



## **Cisco Crosswork Optimization Engine 3.0 ユーザーガイド**

初版：2021年11月12日

### **シスコシステムズ合同会社**

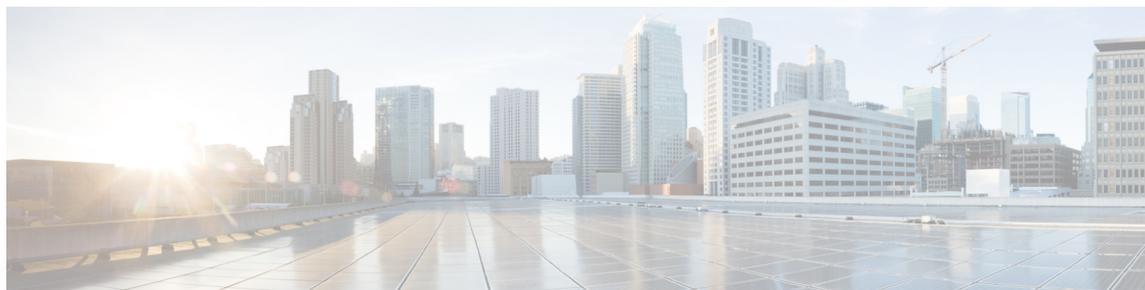
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<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

#### Cisco Crosswork Optimization Engine の概要 1

対象読者 1

Cisco Crosswork 最適化エンジンの概要 2

Crosswork Optimization Engine API 3

Crosswork Optimization Engine と Crosswork Network Controller ソリューション 3

セグメントルーティングパス計算要素 (SR-PCE) 3

セグメントルーティングについて 4

Resource Reservation Protocol (RSVP) について 7

---

### 第 2 章

#### ネットワークビューのセットアップとモニター 11

ダッシュボードでのクイックビューの取得 11

トポロジマップでのデバイスとリンクの表示 13

デバイスとリンクの詳細の表示 16

デバイスグループを使用したトポロジビューのフィルタ処理 22

デバイスグループの作成と変更 25

ダイナミック デバイス グループの有効化 26

マップ表示設定のカスタマイズ 27

リンクとデバイスの表示のカスタマイズ 27

TE トンネルのデバイスグループの表示動作の設定 28

トラフィック エンジニアリングの表示のカスタマイズ 28

タイムアウトの設定 28

簡易アクセスのトポロジビューの保存 29

---

第 3 章	<b>SR-MPLS および SRv6 ポリシーの可視化</b>	<b>31</b>
	トポロジマップでの SR-MPLS および SRv6 ポリシーの表示	32
	SR-MPLS および SRv6 ポリシーの詳細の表示	34
	トラフィック エンジニアリング デバイスの詳細の表示	36
	SR-MPLS または SRv6 ポリシーの可視化の例	37
	複数の候補パス (MCP) の検索	45
	定義済みのバインディングセグメント ID (B-SID) ラベルに関連付けられた基盤となるパスの可視化	49
	ネイティブ SR パスの可視化	51
	ネイティブパスデバイス的前提条件の可視化	53

---

第 4 章	<b>フレキシブルアルゴリズムの可視化</b>	<b>55</b>
	フレキシブルアルゴリズムの可視化	56
	フレキシブルアルゴリズムのアフィニティの設定	57
	リンクとデバイスのフレキシブルアルゴリズムの検索	59

---

第 5 章	<b>RSVP-TE トンネルの可視化</b>	<b>63</b>
	トポロジマップでの RSVP-TE トンネルの表示	63
	RSVP-TE トンネルの詳細の表示	66
	トラフィック エンジニアリング デバイスの詳細の表示	68

---

第 6 章	<b>SR-MPLS ポリシーのプロビジョニング</b>	<b>71</b>
	SR-MPLS ポリシーのサポート	71
	SR-TE ポリシー設定のソース	74
	PCC によって開始された SR-TE ポリシーの例	74
	明示的 SR-MPLS ポリシーの作成	75
	リンクアフィニティの設定	75
	最適化インテントベースのダイナミック SR-MPLS ポリシーの作成	76
	SR-MPLS ポリシーの変更	78

---

第 7 章	<b>RSVP-TE トンネルのプロビジョニング</b>	<b>79</b>
	RSVP-TE トンネルのサポート	79
	RSVP-TE トンネル設定のソース	81
	PCC によって開始された RSVP-TE トンネルの例	81
	明示的 RSVP-TE トンネルの作成	81
	リンクアフィニティの設定	82
	最適化インテントベースのダイナミック RSVP-TE トンネルの作成	83
	RSVP-TE トンネルの変更	84

---

第 8 章	<b>ローカル輻輳緩和 (LCM) を使用したローカルでのネットワーク輻輳の緩和</b>	<b>87</b>
	ローカル輻輳緩和の概要	87
	LCM に関する特記事項	88
	LCM プラットフォームの要件	89
	ASBR 間の専用 IGP インスタンスでの複数 AS ネットワークに対する BGP-LS のスピーカー配置	90
	アップグレード後における以前のモニター対象インターフェイスの欠落	90
	LCM 計算のワークフロー	91
	ローカルインターフェイスでの輻輳の緩和の例	93
	LCM の設定	100
	個別のインターフェイスしきい値の追加	102
	LCM 動作のモニター	102

---

第 9 章	<b>帯域幅最適化 (BWOpt) を使用したネットワークの最適化</b>	<b>105</b>
	帯域幅最適化の概要	105
	BWOpt に関する特記事項	106
	自動化されたネットワーク輻輳の緩和の例	107
	帯域幅最適化の設定	110
	個別のインターフェイスしきい値の追加	111
	帯域幅最適化のトラブルシューティング	111

## 第 10 章

## Intentベースの帯域幅要件の定義と維持 113

BWoD に関する特記事項 114

Intentベースの帯域幅の要件を維持するための SR-TE ポリシーのプロビジョニングの  
例 114

PCC によって開始された BWoD SR-TE のポリシー 116

オンデマンド帯域幅の設定 118

BWoD のトラブルシューティング 119





# 第 1 章

## Cisco Crosswork Optimization Engine の概要

これは、Cisco Crosswork Optimization Engine を起動して実行し、ユーザーインターフェイス (UI) の使用を開始するために必要な手順を説明する、インストール後のドキュメントです。デバイスとユーザー管理を含む管理タスクについては、[Cisco Crosswork Infrastructure](#) および [アプリケーションアドミニストレーションガイド](#)を参照してください。

- [対象読者 \(1 ページ\)](#)
- [Cisco Crosswork 最適化エンジンの概要 \(2 ページ\)](#)
- [Crosswork Optimization Engine API \(3 ページ\)](#)
- [Crosswork Optimization Engine と Crosswork Network Controller ソリューション \(3 ページ\)](#)
- [セグメントルーティングパス計算要素 \(SR-PCE\) \(3 ページ\)](#)
- [セグメントルーティングについて \(4 ページ\)](#)
- [Resource Reservation Protocol \(RSVP\) について \(7 ページ\)](#)

## 対象読者

このガイドは、ネットワークで Cisco Crosswork Optimization Engine を使用する経験豊富なネットワーク管理者を対象としています。このガイドは、次のテクノロジーの使用経験と知識があることを前提としています。

- ネットワーキングテクノロジーとプロトコル (BGP-LS、IGP (OSPF と IS-IS) 、PCEP、モデル駆動型テレメトリなど)
- トラフィック エンジニアリング (TE) トンネル
  - RSVP-TE トンネルのプロビジョニング
  - セグメントルーティング トラフィック エンジニアリング (SR-TE) ポリシーのプロビジョニング
- Cisco セグメントルーティングパス計算要素 (SR-PCE)

# Cisco Crosswork 最適化エンジンの概要

Crosswork 最適化エンジンは、一連の Cisco Crosswork ネットワークの自動化の製品の一部であり、プロアクティブなネットワークモニタリング、ネットワークの可視化、およびクローズドループの自動化により、ネットワークインテントを維持する機能を提供します。また、リアルタイムのネットワーク最適化を提供し、オペレータがネットワーク容量の使用率を効果的に最大化し、サービス速度を高められるようにします。

Crosswork 最適化エンジンは、次のとおりです。

- 次のような有益なリアルタイムのネットワーク可視化を実現するトポロジマップ
  - デバイス
  - リンクとリンク使用率
  - プロビジョニングされた SR-TE (SR-MPLS および SRv6) ポリシーと RSVP-TE トンネル
- ネットワークオペレータが次のタスクを実行できる UI
  - 直感的なワークフローを使用して SR-MPLS ポリシーと RSVP-TE トンネルをプロビジョニングし、変更または削除する
  - SR-MPLS ポリシーまたは RSVP-TE トンネルをネットワークに展開する前にプレビューする
  - SR-MPLS ポリシーのダイナミックパスの計算を継続的に追跡し、SLA の目的を維持する (正しいライセンスを使用)
  - ネットワークデバイス上で直接作成された SR-TE ポリシーと RSVP-TE トンネルを可視化し、アクティブなネットワーク設定の包括的なビューを提供する
  - ネットワークのフレキシブルアルゴリズムを可視化します。
- 他の Crosswork アプリケーションやサードパーティアプリケーションまで Crosswork 最適化エンジンの機能を拡張する API
- Crosswork 最適化エンジンの機能パック (正しいライセンスで使用可能) は、輻輳緩和とクローズドループの帯域幅最適化を提供します。ユーザーは最適化の目的を定義し、ツールはその目的を実現し、継続的にモニター、追跡、対応して元の目的を維持します。

このガイドでは、Crosswork Optimization Engine で許可される機能について説明します。ただし、ライセンス、またはユーザーアカウントに関連付けられたロールの設定により、アクセスできない機能もあります。

ライセンスと発注情報については、シスコパートナーまたはシスコの営業担当者に連絡し、Cisco Crosswork Optimization Engine 発注ガイド [英語] を参照してください。

# Crosswork Optimization Engine API

上級ユーザーは、ネットワーク操作に新しい機能を提供するアプリケーションプログラミングインターフェイス（API）を使用して、他の Crosswork アプリケーションやサードパーティアプリケーションと Crosswork 最適化エンジンの機能を統合できます。

詳細については、[Cisco DevNet の Cisco Crosswork Network Automation API ドキュメント](#)を参照してください。

## Crosswork Optimization Engine と Crosswork Network Controller ソリューション

Cisco Crosswork Network Controller は、IP トランスポートネットワークを展開および運用するためのターンキーネットワーク自動化ソリューションで、サービスの俊敏性、コスト効率、最適化の向上を実現し、お客様に届くまでの時間の迅速化して運用コストを削減します。このソリューションは、インテントベースのネットワーク自動化を組み合わせ、サービスのオーケストレーションと実現、ネットワークの最適化、サービスパスの計算、デバイスの展開と管理、および異常検出と自動修復のための重要な機能を提供します。詳細については、「[Cisco Crosswork Network Controller](#)」 [英語] を参照してください。

Crosswork Network Controller ソリューションの一部として Crosswork Optimization Engine を使用する場合は、このドキュメントで紹介している一部のオプションは使用できないか、または若干異なります。たとえば、[トラフィック エンジニアリング (Traffic Engineering)] > [トラフィック エンジニアリング (Traffic Engineering)] の代わりにトラフィック エンジニアリング UI に移動するには、Crosswork Network Controller ソリューション内で [サービスとトラフィック エンジニアリング (Services & Traffic Engineering)] > [トラフィック エンジニアリング (Traffic Engineering)] に移動します。

## セグメントルーティングパス計算要素 (SR-PCE)

Crosswork Optimization Engine は、テレメトリと Cisco セグメントルーティングパス計算要素 (SR-PCE) から収集されたデータの組み合わせを使用して、最適な TE トンネルを分析および計算します。

Cisco SR-PCE (以前の Cisco XR Traffic Controller (XTC)) は、Cisco IOS XR オペレーティングシステムで実行します。SR-PCE は、ネットワークを最適化するために TE トンネルを制御および再ルーティングするのに役立つステータス PCE 機能を提供します。PCE では、パス計算クライアント (PCC) が PCC を起点とする PCE ピアへのヘッドエンドトンネルを報告し、制御を委任する一連の手順を記述します。PCC および PCE は、更新をネットワークにプッシュするために SR-PCE が使用するパス計算要素通信プロトコル (PCEP) の接続を確立します。

Crosswork は、SR-PCE との PCEP ピアリングを確立しないデバイスを含む、IGP ドメインの一部であるすべてのデバイスを検出します。ただし、TE トンネルをデバイスに展開するには PCEP ピアリングが必要です。



(注) 詳細については、SR-PCE バージョンのサポートと互換性に関する [Crosswork Optimization Engine リリースノート \[英語\]](#) を参照してください。

## セグメントルーティングについて

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。送信元がパスを選択し、セグメントの順序付きリストとしてパケットヘッダー内でエンコードします。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。各セグメントは、32 ビットの符号なし整数で構成されるセグメント ID (SID) で識別されます。

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 (SR-TE) では、ネットワークで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、パケットで指定されている転送命令に従うだけです。

### 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。

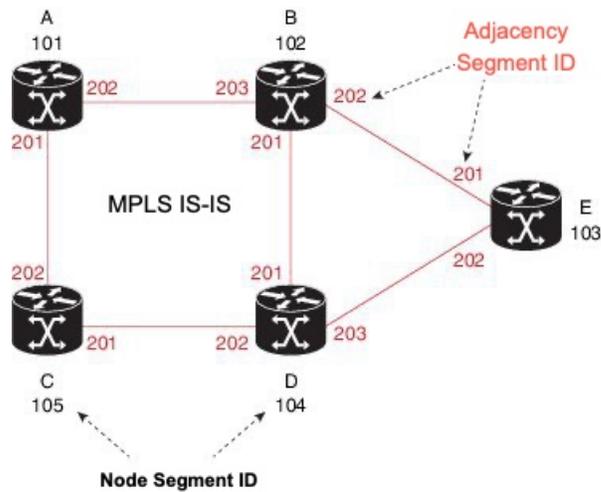
- プレフィックス SID は、IP プレフィックスに関連付けられます。プレフィックス SID は、ラベルのセグメントルーティンググローバルブロック (SRGB) の範囲から手動で設定され、IS-IS または OSPF によって配布されます。プレフィックスセグメントは、その宛先への最短パスに沿ってトラフィックを誘導します。ノード SID は、特定のノードを識別する特別なタイプのプレフィックス SID です。ノードのループバックアドレスをプレフィックスとして使用して、ループバックインターフェイスの下に設定されます。

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、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。

次の図に、各デバイスのノード SID と隣接関係 SID、およびデバイス間の接続を示す基本的なネットワークを示します。



### セグメントルーティング ポリシー

SR ポリシーパスはパス (SID リスト) を指定するセグメントのリストとして表されます。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。

SR ポリシーにはダイナミックと明示的の 2 つのタイプがあります。

#### ダイナミック SR ポリシー

動的パスは、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に関する十分な情報がない場合、ヘッドエンドはパス計算エンジン (PCE) に計算させることがあります。パスが見つからない場合、ポリシーは動作上ダウン (動作ステータスダウン) になり、パケットはポリシーに基づいてルーティングされません。

#### 明示的 SR ポリシー

明示的なポリシーを設定する場合は、プレフィックスまたは隣接 SID のリストで構成される明示的なパスを指定します。各 SID はパス上のノードまたはリンクを表します。各セグメントは、送信元から接続先までのエンドツーエンドのパスであり、ネットワーク内のルータに、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。パケットが SR 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。



- (注) PCC によって開始されたポリシーの場合、明示パスが IP アドレスの形式で設定されている場合、ホップの1つがダウンすると、ポリシーの動作ステータスはダウンになります。ラベルのリストとして設定されている場合、ポリシーは、ダウンした最初のホップである場合にのみ、動作ステータスがダウンになります。残りのホップは PCC によって解決されないため、失敗してもポリシーの動作ステータスはダウンになりません。

### Segment Routing over MPLS (SR-MPLS)

セグメントルーティングは、MPLS データプレーンに適用できます。SR-MPLS 対応ネットワークでは、MPLS ラベルは命令を表します。送信元ノードでは、パケットヘッダーの宛先へのパスがラベルのスタックとしてプログラムされます。詳細については、[IETF RFC 8660 MPLS データプレーンを使用したセグメントルーティング \[英語\]](#) を参照してください。

### Segment Routing over IPv6 (SRv6)

Segment Routing over IPv6 (SRv6) は、IPv6 データプレーンを使用してセグメントルーティングのサポートを拡張します。SRv6 にはネットワーク プログラミング フレームワークが導入されており、IPv6 パケットヘッダー内の一連の命令をエンコードすることで、ネットワークオペレータまたはアプリケーションがパケット処理プログラムを指定できます。各命令は、ネットワーク内の1つまたは複数のノードに実装され、パケット内の SRv6 セグメント識別子 (SID) によって識別されます。詳細については、[IETF RFC 8986 SRv6 ネットワークプログラミング \[英語\]](#) を参照してください。

SRv6 では、IPv6 アドレスは命令を表します。SRv6 では、命令の順序付きリストをエンコードするために、セグメントルーティングヘッダー (SRH) と呼ばれる新しいタイプの IPv6 ルーティング拡張ヘッダーが使用されます。アクティブセグメントはパケットの宛先アドレスによって示され、次のセグメントは SRH のポインタによって示されます。

詳細については、<https://www.segment-routing.net/> を参照してください。

#### SRv6 の制限事項

- Cisco IOS XR 7.3.2 では、IS-IS IGP による SRv6 可視化のみサポートされます。
- SRv6 ポリシーでのトラフィック収集は現在サポートされていません。
- OSPFv3 IGP (PCE によって開始された) SRv6 ポリシーはサポートされていません。
- SRv6 は、帯域幅最適化、オンデマンド帯域幅、またはローカル輻輳緩和機能パックではサポートされていません。
- IPv4 と IPv6 のトポロジは一致している必要があります。IPv4 と IPv6 の異なるリンクメトリックはサポートされていません。
- PCC によって開始されたダイナミックパス SRv6 ポリシーのみ可視化します。PCC によって開始されたパスと明示パスはサポートされていません。

### 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、送信元と接続先のペア間のポリシーを介して実行されます。SR-TE 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。

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。

### 分離

Crosswork では、分離ポリシーを使用して、同じ送信元と接続先からのトラフィックを誘導する2つの一意のパスを計算し、共通の指定リソース（リンクまたはノード）を回避します。これにより、ネットワークを介したトラフィックの誘導ではシングルポイント障害が発生しなくなります。次の分離パスの計算がサポートされています。

- [リンク (Link) ]: 計算されたパス上でリンクが共有されないことを指定します。
- [ノード (Node) ]: 計算されたパス上でノードが共有されないことを指定します。
- [SRLG]: 計算されたパスで同じ共有リスクリンクグループ (SRLG 値) を持つリンクが共有されないことを指定します。
- [SRLGノード (SRLG-node) ]: 計算されたパス上で SRLG とノードが共有されないことを指定します。



- (注)
- 分離は、同じ分離 ID を持つ2つのポリシーでサポートされています。
  - アフィニティと分離の同時設定はサポートされていません。

### 関連リンク

[SR-MPLS ポリシーのプロビジョニング](#) (71 ページ)

[リンクアフィニティの設定](#) (75 ページ)

## Resource Reservation Protocol (RSVP) について

リソース予約プロトコル (RSVP) は、システムによるネットワークからのリソース予約要求を可能にするシグナリングプロトコルです。RSVP は、他のシステムからのプロトコルメッセージを処理し、ローカルクライアントからのリソース要求を処理して、プロトコルメッセージを生成します。結果として、リソースは、ローカルおよびリモートクライアントの代わりにデータフローに予約されます。RSVP は、これらのリソース予約を作成、保守および削除します。

