加されています。

- ノード：セグメント ルーティング機能（SRGB 範囲を含む）およびアルゴリズム
- リンク：隣接関係 SID と LAN 隣接関係 SID
- プレフィックス：プレフィックス SID およびセグメント ルーティング マッピング サーバ（SRMS）のプレフィックス範囲

次の例は、リンクステート情報を BGP ネイバーと交換する方法を示しています。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.0.0.2
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
```

```
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family link-state link-state
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# exit
```

IGP の拡張機能

所定の BGP ノードは、複数の独立したルーティング ドメインに接続できます。BGP への IGP リンク ステート配布が OSPF プロトコルと ISIS プロトコルの両方に追加され、そのノードは、これらの複数のドメインにまたがるまたはドメインを含むパスを構築するアプリケーションに同様の方法でこの情報を渡すことができます。

BGP を使用して ISIS リンクステート データを配布するには、ルータ コンフィギュレーション モードで **distribute bgp-ls** コマンドを使用します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# distribute bgp-ls instance-id 32 level 2 throttle 5
```

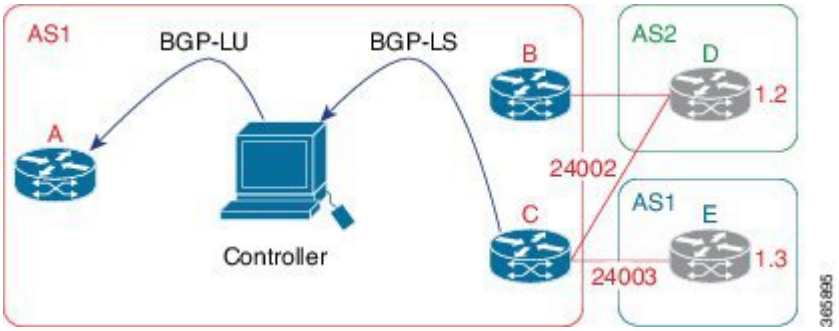
BGP を使用して OSPFv2 および OSPFv3 リンクステート データを配布するには、ルータ コンフィギュレーション モードで **distribute bgp-ls** コマンドを使用します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 100
RP/0/RP0/CPU0:router(config-ospf)# distribute bgp-ls instance-id 32 throttle 10
```

例：SR-EPE および BGP-LS の設定

次の図では、入口ノード A および出口ノード B および C を備えた自律システム AS1 でセグメント ルーティングが有効になっています。この例で、出口ノード C に EPE を設定します。

図 *2:* トポロジ



手順

ステップ 1 eBGP ピア D および E 用に EPE を使用してノード C を設定します。

例：

```
RP/0/RP0/CPU0:router_C(config)# router bgp 1
RP/0/RP0/CPU0:router_C(config-bgp)# neighbor 192.168.1.3
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# remote-as 3
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# description to E
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# egress-engineering
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router_C(config-bgp-nbr-af)# route-policy bgp_in in
RP/0/RP0/CPU0:router_C(config-bgp-nbr-af)# route-policy bgp_out out
RP/0/RP0/CPU0:router_C(config-bgp-nbr-af)# exit
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# exit
RP/0/RP0/CPU0:router_C(config-bgp)# neighbor 192.168.1.2
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# remote-as 2
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# description to D
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# egress-engineering
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router_C(config-bgp-nbr-af)# route-policy bgp_in in
RP/0/RP0/CPU0:router_C(config-bgp-nbr-af)# route-policy bgp_out out
RP/0/RP0/CPU0:router_C(config-bgp-nbr-af)# exit
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# exit
```

ステップ 2 BGP-LS を使用してピア ノード SID をコントローラにアドバタイズするようにノード C を設定します。

例：

```
RP/0/RP0/CPU0:router_C(config-bgp)# neighbor 172.29.50.71
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# description to EPE_controller
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# address-family link-state link-state
RP/0/RP0/CPU0:router_C(config-bgp-nbr)# exit
RP/0/RP0/CPU0:router_C(config-bgp)# exit
```

ステップ 3 設定をコミットします。

例：

```
RP/0/RP0/CPU0:router_C(config)# commit
```

ステップ 4 設定を確認します。

例：

```
RP/0/RP0/CPU0:router_C# show bgp egress-engineering

 Egress Engineering Peer Set: 192.168.1.2/32 (10b87210)
     Nexthop: 192.168.1.2
     Version: 2, rn_version: 2
       Flags: 0x00000002
  Local ASN: 1
 Remote ASN: 2
  Local RID: 1.1.1.3
 Remote RID: 1.1.1.4
  First Hop: 192.168.1.2
       NHID: 3
      Label: 24002, Refcount: 3
     rpc_set: 10b9d408

 Egress Engineering Peer Set: 192.168.1.3/32 (10be61d4)
     Nexthop: 192.168.1.3
     Version: 3, rn_version: 3
```

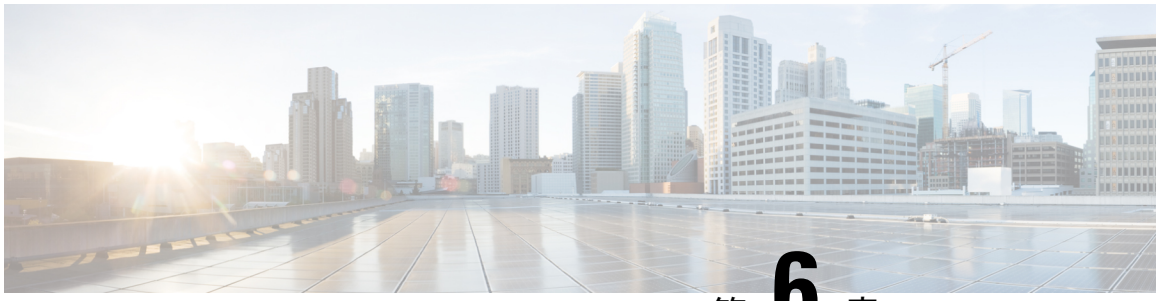
```
      Flags: 0x00000002
  Local ASN: 1
 Remote ASN: 3
  Local RID: 1.1.1.3
 Remote RID: 1.1.1.5
  First Hop: 192.168.1.3
       NHID: 4
      Label: 24003, Refcount: 3
    rpc_set: 10be6250
```

出力は、ノード C が各 eBGP ピアに対してピア SID を割り当てたことを示しています。

例：

```
RP/0/RP0/CPU0:router_C# show mpls forwarding labels 24002 24003
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
24002  Unlabelled  No ID              Te0/0/0/1    192.168.1.2     0
24003  Unlabelled  No ID              Te0/0/0/2    192.168.1.3     0
```

出力は、ノード C が転送情報ベース（FIB）にピア ノード SID をインストールしたことを示しています。



第 6 章

SR-TE ポリシーの設定

このモジュールでは、トラフィック エンジニアリング（SR-TE）ポリシーのセグメント ルーティングの詳細、SR-TE ポリシーの設定方法、および SR-TE ポリシーへのトラフィックの誘導方法について説明します。

制限事項

プラットフォームに関する次の制限事項があります。

SR-TE の自動ルート通知

SR-TE の自動ルート通知では、LDP 中間ノードで SR-TE が終了する場合、LDP-over-SR-TE を処理できません。

次のトポロジについて考えてみましょう。

R1---R2---R3---R4---R5---R6

R1 から R4 への SR-TE ルートがあり、LDP プレフィックスが R6 から学習される場合、自動ルート通知は失敗します。

SR-TE ポリシーの概要

トラフィック エンジニアリングを実現するためのセグメント ルーティング（SR-TE）では、ネットワークを介してトラフィックを誘導する「ポリシー」を使用します。SR-TE ポリシー

パスは、セグメントID（SID）リストと呼ばれるパスを指定するセグメントのリストとして表されます。各セグメントは、送信元から宛先までのエンドツーエンドのパスであり、ネットワークのルータに、IGPによって計算された最短パスに従うのではなく指定されたパスに従うように指示します。パケットがSR-TEポリシーへと誘導される場合、SIDリストはヘッドエンドによってパケットにプッシュされます。残りのネットワークは、SIDリストに埋め込まれた命令を実行します。

SR-TEポリシーは、順序付きリスト（ヘッドエンド、カラー、エンドポイント）として識別されます。

- ヘッドエンド：SR-TE ポリシーがインスタンス化される場所
- カラー：同じノードペアへの2つ以上のポリシーを区別する数値（ヘッドエンド-エンドポイント）
- エンドポイント：SR-TE ポリシーの宛先

すべての SR-TE ポリシーにはカラー値があります。同じノード ペア間の各ポリシーには、一意のカラー値が必要です。

SR-TE ポリシーは、1 つ以上の候補パスを使用します。候補パスは、単一セグメント リスト（SID リスト）または重み付け SID リストのセット（重み付け等コスト マルチパス（WECMP））です。候補パスは動的または明示的のどちらかです。詳細については、「*SR-TE* ポリシーパスタイプ」の項を参照してください。

自動ルート インクルード

自動ルート インクルードを使用して SR-TE ポリシーを設定すると、最短以外のパスを介して特定の IGP（IS-IS、OSPF）プレフィックスを誘導し、そのプレフィックスのトラフィックを SR-TE ポリシーに転送することができます。自動ルート インクルードは、指定された宛先またはプレフィックスに自動ルート アナウンス機能を適用します。

自動ルート SR-TE ポリシーはプレフィックスを IGP に追加します。これにより、エンドポイントのプレフィックスまたはエンドポイントのダウンストリームのプレフィックスが SR-TE ポリシーを使用する資格があるかどうかが決定されます。プレフィックスが適格な場合、IGP はプレフィックスが自動ルートインクルード設定にリストされているかどうかを確認します。プレフィックスが含まれている場合、IGP は発信パスとして SR-TE ポリシーを使用してプレフィックス ルートをダウンロードします。

自動ルート インクルードは、次の 3 つのメトリック タイプをサポートします。

- デフォルト（メトリックなし）：SR-TEポリシーを介したパスは最短パス メトリックを継承します。
- 絶対メトリック：ポリシー エンドポイントへの最短パス メトリックは設定された絶対メトリックに置き換えられます。自動ルートが含まれるプレフィックスへのメトリックは絶対メトリックに変更されます。
- 相対メトリック：ポリシー エンドポイントへの最短パス メトリックは設定された相対値（プラスまたはマイナス）を使用して変更されます。

（注） IGPパス上のロードバランシングを防止するために、IGPが自動ルート設定した宛先（**autoroute metric relative -1** など）に対して考慮する値よりも低いメトリックを指定できます。

設定例

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)#policy P1
Router(config-sr-te-policy)# color 20 end ipv4 1.1.1.2
Router(config-sr-te-policy)# autoroute include ipv4 1.1.1.21/32
Router(config-sr-te-policy)# autoroute include ipv4 1.1.1.23/32
Router(config-sr-te-policy)# autoroute metric constant 1
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy-path)# preference 100
Router(config-sr-te-pp-index)# explicit segment-list Plist-1
```

カラー専用自動ステアリング

カラーのみのステアリングは、エンドポイントに関係なく、特定のカラーでポリシーが作成されるトラフィック ステアリング メカニズムです。

NULLエンドポイント（IPv4 NULLの場合は0.0.0.0、IPv6 NULLエンドポイントの場合は::0）を使用する特定のカラーにSR-TEポリシーを作成できます。つまり、その色に基づいてトラフィックを誘導できる単一のポリシーと、特定の色の拡張コミュニティを持つが宛先が異なるルート（ネクストホップ）のNULLエンドポイントを持つことができます。

（注） NULLエンドポイントを使用したすべてのSR-TEポリシーには、明示パスオプションが必要です。ポリシーの宛先が存在しないため、ポリシーにはダイナミック パスオプション（パスがヘッドエンドまたはPCEによって計算される）を設定することはできません。

また、オーバーレイ ルートのカラー拡張コミュニティでカラーのみ（CO）フラグを指定することもできます。COフラグを使用すると、エンドポイントのサブアドレス ファミリ識別子（SAFI）（IPv4またはIPv6）に関係なく、一致するカラーのSRポリシーを選択できます。CO フラグの設定 （107 ページ）を参照してください。

カラーのみのステアリングの設定

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy P1
Router(config-sr-te-policy)# color 1 end-point ipv4 0.0.0.0

Router# configure
```

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy P2
Router(config-sr-te-policy)# color 2 end-point ipv6 ::0
```

```
Router# show running-configuration
segment-routing
 traffic-eng
  policy P1
   color 1 end-point ipv4 0.0.0.0
  !
  policy P2
   color 2 end-point ipv6 ::
  !
 !
!
end
```

アドレスファミリに依存しない自動ステアリング

アドレスファミリに依存しないステアリングでは、SR-TEポリシーを使用して、ラベル付きとラベルなしの両方のIPv4およびIPv6トラフィックを誘導します。この機能には、IPV4エンドポイント ポリシーを介したIPv6カプセル化（IPv6 caps）のサポートが必要です。

IPv4 NULLエンドポイントのIPv6 capsは、セグメントルーティングパス計算要素（SR-PCE）でポリシーが作成されると自動的に有効になります。各ポリシーのバインディングSID（BSID）状態通知には、IPv6 capsのステータス（有効または無効）をSR-PCEクライアント（PCC）に通知する「ipv6_caps」フラグが含まれます。

特定のカラーとIPv4 NULLエンドポイントを使用するSR-TEポリシーは複数の候補パスを使用できます。候補パスのいずれかでIPv6 capsが有効になっている場合は、残りのすべての候補パスでIPv6 capsが有効になっている必要があります。同じカラーとエンドポイントのすべての候補パスでIPv6 capsが有効になっていない場合、トラフィックが破棄される可能性があります。

ローカル ポリシーで**ipv6 disable**コマンドを使用すると、特定のカラーとIPv4 NULLエンドポイントのIPv6 capsを無効にできます。このコマンドは、同じカラーとIPv4 NULLエンドポイントを共有するすべての候補パスでIPv6 capsを無効にします。

IPv6 カプセル化の無効化

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy P1
Router(config-sr-te-policy)# color 1 end-point ipv4 0.0.0.0
Router(config-sr-te-policy)# ipv6 disable
```

セグメント ルーティング ポリシーを介した LDP

セグメント ルーティング ポリシーを介した LDP 機能を使用すると、2 台のルータ間でセグメントルーティング（SR）ポリシーを介して LDP ターゲット隣接関係を実現できます。この機能は、SR ポリシーをターゲットエンドポイントとして指定できるように、既存の MPLS LDP アドレス ファミリ ネイバー コンフィギュレーションを拡張します。

SR ポリシーを介した LDP は、IPv4 エンドポイントを使用してローカルに設定された SR ポリシーでサポートされます。

MPLS LDP の詳細については、『*MPLS Configuration Guide*』の「Implementing MPLS Label Distribution Protocol」の章を参照してください。

（注） SR ポリシー名を介して LDP ターゲット隣接関係を設定する前に、セグメント ルーティング コンフィギュレーションで SR ポリシーを作成する必要があります。SR ポリシーのインターフェイス名は、ポリシーのカラーとエンドポイントに基づいて内部的に作成されます。SR ポリシー名が不明な場合、LDP は動作できません。

次の機能が適用されます。

1. SR ポリシーを設定する：LDP では、関連付けられたエンドポイントアドレスをインターフェイス マネージャ（IM）から受け取り、設定された SR ポリシーの LDP インターフェイス データベース（IDB）に保存します。
2. LDP で SR ポリシー名を設定する： LDP では、保存されたエンドポイントアドレスを IDB から取得して使用します。SR ポリシーを介して LDP ターゲット隣接関係を作成する際には、ルータによって割り当てられた自動生成 SR ポリシー名を使用します。自動生成 SR ポリシー名で使用される命名規則は、**srte_c_***color_val*_**ep_***endpoint-address* です。次に例を示します。 **srte_c_1000_ep_1.1.1.2**

設定例

```
/* Enter the SR-TE configuration mode and create the SR policy. This example corresponds
 to a local SR policy with an explicit path. */
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# segment-list sample-sid-list
Router(config-sr-te-sl)# index 10 address ipv4 1.1.1.7
Router(config-sr-te-sl)# index 20 address ipv4 1.1.1.2
Router(config-sr-te-sl)# exit
Router(config-sr-te)# policy sample_policy
Router(config-sr-te-policy)# color 1000 end-point ipv4 1.1.1.2
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy-path)# preference 100
Router(config-sr-te-policy-path-pref)# explicit segment-list sample-sid-list
Router(config-sr-te-pp-info)# end

/* Configure LDP over an SR policy */
Router(config)# mpls ldp
Router(config-ldp)# address-family ipv4
Router(config-ldp-af)# neighbor sr-policy srte_c_1000_ep_1.1.1.2 targeted
```

```
Router(config-ldp-af)#
```

（注） ターゲット hello の LDP ディスカバリを設定するには、次のいずれかを実行します。

- アクティブなターゲット hello（SR ポリシーヘッドエンド）：

```
mpls ldp
 interface GigabitEthernet0/0/0/0
  !
 !
```

- パッシブなターゲット hello（SR ポリシーエンドポイント）：

```
mpls ldp
 address-family ipv4
  discovery targeted-hello accept
 !
!
```

実行コンフィギュレーション

```
segment-routing
 traffic-eng
  segment-list sample-sid-list
   index 10 address ipv4 1.1.1.7
   index 20 address ipv4 1.1.1.2
  !
  policy sample_policy
   color 1000 end-point ipv4 1.1.1.2
   candidate-paths
    preference 100
     explicit segment-list sample-sid-list
     !
    !
   !
  !
 !
!

mpls ldp
 address-family ipv4
  neighbor sr-policy srte_c_1000_ep_1.1.1.2 targeted
  discovery targeted-hello accept
 !
!
```

確認

```
Router# show mpls ldp interface brief
Interface       VRF Name            Config Enabled IGP-Auto-Cfg TE-Mesh-Grp cfg
--------------- ------------------- ------ ------- ------------ ---------------
Te0/3/0/0/3     default             Y      Y       0            N/A
Te0/3/0/0/6     default             Y      Y       0            N/A
Te0/3/0/0/7     default             Y      Y       0            N/A
Te0/3/0/0/8     default             N      N       0            N/A
Te0/3/0/0/9     default             N      N       0            N/A
srte_c_1000_    default             Y      Y       0            N/A
```

```
Router# show mpls ldp interface
Interface TenGigE0/3/0/0/3 (0xa000340)
   VRF: 'default' (0x60000000)
   Enabled via config: LDP interface
Interface TenGigE0/3/0/0/6 (0xa000400)
   VRF: 'default' (0x60000000)
   Enabled via config: LDP interface
Interface TenGigE0/3/0/0/7 (0xa000440)
   VRF: 'default' (0x60000000)
   Enabled via config: LDP interface
Interface TenGigE0/3/0/0/8 (0xa000480)
   VRF: 'default' (0x60000000)
   Disabled:
Interface TenGigE0/3/0/0/9 (0xa0004c0)
   VRF: 'default' (0x60000000)
   Disabled:
Interface srte_c_1000_ep_1.1.1.2 (0x520)
   VRF: 'default' (0x60000000)
   Enabled via config: LDP interface


Router# show segment-routing traffic-eng policy color 1000

SR-TE policy database
---------------------

Color: 1000, End-point: 1.1.1.2
  Name: srte_c_1000_ep_1.1.1.2
  Status:
    Admin: up  Operational: up for 00:02:00 (since Jul  2 22:39:06.663)
  Candidate-paths:
    Preference: 100 (configuration) (active)
      Name: sample_policy
      Requested BSID: dynamic
      PCC info:
        Symbolic name: cfg_sample_policy_discr_100
        PLSP-ID: 17
      Explicit: segment-list sample-sid-list (valid)
        Weight: 1, Metric Type: TE
          16007 [Prefix-SID, 1.1.1.7]
          16002 [Prefix-SID, 1.1.1.2]
  Attributes:
    Binding SID: 80011
    Forward Class: 0
    Steering BGP disabled: no
    IPv6 caps enable: yes


Router# show mpls ldp neighbor 1.1.1.2 detail

Peer LDP Identifier: 1.1.1.2:0
  TCP connection: 1.1.1.2:646 - 1.1.1.6:57473
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 421/423; Downstream-Unsolicited
  Up time: 05:22:02
  LDP Discovery Sources:
    IPv4: (1)
      Targeted Hello (1.1.1.6 -> 1.1.1.2, active/passive)
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (9)
      1.1.1.2        2.2.2.99       10.1.2.2       10.2.3.2
```

```
    10.2.4.2       10.2.22.2      10.2.222.2     10.30.110.132
    11.2.9.2
  IPv6: (0)
Peer holdtime: 180 sec; KA interval: 60 sec; Peer state: Estab
NSR: Disabled
Clients: LDP over SR Policy
Capabilities:
  Sent:
    0x508  (MP: Point-to-Multipoint (P2MP))
    0x509  (MP: Multipoint-to-Multipoint (MP2MP))
    0x50a  (MP: Make-Before-Break (MBB))
    0x50b  (Typed Wildcard FEC)
  Received:
    0x508  (MP: Point-to-Multipoint (P2MP))
    0x509  (MP: Multipoint-to-Multipoint (MP2MP))
    0x50a  (MP: Make-Before-Break (MBB))
    0x50b  (Typed Wildcard FEC)
```

SR-TEポリシーを使用したスタティック ルート トラフィック ステアリング

以前のリリースでは、セグメント ルーティング ラベル スイッチド パス（SR-LSP）をスタティック ルートに関連付けることしかできませんでした。SRTEポリシーを使用したスタティック ルート トラフィック ステアリング機能を使用すると、MPLSおよびIPv6データ プレーンのスタティック ルートを設定するときに、セグメント ルーティング（SR）ポリシーをインターフェイス タイプとして指定できます。

スタティック ルートの設定に関する詳細については、『*Routing Configuration Guide for Cisco NCS 560 Series Routers*』の「Implementing Static Routes」の章を参照してください。

設定例

```
Router(config)# router static
Router (config-static)# address-family ipv4 unicast

//configure administrative distance
Router (config-static-afi)# 1.1.1.1/32 sr-policy policy1 110

//Configure load metric
Router (config-static-afi)# 1.1.1.1/32 sr-policy policy1 metric 5

//Install the route in RIB regardless of reachability
Router (config-static-afi)# 1.1.1.1/32 sr-policy policy1 permanent
```

実行コンフィギュレーション

```
configure
 router static
  address-family ipv4 unicast
  1.1.1.1/32 sr-policy policy1 110
  1.1.1.1/32 sr-policy policy1 metric 5
  1.1.1.1/32 sr-policy policy1 permanent
  !
 !
!
```

SR ポリシーのインスタンス化

SR ポリシーは、ヘッドエンドルータでインスタンス化されるか実装されます。

以降の項で、SR ポリシーのインスタンス化方法の詳細について説明します。

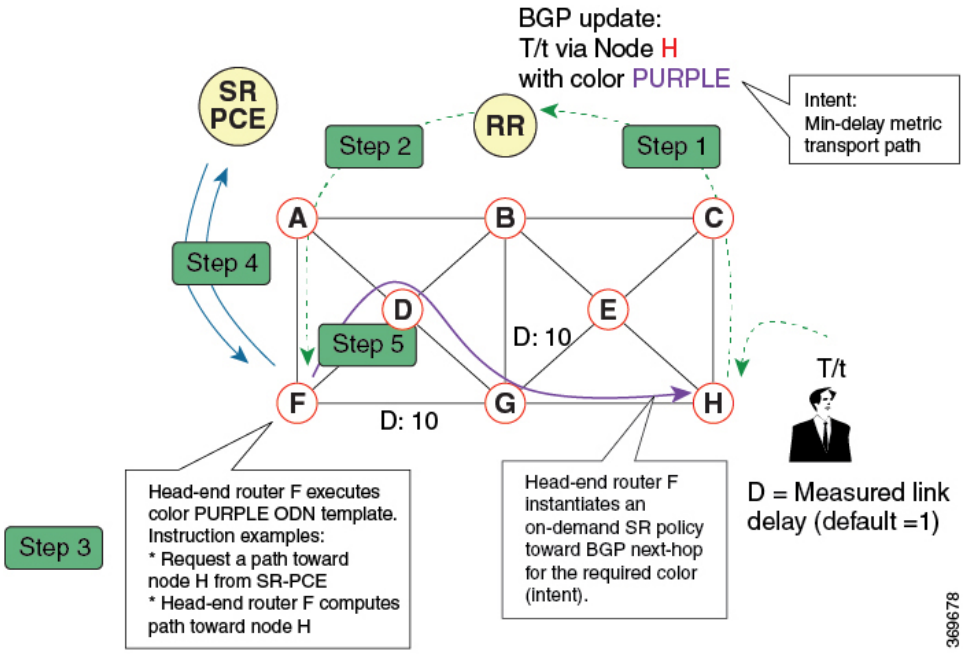
- オンデマンド SR ポリシー：SR オンデマンドネクストホップ （49 ページ）
- 手動でプロビジョニングされた SR ポリシー （84 ページ）
- PCE で開始された SR ポリシー （84 ページ）

オンデマンド SR ポリシー：SR オンデマンドネクストホップ

セグメント ルーティング オンデマンド ネクストホップ（SR-ODN）により、サービスヘッドエンドルータでは、必要に応じて（オンデマンドで）、BGP ネクストホップに対する SR ポリシーを自動的にインスタンス化できます。この機能の主な利点は、次のとおりです。

- **SLA 対応 BGP サービス**：宛先別のステアリング動作を利用して、プレフィックス、プレフィックスのセット、またはサービスからのすべてのプレフィックスを目的のアンダーレイ SLA に関連付けることができます。この機能は、単一ドメインネットワークとマルチドメインネットワークに同様に適用されます。
- **シンプルさ**：SR ポリシーの事前設定を構成して維持する必要がありません。代わりに、オペレータは、ネットワーク全体で共通のインテントに基づく最適化テンプレートをいくつか設定するだけです。
- **拡張性**：ヘッドエンドルータのデバイスリソースは、サービスまたは SLA 接続のニーズに基づいて、必要な場合にのみ使用されます。

次の例は、SR-ODN の仕組みを示しています。



1. 出力 PE（ノード H）は、プレフィックス T/t の BGP ルートをアドバタイズします。このアドバタイズメントには、BGP カラー拡張コミュニティでエンコードされた SLA インテントが含まれます。この例では、オペレータは、遅延について最適化されたパスを介してネットワークを通過するようにするプレフィックスに、カラーとして紫（値の例 = 100）を割り当てます。

2. ルートリフレクタは、アドバタイズされたルートを受信し、他の PE ノードにアドバタイズします。

3. ネットワーク内の入力 PE（ノード F など）には、目的とするカラーのルートが検出された場合に実行する手順をノードに提供する紫色用の ODN テンプレートが事前に設定されています。手順の例を次に示します。

   - 同じディスジョイントネス グループ内の別の LSP とノードを 1 つも共有しないノード H へのパスについては、SR-PCE に問い合わせて計算を要求します。
   - ヘッドエンドルータで、累積的な遅延を最小限に抑える、ノード H へのパスが計算されます。

4. この例では、ヘッドエンドルータは、SR-PCE に問い合わせて、累積的な遅延を最小限に抑えるノード H へのパスを計算するように要求します。

5. SR-PCE が計算パスを提供した後、インテント主導型の SR ポリシーがヘッドエンドルータでインスタンス化されます。同じインテント（カラー）を持ち、同じ出力 PE を宛先とする他のプレフィックスでは、同じオンデマンド SR ポリシーを共有できます。所定のペア（インテントと出力 PE）に関連付けられている最後のプレフィックスが取り消されると、オンデマンド SR ポリシーが削除され、ヘッドエンドルータからリソースが解放されます。

オンデマンドSRポリシーは、BGPグローバルまたはVPN（サービス）ルートに対して動的に作成されます。SR-ODN では、次のサービスがサポートされています。

- IPv4 BGP グローバルルート
- IPv6 BGP グローバルルート（6PE）
- VPNv4
- VPNv6（6vPE）
- EVPN-VPWS（シングルホーミング）

設定手順

SR-ODN を設定するには、次の手順を実行します。

1. SR-TE ヘッドエンドルータで SR-ODN テンプレートを定義します。

   （任意）パス計算にセグメントルーティングパス計算要素（SR-PCE）を使用する場合は、次の手順を実行します。

   1. SR-PCE を設定します。SR-PCE 設定情報の詳細については、SR-PCE の設定 （118 ページ）を参照してください。
   2. ヘッドエンドルータをパス計算要素プロトコル（PCEP）のパス計算クライアント（PCC）として設定します。PCEP PCC 設定情報の詳細については、PCEP PCC としてのヘッドエンドルータの設定 （99 ページ）を参照してください。

2. BGP カラー拡張コミュニティを定義します。『』の「Implementing BGP」の章を参照してください。
3. ルーティングポリシー（ルーティングポリシー言語（RPL）を使用）を定義して、BGP カラー拡張コミュニティを設定します。『』の「Implementing Routing Policy」の章を参照してください。

   BGP カラー拡張コミュニティを設定または照合するための次の RPL 接続点がサポートされています。

（注） 次の表は、サポートされる RPL 照合操作を示しています。ただし、BGP カラー拡張コミュニティを設定するためには、基本的にルーティングポリシーが必要になります。BGP カラー拡張コミュニティに基づく照合は、ODN のオンデマンド カラー テンプレートによって自動的に実行されます。

接続点	セット	一致
VRF export	×	×
VRF import	–	×

接続点	セット	一致
EVI export	×	–
EVI import	×	×
neighbor-in	×	×
neighbor-out	×	×
AFI 間 export	–	×
AFI 間 import	–	×
default-originate	×	–

4. ルーティングポリシーをサービスに適用します。『』の「Implementing Routing Policy」の章を参照してください。

オンデマンド カラー テンプレートの設定

- 指定したカラー値の ODN テンプレートを作成するには、**on-demand color** *color* コマンドを使用します。ヘッドエンドルータは、テンプレートで指定されたカラー値と一致する BGP カラー拡張コミュニティを持つ BGP グローバルルートまたは VPN ルートの到着時に、テンプレートで定義されたアクションを自動的に実行します。

  color の範囲は 1 ～ 4294967295 です。

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# on-demand color 10
```

（注） BGP カラー拡張コミュニティに基づく照合は、ODN のオンデマンド カラー テンプレートによって自動的に実行されます。RPL ルーティングポリシーは必要ありません。

- （TE トポロジデータベースを利用する SR-TE ヘッドエンドルータによって）ローカルで計算されたダイナミックパスまたは（SR-PCE によって）中央で計算されたダイナミックパスを使用するオンデマンド SR ポリシーにテンプレートを関連付けるには、**on-demand color** *color* **dynamic** コマンドを使用します。ヘッドエンドルータは、まず、ローカルで計算されたパスをインストールしようとします。それ以外の場合は、SR-PCE によって計算されたパスを使用します。

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# on-demand color 10 dynamic
```

- SR-PCE によって計算されたパスのみをオンデマンド SR ポリシーに関連付ける必要があることを示すには、**on-demand color** *color* **dynamic pcep** コマンドを使用します。この設定

では、ローカルパスの計算は試行されません。代わりに、ヘッドエンドルータは SR-PCE によって計算されたパスだけをインスタンス化します。

```
Router(config-sr-te)# on-demand color 10 dynamic pcep
```

ダイナミックパス最適化の目的の設定

- パス計算で使用するメトリックを設定するには、**metric type** {**igp** | **te** | **latency**} コマンドを使用します。

```
Router(config-sr-te-color-dyn)# metric type te
```

- オンデマンドのダイナミックパスのメトリックマージンを設定するには、**metric margin** {**absolute** *value*| **relative** *percent*} コマンドを使用します。*value* および *percent* の範囲は 0 ～ 2147483647 です。

```
Router(config-sr-te-color-dyn)# metric margin absolute 5
```

ダイナミックパス制約の設定

- ディスジョイントパス制約を設定するには、**disjoint-path group-id** *group-id* **type** {**link** | **node** | **srlg** | **srlg-node**} [**sub-id** *sub-id*] コマンドを使用します。*group-id* および *sub-id* の範囲は 1 ～ 65535 です。

```
Router(config-sr-te-color-dyn)# disjoint-path group-id 775 type link
```

- アフィニティ制約を設定するには、**affinity** {**include-any** | **include-all** | **exclude-any**} {**name** *WORD*} コマンドを使用します。

```
Router(config-sr-te-color-dyn)# affinity exclude-any name CROSS
```

- SR フレキシブルアルゴリズム制約を設定するには、**sid-algorithm** *algorithm-number* コマンドを使用します。*algorithm-number* の範囲は 128 ～ 255 です。

```
Router(config-sr-te-color-dyn)# sid-algorithm 128
```

- ルータによってアドバタイズされる最大SID深度（MSD）制約をカスタマイズするには、**maximum-sid-depth** *value* コマンドを使用します。

  デフォルトの MSD *value* は、プラットフォームでサポートされている最大 MSD（12）と同じです。

```
Router(config-sr-te-color)# maximum-sid-depth 5
```

（注） プラットフォームの SR-TE ラベルインポジションの能力は、次のとおりです。

- サービスラベルが適用されない場合、最大 12 個のトランスポートラベル
- サービスラベルが適用される場合、最大 9 個のトランスポートラベル

PCE でパスが計算される場合、PCC では、次の方法で MSD を PCE にシグナリングできます。

- PCEP セッションの確立時：シグナリングされた MSD はノード全体のプロパティとして扱われます。
  - MSD は、**segment-routing traffic-eng maximum-sid-depth** *value* コマンドで設定します。
- PCEP LSP パスの要求時：シグナリングされた MSD は LSP プロパティとして扱われます。
  - オンデマンド（ODN）SR ポリシー：MSD は、**segment-routing traffic-eng on-demand color** *color* **maximum-sid-depth** *value* コマンドを使用して設定します。
  - ローカル SR ポリシー：MSD は、**segment-routing traffic-eng policy** *WORD* **candidate-paths preference** *preference* **dynamic metric sid-limit** *value* コマンドを使用して設定します。

（注） 設定された MSD 値が異なる場合、LSP ごとの MSD がノードごとの MSD よりも優先されます。

パス計算の後、MSD 要件と照らし合わせて、結果のラベルスタックサイズが検証されます。

- パス計算が PCE によって実行された場合に、ラベルスタックサイズが MSD よりも大きいときは、PCE は PCC に「パスなし」の応答を返します。
- パス計算が PCC によって実行された場合に、ラベルスタックサイズが MSD よりも大きいときは、PCC はパスを組み込みません。

（注） 次のケースでは、MSD制約を満たす次善のパス（存在する場合）が計算されます。

- TE メトリックを使用したダイナミックパスの場合に、**pce segment-routing te-latency** コマンドを使用して PCE が設定されているか、**segment-routing traffic-eng te-latency** コマンドを使用して PCC が設定されているとき
- LATENCY メトリックを使用したダイナミックパスの場合
- アフィニティ制約を使用したダイナミックパスの場合

たとえば、PCC MSD が 4 で、最適パス（累積メトリックが 100）は 5 個のラベルを必要とするが、4 個のラベルを必要とする次善のパス（累積メトリックが 110）が存在する場合は、次善のパスが組み込まれます。

SR-ODN の設定：例

SR-ODN の設定：レイヤ 3 サービスの例

次の例は、ヘッドエンドルータでの SR-ODN の実装に使用するエンドツーエンドの設定を示しています。

ODN カラーテンプレートの設定：例

SR-TE ヘッドエンドノードとして機能するルータで ODN カラーテンプレートを設定します。次の例は、さまざまな ODN カラーテンプレートを示しています。

- カラー 10：最小化の目的 = TE メトリック
- カラー 20：最小化の目的 = IGP メトリック
- カラー 21：最小化の目的 = IGP メトリック、制約 = アフィニティ
- カラー 22：最小化の目的 = TE メトリック、SR-PCE でパス計算、制約 = アフィニティ
- カラー 30：最小化の目的 = 遅延メトリック
- カラー 128：制約 = フレキシブルアルゴリズム

```
segment-routing
 traffic-eng
  on-demand color 10
   dynamic
    metric
     type te
    !
   !
  !
  on-demand color 20
```

```
   dynamic
    metric
     type igp
    !
   !
  !
  on-demand color 21
   dynamic
    metric
     type igp
    !
    affinity exclude-any
     name CROSS
    !
   !
  !
  on-demand color 22
   dynamic
    pcep
    !
    metric
     type te
    !
    affinity exclude-any
     name CROSS
    !
   !
  !
  on-demand color 30
   dynamic
    metric
     type latency
    !
   !
  !
  on-demand color 128
   dynamic
    sid-algorithm 128
   !
  !
!
end
```

BGP カラー拡張コミュニティセットの設定：例

次の例は、ルートポリシーを介して BGP サービスルートに後で適用される BGP カラー拡張コミュニティを設定する方法を示しています。

（注） 多くの一般的なシナリオでは、BGP サービスルートをアドバタイズする出力 PE ルータは、BGP カラー拡張コミュニティを適用（設定）します。ただし、入力 PE ルータでカラーを設定することもできます。

```
extcommunity-set opaque color10-te
  10
end-set
!
extcommunity-set opaque color20-igp
  20
end-set
```

```
!
extcommunity-set opaque color21-igp-excl-cross
  21
end-set
!
extcommunity-set opaque color30-delay
  30
end-set
!
extcommunity-set opaque color128-fa128
  128
end-set
!
```

BGP カラーを設定する RPL の構成（レイヤ 3 サービス）：例

次の例は、BGP カラーコミュニティを設定する代表的な RPL 定義を示しています。

最初の 4 つの RPL の例には、カラーアクションの設定のみが含まれています。最後の RPL の例では、prefix-set に基づいて選択された宛先に対するカラーアクションの設定を実行します。

```
route-policy SET_COLOR_LOW_LATENCY_TE
  set extcommunity color color10-te
  pass
end-policy
!
route-policy SET_COLOR_HI_BW
  set extcommunity color color20-igp
  pass
end-policy
!
route-policy SET_COLOR_LOW_LATENCY
  set extcommunity color color30-delay
  pass
end-policy
!
route-policy SET_COLOR_FA_128
  set extcommunity color color128-fa128
  pass
end-policy
!

prefix-set sample-set
  88.1.0.0/24
end-set
!
route-policy SET_COLOR_GLOBAL
  if destination in sample-set then
    set extcommunity color color10-te
  else
    pass
  endif
end-policy
```

BGP サービスへの RPL の適用（レイヤ 3 サービス）：例

次の例は、BGP レイヤ 3 VPN サービス（VPNv4/VPNv6）および BGP グローバルに適用される BGP カラーコミュニティを設定する、さまざまな RPL を示しています。

- L3VPN の各例は、VRF export 接続点で適用される RPL を示しています。
- BGP グローバルの例は、BGP neighbor-out 接続点で適用される RPL を示しています。

```
vrf vrf_cust1
 address-family ipv4 unicast
  export route-policy SET_COLOR_LOW_LATENCY_TE
 !
 address-family ipv6 unicast
  export route-policy SET_COLOR_LOW_LATENCY_TE
 !
!
vrf vrf_cust2
 address-family ipv4 unicast
  export route-policy SET_COLOR_HI_BW
 !
 address-family ipv6 unicast
  export route-policy SET_COLOR_HI_BW
 !
!
vrf vrf_cust3
 address-family ipv4 unicast
  export route-policy SET_COLOR_LOW_LATENCY
 !
 address-family ipv6 unicast
  export route-policy SET_COLOR_LOW_LATENCY
 !
!

vrf vrf_cust4
 address-family ipv4 unicast
  export route-policy SET_COLOR_FA_128
 !
 address-family ipv6 unicast
  export route-policy SET_COLOR_FA_128
 !
!
router bgp 100
 neighbor-group BR-TO-RR
  address-family ipv4 unicast
   route-policy SET_COLOR_GLOBAL out
  !
 !
!
end
```

BGP VRF 情報の確認

VRF インスタンスの BGP プレフィックス情報を表示するには、**show bgp vrf** コマンドを使用します。次の出力は、ルータ 1.1.1.8 によってアドバタイズされたカラー 10 のプレフィックス（88.1.1.0/24）を含む BGP VRF テーブルを示しています。

```
RP/0/RP0/CPU0:R4# show bgp vrf vrf_cust1

BGP VRF vrf_cust1, state: Active
BGP Route Distinguisher: 1.1.1.4:101
VRF ID: 0x60000007
BGP router identifier 1.1.1.4, local AS number 100
Non-stop routing is enabled
BGP table state: Active
Table ID: 0xe0000007   RD version: 282
BGP main routing table version 287
BGP NSR Initial initsync version 31 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1.1.1.4:101 (default for vrf vrf_cust1)
*> 44.1.1.0/24        40.4.101.11                            0 400 {1} i
*>i55.1.1.0/24        1.1.1.5                  100           0 500 {1} i
*>i88.1.1.0/24        1.1.1.8 C:10             100           0 800 {1} i
*>i99.1.1.0/24        1.1.1.9                  100           0 800 {1} i

Processed 4 prefixes, 4 paths
```

次の出力は、プレフィックス 88.1.1.0/24 の詳細を示しています。BGP 拡張カラーコミュニティ 10 が存在すること、およびカラー 10 と BSID 値 24036 を使用する SR ポリシーにプレフィックスが関連付けられていることに注目してください。

```
RP/0/RP0/CPU0:R4# show bgp vrf vrf_cust1 88.1.1.0/24

BGP routing table entry for 88.1.1.0/24, Route Distinguisher: 1.1.1.4:101
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                282         282
Last Modified: May 20 09:23:34.112 for 00:06:03
Paths: (1 available, best #1)
  Advertised to CE peers (in unique update groups):
    40.4.101.11
  Path #1: Received by speaker 0
  Advertised to CE peers (in unique update groups):
    40.4.101.11
  800 {1}
    1.1.1.8 C:10 (bsid:24036) (metric 20) from 1.1.1.55 (1.1.1.8)
      Received Label 24012
      Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate,
imported
      Received Path ID 0, Local Path ID 1, version 273
      Extended community: Color:10 RT:100:1
      Originator: 1.1.1.8, Cluster list: 1.1.1.55
      SR policy color 10, up, registered, bsid 24036, if-handle 0x08000024

      Source AFI: VPNv4 Unicast, Source VRF: default, Source Route Distinguisher:
1.1.1.8:101
```

転送（CEF）テーブルの確認

VRF インスタンスの CEF テーブルの内容を表示するには、**show cef vrf** コマンドを使用します。プレフィックス 88.1.1.0/24 が、SR ポリシーに対応する BSID ラベルを指していることに注目してください。55.1.1.0/24 など、その他のカラー付きでないプレフィックスは、BGP ネクストホップを指しています。

```
RP/0/RP0/CPU0:R4# show cef vrf vrf_cust1

Prefix              Next Hop            Interface
------------------- ------------------- ------------------
0.0.0.0/0           drop                default handler
0.0.0.0/32          broadcast
40.4.101.0/24       attached            TenGigE0/0/0/0.101
40.4.101.0/32       broadcast           TenGigE0/0/0/0.101
40.4.101.4/32       receive             TenGigE0/0/0/0.101
40.4.101.11/32      40.4.101.11/32      TenGigE0/0/0/0.101
40.4.101.255/32     broadcast           TenGigE0/0/0/0.101
44.1.1.0/24         40.4.101.11/32      <recursive>
55.1.1.0/24         1.1.1.5/32          <recursive>
88.1.1.0/24         24036 (via-label)   <recursive>
```

```
99.1.1.0/24          1.1.1.9/32          <recursive>
224.0.0.0/4          0.0.0.0/32
224.0.0.0/24         receive
255.255.255.255/32   broadcast
```

次の出力は、プレフィックス 88.1.1.0/24 の CEF の詳細を示しています。BSID 値 24036 を使用する SR ポリシーにプレフィックスが関連付けられていることに注目してください。

```
RP/0/RP0/CPU0:R4# show cef vrf vrf_cust1 88.1.1.0/24

88.1.1.0/24, version 51, internal 0x5000001 0x0 (ptr 0x98c60ddc) [1], 0x0 (0x0), 0x208
(0x98425268)
 Updated May 20 09:23:34.216
 Prefix Len 24, traffic index 0, precedence n/a, priority 3
   via local-label 24036, 5 dependencies, recursive [flags 0x6000]
    path-idx 0 NHID 0x0 [0x97091ec0 0x0]
    recursion-via-label
    next hop VRF - 'default', table - 0xe0000000
    next hop via 24036/0/21
     next hop srte_c_10_ep labels imposed {ImplNull 24012}
```

SR ポリシーの確認

SR ポリシー情報を表示するには、**show segment-routing traffic-eng policy** コマンドを使用します。

次の出力は、ノード 1.1.1.8 からアドバタイズされたカラー 10 のプレフィックスによってトリガーされた、オンデマンド SR ポリシーの詳細を示しています。

```
RP/0/RP0/CPU0:R4# show segment-routing traffic-eng policy color 10 tabular

 Color             Endpoint  Admin   Oper              Binding
                             State   State                 SID
------ --------------------- ------ ------ --------------------
    10              1.1.1.8     up     up                24036
```

次の出力は、BSID 24036 のオンデマンド SR ポリシーの詳細を示しています。

（注） この SR ポリシーには 2 つの候補パスが関連付けられています。ヘッドエンドルータによって計算されたパス（優先順位 200）と、SR-PCE によって計算されたパス（優先順位 100）です。優先順位が最も高い候補パスが、アクティブな候補パス（下の例で強調表示されています）で、転送に組み込まれます。

```
RP/0/RP0/CPU0:R4# show segment-routing traffic-eng policy binding-sid 24036

SR-TE policy database
---------------------

Color: 10, End-point: 1.1.1.8
  Name: srte_c_10_ep_1.1.1.8
  Status:
    Admin: up  Operational: up for 4d14h (since Jul  3 20:28:57.840)
  Candidate-paths:
    Preference: 200 (BGP ODN) (active)
      Requested BSID: dynamic
```

```
      PCC info:
        Symbolic name: bgp_c_10_ep_1.1.1.8_discr_200
        PLSP-ID: 12
      Dynamic (valid)
        Metric Type: TE,   Path Accumulated Metric: 30
            16009 [Prefix-SID, 1.1.1.9]
            16008 [Prefix-SID, 1.1.1.8]
    Preference: 100 (BGP ODN)
      Requested BSID: dynamic
      PCC info:
        Symbolic name: bgp_c_10_ep_1.1.1.8_discr_100
        PLSP-ID: 11
      Dynamic (pce 1.1.1.57) (valid)
        Metric Type: TE,   Path Accumulated Metric: 30
            16009 [Prefix-SID, 1.1.1.9]
            16008 [Prefix-SID, 1.1.1.8]
  Attributes:
    Binding SID: 24036
    Forward Class: 0
    Steering BGP disabled: no
    IPv6 caps enable: yes
```

SR ポリシー転送の確認

SR ポリシー転送情報を表示するには、**show segment-routing traffic-eng forwarding policy** コマンドを使用します。

次の出力は、ノード 1.1.1.8 からアドバタイズされたカラー 10 のプレフィックスによってトリガーされた、オンデマンド SR ポリシーの転送の詳細を示しています。

```
RP/0/RP0/CPU0:R4# show segment-routing traffic-eng forwarding policy binding-sid 24036
tabular

Color Endpoint        Segment      Outgoing Outgoing     Next Hop     Bytes         Pure
                      List         Label    Interface                Switched      Backup
----- --------------- ------------ -------- ------------ ------------ ------------ ------
10    1.1.1.8         dynamic      16009    Gi0/0/0/4    10.4.5.5     0
                                   16001    Gi0/0/0/5    11.4.8.8     0             Yes

RP/0/RP0/CPU0:R4# show segment-routing traffic-eng forwarding policy binding-sid 24036
detail
Mon Jul  8 11:56:46.887 PST

SR-TE Policy Forwarding database
--------------------------------

Color: 10, End-point: 1.1.1.8
  Name: srte_c_10_ep_1.1.1.8
  Binding SID: 24036
  Segment Lists:
    SL[0]:
      Name: dynamic
      Paths:
        Path[0]:
          Outgoing Label: 16009
          Outgoing Interface: GigabitEthernet0/0/0/4
          Next Hop: 10.4.5.5
          Switched Packets/Bytes: 0/0
          FRR Pure Backup: No
          Label Stack (Top -> Bottom): { 16009, 16008 }
          Path-id: 1 (Protected), Backup-path-id: 2, Weight: 64
        Path[1]:
```

```
        Outgoing Label: 16001
        Outgoing Interface: GigabitEthernet0/0/0/5
        Next Hop: 11.4.8.8
        Switched Packets/Bytes: 0/0
        FRR Pure Backup: Yes
        Label Stack (Top -> Bottom): { 16001, 16009, 16008 }
        Path-id: 2 (Pure-Backup), Weight: 64
Policy Packets/Bytes Switched: 0/0
Local label: 80013
```

EVPN-VPWS 用の SR-ODN の設定：使用例

この使用例では、2 つのサイト間で EVPN-VPWS を使用して ELINE サービスのペアを設定する方法を示します。サービスは、そのパス上で共通のリンクを共有しない（リンクディスジョイント）SR ポリシーを介して伝送されます。SR ポリシーは、ODN の原則に基づいてオンデマンドでトリガーされます。ディスジョイントパスは SR-PCE によって計算されます。

この使用例では、2 つのサイトがある次のトポロジを使用します。サイト 1 にはノード A およびノード B が含まれており、サイト 2 にはノード C およびノード D が含まれています。

図 *3 :* 使用例のトポロジ：*EVPN-VPWS* 用の *SR-ODN*

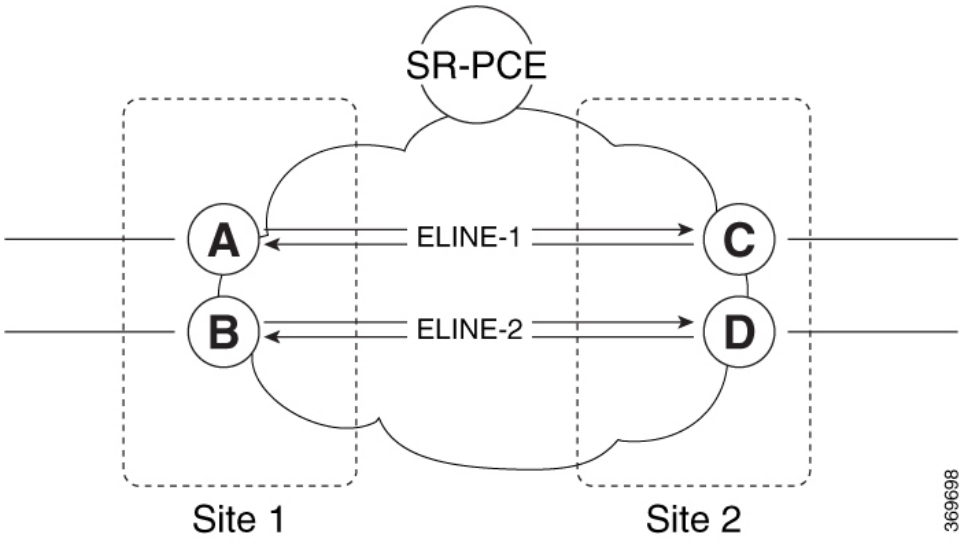


表 *2 :* 使用例のパラメータ

Loopback0（Lo0）インターフェイスの IP アドレス	PCE Lo0：1.1.1.207	
	サイト 1： • ノード A の Lo0：1.1.1.5 • ノード B の Lo0：1.1.1.6	サイト 2： • ノード C の Lo0：1.1.1.2 • ノード D の Lo0：1.1.1.4

EVPN-VPWS サービス パラメータ	ELINE-1： • EVPN-VPWS EVI 100 • ノード A：AC-ID = 11 • ノード C：AC-ID = 21	ELINE-2： • EVPN-VPWS EVI 101 • ノード B：AC-ID = 12 • ノード D：AC-ID = 22
ODN BGP カラー拡張コミュニティ	サイト 1 のルータ（ノード A および B）： • set color 10000 • match color 11000	サイト 2 のルータ（ノード C および D）： • set color 11000 • match color 10000
（注）　これらのカラーは、EVPN-VPWS サービスの EVPN ルートタイプ 1 ルートに関連付けられています。		
PCEP LSP ディスジョイントパス アソシエーション グループ ID	サイト 1 からサイト 2 への LSP（ノード A からノード C へ/ノード B からノード D へ）： • group-id = 775	サイト 2 からサイト 1 への LSP（ノード C からノード A へ/ノード D からノード B へ）： • group-id = 776

この使用例では、すべてのデバイスの設定および確認の出力を提供します。

設定	確認
設定：SR-PCE （63 ページ）	確認：SR-PCE （68 ページ）
設定：サイト 1 のノード A （64 ページ）	確認：サイト 1 のノード A （72 ページ）
設定：サイト 1 のノード B （65 ページ）	確認：サイト 1 のノード B （75 ページ）
設定：サイト 2 のノード C （66 ページ）	確認：サイト 2 のノード C （78 ページ）
設定：サイト 2 のノード D （67 ページ）	確認：サイト 2 のノード D （81 ページ）

設定：SR-PCE

設定されたディスジョイントの LSP のペアを示す PCEP アソシエーショングループ オブジェクトが、PCC ノードによってサポートまたはシグナリングされる場合は、ディスジョイントパス計算をトリガーするために SR-PCE で必要となる追加設定はありません。

（注）　SR-PCE では、PCC ノードが PCEP アソシエーショングループ オブジェクトをサポートしていない場合のディスジョイントパス計算もサポートしています。詳細については、「ディスジョイント ポリシーの設定（オプション） （120 ページ）」を参照してください。

設定：サイト 1 のノード A

このセクションでは、サイト 1 のノード A に関連する設定を示します。これには、サービス設定、BGP カラー拡張コミュニティ、および RPL が含まれます。また、ディスジョイントネス SLA を達成するために必要な対応する ODN テンプレートも含まれています。

サイト 1 のノードは、発信 EVPN ルートにカラー 10000 を設定する一方で、サイト 2 にあるルータからの着信 EVPN ルートではカラー 11000 と照合するように構成されています。

サイト 1 の両方のノードが、同じディスジョイントパス グループ ID（775）を使用して SR-PCE によるパス計算を要求するため、PCE では、サイト 1 からサイト 2 に発信される LSP のペアのディスジョイントネスを計算します。

```
/* EVPN-VPWS configuration */

interface GigabitEthernet0/0/0/3.2500 l2transport
 encapsulation dot1q 2500
 rewrite ingress tag pop 1 symmetric
!
l2vpn
 xconnect group evpn_vpws_group
  p2p evpn_vpws_100
   interface GigabitEthernet0/0/0/3.2500
   neighbor evpn evi 100 target 21 source 11
   !
  !
 !
!

/* BGP color community and RPL configuration */

extcommunity-set opaque color-10000
  10000
end-set
!
route-policy SET_COLOR_EVPN_VPWS
  if evpn-route-type is 1 and rd in (ios-regex '.*..*..*..*:(100)') then
    set extcommunity color color-10000
  endif
  pass
end-policy
!
router bgp 65000
 neighbor 1.1.1.253
  address-family l2vpn evpn
   route-policy SET_COLOR_EVPN_VPWS out
  !
 !
!

/* ODN template configuration */

segment-routing
 traffic-eng
  on-demand color 11000
   dynamic
    pcep
    !
    metric
     type igp
    !
    disjoint-path group-id 775 type link
```

```
   !
  !
 !
!
```

設定：サイト 1 のノード B

このセクションでは、サイト 1 のノード B に関連する設定を示します。

```
/* EVPN-VPWS configuration */

interface TenGigE0/3/0/0/8.2500 l2transport
 encapsulation dot1q 2500
 rewrite ingress tag pop 1 symmetric
!
l2vpn
 xconnect group evpn_vpws_group
  p2p evpn_vpws_101
   interface TenGigE0/3/0/0/8.2500
   neighbor evpn evi 101 target 22 source 12
   !
  !
 !
!

/* BGP color community and RPL configuration */

extcommunity-set opaque color-10000
  10000
end-set
!
route-policy SET_COLOR_EVPN_VPWS
  if evpn-route-type is 1 and rd in (ios-regex '.*..*..*..*:(101)') then
    set extcommunity color color-10000
  endif
  pass
end-policy
!
router bgp 65000
 neighbor 1.1.1.253
  address-family l2vpn evpn
   route-policy SET_COLOR_EVPN_VPWS out
  !
 !
!

/* ODN template configuration */

segment-routing
 traffic-eng
  on-demand color 11000
   dynamic
    pcep
    !
    metric
     type igp
    !
    disjoint-path group-id 775 type link
   !
  !
 !
!
```

設定：サイト 2 のノード C

このセクションでは、サイト 2 のノード C に関連する設定を示します。これには、サービス設定、BGP カラー拡張コミュニティ、および RPL が含まれます。また、ディスジョイントネス SLA を達成するために必要な対応する ODN テンプレートも含まれています。

サイト 2 のノードは、発信 EVPN ルートにカラー 11000 を設定する一方で、サイト 1 にあるルータからの着信 EVPN ルートではカラー 10000 と照合するように構成されています。

サイト 2 の両方のノードが、同じディスジョイントパス グループ ID（776）を使用して SR-PCE によるパス計算を要求するため、PCE では、サイト 2 からサイト 1 に発信される LSP のペアのディスジョイントネスを計算します。

```
/* EVPN-VPWS configuration */

interface GigabitEthernet0/0/0/3.2500 l2transport
 encapsulation dot1q 2500
 rewrite ingress tag pop 1 symmetric
!
l2vpn
 xconnect group evpn_vpws_group
  p2p evpn_vpws_100
   interface GigabitEthernet0/0/0/3.2500
   neighbor evpn evi 100 target 11 source 21
   !
  !
 !
!

/* BGP color community and RPL configuration */

extcommunity-set opaque color-11000
  11000
end-set
!
route-policy SET_COLOR_EVPN_VPWS
  if evpn-route-type is 1 and rd in (ios-regex '.*..*..*..*:(100)') then
    set extcommunity color color-11000
  endif
  pass
end-policy
!
router bgp 65000
 neighbor 1.1.1.253
  address-family l2vpn evpn
   route-policy SET_COLOR_EVPN_VPWS out
  !
 !
!

/* ODN template configuration */

segment-routing
 traffic-eng
  on-demand color 10000
   dynamic
    pcep
    !
    metric
     type igp
    !
    disjoint-path group-id 776 type link
```

```
   !
  !
 !
!
```

設定：サイト 2 のノード D

このセクションでは、サイト 2 のノード D に関連する設定を示します。

```
/* EVPN-VPWS configuration */

interface GigabitEthernet0/0/0/1.2500 l2transport
 encapsulation dot1q 2500
 rewrite ingress tag pop 1 symmetric
!
l2vpn
 xconnect group evpn_vpws_group
  p2p evpn_vpws_101
   interface GigabitEthernet0/0/0/1.2500
   neighbor evpn evi 101 target 12 source 22
   !
  !
 !
!

/* BGP color community and RPL configuration */

extcommunity-set opaque color-11000
  11000
end-set
!
route-policy SET_COLOR_EVPN_VPWS
  if evpn-route-type is 1 and rd in (ios-regex '.*..*..*..*:(101)') then
    set extcommunity color color-11000
  endif
  pass
end-policy
!
router bgp 65000
 neighbor 1.1.1.253
  address-family l2vpn evpn
   route-policy SET_COLOR_EVPN_VPWS out
  !
 !
!

/* ODN template configuration */

segment-routing
 traffic-eng
  on-demand color 10000
   dynamic
    pcep
    !
    metric
     type igp
    !
    disjoint-path group-id 776 type link
   !
  !
 !
!
```

確認：SR-PCE

SR-PCE の PCEP ピアとセッションステータスを表示するには、**show pce ipv4 peer** コマンドを使用します。SR-PCE は、使用例に示されている 4 つのノードのパス計算を実行します。

```
RP/0/0/CPU0:SR-PCE# show pce ipv4 peer
Mon Jul 15 19:41:43.622 UTC

PCE's peer database:
--------------------
Peer address: 1.1.1.2
  State: Up
  Capabilities: Stateful, Segment-Routing, Update, Instantiation

Peer address: 1.1.1.4
  State: Up
  Capabilities: Stateful, Segment-Routing, Update, Instantiation

Peer address: 1.1.1.5
  State: Up
  Capabilities: Stateful, Segment-Routing, Update, Instantiation

Peer address: 1.1.1.6
  State: Up
  Capabilities: Stateful, Segment-Routing, Update, Instantiation
```

特定のアソシエーショングループ ID 値に割り当てられた LSP のペアの情報を表示するには、**show pce association group-id** コマンドを使用します。

この使用例の目標に基づいて、SR-PCE は、サイト 1 とサイト 2 の間の ELINE サービスのペアに関連付けられた SR ポリシーのリンクディスジョイントパスを計算します。具体的には、サイト 1 からサイト 2 へのディスジョイント LSP はアソシエーショングループ ID 775 によって識別されます。出力には、このグループ ID に関連付けられた LSP の概要情報が含まれています。

- ノード A（1.1.1.5）：LSP シンボリック名 = bgp_c_11000_ep_1.1.1.2_discr_100
- ノード B（1.1.1.6）：LSP シンボリック名 = bgp_c_11000_ep_1.1.1.4_discr_100

この場合、SR-PCE は目的のディスジョイントネスレベルを達成できています。したがって、ステータスは「Satisfied」として表示されています。

```
RP/0/0/CPU0:SR-PCE# show pce association group-id 775
Thu Jul 11 03:52:20.770 UTC

PCE's association database:
----------------------
Association: Type Link-Disjoint, Group 775, Not Strict
 Associated LSPs:
  LSP[0]:
   PCC 1.1.1.6, tunnel name bgp_c_11000_ep_1.1.1.4_discr_100,  PLSP ID 18, tunnel ID 17,
 LSP ID 3, Configured on PCC
  LSP[1]:
   PCC 1.1.1.5, tunnel name bgp_c_11000_ep_1.1.1.2_discr_100,  PLSP ID 18, tunnel ID 18,
 LSP ID 3, Configured on PCC
 Status: Satisfied
```

PCE の LSP データベースに存在する LSP の詳細情報を表示するには、**show pce lsp** コマンドを使用します。この出力には、ノード C（1.1.1.2）への EVPN VPWS EVI 100 のトラフィックを伝送するために使用される、ノード A（1.1.1.5）の LSP の詳細が表示されています。

```
RP/0/0/CPU0:SR-PCE# show pce lsp pcc ipv4 1.1.1.5 name bgp_c_11000_ep_1.1.1.2_discr_100
Thu Jul 11 03:58:45.903 UTC

PCE's tunnel database:
----------------------
PCC 1.1.1.5:

Tunnel Name: bgp_c_11000_ep_1.1.1.2_discr_100
Color: 11000
Interface Name: srte_c_11000_ep_1.1.1.2
 LSPs:
  LSP[0]:
   source 1.1.1.5, destination 1.1.1.2, tunnel ID 18, LSP ID 3
   State: Admin up, Operation up
   Setup type: Segment Routing
   Binding SID: 80037
   Maximum SID Depth: 10
   Absolute Metric Margin: 0
   Relative Metric Margin: 0%
   Preference: 100
   Bandwidth: signaled 0 kbps, applied 0 kbps
   PCEP information:
     PLSP-ID 0x12, flags: D:1 S:0 R:0 A:1 O:1 C:0
   LSP Role: Exclude LSP
   State-sync PCE: None
   PCC: 1.1.1.5
   LSP is subdelegated to: None
   Reported path:
     Metric type: IGP, Accumulated Metric 40
      SID[0]: Adj, Label 80003, Address: local 11.5.8.5 remote 11.5.8.8
      SID[1]: Node, Label 16007, Address 1.1.1.7
      SID[2]: Node, Label 16002, Address 1.1.1.2
   Computed path: (Local PCE)
     Computed Time: Thu Jul 11 03:49:48 UTC 2019 (00:08:58 ago)
     Metric type: IGP, Accumulated Metric 40
      SID[0]: Adj, Label 80003, Address: local 11.5.8.5 remote 11.5.8.8
      SID[1]: Node, Label 16007, Address 1.1.1.7
      SID[2]: Node, Label 16002, Address 1.1.1.2
   Recorded path:
     None
   Disjoint Group Information:
     Type Link-Disjoint, Group 775
```

この出力には、ノード D（1.1.1.4）への EVPN VPWS EVI 101 のトラフィックを伝送するために使用される、ノード B（1.1.1.6）の LSP の詳細が表示されています。

```
RP/0/0/CPU0:SR-PCE# show pce lsp pcc ipv4 1.1.1.6 name bgp_c_11000_ep_1.1.1.4_discr_100
Thu Jul 11 03:58:56.812 UTC

PCE's tunnel database:
----------------------
PCC 1.1.1.6:

Tunnel Name: bgp_c_11000_ep_1.1.1.4_discr_100
Color: 11000
Interface Name: srte_c_11000_ep_1.1.1.4
 LSPs:
  LSP[0]:
   source 1.1.1.6, destination 1.1.1.4, tunnel ID 17, LSP ID 3
```

```
  State: Admin up, Operation up
  Setup type: Segment Routing
  Binding SID: 80061
  Maximum SID Depth: 10
  Absolute Metric Margin: 0
  Relative Metric Margin: 0%
  Preference: 100
  Bandwidth: signaled 0 kbps, applied 0 kbps
  PCEP information:
    PLSP-ID 0x12, flags: D:1 S:0 R:0 A:1 O:1 C:0
  LSP Role: Disjoint LSP
  State-sync PCE: None
  PCC: 1.1.1.6
  LSP is subdelegated to: None
  Reported path:
    Metric type: IGP, Accumulated Metric 40
      SID[0]: Node, Label 16001, Address 1.1.1.1
      SID[1]: Node, Label 16004, Address 1.1.1.4
  Computed path: (Local PCE)
    Computed Time: Thu Jul 11 03:49:48 UTC 2019 (00:09:08 ago)
    Metric type: IGP, Accumulated Metric 40
      SID[0]: Node, Label 16001, Address 1.1.1.1
      SID[1]: Node, Label 16004, Address 1.1.1.4
  Recorded path:
    None
  Disjoint Group Information:
    Type Link-Disjoint, Group 775
```

この使用例の目標に基づいて、SR-PCE は、サイト 1 とサイト 2 の間の ELINE サービスのペアに関連付けられた SR ポリシーのリンクディスジョイントパスを計算します。具体的には、サイト 2 からサイト 1 へのディスジョイント LSP はアソシエーショングループ ID 776 によって識別されます。出力には、このグループ ID に関連付けられた LSP の概要情報が含まれています。

- ノード C（1.1.1.2）：LSP シンボリック名 = bgp_c_10000_ep_1.1.1.5_discr_100
- ノード D（1.1.1.4）：LSP シンボリック名 = bgp_c_10000_ep_1.1.1.6_discr_100

この場合、SR-PCE は目的のディスジョイントネスレベルを達成できています。したがって、ステータスは「Satisfied」として表示されています。