RSVP-TE プロセスには、次の機能が含まれています。

- エンドポイント制御。ヘッドエンドとテールエンドでの TE トンネルの確立と管理に関連付けられます。
- リンク管理。TE LSP のリソース認識型ルーティングを実行し、MPLS ラベルをプログラムします。
- 高速再ルーティング (FRR)。保護が必要な LSP を管理し、これらの LSP にバックアップトンネル情報を割り当てます。

TE と RSVP 間の連携動作では、TE 内にエンドポイント制御、リンク管理、および FRR 機能が存在することを前提としています。

### RSVP-TE 明示的ルーティング (ストリクト、ルーズ)

RSVP-TE の明示的ルートは、ネットワークトポロジ内の抽象ノードとして指定可能な特別なパスです。これは、明示的ルートオブジェクト (ERO) 内 IP プレフィックスのシーケンスまたは自律システムのシーケンスです。明示的パスは管理上指定することも、制約付き最短パス優先 (CSPF) などのアルゴリズムを使用して自動的に計算することもできます。

ERO で指定された明示的パスは、ストリクトパスまたはルーズパスです。

ストリクトパスとは、ERO 内のネットワークノードとその先行ノードが隣接し、直接接続されている必要があることを意味します。

ルーズホップとは、ERO で指定されたネットワークノードがパス内にある必要があるものの、その前のノードと直接接続されている必要がないことを意味します。ERO の処理中にルーズホップに遭遇した場合、ルーズホップを処理するノードは、パスに沿った、それ自身から ERO 内の次のノードまで、1 つ以上のノードを使用して ERO を更新できます。ルーズパスの利点は、ERO の作成時にパス全体を指定したり、既知にする必要がないことです。ルーズパスの欠点は、下位のルーティングプロトコルでの一時的な状態中に転送ループが発生する可能性があることです。



---

(注) RSVP-TE トンネルは、UI 内でのプロビジョニング時にルーズホップを使用して設定できません。

---

### RSVP FRR

ルータのリンクまたは隣接デバイスに障害が発生すると、インターフェイス停止の通知を受信することでルータはこの障害を検出する場合があります。インターフェイスが停止したことをルータが認識すると、ルータはそのインターフェイスを出る LSP を、それぞれのバックアップトンネルに切り替えます (バックアップトンネルがある場合)。

FRR オブジェクトは PATH メッセージ中で使用され、ファシリティバックアップとして使用されるバックアップ方式を示すフラグが格納されています。FRR オブジェクトは、セットアップと保留の優先順位を指定します。これらは、バックアップパスの選択に使用される属性フィルタと帯域幅要件のセットに含まれています。

レコードルートオブジェクト (RRO) は、LSPでのローカル保護の可用性または使用、および帯域幅とノード保護がその LSP で使用可能かどうかを RESV メッセージで報告します。

FRR 要件のシグナリングは、TE トンネルヘッドエンドで開始されます。パスに沿ったローカル修復ポイント (PLR) は、PLR でのバックアップトンネルの可用性に基づき、FRR 要件に従って動作し、バックアップトンネル選択情報をヘッドエンドにシグナリングします。FRR イベントがトリガーされると、PLR はバックアップトンネルを介して PATH メッセージをバックアップトンネルが元の LSP に再参加するマージポイント (MP) に送信します。また、MP は PATH メッセージ内の PLR によって組み込まれた RSVP-Hop オブジェクトを使用して RESV メッセージを PLR に送信します。このプロセスにより、元の LSP が MP によって切断されることを防ぎます。また、PLR は PATH-ERROR メッセージを使用してトンネルヘッドエンドにシグナリングし、LSP に沿った障害と、その LSP で FRR がアクティブに使用されていることを示します。この情報はヘッドエンドで使用され、TE トンネルの新しい LSP をシグナリングし、メイクビフォアブレイク技術によって新しい LSP がセットアップされた後に障害が発生した既存のパスを切断します。





## 第 2 章

# ネットワークビューのセットアップとモニター

---

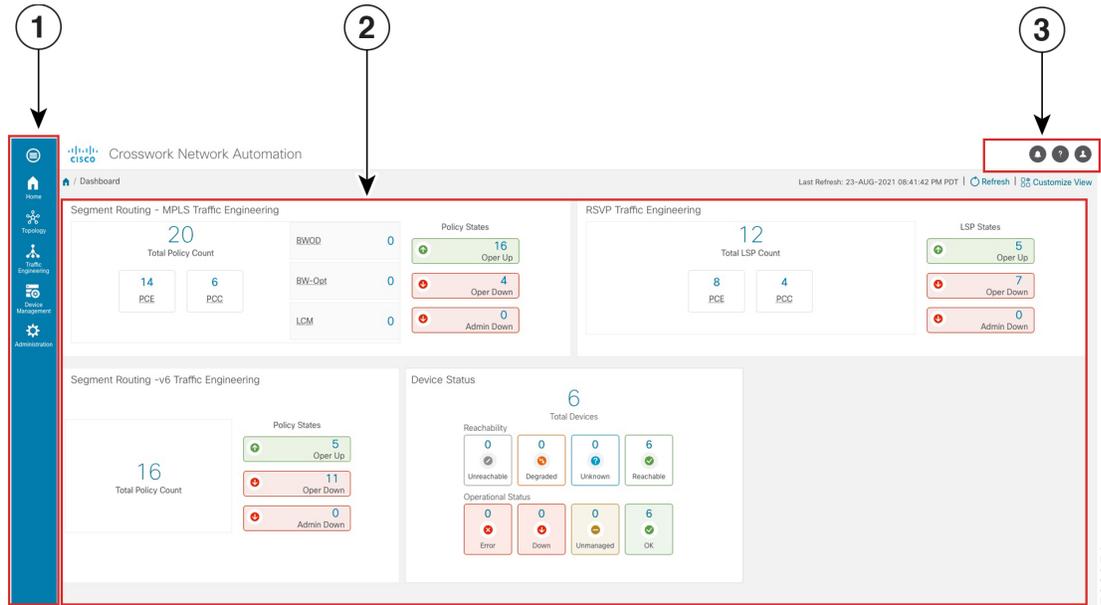
SR ポリシーと RSVP-TE トンネルを管理する前に、UI をよく理解して、ネットワークビューを設定します。ここでは、次の内容について説明します。

- [ダッシュボードでのクイックビューの取得 \(11 ページ\)](#)
- [トポロジマップでのデバイスとリンクの表示 \(13 ページ\)](#)
- [デバイスグループを使用したトポロジビューのフィルタ処理 \(22 ページ\)](#)
- [マップ表示設定のカスタマイズ \(27 ページ\)](#)
- [タイムアウトの設定 \(28 ページ\)](#)
- [簡易アクセスのトポロジビューの保存 \(29 ページ\)](#)

## ダッシュボードでのクイックビューの取得

ホームページにはカスタマイズ可能な一連のダッシュレットが表示され、デバイスの到達可能性や動作ステータスなど、管理対象ネットワークの運用の概要がひと目でわかります。各ダッシュレットには、同じカテゴリに属しているさまざまなタイプのデータが表示されます。

図 1: Crosswork のホームページ



522051

引き出し線番号	説明
1	<p><b>メインメニュー</b>：メインメニューでは、インストールされている Cisco Crosswork アプリケーションと、デバイス管理および管理のタスクに移動できます。メニューオプションは、インストールされている Cisco Crosswork アプリケーションによって若干異なる場合があります。</p>
2	<p><b>ダッシュレット</b>：情報は、インストールされている Cisco Crosswork アプリケーションによって異なります。</p> <ul style="list-style-type: none"> <li>ダッシュレット内の詳細情報をドリルダウンするには、値をクリックします。クリックしたフィルタ処理済みデータのみを表示するウィンドウが表示されます。</li> <li>ダッシュレットのレイアウトを追加または変更するには、[ビューのカスタマイズ (Customize View)] をクリックします。ダッシュレットを目的のレイアウトに移動し、[保存 (Save)] をクリックします。</li> </ul>

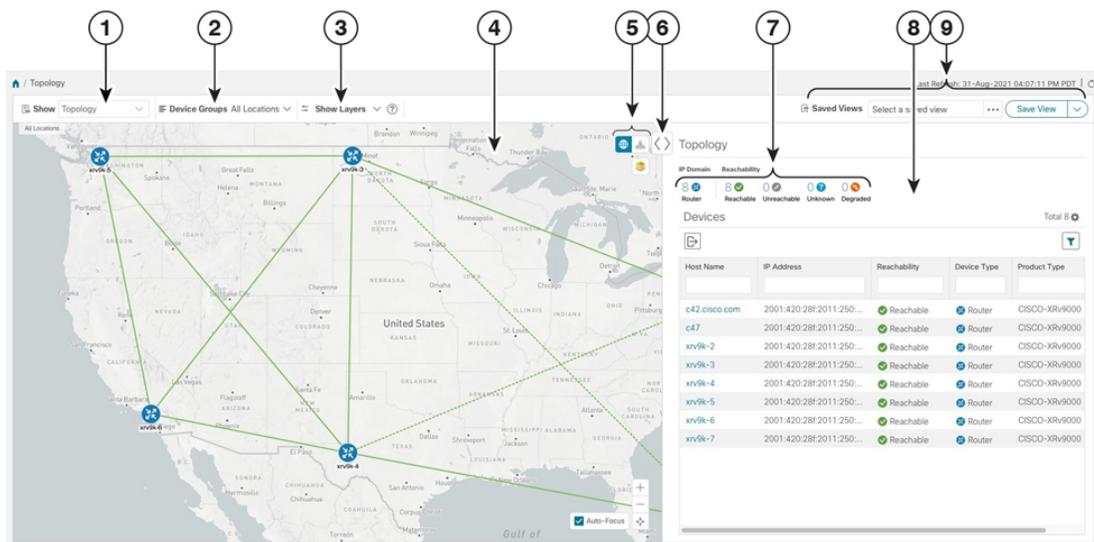
引き出し線番号	説明
3	<p>設定のアイコン：</p> <ul style="list-style-type: none"> <li>🔔 [アラート (Alerts)] アイコンは、注意が必要なシステム操作に関連する現在のエラー状態を通知し、それらの状態に関する詳細情報へのリンクを提供します。</li> <li>📅 [イベント (Events)] アイコンは、システム操作に関連する新しいイベントを通知し、すべてのシステムイベントの履歴にアクセスできるようにします。</li> <li>❓ [バージョン情報 (About)] アイコンには、Cisco Crosswork 製品の現在のバージョンが表示されます。</li> <li>👤 [ユーザーアカウント (User Account)] アイコンを使用すると、ユーザー名の表示、パスワードの変更、ログアウトを行えます。</li> </ul>

## トポロジマップでのデバイスとリンクの表示

ネットワークトポロジマップを表示するには、メインメニューから[トポロジ (Topology)] を選択します。

詳細については、「[デバイスとリンクの詳細の表示 \(16 ページ\)](#)」を参照してください。

図 2: Cisco Crosswork UI とトポロジマップ



引き出し線番号	説明
1	<p>[トポロジマップビュー (Topology Map View) ] : [表示 (Show) ] ドロップダウンリストから、マップに表示するデータを表示するオプションをクリックします。</p> <p>[トポロジ (Topology) ] を選択すると、ネットワーク内のデバイスとリンクが表示されます。</p> <p>[トラフィック エンジニアリング (Traffic Engineering) ] を選択すると、TE トンネル情報が表示されます。トラフィックエンジニアリングのトポロジマップの詳細については、「<a href="#">トポロジマップでの SR-MPLS および SRv6 ポリシーの表示 (32 ページ)</a>」および「<a href="#">トポロジマップでの RSVP-TE トンネルの表示 (63 ページ)</a>」を参照してください。</p>
2	<p>[デバイスグループ (Device Groups) ] : ドロップダウンリストから、マップに表示するデバイスのグループをクリックします。他のすべてのデバイスグループは非表示になります。</p>
3	<p>[表示/非表示 (Show/Hide) ] : ドロップダウンリストから、マップに表示するネットワークレイヤをクリックします。選択したレイヤに属するすべてのデバイスとリンクが表示されます。デフォルトでは、すべてのレイヤが表示されます。</p>

引き出し線番号	説明
4	<p>[トポロジマップ (Topology Map) ]: ネットワークトポロジは、論理マップまたは地理的マップに表示できます。ここでは、デバイスとリンクが地理的コンテキストで表示されます。マップでドリルダウンすると、デバイスとリンクに関する詳細を確認できます。</p> <p>[デバイス (Device) ]:</p> <ul style="list-style-type: none"> <li>• デバイス設定の概要を表示するには、マウスカーソルをデバイスアイコンの上に合わせます。ホスト名、状態、ノードID、およびデバイスタイプを表示するポップアップウィンドウが表示されます。</li> <li>• デバイスの詳細を表示するには、デバイスアイコンをクリックします。</li> <li>• デバイスが物理的に近接している場合、地理的なマップはそれらをクラスタとして表示します。青色の円内の番号 (4) は、クラスタ内のデバイスの数を示します。この方法でデバイスを表示すると、マップ上での重複や混乱を防ぐことができます。</li> </ul> <p>[リンク (Link) ]:</p> <ul style="list-style-type: none"> <li>• 実線は、2つのデバイス間の単一リンクを示します。2つのデバイス間、またはデバイスとデバイスのクラスタの間に複数のリンクがある場合は、代わりに線は点線で表示されます。破線は、複数のリンクを表す集約リンクか、または同じ物理リンクでの複数のプロトコル (IPv4やIPv6など) の使用を示します。</li> <li>• A と Z はそれぞれヘッドエンドとエンドポイントを示します。</li> <li>• リンク情報の詳細を表示するには、リンクをクリックします。</li> </ul> <p>(注) デュアルスタックリンクは、集約されていても1本の線で表示されます。</p>
5	<p>🏠: 論理マップは、自動レイアウトアルゴリズムに従って配置されたデバイスとそれらのリンクを示し、地理的な位置は無視されます。レイアウトアルゴリズムを変更できます。</p> <p>🌐: 地理的マップは、単一のデバイス、デバイスクラスタ、リンク、およびトンネルを世界地図に重ねて表示します。マップ上の各デバイスの位置は、デバイスインベントリで定義されているデバイスの GPS 座標 (経度と緯度) を反映します。</p> <p>⚙️: [表示設定 (Display Preferences) ] ウィンドウでは、デバイス、リンク、利用率、フレキシブルアルゴリズム、および TE トンネルメトリックの表示設定を変更できます。</p>

引き出し線番号	説明
6	[サイドパネルの展開/折りたたみ/非表示 (Expand/Collapse/Hide Side Panel) ]: サイドパネルの内容を展開するか、または折りたたみます。トポロジマップを拡大表示するには、サイドパネルを閉じます。
7	[ミニダッシュボード (Mini Dashboard) ]には、IP ドメインとデバイスの到達可能性ステータスの概要が表示されます。フィルタが適用されると、[ミニダッシュボード (Mini Dashboard) ]が更新され、[デバイス (Devices) ]テーブルに表示される内容が反映されます。
8	このウィンドウの内容は、トポロジマップの [表示 (Show) ] に設定されている内容と、デバイス、リンク、SR-MPLS ポリシー、SRv6 ポリシー、または RSVP-TE トンネルの詳細情報を表示することを選択しているかによって異なります。
9	[保存済みカスタムマップビュー (Saved Custom Map Views) ]: 現在のマップの設定とレイアウト、保存済みビューに保存されているテーブルの設定を使用して名前付きカスタムビューを作成したり、以前に作成したカスタムビューを表示できます。また、[デバイス (Devices) ]テーブルと [トラフィック エンジニアリング (Traffic Engineering) ]テーブルに適用されるフィルタもすべて保存されます。

## デバイスとリンクの詳細の表示

次に、トポロジマップを使用してデバイスとリンクの詳細 (Link Aggregation Group (LAG) の詳細を含む (ステップ 6 参照) ) を表示する例を示します。

- 
- ステップ 1** メインメニューから、[トポロジ (Topology) ]または[トラフィックエンジニアリング (Traffic Engineering) ] > [トラフィックエンジニアリング (Traffic Engineering) ]を選択します。
- ステップ 2** デバイスのホスト名、到達可能性の状態、IP アドレス、およびタイプをすばやく表示するには、デバイスアイコン上にマウスを合わせます。

The screenshot displays the network topology view with a popup window for device details. The popup shows the following information:

- Reachability State: Reachable
- Host Name: P2-ASR9k
- Node IP: 172.29.10.112
- Type: ciscoASR9001

The main interface includes a map of the United States and Mexico with various routers (ASR9k, NCS5501, XRV9k) connected by links. A table on the right lists the devices with their host names, node IPs, operational and reachability states, and product types.

Host Name	Node IP	Oper...	Reac...	Product Type
P1-ASR9k	172.29.10.111	OK	Re...	ciscoASR9001
P2-ASR9k	172.29.10.112	OK	Re...	ciscoASR9001
P3-NCS5501	172.29.10.113	OK	Re...	ciscoNCS5501
P4-NCS5501	172.29.10.114	OK	Re...	ciscoNCS5501SE
PE1-ASR9k	172.29.10.115	OK	Re...	ciscoASR9001
PE2-ASR9k	172.29.10.116	OK	Re...	ciscoASR9001
PE3-ASR9k	172.29.10.117	OK	Re...	ciscoASR9001
PE4-ASR9k.cis...	172.29.10.118	OK	Re...	ciscoASR9001
PE7-XRV9k	172.29.10.61	OK	Re...	CISCO-XRV9000
PE8-XRV9k.cis...	172.29.10.62	OK	Re...	CISCO-XRV9000
PE9-XRV9k	172.29.10.63	OK	Re...	CISCO-XRV9000

ステップ3 デバイスの詳細をさらに表示するには、デバイスアイコンをクリックします。

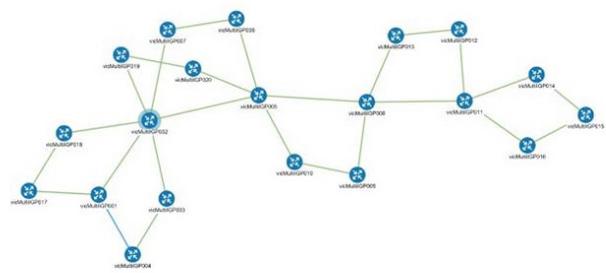
a) 次の例は、トポロジマップのデバイスの詳細を示しています。

The screenshot shows the network topology map with a detailed view of a device. The device details panel includes the following information:

- Summary**
  - Host Name: P2-ASR9k
  - Reachability State: Reachable
  - Operational State: OK
  - Node IP: 172.29.10.112
  - Civic Address: Chicago, Illinois, United States, North America, 7045
  - Geo Location: Latitude 42.030000, Longitude -88.250000
  - Device Group: All Locations > ASR9k
  - Product Type: ciscoASR9001
  - Connect To Device: Telnet IPv4, SSH IPv4
  - Last Update: 2021-Jan-08, 13:20:59 (GMT -08:00)
- Routing**
  - TE Router ID: 192.168.60.22
  - ISIS System ID: 0168.0060.0022 Level-2
  - ASN: 0

複数の IGP のセットアップでは、ルーティングの詳細ですべての IGP、IS-IS、および OSPF プロセスを表示することもできます。次の例を参照してください。

図 3: 複数の IGP : OSPF プロセス



The network diagram shows a mesh of routers labeled vicMultiGP001 through vicMultiGP017. A 'Device Details' panel is open for vicMultiGP002, showing the following configuration:

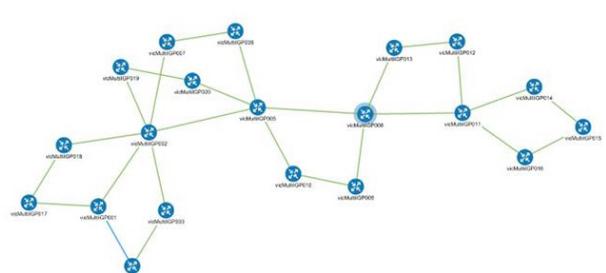
Host Name	vicMultiGP002
Reachability State	Reachable
Operational State	OK
Node IP	192.168.1.2
Geo Location	Lat. 0.000000, Lng. 0.000000
Product Type	ciscoCRS16S
Connect To Device	Telnet IPv4, SSH IPv4
Last Update	2020-Feb-27, 13:41:01 (GMT -08:00)