```
RP/0/0/CPU0:SR-PCE# show pce association group-id 776
Thu Jul 11 03:52:24.370 UTC

PCE's association database:
----------------------
Association: Type Link-Disjoint, Group 776, Not Strict
 Associated LSPs:
  LSP[0]:
   PCC 1.1.1.4, tunnel name bgp_c_10000_ep_1.1.1.6_discr_100,  PLSP ID 16, tunnel ID 14,
 LSP ID 1, Configured on PCC
  LSP[1]:
   PCC 1.1.1.2, tunnel name bgp_c_10000_ep_1.1.1.5_discr_100,  PLSP ID 6, tunnel ID 21,
 LSP ID 3, Configured on PCC
 Status: Satisfied
```

PCE の LSP データベースに存在する LSP の詳細情報を表示するには、**show pce lsp** コマンドを使用します。この出力には、ノード A（1.1.1.5）への EVPN VPWS EVI 100 のトラフィックを伝送するために使用される、ノード C（1.1.1.2）の LSP の詳細が表示されています。

```
RP/0/0/CPU0:SR-PCE# show pce lsp pcc ipv4 1.1.1.2 name bgp_c_10000_ep_1.1.1.5_discr_100
Thu Jul 11 03:55:21.706 UTC

PCE's tunnel database:
----------------------
PCC 1.1.1.2:

Tunnel Name: bgp_c_10000_ep_1.1.1.5_discr_100
Color: 10000
Interface Name: srte_c_10000_ep_1.1.1.5
 LSPs:
  LSP[0]:
   source 1.1.1.2, destination 1.1.1.5, tunnel ID 21, LSP ID 3
   State: Admin up, Operation up
   Setup type: Segment Routing
   Binding SID: 80052
   Maximum SID Depth: 10
   Absolute Metric Margin: 0
   Relative Metric Margin: 0%
   Preference: 100
   Bandwidth: signaled 0 kbps, applied 0 kbps
   PCEP information:
     PLSP-ID 0x6, flags: D:1 S:0 R:0 A:1 O:1 C:0
   LSP Role: Exclude LSP
   State-sync PCE: None
   PCC: 1.1.1.2
   LSP is subdelegated to: None
   Reported path:
     Metric type: IGP, Accumulated Metric 40
      SID[0]: Node, Label 16007, Address 1.1.1.7
      SID[1]: Node, Label 16008, Address 1.1.1.8
      SID[2]: Adj, Label 80005, Address: local 11.5.8.8 remote 11.5.8.5
   Computed path: (Local PCE)
     Computed Time: Thu Jul 11 03:50:03 UTC 2019 (00:05:18 ago)
     Metric type: IGP, Accumulated Metric 40
      SID[0]: Node, Label 16007, Address 1.1.1.7
      SID[1]: Node, Label 16008, Address 1.1.1.8
      SID[2]: Adj, Label 80005, Address: local 11.5.8.8 remote 11.5.8.5
   Recorded path:
     None
   Disjoint Group Information:
     Type Link-Disjoint, Group 776
```

この出力には、ノードB（1.1.1.6）へのEVPN VPWS EVI 101のトラフィックを伝送するために使用される、ノードD（1.1.1.4）のLSPの詳細が表示されています。

```
RP/0/0/CPU0:SR-PCE# show pce lsp pcc ipv4 1.1.1.4 name bgp_c_10000_ep_1.1.1.6_discr_100
Thu Jul 11 03:55:23.296 UTC

PCE's tunnel database:
----------------------
PCC 1.1.1.4:

Tunnel Name: bgp_c_10000_ep_1.1.1.6_discr_100
Color: 10000
Interface Name: srte_c_10000_ep_1.1.1.6
 LSPs:
  LSP[0]:
   source 1.1.1.4, destination 1.1.1.6, tunnel ID 14, LSP ID 1
   State: Admin up, Operation up
   Setup type: Segment Routing
   Binding SID: 80047
   Maximum SID Depth: 10
   Absolute Metric Margin: 0
```

```
  Relative Metric Margin: 0%
  Preference: 100
  Bandwidth: signaled 0 kbps, applied 0 kbps
  PCEP information:
    PLSP-ID 0x10, flags: D:1 S:0 R:0 A:1 O:1 C:0
  LSP Role: Disjoint LSP
  State-sync PCE: None
  PCC: 1.1.1.4
  LSP is subdelegated to: None
  Reported path:
    Metric type: IGP, Accumulated Metric 40
     SID[0]: Node, Label 16001, Address 1.1.1.1
     SID[1]: Node, Label 16006, Address 1.1.1.6
  Computed path: (Local PCE)
    Computed Time: Thu Jul 11 03:50:03 UTC 2019 (00:05:20 ago)
    Metric type: IGP, Accumulated Metric 40
     SID[0]: Node, Label 16001, Address 1.1.1.1
     SID[1]: Node, Label 16006, Address 1.1.1.6
  Recorded path:
    None
  Disjoint Group Information:
    Type Link-Disjoint, Group 776
```

確認：サイト 1 のノード A

このセクションでは、ノード A での確認手順を示します。

EVPN-VPWS EVI 100（rd 1.1.1.5:100）の BGP プレフィックス情報を表示するには、**show bgp l2vpn evpn** コマンドを使用します。出力には、ノードC（1.1.1.2）を発信元とするカラー 11000 の EVPN ルートタイプ 1 ルートが含まれています。

```
RP/0/RSP0/CPU0:Node-A# show bgp l2vpn evpn rd 1.1.1.5:100
Wed Jul 10 18:57:57.704 PST
BGP router identifier 1.1.1.5, local AS number 65000
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 360
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1.1.1.5:100 (default for vrf VPWS:100)
*> [1][0000.0000.0000.0000.0000][11]/120
                      0.0.0.0                                0 i
*>i[1][0000.0000.0000.0000.0000][21]/120
                      1.1.1.2 C:11000              100       0 i
```

次の出力には、着信 EVPN RT1 の詳細が表示されています。BGP 拡張カラーコミュニティ 11000 が存在すること、およびカラー 11000 と BSID 値 80044 を使用する SR ポリシーにプレフィックスが関連付けられていることに注目してください。

```
RP/0/RSP0/CPU0:Node-A# show bgp l2vpn evpn rd 1.1.1.5:100
[1][0000.0000.0000.0000.0000][21]/120
Wed Jul 10 18:57:58.107 PST
BGP routing table entry for [1][0000.0000.0000.0000.0000][21]/120, Route Distinguisher:
```

```
 1.1.1.5:100
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                360         360
Last Modified: Jul 10 18:36:18.369 for 00:21:40
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local
    1.1.1.2 C:11000 (bsid:80044) (metric 40) from 1.1.1.253 (1.1.1.2)
      Received Label 80056
      Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate,
imported, rib-install
      Received Path ID 0, Local Path ID 1, version 358
      Extended community: Color:11000 RT:65000:100
      Originator: 1.1.1.2, Cluster list: 1.1.1.253
      SR policy color 11000, up, registered, bsid 80044, if-handle 0x00001b20

     Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 1.1.1.2:100
```

EVPN-VPWS EVI 100 サービスに関連付けられている状態を表示するには、**show l2vpn xconnect** コマンドを使用します。

```
RP/0/RSP0/CPU0:Node-A# show l2vpn xconnect group evpn_vpws_group
Wed Jul 10 18:58:02.333 PST
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect                    Segment 1                       Segment 2
Group      Name       ST    Description            ST       Description             ST
------------------------   ------------------------------   ------------------------------
evpn_vpws_group
           evpn_vpws_100
                      UP    Gi0/0/0/3.2500         UP       EVPN 100,21,1.1.1.2     UP
------------------------------------------------------------------------------------------
```

次の出力はサービスの詳細を示しています。カラー 11000 とエンドポイント 1.1.1.2（ノード C）を使用するオンデマンド SR ポリシーにサービスが関連付けられていることに注目してください。

```
RP/0/RSP0/CPU0:Node-A# show l2vpn xconnect group evpn_vpws_group xc-name evpn_vpws_100
detail
Wed Jul 10 18:58:02.755 PST

Group evpn_vpws_group, XC evpn_vpws_100, state is up; Interworking none
  AC: GigabitEthernet0/0/0/3.2500, state is up
    Type VLAN; Num Ranges: 1
    Rewrite Tags: []
    VLAN ranges: [2500, 2500]
    MTU 1500; XC ID 0x120000c; interworking none
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
      drops: illegal VLAN 0, illegal length 0
  EVPN: neighbor 1.1.1.2, PW ID: evi 100, ac-id 21, state is up ( established )
    XC ID 0xa0000007
    Encapsulation MPLS
    Source address 1.1.1.5
```

```
  Encap type Ethernet, control word enabled
  Sequencing not set
  Preferred path Active : SR TE srte_c_11000_ep_1.1.1.2, On-Demand, fallback enabled
  Tunnel : Up
  Load Balance Hashing: src-dst-mac

    EVPN         Local                          Remote
    ------------ ------------------------------ ------------------------------
    Label        80040                          80056
    MTU          1500                           1500
    Control word enabled                        enabled
    AC ID        11                             21
    EVPN type    Ethernet                       Ethernet

    ------------ ------------------------------ ------------------------------
  Create time: 10/07/2019 18:31:30 (1d17h ago)
  Last time status changed: 10/07/2019 19:42:00 (1d16h ago)
  Last time PW went down: 10/07/2019 19:40:55 (1d16h ago)
  Statistics:
    packets: received 0, sent 0
    bytes: received 0, sent 0
```

SR ポリシーの要約情報を表示するには、**tabular** オプションを指定して **show segment-routing traffic-eng policy** コマンドを使用します。

次の出力は、ノードC（1.1.1.2）からアドバタイズされたカラー11000のEVPN RT1プレフィックスによってトリガーされた、BSID 80044を使用するオンデマンドSRポリシーの詳細を示しています。

```
RP/0/RSP0/CPU0:Node-A# show segment-routing traffic-eng policy color 11000 tabular
Wed Jul 10 18:58:00.732 PST

 Color             Endpoint  Admin   Oper              Binding
                             State   State                 SID
------ -------------------- ------ ------ --------------------
 11000              1.1.1.2     up     up                80044
```

次の出力は、オンデマンドSRポリシーの詳細を示しています。SRポリシーのアクティブな候補パス（優先順位100）がSR-PCE（1.1.1.207）によって計算されていることに注目してください。

この使用例の目標に基づいて、SR-PCEは、サイト1とサイト2の間のELINEサービスのペアに関連付けられたSRポリシーのリンクディスジョイントパスを計算します。具体的には、サイト1からサイト2への、ノードAのLSP（srte_c_11000_ep_1.1.1.2）は、ノードBのLSP（srte_c_11000_ep_1.1.1.4）からリンクディスジョイントされます。

```
RP/0/RSP0/CPU0:Node-A# show segment-routing traffic-eng policy color 11000
Wed Jul 10 19:15:47.217 PST

SR-TE policy database
---------------------

Color: 11000, End-point: 1.1.1.2
  Name: srte_c_11000_ep_1.1.1.2
  Status:
    Admin: up  Operational: up for 00:39:31 (since Jul 10 18:36:00.471)
  Candidate-paths:
    Preference: 200 (BGP ODN) (shutdown)
      Requested BSID: dynamic
```

```
      PCC info:
        Symbolic name: bgp_c_11000_ep_1.1.1.2_discr_200
        PLSP-ID: 19
      Dynamic (invalid)
    Preference: 100 (BGP ODN) (active)
      Requested BSID: dynamic
      PCC info:
        Symbolic name: bgp_c_11000_ep_1.1.1.2_discr_100
        PLSP-ID: 18
      Dynamic (pce 1.1.1.207) (valid)
        Metric Type: IGP,   Path Accumulated Metric: 40
          80003 [Adjacency-SID, 11.5.8.5 - 11.5.8.8]
          16007 [Prefix-SID, 1.1.1.7]
          16002 [Prefix-SID, 1.1.1.2]
  Attributes:
    Binding SID: 80044
    Forward Class: 0
    Steering BGP disabled: no
    IPv6 caps enable: yes
```

確認：サイト 1 のノード B

このセクションでは、ノード B での確認手順を示します。

EVPN-VPWS EVI 101（rd 1.1.1.6:101）の BGP プレフィックス情報を表示するには、**show bgp l2vpn evpn** コマンドを使用します。出力には、ノード D（1.1.1.4）を発信元とするカラー 11000 の EVPN ルートタイプ 1 ルートが含まれています。

```
RP/0/RSP0/CPU0:Node-B# show bgp l2vpn evpn rd 1.1.1.6:101
Wed Jul 10 19:08:54.964 PST
BGP router identifier 1.1.1.6, local AS number 65000
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 322
BGP NSR Initial initsync version 7 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1.1.1.6:101 (default for vrf VPWS:101)
*> [1][0000.0000.0000.0000.0000][12]/120
                      0.0.0.0                                0 i
*>i[1][0000.0000.0000.0000.0000][22]/120
                       1.1.1.4 C:11000              100      0 i

Processed 2 prefixes, 2 paths
```

次の出力には、着信 EVPN RT1 の詳細が表示されています。BGP 拡張カラーコミュニティ 11000 が存在すること、およびカラー 11000 と BSID 値 80061 を使用する SR ポリシーにプレフィックスが関連付けられていることに注目してください。

```
RP/0/RSP0/CPU0:Node-B# show bgp l2vpn evpn rd 1.1.1.6:101
[1][0000.0000.0000.0000.0000][22]/120
Wed Jul 10 19:08:55.039 PST
BGP routing table entry for [1][0000.0000.0000.0000.0000][22]/120, Route Distinguisher:
 1.1.1.6:101
```

```
Versions:
  Process            bRIB/RIB  SendTblVer
  Speaker                 322         322
Last Modified: Jul 10 18:42:10.408 for 00:26:44
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local
    1.1.1.4 C:11000 (bsid:80061) (metric 40) from 1.1.1.253 (1.1.1.4)
      Received Label 80045
      Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate,
imported, rib-install
      Received Path ID 0, Local Path ID 1, version 319
      Extended community: Color:11000 RT:65000:101
      Originator: 1.1.1.4, Cluster list: 1.1.1.253
      SR policy color 11000, up, registered, bsid 80061, if-handle 0x00000560

     Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 1.1.1.4:101
```

EVPN-VPWS EVI 101 サービスに関連付けられている状態を表示するには、**show l2vpn xconnect** コマンドを使用します。

```
RP/0/RSP0/CPU0:Node-B# show l2vpn xconnect group evpn_vpws_group
Wed Jul 10 19:08:56.388 PST
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect                    Segment 1                         Segment 2
Group      Name       ST    Description             ST       Description             ST
------------------------   -----------------------------   -------------------------------
evpn_vpws_group
           evpn_vpws_101
                      UP    Te0/3/0/0/8.2500        UP       EVPN 101,22,1.1.1.4     UP
------------------------------------------------------------------------------------------
```

次の出力はサービスの詳細を示しています。カラー 11000 とエンドポイント 1.1.1.4（ノード D）を使用するオンデマンド SR ポリシーにサービスが関連付けられていることに注意してください。

```
RP/0/RSP0/CPU0:Node-B# show l2vpn xconnect group evpn_vpws_group xc-name evpn_vpws_101
Wed Jul 10 19:08:56.511 PST

Group evpn_vpws_group, XC evpn_vpws_101, state is up; Interworking none
  AC: TenGigE0/3/0/0/8.2500, state is up
    Type VLAN; Num Ranges: 1
    Rewrite Tags: []
    VLAN ranges: [2500, 2500]
    MTU 1500; XC ID 0x2a0000e; interworking none
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
      drops: illegal VLAN 0, illegal length 0
  EVPN: neighbor 1.1.1.4, PW ID: evi 101, ac-id 22, state is up ( established )
    XC ID 0xa0000009
    Encapsulation MPLS
    Source address 1.1.1.6
    Encap type Ethernet, control word enabled
    Sequencing not set
```

```
  Preferred path Active : SR TE srte_c_11000_ep_1.1.1.4, On-Demand, fallback enabled
  Tunnel : Up
  Load Balance Hashing: src-dst-mac

    EVPN         Local                          Remote
    ------------ ------------------------------ ------------------------------
    Label        80060                          80045
    MTU          1500                           1500
    Control word enabled                        enabled
    AC ID        12                             22
    EVPN type    Ethernet                       Ethernet

    ------------ ------------------------------ ------------------------------
  Create time: 10/07/2019 18:32:49 (00:36:06 ago)
  Last time status changed: 10/07/2019 18:42:07 (00:26:49 ago)
  Statistics:
    packets: received 0, sent 0
    bytes: received 0, sent 0
```

SR ポリシーの要約情報を表示するには、**tabular** オプションを指定して **show segment-routing traffic-eng policy** コマンドを使用します。

次の出力は、ノードD（1.1.1.4）からアドバタイズされたカラー11000のEVPN RT1プレフィックスによってトリガーされた、BSID 80061を使用するオンデマンドSRポリシーの詳細を示しています。

```
RP/0/RSP0/CPU0:Node-B# show segment-routing traffic-eng policy color 11000 tabular
Wed Jul 10 19:08:56.146 PST

 Color             Endpoint  Admin   Oper              Binding
                             State   State                 SID
------ -------------------- ------ ------ --------------------
 11000              1.1.1.4     up     up                80061
```

次の出力は、オンデマンドSRポリシーの詳細を示しています。SRポリシーのアクティブな候補パス（優先順位100）がSR-PCE（1.1.1.207）によって計算されていることに注目してください。

この使用例の目標に基づいて、SR-PCEは、サイト1とサイト2の間のELINEサービスのペアに関連付けられたSRポリシーのリンクディスジョイントパスを計算します。具体的には、サイト1からサイト2への、ノードBのLSP（srte_c_11000_ep_1.1.1.4）は、ノードAのLSP（srte_c_11000_ep_1.1.1.2）からリンクディスジョイントされます。

```
RP/0/RSP0/CPU0:Node-B# show segment-routing traffic-eng policy color 11000
Wed Jul 10 19:08:56.207 PST

SR-TE policy database
---------------------

Color: 11000, End-point: 1.1.1.4
  Name: srte_c_11000_ep_1.1.1.4
  Status:
    Admin: up  Operational: up for 00:26:47 (since Jul 10 18:40:05.868)
  Candidate-paths:
    Preference: 200 (BGP ODN) (shutdown)
      Requested BSID: dynamic
      PCC info:
        Symbolic name: bgp_c_11000_ep_1.1.1.4_discr_200
        PLSP-ID: 19
```

```
    Dynamic (invalid)
  Preference: 100 (BGP ODN) (active)
    Requested BSID: dynamic
    PCC info:
      Symbolic name: bgp_c_11000_ep_1.1.1.4_discr_100
      PLSP-ID: 18
    Dynamic (pce 1.1.1.207) (valid)
      Metric Type: IGP,   Path Accumulated Metric: 40
        16001 [Prefix-SID, 1.1.1.1]
        16004 [Prefix-SID, 1.1.1.4]
Attributes:
  Binding SID: 80061
  Forward Class: 0
  Steering BGP disabled: no
  IPv6 caps enable: yes
```

確認：サイト 2 のノード C

このセクションでは、ノード C での確認手順を示します。

EVPN-VPWS EVI 100（rd 1.1.1.2:100）の BGP プレフィックス情報を表示するには、**show bgp l2vpn evpn** コマンドを使用します。出力には、ノード A（1.1.1.5）を発信元とするカラー 10000 の EVPN ルートタイプ 1 ルートが含まれています。

```
RP/0/RSP0/CPU0:Node-C# show bgp l2vpn evpn rd 1.1.1.2:100
BGP router identifier 1.1.1.2, local AS number 65000
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 21
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1.1.1.2:100 (default for vrf VPWS:100)
*>i[1][0000.0000.0000.0000.0000][11]/120
                      1.1.1.5 C:10000              100      0 i
*> [1][0000.0000.0000.0000.0000][21]/120
                      0.0.0.0                                0 i
```

次の出力には、着信 EVPN RT1 の詳細が表示されています。BGP 拡張カラーコミュニティ 10000 が存在すること、およびカラー 10000 と BSID 値 80058 を使用する SR ポリシーにプレフィックスが関連付けられていることに注目してください。

```
RP/0/RSP0/CPU0:Node-C# show bgp l2vpn evpn rd 1.1.1.2:100
[1][0000.0000.0000.0000.0000][11]/120
BGP routing table entry for [1][0000.0000.0000.0000.0000][11]/120, Route Distinguisher:
 1.1.1.2:100
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker                 20          20
Last Modified: Jul 10 18:36:20.503 for 00:45:21
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
```

```
  Local
    1.1.1.5 C:10000 (bsid:80058) (metric 40) from 1.1.1.253 (1.1.1.5)
      Received Label 80040
      Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate,
imported, rib-install
      Received Path ID 0, Local Path ID 1, version 18
      Extended community: Color:10000 RT:65000:100
      Originator: 1.1.1.5, Cluster list: 1.1.1.253
      SR policy color 10000, up, registered, bsid 80058, if-handle 0x000006a0

     Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 1.1.1.5:100
```

EVPN-VPWS EVI 100 サービスに関連付けられている状態を表示するには、**show l2vpn xconnect** コマンドを使用します。

```
RP/0/RSP0/CPU0:Node-C# show l2vpn xconnect group evpn_vpws_group
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect                    Segment 1                       Segment 2
Group      Name       ST    Description             ST      Description             ST
------------------------   -----------------------------   -----------------------------
evpn_vpws_group
           evpn_vpws_100
                      UP    Gi0/0/0/3.2500          UP      EVPN 100,11,1.1.1.5     UP
------------------------------------------------------------------------------------------
```

次の出力はサービスの詳細を示しています。カラー 10000 とエンドポイント 1.1.1.5（ノード A）を使用するオンデマンド SR ポリシーにサービスが関連付けられていることに注目してください。

```
RP/0/RSP0/CPU0:Node-C# show l2vpn xconnect group evpn_vpws_group xc-name evpn_vpws_100

Group evpn_vpws_group, XC evpn_vpws_100, state is up; Interworking none
  AC: GigabitEthernet0/0/0/3.2500, state is up
    Type VLAN; Num Ranges: 1
    Rewrite Tags: []
    VLAN ranges: [2500, 2500]
    MTU 1500; XC ID 0x1200008; interworking none
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
      drops: illegal VLAN 0, illegal length 0
  EVPN: neighbor 1.1.1.5, PW ID: evi 100, ac-id 11, state is up ( established )
    XC ID 0xa0000003
    Encapsulation MPLS
    Source address 1.1.1.2
    Encap type Ethernet, control word enabled
    Sequencing not set
    Preferred path Active : SR TE srte_c_10000_ep_1.1.1.5, On-Demand, fallback enabled
    Tunnel : Up
    Load Balance Hashing: src-dst-mac

      EVPN         Local                          Remote
      ------------ ------------------------------ ------------------------------
      Label        80056                          80040
      MTU          1500                           1500
      Control word enabled                        enabled
      AC ID        21                             11
```

```
  EVPN type    Ethernet                        Ethernet

  ------------ ------------------------------ ------------------------------
Create time: 10/07/2019 18:36:16 (1d19h ago)
Last time status changed: 10/07/2019 19:41:59 (1d18h ago)
Last time PW went down: 10/07/2019 19:40:54 (1d18h ago)
Statistics:
  packets: received 0, sent 0
  bytes: received 0, sent 0
```

SR ポリシーの要約情報を表示するには、**tabular** オプションを指定して **show segment-routing traffic-eng policy** コマンドを使用します。

次の出力は、ノードA（1.1.1.5）からアドバタイズされたカラー10000のEVPN RT1プレフィックスによってトリガーされた、BSID 80058を使用するオンデマンドSRポリシーの詳細を示しています。

```
RP/0/RSP0/CPU0:Node-C# show segment-routing traffic-eng policy color 10000 tabular

 Color             Endpoint  Admin   Oper              Binding
                             State   State                 SID
------ -------------------- ------ ------ --------------------
10000              1.1.1.5     up     up                80058
```

次の出力は、オンデマンドSRポリシーの詳細を示しています。SRポリシーのアクティブな候補パス（優先順位100）がSR-PCE（1.1.1.207）によって計算されていることに注目してください。

この使用例の目標に基づいて、SR-PCEは、サイト1とサイト2の間のELINEサービスのペアに関連付けられたSRポリシーのリンクディスジョイントパスを計算します。具体的には、サイト2からサイト1への、ノードCのLSP（srte_c_10000_ep_1.1.1.5）は、ノードDのLSP（srte_c_10000_ep_1.1.1.6）からリンクディスジョイントされます。

```
RP/0/RSP0/CPU0:Node-C# show segment-routing traffic-eng policy color 10000

SR-TE policy database
---------------------

Color: 10000, End-point: 1.1.1.5
  Name: srte_c_10000_ep_1.1.1.5
  Status:
    Admin: up  Operational: up for 00:12:35 (since Jul 10 19:49:21.890)
  Candidate-paths:
    Preference: 200 (BGP ODN) (shutdown)
      Requested BSID: dynamic
      PCC info:
        Symbolic name: bgp_c_10000_ep_1.1.1.5_discr_200
        PLSP-ID: 7
      Dynamic (invalid)
    Preference: 100 (BGP ODN) (active)
      Requested BSID: dynamic
      PCC info:
        Symbolic name: bgp_c_10000_ep_1.1.1.5_discr_100
        PLSP-ID: 6
      Dynamic (pce 1.1.1.207) (valid)
        Metric Type: IGP,   Path Accumulated Metric: 40
          16007 [Prefix-SID, 1.1.1.7]
          16008 [Prefix-SID, 1.1.1.8]
          80005 [Adjacency-SID, 11.5.8.8 - 11.5.8.5]
```

```
  Attributes:
    Binding SID: 80058
    Forward Class: 0
    Steering BGP disabled: no
    IPv6 caps enable: yes
```

確認：サイト 2 のノード D

このセクションでは、ノード D での確認手順を示します。

EVPN-VPWS EVI 101（rd 1.1.1.4:101）の BGP プレフィックス情報を表示するには、**show bgp l2vpn evpn** コマンドを使用します。出力には、ノード B（1.1.1.6）を発信元とするカラー 10000 の EVPN ルートタイプ 1 ルートが含まれています。

```
RP/0/RSP0/CPU0:Node-D# show bgp l2vpn evpn rd 1.1.1.4:101
BGP router identifier 1.1.1.4, local AS number 65000
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 570
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1.1.1.4:101 (default for vrf VPWS:101)
*>i[1][0000.0000.0000.0000.0000][12]/120
                      1.1.1.6 C:10000              100      0 i
*> [1][0000.0000.0000.0000.0000][22]/120
                      0.0.0.0                             0 i

Processed 2 prefixes, 2 paths
```

次の出力には、着信 EVPN RT1 の詳細が表示されています。BGP 拡張カラーコミュニティ 10000 が存在すること、およびカラー 10000 と BSID 値 80047 を使用する SR ポリシーにプレフィックスが関連付けられていることに注目してください。

```
RP/0/RSP0/CPU0:Node-D# show bgp l2vpn evpn rd 1.1.1.4:101
[1][0000.0000.0000.0000.0000][12]/120
BGP routing table entry for [1][0000.0000.0000.0000.0000][12]/120, Route Distinguisher:
 1.1.1.4:101
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker               569         569
Last Modified: Jul 10 18:42:12.455 for 00:45:38
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local
    1.1.1.6 C:10000 (bsid:80047) (metric 40) from 1.1.1.253 (1.1.1.6)
      Received Label 80060
      Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate,
imported, rib-install
      Received Path ID 0, Local Path ID 1, version 568
      Extended community: Color:10000 RT:65000:101
      Originator: 1.1.1.6, Cluster list: 1.1.1.253
```

```
SR policy color 10000, up, registered, bsid 80047, if-handle 0x00001720

Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 1.1.1.6:101
```

EVPN-VPWS EVI 101 サービスに関連付けられている状態を表示するには、**show l2vpn xconnect** コマンドを使用します。

```
RP/0/RSP0/CPU0:Node-D# show l2vpn xconnect group evpn_vpws_group
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect                   Segment 1                       Segment 2
Group      Name       ST   Description             ST       Description             ST
------------------------   -----------------------------   -----------------------------
evpn_vpws_group
           evpn_vpws_101
                      UP   Gi0/0/0/1.2500          UP       EVPN 101,12,1.1.1.6     UP
------------------------------------------------------------------------------------------
```

次の出力はサービスの詳細を示しています。カラー 10000 とエンドポイント 1.1.1.6（ノード B）を使用するオンデマンド SR ポリシーにサービスが関連付けられていることに注目してください。

```
RP/0/RSP0/CPU0:Node-D# show l2vpn xconnect group evpn_vpws_group xc-name evpn_vpws_101

Group evpn_vpws_group, XC evpn_vpws_101, state is up; Interworking none
  AC: GigabitEthernet0/0/0/1.2500, state is up
    Type VLAN; Num Ranges: 1
    Rewrite Tags: []
    VLAN ranges: [2500, 2500]
    MTU 1500; XC ID 0x120000c; interworking none
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
      drops: illegal VLAN 0, illegal length 0
  EVPN: neighbor 1.1.1.6, PW ID: evi 101, ac-id 12, state is up ( established )
    XC ID 0xa000000d
    Encapsulation MPLS
    Source address 1.1.1.4
    Encap type Ethernet, control word enabled
    Sequencing not set
    Preferred path Active : SR TE srte_c_10000_ep_1.1.1.6, On-Demand, fallback enabled
    Tunnel : Up
    Load Balance Hashing: src-dst-mac

      EVPN         Local                          Remote
      ------------ ------------------------------ ------------------------------
      Label        80045                          80060
      MTU          1500                           1500
      Control word enabled                        enabled
      AC ID        22                             12
      EVPN type    Ethernet                       Ethernet

      ------------ ------------------------------ ------------------------------
    Create time: 10/07/2019 18:42:07 (00:45:49 ago)
    Last time status changed: 10/07/2019 18:42:09 (00:45:47 ago)
    Statistics:
      packets: received 0, sent 0
```

```
      bytes: received 0, sent 0
```

SR ポリシーの要約情報を表示するには、**tabular** オプションを指定して **show segment-routing traffic-eng policy** コマンドを使用します。

次の出力は、ノードB（1.1.1.6）からアドバタイズされたカラー10000のEVPN RT1プレフィックスによってトリガーされた、BSID 80047を使用するオンデマンドSRポリシーの詳細を示しています。

```
RP/0/RSP0/CPU0:Node-D# show segment-routing traffic-eng policy color 10000 tabular

 Color             Endpoint  Admin   Oper              Binding
                             State  State                 SID
------ --------------------- ------ ------ --------------------
10000              1.1.1.6     up     up                 80047
```

次の出力は、オンデマンドSRポリシーの詳細を示しています。SRポリシーのアクティブな候補パス（優先順位100）がSR-PCE（1.1.1.207）によって計算されていることに注目してください。

この使用例の目標に基づいて、SR-PCEは、サイト1とサイト2の間のELINEサービスのペアに関連付けられたSRポリシーのリンクディスジョイントパスを計算します。具体的には、サイト2からサイト1への、ノードDのLSP（srte_c_10000_ep_1.1.1.6）は、ノードCのLSP（srte_c_10000_ep_1.1.1.5）からリンクディスジョイントされます。