**Routing**

- OSPF Router ID: 192.168.1.2 Area-9911
- OSPF Router ID: 192.168.1.2 Area-9966
- OSPF Router ID: 192.168.1.2 Area-0
- OSPF Router ID: 192.168.1.2 Area-9917
- OSPF Router ID: 192.168.1.2 Area-9912

TE Router ID: 192.168.1.2  
ASN: 991

図 4: 複数の IGP : ISIS プロセス



The network diagram shows the same mesh of routers as in Figure 3. A 'Device Details' panel is open for vicMultiGP008, showing the following configuration:

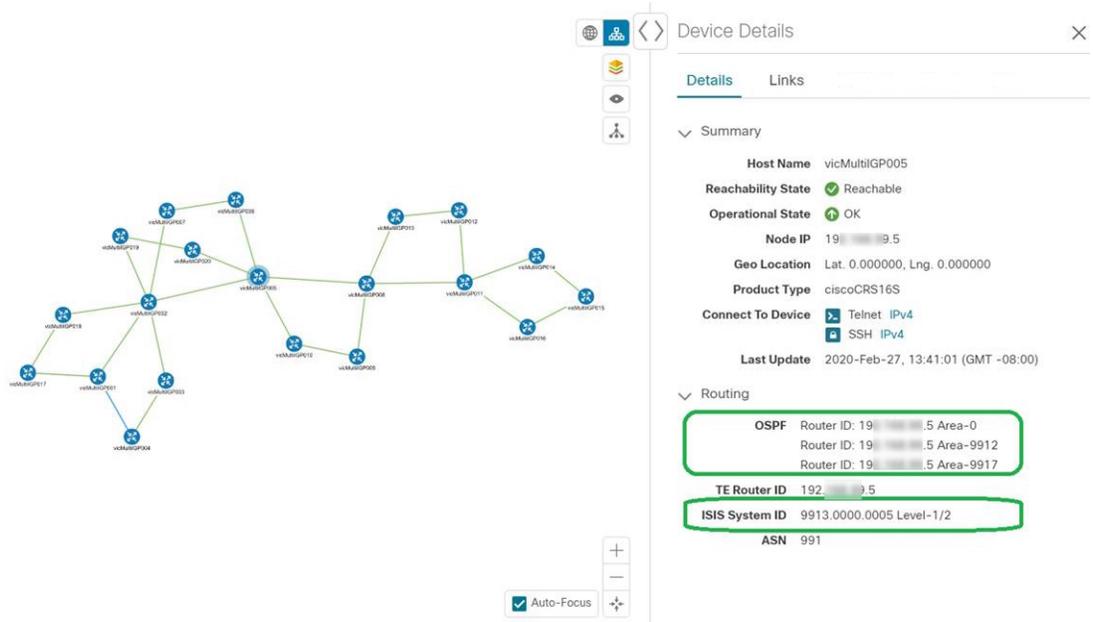
Host Name	vicMultiGP008
Reachability State	Reachable
Operational State	OK
Node IP	192.168.1.8
Geo Location	Lat. 0.000000, Lng. 0.000000
Product Type	ciscoCRS16S
Connect To Device	Telnet IPv4, SSH IPv4
Last Update	2020-Feb-27, 13:41:01 (GMT -08:00)

**Routing**

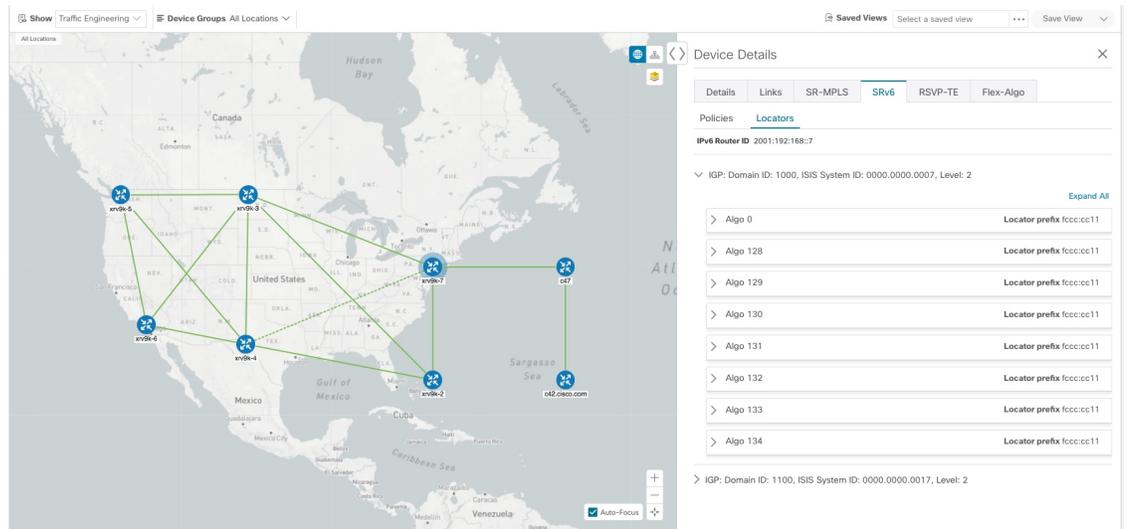
- ISIS System ID: 9913.0000.0008 Level-1/2
- ISIS System ID: 9914.0000.0008 Level-1/2

TE Router ID: 192.168.1.8  
ASN: 991

図 5: 複数の IGP : OSPF および ISIS プロセス



- b) 次の例は、トラフィック エンジニアリング マップの追加のトラフィック エンジニアリング デバイスの詳細 ([SR-MPLS]、[SRv6]、[RSVP-TE]、および [フレキシブルアルゴリズム (Flexible Algorithm)] タブ) を示しています。この例では、2つのドメインの SRv6 ローターがリストされています。



**ステップ 4** デバイスのリンクを表示するには、[リンク (Links)] タブをクリックし、右側のパネルを展開してすべてのリンクの詳細を表示します。

## デバイスとリンクの詳細の表示

Show Topology | Device Groups All Locations | Saved Views Select a saved view | Save View

Device Details

Details Links

Links on Device P2-ASR9k

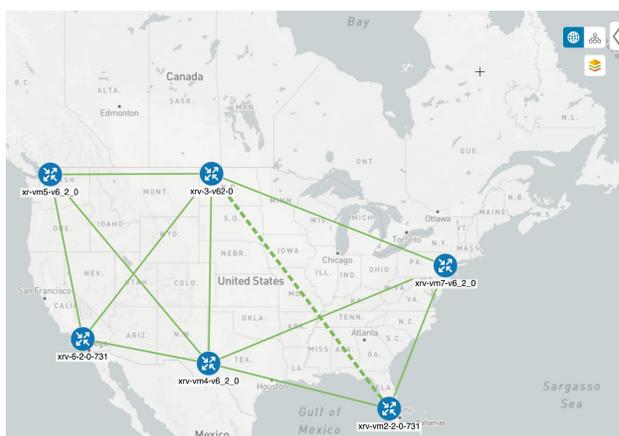
Total 14

State	Link Type	A Side Interface	Z Side Interface	A Side Utilization	Z Side Utilization
+	L3 ISIS IPV4	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/3	0% (0Bps/1Gbps)	15.35% (153.5Mbps/1Gbps)
+	L2 LLDP	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/3	0% (0Bps/1Gbps)	15.35% (153.5Mbps/1Gbps)
+	L3 ISIS IPV4	GigabitEthernet0/0/0/4	GigabitEthernet0/0/0/2	20.34% (203.4Mbps/1Gbps)	0% (0Bps/1Gbps)
+	L2 LLDP	GigabitEthernet0/0/0/4	GigabitEthernet0/0/0/2	20.34% (203.4Mbps/1Gbps)	0% (0Bps/1Gbps)
+	L2 CDP	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/3	0% (0Bps/1Gbps)	22.39% (223.9Mbps/1Gbps)
+	L3 ISIS IPV4	GigabitEthernet0/0/0/3	GigabitEthernet0/0/0/7	8.14% (81.4Mbps/1Gbps)	0% (0Bps/1Gbps)
+	L2 LLDP	GigabitEthernet0/0/0/3	GigabitEthernet0/0/0/7	8.14% (81.4Mbps/1Gbps)	0% (0Bps/1Gbps)
+	L2 LLDP	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/3	0% (0Bps/1Gbps)	22.39% (223.9Mbps/1Gbps)
+	L3 ISIS IPV4	GigabitEthernet0/0/0/5	GigabitEthernet0/0/0/6	0% (0Bps/1Gbps)	0% (0Bps/1Gbps)
+	L2 CDP	GigabitEthernet0/0/0/5	GigabitEthernet0/0/0/6	0% (0Bps/1Gbps)	0% (0Bps/1Gbps)
+	L3 ISIS IPV4	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/4	0% (0Bps/1Gbps)	7.33% (73.3Mbps/1Gbps)
+	L2 LLDP	GigabitEthernet0/0/0/5	GigabitEthernet0/0/0/6	0% (0Bps/1Gbps)	0% (0Bps/1Gbps)
+	L2 LLDP	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/4	0% (0Bps/1Gbps)	7.33% (73.3Mbps/1Gbps)
+	L3 ISIS IPV4	Bundle-Ether9	Bundle-Ether9	0% (0Bps/1Gbps)	22.39% (223.9Mbps/1Gbps)

ステップ5 サイドパネルを折りたたんで、[デバイスの詳細 (Device Details)] ウィンドウを閉じます。

ステップ6 破線をクリックします。破線は、複数のリンクを表す集約リンクを示します。

(注) デュアルスタックリンク (集約) は、1本の線で表示されます。



Links

Total 5

State	Link Type	A Side Interface	Z Side Interface
+	L3 ISIS IPV6	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/1
+	L2 LLDP	GigabitEthernet0/0/0/6	GigabitEthernet0/0/0/6
+	L3 ISIS IPV4	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/1
+	L2 LLDP	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/1
+	L2 LAG	Bundle-Ether2	Bundle-Ether2

Link Aggregation Group (LAG) のさまざまなバンドルメンバーとメンバーの詳細を表示するには、LAG ディスカバリが有効になっていることを確認します ([管理 (Administration)] > [設定 (Settings)] > [システム設定 (System Settings)] タブ > [ディスカバリ (Discovery)] > [LAG] チェックボックス)。

(注) LAG ディスカバリが有効になった後、LAG 収集が完了するまでに数分かかります。

a) [LAG] リンクをクリックします。次に例を示します。

Links

Total 2

State	Link Type	A Si...	Z Si...	A Si...	Z Si...
Up	L2 LAG	Bundl...	Bundl...	0% (...)	0% (...)
Up	L2 CDP	Gigabi...	Gigabi...	0% (...)	0% (...)

b) [メンバー (Members)] タブをクリックします。この例では、1つのリンクのみが表示されます。

Link Details

Summary **Members**

Total 1

State	Link Type	A Si...	Z Si...	A Si...	Z Si...
Up	L2 LAG MEM...	Gigabi...	Gigabi...	0% (...)	0% (...)

c) [LAG メンバー (LAG member)] リンクをクリックします。

Link Details

**Summary**

**Name** GigabitEthernet0/0/0/3-GigabitEthernet0/0/0/3  
**State** Up  
**Link Type** L2 LAG MEMBER  
**Last Update** 25-Mar-2021 05:29:32 AM GMT+2

	A Side	Z Side
<b>Node</b>	P-BOTTOMRIGHT-L2	P-BOTTOMLEFT-L2
<b>TE Router ID</b>	101.101.101.4	101.101.101.3
<b>IF Name</b>	GigabitEthernet0/0/0/3	GigabitEthernet0/0/0/3
<b>IF Description</b>	GigabitEthernet0/0/0/3	GigabitEthernet0/0/0/3
<b>Type</b>	ETHERNETCSMACD	ETHERNETCSMACD
<b>Utilization</b>	0% (0Bps/1Gbps)	0% (0Bps/1Gbps)

# デバイスグループを使用したトポロジビューのフィルタ処理

さまざまな目的でデバイスを識別、検索、およびグループ化するためにデバイスグループを作成できます。[デバイスグループ (Device Group)] ウィンドウ ([**デバイス管理 (Device Management)**] > [**グループ (Groups)**]) には、すべてのデバイスとそれらが属するデバイスグループが表示されます。デフォルトでは、すべてのデバイスが最初は [未割り当てデバイス (Unassigned Devices)] グループに表示されます。

この例では、地理的マップと論理マップでのデバイスのグループ化の仕組みを説明します。

**ステップ 1** メインメニューから、[トポロジ (Topology)] を選択します。デフォルトでは、地理的な位置が設定されているデバイスのみが地理的マップに表示されます。

The screenshot shows the 'Topology' view in the Cisco Crosswork Optimization Engine 3.0. The 'Show' dropdown is set to 'Topology' and the 'Device Groups' dropdown is set to 'All Locations'. The geographical map displays several nodes (represented by blue circles with the number '12') connected by green dashed lines. The 'Devices' table on the right lists the following devices and their IP addresses:

Host Name	Node IP
P-TOPRIGHT	172.16.1.42
P-TOPRIGHT1	172.16.4.42
S10AG1-1	172.16.4.71
S10AG1-2	172.16.4.72
S10AG1E1	172.16.4.73
S10AG1E2	172.16.4.74
S10AG1E3	172.16.4.75
S10AG2-1	172.16.4.76
S10AG2-2	172.16.4.77
S10AG2E1	172.16.4.78
S10AG2E2	172.16.4.79
S10AG2E3	172.16.4.80
S10C1	172.16.4.24
S10C2	172.16.4.23
S1AG1-1	172.16.1.43
S1AG1-2	172.16.1.44
S1AG1E1	172.16.1.48

**ステップ 2** [デバイスグループ (Device Group)] ドロップダウンリストからグループ (米国西部) を選択します。そのグループ内のデバイスと関連リンクのみが地理的マップに表示されます。[デバイス (Devices)] テーブルもフィルタ処理され、グループ内のデバイスのみが表示されることに注意してください。

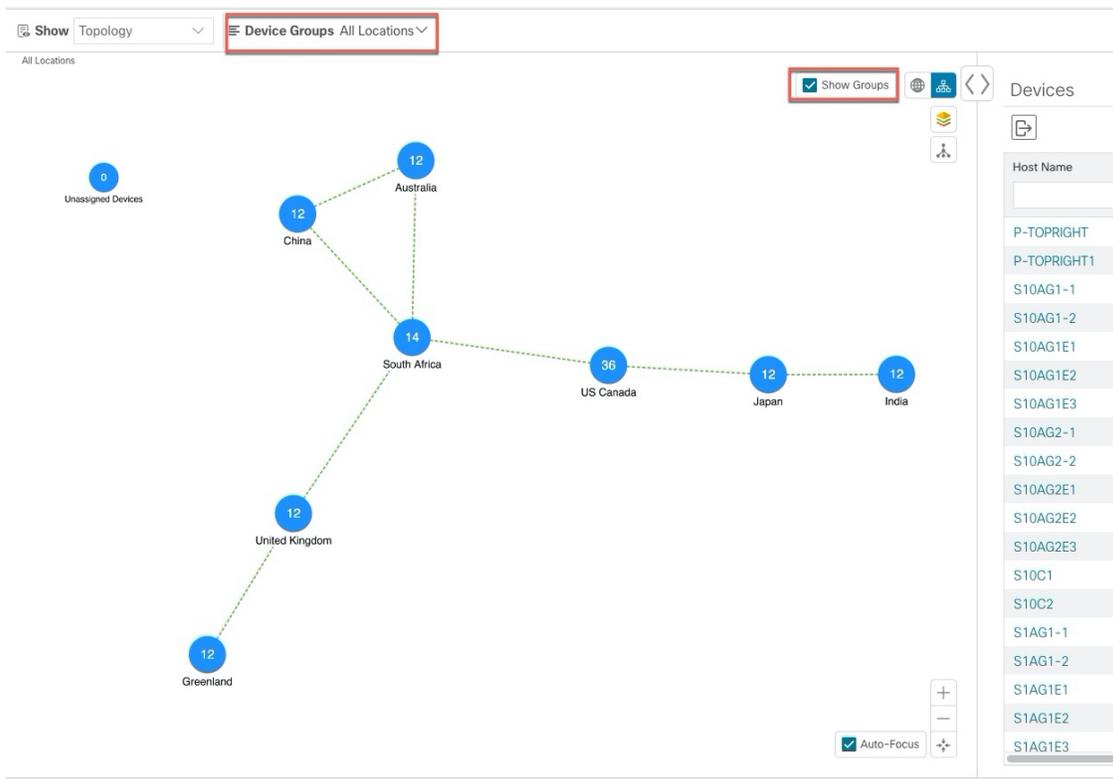
Host Name	Node IP
S7AG1-1	172.16.4.38
S7AG1-2	172.16.4.37
S7AG1E1	172.16.4.34
S7AG1E2	172.16.4.35
S7AG1E3	172.16.4.36
S7AG2-1	172.16.4.81
S7AG2-2	172.16.4.82
S7AG2E1	172.16.4.83
S7AG2E2	172.16.4.84
S7AG2E3	172.16.4.85
S7C1	172.16.4.46
S7C2	172.16.4.47

**ステップ 3**  をクリックします。

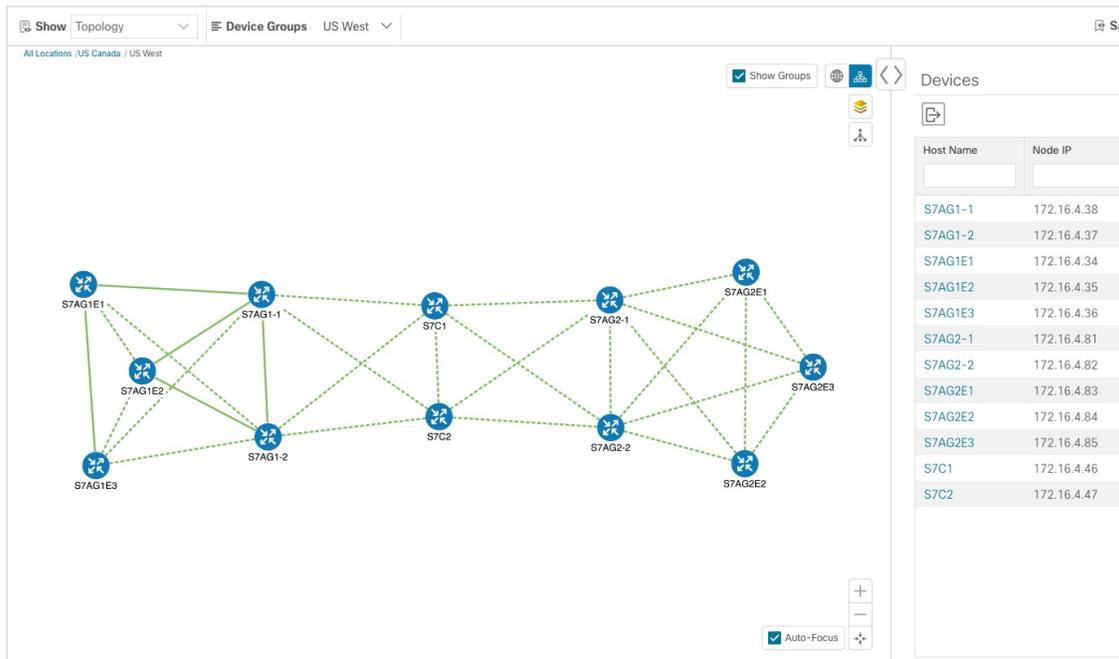
**ステップ 4** [デバイスグループ (Device Group)] ドロップダウンリストから [すべての場所 (All Locations)] を選択し、[グループの表示 (Show Groups)] がオンになっていない場合はオンにします。このビューでは、すべてのデバイスグループを表示できます。デバイスグループは、論理マップ内でのみこの方法で表示できません。

(注) [グループの表示 (Show Groups)] チェックボックスをオフにすると、すべてのデバイスグループが展開され、マップが乱雑になる可能性があります。

## デバイスグループを使用したトポロジビューのフィルタ処理



**ステップ 5** [米国西部 (US West)] グループをクリックします。この場合も、このグループに属するデバイスのみがトポロジマップと [デバイス (Devices)] テーブルに表示されます。



**ステップ 6** ホスト名に S7C と入力して、[デバイス (Device)] テーブルのデバイスをフィルタ処理します。[デバイス (Device)] テーブルには、フィルタ処理の基準に一致するデバイスのみが表示されます。ただし、[デバ

イス (Device) ]テーブルをフィルタ処理しても、トポロジマップ上のデバイスは視覚的にフィルタ処理されません。地理的マップまたは論理マップ上のデバイスを視覚的にフィルタ処理する唯一の方法は、デバイスグループを使用することです。

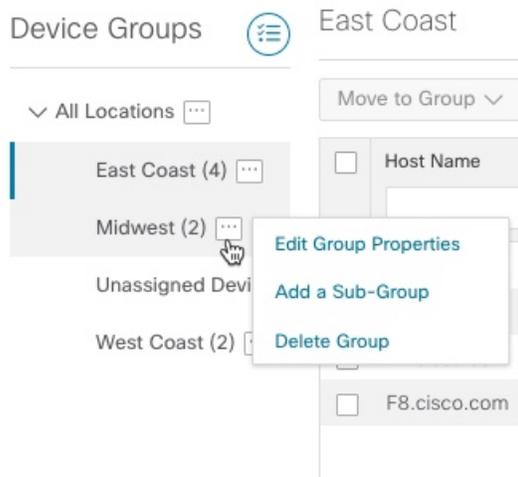
The screenshot shows the 'Devices' table with the following data:

Host Name	Node IP	Oper...	Reac...	Product Type
S7C1	172.16.4.46	OK	Re...	ciscoCRS16S
S7C2	172.16.4.47	OK	Re...	ciscoCRS16S

## デバイスグループの作成と変更

デバイスグループ、およびグループへのデバイスの割り当ては、手動（この項で説明）または自動（次の項で説明）で実行できます。

- ステップ 1** メインメニューから [デバイス管理 (Device Management) ] > [グループ (Groups) ] を選択します。
- ステップ 2** 新しいサブグループを追加するには、[すべての場所 (All Locations) ]の横にある  をクリックします。[すべての場所 (All Locations) ]の下に新しいサブグループが追加されます。
- ステップ 3** 既存グループの下で、サブグループを編集、削除、または追加するには、[デバイスグループ (Device Groups) ] ツリーでグループの横にある  をクリックします。



**ステップ 4** グループの追加、削除、または編集（名前の変更または移動）を選択します。グループを削除すると、そのグループに属しているすべてのデバイスが [未割り当てデバイス（Unassigned Devices）] グループに移動します。また、グループを削除すると、そのグループのサブグループがすべて削除されます。

（注） デバイスは、1つのデバイスグループにのみ属することができます。

**ステップ 5** [保存（Save）] をクリックします。

## ダイナミック デバイス グループの有効化

デバイスホスト名で正規表現（regex）を使用して、デバイスグループを動的に作成し、未割り当てのデバイスをこれらのグループに自動的に追加するルールを作成できます。ルールに一致する新たに追加または検出されたデバイスは、適切なグループに配置されます。



（注） ダイナミックルールは、すでにグループに属しているデバイスには適用されません。ルールで考慮されるようにするデバイスは、[未割り当てデバイス（Unassigned Devices）] に移動する必要があります。

### 始める前に

[ダイナミックグループ（Dynamic Groups）] ダイアログに示されている例に従うこともできますが、正規表現に精通していると有利です。

**ステップ 1** メインメニューから [デバイス管理（Device Management）] > [グループ（Groups）] を選択します。

**ステップ 2** [ダイナミックグループの管理（Manage Dynamic Groups）] アイコンをクリックして、[ダイナミックグループ作成ルールの管理（Manage Dynamic Grouping Rule）] ウィンドウを開きます。 

- ステップ 3** [他の詳細と例の表示 (Show more details and examples)] をクリックして、必要な [ホスト名 (Host Name)] フィールドと [グループ名 (Group Name)] フィールドに入力します。
- ステップ 4** [未割り当てデバイス (Unassigned Devices)] グループに既存のデバイスがある場合は、[ルール of テスト (Test Rule)] をクリックして、作成されるグループ名のタイプのサンプリングを表示します。
- ステップ 5** [ルール of 有効化 (Enable Rule)] チェックボックスをオンにします。ルールが有効になると、システムは未割り当てのデバイスを 1 分おきに確認し、ルールに基づいてそれらを適切なグループに割り当てます。
- ステップ 6** [保存 (Save)] をクリックします。
- ステップ 7** この方法で作成されたグループは、最初は [未割り当てグループ (Unassigned Groups)] の下に表示されず (ルールが初めて有効になったときに作成されます)。新たに作成したグループを必要なグループ階層に移動します。
- ステップ 8** 新しく作成した未割り当てグループを適切なグループに移動するには、次の手順を実行します。
- [すべての場所 (All Locations)] の横にある [...] を選択し、[サブグループの追加 (Add a Sub-Group)] をクリックします。
  - [新しいグループ (New Group)] に詳細を入力して [保存 (Save)] をクリックします。
  - 未割り当ての作成済みダイナミックグループの横にある [...] を選択し、[グループプロパティの編集 (Edit Group Properties)] を選択します。
  - [親グループの変更 (Change Parent Group)] をクリックし、適切なグループを選択します。

## マップ表示設定のカスタマイズ

ニーズと設定に基づいて、トポロジマップを視覚的な設定を行うことができます。次を実行できます。

- [リンクとデバイスの表示のカスタマイズ \(27 ページ\)](#)
- [TE トンネルのデバイスグループの表示動作の設定 \(28 ページ\)](#)

## リンクとデバイスの表示のカスタマイズ

デバイスとリンクマップの表示設定を設定するには、[トポロジ (Topology)] を選択し、トポロジマップの  をクリックします。

- 集約リンク、およびリンクの状態と使用状況を簡単に確認できるようにするリンクの色付け方法を表示するには、[リンク (Links)] をクリックします。デフォルトでは、集約リンクはマップ上で単一リンクと区別され、リンクはリンク使用率のしきい値に基づいて色付けされます。管理者は、使用率のしきい値と対応する色を変更できます。
- デバイスの状態とデバイスのラベル付けを表示するには、[デバイス (Devices)] をクリックします。デフォルトでは、デバイスの状態はマップに表示され、ホスト名はデバイスのラベル付けに使用されます。

## TE トンネルのデバイスグループの表示動作の設定

デバイスグループを選択し、選択した TE トンネル内のデバイスがグループに属していない場合に、トポロジマップに表示される内容を設定できます。動作を設定するには、[管理 (Admin)] > [設定 (Settings)] > [ユーザー設定 (User Settings)] を選択し、動作オプションのいずれかを選択します。

デフォルトでは、ユーザーは毎回デバイスグループビューを選択するように求められます。

## トラフィック エンジニアリングの表示のカスタマイズ

トラフィック エンジニアリングの表示設定を設定するには、[Traffic Engineering] > [Traffic Engineering] を選択し、トポロジマップで  をクリックします。

- 集約リンク、およびリンクの状態と使用状況を簡単に確認できるようにするリンクの色付け方法を表示するには、[リンク (Links)] をクリックします。デフォルトでは、集約リンクはマップ上で単一リンクと区別され、リンクはリンク使用率のしきい値に基づいて色付けされます。管理者は、使用率のしきい値と対応する色を変更できます。



(注) デュアルスタックリンク (集約) は、1 本の線で表示されます。

- デバイスの状態とデバイスのラベル付けを表示するには、[デバイス (Devices)] をクリックします。デフォルトでは、デバイスの状態はマップに表示され、ホスト名はデバイスのラベル付けに使用されます。
- IGP パスを表示するときに、IGP、TE、および遅延メトリックを表示するには、[Metrics] をクリックします。デフォルトでは、これらのメトリックは有効になっていません。



(注) IGP パスが集約リンクを通過する場合、メトリックは表示できません。IPv4 と IPv6 の両方のリンクがある IPv6 ネットワークを表示する場合、IPv6 メトリックを表示するには、[Show Participating Only] チェックボックスをオンにする必要があります。

- フレキシブルアルゴリズムのパスを表示するには、[Flex Algo] をクリックします。詳細については、[フレキシブルアルゴリズムの可視化 \(55 ページ\)](#) を参照してください。

## タイムアウトの設定

SR-TE ポリシー、RSVP-TE トンネル、オンデマンド帯域幅、および IGP パスのデータのプロビジョニングと取得のタイムアウト設定を行うには、[管理 (Administration)] > [システム設

定 (System Settings) ]> [タイムアウト設定 (Timeout Configuration) ] タブを選択します。タイムアウト期間のオプションを入力します。詳細については、 をクリックしてください。



(注) SR-PCE の応答が遅い場合、タイムアウトの設定で各アクションの応答時間を変更します。大規模トポロジの設定を変更したり、遅延や負荷による SR-PCE 応答の遅延に対処したりできます。

## 簡易アクセスのトポロジビューの保存

マップ上のデバイスとリンクを再配置すると、通常、変更は保存されません。便利なマップレイアウトに簡単にアクセスするには、名前付きカスタムビューとして保存すると、毎回マップを再配置することなくすばやく取得できます。これは、多数のデバイスを含む大規模なネットワークを管理する場合に特に役立ちます。

カスタムビューを保存すると、次の設定が保存されます。

- 地理的マップか論理マップか。
- 論理マップのレイアウト内のデバイスの位置。
- デバイスとリンクの表示設定。
- デバイステーブルとトラフィック エンジニアリング テーブルで 사용되는フィルタ



(注) すべてのカスタムビューは、すべてのユーザーに表示されます。ただし、ビューを変更できるのは管理者ロールを持つユーザーまたはカスタムビューを作成したユーザーのみです。

**ステップ 1** 必要な情報のみが含まれ、レイアウトがニーズを満たすまで、現在のマップビューをカスタマイズします。

**ステップ 2** 思いどおりになったら、[ビューの保存 (Save View) ] をクリックします。

## 簡易アクセスのトポロジビューの保存

The screenshot displays the network management interface. On the left, a map of the United States shows a network topology with nodes labeled xrv9k-5, xrv9k-3, xrv9k-6, xrv9k-4, xrv9k-7, and srpce1. On the right, the 'Traffic Engineering' panel is visible, featuring a 'Save View' button in a red box. Below the map, there are statistics for SR-MPLS, SRv6, and RSVP-TE, and a table for SR POLICY.

Hea...	End...	C...	Ad...	Op...	Actions
<input type="checkbox"/>					
<input type="checkbox"/>	xrv9k-5	xrv9k-7	123...	↑	↑
<input type="checkbox"/>	xrv9k-5	xrv9k-7	222	↑	↑
<input type="checkbox"/>	xrv9k-5	xrv9k-7	333	↑	↑
<input type="checkbox"/>	xrv9k-6	xrv9k-7	607...	↑	↑
<input type="checkbox"/>	xrv9k-5	xrv9k-7	6521	↑	↑

**ステップ3** 新しいカスタムビューの一意の名前を入力し、[保存 (Save)] をクリックします。後でビューを変更 ([Select a saved view] をクリック) し、トポロジの編集、名前の変更、またはビューの削除を選択できます。



## 第 3 章

# SR-MPLS および SRv6 ポリシーの可視化

Crosswork 最適化エンジンを使用すると、ネットワーク内の SR-MPLS および SRv6 ポリシーを可視化できます。SR-PCE はポリシーを検出し、トラフィック エンジニアリングのトポロジマップに表示します。

### SRv6 の注意事項と制限事項

- IS-IS IGP による SRv6 の可視化は、Cisco IOS XR 7.3.2 を実行する SR-PCE でのみサポートされています。
- SRv6 ポリシーでのトラフィック収集は現在サポートされていません。
- OSPFv3 IGP (PCE によって開始された) SRv6 ポリシーはサポートされていません。
- IPv4 と IPv6 の両方のリンクを持つ IPv6 ネットワークのメトリックを表示する場合は、[Show Participating Only] チェックボックス ([Traffic Engineering] > [Traffic Engineering] >  > [Metrics]) をオンにする必要があります。
- IPv4 と IPv6 のトポロジは一致している必要があります。IPv4 と IPv6 の異なるリンクメトリックはサポートされていません。
- SRv6 は、帯域幅最適化、オンデマンド帯域幅、またはローカル輻輳緩和機能パックではサポートされていません。
- PCC によって開始されたダイナミックパス SRv6 ポリシーを可視化します。SRv6 の PCE によって開始された明示パスの可視化はサポートされていません。

ここでは、次の内容について説明します。

- [トポロジマップでの SR-MPLS および SRv6 ポリシーの表示 \(32 ページ\)](#)
- [SR-MPLS および SRv6 ポリシーの詳細の表示 \(34 ページ\)](#)
- [トラフィック エンジニアリング デバイスの詳細の表示 \(36 ページ\)](#)
- [SR-MPLS または SRv6 ポリシーの可視化の例 \(37 ページ\)](#)
- [複数の候補パス \(MCP\) の検索 \(45 ページ\)](#)
- [定義済みのバインディングセグメント ID \(B-SID\) ラベルに関連付けられた基盤となるパスの可視化 \(49 ページ\)](#)
- [ネイティブ SR パスの可視化 \(51 ページ\)](#)

# トポロジマップでの SR-MPLS および SRv6 ポリシーの表示

Crosswork 最適化エンジン 可視化は、SR-MPLS および SRv6 ポリシーの表示と管理を容易にする機能を提供することで、多くの価値をもたらします。ネットワークを視覚的に調べることで、SR-TE ポリシーのプロビジョニングと管理の複雑さが大幅に軽減されます。

トラフィック エンジニアリングのトポロジマップを表示するには、[トラフィック エンジニアリング (Traffic Engineering)] > [トラフィック エンジニアリング (Traffic Engineering)] を選択します。



- (注) この項では、ナビゲーションを [トラフィック エンジニアリング (Traffic Engineering)] > [トラフィック エンジニアリング (Traffic Engineering)] と記載しています。ただし、Crosswork Network Controller ソリューション内で Crosswork 最適化エンジンを使用する場合のナビゲーションは [トラフィック エンジニアリング & サービス (Traffic Engineering & Services)] > [トラフィック エンジニアリング (Traffic Engineering)] であり、[SR-MPLS] または [SRv6] タブを選択します。

図 6: トラフィック エンジニアリング UI : SR-MPLS および SRv6 ポリシー

Headend	Endpoint	Color	Admin Sta...	Oper Status	Actions
<input type="checkbox"/>	iosrv-2	iosrv-5	12345	<span style="color: green;">●</span>	<span style="color: green;">●</span>
<input checked="" type="checkbox"/>	iosrv-2	iosrv-5	54321	<span style="color: green;">●</span>	<span style="color: green;">●</span>
<input type="checkbox"/>	iosrv-2	iosrv-6	1868	<span style="color: green;">●</span>	<span style="color: green;">●</span>
<input checked="" type="checkbox"/>	iosrv-7	iosrv-5	123	<span style="color: green;">●</span>	<span style="color: green;">●</span>
<input type="checkbox"/>	iosrv-2	ic iosrv-5	8000	<span style="color: green;">●</span>	<span style="color: green;">●</span>
<input checked="" type="checkbox"/>	iosrv-2	iosrv-5	8500	<span style="color: green;">●</span>	<span style="color: green;">●</span>
<input type="checkbox"/>	iosrv-2	iosrv-5	111	<span style="color: green;">●</span>	<span style="color: green;">●</span>
<input checked="" type="checkbox"/>	iosrv-2	iosrv-5	888	<span style="color: green;">●</span>	<span style="color: green;">●</span>

522544

引き出し線番号	説明
1	<p>オレンジ色のアウトラインが付いたデバイス () は、そのデバイスまたはクラスタ内のデバイスにノード SID が関連付けられていることを示します。</p>
2	<p>該当するチェックボックスをクリックして、次のオプションを有効にします。</p> <ul style="list-style-type: none"> <li>• [IGPパスの表示 (Show IGP Path) ] : 選択した SR-TE ポリシーの IGP パスを表示します。</li> <li>• [参加デバイスのみ表示 (Show Participating Only) ] : 選択した SR-TE ポリシーに属するリンクのみを表示します。他のすべてのリンクとデバイスは表示されなくなります。</li> </ul>
3	<p>SR-TE ポリシーは [SR-MPLS] または [SRv6] テーブルで選択されると、送信元と宛先を示す紫色の矢印線としてマップに表示されます。</p> <p>隣接関係セグメント ID (SID) は、パスに沿ったリンクにオレンジ色の円 () として表示されます。</p>
4	<p>[SR-MPLS および SRv6 ポリシーの送信元と宛先 (SR-MPLS and SRv6 Policy Origin and Destination) ] : デバイスクラスタに A と Z の両方が表示される場合、クラスタ内の1つ以上のノードが送信元で、他のノードが宛先です。A+は、1つのノードから発信される複数の SR-TE ポリシーがあることを示します。Z+は、ノードが複数の SR ポリシーの宛先であることを示します。</p>
5	<p>このウィンドウの内容は、選択またはフィルタ処理された内容によって異なります。この例では、[SR-MPLS] タブが選択され、[SR ポリシー (SR Policy) ] テーブルが表示されます。トポロジマップで選択した内容、または SR-TE ポリシーを表示および管理しているプロセスに応じて、次の操作を実行できます。</p> <ul style="list-style-type: none"> <li>• <a href="#">SR-MPLS または SRv6 ポリシーの可視化の例 (37 ページ)</a></li> <li>• <a href="#">SR-MPLS ポリシーのプロビジョニング (71 ページ)</a></li> <li>• <a href="#">デバイスとリンクの詳細の表示 (16 ページ)</a></li> </ul>
6	<p>[SR-MPLS] タブまたは [SRv6] タブをクリックして、SR-TE ポリシーの各リストを表示します。</p>

引き出し線番号	説明
7	[ミニダッシュボード (Mini Dashboard)] には、動作中の SR-MPLS または SRv6 ポリシーステータスの概要が表示されます。フィルタが適用されると、[ミニダッシュボード (Mini Dashboard)] が更新され、[SR ポリシー (SR Policy)] および [SRv6 ポリシー (SRv6 Policy)] テーブルに表示される内容が反映されます。[SR-MPLS ミニダッシュボード (SR-MPLS Mini Dashboard)] テーブルには、ポリシーステータスに加えて、現在 [SR ポリシー (SR Policy)] テーブルにリストされている PCC および PCE によって開始されたトンネルの数が表示されます。
8	このオプションでは、グループフィルタ (使用している場合) をテーブルデータに適用する方法を選択できます。たとえば、[ヘッドエンドのみ (Headend only)] を選択した場合、ポリシーのヘッドエンドデバイスが選択されたグループにあるポリシーのみが表示されます。このフィルタを使用すると、特定の設定を確認でき、大規模なネットワークがある場合に役立ちます。 フィルタオプション： <ul style="list-style-type: none"> <li>• [ヘッドエンドまたはエンドポイント (Headend or Endpoint)] : 選択したグループ内のヘッドエンドまたはエンドポイントデバイスを含むポリシーを表示します。</li> <li>• [ヘッドエンドとエンドポイント (Headend and Endpoint)] : ヘッドエンドとエンドポイントの両方がグループ内にある場合にポリシーを表示します。</li> <li>• [ヘッドエンドのみ (Headend only)] : ポリシーのヘッドエンドデバイスが選択したグループにある場合にポリシーを表示します。</li> <li>• [エンドポイントのみ (Endpoint only)] : ポリシーのエンドポイントデバイスが選択したグループ内にある場合にポリシーを表示します。</li> </ul>
9	CSV ファイルにすべてのデータをエクスポートします。選択またはフィルタ処理されたデータをエクスポートすることはできません。

## SR-MPLS および SRv6 ポリシーの詳細の表示

分離グループ、メトリックタイプ、候補パス、セグメントホップ情報など、SR-MPLS または SRv6 ポリシーの詳細を表示します。

ステップ 1 [アクション (Actions)] 列で、いずれかの SR-MPLS または SRv6 ポリシーに対して  > [詳細の表示 (View Details)] をクリックします。

The screenshot displays the Traffic Engineering interface. On the left, a map of the United States shows a network topology with nodes and links. On the right, the 'SRv6 POLICY' table is visible, listing various policies with their endpoints, colors, and operational statuses.