```
RP/0/RSP0/CPU0:Node-D# show segment-routing traffic-eng policy color 10000

SR-TE policy database
---------------------

Color: 10000, End-point: 1.1.1.6
  Name: srte_c_10000_ep_1.1.1.6
  Status:
    Admin: up  Operational: up for 01:23:04 (since Jul 10 18:42:07.350)
  Candidate-paths:
    Preference: 200 (BGP ODN) (shutdown)
      Requested BSID: dynamic
      PCC info:
        Symbolic name: bgp_c_10000_ep_1.1.1.6_discr_200
        PLSP-ID: 17
      Dynamic (invalid)
    Preference: 100 (BGP ODN) (active)
      Requested BSID: dynamic
      PCC info:
        Symbolic name: bgp_c_10000_ep_1.1.1.6_discr_100
        PLSP-ID: 16
      Dynamic (pce 1.1.1.207) (valid)
        Metric Type: IGP,   Path Accumulated Metric: 40
          16001 [Prefix-SID, 1.1.1.1]
          16006 [Prefix-SID, 1.1.1.6]
  Attributes:
    Binding SID: 80047
    Forward Class: 0
    Steering BGP disabled: no
    IPv6 caps enable: yes
```

手動でプロビジョニングされた SR ポリシー

手動でプロビジョニングされた SR ポリシーはヘッドエンドルータで設定されます。これらのポリシーは、ダイナミックパスまたは明示パスを使用できます。ダイナミックパスまたは明示パスを使用した SR ポリシーの手動プロビジョニングに関する詳細については、SR-TE ポリシーのパスタイプ （84 ページ）の項を参照してください。

PCE で開始された SR ポリシー

SR-TE ポリシーは、リンクの輻輳を軽減したり、ネットワーク タッチ ポイントの数を最小限に抑えたりするようにパス計算要素（PCE）で設定することができます。

PCE は、トラフィック需要やリンク使用率などのネットワーク情報を収集します。PCE はリンクが輻輳していると判断すると、輻輳の原因となっている 1 つ以上のフローを特定します。PCE は適切なパスを見つけ、ネットワークの別の部分に輻輳を移動せずに、そのフローを転送するように SR-TE ポリシーを展開します。リンクの輻輳がない場合、ポリシーは削除されます。

ネットワーク タッチ ポイントの数を最小限に抑えるために、ネットワーク サービス オーケストレータ（NSO）などのアプリケーションは PCE に SR-TE ポリシーを作成するように要求できます。PCE は、PCC-PCE 通信プロトコル（PCEP）を使用して SR-TE ポリシーを展開します。

詳細については、トラフィック管理の PCE 開始 SR ポリシー （122 ページ）を参照してください。

SR-TE ポリシーのパスタイプ

ダイナミックパスは、最適化の目的と一連の制約に基づいています。ヘッドエンドはソリューションを計算し、結果として SID リストまたは SID リストのセットを生成します。トポロジが変更されると、新しいパスが計算されます。ヘッドエンドにトポロジーに関する十分な情報がない場合、ヘッドエンドは計算をセグメントルーティングパス計算要素（SR-PCE）に委任できます。SR-PCE の設定については、セグメント ルーティング パス計算要素の設定 （117 ページ）の章を参照してください。

明示パスは、指定された SID リストまたは一連の SID リストです。

SR-TE ポリシーは、RIB/FIB 内で単一の（選択された）パスを開始します。これが優先される有効な候補パスです。

候補パスには次の特性があります。

- 優先順位があります：2 つのポリシーに同じ {color, endpoint} があり、優先順位が異なる場合は、優先順位が最も高いポリシーが選択されます。
- 単一のバインド SID（BSID）に関連付けられます：同じ BSID を持つ異なる SR ポリシーがある場合、BSID 競合が発生します。この場合、最初にインストールされたポリシーが BSID を取得し、選択されます。

- 使用可能な場合に有効になります。

パスが有効で、その設定がそのポリシーのすべての候補パスの中でベストの場合にそのパスが選択されます。

（注） 送信元のプロトコルは、パス選択ロジックには関係ありません。

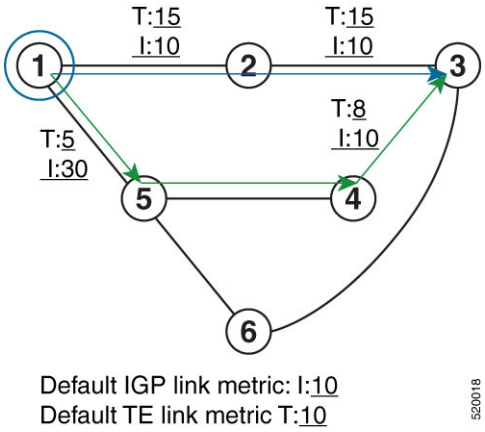
ダイナミックパス

最適化の目的

最適化の目的を使用すると、ヘッドエンドルータは、選択したメトリックタイプに従って最短のダイナミックパスを表す SID リストを計算することができます。

- IGP メトリック：『*Routing Configuration Guide for Series Routers*』の「Implementing IS-IS」および「Implementing OSPF」 の章を参照してください。
- TE メトリック：TE メトリックの設定については、インターフェイス TE メトリックの設定 （85 ページ）の項を参照してください。

次に、ヘッドエンドルータ 1 からエンドポイントルータ 3 へのダイナミックパスを使用して、IGP または TE メトリックを最小限にする例を示します。



- 青色のパスでは、最小 IGP メトリックを使用：最小メトリック（1 → 3、IGP）= SID リスト <16003>、累積 IGP メトリック：20
- 緑色のパスでは最小 TE メトリックを使用：最小メトリック（1 →3、TE）= SID リスト <16005, 16004, 16003>、累積 TE メトリック：23

インターフェイス TE メトリックの設定

インターフェイスの TE メトリックを設定するには、SR-TE インターフェイスサブモードで **metric** *value* コマンドを使用します。*value* の範囲は 0 ～ 2147483647 です。

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# interface type interface-path-id
Router(config-sr-te-if)# metric value
```

TE メトリックの設定：例

次の設定例は、さまざまなインターフェイスのTEメトリックを設定する方法を示しています。

```
segment-routing
 traffic-eng
  interface TenGigE0/0/0/0
   metric 100
  !
  interface TenGigE0/0/0/1
   metric 1000
  !
  interface TenGigE0/0/2/0
   metric 50
  !
 !
end
```

制約

制約では、ヘッドエンドルータは、選択したメトリックタイプに従ってダイナミックパスを計算できます。

- TE アフィニティ：アフィニティビットマップを割り当てることによって、リンクまたはインターフェイスに色または名前を適用できます。次に、SR ポリシーのパスとリンクの色との間にアフィニティ（または関係）を指定できます。SR-TEは、特定の色または色の組み合わせを持つリンクを含めるか、または除外するパスを計算します。名前付きインターフェイスリンクの管理者グループとSR-TEアフィニティマップに関する詳細については、名前付きインターフェイスリンク管理者グループと SR-TE アフィニティマップ （86 ページ）の項を参照してください。
- 分離：SR-TEは、同じ分離グループ内の別のパスから切り離されたパスを計算します。分離パスは、ネットワークリソースを共有しません。パスの分離は、ノードの同じペア間、異なるノードのペア間、またはある組み合わせ（同じヘッドエンドのみか、または同じエンドポイントのみ）のパスに必要になる場合があります。

名前付きインターフェイスリンク管理者グループと SR-TE アフィニティマップ

名前付きインターフェイスリンク管理者グループと SR-TE アフィニティマップは、SR-TE ポリシーのパスを計算するために、リンク属性とパスアフィニティを簡単かつより柔軟に設定する方法を提供します。

従来の TE スキームでは、リンクは、Open Shortest Path First（OSPF）などの Interior Gateway Protocol（IGP）を使用して、TE リンクステート パラメータが設定されてフラッディングされる attribute-flags で設定されます。

名前付きインターフェイスリンク管理者グループとSR-TEアフィニティマップを使用すると、affinity 属性と attribute-flag 属性に対して、32 ビットの 16 進数値の代わりに最大 256 のカラー

名を割り当てる（マップする）ことができます。マッピングの定義後に、CLI で対応するカラー名を使用して属性を参照することができます。さらに、*include-any*、*include-all*、および *exclude-any* 引数を使用して制約を定義できます。ここで、各ステートメントには、最大 10 個のカラーを含めることができます。

（注） 属性フラグまたは柔軟な名前ベースのポリシー制約スキームを使用してアフィニティ制約を設定できますが、両方のスキームの設定が存在する場合、新しいスキームに関する設定のみが適用されます。

名前付きインターフェイスリンク管理者グループと *SR-TE* アフィニティマップの設定

アフィニティをインターフェイスに割り当てるには、SR-TE インターフェイスサブモードで **affinity name** *NAME* コマンドを使用します。管理者グループ属性が関連付けられているインターフェイスを持つルータで、この設定を行います。

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# interface TenGigE0/0/1/2
Router(config-sr-if)# affinity
Router(config-sr-if-affinity)# name RED
```

アフィニティマップを定義するには、SR-TE サブモードで **affinity-map name** *NAME* **bit-position** *bit-position* コマンドを使用します。*bit-position* の範囲は 0 ～ 255 です。

次のルータでアフィニティマップを設定します。

- 管理者グループ属性が関連付けられているインターフェイスを持つルータ
- アフィニティ制約を含む SR ポリシーの SR-TE ヘッドエンドとして機能するルータ

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# affinity-map
Router(config-sr-te-affinity-map)# name RED bit-position 23
```

管理者グループのリンクの設定：例

次の例は、アフィニティをインターフェイスに割り当て、アフィニティマップを定義する方法を示しています。この設定は、カラー付きインターフェイスを持つすべてのルータ（SR-TE ヘッドエンドまたは中継ノード）に適用されます。

```
segment-routing
 traffic-eng
  interface TenGigE0/0/1/1
   affinity
    name CROSS
    name RED
   !
  !
  interface TenGigE0/0/1/2
   affinity
```

```
    name RED
   !
  !
  interface TenGigE0/0/2/0
   affinity
    name BLUE
   !
  !
  affinity-map
   name RED bit-position 23
   name BLUE bit-position 24
   name CROSS bit-position 25
  !
end
```

ダイナミックパスを使用した SR ポリシーの設定

ダイナミックパス、最適化の目的、およびアフィニティ制約を使用して SR-TE ポリシーを設定するには、次の設定を実行します。

1. 最適化の目的を定義します。最適化の目的 （85 ページ）の項を参照してください。
2. 制約を定義します。制約 （86 ページ）の項を参照してください。
3. ポリシーを作成します。

次の例は、SR-TE ヘッドエンドルータでの SR ポリシーの設定を示しています。このポリシーには、最適化の目的が設定されたダイナミックパスと、ヘッドエンドルータによって計算されたアフィニティ制約があります。

```
segment-routing
 traffic-eng
  policy foo
   color 100 end-point ipv4 1.1.1.2
   candidate-paths
    preference 100
     dynamic
      metric
       type te
      !
     !
     constraints
      affinity
       exclude-any
        name RED
       !
      !
     !
    !
   !
  !
```

次の例は、SR-TE ヘッドエンドルータでの SR ポリシーの設定を示しています。このポリシーには、最適化の目的が設定されたダイナミックパスと、SR-PCE によって計算されたアフィニティ制約があります。

```
segment-routing
 traffic-eng
  policy baa
```

```
color 101 end-point ipv4 1.1.1.2
candidate-paths
 preference 100
  dynamic
   pcep
   !
   metric
    type te
   !
  !
  constraints
   affinity
    exclude-any
     name BLUE
    !
   !
  !
 !
!
```

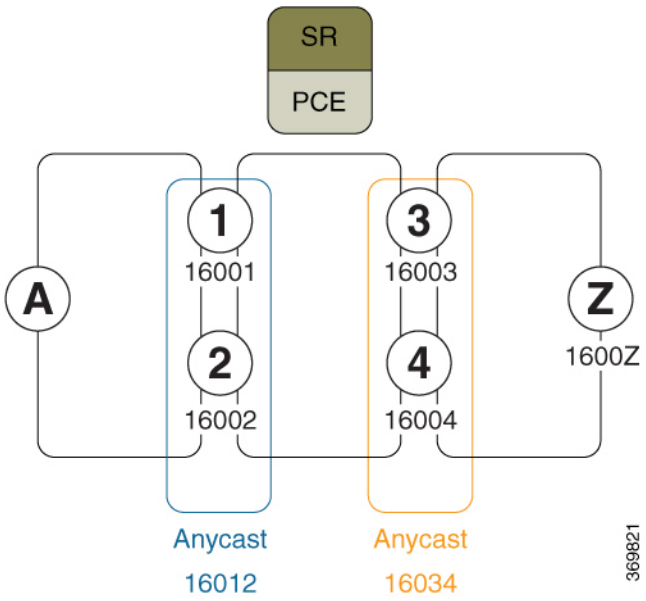
エニーキャスト SID 対応パス計算

エニーキャスト SID は、一連のノードを識別するタイプのプレフィックス SID であり、n-flag-clear を使用して設定されます。一連のノード（エニーキャストグループ）は、共有プレフィックスアドレスとプレフィックス SID をアドバタイズするように設定されます。エニーキャストルーティングにより、複数のアドバタイズノードへのトラフィックのステアリングが可能になり、ロードバランシングと冗長性が実現されます。エニーキャストアドレス宛てのパケットは、トポロジ的に最も近いノードに転送されます。

（注） エニーキャスト SID の設定については、IS-IS 対応ループバック インターフェイスでのプレフィックス SID の設定 （13 ページ）およびOSPF 対応ループバック インターフェイスでのプレフィックス SID の設定 （29 ページ）を参照してください。

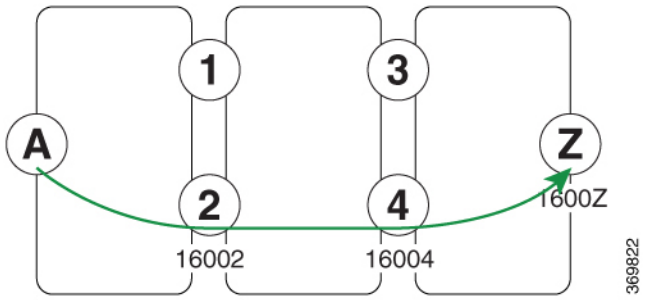
この例は、エニーキャスト SID を計算済みの SID リストに挿入する方法を示しています。

次の図は、再配布がなく、BGP 3107 も使用しない、3 つの独立した IGP ドメインを示しています。各エリア境界ルータ（ABR）1 ～ 4 は、ノード SID を使用して設定されています。ABR 1 と ABR 2 はエニーキャスト SID 16012 を共有し、ABR 3 と ABR 4 はエニーキャスト SID 16034 を共有します。



ルータ A およびルータ Z が同じ VPN 内のプロバイダーエッジ（PE）ルータである場合について考えてみましょう。ルータ A は、ルータ Z への BGP ネクストホップを持つ VPN ルートを受信します。ルータ A は、SR-ODN または SR-PCE を使用してルータ Z への SR パスを解決します。

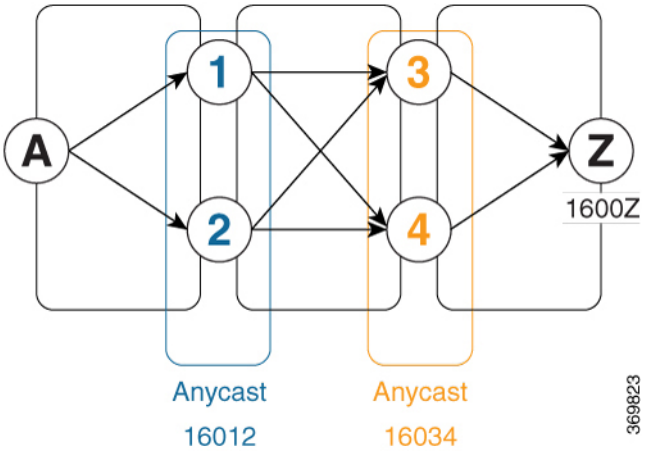
エニーキャスト SID が考慮される前に、ヘッドエンドルータまたは SR-PCE は SID リストを計算します。



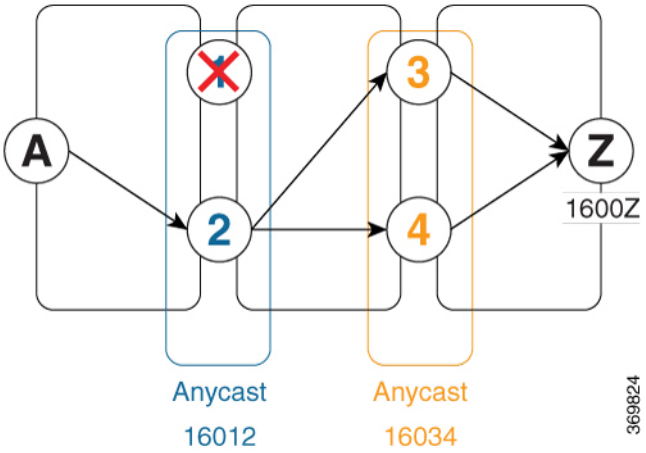
この場合、ルータ A からルータ Z への計算される最適パスは、16002 > 16004 > 1600Z となります。

パス計算プロセスでは、元の SID リストを反復処理し、ノード SID をエニーキャスト SID に置き換えます（可能な場合）。SR-TE は、エニーキャストでエンコードされた SID リストが最適パスを保持しており、どのパス制約（リンクアフィニティ、メトリック境界）にも違反していないことを確認します。SID リストの検証後、エニーキャストでエンコードされた SID リストが転送でシグナリングおよびインスタンス化されます。

エニーキャストでエンコードされた SID リストを使用すると、ルータ A からルータ Z への計算される最適パスは、16012 > 16034 > 1600Z になります。エニーキャスト SID 対応のパス計算はロードバランシングを提供します。



エニーキャスト SID 対応のパス計算は復元力も提供します。たとえば、ABR の 1 つ（この場合は ABR 1）が使用不可または到達不能になっても、ルータ A からルータ Z へのパス（16012 > 16034 > 1600Z）は引き続き有効で使用可能です。



設定例

1. ABR ノードでプレフィックス SID を設定します。
   1. ノード SID を使用して、各ノードを設定します。
   2. 共有エニーキャスト SID を使用して、ノードの各グループを設定します。

   IS-IS 対応ループバック インターフェイスでのプレフィックス SID の設定 （13 ページ）およびOSPF 対応ループバック インターフェイスでのプレフィックス SID の設定 （29 ページ）を参照してください。

2. **anycast-sid-inclusion** コマンドを使用し、パス計算にエニーキャスト SID を含めるように SR ポリシーを設定します。

   次に、ヘッドエンドルータで PCC によって開始されたパス計算にエニーキャスト SID を含めるようにローカル SR ポリシーを設定する例を示します。

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# policy FOO
Router(config-sr-te-policy)# color 10 end-point ipv4 1.1.1.10
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy-path)# preference 100
Router(config-sr-te-policy-path-pref)# dynamic
Router(config-sr-te-pp-info)# anycast-sid-inclusion
```

実行コンフィギュレーション

anycast-sid-inclusion コマンドを使用して、次のポリシータイプの計算パスにエニーキャスト SID を含めます。

- ヘッドエンドルータで PCC によって開始されたパス計算を使用するローカル SR ポリシー

```
segment-routing
  traffic-eng
    policy FOO
      color 10 end-point ipv4 1.1.1.10
      candidate-paths
        preference 100
          dynamic
            anycast-sid-inclusion
```

- SR-PCE で PCC によって開始または PCE によって委任されたパス計算を使用するローカル SR ポリシー

```
segment-routing
 traffic-eng
  policy BAR
   color 20 end-point ipv4 1.1.1.20
    candidate-paths
     preference 100
      dynamic
       pcep
       anycast-sid-inclusion
```

- ヘッドエンドでローカルに計算されたダイナミックパス、または SR-PCE によって中央で計算されたダイナミックパスを使用するオンデマンド SR ポリシー

```
segment-routing
  traffic-eng
   on-demand color 10
    dynamic
     anycast-sid-inclusion
```

- SR-PCE によって中央で計算されたダイナミックパスを使用するオンデマンド SR ポリシー

```
segment-routing
 traffic-eng
  on-demand color 20
   dynamic
    pcep
    anycast-sid-inclusion
```

条件付きプレフィックス アドバタイズメント

ABR（ABR 1 など）が使用不可または到達不能になっても、そのエニーキャスト SID をアドバタイズしている場合、トラフィックは ABR にルーティングされたままになり、その結果、ド

ロップされます。条件付きプレフィックス アドバタイズメントでは、ABR がドメインに接続されているときにそのループバックアドレスをアドバタイズし、ドメイン内の他の ABR のループバックアドレスを追跡できます。ABR が使用不可または到達不能になった場合、その ABR はループバックアドレスのアドバタイズを停止します。

rib-has-route 属性を使用したルートポリシーで、ルートがルーティング情報ベース（RIB）内にあるかどうかを確認します。**rib-has-route** 属性の新しい **async** サブオプションがイベント駆動型の rib-has-route の実装と既存のポーリング（または同期）メカニズムとを区別するために導入されました。

コンフィギュレーション

他の ABR への接続を追跡するには、ドメイン内の ABR のプレフィックスセットを作成します。次に、ABR への接続を確認するためのルートポリシーを作成します。

```
Router(config)# prefix-set prefix-set-name
Router(config-pfx)# prefix-address-1/length[, prefix-address-2/length,,,
prefix-address-16/length]
Router(config-pfx)# end-set

Router(config)# route-policy rpl-name
Router(config-rpl)# if rib-has-route async prefix-set-name then
Router(config-rpl-if)# pass
Router(config-rpl-if)# endif
Router(config-rpl)# end-policy
```

ループバックアドレスをドメイン内の他の ABR にアドバタイズするには、IS-IS アドレス ファミリ コンフィギュレーション モードで **advertise prefix route-policy** コマンドを使用します。

```
Router(config)# router isis 1
Router(config-isis)# interface Loopback0
Router(config-isis-if)# address-family ipv4 unicast
Router(config-isis-if-af)# advertise prefix route-policy rpl-name
Router(config-isis-if-af)# prefix-sid {index SID-index | absolute SID-value}
Router(config-isis-if-af)# commit
```

例

```
Router(config)# prefix-set domain_2
Router(config-pfx)# 2.3.3.3/32, 2.4.4.4/32
Router(config-pfx)# end-set
Router(config)# route-policy track_domain-2
Router(config-rpl)# if rib-has-route async domain-2 then
Router(config-rpl-if)# pass
Router(config-rpl-if)# endif
Router(config-rpl)# end-policy
Router(config)# router isis 1
Router(config-isis)# interface Loopback0
Router(config-isis-if)# address-family ipv4 unicast
Router(config-isis-if-af)# advertise prefix route-policy track_domain-2
Router(config-isis-if-af)# prefix-sid index 202
Router(config-isis-if-af)# commit
```

実行コンフィギュレーション

```
prefix-set domain_2
  2.3.3.3/32,
  2.4.4.4/32
end-set
!
route-policy track_domain-2
  if rib-has-route async domain-2 then
    pass
  endif
end-policy
!
router isis 1
 interface Loopback0
  address-family ipv4 unicast
   advertise prefix route-policy track_domain-2
   prefix-sid index 202
  !
 !
!
```

明示パス

明示パスを使用した SR-TE ポリシーの設定

SR-TE ポリシーを明示パスを使用して設定するには、次の設定を実行します。

1. セグメント リストを作成します。セグメントリストでは、IP アドレスまたは MPLS ラベルを使用することも、両方を組み合わせて使用することもできます。

（注） セグメントリストでは、IP アドレスと MPLS ラベルの両方を使用できますが、MPLS ラベルを入力すると、IP アドレスを入力することはできません。

2. SR-TE ポリシーを作成します。

明示パスを使用したローカル SR-TE ポリシーの設定

IP アドレスを使用してセグメントリストを作成します。

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# segment-list name SIDLIST1
Router(config-sr-te-sl)# index 10 address ipv4 1.1.1.2
Router(config-sr-te-sl)# index 20 address ipv4 1.1.1.3
Router(config-sr-te-sl)# index 30 address ipv4 1.1.1.4
Router(config-sr-te-sl)# exit
```

MPLS ラベルを使用してセグメントリストを作成します。

```
Router(config-sr-te)# segment-list name SIDLIST2
Router(config-sr-te-sl)# index 10 mpls label 16002
```

```
Router(config-sr-te-sl)# index 20 mpls label 16003
Router(config-sr-te-sl)# index 30 mpls label 16004
Router(config-sr-te-sl)# exit
```

IP アドレスと MPLS ラベルを使用してセグメントリストを作成します。

```
Router(config-sr-te)# segment-list name SIDLIST3
Router(config-sr-te-sl)# index 10 address ipv4 1.1.1.2
Router(config-sr-te-sl)# index 20 mpls label 16003
Router(config-sr-te-sl)# index 30 mpls label 16004
Router(config-sr-te-sl)# exit
```

SR TE ポリシーを作成します。

```
Router(config-sr-te)# policy POLICY1
Router(config-sr-te-policy)# color 10 end-point ipv4 1.1.1.4
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy-path)# preference 100
Router(config-sr-te-policy-path-pref)# explicit segment-list SIDLIST1
Router(config-sr-te-policy-path-pref)# exit
Router(config-sr-te-pp-info)# exit

Router(config-sr-te)# policy POLICY2
Router(config-sr-te-policy)# color 20 end-point ipv4 1.1.1.4
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy-path)# preference 100
Router(config-sr-te-policy-path-pref)# explicit segment-list SIDLIST2
Router(config-sr-te-policy-path-pref)# exit
Router(config-sr-te-pp-info)# exit

Router(config-sr-te)# policy POLICY3
Router(config-sr-te-policy)# color 30 end-point ipv4 1.1.1.4
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy-path)# preference 100
Router(config-sr-te-policy-path-pref)# explicit segment-list SIDLIST3
Router(config-sr-te-policy-path-pref)# commit
```

実行コンフィギュレーション

```
Router# show running-configuration
segment-routing
 traffic-eng
  segment-list SIDLIST1
   index 10 address ipv4 1.1.1.2
   index 20 address ipv4 1.1.1.3
   index 30 address ipv4 1.1.1.4
  !
  segment-list SIDLIST2
   index 10 mpls label 16002
   index 20 mpls label 16003
   index 30 mpls label 16004
  !
  segment-list SIDLIST3
   index 10 address ipv4 1.1.1.2
   index 20 mpls label 16003
   index 30 mpls label 16004
  !
  policy POLICY1
   color 10 end-point ipv4 1.1.1.4
```

```
 candidate-paths
  preference 100
   explicit segment-list SIDLIST1
  !
 !
!
policy POLICY2
 color 20 end-point ipv4 1.1.1.4
 candidate-paths
  preference 100
   explicit segment-list SIDLIST2
  !
 !
!
policy POLICY3
 color 30 end-point ipv4 1.1.1.4
 candidate-paths
  preference 100
   explicit segment-list SIDLIST3
  !
 !
!
```

確認

```
Router# show segment-routing traffic-eng policy name srte_c_20_ep_1.1.1.4
Sat Jul  8 12:25:34.114 UTC
SR-TE policy database
---------------------
Name: P1 (Color: 20, End-point: 1.1.1.4)
  Status:
    Admin: up  Operational: up for 00:06:21 (since Jul  8 12:19:13.198)
  Candidate-paths:
    Preference 10:
      Explicit: segment-list SIDLIST1 (active)
        Weight: 2
          400102 [Prefix-SID, 2.1.1.1]
          400106
      Explicit: segment-list SIDLIST2 (active)
        Weight: 2
          400222 [Prefix-SID, 22.11.1.1]
          400106
  Attributes:
    Binding SID: 15001
      Allocation mode: explicit
      State: programmed
      Policy selected: yes
    Forward Class: 0
```

アフィニティ制約検証を使用した明示パスの設定

SR-TEの柔軟な名前ベースのポリシー制約を完全に設定するには、次の高レベルのタスクを順番に実行する必要があります。

1. 数値へのカラー名の割り当て
2. アフィニティ名の SR-TE リンクとの関連付け
3. SR-TE ポリシーのアフィニティ制約の関連付け

```
/* Enter the global configuration mode and assign color names to numeric values
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# affinity-map
Router(config-sr-te-affinity-map)# blue bit-position 0
Router(config-sr-te-affinity-map)# green bit-position 1
Router(config-sr-te-affinity-map)# red bit-position 2
Router(config-sr-te-affinity-map)# exit


/* Associate affinity-names with SR-TE links
Router(config-sr-te)# interface Gi0/0/0/0
Router(config-sr-te-if)# affinity
Router(config-sr-te-if-affinity)# blue
Router(config-sr-te-if-affinity)# exit
Router(config-sr-te-if)# exit
Router(config-sr-te)# interface Gi0/0/0/1
Router(config-sr-te-if)# affinity
Router(config-sr-te-if-affinity)# blue
Router(config-sr-te-if-affinity)# green
Router(config-sr-te-if-affinity)# exit
Router(config-sr-te-if)# exit
Router(config-sr-te)#


/* Associate affinity constraints for SR-TE policies
Router(config-sr-te)# segment-list name SIDLIST1
Router(config-sr-te-sl)# index 10 address ipv4 1.1.1.2
Router(config-sr-te-sl)# index 20 address ipv4 2.2.2.23
Router(config-sr-te-sl)# index 30 address ipv4 1.1.1.4
Router(config-sr-te-sl)# exit
Router(config-sr-te)# segment-list name SIDLIST2
Router(config-sr-te-sl)# index 10 address ipv4 1.1.1.2
Router(config-sr-te-sl)# index 30 address ipv4 1.1.1.4
Router(config-sr-te-sl)# exit
Router(config-sr-te)# segment-list name SIDLIST3
Router(config-sr-te-sl)# index 10 address ipv4 1.1.1.5
Router(config-sr-te-sl)# index 30 address ipv4 1.1.1.4
Router(config-sr-te-sl)# exit

Router(config-sr-te)# policy POLICY1
Router(config-sr-te-policy)# color 20 end-point ipv4 1.1.1.4
Router(config-sr-te-policy)# binding-sid mpls 1000
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy-path)# preference 200
Router(config-sr-te-policy-path-pref)# constraints affinity exclude-any red
Router(config-sr-te-policy-path-pref)# explicit segment-list SIDLIST1
Router(config-sr-te-pp-info)# exit
Router(config-sr-te-policy-path-pref)# explicit segment-list SIDLIST2
Router(config-sr-te-pp-info)# exit
Router(config-sr-te-policy-path-pref)# exit
Router(config-sr-te-policy-path)# preference 100
Router(config-sr-te-policy-path-pref)# explicit segment-list SIDLIST3
```

実行コンフィギュレーション

```
Router# show running-configuration
```

```
segment-routing
 traffic-eng

  interface GigabitEthernet0/0/0/0
   affinity
    blue
   !
  !
  interface GigabitEthernet0/0/0/1
   affinity
    blue
    green
   !
  !


  segment-list name SIDLIST1
   index 10 address ipv4 1.1.1.2
   index 20 address ipv4 2.2.2.23
   index 30 address ipv4 1.1.1.4
  !
  segment-list name SIDLIST2
   index 10 address ipv4 1.1.1.2
   index 30 address ipv4 1.1.1.4
  !
  segment-list name SIDLIST3
   index 10 address ipv4 1.1.1.5
   index 30 address ipv4 1.1.1.4
  !
  policy POLICY1
   binding-sid mpls 1000
   color 20 end-point ipv4 1.1.1.4
   candidate-paths
    preference 100
     explicit segment-list SIDLIST3
     !
    !
    preference 200
     explicit segment-list SIDLIST1
     !
     explicit segment-list SIDLIST2
     !
     constraints
      affinity
       exclude-any
        red
       !
      !
     !
    !
   !
  !
  affinity-map
   blue bit-position 0
   green bit-position 1
   red bit-position 2
  !
 !
!
```

プロトコル

パス計算要素プロトコル

パス計算要素プロトコル（PCEP）は、パス計算クライアント（PCC）がPCCを起点とするヘッドエンド ラベル スイッチド パス（LSP）の制御を PCE ピアに報告し委任できる一連の手順を記述しています。PCE は、PCC が制御している LSP のパラメータの更新と変更を PCC に要求することができます。また、ステートフル モデルでは、PCC は PCE が計算を開始することを許可でき、PCE はネットワーク全体のオーケストレーションを実行できます。

PCEP PCC としてのヘッドエンドルータの設定

PCE への接続を確立するために、ヘッドエンドルータを PCEP パス計算クライアント（PCC）として設定します。PCC と PCE 間で TCP 接続（PCEP メッセージの交換用）を確立できるように、PCC アドレスと PCE アドレスをルーティング可能にする必要があります。

PCE への接続を確立するための PCC の設定

PCC 送信元アドレス、SR-PCE アドレス、および SR-PCE オプションを設定するには、**segment-routing traffic-eng pcc** コマンドを使用します。

PCE には任意の優先順位を付与することができます。PCC が複数の PCE に接続されている場合、PCC は最も低い優先順位値の PCE を選択します。タイがある場合は、最高位の IP アドレスの PCE がコンピューティング パス用に選択されます。優先順位（precedence）の *value* の範囲は 0 ～ 255 です。

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# pcc
Router(config-sr-te-pcc)# source-address ipv4 local-source-address
Router(config-sr-te-pcc)# pce address ipv4 PCE-address[precedence value]
Router(config-sr-te-pcc)# pce address ipv4 PCE-address[password {clear | encrypted} LINE]
Router(config-sr-te-pcc)# pce address ipv4 PCE-address[keychain WORD]
```

PCEP 関連タイマーの設定

PCC からピアにキープアライブメッセージを送信する頻度を指定するには、**timers keepalive** コマンドを使用します。範囲は 0 ～ 255 秒で、デフォルト値は 30 秒です。

```
Router(config-sr-te-pcc)# timers keepalive seconds
```

この PCC から PCEP メッセージが受信されない場合にリモートピアが PCEP セッションを停止するまでの待機時間を指定するには、**timers deadtimer** コマンドを使用します。範囲は 1 ～ 255 秒で、デフォルト値は 120 秒です。

```
Router(config-sr-te-pcc)# timers deadtimer seconds
```

委任された SR ポリシーが PCE へのアクティブな接続なしに有効な状態を維持できる期間を指定するには、**timers delegation-timeout** コマンドを使用します。範囲は 0 ～ 3600 秒で、デフォルト値は 60 秒です。

```
Router(config-sr-te-pcc)# timers delegation-timeout seconds
```

PCE 開始 SR ポリシータイマー

PCE によって開始された SR ポリシーを PCC から到達できなくなった PCE ピアに委任された状態のままにする時間を指定するには、**timers initiated orphans** コマンドを使用します。範囲は 10 ～ 180 秒で、デフォルト値は 180 秒です。

```
Router(config-sr-te-pcc)# timers initiated orphans seconds
```

PCE によって開始された SR ポリシーを PCE に委任されていないときにプログラムされた状態のままにする時間を指定するには、**timers initiated state** コマンドを使用します。範囲は 15 ～ 14440 秒（24 時間）で、デフォルト値は 600 秒です。

```
Router(config-sr-te-pcc)# timers initiated state seconds
```

PCE 開始 SR ポリシータイマーの動作に対する理解を深めるには、次の例を検討してください。

- PCE A は、ヘッドエンド N で SR ポリシー P をインスタンス化します。
- ヘッドエンド N は、SR ポリシー P を PCE A に委任し、転送にプログラムします。
- ヘッドエンド N は、PCE A が到達不能になったことを検出すると、SR ポリシー P の PCE 開始 **orphans** および **state** タイマーを開始します。
- **orphans** タイマーが期限切れになる前に PCE A が再接続すると、SR ポリシー P は自動的に元の PCE（PCE A）に再度委任されます。
- **orphans** タイマーが期限切れになると、SR ポリシー P は他の存続している PCE のいずれにも委任可能な状態となります。
- **state** タイマーが期限切れになるまでに SR ポリシー P が別の PCE に委任されないと、ヘッドエンド N は転送から SR ポリシー P を削除します。

SR-TE SYSLOG アラームの有効化

SR-TE 関連の SYSLOG アラームを有効にするには、**logging policy status** コマンドを使用します。

```
Router(config-sr-te)# logging policy status
```

SR-PCE への PCEP レポートの有効化

データベース内のすべての SR ポリシーを PCC から PCE に報告できるようにするには、**report-all** コマンドを使用します。

```
Router(config-sr-te-pcc)# report-all
```

PCC での MSD 値のカスタマイズ

PCEP セッションの確立時に PCC によってシグナリングされた最大 SID 深度（MSD）をカスタマイズするには、**maximum-sid-depth** *value* コマンドを使用します。

デフォルトの MSD *value* は、プラットフォームでサポートされている最大 MSD（12）と同じです。

```
Router(config-sr-te)# maximum-sid-depth value
```

（注） プラットフォームの SR-TE ラベルインポジションの能力は、次のとおりです。

- サービスラベルが適用されない場合、最大 12 個のトランスポートラベル
- サービスラベルが適用される場合、最大 9 個のトランスポートラベル

PCE でパスが計算される場合、PCC では、次の方法で MSD を PCE にシグナリングできます。

- PCEP セッションの確立時：シグナリングされた MSD はノード全体のプロパティとして扱われます。
  - MSD は、**segment-routing traffic-eng maximum-sid-depth** *value* コマンドで設定します。
- PCEP LSP パスの要求時：シグナリングされた MSD は LSP プロパティとして扱われます。
  - オンデマンド（ODN）SR ポリシー：MSD は、**segment-routing traffic-eng on-demand color** *color* **maximum-sid-depth** *value* コマンドを使用して設定します。
  - ローカル SR ポリシー：MSD は、**segment-routing traffic-eng policy** *WORD* **candidate-paths preference** *preference* **dynamic metric sid-limit** *value* コマンドを使用して設定します。

（注） 設定された MSD 値が異なる場合、LSP ごとの MSD がノードごとの MSD よりも優先されます。

パス計算の後、MSD 要件と照らし合わせて、結果のラベルスタックサイズが検証されます。

- パス計算が PCE によって実行された場合に、ラベルスタックサイズが MSD よりも大きいときは、PCE は PCC に「パスなし」の応答を返します。
- パス計算が PCC によって実行された場合に、ラベルスタックサイズが MSD よりも大きいときは、PCC はパスを組み込みません。

（注） 次のケースでは、MSD 制約を満たす次善のパス（存在する場合）が計算されます。

- TE メトリックを使用したダイナミックパスの場合に、**pce segment-routing te-latency** コマンドを使用して PCE が設定されているか、**segment-routing traffic-eng te-latency** コマンドを使用して PCC が設定されているとき
- LATENCY メトリックを使用したダイナミックパスの場合
- アフィニティ制約を使用したダイナミックパスの場合

たとえば、PCC MSD が 4 で、最適パス（累積メトリックが 100）は 5 個のラベルを必要とするが、4 個のラベルを必要とする次善のパス（累積メトリックが 110）が存在する場合は、次善のパスが組み込まれます。

SR-TE パス計算のカスタマイズ

TE メトリックの ECMP 対応パス計算を有効にするには、**te-latency** コマンドを使用します。

```
Router(config-sr-te)# te-latency
```

（注） ECMP 対応パス計算は、IGP および LATENCY メトリックに対してデフォルトで有効になっています。

PCEP 冗長タイプの設定

優先順位が最も低い PCE によるポリシーの開始しか PCC が許可しない、PCC 中心の高可用性モデルを有効にするには、**redundancy pcc-centric** コマンドを使用します。

```
Router(config-sr-te-pcc)# redundancy pcc-centric
```

PCEP PCC としてのヘッドエンドルータの設定および SR-TE 関連オプションのカスタマイズ：例

次の例は、以下の機能を使用して SR-TE ヘッドエンドルータを設定する方法を示しています。

- 異なる優先順位値を持つ 3 つの PCEP サーバ（PCE）で SR-TE ヘッドエンドルータを PCEP クライアント（PCC）として有効にする。IP アドレスが 1.1.1.57 の PCE が最適として選択されます。
- SR-TE 関連の syslog を有効にする。
- PCEP セッションの確立時にシグナリングされる最大 SID 深度（MSD）を 5 に設定する。
- ノード内のすべてのポリシーに対して PCEP レポートを有効にする。

```
segment-routing
 traffic-eng
  pcc
```

```
   source-address ipv4 1.1.1.2
   pce address ipv4 1.1.1.57
    precedence 150
    password clear <password>
   !
   pce address ipv4 1.1.1.58
    precedence 200
    password clear <password>
   !
   pce address ipv4 1.1.1.59
    precedence 250
    password clear <password>
   !
  !
  logging
   policy status
  !
  maximum-sid-depth 5
  pcc
   report-all
  !
 !
!
end
```

確認

```
RP/0/RSP0/CPU0:Router# show segment-routing traffic-eng pcc ipv4 peer

PCC's peer database:
--------------------

Peer address: 1.1.1.57, Precedence: 150, (best PCE)
  State up
  Capabilities: Stateful, Update, Segment-Routing, Instantiation

Peer address: 1.1.1.58, Precedence: 200
  State up
  Capabilities: Stateful, Update, Segment-Routing, Instantiation

Peer address: 1.1.1.59, Precedence: 250
  State up
  Capabilities: Stateful, Update, Segment-Routing, Instantiation
```

BGP SR-TE

SR-TE は、データセンター（DC）のオペレータがさまざまなレベルの Service Level Assurance（SLA）を提供するために使用できます。BGP（BGP SR-TE）を使用して SR-TE パスを設定すると、この目的のために新しいプロトコルを導入することなく、DC ネットワーク操作が簡素化されます。

明示的 BGP SR-TE

明示的 BGP SR-TE は、各明示パスに対応する SID を持つ明示パスの一覧を含む SR-TE ポリシー（固有色 ID で識別される）を使用します。BGP スピーカーは明示的 SR-TE ポリシーをリモートピアに信号で伝え、特定の特性と明示パスを持つ SR-TE ポリシーの設定がトリガーされます。受信側では、明示パスに対応する SR-TE ポリシーが BGP によって設定されます。BGP

更新で言及された宛先のパケットは、ポリシーによって記述された明示パスに従います。各ポリシーは複数の明示パスを含むことができ、TE はパスごとにポリシーを作成します。

（注） ルーティング ポリシーとルーティング ポリシー言語（RPL）の詳細については、『*Routing Configuration Guide for Cisco NCS 540 Series Routers*』の「Implementing Routing Policy」の章を参照してください。

明示的 BGP SR-TE の設定

明示的な BGP SR-TE を設定するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**extcommunity-set opaque** *name* 例： `RP/0/RP0/CPU0:router(config)# extcommunity-set opaque color1`	カラー拡張コミュニティセットを定義します。
ステップ 3	*name* 例： `RP/0/RP0/CPU0:router(config-ext)# 1`	カラー拡張コミュニティセットを定義します。
ステップ 4	**end-set** 例： `RP/0/RP0/CPU0:router(config-ext)# end-set`	拡張コミュニティセットの定義を終了します。

ステップ 5	**route-policy** *route-policy-name*
	例：
	`RP/0/RP0/CPU0:router(config)# route-policy color`
	`RP/0/RP0/CPU0:router(config-rpl)# if destination in (5.5.5.1/32) then`
	`RP/0/RP0/CPU0:router(config-rpl-if)# set extcommunity color color1`
	`RP/0/RP0/CPU0:router(config-rpl-if)# endif`
	`RP/0/RP0/CPU0:router(config-rpl)#`
		ルートポリシーを作成し、ルートポリシー コンフィギュレーション モードを開始します。このモードでは、カラー拡張コミュニティ値を使用してプレフィックスをマークするルート ポリシーを定義できます。

	コマンドまたはアクション	目的
	end-policy	
ステップ 6	**end-policy** 例： `RP/0/RP0/CPU0:router(config-rpl)# end-policy`	ルート ポリシーの定義を終了して、ルートポリシー コンフィギュレーション モードを終了します。
ステップ 7	**router bgp** *as-number* 例： `RP/0/RP0/CPU0:router(config)# router bgp 1`	BGP AS 番号を指定し、BGP コンフィギュレーションモードを開始します。このモードでは、BGP ルーティング プロセスを設定できます。
ステップ 8	**bgp router-id** *ip-address* 例： `RP/0/RP0/CPU0:router(config-bgp)# bgp router-id 10.10.0.2`	指定したルータ ID で、ローカル ルータを設定します。
ステップ 9	**address-family** {**ipv4** | **ipv6**} **sr-policy** 例： `RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 sr-policy`	IPv4 または IPv6 のいずれかのアドレス ファミリを指定し、アドレス ファミリのコンフィギュレーション サブモードを開始します。
ステップ 10	**exit**	
ステップ 11	**neighbor** *ip-address* 例： `RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.10.0.1`	BGP ルーティングのためにルータをネイバー コンフィギュレーション モードにして、ネイバーの IP アドレスを BGP ピアとして設定します。
ステップ 12	**remote-as** *as-number* 例： `RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1`	ネイバーを作成し、リモート自律システム番号を割り当てます。
ステップ 13	**address-family** {**ipv4** | **ipv6**} **unicast** 例：	IPv4 または IPv6 のいずれかのアドレス ファミリを指定し、アドレス ファミリ

	コマンドまたはアクション	目的
	RP/0/RP0/CPU0:router(config-bgp-nbr)# **address-family ipv4 unicast**	のコンフィギュレーションサブモードを開始します。
ステップ 14	**route-policy** *route-policy-name* {**in** | **out**} 例： RP/0/RP0/CPU0:router(config-bgp-nbr-af)# **route-policy color out**	指定したポリシーを IPv4 ユニキャストルートに適用します。
ステップ 15	**send-extended-community-ebgp** 例： RP/0/RP0/CPU0:router(config-bgp-nbr-af)# **send-extended-community-ebgp**	拡張コミュニティ属性を外部□ボーダーゲートウェイ プロトコル（eBGP）ネイバーに送信します。

トラフィックステアリング

自動ステアリング

自動ステアリング（AS）とは、SR ポリシーによってプログラムされた適切な SLA パス上で BGP サービストラフィックが再度自動ステアリングされる機能をいいます。SR ポリシーへのトラフィックの誘導は、ポリシーのインスタンス化方式（BGP TE によってプッシュされ、手動でプロビジョニングされ、オンデマンドで自動的にインスタンス化される（SR-ODN）か、または PCEP によってプッシュされる）に関係なく、目的（色）とサービスルートのネクストホップに基づいて決定されます。AS では、宛先単位でステアリングを実行します。一致する SR ポリシーは、ヘッドエンドルータにすでに存在するか、またはサービスルートの更新を受信するときにオンデマンド（SR ODN）でインスタンス化できます。

AS の実装を示す出力例については、BGP VRF 情報の確認 （58 ページ）および転送（CEF）テーブルの確認 （59 ページ）の項を参照してください。

カラー専用自動ステアリング

カラーのみのステアリングは、エンドポイントに関係なく、特定のカラーでポリシーが作成されるトラフィック ステアリング メカニズムです。

NULL エンドポイント（IPv4 NULL の場合は 0.0.0.0、IPv6 NULL エンドポイントの場合は ::0）を使用する特定のカラーに SR-TE ポリシーを作成できます。つまり、その色に基づいてトラフィックを誘導できる単一のポリシーと、特定の色の拡張コミュニティを持つが宛先が異なるルート（ネクストホップ）の NULL エンドポイントを持つことができます。

（注） NULLエンドポイントを使用したすべてのSR-TEポリシーには、明示パスオプションが必要です。ポリシーの宛先が存在しないため、ポリシーにはダイナミック パスオプション（パスがヘッドエンドまたは PCE によって計算される）を設定することはできません。

また、オーバーレイ ルートのカラー拡張コミュニティでカラーのみ（CO）フラグを指定することもできます。CO フラグを使用すると、エンドポイントのサブアドレス ファミリ識別子（SAFI）（IPv4 または IPv6）に関係なく、一致するカラーの SR ポリシーを選択できます。CO フラグの設定 （107 ページ）を参照してください。

カラーのみのステアリングの設定

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy P1
Router(config-sr-te-policy)# color 1 end-point ipv4 0.0.0.0

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy P2
Router(config-sr-te-policy)# color 2 end-point ipv6 ::0


Router# show running-configuration
segment-routing
 traffic-eng
  policy P1
   color 1 end-point ipv4 0.0.0.0
  !
  policy P2
   color 2 end-point ipv6 ::
  !
 !
!
end
```

CO フラグの設定

BGP ベースのステアリング メカニズムでは、BGP のカラーおよびネクストホップと SR-TE ポリシーのそれらが照合されます。ポリシーが存在しない場合、BGPは、関連付けられたカラー、エンドポイント、および明示パスを使用して SR-TE ポリシーを作成するように SR-PCE に要求します。カラーのみのステアリング（NULL エンドポイント）の場合、BGP のカラー拡張コミュニティの一部としてカラーのみ（CO）フラグを設定できます。

（注） カラーのみのステアリング（NULLエンドポイント）の詳細については、カラー専用自動ステアリング （43 ページ）を参照してください。

ステアリング メカニズムの動作は CO フラグの次の値に基づいています。

co-flag 00	1. BGP のネクストホップおよびカラー <N, C> が SR-TE ポリシーのネクストホップとカラー <N, C> に一致します。 2. ポリシーが存在しない場合は、ネクストホップ N の IGP パスが選択されます。
co-flag 01	1. BGP のネクストホップおよびカラー <N, C> が SR-TE ポリシーのネクストホップとカラー <N, C> に一致します。 2. ポリシーが存在しない場合は、N と カラー C と同じアドレスファミリを持つ NULL エンドポイントを使用する SR-TE ポリシーが選択されます。 3. N と同じアドレスファミリを持つ NULL エンドポイントを使用するポリシーが存在しない場合は、NULL エンドポイントとカラー C を使用する SR-TE ポリシーが選択されます。 4. 一致が見つからない場合は、ネクストホップ N の IGP パスが選択されます。

設定例

```
Router(config)# extcommunity-set opaque overlay-color
Router(config-ext)# 1 co-flag 01
Router(config-ext)# end-set
Router(config)#
Router(config)# route-policy color
Router(config-rpl)# if destination in (5.5.5.1/32) then
Router(config-rpl-if)# set extcommunity color overlay-color
Router(config-rpl-if)# endif
Router(config-rpl)# pass
Router(config-rpl)# end-policy
Router(config)#
```

アドレスファミリに依存しない自動ステアリング

アドレスファミリに依存しないステアリングでは、SR-TE ポリシーを使用して、ラベル付きとラベルなしの両方の IPv4 および IPv6 トラフィックを誘導します。この機能には、IPV4 エンドポイント ポリシーを介した IPv6 カプセル化（IPv6 caps）のサポートが必要です。

IPv4 NULL エンドポイントの IPv6 caps は、セグメントルーティングパス計算要素（SR-PCE）でポリシーが作成されると自動的に有効になります。各ポリシーのバインディング SID（BSID）状態通知には、IPv6 caps のステータス（有効または無効）を SR-PCE クライアント（PCC）に通知する「ipv6_caps」フラグが含まれます。

特定のカラーと IPv4 NULL エンドポイントを使用する SR-TE ポリシーは複数の候補パスを使用できます。候補パスのいずれかで IPv6 caps が有効になっている場合は、残りのすべての候

補パスで IPv6 caps が有効になっている必要があります。同じカラーとエンドポイントのすべての候補パスで IPv6 caps が有効になっていない場合、トラフィックが破棄される可能性があります。

ローカル ポリシーで **ipv6 disable** コマンドを使用すると、特定のカラーと IPv4 NULL エンドポイントの IPv6 caps を無効にできます。このコマンドは、同じカラーと IPv4 NULL エンドポイントを共有するすべての候補パスで IPv6 caps を無効にします。

IPv6 カプセル化の無効化

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy P1
Router(config-sr-te-policy)# color 1 end-point ipv4 0.0.0.0
Router(config-sr-te-policy)# ipv6 disable
```

バインド セグメントの使用

バインド セグメントは、SR-TE ポリシーを識別するローカル セグメントです。各 SR-TE ポリシーは、バインドセグメント ID（BSID）に関連付けられています。BSID は、SR-TE ポリシーがインスタンス化されるときに SR-TE ポリシーごとに自動的に割り当てられるローカル ラベルです。

（注） Cisco IOS XR 6.3.2 以降のリリースでは、SR-TE ポリシーに明示的な BSID を指定できます。次の「**明示的なバインド SID**」の項を参照してください。

BSID を使用して、トラフィックを SR-TE ポリシーにドメイン境界を超えて誘導し、シームレスなエンドツーエンドのドメイン間 SR-TE ポリシーを作成できます。各ドメインはローカルの SR-TE ポリシーを制御します。リモート ドメインのヘッドエンドとは独立して、ローカルの SR-TE ポリシーを検証し、必要に応じて再ルーティングすることができます。バインド セグメントを使用すると、リモート ドメインのトポロジの変更からヘッドエンドが分離されます。

トップ ラベルとして BSID で受信されたパケットは、BSID に関連付けられている SR-TE ポリシーに誘導されます。BSID ラベルがポップされると、SR-TE ポリシーの SID リストがプッシュされます。

BSID は次の場合に使用できます。

- マルチドメイン（ドメイン間、自律システム間）：BSID を使用して、ドメイン境界を越えてトラフィックを誘導し、シームレスなエンドツーエンドのドメイン間 SR-TE ポリシーを作成できます。
- 単一ドメイン内の大規模：ヘッドエンドは、SR-TE ポリシーの別のレイヤ内でエンドツーエンド（エッジツーエッジ）の SR-TE ポリシーをネストすることにより、階層型 SR-TE ポリシーを使用できます（アグリゲーションからアグリゲーションまで）。SR-TE ポリ

シーは、BSIDを使用する別のポリシーのレイヤ内にネストされ、シームレスなエンドツーエンドの SR-TE ポリシーが作成されます。

- ラベルスタック圧縮：SR-TEポリシーに必要なラベルスタックのサイズがプラットフォーム機能を超えている場合、SR-TEポリシーは、バインドセグメントを使用して他のSR-TEポリシーにシームレスにステッチしたり、ネストすることができます。

明示的なバインド SID

明示的なBSIDを指定するには、SR-TEポリシーコンフィギュレーションモードで**binding-sid mpls** *label* コマンドを使用します。明示的な BSID は、セグメント ルーティング ローカル ブロック（SRLB）またはラベルのダイナミック レンジから割り当てられます。SR-TE ポリシーの BSID の要求と取得はベストエフォートで行われます。要求された BSID が利用できない場合（利用可能な SRLB に属していない、または別のアプリケーションまたは SR-TE ポリシーによってすでに使用されている場合）、ポリシーはダウン状態のままです。

BSID 値を使用できない場合に BSID の割り当て動作を指定するには、**binding-sid explicit** {**fallback-dynamic** | **enforce-srlb**} コマンドを使用します。

- 動的割り当てへのフォールバック：BSIDが利用できない場合、BSIDは動的に割り当てられ、ポリシーが起動します。

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# binding-sid explicit fallback-dynamic
```

- 厳格な SRLB 適用：BSID が SRLB 内にない場合、ポリシーはダウン状態のままです。

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# binding-sid explicit enforce-srlb
```

次に、明示的な BSID 1000 を使用するように SR ポリシーを設定する例を示します。明示的な BSID が使用できない場合、BSID は動的に割り当てられ、ポリシーが起動します。

```
segment-routing
 traffic-eng
  binding-sid explicit fallback-dynamic
  policy goo
   binding-sid mpls 1000
  !
 !
!
```

L2VPN 優先パス

SR-TE ポリシーを介した EVPN VPWS 優先パス機能では、SR-TE ポリシーを使用して、EVPN VPWS 疑似回線（PW）の 2 つのエンドポイント間に優先パスを設定できます。

SR-TE ポリシーを介した L2VPN VPLS または VPWS 優先パス機能では、L2VPN 仮想プライベート LAN サービス（VPLS）または仮想プライベート ワイヤ サービス（VPWS）の 2 つのエンドポイント間に SR-TE ポリシーを使用して優先パスを設定できます。

『*L2VPN and Ethernet Services Configuration Guide*』の「L2VPN Services over Segment Routing for Traffic Engineering Policy」の章にある「EVPN VPWS Preferred Path over SR-TE Policy」および「L2VPN VPLS or VPWS Preferred Path over SR-TE Policy」の項を参照してください。

SR-TEポリシーを使用したスタティック ルート トラフィック ステアリング

以前のリリースでは、セグメント ルーティング ラベル スイッチド パス（SR-LSP）をスタティック ルートに関連付けることしかできませんでした。SRTEポリシーを使用したスタティック ルート トラフィック ステアリング機能を使用すると、MPLS および IPv6 データ プレーンのスタティック ルートを設定するときに、セグメント ルーティング（SR）ポリシーをインターフェイス タイプとして指定できます。

スタティック ルートの設定に関する詳細については、『*Routing Configuration Guide for Cisco NCS 560 Series Routers*』の「Implementing Static Routes」の章を参照してください。

設定例

```
Router(config)# router static
Router (config-static)# address-family ipv4 unicast

//configure administrative distance
Router (config-static-afi)# 1.1.1.1/32 sr-policy policy1 110

//Configure load metric
Router (config-static-afi)# 1.1.1.1/32 sr-policy policy1 metric 5

//Install the route in RIB regardless of reachability
Router (config-static-afi)# 1.1.1.1/32 sr-policy policy1 permanent
```

実行コンフィギュレーション

```
configure
 router static
  address-family ipv4 unicast
  1.1.1.1/32 sr-policy policy1 110
  1.1.1.1/32 sr-policy policy1 metric 5
  1.1.1.1/32 sr-policy policy1 permanent
  !
 !
!
```

自動ルート インクルード

自動ルート インクルードを使用して SR-TE ポリシーを設定すると、最短以外のパスを介して特定の IGP（IS-IS、OSPF）プレフィックスを誘導し、そのプレフィックスのトラフィックを

SR-TE ポリシーに転送することができます。自動ルート インクルードは、指定された宛先またはプレフィックスに自動ルート アナウンス機能を適用します。

自動ルート SR-TE ポリシーはプレフィックスを IGP に追加します。これにより、エンドポイントのプレフィックスまたはエンドポイントのダウンストリームのプレフィックスが SR-TE ポリシーを使用する資格があるかどうかが決定されます。プレフィックスが適格な場合、IGP はプレフィックスが自動ルートインクルード設定にリストされているかどうかを確認します。プレフィックスが含まれている場合、IGP は発信パスとして SR-TE ポリシーを使用してプレフィックス ルートをダウンロードします。

自動ルート インクルードは、次の 3 つのメトリック タイプをサポートします。

- デフォルト（メトリックなし）：SR-TE ポリシーを介したパスは最短パス メトリックを継承します。
- 絶対メトリック：ポリシー エンドポイントへの最短パス メトリックは設定された絶対メトリックに置き換えられます。自動ルートが含まれるプレフィックスへのメトリックは絶対メトリックに変更されます。
- 相対メトリック：ポリシー エンドポイントへの最短パス メトリックは設定された相対値（プラスまたはマイナス）を使用して変更されます。

（注） IGP パス上のロードバランシングを防止するために、IGP が自動ルート設定した宛先（**autoroute metric relative -1** など）に対して考慮する値よりも低いメトリックを指定できます。

設定例

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)#policy P1
Router(config-sr-te-policy)# color 20 end ipv4 1.1.1.2
Router(config-sr-te-policy)# autoroute include ipv4 1.1.1.21/32
Router(config-sr-te-policy)# autoroute include ipv4 1.1.1.23/32
Router(config-sr-te-policy)# autoroute metric constant 1
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy-path)# preference 100
Router(config-sr-te-pp-index)# explicit segment-list Plist-1
```

その他

セグメント ルーティング ポリシーを介した LDP

セグメント ルーティング ポリシーを介した LDP 機能を使用すると、2 台のルータ間でセグメントルーティング（SR）ポリシーを介して LDP ターゲット隣接関係を実現できます。この機

能は、SR ポリシーをターゲットエンドポイントとして指定できるように、既存の MPLS LDP アドレス ファミリ ネイバー コンフィギュレーションを拡張します。

SR ポリシーを介した LDP は、IPv4 エンドポイントを使用してローカルに設定された SR ポリシーでサポートされます。

MPLS LDP の詳細については、『*MPLS Configuration Guide*』の「Implementing MPLS Label Distribution Protocol」の章を参照してください。

（注） SR ポリシー名を介して LDP ターゲット隣接関係を設定する前に、セグメント ルーティング コンフィギュレーションで SR ポリシーを作成する必要があります。SR ポリシーのインターフェイス名は、ポリシーのカラーとエンドポイントに基づいて内部的に作成されます。SR ポリシー名が不明な場合、LDP は動作できません。

次の機能が適用されます。

1. SR ポリシーを設定する：LDP では、関連付けられたエンドポイントアドレスをインターフェイス マネージャ（IM）から受け取り、設定された SR ポリシーの LDP インターフェイス データベース（IDB）に保存します。
2. LDP で SR ポリシー名を設定する： LDP では、保存されたエンドポイントアドレスを IDB から取得して使用します。SR ポリシーを介して LDP ターゲット隣接関係を作成する際には、ルータによって割り当てられた自動生成SRポリシー名を使用します。自動生成SRポリシー名で使用される命名規則は、**srte_c_***color_val*_**ep_***endpoint-address* です。次に例を示します。 **srte_c_1000_ep_1.1.1.2**

設定例

```
/* Enter the SR-TE configuration mode and create the SR policy. This example corresponds
 to a local SR policy with an explicit path. */
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# segment-list sample-sid-list
Router(config-sr-te-sl)# index 10 address ipv4 1.1.1.7
Router(config-sr-te-sl)# index 20 address ipv4 1.1.1.2
Router(config-sr-te-sl)# exit
Router(config-sr-te)# policy sample_policy
Router(config-sr-te-policy)# color 1000 end-point ipv4 1.1.1.2
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy-path)# preference 100
Router(config-sr-te-policy-path-pref)# explicit segment-list sample-sid-list
Router(config-sr-te-pp-info)# end

/* Configure LDP over an SR policy */
Router(config)# mpls ldp
Router(config-ldp)# address-family ipv4
Router(config-ldp-af)# neighbor sr-policy srte_c_1000_ep_1.1.1.2 targeted
Router(config-ldp-af)#
```

（注） ターゲット hello の LDP ディスカバリを設定するには、次のいずれかを実行します。

- アクティブなターゲット hello（SR ポリシーヘッドエンド）：

```
mpls ldp
 interface GigabitEthernet0/0/0/0
 !
!
```

- パッシブなターゲット hello（SR ポリシーエンドポイント）：

```
mpls ldp
 address-family ipv4
  discovery targeted-hello accept
 !
!
```

実行コンフィギュレーション

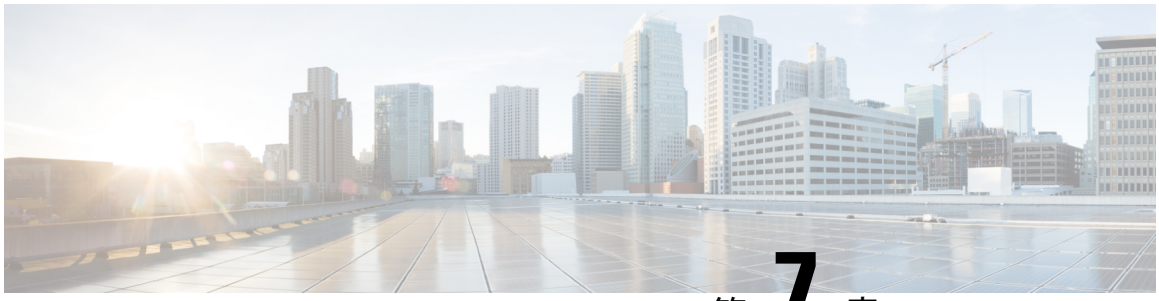
```
segment-routing
 traffic-eng
  segment-list sample-sid-list
   index 10 address ipv4 1.1.1.7
   index 20 address ipv4 1.1.1.2
  !
  policy sample_policy
   color 1000 end-point ipv4 1.1.1.2
   candidate-paths
    preference 100
     explicit segment-list sample-sid-list
     !
    !
   !
  !
 !
!

mpls ldp
 address-family ipv4
  neighbor sr-policy srte_c_1000_ep_1.1.1.2 targeted
  discovery targeted-hello accept
 !
!
```

確認

```
Router# show mpls ldp interface brief
Interface       VRF Name            Config Enabled IGP-Auto-Cfg TE-Mesh-Grp cfg
--------------- ------------------- ------ ------- ------------ ---------------
Te0/3/0/0/3     default             Y      Y       0            N/A
Te0/3/0/0/6     default             Y      Y       0            N/A
Te0/3/0/0/7     default             Y      Y       0            N/A
Te0/3/0/0/8     default             N      N       0            N/A
Te0/3/0/0/9     default             N      N       0            N/A
srte_c_1000_    default             Y      Y       0            N/A


Router# show mpls ldp interface
Interface TenGigE0/3/0/0/3 (0xa000340)
```

```
   VRF: 'default' (0x60000000)
   Enabled via config: LDP interface
Interface TenGigE0/3/0/0/6 (0xa000400)
   VRF: 'default' (0x60000000)
   Enabled via config: LDP interface
Interface TenGigE0/3/0/0/7 (0xa000440)
   VRF: 'default' (0x60000000)
   Enabled via config: LDP interface
Interface TenGigE0/3/0/0/8 (0xa000480)
   VRF: 'default' (0x60000000)
   Disabled:
Interface TenGigE0/3/0/0/9 (0xa0004c0)
   VRF: 'default' (0x60000000)
   Disabled:
Interface srte_c_1000_ep_1.1.1.2 (0x520)
   VRF: 'default' (0x60000000)
   Enabled via config: LDP interface


Router# show segment-routing traffic-eng policy color 1000

SR-TE policy database
---------------------

Color: 1000, End-point: 1.1.1.2
  Name: srte_c_1000_ep_1.1.1.2
  Status:
    Admin: up  Operational: up for 00:02:00 (since Jul  2 22:39:06.663)
  Candidate-paths:
    Preference: 100 (configuration) (active)
      Name: sample_policy
      Requested BSID: dynamic
      PCC info:
        Symbolic name: cfg_sample_policy_discr_100
        PLSP-ID: 17
      Explicit: segment-list sample-sid-list (valid)
        Weight: 1, Metric Type: TE
          16007 [Prefix-SID, 1.1.1.7]
          16002 [Prefix-SID, 1.1.1.2]
  Attributes:
    Binding SID: 80011
    Forward Class: 0
    Steering BGP disabled: no
    IPv6 caps enable: yes


Router# show mpls ldp neighbor 1.1.1.2 detail

Peer LDP Identifier: 1.1.1.2:0
  TCP connection: 1.1.1.2:646 - 1.1.1.6:57473
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 421/423; Downstream-Unsolicited
  Up time: 05:22:02
  LDP Discovery Sources:
    IPv4: (1)
      Targeted Hello (1.1.1.6 -> 1.1.1.2, active/passive)
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (9)
      1.1.1.2         2.2.2.99        10.1.2.2        10.2.3.2
      10.2.4.2        10.2.22.2       10.2.222.2      10.30.110.132
      11.2.9.2
    IPv6: (0)
```

```
Peer holdtime: 180 sec; KA interval: 60 sec; Peer state: Estab
NSR: Disabled
Clients: LDP over SR Policy
Capabilities:
  Sent:
    0x508  (MP: Point-to-Multipoint (P2MP))
    0x509  (MP: Multipoint-to-Multipoint (MP2MP))
    0x50a  (MP: Make-Before-Break (MBB))
    0x50b  (Typed Wildcard FEC)
  Received:
    0x508  (MP: Point-to-Multipoint (P2MP))
    0x509  (MP: Multipoint-to-Multipoint (MP2MP))
    0x50a  (MP: Make-Before-Break (MBB))
    0x50b  (Typed Wildcard FEC)
```