Headend	Endpoint	Color	Admin Sta...	Oper Status	Actions	
<input type="checkbox"/>	xrv9k-4	xrv9k-2	4502	<span style="color: green;">●</span>	<span style="color: red;">●</span>	...
<input type="checkbox"/>	xrv9k-7	xrv9k-5	90009	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	xrv9k-7	xrv9k-6	90007	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	xrv9k-6	xrv9k-7	1002	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	c42.cisco.com	xrv9k-2	22916	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	c42.cisco.com	xrv9k-7	9977	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	c42.cisco.com	xrv9k-5	4215	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input checked="" type="checkbox"/>	xrv9k-2	xrv9k-5	10011	<span style="color: green;">●</span>	<span style="color: green;">●</span>	View Details
<input type="checkbox"/>	xrv9k-2	xrv9k-5	10010	<span style="color: green;">●</span>	<span style="color: green;">●</span>	Edit / Delete
<input type="checkbox"/>	xrv9k-2	xrv9k-5	22255	<span style="color: green;">●</span>	<span style="color: red;">●</span>	...
<input type="checkbox"/>	xrv9k-2	xrv9k-5	10000	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...

ステップ2 SR-MPLS または SRv6 ポリシーの詳細を表示します。

(注) すべてのポリシーの [遅延 (Delay)] 値は 10 分ごとに計算されます。[遅延 (Delay)] 値の横にある [i] アイコンの上にマウスポインタを合わせると、値が最後に更新された時刻が表示されます。

**SRv6 Policy Details**

**Headend** xrv9k-2 (TE RID: 192.168.0.2) PCC IP: 192.168.0.2  
Source IP: 2001:192:168::2

**Endpoint** xrv9k-5 (TE RID: 192.168.0.5)  
Dest IP: 2001:192:168::5

**Color** 10011

**Summary**

- Admin State ↑ Up
- Oper State ↑ Up
- Binding SID fccc:cc11:22:e01d::/64, Behavior - uB6 (Insert.Red)
- Segment Type -
- Policy Type Unknown
- Profile ID -
- Utilization 0 Mbps
- Delay 124 Last Updated  
27-Oct-2021 06:42:22 PM PDT
- BWOD Policy Bandwidth 0 Mbps
- Accumulated Metric 124
- Delegated PCE 2001:420:28f:2011:250:56ff:fe85:a025
- Non-delegated PCEs -
- PCE Computed Time 27-Oct-2021 12:33:03 PM PDT
- Last Update 27-Oct-2021 12:39:55 PM PDT

**Candidate Path** Expand All

Path Name	Preference	Path Type
cfgr_srv6_test_disjoint2_discr_100	100	Unknown

Seg...	Seg...	SID	Behavior	Algo	Address	Node	Interface
0	uN	fccc:cc11:6...	uN (PSP/U...	0	2001:192:...	xrv9k...	
1	uN	fccc:cc11:5...	uN (PSP/U...	0	2001:192:...	xrv9k...	

**Path Name** cfgr\_srv6\_test\_disjoint2\_discr\_100  
**Metric Type** TE  
**Disjoint Group** ID: 18115  
Association Source: 0.0.0.0  
Type: Node-disjoint

## トラフィック エンジニアリング デバイスの詳細の表示

トラフィック エンジニアリング デバイスの詳細 (SR-MPLS、SRv6、RSVP-TE、およびフレキシブルアルゴリズム情報) を表示するには、次の手順を実行します。

- ステップ 1** メインメニューから、[トラフィックエンジニアリング (Traffic Engineering)] > [トラフィックエンジニアリング (Traffic Engineering)] を選択します。
- ステップ 2** トラフィック エンジニアリング マップから、デバイスをクリックします。

**ステップ 3** [デバイスの詳細 (Device Details)] ページで、目的の[トラフィックエンジニアリング (Traffic Engineering)] タブをクリックします。このタブには、そのデバイスの関連データが表示されます。次の例は、デバイスの MSD 値を含む SR-MPLS プレフィックス情報を示しています。

## SR-MPLS または SRv6 ポリシーの可視化の例

次の例では、トポロジマップから使用できる SR-TE (SR-MPLS および SRv6) ポリシー仮想化の一部の機能について説明します。トポロジマップには、UI を使用してプロビジョニングされた SR-TE ポリシーと、SR-PCE によってネットワークから検出されたポリシーが表示されます。トポロジマップから、参加している SR-TE ポリシーの詳細と可視化にドリルダウンできます。

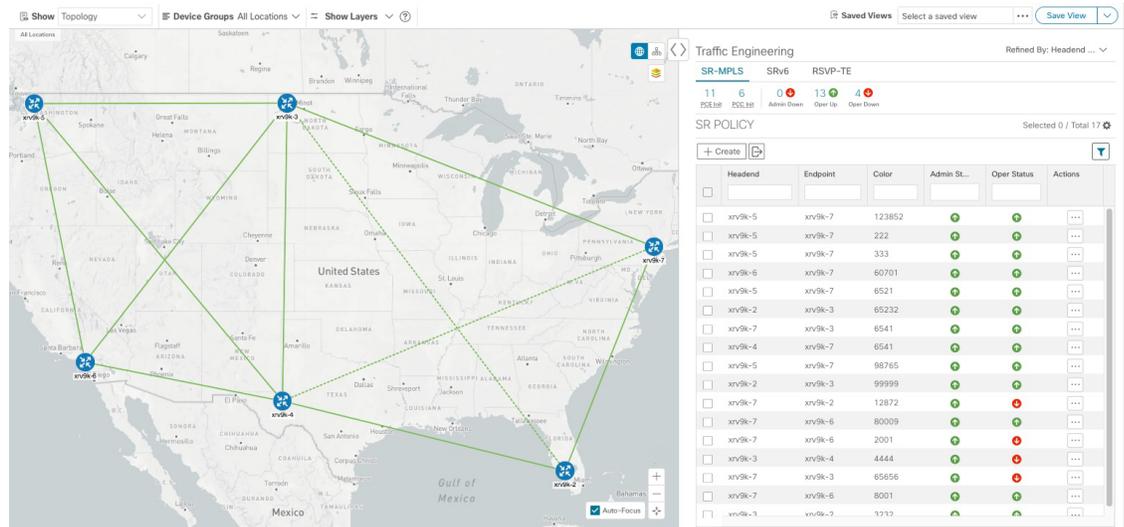
この例は、デバイスと SR-MPLS ポリシーが追加され、デバイスグループが作成されていることを前提としています。



(注) この例では SR-MPLS ポリシーを使用していますが、SR-MPLS ポリシーと SRv6 ポリシーのマップの基本機能は同じです。

拡大表示するには画像をクリックします。

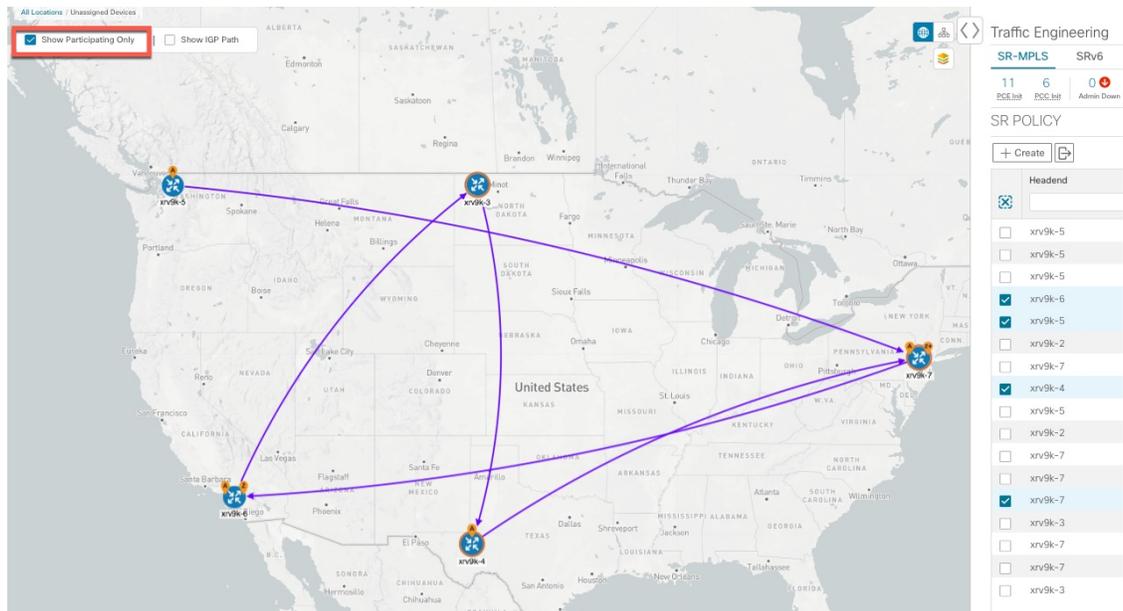
図 7: トポロジマップの例



ステップ1 可視化する SR-MPLS ポリシーを選択し、マップ上で分離します。

- メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [トラフィック エンジニアリング (Traffic Engineering)] を選択します。
  - [SR Policy] テーブルで、目的の SR-MPLS ポリシーの横にあるチェックボックスをオンにします。
  - [Show Participating Only] の横にあるチェックボックスをオンにして、選択した SR-TE ポリシーの一部ではない他のリンクとデバイスを非表示にします。
- 次の例では、トポロジマップに次のように表示されます。

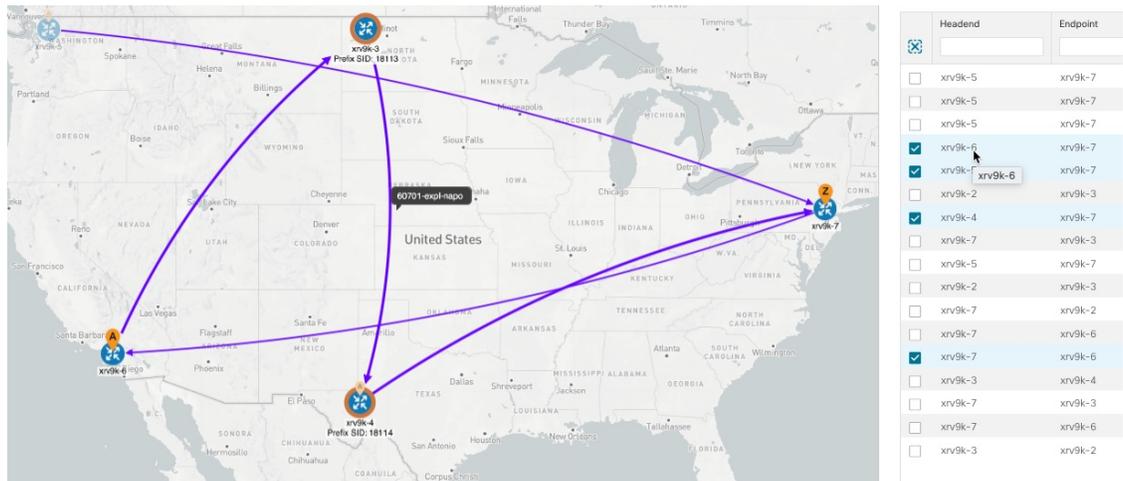
- 4つの SR-MPLS ポリシーが選択されています。
- SR-MPLS ポリシーは、パスの方向を示す矢印付きの紫色のリンクとして表示されます。
- xrv9k-7 ノードは、選択した 2 つのポリシーの宛先です。xrv9k-3 と xrv9k-2 はどちらも、選択したポリシーの宛先です。SR-MPLS ポリシーの送信元と宛先は、それぞれ A と Z でマークされます。A+ は、デバイスから発信される複数のポリシーがあることを示します。Z+ は、デバイスが複数のポリシーの宛先であることを示します。
- オレンジ色のアウトライン (🔴) は、xrv9k-3、xrv9k-7、および xrv9k-4 にノード SID があることを示します。



ステップ2 特定の SR-MPLS ポリシーの詳細を強調表示して表示します。

a) [SRポリシー (SR Policy)] テーブルで、選択したポリシーにカーソルを合わせます。トポロジマップには、次の詳細が表示されます。

- パスはマップ上で強調表示されます。パスの順番は、xrv9k-6 > xrv9k-3 > xrv9k-4 > xrv9k です。
- xrv9k-3 および xrv9k-4 のプレフィックス SID が表示されます。
- パス名は 60701-expl-napo と表示されます。



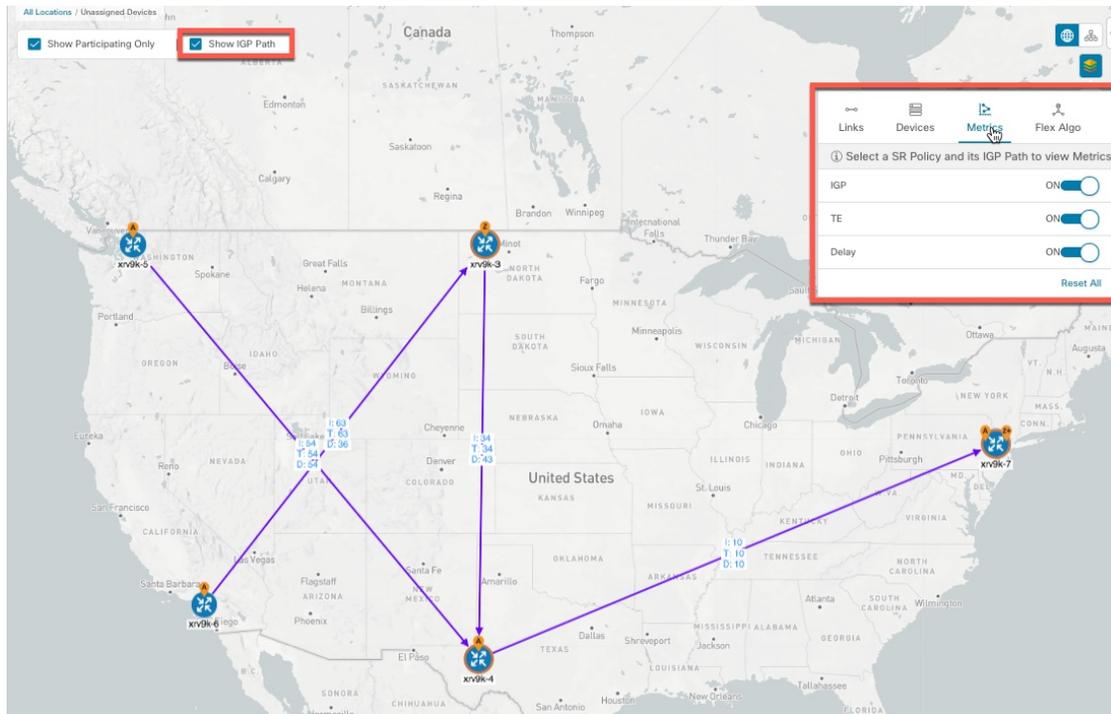
ステップ3 選択した SR-MPLS ポリシーのエンドポイント間の物理パスとメトリックを表示します。

a) [Show IGP Path] チェックボックスをオンにします。選択した SR-MPLS ポリシーの IGP パスが、セグメントホップの代わりに直線が表示されます。

b)  をクリックします。

- c) [メトリック (Metrics)] タブをクリックします。  
 d) 該当するメトリックを [オン (ON)] に切り替えます。

(注) メトリックを表示するには、[Show IGP Path] チェックボックスをオンにする必要があります。



**ステップ 4** 分離グループ、メトリックタイプ、セグメントホップ情報、遅延（10分ごとにすべてのポリシーに対して計算）などの SR-MPLS ポリシーの詳細を表示します。

- a) [Actions] 列で、いずれかの SR-MPLS ポリシーに対して  > [View Details] をクリックします。

サイドパネルに [SRポリシーの詳細 (SR Policy Details)] ウィンドウが表示されます。選択したポリシーのみがトポロジマップに表示されていることに注意してください。

**ステップ 5** トポロジの論理ビューをカスタマイズして保存します。

- 🔍 クリックして、選択した SR-MPLS ポリシーの論理ビューを表示します。
- 必要に応じてノードを配置します。
- (SR-MPLS ポリシーの選択ではなく) トポロジレイアウトを保存するには、選択したすべての SR-MPLS ポリシーをクリアし、[Save View] をクリックします。

例：

図 8: 論理マップ (SR-MPLS ポリシーを選択済み)

Hea...	Endp...	Color	Ad...	Op...	Actions
<input type="checkbox"/>	iosxrv...	iosxrv-6	1868	🟢	🟢
<input checked="" type="checkbox"/>	iosxrv...	iosxrv-5	123	🟢	🟢
<input type="checkbox"/>	iosxrv...	iosxrv-6	8000	🟢	🟢
<input type="checkbox"/>	iosxrv...	iosxrv-5	8500	🟢	🟢
<input checked="" type="checkbox"/>	iosxrv...	iosxrv-5	111	🟢	🟢
<input type="checkbox"/>	iosxrv...	iosxrv-5	888	🟢	🟢

例：

図 9: 論理マップ (SR-MPLS ポリシーを選択せずに保存)

The screenshot shows the 'Traffic Engineering' view. On the left, a network diagram displays several routers labeled iosxrv-2 through iosxrv-7 and xtc-iosxrv. On the right, the 'SR POLICY' table is visible, showing a list of policies with columns for Headend, Endpoint, Color, Admin Status, and Oper Status. A 'Save View' button is highlighted in the top right corner.

ステップ 6 現在のビュー (X) を閉じて、[SRポリシー (SR Policy)] テーブルに戻ります。

ステップ 7 SR-MPLS ポリシーを選択した場合のデバイスグループの表示方法を理解するには、選択されている可能性のある SR-MPLS ポリシーをオフにし、[Show Groups] をオンにします。

The screenshot shows the 'Traffic Engineering' view with the 'Show Groups' checkbox checked. The network diagram on the left now displays geographical regions: Australia, China, South Africa, United Kingdom, Greenland, US Canada, Japan, and India. The 'SR POLICY' table on the right shows a list of policies with columns for Headend, Endpoint, Color, Admin Status, and Oper Status. A 'Save View' button is visible in the top right corner.

ステップ 8 [デバイスグループ (Device Groups)] ドロップダウンリストから特定のグループを選択すると、マップとにそのグループが表示されます。この例では、[Australia] が選択され、関連する SR-MPLS ポリシーが

選択されて表示されます。

The screenshot shows the Cisco Crosswork Network Automation interface. On the left, there is a network topology diagram with nodes labeled S1AG1E1, S1AG1E2, S1AG1E3, S1AG1-1, S1AG1-2, S1C1, S1AG2E1, S1AG2E2, S1AG2E3, and S1C2. A purple path is highlighted across the network. On the right, the 'SR POLICY' table is displayed with the following data:

Headend	Endpoint	Color	Admin St...	Oper St...	Actions
<input type="checkbox"/>	S1AG1E1	SSAG1E2	63212	<span style="color: green;">●</span>	<span style="color: green;">●</span>
<input type="checkbox"/>	S1C2	S2C1	100	<span style="color: green;">●</span>	<span style="color: green;">●</span>
<input checked="" type="checkbox"/>	S1AG2E1	S1AG1E2	100	<span style="color: green;">●</span>	<span style="color: green;">●</span>
<input type="checkbox"/>	S5C1	S1C2	111	<span style="color: green;">●</span>	<span style="color: red;">●</span>
<input type="checkbox"/>	S7C1	S1C2	202	<span style="color: green;">●</span>	<span style="color: red;">●</span>
<input checked="" type="checkbox"/>	S1AG1-2	S1C2	4521	<span style="color: green;">●</span>	<span style="color: green;">●</span>
<input type="checkbox"/>	S10AG1-1	S1AG1-1	3256	<span style="color: green;">●</span>	<span style="color: red;">●</span>

**ステップ 9** 参加中のデバイスが選択したグループの一部ではないポリシーを選択すると、グループビューを切り替えるオプションを示すダイアログが表示されます。これはデフォルトの動作です。このウィンドウが表示されない場合、自動的にビューを切り替えるか、または現在のビューにとどまるように管理者が表示を設定しています。詳細については、「[TE トンネルのデバイスグループの表示動作の設定 \(28 ページ\)](#)」を参照してください。

The screenshot shows the same interface as before, but with a dialog box overlaid. The dialog box contains the following text:

Some of the participating devices are not in the current device group.  
Click "Switch Device Group" to automatically switch to the device group that will show all participating devices.

Buttons:

Don't show this message again

The 'SR POLICY' table on the right now shows 3 selected items:

Headend	Endpoint	Color	Admin St...	Oper St...	Actions
<input checked="" type="checkbox"/>	S1AG1E1	SSAG1E2	63212	<span style="color: green;">●</span>	<span style="color: green;">●</span>
<input checked="" type="checkbox"/>	S1AG2E1	S1AG1E2	100	<span style="color: green;">●</span>	<span style="color: green;">●</span>
<input checked="" type="checkbox"/>	S1AG1-2	S1C2	4521	<span style="color: green;">●</span>	<span style="color: green;">●</span>

**ステップ 10** [Switch Device Group] を選択すると、グループが変更され、選択した SR-MPLS ポリシーに参加中のデバイスがすべて表示されます。

## SR-MPLS または SRv6 ポリシーの可視化の例

前のグループビューに戻るには、[戻る (Back)] をクリックします (このリンクは、次の図に示す黄色のテキスト領域に後で表示されます)。

The screenshot shows the Cisco Crosswork Network Automation interface. On the left, there is a navigation sidebar with options like Home, Traffic Engineering, and Device Management. The main area displays a network topology with nodes representing different locations: United Kingdom, Australia, South Africa, US Canada, Japan, India, and China. A specific path is highlighted in purple. On the right, the 'Traffic Engineering' dashboard is visible, showing a summary for SR-MPLS, SRv6, and RSVP-TE. Below this is a table titled 'SR POLICY' with columns for Headend, Endpoint, Color, Admin St., Oper St., and Actions. The 'PCE Init' column header is highlighted in yellow.

Headend	Endpoint	Color	Admin St.	Oper St.	Actions	
<input checked="" type="checkbox"/>	S1AG1E1	S5AG1E2	63212	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	SBAG1-1	S6C1	5522	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	SSAG1-1	S3AG1-1	102	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	SC1	S7C1	22332	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	S10C1	S3C1	5123	<span style="color: green;">●</span>	<span style="color: red;">●</span>	...
<input type="checkbox"/>	S10AG2E3	S6AG2E1	3215	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	S2AG1-1	S2AG2-2	106	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	S10AG1-1	S10AG2E2	434	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	S2AG1E3	S2C1	6325	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	S10AG1-1	S10AG1E1	6325	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	SSC2	P-TOPRIGHT	100	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	S1C2	S2C1	100	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	S2AG1-1	S2AG2E3	100	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input checked="" type="checkbox"/>	S1AG2E1	S1AG1E2	100	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	SSC1	S1C2	111	<span style="color: green;">●</span>	<span style="color: red;">●</span>	...

**ステップ 11** ミニダッシュボードを使用して、特定の SR-TE ポリシーにドリルダウンして焦点を当てることもできます。

PCE によって開始されたポリシーのみを表示するように [SR Policy] テーブルをフィルタ処理するには、[SR-MPLS Mini Dashboard] で [PCE Init] の値をクリックします。[適用されたフィルタ (Filters Applied)] テキストが表示されます。

The screenshot shows the Cisco Crosswork Network Automation interface. On the left, there is a navigation sidebar. The main area displays a network topology with nodes representing different locations: PE4-ASBRk.cisco.com, P3-NC-0501, PE1-ASBRk, PE4-ASBRk, PE7-XRvRk, PE3-ASBRk, PE2-ASBRk, PE5-ASBRk, and PE6-XRvRk.cisco.com. On the right, the 'Traffic Engineering' dashboard is visible, showing a summary for SR-MPLS, SRv6, and RSVP-TE. Below this is a table titled 'SR POLICY' with columns for Headend, Endpoint, Color, Admi..., Oper ..., and Actions. The 'PCE Init' value '4' and the 'Filters Applied (1)' text are highlighted in red.

Headend	Endpoint	Color	Admi...	Oper ...	Actions	
<input type="checkbox"/>	PE1-AS...	P3-NCS...	345	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	PE4-AS...	PE7-XR...	123	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	PE7-XR...	P4-NCS...	234	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...
<input type="checkbox"/>	PE4-AS...	PE2-AS...	2258	<span style="color: green;">●</span>	<span style="color: green;">●</span>	...

**ステップ 12** フィルタ条件を削除するには、[適用されたフィルタ (Filters Applied)] > [すべてのフィルタをクリア (Clear All Filters)] をクリックします。複数のフィルタが適用されている場合は、個々のフィルタを選択することもできます。

## 複数の候補パス (MCP) の検索

MCP を可視化することで、現在アクティブなパスに代わる適切なパスを確認できます。この場合、手動でデバイスを設定し、アクティブになるパスを変更できます。

### 特記事項

- MCP を設定した PCC によって初期化された SR-TE ポリシーのみがサポートされます。
- Crosswork 最適化エンジンでは、ダイナミックパスと明示パスは区別されません。[Policy Type] フィールドの値は「Unknown」と表示されます。
- アクティブな明示パスは表示できますが、非アクティブな候補明示パスは UI に表示できません。

### 始める前に

ポリシーは、トラフィックエンジニアリングのトポロジマップで表示する前に、デバイス上で MCP を指定して設定する必要があります。この設定は、手動で、または Crosswork ネットワークコントローラ 内で実行できます。

---

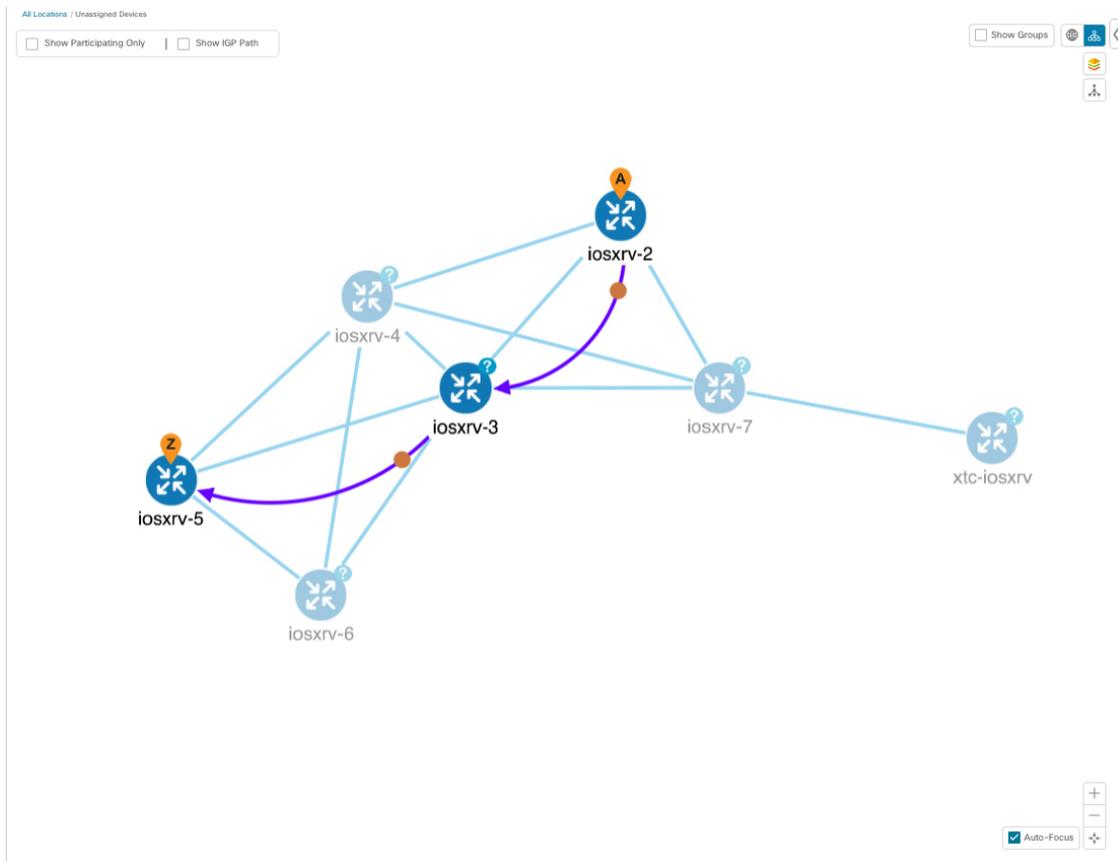
**ステップ 1** メインメニューから、[Traffic Engineering] > [Traffic Engineering] > [SR-MPLS] または [SRv6] タブを選択します。

**ステップ 2** MCP が設定されているアクティブな SR-TE ポリシーに移動し、トポロジマップで表示します。

- a) MCP が設定されている SR-TE ポリシーの横にあるチェックボックスをオンにします。
- b) トポロジマップに強調表示されている SR-TE ポリシーを表示します。

この例では、アクティブなパスが iosxrv-2 > iosxrv-3 > iosxrv-5 の順で移動していることがわかります。

## 複数の候補パス (MCP) の検索



ステップ 3 候補パスのリストを表示します。

- a) [SR-TE Policy] テーブルの [Actions] 列で、 > **[View Details]** をクリックします。[SR Policy Details] ウィンドウに、候補パスのリストがポリシーの詳細とともに表示されます。緑色の丸はアクティブなパス

を示します。

The screenshot shows the 'SR Policy Details' window. It includes a 'Summary' section with various status and configuration parameters, and a 'Candidate Path' section with a table of paths.

**Summary**

- Headend: iosxrv-2 (TE RiD: 192.168.0.2) PCC IP: 192.168.0.101  
Source IP: 192.168.0.2
- Endpoint: iosxrv-5 (TE RiD: 192.168.0.5)  
Dest IP: 192.168.0.5
- Color: 20000
- Admin State: Up
- Oper State: Up
- Binding SID: 24011
- Profile ID: -
- Utilization (Mbps): 0 Mbps
- Delay: -
- BWOD Policy Bandwidth (Mbps): 0 Mbps
- Accumulated Metric: 2
- Delegated PCE: 10.194.59.124
- Non-delegated PCEs: -
- PCE Computed Time: 26-Aug-2021 03:31:10 PM PDT
- Last Update: 26-Aug-2021 03:39:23 PM PDT

**Candidate Path**

Path Name	Preference	Path Type
<input checked="" type="checkbox"/> > cfg_test_mcp_diff_paths_discr_10000	10000	Unknown
<input type="checkbox"/> > cfg_test_mcp_diff_paths_discr_5000	5000	Unknown

An arrow points to the checked checkbox for the path with preference 10000. The text 'Active Path' is written above the table, and 'Expand All' is a button to the right.

**ステップ 4** 個々のパスを展開するか、[Expand All] をクリックして各パスの詳細を表示できます。各セグメントにカーソルを合わせると、そのセグメントがマップ上で強調表示されます。

**ステップ 5** トポロジマップで候補パスを可視化します。

a) 候補パスの横にあるチェックボックスをオンにします。

(注) 明示的な候補パスを選択または表示することはできません。

SR Policy Details

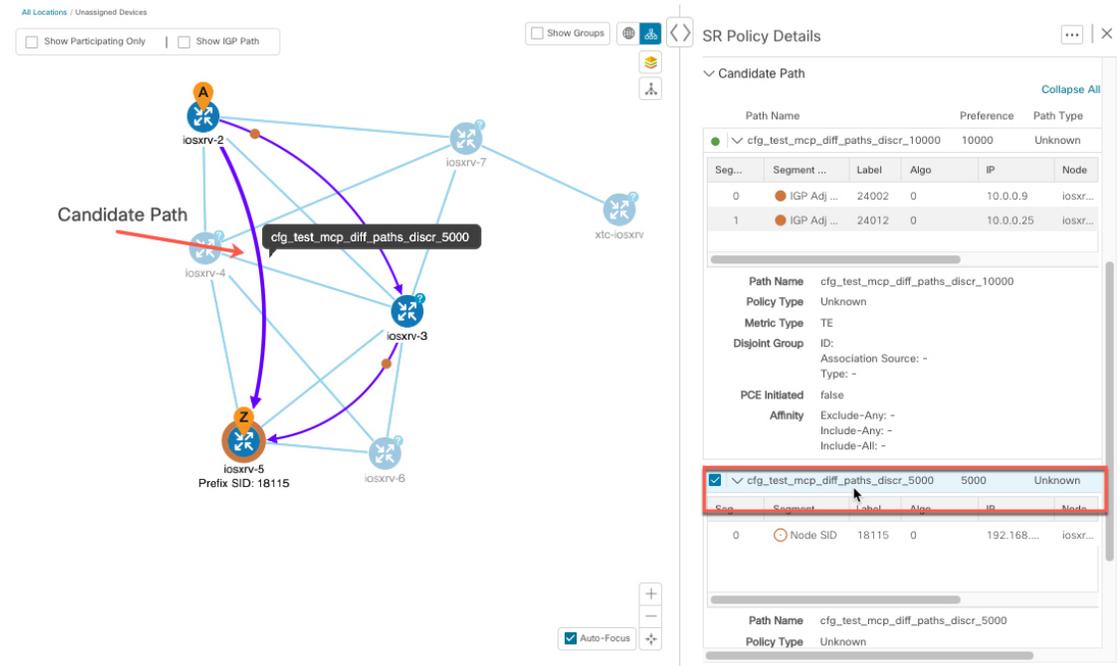
PCE Computed Time 26-Aug-2021 03:31:10 PM PDT  
Last Update 26-Aug-2021 03:39:23 PM PDT

▼ Candidate Path Collapse All

Path Name	Preference	Path Type																								
● ▼ cfg_test_mcp_diff_paths_discr_10000	10000	Unknown																								
<table border="1"> <thead> <tr> <th>Segm...</th> <th>Segment Type</th> <th>Label</th> <th>Algo</th> <th>IP</th> <th>Node</th> <th>Interface</th> <th>Sid T...</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>● IGP Adj SID</td> <td>24002</td> <td>0</td> <td>10.0.0.9</td> <td>iosxrv-2</td> <td></td> <td>P</td> </tr> <tr> <td>1</td> <td>● IGP Adj SID</td> <td>24012</td> <td>0</td> <td>10.0.0.25</td> <td>iosxrv-3</td> <td></td> <td>P</td> </tr> </tbody> </table>	Segm...	Segment Type	Label	Algo	IP	Node	Interface	Sid T...	0	● IGP Adj SID	24002	0	10.0.0.9	iosxrv-2		P	1	● IGP Adj SID	24012	0	10.0.0.25	iosxrv-3		P		
Segm...	Segment Type	Label	Algo	IP	Node	Interface	Sid T...																			
0	● IGP Adj SID	24002	0	10.0.0.9	iosxrv-2		P																			
1	● IGP Adj SID	24012	0	10.0.0.25	iosxrv-3		P																			
<p><b>Path Name</b> cfg_test_mcp_diff_paths_discr_10000</p> <p><b>Policy Type</b> Unknown</p> <p><b>Metric Type</b> TE</p> <p><b>Disjoint Group</b> ID: Association Source: - Type: -</p> <p><b>PCE Initiated</b> false</p> <p><b>Affinity</b> Exclude-Any: - Include-Any: - Include-All: -</p>																										
☑ ▼ cfg_test_mcp_diff_paths_discr_5000	5000	Unknown																								
<table border="1"> <thead> <tr> <th>Segm...</th> <th>Segment Type</th> <th>Label</th> <th>Algo</th> <th>IP</th> <th>Node</th> <th>Interface</th> <th>Sid T...</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>○ Node SID</td> <td>18115</td> <td>0</td> <td>192.168.0.5</td> <td>iosxrv-5</td> <td></td> <td></td> </tr> </tbody> </table>	Segm...	Segment Type	Label	Algo	IP	Node	Interface	Sid T...	0	○ Node SID	18115	0	192.168.0.5	iosxrv-5												
Segm...	Segment Type	Label	Algo	IP	Node	Interface	Sid T...																			
0	○ Node SID	18115	0	192.168.0.5	iosxrv-5																					
<p><b>Path Name</b> cfg_test_mcp_diff_paths_discr_5000</p> <p><b>Policy Type</b> Unknown</p> <p><b>Metric Type</b> IGP</p> <p><b>Disjoint Group</b> ID: Association Source: - Type: -</p> <p><b>PCE Initiated</b> false</p> <p><b>Affinity</b> Exclude-Any: - Include-Any: - Include-All: -</p>																										

- b) [Candidate Path] エリアで、候補パス名の上にマウスポインタを合わせます。候補パスがトポロジマップに強調表示されます。

この例では、代替パスが iosxrv-2 から iosxrv-5 に直接移動していることがわかります。



## 定義済みのバインディングセグメント ID (B-SID) ラベルに関連付けられた基盤となるパスの可視化

Crosswork 最適化エンジンを使用すると、デバイスで手動で設定した、または Crosswork ネットワークコントローラを使用して設定した B-SID ホップの基盤となるパスを可視化できます。この例では、SR-MPLS ポリシーホップの B-SID ラベルとして 24020 を割り当てています。



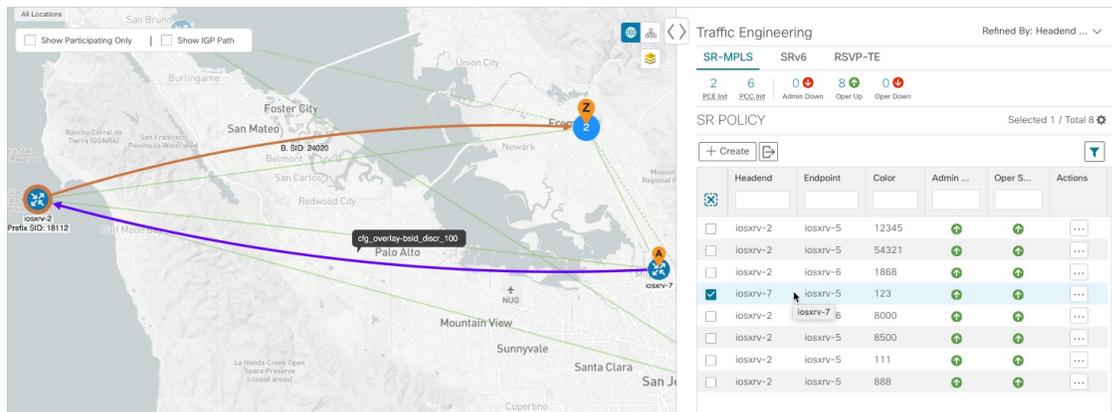
(注) 拡大表示するには、画像の例をクリックします。

SR-MPLS または SRv6 ポリシーに関する B-SID の基盤となるパスを表示するには、次の手順を実行します。

- ステップ 1** メインメニューから、[トラフィックエンジニアリング (Traffic Engineering)] > [トラフィックエンジニアリング (Traffic Engineering)] > [SR-MPLS] または [SRv6] タブを選択します。
- ステップ 2** B-SID ラベルが割り当てられたホップを含む SR-MPLS ポリシーの横にあるチェックボックスをオンにし、SR-MPLS 行の任意の部分にマウスポインタを合わせると B-SID 名が表示されます。B-SID パスは、トポロジマップ上でオレンジ色で強調表示されます。