第 7 章

セグメント ルーティング パス計算要素の設定

セグメント ルーティング パス計算要素（SR-PCE）は、既存の IOS-XR PCEP 機能に追加機能を拡張してステートフル PCE 機能を提供します。SR-PCE は、MPLS データ プレーンと IPv4 コントロール プレーンでサポートされています。

（注） SR-PCE をインストールするには、Cisco IOS XRv 9000 ルータのインスタンスをインストールする必要があります。詳細については、『Cisco IOS XRv 9000 Router Installation and Configuration Guide』を参照してください。

SR-PCE について

パス計算要素プロトコル（PCEP）は、パス計算クライアント（PCC）が PCC を起点とするヘッドエンド ラベル スイッチド パス（LSP）の制御を PCE ピアに報告し委任できる一連の手順を記述しています。PCE は、PCC が制御している LSP のパラメータの更新と変更を PCC に要求することができます。また、ステートフル モデルでは、PCC は PCE が計算を開始することを許可でき、PCE はネットワーク全体のオーケストレーションを実行できます。

SR-PCE は、IGP（OSPF または IS-IS）または BGP リンクステート（BGP-LS）経由でトポロジ情報を学習します。

SR-PCE は、以下の方法を使用してパスを計算できます。

- TE メトリック：SR-PCE は TE メトリックを使用してパス計算を行い、累積 TE メトリックを最適化します。

- IGP メトリック：SR-PCE は IGP メトリックを使用してパス計算を行い、到達可能性を最適化します。
- LSP ディスジョイントネス：SR-PCE はパス計算アルゴリズムを使用して、ディスジョイント LSP のペアを計算します。ディスジョイント パスの起点は、同じヘッドエンドまたは異なるヘッドエンドです。ディスジョイント レベルとは、2 つの計算されたパスで共有すべきではないリソースのタイプを指します。SR-PCE は、次のディスジョイント パス計算をサポートしています。
  - リンク：リンクが計算されたパスで共有されないことを指定します。
  - ノード：ノードが計算されたパス上で共有されないことを指定します。
  - SRLG：同じ SRLG 値を持つリンクが計算されたパスで共有されないことを指定します。
  - SRLG ノード：SRLG とノードが計算されたパス上で共有されないことを指定します。

所定のディスジョイントグループ ID で最初の要求が受信されると、最初の LSP が計算され、最初の送信元から最初の宛先への最短パスがエンコードされます。2 つ目の LSP 要求が同じディスジョイントグループ ID で受信されると、両方の要求で受信された情報を使用して 2 つのディスジョイント パス（1 つは最初の送信元から最初の宛先へのパス、もう 1 つは 2 つ目の送信元から 2 つ目の宛先へのパス）が計算されます。両方のパスが同時に計算されます。

SR-PCE の設定

このタスクでは、SR-PCE を設定する方法について説明します。

始める前に

必要に応じて、Cisco IOS XRv 9000 ルータのインスタンスをインストールして設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**pce** 例： `RP/0/RP0/cpu 0: router(config)# pce`	PCE を有効にし、PCE 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	**address ipv4** *address* 例：	PCE IPv4 アドレスを設定します。

	コマンドまたはアクション	目的
	RP/0/RP0/cpu 0: router(config-pce)# **address ipv4 192.168.0.1**	
ステップ 4	**state-sync ipv4** *address* 例： RP/0/RP0/cpu 0: router(config-pce)# **state-sync ipv4 192.168.0.3**	リモート ピアに状態同期を設定します。
ステップ 5	**tcp-buffer** *size* 例： RP/0/RP0/cpu 0: router(config-pce)# **tcp-buffer 1024000**	各 PCEP セッションの送受信 TCP バッファ サイズをバイト単位で設定します。デフォルトのバッファ サイズは 256000 です。有効な範囲は 204800 ～ 1024000 です。
ステップ 6	**password** {**clear** | **encrypted**} *password* 例： RP/0/RP0/cpu 0: router(config-pce)# **password encrypted pwd1**	すべての PCEP ピアの TCP 認証を有効にします。設定されたパスワードと一致する MAC を含まない PCC から来る TCP セグメントはすべて拒否されます。パスワードが暗号化されているか、またはクリアテキストであるかを指定します。
ステップ 7	**segment-routing** {**strict-sid-only** | **te-latency**} 例： RP/0/RP0/cpu 0: router(config-pce)# **segment-routing strict-sid-only**	厳格な SID または TE のレイテンシを使用するようにセグメント ルーティング アルゴリズムを設定します。 （注） この設定はグローバルで、このコントローラからパスを要求するすべての LSP に適用されます。
ステップ 8	**timers** 例： RP/0/RP0/cpu 0: router(config-pce)# **timers**	タイマー コンフィギュレーション モードを開始します。
ステップ 9	**keepalive** *time* 例： RP/0/RP0/cpu 0: router(config-pce-timers)# **keepalive 60**	ローカルで生成されたキープアライブ メッセージのタイマー値を設定します。デフォルトの時間は 30 秒です。

	コマンドまたはアクション	目的

ステップ 10	**minimum-peer-keepalive** *time*
	例：
	`RP/0/RP0/cpu 0:`
	`router(config-pce-timers)#`
	`minimum-peer-keepalive 30`
		セッション確立中にリモート ピアが PCEP OPEN メッセージで提案できる最小の許容キープアライブ タイマーを設定します。デフォルトの時間は20秒です。

ステップ 11	**reoptimization** *time*
	例：
	`RP/0/RP0/cpu 0:`
	`router(config-pce-timers)#`
	`reoptimization 30`
		再最適化タイマーを設定します。デフォルト タイマーは 60 秒です。

ステップ 12	**exit** 例： `RP/0/RP0/cpu 0:` `router(config-pce-timers)#` **`exit`**	タイマー コンフィギュレーション モードを終了し、PCE コンフィギュレーション モードに戻ります。

ディスジョイント ポリシーの設定（オプション）

次のタスクでは、PCEP 要求に PCEP 関連グループ ID オブジェクトを含まない PCC によってシグナリングされた LSP のペアのディスジョイントネスを計算するように SR-PCE を設定する方法について説明します。これは、PCC がこの PCEP オブジェクトをサポートしていない場合、またはネットワーク オペレータが LSP ディスジョイント設定を一元管理する場合の展開に便利です。

手順

	コマンドまたはアクション	目的
ステップ 1	**disjoint-path** 例： `RP/0/RP0/cpu 0: router(config-pce)#` **`disjoint-path`**	ディスジョイント コンフィギュレーション モードを開始します。
ステップ 2	**group-id** *value* **type** {**link** | **node** | **srlg** | **srlg-node**} [**sub-id** *value*] 例： `RP/0/RP0/cpu 0:`	ディスジョイント グループ ID を設定し、ディスジョイントネスの優先レベル（2つのパスで共有されるべきでないリソースのタイプ）を定義します。

	コマンドまたはアクション	目的
	`router(config-pce-disjoint)# group-id 1 type node sub-id 1`	• **link**：リンクが計算されたパス上で共有されないことを指定します。 • **node**：ノードが計算されたパス上で共有されないことを指定します。 • **srlg**：同じ SRLG 値を持つリンクが計算されたパスで共有されないことを指定します。 • **srlg-node**：SRLG とノードが計算されたパス上で共有されないことを指定します。 要求されたディスジョイントネス レベルを満たすパスのペアが見つからない場合、パスは自動的に下位レベルにフォールバックされます。 • 要求されたディスジョイントネス レベルが SRLG またはノードの場合、リンクディスジョイント パスが計算されます。 • 要求されたディスジョイントネス レベルがリンクの場合、または SRLG またはノードのディスジョイントネスからの最初のフォールバックが失敗した場合は、2 つの最短パスをエンコードするセグメントのリストが、ディスジョイントネスの制約なしで計算されます。

ステップ 3	**strict**
	例：
	`RP/0/RP0/cpu 0:`
	`router(config-pce-disjoint)# strict`
		（任意）優先レベルのディスジョイントネスの自動フォールバック動作を防止します。要求されたディスジョイントネス レベルを満たすパスのペアが見つからない場合、ディスジョイントの計算は終了し、新しいパスは提供されません。既存のパスは変更されません。

ステップ 4	**lsp** {**1** | **2**} **pcc ipv4** *address* **lsp-name** *lsp_name* ［**shortest-path**］ **例**： `RP/0/RP0/cpu 0:`	ディスジョイント グループに LSP を追加します。 **shortest-path** キーワードは、ディスジョイント パスの 1 つに、送信元から宛先までの最短パスに従うよう強制します。

	コマンドまたはアクション	目的
	router(config-pce-disjoint)# **lsp 1 pcc ipv4 192.168.0.1 lsp-name rtrA_t1 shortest-path** RP/0/RP0/cpu 0: router(config-pce-disjoint)# **lsp 2 pcc ipv4 192.168.0.5 lsp-name rtrE_t2**	このオプションは、指定された最初の LSP にのみ適用できます。

トラフィック管理の PCE 開始 SR ポリシー

SR-TE ポリシーは、リンクの輻輳を軽減したり、ネットワーク タッチ ポイントの数を最小限に抑えたりするようにパス計算要素（PCE）で設定することができます。

（注） PCE 開始 SR-TE ポリシーは PCE コンフィギュレーション モードで入力されます。SR-TE ポリシーの設定に関する詳細については、SR-TE ポリシーの概要 （41 ページ）を参照してください。

PCE は、トラフィック需要やリンク使用率などのネットワーク情報を収集します。PCE はリンクが輻輳していると判断すると、輻輳の原因となっている 1 つ以上のフローを特定します。PCE は適切なパスを見つけ、ネットワークの別の部分に輻輳を移動せずに、そのフローを転送するように SR-TE ポリシーを展開します。リンクの輻輳がない場合、ポリシーは削除されます。

ネットワーク タッチ ポイントの数を最小限に抑えるために、ネットワーク サービス オーケストレータ（NSO）などのアプリケーションは PCE に SR-TE ポリシーを作成するように要求できます。PCE は、PCC-PCE 通信プロトコル（PCEP）を使用して SR-TE ポリシーを展開します。

1. PCE は PCInitiate メッセージを PCC に送信します。
2. PCInitiate メッセージが有効な場合、PCC は PCRpt メッセージを送信します。それ以外の場合は、PCErr メッセージが送信されます。
3. PCInitiate メッセージが受け入れられると、PCE は PCUpd メッセージを送信して SR-TE ポリシーを更新します。

SR-TE ポリシーを使用して複数の PCE を設定すると、ハイアベイラビリティを実現できます。ヘッドエンド（PCC）が 1 つの PCE との接続を失った場合、別の PCE が SR-TE ポリシーの制御を引き継ぐことになります。

設定例

PCE 開始 SR-TE ポリシーを設定するには、次の設定を完了する必要があります。

1. PCE コンフィギュレーション モードを開始します。

2. セグメント リストを作成します。
3. ポリシーを作成します。

```
/* Enter PCE configuration mode and create the SR-TE segment lists */
Router# configure
Router(config)# pce

/* Create the SR-TE segment lists */
Router(config-pce)# segment-routing
Router(config-pce-sr)# traffic-eng
Router(config-pce-sr-te)# segment-list name addr2a
Router(config-pce-sr-te-sl)# index 1 address ipv4 14.14.14.4
Router(config-pce-sr-te-sl)# exit

/* Create the SR-TE policy */
Router(config-pce-sr-te)# peer ipv4 1.1.1.1
Router(config-pce-sr-te)# policy P1
Router(config-pce-sr-te-policy)# color 2 end-point ipv4 2.2.2.2
Router(config-pce-sr-te-policy)# candidate-paths
Router(config-pce-sr-te-policy-path)# preference 50
Router(config-pce-sr-te-pp-index)# explicit segment-list addr2a
Router(config-pce-sr-te-pp-info)# end
Router(config)#
```

ランニング コンフィギュレーション

```
pce
 segment-routing
  traffic-eng
   segment-list name addr2a
    index 1 address ipv4 14.14.14.4
   !
   peer ipv4 1.1.1.1
    policy P1
     color 2 end-point ipv4 2.2.2.2
     candidate-paths
      preference 50
       explicit segment-list addr2a
      !
     !
```

PCEP 接続の ACL サポート

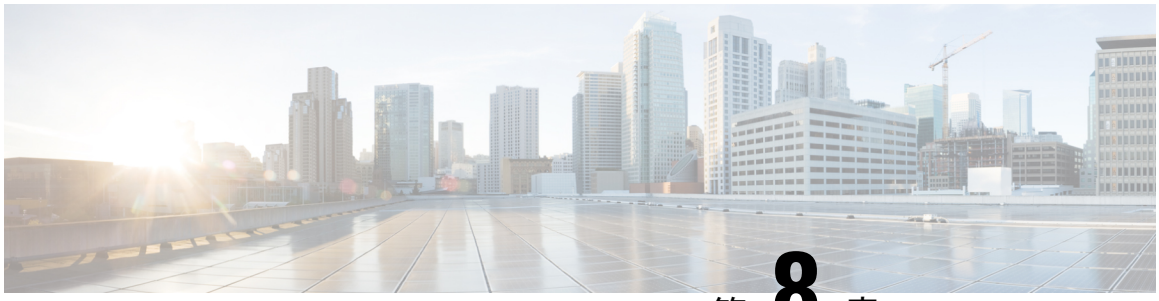
PCE プロトコル（PCEP）（RFC5440）は TCP/IP を介して実行されているクライアントサーバ モデルであり、サーバ（PCE）がポートをオープンし、クライアント（PCC）が接続を開始します。ピアが TCP 接続を確立すると、その接続上で PCE セッションを作成します。

PCEP 接続の ACL サポート機能は、アクセス コントロール リスト（ACL）を使用して PCE サーバを保護し、クライアントの送信元アドレスに基づいて TCP 接続が作成されたときに IPv4 PCC ピアを制限する方法を提供します。クライアントが TCP 接続を開始すると、ACL が参照

され、クライアントの送信元アドレスが比較されます。ACLはアドレスを許可または拒否し、TCP 接続を続行するかどうかを選択できます。

ACL 設定情報については、『*IP Addresses and Services Configuration Guide for* 』の「」の章を参照してください。

ACL を PCE に適用するには、**pce peer-filter ipv4 access-list** *acl_name* コマンドを使用します。



第 8 章

トポロジに依存しないループフリー代替（TI-LFA）の設定

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。

（注） TI-LFA は IPv4 のみをサポートします。

TI-LFA はリンク保護を提供します。リンクはコンバージェンス後のバックアップ パスの計算中に除外されます。

制限事項

サポートされるバックアップラベルは 2 個だけです。

IS-IS 用の TI-LFA 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。

始める前に

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 IS-IS で設定されている。
- IS-IS のセグメント ルーティングが設定されている。IS-IS プロトコル用のセグメント ルーティングの有効化 （11 ページ）を参照してください。
- グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
Router(config)# ipv4 unnumbered mpls traffic-eng Loopback0
Router(config)# mpls traffic-eng
Router(config-mpls-te)# exit
Router(config)#
```

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**router isis** *instance-id* 例： `RP/0/RP0/cpu 0: router(config)# router isis 1`	指定したルーティング インスタンスの IS-IS ルーティングを有効にし、ルータをルータ コンフィギュレーション モードにします。 （注） **is-type** ルータ コンフィギュレーション コマンドを使用して、特定のルーティング インスタンスによって実行されるルーティングのレベルを変更できます。
ステップ 3	**interface** *type interface-path-id* 例： `RP/0/RP0/cpu 0: router(config-isis)# interface GigabitEthernet0/0/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv4** ［**unicast**］ 例： `RP/0/RP0/cpu 0: router(config-isis-if)# address-family ipv4 unicast`	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 5	**fast-reroute per-prefix** 例：	プレフィックスごとの Fast Reroute を有効にします。

	コマンドまたはアクション	目的
	RP/0/RP0/cpu 0: router(config-isis-if-af)# **fast-reroute per-prefix**	
ステップ 6	**fast-reroute per-prefix ti-lfa** 例： RP/0/RP0/cpu 0: router(config-isis-if-af)# **fast-reroute per-prefix ti-lfa**	プレフィックスごとの TI LFA Fast Reroute リンク保護を有効にします。
ステップ 7	**fast-reroute per-prefix tiebreaker** {**node-protecting** | **srlg-disjoint**} **index** *priority* 例： RP/0/RP0/cpu 0: router(config-isis-if-af)# **fast-reroute per-prefix srlg-disjoint index 100**	TI-LFA ノードまたは SRLG 保護を有効にし、タイブレーカーの優先順位を指定します。有効な優先順位の値は 1 ～ 255 です。優先順位の値を小さくすると、ルールの優先順位が高くなります。リンク保護は、ノードまたは SRLG 保護よりも常に優先度が低くなります。 （注） インターフェイス上で同じ属性を複数回設定することはできません。

TI-LFA がセグメント ルーティング用に正常に設定されました。

OSPF 用の TI-LFA 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。

（注） TI-LFA は、インスタンス、エリア、またはインターフェイスで設定できます。インスタンスまたはエリアに設定すると、インスタンスまたはエリア内のすべてのインターフェイスが設定を継承します。

始める前に

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。

- OSPF のセグメント ルーティングが設定されている。OSPF プロトコル用のセグメント ルーティングの有効化 （27 ページ）を参照してください。
- グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
Router(config)# ipv4 unnumbered mpls traffic-eng Loopback0
Router(config)# mpls traffic-eng
Router(config-mpls-te)# exit
Router(config)#
```

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**router ospf** *process-name* 例： `RP/0/RP0/cpu 0: router(config)# router ospf 1`	指定したルーティング プロセスに OSPF ルーティングを有効にし、ルータ コンフィギュレーション モードでルータを配置します。
ステップ 3	**area** *area-id* 例： `RP/0/RP0/cpu 0: router(config-ospf)# area 1`	エリア コンフィギュレーション モードを開始します。
ステップ 4	**interface** *type interface-path-id* 例： `RP/0/RP0/cpu 0: router(config-ospf-ar)# interface GigabitEthernet0/0/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**fast-reroute per-prefix** 例： `RP/0/RP0/cpu 0: router(config-ospf-ar-if)# fast-reroute per-prefix`	プレフィックスごとの Fast Reroute を有効にします。
ステップ 6	**fast-reroute per-prefix ti-lfa** 例： `RP/0/RP0/cpu 0: router(config-ospf-ar-if)# fast-reroute per-prefix ti-lfa`	プレフィックスごとの TI LFA Fast Reroute リンク保護を有効にします。
ステップ 7	**fast-reroute per-prefix tiebreaker** {**node-protecting** | **srlg-disjoint**} **index** *priority*	TI-LFA ノードまたは SRLG 保護を有効にし、タイブレーカーの優先順位を指定します。有効な優先順位の値は 1 ～ 255

	コマンドまたはアクション	目的

	例：
	
	`RP/0/RP0/cpu 0:`
	`router(config-isis-ar-if)# fast-reroute per-prefix srlg-disjoint index 100`
		です。優先順位の値を小さくすると、ルールの優先順位が高くなります。リンク保護は、ノードまたはSRLG保護よりも常に優先度が低くなります。
		
		（注） インターフェイス上で同じ属性を複数回設定することはできません。

TI-LFA がセグメント ルーティング用に正常に設定されました。

TI-LFA ノードと SRLG の保護：例

次の例は、TI-LFA ノードと SRLG の保護に関するタイブレイカー優先順位の設定と、コンバージェンス後のバックアップ パスの動作を示しています。これらの例ではOSPF を使用していますが、IS-IS にも同じ設定と動作が適用されます。

例：リンク保護およびノード保護の TI-LFA の有効化

```
router ospf 1
 area 1
  interface GigabitEthernet0/0/2/1
    fast-reroute per-prefix
    fast-reroute per-prefix ti-lfa
    fast-reroute per-prefix tiebreaker node-protecting index 100
```

リンク保護とノード保護の両方の TI-LFA バックアップ パスが計算されます。ノード保護タイブレーカーに関連する優先順位が他のタイブレーカーよりも高い場合、ノード保護のコンバージェンス後バックアップ パスが選択されます（使用可能な場合）。

例：リンク保護および SRLG 保護の TI-LFA の有効化

```
router ospf 1
 area 1
  interface GigabitEthernet0/0/2/1
    fast-reroute per-prefix
    fast-reroute per-prefix ti-lfa
    fast-reroute per-prefix tiebreaker srlg-disjoint index 100
```

リンク保護と SRLG 保護の両方の TI-LFA バックアップ パスが計算されます。SRLG 保護タイブレーカーに関連する優先順位が他のタイブレーカーよりも高い場合、SRLG 保護のコンバージェンス後バックアップ パスが選択されます（使用可能な場合）。

例：リンク保護、ノード保護および SRLG 保護の TI-LFA の有効化

```
router ospf 1
```

```
area 1
 interface GigabitEthernet0/0/2/1
   fast-reroute per-prefix
   fast-reroute per-prefix ti-lfa
   fast-reroute per-prefix tiebreaker node-protecting index 100
   fast-reroute per-prefix tiebreaker srlg-disjoint index 200
```

リンク保護、ノード保護、および SRLG 保護の TI-LFA バックアップ パスが計算されます。ノード保護タイブレーカーに関連する優先順位がすべてのタイブレーカーで最も高い場合、ノード保護のコンバージェンス後バックアップパスが選択されます（使用可能な場合）。ノード保護のバックアップ パスが使用できない場合は、SRLG 保護のコンバージェンス後バックアップ パスが使用されます（使用可能な場合）。

グローバル重み付け SRLG 保護の設定

共有リスク リンク グループ（SRLG）は、共通のリソースを共有する一連のリンクであり、同じ障害リスクを共有します。内部ゲートウェイ プロトコル（IGP）における既存のループ フリー代替（LFA）の実装では、SRLG保護がサポートされています。ただし、既存の実装では、バックアップパスの計算中に直接接続されたリンクのみが考慮されます。したがって、直接接続されていないものの同じ SRLG を共有しているリンクが、バックアップ パスの計算中に追加された場合、SRLG 保護が失敗することがあります。グローバル重み付け SRLG 保護機能は、SRLG 値に重みを関連付けて、バックアップ パスの計算時に SRLG 値の重みを使用することにより、SRLG のパス選択を向上させることができます。

グローバル重み付け SRLG 保護をサポートするには、エリア トポロジ内のすべてのリンクで SRLG に関する情報が必要です。ISIS を使用してリモート リンクの SRLG をフラッディングすることも、リモート リンクで SRLGS を手動で設定することもできます。

設定例：グローバル重み付け SRLG 保護

グローバル重み付け SRLG 保護機能では 3 種類の設定がサポートされています。

- グローバル重み付け SRLG 保護を使用したローカル SRLG
- リモート SRLG フラッディング
- リモート SRLG スタティック プロビジョニング

次に、グローバル重み付け SRLG 保護機能を使用してローカル SRLG を設定する例を示します。

```
RP/0/RP0/CPU0:router(config)# srlg
RP/0/RP0/CPU0:router(config-srlg)# interface TenGigE0/0/0/0
RP/0/RP0/CPU0:router(config-srlg-if)# name group1
RP/0/RP0/CPU0:router(config-srlg-if)# exit
RP/0/RP0/CPU0:router(config-srlg)# interface TenGigE0/0/0/1
RP/0/RP0/CPU0:router(config-srlg-if)# name group1
RP/0/RP0/CPU0:router(config-srlg)# name group value 100
RP/0/RP0/CPU0:router(config)# router isis 1
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-if-af)# fast-reroute per-prefix srlg-protection
```

```
weighted-global
RP/0/RP0/CPU0:router(config-isis-if-af)# fast-reroute per-prefix tiebreaker srlg-disjoint
 index 1
RP/0/RP0/CPU0:router(config-isis)# interface TenGigE0/0/0/0
RP/0/RP0/CPU0:router(config-isis-if)# point-to-point
RP/0/RP0/CPU0:router(config-isis-if)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-if-af)# fast-reroute per-prefix
RP/0/RP0/CPU0:router(config-isis-if-af)# fast-reroute per-prefix ti-lfa
RP/0/RP0/CPU0:router(config-isis)# srlg
RP/0/RP0/CPU0:router(config-isis-srlg)# name group1
RP/0/RP0/CPU0:router(config-isis-srlg-name)# admin-weight 5000
```

次に、リモート SRLG フラッディングを使用してグローバル重み付け SRLG 保護機能を設定する例を示します。この設定には、ローカルおよびリモート ルータの設定が含まれています。ローカル ルータでは、**fast-reroute per-prefix srlg-protection weighted-global** コマンドを使用してグローバル重み付け SRLG 保護を有効にします。リモート ルータの設定では、**advertise application lfa link-attributes srlg** コマンドを使用して、SRLG 値のフラッディングを制御できます。また、リモート ルータで SRLG をグローバルに設定する必要もあります。

リモート SRLG フラッディングを使用したグローバル重み付け SRLG 保護のローカル ルータ設定は、次のとおりです。

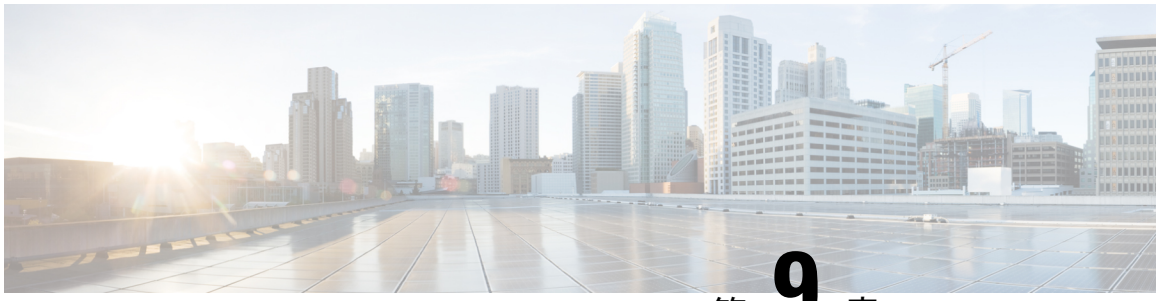
```
RP/0/RP0/CPU0:router(config)# router isis 1
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-if-af)# fast-reroute per-prefix srlg-protection
weighted-global
RP/0/RP0/CPU0:router(config-isis-if-af)# fast-reroute per-prefix tiebreaker srlg-disjoint
 index 1
RP/0/RP0/CPU0:router(config-isis-if-af)# exit
RP/0/RP0/CPU0:router(config-isis)# interface TenGigE0/0/0/0
RP/0/RP0/CPU0:router(config-isis-if)# point-to-point
RP/0/RP0/CPU0:router(config-isis-if)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-if-af)# fast-reroute per-prefix
RP/0/RP0/CPU0:router(config-isis-if-af)# fast-reroute per-prefix ti-lfa
RP/0/RP0/CPU0:router(config-isis-if-af)# exit
RP/0/RP0/CPU0:router(config-isis)# srlg
RP/0/RP0/CPU0:router(config-isis-srlg)# name group1
RP/0/RP0/CPU0:router(config-isis-srlg-name)# admin-weight 5000
```

リモート SRLG フラッディングを使用したグローバル重み付け SRLG 保護のリモート ルータ設定は、次のとおりです。

```
RP/0/RP0/CPU0:router(config)# srlg
RP/0/RP0/CPU0:router(config-srlg)# interface TenGigE0/0/0/0
RP/0/RP0/CPU0:router(config-srlg-if)# name group1
RP/0/RP0/CPU0:router(config-srlg-if)# exit
RP/0/RP0/CPU0:router(config-srlg)# interface TenGigE0/0/0/1
RP/0/RP0/CPU0:router(config-srlg-if)# name group1
RP/0/RP0/CPU0:router(config-srlg)# name group value 100
RP/0/RP0/CPU0:router(config-srlg)# exit
RP/0/RP0/CPU0:router(config)# router isis 1
RP/0/RP0/CPU0:(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# advertise application lfa link-attributes srlg
```

次に、リモート リンクの SRLG 値のスタティックプロビジョニングを使用したグローバル重み付け SRLG 保護機能の設定例を示します。これらの設定はローカル ルータで行う必要があります。

```
RP/0/RP0/CPU0:router(config)# srlg
RP/0/RP0/CPU0:router(config-srlg)# interface TenGigE0/0/0/0
RP/0/RP0/CPU0:router(config-srlg-if)# name group1
RP/0/RP0/CPU0:router(config-srlg-if)# exit
RP/0/RP0/CPU0:router(config-srlg)# interface TenGigE0/0/0/1
RP/0/RP0/CPU0:router(config-srlg-if)# name group1
RP/0/RP0/CPU0:router(config-srlg)# name group value 100
RP/0/RP0/CPU0:router(config-srlg)# exit
RP/0/RP0/CPU0:router(config)# router isis 1
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-if-af)# fast-reroute per-prefix srlg-protection
weighted-global
RP/0/RP0/CPU0:router(config-isis-if-af)# fast-reroute per-prefix tiebreaker srlg-disjoint
 index 1
RP/0/RP0/CPU0:router(config-isis)# interface TenGigE0/0/0/0
RP/0/RP0/CPU0:router(config-isis-if)# point-to-point
RP/0/RP0/CPU0:router(config-isis-if)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-if-af)# fast-reroute per-prefix
RP/0/RP0/CPU0:router(config-isis-if-af)# fast-reroute per-prefix ti-lfa
RP/0/RP0/CPU0:router(config-isis)# srlg
RP/0/RP0/CPU0:router(config-isis-srlg)# name group1
RP/0/RP0/CPU0:router(config-isis-srlg-name)# admin-weight 5000
RP/0/RP0/CPU0:router(config-isis-srlg-name)# static ipv4 address 10.0.4.1 next-hop ipv4
 address 10.0.4.2
RP/0/RP0/CPU0:router(config-isis-srlg-name)# static ipv4 address 10.0.4.2 next-hop ipv4
 address 10.0.4.1
```



第 9 章

セグメント ルーティング マイクロループ回避の設定

セグメント ルーティング マイクロループ回避機能により、IS-IS 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 マイクロループ回避について

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、まだ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は、トポロジの変更後にマイクロループが可能かどうかを検出します。新しいトポロジでマイクロループが発生する可能性があるとノードが計算した場合、ノードはセグメントのリストを使用して宛先へのループフリー SR-TE ポリシーパスを作成します。RIB 更新遅延タイマーの有効期限が切れた後、SR-TE ポリシーは通常の転送パスに置き換えられます。

セグメントルーティングマイクロループ回避の制限事項

IS-IS では、Incremental Shortest Path First（ISPF）が設定されている場合、セグメント ルーティング マイクロループ回避はサポートされません。

IS-IS 向けセグメント ルーティング マイクロループ回避の設定

このタスクでは、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、IS-IS のルーティング情報ベース（RIB）更新遅延値を設定する方法について説明します。