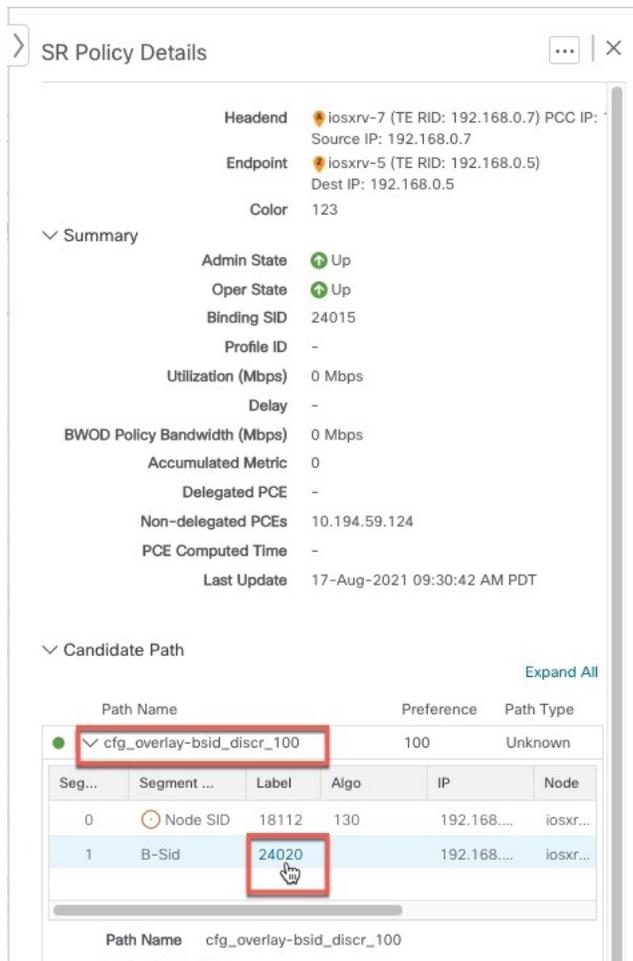
この例では、パスが iosxrv-2 から 2 デバイスクラスタに移動していることがわかります。

定義済みのバインディングセグメント ID (B-SID) ラベルに関連付けられた基盤となるパスの可視化



ステップ3 [アクション (Actions)] 列で、⋮ > [詳細の表示 (View Details)] をクリックします。

ステップ4 [SR Policy Details] ウィンドウで、アクティブパス名を展開し、B-SID ラベルをクリックします。



ステップ5 基盤となるパスの [SR ポリシーの詳細 (SR Policy Details)] ウィンドウで、アクティブなパス名を展開して詳細を表示します。この例では、基盤となるパスは実際には **iosxrv-2** > **iosxrv-3** > **iosxrv-5** となっています。

**SR Policy Details**

**Headend** iosxr-2 (TE RID: 192.168.0.2) PCC IP: 192.168.0.2  
**Endpoint** iosxr-5 (TE RID: 192.168.0.5) Dest IP: 192.168.0.5  
**Color** 111

**Summary**

- Admin State: Up
- Oper State: Up
- Binding SID: 24020
- Profile ID: -
- Utilization (Mbps): 0 Mbps
- Delay: -
- BWOD Policy Bandwidth (Mbps): 0 Mbps
- Accumulated Metric: 0
- Delegated PCE: -
- Non-delegated PCEs: 10.194.59.124
- PCE Computed Time: -
- Last Update: 17-Aug-2021 01:29:02 AM PDT

**Candidate Path**

Path Name	Preference	Path Type
cfg_test_explicit_mcp_discr_600	600	Unknown

Seg...	Segment ...	Label	Algo	IP	Node
0	Node SID	18113	0	192.168...	iosxr...
1	Node SID	18115	0	192.168...	iosxr...

**Path Name** cfg\_test\_explicit\_mcp\_discr\_600  
**Policy Type** Unknown  
**Metric Type** TE  
**Disjoint Group** ID: -  
 Association Source: -  
 Type: -  
**PCE Initiated** false

## ネイティブ SR パスの可視化

Crosswork 最適化エンジン L3VPN サービスのトポロジには、実際の物理パスではなく、論理パスのみが表示されます。この機能ではマルチパスが使用されるため、すべての ECMP パスは送信元と宛先の間に表示されます。ネイティブパスを可視化すると、OAM（運用、管理、メンテナンス）アクティビティで、ラベルスイッチドパス（LSP）をモニターして転送の問題を迅速に隔離できるため、ネットワークの異常検出とトラブルシューティングに役立ちます。



(注) これは、SR-MPLS ポリシーにのみ適用されます。

パスクエリを作成するには、次の手順を実行します。

### 始める前に

デバイスの要件を満たしていることを確認します。「[ネイティブパスデバイスの前提条件の可視化 \(53 ページ\)](#)」を参照してください。

詳細については、[Cisco Crosswork Infrastructure](#) および [アプリケーションアドミニストレーションガイド](#) および [Cisco Crosswork Infrastructure](#) および [アプリケーションインストールガイド](#) を参照してください。

- ステップ 1** メインメニューから、[トラフィックエンジニアリング (Traffic Engineering)] > [パスクエリ (Path Query)] を選択します。
- ステップ 2** [クエリパスダッシュボード (Query Path Dashboard)] で、[新しいクエリ (New Query)] をクリックします。
- ステップ 3** [新しいパスクエリ (New Path Query)] で必要な値を選択し、[パスを取得 (Get Paths)] をクリックします。
- ステップ 4** [結果の表示 (View Result)] をクリックして、クエリ結果を表示します。
- ステップ 5** (オプション) [結果 (Result)] ポップアップで、[以前の結果の表示 (View Past Result)] をクリックします。クエリ ID を確認して、利用可能な結果を表示します。

例：

次の例では、使用可能なパス (Path 0) を表示できます。

図 10: パスの詳細

The screenshot displays the Path Query interface. On the left, a map of the United States shows a path highlighted in blue between two points labeled 'P-TOPLEFT' and 'P-TOPRIGHT'. On the right, the 'Path Details' panel is open, showing the following information:

**Path Details**

Select from the fields below to find available Native SR IGP Paths

Select Service: Select Type, Select Instance

Headend: PE-A (100.100.100.5)

Endpoint: PE-B (100.100.100.6)

Get Paths

**Available Paths**

**Path 0**

Output: tunnel-16220

NextHop: 20.20.10.2

Source: 100.100.100.5

Destination: 127.0.0.0

**Hop Details**

Hop Index: 0 | Hop Origin IP: 100.100.100.5 | Hop Destination IP: 20.20.10.2 | MRU: 1500 | Labels: [24007/implicit-null] | ret code: 0 | return char: | multipaths: 0

Hop Index: 1 | Hop Origin IP: 20.20.10.2 | Hop Destination IP: 20.20.10.14 | MRU: 1500 | Labels: [24022/implicit-null] | ret code: 8 | return char: L | multipaths: 1

Hop Index: 2 | Hop Origin IP: 20.20.10.14 | Hop Destination IP: 20.20.10.26 | MRU: 1500 | Labels: [implicit-null/implicit-null] | ret code: 8 | return char: L | multipaths: 1

Hop Index: 3 | Hop Origin IP: 20.20.10.26 | MRU: 0 | ret code: 3 | return char: ! | multipaths: 0

- ステップ 6** [アクション (Actions)] 列で、[詳細の表示 (View Details)] をクリックします。
- ステップ 7** 使用可能なパスから [Path 0] をクリックして展開し、アクティブなパスを表示します。

例：

図 11: パスの詳細

The screenshot shows a 'Path Details' window with the following configuration:

- Select Service: Select Type (dropdown), Select Instance (dropdown)
- Headend \*: PE-A (100.100.100.5)
- Endpoint \*: PE-B (100.100.100.6)
- Get Paths button

Available Paths section:

Path 0	Output	Nexthop	Source	Destination
	tunnel-te220	20.20.10.2	100.100.100.5	127.0.0.0

Hop Details for Path 0:

- Hop Index: 0 | Hop Origin IP: 100.100.100.5 | Hop Destination IP: 20.20.10.2 | MRU: 1500 | Labels: [24007/implicit-null] | ret code: 0 | return char: | multipaths: 0
- Hop Index: 1 | Hop Origin IP: 20.20.10.2 | Hop Destination IP: 20.20.10.14 | MRU: 1500 | Labels: [24022/implicit-null] | ret code: 8 | return char: L | multipaths: 1
- Hop Index: 2 | Hop Origin IP: 20.20.10.14 | Hop Destination IP: 20.20.10.26 | MRU: 1500 | Labels: [implicit-null/implicit-null] | ret code: 8 | return char: L | multipaths: 1
- Hop Index: 3 | Hop Origin IP: 20.20.10.26 | MRU: 0 | ret code: 3 | return char: ? | multipaths: 0

## ネイティブパスデバイスの前提条件の可視化

ネイティブパスを可視化する前に、次のデバイスソフトウェアと設定の要件を満たしていることを確認します。

1. デバイスは Cisco IOS XR 7.3.2 を実行している必要があります。show version コマンドを実行して確認します。
2. デバイスで GRPC を有効にする必要があります。
  1. show grpc を実行して GRPC の設定を確認します。以下のように表示されている必要があります。

```
grpc
port 50000
no-tls
address-family dual
!
mpls oam
!
```



- (注)
- address-family は、IPv4 トポロジでのみ必要です。
  - セキュアな接続で GRPC を有効にするには、セキュリティ証明書をアップロードしてデバイスに接続する必要があります。

3. デバイスでは、GNMI 機能を有効にして設定する必要があります。

1. [Device Management] で、デバイスをクリックし、デバイスの詳細 (📄) を表示します。
2. GNMI 機能、および接続の詳細が設定されていることを確認します。

▼ Connectivity Details

Protocol *	IP Address / Subnet Mask *	Port *	Timeout	Encoding Type
TELNET	172.29.105.236 / 24	23	30	
SNMP	172.29.105.236 / 24	161	30	
SSH	172.29.105.236 / 24	22	30	
GNMI	172.29.105.236 / 24	57400	30	JSON

+ Add Another

Capability\*

YANG MDT
  TL1
  YANG CLI
  YANG EPNM
  SNMP
  GNMI

4. デバイスには、CDG ルータの静的アドレスが必要です。スタティックルートは、デバイスからサウスバウンド CDG IP アドレスに追加する必要があります。次に例を示します。

```
RP/0/RP0/CPU0:xrvr-7.2.1#config
```

```
RP/0/RP0/CPU0:xrvr-7.2.1(config)#router static
```

```
RP/0/RP0/CPU0:xrvr-7.2.1(config-static)#address-family ipv4 unicast <CDG Southbound interface IP: eg. 172.24.97.110> <Device Gateway eg: 172.29.105.1>
```

```
RP/0/RP0/CPU0:xrvr-7.2.1(config-static)#commit
```



## 第 4 章

# フレキシブルアルゴリズムの可視化

フレキシブルアルゴリズムを使用すると、オペレータは、独自のニーズと制約（特定のメトリックとリンクプロパティ）に従って IGP 最短パスをカスタマイズおよび計算できます。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。たとえば、フレキシブルアルゴリズムでは、複数の論理プレーンを持つネットワークに対する特定のプレーンへのパスを制限できます。アルゴリズムの意味が標準規格によってではなく、ユーザー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。

Crosswork を使用すると、フレキシブルアルゴリズムに基づいて IGP トポロジをフィルタ処理し、特定の一連のトランスポート特性を提供できるネットワークのサブセットを可視化できます。フレキシブルアルゴリズムのトポロジを可視化する機能により、フレキシブルアルゴリズムの展開、維持、および設定されたフレキシブルアルゴリズムの目的がネットワークで実現されていることを検証するための重要なツールが提供されます。たとえば、サービスの可用性を向上させるために、フレキシブルアルゴリズムを使用して分離論理トポロジを定義し、ネットワーク障害に対する復元力を高めることができます。Crosswork を使用すると、両方のフレキシブルアルゴリズムのトポロジを同時に可視化し、共通のノードやリンクがないことを確認できます。また、共通のノードやリンクがある場合は、共通のネットワーク要素を確認して、フレキシブルアルゴリズムの設定を更新できます。

### 特記事項

- フレキシブルアルゴリズムの情報は、SR-PCE（Cisco IOS XR 7.3.2 を実行）から収集されます。
- フレキシブルアルゴリズムの制約を指定して、SR-MPLS ポリシーまたは RSVP-TE トンネルをプロビジョニングすることはできません。
- 複数のドメインにあるフレキシブルアルゴリズムはフィルタ処理できません。



(注) この項では、ナビゲーションを [トラフィックエンジニアリング (Traffic Engineering)] > [トラフィックエンジニアリング (Traffic Engineering)] と記載しています。ただし、Crosswork Network Controller ソリューションを使用する場合、ナビゲーションは [トラフィックエンジニアリング & サービス (Traffic Engineering & Services)] > [トラフィックエンジニアリング (Traffic Engineering)] です。

- [フレキシブルアルゴリズムの可視化 \(56 ページ\)](#)
- [フレキシブルアルゴリズムのアフィニティの設定 \(57 ページ\)](#)
- [リンクとデバイスのフレキシブルアルゴリズムの検索 \(59 ページ\)](#)

## フレキシブルアルゴリズムの可視化

Crosswork を使用すると、ネットワーク内で手動で設定したフレキシブルアルゴリズムのノードやリンクを可視化できます。

### 始める前に

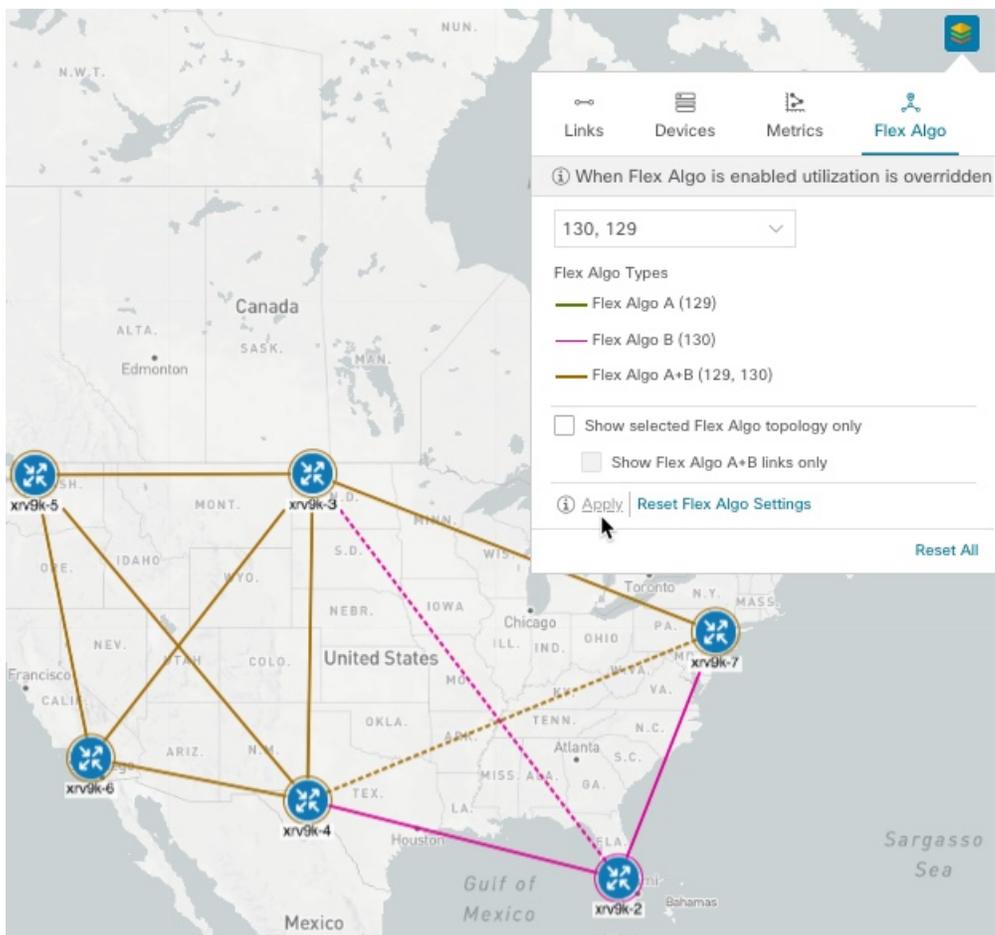
- ネットワークでフレキシブルアルゴリズムを設定する必要があります。特定のデバイスの SR 設定のマニュアルを参照して、説明とサポートされている設定コマンドを確認してください（『*Asr900 Flex Algorithm*』など）。
- ネットワークで使用されているフレキシブルアルゴリズム ID を知っている必要があります。フレキシブルアルゴリズム メンバーシップを表示するには、[リンクとデバイスのフレキシブルアルゴリズムの検索 \(59 ページ\)](#) を参照してください。



(注) フレキシブルアルゴリズム ID が異なるドメイン間で同じ場合、フレキシブルアルゴリズムは可視化できません。

- ステップ 1** メインメニューから、**[Traffic Engineering]** > **[Traffic Engineering]** を選択します。
- ステップ 2** トポロジマップから、 をクリックします。
- ステップ 3** **[Flex Algo]** タブをクリックします。
- ステップ 4** ドロップダウンリストから、最大 2 つのフレキシブルアルゴリズム ID を選択します。
- ステップ 5** **[Flexible Algorithm Types]** を表示し、選択内容が正しいことを確認します。各フレキシブルアルゴリズムの色の割り当てにも注意してください。
- ステップ 6** (オプション) **[Show selected Flex Algo topology only]** チェックボックスをオンにして、トポロジマップでフレキシブルアルゴリズムを分離します。このオプションを有効にすると、SR ポリシーの選択が無効になります。
  - a) 両方のフレキシブルアルゴリズムに参加しているリンクとノードのみを表示するには、**[Show Flex Algo A+B links only]** をオンにします。
- ステップ 7** **[Apply]** をクリックします。フレキシブルアルゴリズムの選択内容に追加の変更を加えるには、**[Apply]** をクリックして、トポロジマップの更新内容を確認する必要があります。

例：



- (注)
- 複数のドメインにあるフレキシブルアルゴリズム ID はフィルタ処理できません。ドメインフィルタリングは、フレキシブルアルゴリズムに基づいてサポートされていません。
  - 選択したフレキシブルアルゴリズムが基準で定義されているが、（青色ですべてのノードやリンクを含むように定義されたアフィニティなど）一致するリンクとノードの組み合わせがない場合、トポジマップは空白になります。選択したフレキシブルアルゴリズムがノードまたはリンクに設定されていない場合は、青色（デフォルト）のリンクまたはノードの色が表示されます。

**ステップ 8** (オプション) [Save View] をクリックして、トポジビューとフレキシブルアルゴリズムの選択を保存します。

## フレキシブルアルゴリズムのアフィニティの設定

デバイスで定義されたフレキシブルアルゴリズムのアフィニティは Crosswork 最適化エンジンによって収集されません。アフィニティマッピング名は可視化に使用されます。このため、デ

バイスインターフェイスでフレキシブルアルゴリズムのアフィニティを手動で収集してから、デバイスインターフェイスで使用されているものと同じ名前とビットを使用してUI内でアフィニティマッピングを定義する必要があります。

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。

```
router isis instance flex-algo algo
```

```
router ospf process flex-algo algo
```

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

```
□□□□□□□□□□□□
```



(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、リンク上でアダプ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、リンク上でアダプ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。