始める前に

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 IS-IS で設定されている。
- IS-IS のセグメント ルーティングが設定されている。IS-IS プロトコル用のセグメント ルーティングの有効化 （11 ページ）を参照してください。
- グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
Router(config)# ipv4 unnumbered mpls traffic-eng Loopback0
Router(config)# mpls traffic-eng
Router(config-mpls-te)# exit
Router(config)#
```

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**router isis** *instance-id* 例： `RP/0/RP0/cpu 0: router(config)# router isis 1`	指定したルーティング インスタンスの IS-IS ルーティングを有効にし、ルータをルータ コンフィギュレーション モードにします。 **is-type** ルータ コンフィギュレーション コマンドを使用して、特定のルーティング インスタンスによって実行されるルーティングのレベルを変更できます。
ステップ 3	**address-family ipv4** [**unicast**] 例： `RP/0/RP0/cpu 0: router(config-isis)# address-family ipv4 unicast`	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 4	**microloop avoidance segment-routing** 例：	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。

	コマンドまたはアクション	目的
	`RP/0/RP0/cpu 0: router(config-isis-af)#` **`microloop avoidance segment-routing`**	
ステップ 5	**microloop avoidance rib-update-delay** *delay-time* 例： `RP/0/RP0/cpu 0: router(config-isis-af)#` **`microloop avoidance rib-update-delay 3000`**	転送テーブルを更新する前に、ノードがマイクロループ回避ポリシーを使用する時間を指定します。*delay-time* の単位はミリ秒です。値の範囲は 1 ～ -60000 です。デフォルト値は 5000 です。

第 10 章

セグメント ルーティング マッピング サーバの設定

マッピング サーバは LDP とセグメント ルーティング間のインターワーキングの主要コンポーネントです。LDP ノードと相互接続できるように SR 対応ノードを有効にします。マッピング サーバは、他の非 SR 対応ノードの代わりに IGP でプレフィックスと SID のマッピングをアドバタイズします。

セグメント ルーティング マッピング サーバ

Cisco IOS XR セグメント ルーティングのマッピング サーバ機能では、プレフィックス SID が既知のプレフィックスの一部またはすべてに集中的に割り当てられます。ルータは、マッピング サーバ、マッピング クライアント、またはその両方として動作できる必要があります。

- マッピング サーバとして機能するルータでは、ユーザは、SID マッピング エントリを設定して、一部またはすべてのプレフィックスに対しプレフィックス SID を指定できます。これにより、ローカル SID マッピング ポリシーが作成されます。ローカル SID マッピング ポリシーには、重複しない SID マッピング エントリが含まれています。マッピング サーバは、ローカル SID マッピング ポリシーをマッピング クライアントにアドバタイズします。
- マッピング クライアントとして機能するルータは、マッピング サーバからリモートで受信した SID を受信して解析し、リモート SID マッピング エントリを作成します。
- マッピング サーバおよびマッピング クライアントとして機能するルータは、リモートで学習されローカルに設定されたマッピングエントリを使用して、重複しない一貫したアクティブなマッピング ポリシーを構築します。IGP インスタンスは、アクティブなマッピン

グ ポリシーを使用して、一部またはすべてのプレフィックスのプレフィックス SID を計算します。

マッピング サーバは、マッピング エントリの挿入および削除を自動的に管理して、重複しない一貫した SID マッピング エントリを含むアクティブなマッピング ポリシーを常に生成します。

- ローカルに設定されたマッピング エントリは、互いに重複してはいけません。
- マッピング サーバは、ローカルに設定されたマッピング ポリシーと、特定の IGP インスタンスからリモートで学習されたマッピング エントリを入力として受け取り、その IGP インスタンスの設定ルールに従って重複するマッピングエントリの中から単一のマッピング エントリを選択します。その結果、重複しない一貫したマッピング エントリで構成されるアクティブなマッピング ポリシーが作成されます。
- 定常状態では、少なくとも同じエリアまたはレベルにあるすべてのルータは、同一のアクティブなマッピング ポリシーを持っている必要があります。

セグメント ルーティング マッピング サーバの制約事項

- ネットワーク内のマッピング サーバの位置は重要ではありません。ただし、マッピング アドバタイズメントは通常の IGP アドバタイズメント メカニズムを使用して IGP に配布されるため、マッピング サーバにはネットワークへの IGP 隣接関係が必要です。
- マッピングサーバの役割は非常に重要です。冗長性を確保するには、ネットワーク内に複数のマッピング サーバを設定する必要があります。
- マッピング サーバ機能は、1 つの IS-IS インスタンスを通じて学習された SID マッピング エントリが、プレフィックスのプレフィックス SID を決定するために別の IS-IS インスタンスによって使用されるというシナリオをサポートしていません。たとえば、「ルータの isis 1」によってリモート ルータから学習されたマッピング エントリを使用して、「ルータ isis 2」によって FIB に学習、アドバタイズ、またはダウンロードされたプレフィックスのプレフィックス SID を計算することはできません。マッピング サーバは IS-IS 領域ごとに必要です。
- セグメント ルーティング マッピング サーバは現在、Virtual Routing and Forwarding（VRF）をサポートしていません。

セグメント ルーティングと LDP の相互運用性

IGP では、セグメント ルーティング（SR）が Label Distribution Protocol（LDP; ラベル配布プロトコル）と相互運用するためのメカニズムが提供されます。セグメント ルーティングのコントロール プレーンは、LDP と共存します。

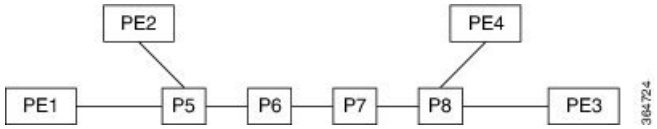
SR のセグメント ルーティング マッピング サーバ（SRMS）機能は、SR をサポートしていないネットワークの LDP 部分で、宛先に SID をアドバタイズするために使用されます。SRMS

は、そのような宛先へのセグメント識別子（SID）マッピングエントリを維持およびアドバタイズします。IGP は SRMS マッピングエントリを伝播し、SRMS と相互に作用して、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。IGP は、転送情報ベース（FIB）をプログラムするために使用されるプレフィックスと対応するラベルをルーティング情報ベース（RIB）にインストールします。

例：セグメント ルーティング LDP の相互運用性

セグメント ルーティング（SR）と Label Distribution Protocol（LDP; ラベル配布プロトコル）を混在させたネットワークを考えてみましょう。相互運用性を促進することにより、連続するマルチプロトコル ラベル スイッチング（MPLS）LSP（ラベル付きスイッチドパス）を確立できます。SR ドメイン内の 1 つ以上のノードがセグメント ルーティング マッピング サーバ（SRMS）として機能します。SRMS は、非 SR 対応ノードに代わって SID マッピングをアドバタイズします。各 SR 対応ノードは、個々のノードを明示的に構成することなく、非 SR 対応ノードに割り当てられた SID について学習します。

次の図に示すようなネットワークを考えてみましょう。このネットワークは、LDP 対応ノードと SR 対応ノードの両方を組み合わせたものです。



この混在ネットワークでは、

- ノード P6、P7、P8、PE4、および PE3 は LDP に対応しています。
- ノード PE1、PE2、P5、P6 は SR に対応しています。
- ノード PE1、PE2、P5、および P6 は、セグメント ルーティング グローバル ブロック（SRGB）が（100, 200）に設定されています。
- ノード PE1、PE2、P5、および P6 は、ノード セグメントがそれぞれ 101、102、105、106 に設定されています。

サービスフローは、連続する MPLS トンネル上で PE1 から PE3 まで確立する必要があります。これには、SR と LDP の相互運用が必要です。

LDP から SR へ

LDP から SR へのトラフィック フロー（右から左へ）では、次のような流れとなります。

1. PE3 は、nhop が PE1 であるサービス ルートを学習します。PE3 には、FEC PE1 用に nhop P8 からの LDP ラベル バインドがあります。PE3 はパケット P8 を転送します。
2. P8 には、FEC PE1 用に nhop P7 からの LDP ラベル バインドがあります。P8 はパケットを P7 に転送します。
3. P7 には、FEC PE1 用に nhop P6 からの LDP ラベル バインドがあります。P7 はパケットを P6 に転送します。

4. P6 には、FEC PE1 用の nhop P5 からの LDP バインドがありません。しかし、P6 には、IGP ルート PE1 への SR ノード セグメントがあります。P6 はパケットを P5 に転送し、等価ノード セグメント 101 によってローカル LDP ラベルを FEC PE1 と交換します。このプロセスは、ラベルのマージと呼ばれます。
5. P5 は、PE1 が最後から 2 番目のポップ フラグがセットされたノード セグメント 101 をアドバタイズしたと仮定して 101 をポップし、PE1 に転送します。
6. PE1 は、トンネリングされたパケットを受信し、サービス ラベルを処理します。

エンドツーエンドの MPLS トンネルは、PE3 から P6 までの LDP LSP と、P6 から PE1 までの関連ノード セグメントから確立されます。

SR から LDP へ

オペレータがセグメント ルーティング マッピング サーバ（SRMS）として P5 を設定し、マッピング（P7, 107）、（P8, 108）、（PE3, 103）および（PE4, 104）をアドバタイズすると仮定します。PE3 が SR 対応だった場合、オペレータは PE3 にノード セグメント 103 を設定している可能性があります。PE3 は非 SR 対応であるため、オペレータはそのポリシーを SRMS で設定します。SRMS は非 SR 対応ノードに代わってマッピングをアドバタイズします。冗長性のために、複数の SRMS サーバをネットワークにプロビジョニングできます。マッピング サーバのアドバタイズメントは、SR 対応ノードによってのみ認識されます。SR 対応ルータは、ノードセグメントがノード自体によってアドバタイズされた場合と全く同じ方法で、関連するノード セグメントを MPLS データ プレーンにインストールします。

SR から LDP へのトラフィック フロー（左から右へ）では、次のような流れとなります。

1. PE1 は、PE3 がノード セグメント 103 をアドバタイズした場合と全く同じ方法で、ノード セグメント 103 を nhop P5 でインストールします。
2. P5 は 103 を 103 と交換し、P6 に転送します。
3. IGP ルート PE3 に対する P6 の nhop は非 SR 対応です。（P7 は SR 機能をアドバタイズしません）。ただし、P6 には同じ FEC に対してその nhop からの LDP ラベル バインドがあります。（たとえば、LDP ラベル 1037）。P6 は 103 を 1037 と交換し、P7 に転送します。このプロセスをラベル マージと呼びます。
4. P7 はこのラベルを P8 から受け取った LDP ラベルと交換し、P8 に転送します。
5. P8 は LDP ラベルをポップし、PE3 に転送します。
6. PE3 はパケットを受信し、必要に応じて処理します。

エンドツーエンドの MPLS LSP は、PE1 から P6 までの SR ノード セグメントと、P6 から PE3 までの LDP LSP から確立されます。

マッピング サーバの設定

これらのタスクを実行して、マッピング サーバを設定し、プレフィックス SID マッピング エントリをアクティブなローカル マッピング ポリシーに追加します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**segment-routing** 例： `RP/0/RP0/cpu 0: router(config)# segment-routing`	セグメント ルーティングを有効にします。
ステップ 3	**mapping-server** 例： `RP/0/RP0/cpu 0: router(config-sr)# mapping-server`	マッピング サーバ コンフィギュレーション モードを有効にします。
ステップ 4	**prefix-sid-map** 例： `RP/0/RP0/cpu 0: router(config-sr-ms)# prefix-sid-map`	プレフィックス SID マッピング コンフィギュレーション モードを有効にします。 （注） 双方向プレフィックス SID は、IS-IS の下で直接、またはマッピング サーバ経由で有効にできます。

ステップ 5	**address-family ipv4 | ipv6**
	例：
	次の例に、ipv4 用のアドレスファミリを示します。
	`RP/0/RP0/cpu 0: router(config-sr-ms-map)# address-family ipv4`
	次の例に、ipv6 用のアドレスファミリを示します。
	`RP/0/RP0/cpu 0: router(config-sr-ms-map)# address-family ipv6`
		IS-IS 用のアドレスファミリを設定します。

	コマンドまたはアクション	目的

ステップ 6	*ip-address/prefix-length first-SID-value* **range** *range*
	例：
	`RP/0/RP0/cpu 0:`
	`router(config-sr-ms-map-af)#`
	`10.1.1.1/32 10 range 200`
	`RP/0/RP0/cpu 0:`
	`router(config-sr-ms-map-af)#`
	`20.1.0.0/16 400 range 300`
		アクティブなローカル マッピング ポリシーに SID マッピング エントリを追加します。設定された例では、
		• プレフィックス 10.1.1.1/32 にはプレフィックス SID 10 が割り当てられ、プレフィックス 10.1.1.2/32 にはプレフィックス SID SID 11 が割り当てられ、プレフィックス 10.1.1.199/32 にはプレフィックス SID 200 が割り当てられています。
		• プレフィックス 20.1.0.0/16 にはプレフィックス SID 400 が割り当てられ、プレフィックス 20.2.0.0/16 にはプレフィックス SID SID 401 が割り当てられ、以下同様となります。

ステップ 7	**commit**	

ステップ 8	**show segment-routing mapping-server prefix-sid-map** [**ipv4** | **ipv6**] [**detail**]
	例：
	`RP/0/RP0/cpu 0: router# show segment-routing mapping-server prefix-sid-map ipv4`
	`Prefix SID Index Range Flags`
	`20.1.1.0/24 400 300`
	`10.1.1.1/32 10 200`
	`Number of mapping entries: 2`
	`RP/0/RP0/cpu 0: router# show segment-routing mapping-server prefix-sid-map ipv4 detail`
	`Prefix`
	`20.1.1.0/24`
	`SID Index: 400`
	`Range: 300`
	`Last Prefix: 20.2.44.0/24`
	`Last SID Index: 699`
	`Flags:`
	`10.1.1.1/32`
	`SID Index: 10`
	`Range: 200`
	`Last Prefix: 10.1.1.200/32`
	`Last SID Index: 209`
	`Flags:`
	`Number of mapping entries: 2`
		ローカルで設定されたプレフィックス/SID マッピングに関する情報を表示します。
		（注） IS-IS 用のアドレス ファミリを指定します。

	コマンドまたはアクション	目的

次のタスク

IGP でローカル SID マッピング ポリシーのアドバタイズメントを有効にします。

マッピング アドバタイズメントの有効化

スタティック マッピング ポリシーの設定に加えて、IGP でマッピングのアドバタイズメントを有効にする必要があります。

IGP がローカルに設定されたプレフィックス SID マッピングをアドバタイズできるようにするには、次の手順を実行します。

IS-IS 向けマッピング アドバタイズメントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**router isis** *instance-id* **例**： `RP/0/RP0/cpu 0: router(config)# router isis 1`	指定したルーティング インスタンスの IS-IS ルーティングを有効にし、ルータをルータ コンフィギュレーション モードにします。 • **is-type** ルータ コンフィギュレーション コマンドを使用して、特定のルーティング インスタンスによって実行されるルーティングのレベルを変更できます。
ステップ 2	**address-family** { **ipv4** | **ipv6** } [**unicast**] **例**： 次に、IPv4 アドレス ファミリの例を示します。 `RP/0/RP0/cpu 0: router(config-isis)# address-family ipv4 unicast`	IPv4 または IPv6 アドレス ファミリを指定して、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 3	**segment-routing prefix-sid-map advertise-local** **例**：	ローカルに設定されたプレフィックス SID マッピングをアドバタイズするように IS-IS を設定します。

	コマンドまたはアクション	目的
	RP/0/RP0/cpu 0: router(config-isis-af)# **segment-routing prefix-sid-map advertise-local**	
ステップ 4	**commit**	
ステップ 5	**show isis database verbose** 例： RP/0/RP0/cpu 0: router# **show isis database verbose** <...removed...> SID Binding: 10.1.1.1/32 F:0 M:0 S:0 D:0 A:0 Weight:0 **Range:200** SID: **Start:10**, Algorithm:0, R:0 N:0 P:0 E:0 V:0 L:0 SID Binding: 20.1.1.0/24 F:0 M:0 S:0 D:0 A:0 Weight:0 **Range:300** SID: **Start:400**, Algorithm:0, R:0 N:0 P:0 E:0 V:0 L:0	IS-IS プレフィックス SID マッピング アドバタイズメントと TLV を表示します。

OSPF 向けマッピング アドバタイズメントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**router ospf** *process-name* 例： RP/0/RP0/cpu 0: router(config)# **router ospf 1**	指定したルーティング インスタンスに OSPF ルーティングを有効にし、ルータ コンフィギュレーション モードでルータを配置します。
ステップ 2	**segment-routing prefix-sid-map advertise-local** 例： RP/0/RP0/cpu 0: router(config-ospf)# **segment-routing prefix-sid-map advertise-local**	ローカルに設定されたプレフィックス SID マッピングをアドバタイズするように OSPF を設定します。
ステップ 3	**commit**	
ステップ 4	**show ospf database opaque-area** 例： RP/0/RP0/cpu 0: router# **show ospf**	OSPF プレフィックス SID マッピング アドバタイズメントと TLV を表示します。

	コマンドまたはアクション	目的
	database opaque-area <...removed...> Extended Prefix Range TLV: Length: 24 AF : 0 Prefix : 10.1.1.1/32 **Range Size: 200** Flags : 0x0 SID sub-TLV: Length: 8 Flags : 0x60 MTID : 0 Algo : 0 **SID Index : 10**	

マッピング クライアントの有効化

デフォルトでは、マッピング クライアント機能は有効になっています。

segment-routing prefix-sid-map receive disable コマンドを使用して、マッピング クライアント機能を無効にできます。

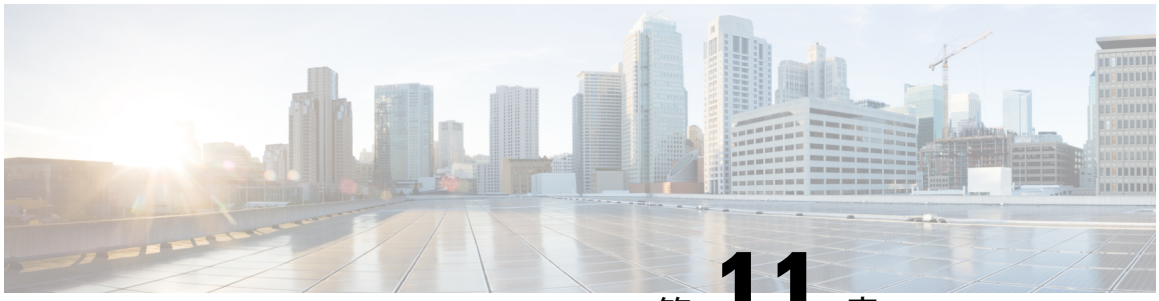
segment-routing prefix-sid-map receive コマンドを使用して、マッピング クライアント機能を再び有効にできます。

次に、IS-IS 用にマッピング クライアントを有効にする例を示します。

```
RP/0/RP0/cpu 0: router(config)# router isis 1
RP/0/RP0/cpu 0: router(config-isis)# address-family ipv4 unicast
RP/0/RP0/cpu 0: router(config-isis-af)# segment-routing prefix-sid-map receive
```

次に、OSPF 用にマッピング クライアントを有効にする例を示します。

```
RP/0/RP0/cpu 0: router(config)# router ospf 1
RP/0/RP0/cpu 0: router(config-ospf)# segment-routing prefix-sid-map receive
```



第 11 章

セグメント ルーティング OAM の使用

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、BGP プレフィックス SID、IGP プレフィックスおよびフレキシブルアルゴリズム SID と Nil-FEC（転送透過クラス）LSP ping およびトレースルート機能のサポートを提供します。

BGP および IGP プレフィックス SID 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 BGP および 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
- エニーキャスト プレフィックス SID
- BGP と LDP によってシグナリングされた LSP の組み合わせ

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。宛先 IP アドレスは 127.x.y.z/8 アドレスとして定義され、LSP が壊れている場合は IP パケットがそれ自体の宛先へ IP を切り替えないようにします。

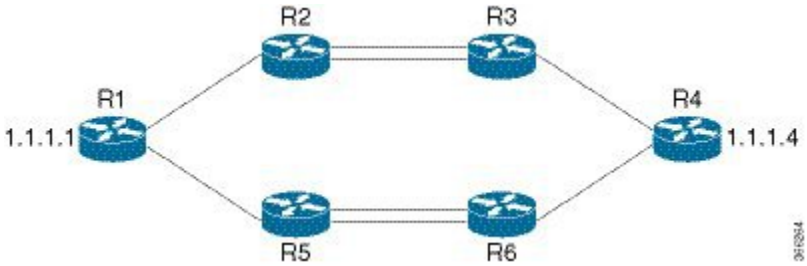
MPLS LSP traceroute 機能を使用して、LSP の障害ポイントを隔離します。これはホップバイホップ エラーのローカリゼーションとパス トレースに使用されます。MPLS LSP traceroute 機能は、エコー要求を伝送するパケットの存続可能時間（TTL）値の期限切れに依存します。MPLS エコー要求メッセージが中継ノードを見つけると TTL 値をチェックし、期限が切れている場合はコントロールプレーンにパケットが渡されます。それ以外の場合は、メッセージが転送されます。エコー メッセージがコントロール プレーンに渡されると、要求メッセージの内容に基づいて応答メッセージが生成されます。

MPLS LSP ツリー トレース（traceroute マルチパス）操作は、BGP および 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。BGP および IGP IPv4 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。BGP IPv4 プレフィックス サブ TLV には、プレフィックス SID とプレフィックス長が含まれています。

例：プレフィックス SID の MPLS Ping、Traceroute、および ツリー トレース

これらの例では、次のトポロジを使用しています。



プレフィックス SID の MPLS Ping

```
RP/0/RP0/cpu 0: router-arizona# ping mpls ipv4 1.1.1.4/32
Thu Dec 17 01:01:42.301 PST

Sending 5, 100-byte MPLS Echos to 1.1.1.4,
      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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

プレフィックス SID の MPLS Traceroute

```
RP/0/RP0/cpu 0: router-arizona# traceroute mpls ipv4 1.1.1.4/32
Thu Dec 17 14:45:05.563 PST

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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

  0 12.12.12.1 MRU 4470 [Labels: 16004 Exp: 0]
L 1 12.12.12.2 MRU 4470 [Labels: 16004 Exp: 0] 3 ms
L 2 23.23.23.3 MRU 4470 [Labels: implicit-null Exp: 0] 3 ms
! 3 34.34.34.4 11 ms
```

プレフィックス SID の MPLS ツリー トレース

```
RP/0/RP0/cpu 0: router-arizona# traceroute mpls multipath ipv4 1.1.1.4/32
Thu Dec 17 14:55:46.549 PST

Starting LSP Path Discovery for 1.1.1.4/32

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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
```

```
LL!
Path 0 found,
 output interface TenGigE0/0/0/0 nexthop 12.12.12.2  source 12.12.12.1 destination
127.0.0.0 L!
Path 1 found,
 output interface TenGigE0/0/0/0 nexthop 12.12.12.2  source 12.12.12.1 destination
127.0.0.2 LL!
Path 2 found,
 output interface TenGigE0/0/0/1 nexthop 15.15.15.5  source 15.15.15.1 destination
127.0.0.1 L!
Path 3 found,
 output interface TenGigE0/0/0/1 nexthop 15.15.15.5  source 15.15.15.1 destination
127.0.0.0

Paths (found/broken/unexplored) (4/0/0)
 Echo Request (sent/fail) (10/0)
 Echo Reply (received/timeout) (10/0)
 Total Time Elapsed 53 ms
```

MPLS LSP ping および traceroute Nil FEC ターゲット

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/Traceroute 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、オペレータに以下を指定することを許可することで、オペレータがラベル スタックを自由にテスト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。

次の表に、ping および traceroute コマンドの構文を示します。

表 *3 : LSP ping* および *traceroute Nil FEC* コマンド

コマンド構文
ping mpls nil-fec labels {*label*[**,***label*]} [**output** { **interface** *tx-interface*} [**nexthop** *nexthop-ip-addr*]]
traceroute mpls nil-fec labels {*label*[**,***label*]} [**output** { **interface** *tx-interface*} [**nexthop** *nexthop-ip-addr*]]

例：Nil_FEC ターゲットの LSP Ping および Traceroute

これらの例では、次のトポロジを使用しています。

```
Node loopback IP address: 172.18.1.3   172.18.1.4   172.18.1.5   172.18.1.7
Node label:                            16004        16005        16007
Nodes:                    Arizona ---- Utah ------- Wyoming ---- Texas

Interface:            GigabitEthernet0/0/0/1   GigabitEthernet0/0/0/1
Interface IP address:         10.1.1.3              10.1.1.4
```

```
RP/0/RP0/cpu 0: router-utah# show mpls forwarding

Tue Jul  5 13:44:31.999 EDT
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
16004  Pop         No ID              Gi0/0/0/1    10.1.1.4        1392
       Pop         No ID              Gi0/0/0/2    10.1.2.2        0
16005  16005       No ID              Gi0/0/0/0    10.1.1.4        0
       16005       No ID              Gi0/0/0/1    10.1.2.2        0
16007  16007       No ID              Gi0/0/0/0    10.1.1.4        4752
       16007       No ID              Gi0/0/0/1    10.1.2.2        0
24000  Pop         SR Adj (idx 0)     Gi0/0/0/0    10.1.1.4        0
24001  Pop         SR Adj (idx 2)     Gi0/0/0/0    10.1.1.4        0
24002  Pop         SR Adj (idx 0)     Gi0/0/0/1    10.1.2.2        0
24003  Pop         SR Adj (idx 2)     Gi0/0/0/1    10.1.2.2        0
24004  Pop         No ID              tt10         point2point     0
24005  Pop         No ID              tt11         point2point     0
24006  Pop         No ID              tt12         point2point     0
24007  Pop         No ID              tt13         point2point     0
24008  Pop         No ID              tt30         point2point     0
```

Ping Nil FEC ターゲット

```
RP/0/RP0/cpu 0: router-arizona# ping mpls nil-fec labels 16005,16007 output interface
GigabitEthernet 0/0/0/1 nexthop 10.1.1.4 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
```

Traceroute Nil FEC ターゲット

```
RP/0/RP0/cpu 0: router-arizona# traceroute mpls nil-fec labels 16005,16007 output interface
 GigabitEthernet 0/0/0/1 nexthop 10.1.1.4
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 10.1.1.3 MRU 1500 [Labels: 16005/16007/explicit-null Exp: 0/0/0]
L 1 10.1.1.4 MRU 1500 [Labels: implicit-null/16007/explicit-null Exp: 0/0/0] 1 ms
L 2 10.1.1.5 MRU 1500 [Labels: implicit-null/explicit-null Exp: 0/0] 1 ms
! 3 10.1.1.7 1 ms
```

セグメントルーティングの ping およびトレースルート

セグメント ルーティング Ping

MPLS LSP ping 機能を使用して、LSP の入力と出力の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。セグメント ルーティング ping は、セグメント ルーティング コントロール プレーン上で接続性検証を実行するための MPLS LSP ping の拡張機能です。

（注） セグメント ルーティング ping は、発信デバイスがセグメント ルーティングを実行している場合にのみ使用できます。

セグメント ルーティング ping の操作は、セグメント ルーティング コントロール プレーンが発信者側で使用可能な場合（優先されていない場合でも）にのみ開始できます。これにより、パス上でトラフィックを誘導する前に、SR パスを検証できます。セグメント ルーティング ping は、汎用 FEC タイプまたは SR コントロール プレーン FEC タイプ（SR-OSPF、SR-ISIS）のいずれかを使用できます。複数のデバイスが MPLS コントロール プレーンを実行している（LDP など）、または SR FEC を認識していない混合ネットワークでは、汎用 FEC タイプを使用することで、デバイスがエコー要求を正常に処理して応答することができます。デフォルトでは、汎用 FEC タイプがセグメント ルーティング ping エコー要求のターゲット FEC スタックで使用されます。汎用 FEC は、特定のコントロール プレーンに結合されていません。そのため、アドバタイジング プロトコルが不明の場合、またはエコー要求のパス中に変更される可能性がある場合に、パス検証を行うことができます。ターゲット FEC を指定する必要がある場合は、FEC タイプを OSPF、IS-IS、または BGP として選択できます。これにより、セグメ

ント ルーティング コントロール プレーンを実行し、セグメント ルーティング IGP FEC を理解できるデバイスだけがエコー要求に応答することが保証されます。

設定例

次の例に、セグメント ルーティング コントロール プレーンの接続性をテストするためにセグメント ルーティング ping を使用する方法を示します。最初の例では、FEC のタイプは指定されていません。他の例に示すように、FEC タイプを指定することもできます。

```
RP/0/RP0/cpu 0: router# ping sr-mpls 10.1.1.2/32

Sending 5, 100-byte MPLS Echos to 10.1.1.2/32,
      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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/5 ms

RP/0/RP0/cpu 0: router# ping sr-mpls 10.1.1.2/32 fec-type generic

Sending 5, 100-byte MPLS Echos to 10.1.1.2/32,
      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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms


RP/0/RP0/cpu 0: router# ping sr-mpls 10.1.1.2/32 fec-type igp ospf

Sending 5, 100-byte MPLS Echos to 10.1.1.2/32,
      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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms


RP/0/RP0/cpu 0: router# ping sr-mpls 10.1.1.2/32 fec-type igp isis

Sending 5, 100-byte MPLS Echos to 10.1.1.2/32,
      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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms


RP/0/RP0/cpu 0: router# ping sr-mpls 10.1.1.2/32 fec-type bgp

Sending 5, 100-byte MPLS Echos to 10.1.1.2/32,
      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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

セグメント ルーティング Traceroute

MPLS LSP traceroute 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。セグメント ルーティング traceroute 機能は、MPLS LSP traceroute 機能をセグメント ルーティング ネットワークに拡張します。

セグメント ルーティング ping と同様に、セグメント ルーティング traceroute 操作は、セグメント ルーティング コントロール プレーンが発信者側で使用可能な場合（優先されていない場合でも）にのみ開始できます。セグメント ルーティング traceroute は、汎用 FEC タイプまたは SR コントロール プレーン FEC タイプ（SR-OSPF、SR-ISIS）のいずれかを使用できます。デフォルトでは、汎用 FEC タイプがセグメント ルーティング traceroute エコー要求のターゲット FEC スタックで使用されます。ターゲット FEC を指定する必要がある場合は、FEC タイプを

OSPF、IS-IS、または BGP として選択できます。これにより、セグメント ルーティング コントロール プレーンを実行し、セグメント ルーティング IGP FEC を理解できるデバイスだけがエコー要求に応答することが保証されます。

MPLS ネットワーク内のルータにロード バランシングが存在すると、MPLS トラフィックをターゲット ルータに伝送するための代替パスが提供されます。マルチパス セグメント ルーティング traceroute 機能は、入力ルータと出力ルータ間で LSP のすべての可能なパスを検出する手段を提供します。

設定例

次の例に、セグメント ルーティング traceroute を使用して、指定された IPv4 プレフィックス SID アドレスの LSP をトレースする方法を示します。最初の例では、FEC のタイプは指定されていません。他の例に示すように、FEC タイプを指定することもできます。

```
RP/0/RP0/cpu 0: router# traceroute sr-mpls 10.1.1.2/32

Tracing MPLS Label Switched Path to 10.1.1.2/32, 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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

  0 10.12.12.1 MRU 1500 [Labels: implicit-null Exp: 0]
! 1 10.12.12.2 3 ms


RP/0/RP0/cpu 0: router# traceroute sr-mpls 10.1.1.2/32  fec-type generic

Tracing MPLS Label Switched Path to 10.1.1.2/32, 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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

  0 10.12.12.1 MRU 1500 [Labels: implicit-null Exp: 0]
! 1 10.12.12.2 2 ms


RP/0/RP0/cpu 0: router# traceroute sr-mpls 10.1.1.2/32  fec-type  igp ospf

Tracing MPLS Label Switched Path to 10.1.1.2/32, 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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
```

```
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

  0 10.12.12.1 MRU 1500 [Labels: implicit-null Exp: 0]
! 1 10.12.12.2 2 ms


RP/0/RP0/cpu 0: router# traceroute sr-mpls 10.1.1.2/32  fec-type  igp isis

Tracing MPLS Label Switched Path to 10.1.1.2/32, 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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

  0 10.12.12.1 MRU 1500 [Labels: implicit-null Exp: 0]
! 1 10.12.12.2 2 ms


RP/0/RP0/cpu 0: router#traceroute sr-mpls 10.1.1.2/32 fec-type bgp


Tracing MPLS Label Switched Path to 10.1.1.2/32, 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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.


  0 10.12.12.1 MRU 1500 [Labels: implicit-null/implicit-null Exp: 0/0]
! 1 10.12.12.2 2 ms
```

次の例に、マルチパス traceroute を使用して、IPv4 プレフィックス SID に可能なすべてのパスを検出する方法を示します。

```
RP/0/RP0/cpu 0: router# traceroute sr-mpls multipath 10.1.1.2/32

Starting LSP Path Discovery for 10.1.1.2/32

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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!
Path 0 found,
```

```
 output interface GigabitEthernet0/0/0/2 nexthop 10.13.13.2
source 10.13.13.1 destination 127.0.0.0
!
Path 1 found,
 output interface Bundle-Ether1 nexthop 10.12.12.2
source 10.12.12.1 destination 127.0.0.0

Paths (found/broken/unexplored) (2/0/0)
Echo Request (sent/fail) (2/0)
Echo Reply (received/timeout) (2/0)
Total Time Elapsed 14 ms
```

フレキシブルアルゴリズムのセグメントルーティングの ping およびトレースルート

フレキシブルアルゴリズムの検証方法は、IPアドレスに基づいているのではなく、セグメント識別子（SID）ラベルとラベルアサイナに基づいています。アサイナは、SR-PCEデータベースによって提供されたトポロジプレフィックス情報と照合して検証されます。アサイナが有効な場合は、指定されたラベルもSR-PCEデータベースと照合して検証されます。出力側では、新しいSR ラベルサブ TLV に宛先ラベルが含まれています。このラベルは、SR-PCE によって提供される SID リストと照合して検証されます。

（注） 次の注意事項および制約事項を確認します。

- エリア内のすべてのルータが同じフレキシブルアルゴリズムの定義を共有して、フレキシブルアルゴリズムが有効になっている必要があります。
- ドメイン内のすべてのルータが同じSRGB範囲の値を使用して設定されている必要があります。
- プレフィックスのSIDとフレキシブルアルゴリズムのSIDのみがサポートされています。
- サポートされるのは、1 つのラベルスタックのみです。

フレキシブルアルゴリズムのセグメントルーティングの ping

```
Router# ping sr-mpls labels 16131 lsp-end-point 1.1.1.5
Fri Dec 13 19:26:29.517 IST

Sending 5, 100-byte MPLS Echos with SR Label FEC with lsp end point 1.1.1.5, SID Label(s)
 [16131],
      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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
```

```
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/6 ms
```

フレキシブルアルゴリズムのセグメントルーティングのトレースルート

```
Router# traceroute sr-mpls labels 16130 lsp-end-point 1.1.1.5
Fri Dec 13 19:26:59.368 IST

Tracing MPLS Label Switched Path to SR Label FEC with lsp end point 1.1.1.5, SID Label(s)
 [16130], 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 rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

  0 13.13.13.1 MRU 1500 [Labels: 16130 Exp: 0]
L 1 13.13.13.3 MRU 1500 [Labels: 16130 Exp: 0] 5 ms
L 2 16.16.16.4 MRU 1500 [Labels: implicit-null Exp: 0] 4 ms
! 3 18.18.18.5 4 ms
```

IPv6 OAM を介したセグメント ルーティング

IPv6 データ プレーンを介したセグメント ルーティング（SRv6）の実装では、新しいタイプのルーティング拡張ヘッダーが追加されます。そのため、pingやtracerouteなどの既存のICMPv6メカニズムをSRv6ネットワークで使用できます。pingとtraceroute操作がSRv6ネットワーク内のIPv6対応またはSRv6対応ノードに対して動作する方法に変更はありません。

制約事項および使用上の注意事項

SRv6 OAMには、次の制限が適用されます。

- SRv6 SIDへのpingはサポートされていません。

例：SRv6 OAM

次に、SRv6ネットワークでpingを使用する例を示します。

```
RP/0/RP0/CPU0:Router# ping ipv6 2001::33:33:33:33
Mon Sep 17 20:04:10.068 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::33:33:33:33, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

次に、SRv6 ネットワークで traceroute を使用する例を示します。

```
RP/0/RP0/CPU0:Router# traceroute ipv6 2001::33:33:33:33 probe 1 timeout 0 srv6
Fri Sep 14 15:59:25.170 UTC
Type escape sequence to abort.
Tracing the route to 2001::33:33:33:33
 1  2001::22:22:22:22[IP tunnel: DA=cafe:0:0:a4:1:::: SRH =(2001::33:33:33:33   ,SL=1)]
 2 msec
 2  2001::2:2:2:2[IP tunnel: DA=cafe:0:0:a4:1:::: SRH =(2001::33:33:33:33   ,SL=1)] 2
msec
 3  2001::44:44:44:44 2 msec
 4  2001::33:33:33:33 3 msec
```

次に、SRH を使用しない SRv6 ネットワークで traceroute を使用する例を示します。

```
RP/0/RSP1/CPU0:Router# traceroute ipv6 2001::44:44:44:44 srv6
Wed Jan 16 14:35:27.511 UTC
Type escape sequence to abort.
Tracing the route to 2001::44:44:44:44
 1 2001::2:2:2:2 3 msec 2 msec 2 msec
 2 2001::44:44:44:44 3 msec 3 msec 3 msec
```

次に、VRF で指定した IP アドレスに対して ping を使用する例を示します。

```
RP/0/RP0/CPU0:Router# ping 10.15.15.1 vrf red
Mon Sep 17 20:07:10.085 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.15.15.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

次に、VRF で指定した IP アドレスに対して traceroute を使用する例を示します。

```
RP/0/RP0/CPU0:Router# traceroute 10.15.15.1 vrf red
Mon Sep 17 20:07:18.478 UTC

Type escape sequence to abort.
Tracing the route to 10.15.15.1
 1  10.15.15.1 3 msec  2 msec  2 msec
```

次に、VRF の CE1（4.4.4.5）から CE2（5.5.5.5）に対して traceroute を使用する例を示します。

```
RP/0/RP0/CPU0:Router# traceroute 5.5.5.5 vrf a
Wed Jan 16 15:08:46.264 UTC

Type escape sequence to abort.
Tracing the route to 5.5.5.5
 1  14.14.14.1 5 msec 1 msec 1 msec
 2  15.15.15.1 3 msec 2 msec 2 msec
 3  15.15.15.2 2 msec * 3 msec
```

セグメント ルーティング データ プレーンのモニタリング

MPLS ネットワークのトラフィックブラックホールは、検出して分離することが難しい場合があります。この原因としては、ユーザの設定、同期されていないネイバー、データプレーンの不適切なプログラミングなどが挙げられます。セグメント ルーティング データ プレーンのモニタリング（SR DPM）は、データプレーンの整合性検査とトラフィックブラックホールの検出に対応できる拡張性の高いソリューションを提供します。SR DPM は、SR IGP プレフィックス SID に関連付けられているすべての FIB エントリの実際のデータプレーンステータスを検証します。

SR DPM の主な利点は、次のとおりです。

- **自動化**：ノードで、中継トラフィックによって実行される実際の転送エントリの整合性が自動的に確認されます。
- **包括的なカバレッジ**：テストにより、アップストリームネイバーとダウンストリームネイバーの各組み合わせで、また考えられるすべての ECMP で、宛先プレフィックスのセットごとに転送の一貫性が検証されます。
- **拡張性**：SR DPM は、その局所的な検出プロセスにより、拡張性に優れたソリューションとなっています。
- **プロアクティブ動作モードとリアクティブ動作モード**：継続的な検証とオンデマンド検証の両方に対応しています。
- **標準規格に準拠**：SR DPM では、既存の MPLS OAM ツールを使用し、SR を活用して、テストトラフィックパスを適用します。

DPM は、次の 2 つのフェーズでデータプレーンの検証を実行します。

- 隣接関係検証：隣接関係検証では、特別な MPLS エコー要求パケットを使用して、すべてのローカルリンクがネイバーからの MPLS トラフィックを正しく転送および受信できることを確認します。また、DPM がすべてのローカル隣接関係 SID ラベルを検証できること、および不整合にフラグを設定できることも確認されます。この不整合には、トラフィックのドロップ、ローカルデバイスまたはネイバーデバイスによる指定の隣接関係に関連しない誤ったネイバーへの転送、ローカルデバイスまたはネイバーデバイスによる正しいネイバーへの転送だが指定の隣接関係に関連しない誤ったリンクの経由などが含まれます。
  DPM は、リンクごとに次の隣接関係（使用可能な場合）を検証します。
  - 保護されていない隣接関係
  - 保護された隣接関係
  - 静的な隣接関係
  - 動的な隣接関係
  - 共有の隣接関係

（注） 隣接関係検証には次の制限事項があります。

- 隣接関係検証フェーズでは、IGP（OSPF および IS-IS）インスタンスに参加しているリンクだけが検証されます。1 つ以上のリンクが IGP に含まれていない場合、隣接関係 SID ラベルがないため、そのリンクは検証されません。
- 隣接関係検証では、ブロードキャストリンクを含む、物理リンクおよびバンドルリンクのみが検証されます。

- プレフィックス検証：プレフィックス検証では、デバイスから到達可能な IGP プレフィックス SID の転送の不整合を特定します。各プレフィックス SID のすべてのアップストリームネイバーおよびダウンストリームネイバーの組み合わせに対して検証が行われ、ダウンストリームネイバーの不整合が特定されます。プレフィックス検証フェーズでは、DPM 処理ノードで入力と出力の両方の転送チェーンを検証して、カスタマートラフィックパスをシミュレートします。

  プレフィックス検証は、DPM を実行するデバイスおよび直接のネイバーに限定されるため、エンドツーエンドのモニタリングの規模に関する制限事項の影響を受けません。

  プレフィックス検証は、特別な MPLS エコー要求を使用して隣接関係検証に基づいて実施されます。この要求はアップストリームノードに移動してから、DPM 処理ノードに戻り、直接のダウンストリームノードで存続可能時間（TTL）の期限切れとなるため、ダウンストリームへの転送パス全体が実行されます。

  （注） プレフィックス検証には次の制限事項があります。

  - プレフィックス検証は隣接関係検証に基づいて実施されるため、隣接関係検証に含まれないリンクは、プレフィックス検証では使用されません。
  - 隣接関係検証ですべての隣接関係が「問題あり」と評価された場合、プレフィックス検証は実行されません。
  - ノードに特定のノードのダウンストリームリンクしかなく、アップストリームノードがない場合（特定の PE ノードシナリオであり得る状況）、プレフィックス検証は実行されません。
  - プレフィックス検証では、TI-LFA はサポートされません。

DPM は、モニタリング対象のすべてのプレフィックスと隣接関係のデータベースを維持します。

プレフィックスデータベースへの入力は、RIB に再配布クライアントとして登録することによって行われます。そのため、DPM では、IGP が新しいプレフィックス SID を RIB にプッシュしたり既存のプレフィックス SID を削除したときや、既存のプレフィックス SID のパスが変更されたときに、データベースを常に最新の状態に保つことができます。

DPM は、次のプレフィックスデータを維持します。

- IPv4 プレフィックス
- Prefix Length
- プレフィックス SID ラベル
- エラー統計情報

また、DPM は、すべてのローカル隣接関係のリストも維持します。DPM は、ローカルリンク、各ローカル隣接関係およびリモート隣接関係のラベルと IP アドレス、エラー統計情報が格納されたデータベースを維持します。

SR-DPM の運用：例

この SR-DPM の運用例では、次のシナリオを使用します。

図 *4:* テストパターン *A* のパス

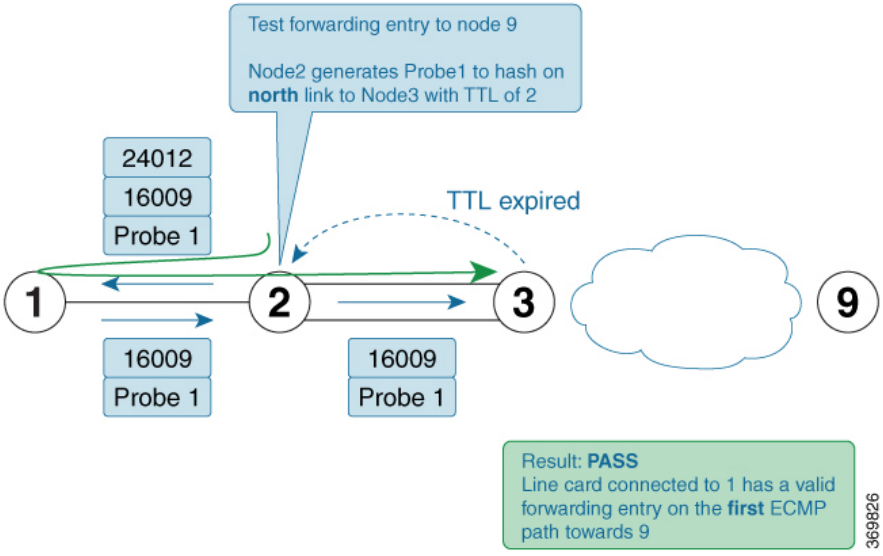
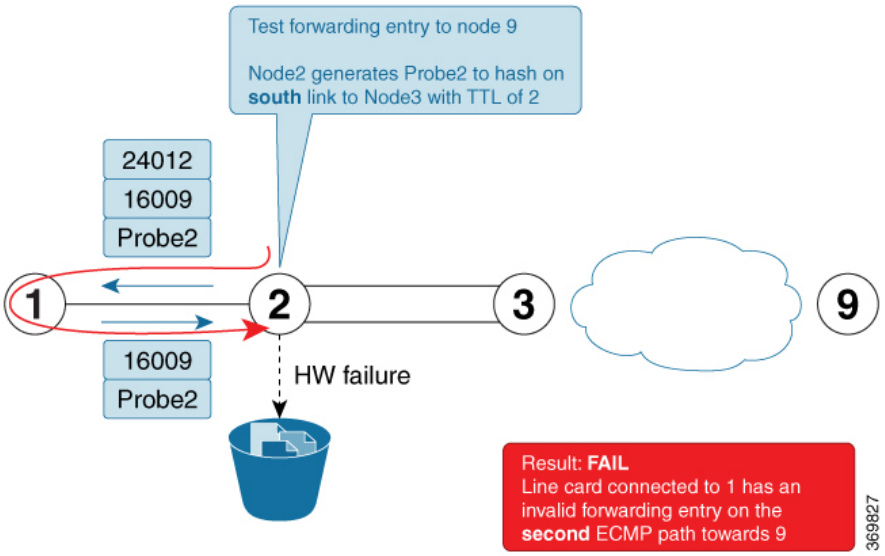


図 *5:* テストパターン *B* のパス



ノード 2 は、DPM 対応デバイスです。ネットワーク内のすべてのプレフィックス SID について転送整合性テストを実行するために、DPM は**プロアクティブモードで**有効化されます。宛先プレフィックスごとに、ルータは、特定の宛先に到達するために使用する、直接接続されたアップストリームネイバーとダウンストリームネイバーを識別します。

ノード 9 をテスト対象のプレフィックスとして使用し（プレフィックス SID = 16009）、ノード 1 をアップストリームノードとして、ノード 3 を 2 つの ECMP を持つダウンストリームノードとして使用します。

1. ノード 2 は、アップストリームとダウンストリームのすべての組み合わせで転送をテストするために、テストトラフィック（ノード 2 の source_ip（送信元 IP）を使用した MPLS OAM ping）を生成します。この場合、次の 2 つの組み合わせが存在します。
   - プレフィックス SID ノード 9：テストパターン A のパス = ノード 2、ノード 1、ノード 2、ノード 3 の順に移動（**上**の ECMP を経由）
   - プレフィックス SID ノード 9：テストパターン B のパス = ノード 2、ノード 1、ノード 2、ノード 3 の順に移動（**下**の ECMP を経由）

2. ノード 2 は、テストトラフィックの目的のパスを適用するために、ラベルスタックを追加します。たとえば、テストパターン A とテストパターン B に対して、次の 2 つのラベルがパケットに追加されます。
   - トップラベルは、ノード 2 向けのインターフェイスに対する、ノード 1 の隣接関係 SID と同じです（隣接関係 SID = 24012）。ボトムラベルは、テスト対象のプレフィックス SID です（16009）。テストトラフィックは、ノード 1 向けのインターフェイス上で送信されます。
   - トップラベル（ノード 1 でポップされた後）により、テストトラフィックはノード 2 に戻ります。このリターントラフィックは、テスト対象のプレフィックス SID（16009）の転送エントリに基づいて、完全にハードウェアスイッチングされます。ラベル付き

のテストトラフィックは、存続可能時間（TTL）が 2 であり、ダウンストリームルータを越えて転送されることはない点に注意してください。

- テストトラフィックがノード 3 に到達すると、TTL 期限切れの応答がノード 2 に返送されます。期待されるインターフェイス（上の ECMP リンク）を介して応答パケットが到着した場合、ノード 9 への最初のパターンにおけるノード 2 での転送検証は成功と見なされます。
- この例のテストパターン A とテストパターン B のテストトラフィックの違いは、MPLS OAM ping の destination_ip（宛先 IP）です。ノード 2 は、この順序で計算を行い、指定された ECMP パス（存在する場合）が実行されるようにします。したがって、パターン A のテストトラフィックは上の ECMP リンクにハッシュされ、パターン B のテストトラフィックは下の ECMP リンクにハッシュされます。

3. ネットワーク内の残りのプレフィックス SID に対して、DPM テストが繰り返されます。

SR DPM の設定

SR-DPM を設定するには、次の手順を実行します。

- SR DPM の有効化
- SR DPM インターバルタイマーの設定
- SR DPM レート制限の設定

SR DPM の有効化

mpls oam dpm コマンドを使用して、SR DPM を有効にし、MPLS OAM DPM コマンドモードを開始します。

```
Router(config)# mpls oam dpm
Router(config-oam-dpm)#
```

SR DPM インターバルタイマーの設定

MPLS OAM DPM コマンドモードで **interval** *minutes* コマンドを使用して、DPM スキャンの実行頻度を指定します。範囲は 1 ～ 3600 分です。デフォルトは 30 分です。

```
Router(config-oam-dpm)# interval 240
Router(config-oam-dpm#
```

SR DPM レート制限の設定

MPLS OAM DPM コマンドモードで **pps** *pps* コマンドを使用して、DPM によって生成されるエコー要求の 1 秒あたりパケット数（PPS）を制限します。範囲は、1 ～ 250 PPS です。デフォルトは 50 PPS です。

（注） 指定したレート制限がMPLS OAM要求全体のレート制限を超えている場合は、エラーメッセージが表示されます。

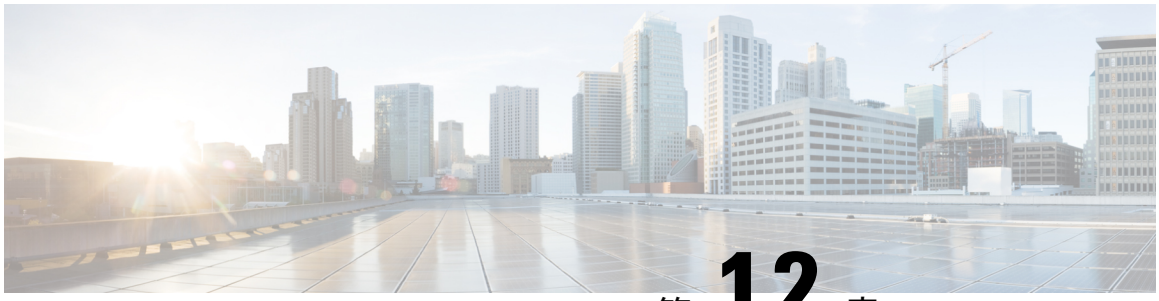
```
Router(config-oam-dpm)# pps 45
Router(config-oam-dpm#
```

確認

```
Router# show mpls oam dpm summary
  Displays the overall status of SR-DPM from the last run.
Router# show mpls oam dpm adjacency summary
  Displays the result of DPM adjacency SID verification for all local interfaces from
the last run.
Router# show mpls oam dpm adjacency interface
  Displays the result of DPM adjacency SID verification for all adjacencies for the
specified local interface.
Router# show mpls oam dpm counters
  Outputs various counters for DPM from last run as well as since the start of DPM
process.
Router# show mpls oam dpm prefix summary
  Displays the result of DPM prefix SID verification for all reachable IGP prefix SIDs
from the last run.
Router# show mpls oam dpm prefix prefix
  Displays the result of DPM prefix SID verification for the specified prefix including
 all upstream and downstream combinations.
Router# show mpls oam dpm trace
  Returns logged traces for DPM.
```

さらに、DPM カウンタを指定できるように既存の **show mpls oam** コマンドが拡張されています。

```
Router# show mpls oam counters packet dpm
```



第 12 章

セグメント ルーティング フレキシブル アルゴリズムの有効化

セグメントルーティングフレキシブルアルゴリズムを使用すると、オペレータは、独自のニーズに応じてIGP最短パス計算をカスタマイズできます。オペレータは、リンクコストベースのSPF よりも優れた転送を実現するために、カスタムの SR プレフィックス SID を割り当てることができます。結果として、フレキシブルアルゴリズムにより、IGPから到達可能なあらゆる宛先へのトラフィック エンジニアリングに基づくパスを IGP で自動的に計算できます。

SR アーキテクチャでは、パスの計算方法を定義するアルゴリズムにプレフィックス SID が関連付けられます。フレキシブルアルゴリズムにより、ユーザが定義したメトリックタイプと制約の組み合わせに基づいて IGP でパスを計算する、ユーザ定義のアルゴリズムを実現できます。

このマニュアルでは、MPLS データプレーンでセグメント ルーティング フレキシブル アルゴリズムをサポートするための IS-IS および OSPF 拡張機能について説明します。

フレキシブルアルゴリズムの前提条件

フレキシブルアルゴリズム機能をアクティブ化する前に、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。

セグメント ルーティング フレキシブル アルゴリズムの構成要素

このセクションでは、IS-IS および OSPF で SR フレキシブルアルゴリズム機能をサポートするために必要な構成要素について説明します。

フレキシブルアルゴリズムの定義

ネットワーク上のパスを計算するために、考えられる多くの制約が使用される可能性があります。一部のネットワークは複数のプレーンを使用して展開されます。単純な形の制約は、特定のプレーンを使用することである場合もあります。より洗練された形の制約には、「RFC7810」で説明されているように、遅延など、一部の拡張メトリックが含まれます。さらに高度なケースでは、パスを制限し、特定のアフィニティを持つリンクを回避することも考えられます。また、これらを組み合わせて使用することも可能です。最大限の柔軟性を得られるように、ユーザは、アルゴリズム値とその意味の間のマッピングを定義できます。ドメイン内のすべてのルータで、特定のアルゴリズム値が持つ意味について共通の認識が確立されている場合、アルゴリズムの計算は一貫性のあるものとなり、トラフィックがループすることもありません。つまり、アルゴリズムの意味が標準によってではなく、ユーザによって定義されるため、フレキシブルアルゴリズムと呼ばれます。

フレキシブルアルゴリズムのサポートのアドバタイズメント

アルゴリズムは、IGP によるベストパスの計算方法を定義します。ルータは、ノード機能としてアルゴリズムのサポートをアドバタイズします。プレフィックス SID もアルゴリズム値とともにアドバタイズされ、アルゴリズム自体と密接に結び付けられます。

アルゴリズムは 1 つのオクテット値です。128 ～ 255 までの値が、ユーザ定義の値用に予約されており、フレキシブルアルゴリズムの表現に使用されます。

フレキシブルアルゴリズムの定義のアドバタイズメント

特定のフレキシブルアルゴリズムで計算されたパスについてループフリーの転送を実現するためには、ネットワーク内のすべてのルータでフレキシブルアルゴリズムの同じ定義を共有する必要があります。これは、各フレキシブルアルゴリズムの定義をアドバタイズする専用ルータによって実現されます。このようなアドバタイズメントでは、優先度を設定して、フレキシブルアルゴリズムごとに一貫した 1 つの定義がすべてのルータで適用されるようにします。

フレキシブルアルゴリズムの定義には以下が含まれます。

- メトリックタイプ
- アフィニティ制約

特定のフレキシブルアルゴリズムの定義をルータからアドバタイズできるようにするには、**advertise-definition** コマンドを使用します。エリア内の少なくとも 1 つのルータ、または可能であれば冗長性を確保するために2つのルータで、フレキシブルアルゴリズム定義をアドバタイズする必要があります。有効な定義がアドバタイズされない場合、フレキシブルアルゴリズムは機能しません。

フレキシブルアルゴリズムのプレフィックス SID のアドバタイズメント

フレキシブルアルゴリズム固有のパスでトラフィックを転送できるように、フレキシブルアルゴリズムに参加するすべてのルータは、プレフィックスに対してアドバタイズされるフレキシブルアルゴリズム固有のSIDのMPLSラベル付きパスを組み込みます。フレキシブルアルゴリズム固有のプレフィックスSIDがアドバタイズされるプレフィックスだけが、フレキシブルアルゴリズム固有の転送の対象となります。

フレキシブル アルゴリズム パスの計算

ルータは、複数のフレキシブルアルゴリズムのパスを計算できます。このようなフレキシブルアルゴリズムのパスを計算する前に、特定のフレキシブルアルゴリズムをサポートするようにルータを設定する必要があります。このようなフレキシブルアルゴリズムを使用する場合は、あらかじめ、フレキシブルアルゴリズムの有効な定義をルータで確立しておく必要があります。

特定のフレキシブルアルゴリズムの最短パスツリーを計算する場合は、次のようなプロセスになります。

- このようなフレキシブルアルゴリズムのサポートをアドバタイズしないすべてのノードは、トポロジからプルーニングされます。
- 除外されるアフィニティがフレキシブルアルゴリズム定義に含まれている場合、そのようなアフィニティのいずれかがアドバタイズされるすべてのリンクは、トポロジからプルーニングされます。
- ルータは、フレキシブルアルゴリズム定義の一部であるメトリックを使用します。特定のリンクに対してメトリックがアドバタイズされていない場合、そのリンクはトポロジからプルーニングされます。

IS-IS では、特定のフレキシブルアルゴリズムのループフリー代替（LFA）パス、TI-LFA バックアップパス、およびマイクロループ回避パスは、このようなフレキシブルアルゴリズムのプライマリパスの計算と同じ制約を使用して計算されます。これらのパスでは、バックアップパスまたはマイクロループ回避パスを適用するために、フレキシブルアルゴリズム用にアドバタイズされたプレフィックス SID が使用されます。

（注） フレキシブル アルゴリズム ルートの LFA、TI-LFA、およびマイクロループ回避は、OSPF ではサポートされていません。

フレキシブル アルゴリズム パスの転送エントリの組み込み

フレキシブルアルゴリズム用にアドバタイズされたプレフィックスSIDを使用して、あらゆるプレフィックスに対するフレキシブル アルゴリズム パスを転送に組み込む必要があります。フレキシブルアルゴリズムのプレフィックスSIDが不明な場合、そのようなプレフィックスの転送にフレキシブル アルゴリズム パスは組み込まれません。

フレキシブル アルゴリズム パスの MPLS から MPLS へのエントリのみが組み込まれます。IP から IP へのエントリまたは IP から MPLS へのエントリは組み込まれません。これらは、デフォルトのアルゴリズムと通常のIGPメトリックに基づいて計算されたネイティブIPGパスに従います。

フレキシブルアルゴリズムのプレフィックス SID の再配布

これまで、IS-IS インスタンスまたは IS-IS プロトコル間のプレフィックスの再配布は、SR アルゴリズム 0（通常の SPF）のプレフィックス SID に制限されていました。SR アルゴリズム 1（厳格な SPF）および SR アルゴリズム 128-255（フレキシブルアルゴリズム）のプレフィックス SID がプレフィックスとともに再配布されることはありませんでした。セグメントルーティング IS-IS フレキシブルアルゴリズムのプレフィックス SID の再配布機能により、IS-IS インスタンスまたは IS-IS プロトコル間で厳格な SPF およびフレキシブルアルゴリズムのプレフィックス SID を再配布できます。この機能は、厳格な SPF またはフレキシブルアルゴリズムの SID を使用する IS-IS ルートの再配布を設定すると、自動的に有効になります。

フレキシブルアルゴリズムの設定

（注） コマンドの使用方法については、『』を参照してください。

フレキシブルアルゴリズムを設定するには、次の ISIS および OSPF コンフィギュレーション サブモードを使用します。

flex-algo *algorithm number*

algorithm number：128 ～ 255 の値

フレキシブル アルゴリズム コンフィギュレーション モードでのコマンド

フレキシブル アルゴリズム サブモードでフレキシブルアルゴリズム定義を設定するには、次のコマンドを使用します。

- IS-IS

  metric-type delay

  （注） デフォルトでは、通常の IGP メトリックが使用されます。遅延メトリックが有効になっている場合、リンク上でアドバタイズされた遅延が、フレキシブルアルゴリズム計算のメトリックとして使用されます。

  OSPF

  metric-type {**delay** | **te-metric**}

  （注） デフォルトでは、通常の IGP メトリックが使用されます。遅延または TE メトリックが有効になっている場合、リンク上でアドバタイズされた遅延または TE メトリックが、フレキシブルアルゴリズム計算のメトリックとして使用されます。

- **affinity** { **include-any** | **include-all** | **exclude-any**} *name1, name2, …*

  name：アフィニティマップの名前

- **priority** *priority value*

  priority value：フレキシブルアルゴリズム定義の選択時に使用される優先度

IS-IS でのフレキシブルアルゴリズム定義のアドバタイズメントを有効にするには、次のコマンドを使用します。

advertise-definition

アフィニティ設定用のコマンド

アフィニティマップを定義する際は、次のコマンドを使用します。アフィニティマップは、拡張管理者グループのビットマスク内の特定のビット位置に名前を関連付けます。

affinity-map *name* **bit-position** *bit number*

- *name*：アフィニティマップの名前
- *bit number*：拡張管理者グループのビットマスク内のビット位置

アフィニティをインターフェイスに関連付けるには、次のコマンドを使用します。

affinity flex-algo *name 1, name 2, …*

name：アフィニティマップの名前

プレフィックス SID 設定用のコマンド

デフォルトおよび厳格なSPFのアルゴリズムのプレフィックスSIDをアドバタイズするには、次のコマンドを使用します。

prefix-sid [**strict-spf** | **algorithm** *algorithm-number*] [**index** | **absolute**] *sid value*

- *algorithm-number*：フレキシブルアルゴリズム番号
- *sid value*：SID 値

例：IS-IS フレキシブルアルゴリズムの設定

```
router isis 1
 affinity-map red bit-position 65
 affinity-map blue bit-position 8
 affinity-map green bit-position 201

 flex-algo 128
  advertise-definition
  affinity exclude-any red
  affinity include-any blue
 !
 flex-algo 129
  affinity exclude-any green
 !
!
address family ipv4 unicast
 segment-routing mpls
!
interface Loopback0
 address-family ipv4 unicast
  prefix-sid algorithm 128 index 100
  prefix-sid algorithm 129 index 101
!
!
interface GigabitEthernet0/0/0/0
 affinity flex-algo red
!
interface GigabitEthernet0/0/0/1
 affinity flex-algo blue red
!
interface GigabitEthernet0/0/0/2
 affinity flex-algo blue
!
```

例：OSPF フレキシブルアルゴリズムの設定

```
router ospf 1
 flex-algo 130
```

```
 priority 200
 affinity exclude-any
  red
  blue
 !
 metric-type delay
!
flex-algo 140
 affinity include-all
  green
 !
 affinity include-any
  red
 !
!

 interface Loopback0
  prefix-sid index 10
  prefix-sid strict-spf index 40
  prefix-sid algorithm 128 absolute 16128
  prefix-sid algorithm 129 index 129
  prefix-sid algorithm 200 index 20
  prefix-sid algorithm 210 index 30
 !
!

 interface GigabitEthernet0/0/0/0
  flex-algo affinity
   color red
   color blue
  !
 !

affinity-map
 color red bit-position 10
 color blue bit-position 11
!
```

例：フレキシブルアルゴリズムパスへのトラフィックのステアリング

PE 上の BGP ルート：カラーベースのステアリング

SR-TE オンデマンドネクストホップ（ODN）機能を使用すると、BGP トラフィックをフレキシブル アルゴリズム パスに誘導できます。

次の設定例は、トポロジ内の 2 つのルータ、R1（2.2.2.2）と R2（4.4.4.4）を前提として、BGP ステアリング ローカル ポリシーを設定する方法を示しています。

ルータ R1 での設定

```
vrf Test
address-family ipv4 unicast
  import route-target
   1:150
  !
```

```
  export route-policy SET_COLOR_RED_HI_BW
  export route-target
   1:150
  !
!
!
interface Loopback0
ipv4 address 2.2.2.2 255.255.255.255
!
interface Loopback150
vrf Test
ipv4 address 2.2.2.222 255.255.255.255
!
interface TenGigE0/1/0/3/0
description exr1 to cxr1
ipv4 address 10.0.20.2 255.255.255.0
!
extcommunity-set opaque color129-red-igp
  129
end-set
!
route-policy PASS
  pass
end-policy
!
route-policy SET_COLOR_RED_HI_BW
  set extcommunity color color129-red-igp
  pass
end-policy
!
router isis 1
is-type level-2-only
net 49.0001.0000.0000.0002.00
log adjacency changes
affinity-map RED bit-position 28
flex-algo 128
  priority 228
!
address-family ipv4 unicast
  metric-style wide
  advertise link attributes
  router-id 2.2.2.2
  segment-routing mpls
!
interface Loopback0
  address-family ipv4 unicast
   prefix-sid index 2
   prefix-sid algorithm 128 index 282
  !
!
interface TenGigE0/1/0/3/0
  point-to-point
  address-family ipv4 unicast
  !
!
!
router bgp 65000
bgp router-id 2.2.2.2
address-family ipv4 unicast
!
address-family vpnv4 unicast
  retain route-target all
!
neighbor-group RR-services-group
```

```
  remote-as 65000
  update-source Loopback0
  address-family ipv4 unicast
  !
  address-family vpnv4 unicast
  !
!
neighbor 4.4.4.4
  use neighbor-group RR-services-group
!
vrf Test
  rd auto
  address-family ipv4 unicast
   redistribute connected
  !
segment-routing
traffic-eng
  logging
   policy status
  !
  segment-list sl-cxr1
   index 10 mpls label 16294
  !
  policy pol-foo
   color 129 end-point ipv4 4.4.4.4
   candidate-paths
    preference 100
     explicit segment-list sl-cxr1
     !
    !
   !
  !
!
!
```

ルータ R2 での設定

```
vrf Test
address-family ipv4 unicast
  import route-target
   1:150
  !
  export route-policy SET_COLOR_RED_HI_BW
  export route-target
   1:150
  !
!
!
interface TenGigE0/1/0/1
description cxr1 to exr1
ipv4 address 10.0.20.1 255.255.255.0
!
extcommunity-set opaque color129-red-igp
  129
end-set
!
route-policy PASS
  pass
end-policy
!
route-policy SET_COLOR_RED_HI_BW
  set extcommunity color color129-red-igp
  pass
end-policy
```

```
!
router isis 1
is-type level-2-only
net 49.0001.0000.0000.0004.00
log adjacency changes
affinity-map RED bit-position 28
affinity-map BLUE bit-position 29
affinity-map GREEN bit-position 30
flex-algo 128
  priority 228
!
flex-algo 129
  priority 229
!
flex-algo 130
  priority 230
!
address-family ipv4 unicast
  metric-style wide
  advertise link attributes
  router-id 4.4.4.4
  segment-routing mpls
!
interface Loopback0
  address-family ipv4 unicast
   prefix-sid index 4
   prefix-sid algorithm 128 index 284
   prefix-sid algorithm 129 index 294
   prefix-sid algorithm 130 index 304
  !
!
interface GigabitEthernet0/0/0/0
  point-to-point
  address-family ipv4 unicast
  !
!
interface TenGigE0/1/0/1
  point-to-point
  address-family ipv4 unicast
  !
!
router bgp 65000
bgp router-id 4.4.4.4
address-family ipv4 unicast
!
address-family vpnv4 unicast
!
neighbor-group RR-services-group
  remote-as 65000
  update-source Loopback0
  address-family ipv4 unicast
  !
  address-family vpnv4 unicast
  !
!
neighbor 1.1.1.1
  use neighbor-group RR-services-group
!
neighbor 2.2.2.2
  use neighbor-group RR-services-group
!
vrf Test
  rd auto
  address-family ipv4 unicast
```

```
   redistribute connected
  !
  neighbor 25.1.1.2
   remote-as 4
   address-family ipv4 unicast
    route-policy PASS in
    route-policy PASS out
   !
  !
!
!
segment-routing
!
end
```