- **name** : アフィニティマップの名前

```
affinity exclude-any name1, name2, ...
```

- **priority value** : 優先順位

```
priority priority value
```

特定のデバイスの SR 設定のマニュアルを参照して、説明とサポートされている設定コマンドを確認してください（『[Segment Routing Configuration Guide for Cisco ASR 9000 Series Routers](#)』など）。



(注) アフィニティマッピングを編集または削除するには、関連するメニューオプションをクリックします。

- 
- ステップ 1** メインメニューから、[トラフィックエンジニアリング (Traffic Engineering)] > [アフィニティ (Affinities)] > [Flex-Algoアフィニティ (Flex-Algo Affinities)] を選択します。
- ステップ 2** 新しいフレキシブルアルゴリズムのアフィニティマッピングを追加するには、[+作成 (+Create)] をクリックします。
- ステップ 3** 割り当てる名前 (色) とビットを入力します。
- ステップ 4** [保存 (Save)] をクリックしてマッピングを保存します。
- 

## リンクとデバイスのフレキシブルアルゴリズムの検索

デバイスまたはリンクがメンバーとなっているすべてのフレキシブルアルゴリズムを確認するには、次の手順を実行します。

### 始める前に

ネットワークでフレキシブルアルゴリズムを設定する必要があります。

---

- ステップ 1** メインメニューから、[Traffic Engineering] > [Traffic Engineering] を選択します。
- ステップ 2** デバイスのフレキシブルアルゴリズムメンバーシップを表示するには、次の手順を実行します。
- トポロジマップから、少なくとも 1 つのフレキシブルアルゴリズムのメンバーであることがわかっているデバイスをクリックします。
  - [Device Details] ウィンドウで、[Flex-Algo] タブをクリックします。

Device Details ×

Links SR-MPLS SRv6 RSVP-TE **Flex-Algo**

▼ Algo 128

**Participating** Yes

**Elected Definition** Metric Type: LATENCY  
 Exclude-Any Affinity: Yellow(253), Red(255)  
 Include-Any Affinity: Blue(3)  
 Include-All Affinity: Green(5)

**Advertised** Yes  
 Priority: 210  
 Definition Equal to Local: No

▼ Algo 130

**Participating** Yes

**Elected Definition** Metric Type: LATENCY  
 Exclude-Any Affinity:  
 Include-Any Affinity:  
 Include-All Affinity:

**Advertised** No  
 Priority: 200

**ステップ 3** リンクのフレキシブルアルゴリズムメンバーシップを表示するには、次の手順を実行します。

- a) トポロジマップから、少なくとも 1 つのフレキシブルアルゴリズムのメンバーであることがわかっているリンクをクリックします。
- b) [Links] ページで、いずれかのリンクタイプをクリックします。
- c) デフォルトでは、[Summary] タブが [Link Details] ウィンドウ内に表示されます。外部エージェントトポロジを表示して、各送信元デバイスと宛先デバイスが属するフレキシブルアルゴリズムを確認します。

Link Details



Summary SR-MPLS SRv6 RSVP-TE

**Name** GigabitEthernet0/0/0/1-GigabitEthernet0/0/0/0  
**State** ↑ Up  
**Link Type** L3 ISIS IPV4  
**ISIS Level** 2  
**Last Update** 24-Aug-2021 09:51:59 AM PDT

	A Side	Z Side
<b>Node</b>	xrv9k-7	xrv9k-3
<b>TE Router ID</b>	192.168.0.7	192.168.0.3
<b>IF Name</b>	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/0
<b>IF Description</b>	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/0
<b>IF Alias</b>	T-SDN Interface	
<b>Type</b>	ETHERNETCSMACD	ETHERNETCSMACD
<b>IP Address</b>	10.0.0.42	10.0.0.41
<b>Utilization</b>	0% (0Bps/1Gbps)	0% (0Bps/1Gbps)
<b>IGP Metric</b>	10	10
<b>Delay Metric</b>	10	10
<b>TE Metric</b>	10	10
<b>FA Affinities</b>		
<b>Admin Groups</b>	2,5	2,5
<b>FA Topologies</b>	128, 129, 130, 131, 132, 133, 134, 207	128, 129, 130, 131, 132, 133, 134





## 第 5 章

# RSVP-TE トンネルの可視化



- (注) この項では、ナビゲーションを [トラフィックエンジニアリング (Traffic Engineering)] > [トラフィックエンジニアリング (Traffic Engineering)] と記載しています。ただし、Crosswork Network Controller ソリューションを使用する場合、ナビゲーションは [トラフィックエンジニアリング & サービス (Traffic Engineering & Services)] > [トラフィックエンジニアリング (Traffic Engineering)] です。

ここでは、次の内容について説明します。

- [トポロジマップでの RSVP-TE トンネルの表示 \(63 ページ\)](#)
- [RSVP-TE トンネルの詳細の表示 \(66 ページ\)](#)
- [トラフィック エンジニアリング デバイスの詳細の表示 \(68 ページ\)](#)

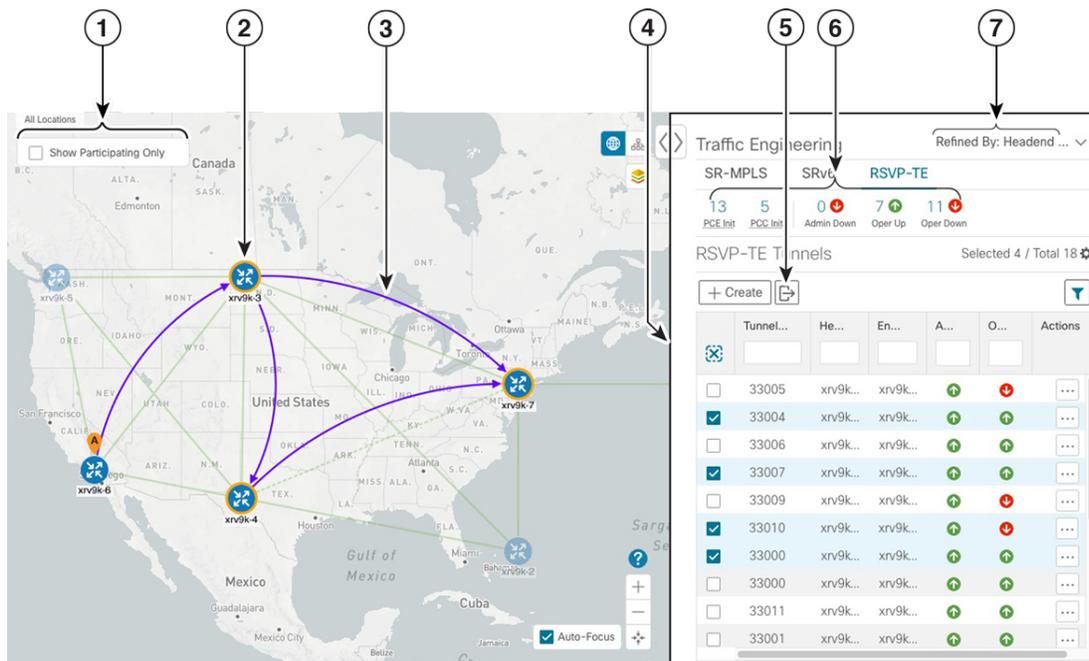
## トポロジマップでの RSVP-TE トンネルの表示

RSVP-TE の可視化のためにトラフィック エンジニアリングのトポロジマップを取得するには、[トラフィックエンジニアリング (Traffic Engineering)] > [トラフィックエンジニアリング (Traffic Engineering)] > [RSVP-TE] を選択します。



- (注) この項では、ナビゲーションを [トラフィックエンジニアリング (Traffic Engineering)] > [トラフィックエンジニアリング (Traffic Engineering)] と記載しています。ただし、Crosswork Network Controller ソリューションを使用する場合、ナビゲーションは [トラフィックエンジニアリング & サービス (Traffic Engineering & Services)] > [トラフィックエンジニアリング (Traffic Engineering)] です。

図 12: トラフィック エンジニアリング UI : RSVP-TE トンネル



522085

引き出し線番号	説明
1	[参加デバイスのみ表示 (Show Participating Only)] をクリックして、選択した RSVP-TE トンネルに属するリンクのみを表示します。他のすべてのリンクとデバイスは表示されなくなります。
2	オレンジ色のアウトラインが付いたデバイス (🌀) は、ストリクトホップであることを示します。オレンジ色の点線のアウトラインは、ルーズホップが検出されたことを示します。  (注) RSVP-TE トンネルは、UI でのプロビジョニング時にルーズホップを使用して設定できません。

引き出し線番号	説明
3	<p>RSVP-TE トンネルは [RSVP-TE Tunnels] テーブルで選択されると、送信元と宛先を示す紫色の矢印線としてマップに表示されます。</p> <ul style="list-style-type: none"> <li>レコードルートオブジェクト (RRO) パスは直線に表示されます。</li> <li>明示的ルートオブジェクト (ERO) パスは曲線として表示されます。</li> </ul> <p>(注) RRO と ERO の両方のパスが使用可能な場合、デフォルトで RRO パスが表示されます。</p> <ul style="list-style-type: none"> <li>隣接セグメント ID (SID) は、パスに沿ったリンクに緑色のドット (●) として表示されます。</li> </ul> <p>A と Z の両方が 1 つのデバイスクラスタに表示される場合、クラスタ内の 1 つ以上のノードが送信元で、別のノードが宛先です。A+ は、1 つのノードから発信される複数の RSVP-TE トンネルがあることを示します。Z+ は、ノードが複数の RSVP-TE トンネルの宛先であることを示します。</p>
4	<p>このウィンドウの内容は、選択またはフィルタ処理された内容によって異なります。この例では、[RSVP-TE] タブが選択され、[RSVP-TE Tunnels] テーブルが表示されます。トポロジマップで選択した内容、または RSVP-TE トンネルを表示および管理しているプロセスに応じて、次の手順を実行できます。</p> <ul style="list-style-type: none"> <li><a href="#">最適化インテントベースのダイナミック RSVP-TE トンネルの作成 (83 ページ)</a></li> <li><a href="#">明示的 RSVP-TE トンネルの作成 (81 ページ)</a></li> <li><a href="#">RSVP-TE トンネルの変更 (84 ページ)</a></li> <li><a href="#">RSVP-TE トンネルの詳細の表示 (66 ページ)</a></li> <li><a href="#">デバイスとリンクの詳細の表示 (16 ページ)</a></li> </ul>
5	<p>CSV ファイルにすべてのデータをエクスポートします。選択またはフィルタ処理されたデータをエクスポートすることはできません。</p>
[6]	<p>[Mini Dashboard] には、動作中の RSVP-TE トンネルの概要と、[RSVP-TE] テーブルに現在リストされている PCC および PCE によって開始されたトンネルの数が表示されます。フィルタが適用されると、[Mini Dashboard] が更新され、[RSVP-TE] テーブルに表示される内容が反映されます。</p>

引き出し線番号	説明
7	<p>このオプションでは、グループフィルタ（使用している場合）をテーブルデータに適用する方法を選択できます。たとえば、[ヘッドエンドのみ（Headend only）]を選択した場合、ポリシーのヘッドエンドデバイスが選択されたグループにあるポリシーのみが表示されます。このフィルタを使用すると、特定の設定を確認でき、大規模なネットワークがある場合に役立ちます。</p> <p>フィルタオプション：</p> <ul style="list-style-type: none"> <li>• [Headend or Endpoint]：選択したグループ内のヘッドエンドまたはエンドポイントデバイスを含むポリシーを表示します。</li> <li>• [Headend and Endpoint]：ヘッドエンドとエンドポイントの両方がグループ内にある場合にポリシーを表示します。</li> <li>• [Headend only]：ポリシーのヘッドエンドデバイスが選択したグループにある場合にポリシーを表示します。</li> <li>• [Endpoint only]：ポリシーのエンドポイントデバイスが選択したグループ内にある場合にポリシーを表示します。</li> </ul>

## RSVP-TE トンネルの詳細の表示

バインディングラベル、委任 PCE、メトリックタイプ、ERO/RRO、遅延など、RSVP-TE トンネルの詳細を表示します。

ステップ 1 [アクション (Actions) ] 列で、いずれかの RSVP-TE トンネルに対して  > [詳細の表示 (View Details) ] をクリックします。

Traffic Engineering

SR-MPLS SRv6 **RSVP-TE**

13 2 0 7 6  
 ECE:Err FGC:Err Admin Down Oper Up Oper Down

RSVP-TE Tunnels Selected 1 / Total 15

Tunnel ID	Headend	Endpoint	Admin St...	Oper Sta...	Actions
<input type="checkbox"/> 33005	xrv9k-3	xrv9k-7	🟢	🔴	⋮
<input type="checkbox"/> 33004	xrv9k-3	xrv9k-7	🟢	🟢	⋮
<input type="checkbox"/> 33006	xrv9k-3	xrv9k-7	🟢	🟢	⋮
<input type="checkbox"/> 33007	xrv9k-3	xrv9k-7	🟢	🟢	⋮
<input type="checkbox"/> 33009	xrv9k-3	xrv9k-7	🟢	🔴	⋮
<input type="checkbox"/> 33010	xrv9k-3	xrv9k-7	🟢	🟢	⋮
<input checked="" type="checkbox"/> 33000	xrv9k-6	xrv9k-7	🟢	🟢	View Details Edit / Delete
<input type="checkbox"/> 33000	xrv9k-7	xrv9k-5	🟢	🟢	⋮
<input type="checkbox"/> 33011	xrv9k-3	xrv9k-5	🟢	🟢	⋮
<input type="checkbox"/> 33001	xrv9k-7	xrv9k-5	🟢	🟢	⋮
<input type="checkbox"/> 32321	xrv9k-5	xrv9k-7	🟢	🔴	⋮
<input type="checkbox"/> 33013	xrv9k-3	xrv9k-7	🟢	🔴	⋮
<input type="checkbox"/> 33014	xrv9k-3	xrv9k-7	🟢	🔴	⋮
<input type="checkbox"/> 33015	xrv9k-3	xrv9k-7	🟢	🔴	⋮
<input type="checkbox"/> 1235	xrv9k-3	xrv9k-7	🟢	🔴	⋮

ステップ2 RSVP-TE トンネルの詳細を表示します。

- (注)
- RSVP-TE トンネルのエンドツーエンド遅延の場合、ドメイン間 RSVP-TE トンネルはすべて明示的である必要があります（パスに沿ったすべてのインターフェイスが隣接関係ホップとして指定されます）。
  - すべてのポリシーの [遅延 (Delay)] 値は 10 分ごとに計算されます。[遅延 (Delay)] 値の横にある [i] アイコンの上にマウスポインタを合わせると、値が最後に更新された時刻が表示されます。

RSVP-TE Tunnel Details
⋮ | ✕

---

**Headend** A xrv9k-6 (192.168.0.6)  
**Endpoint** Z xrv9k-7 (192.168.0.7)  
**Tunnel ID** 33000

Summary

- Description -
- Path Name 60701-rsvp
- LSP ID 6
- Path Type Unknown
- Admin State ↑ Up
- Oper State ↑ Up
- Utilization 0 Mbps
- Delay 109 ⏱
- Signaled Bandwidth 0 Mbps
- Setup / Hold Priority 7 / 7
- Metric Type IGP
- Fast Re-route (FRR) Disable
- Binding Label 24012
- Accumulated Metric 20
- Disjoint Group ID:  
Association Source: -  
Type: -
- PCE Initiated true
- Delegated PCE 2001:420:28f:2011:250:56ff:fe85:a025
- Non-delegated PCEs -
- Affinity Exclude-Any: -  
Include-Any: -  
Include-All: -
- PCE Computed Time 27-Oct-2021 12:33:03 PM PDT
- Last Update 27-Oct-2021 12:39:58 PM PDT

Last Updated ✕  
 27-Oct-2021 06:41:22 PM PDT

Explicit Route Object (ERO)

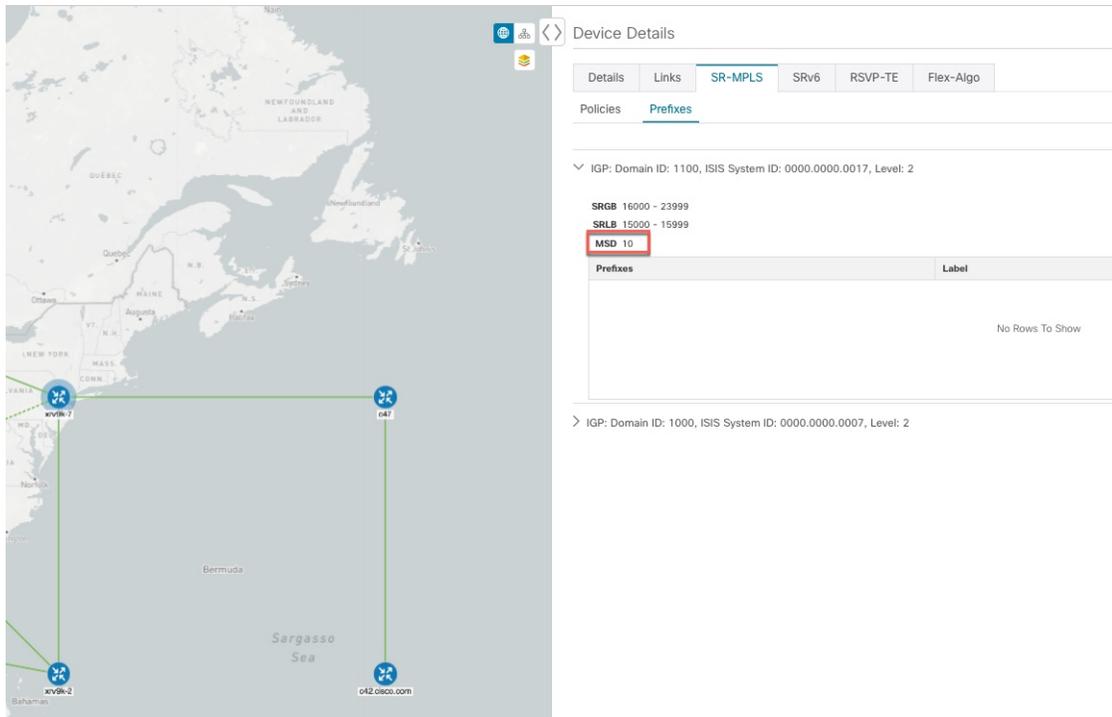
Hop	Node	IP	Interface Name	Type
0	xrv9k-3	10.0.0.29	GigabitEthernet0/0/0/4	Strict
1	xrv9k-7	10.0.0.42	GigabitEthernet0/0/0/1	Strict

## トラフィック エンジニアリング デバイスの詳細の表示

トラフィック エンジニアリング デバイスの詳細（SR-MPLS、SRv6、RSVP-TE、およびフレキシブルアルゴリズム情報）を表示するには、次の手順を実行します。

- ステップ 1** メインメニューから、[トラフィックエンジニアリング (Traffic Engineering)] > [トラフィックエンジニアリング (Traffic Engineering)] を選択します。
- ステップ 2** トラフィック エンジニアリング マップから、デバイスをクリックします。

**ステップ 3** [デバイスの詳細 (Device Details)] ページで、目的の[トラフィックエンジニアリング (Traffic Engineering)] タブをクリックします。このタブには、そのデバイスの関連データが表示されます。次の例は、デバイスの MSD 値を含む SR-MPLS プレフィックス情報を示しています。



Device Details

Details Links **SR-MPLS** SRv6 RSVP-TE Flex-Algo

Policies **Prefixes**

IGP: Domain ID: 1100, ISIS System ID: 0000.0000.0017, Level: 2

SRGB 16000 - 23999  
SRLB 15000 - 15999  
**MSD 10**

Prefixes	Label
No Rows To Show	

IGP: Domain ID: 1000, ISIS System ID: 0000.0000.0007, Level: 2





## 第 6 章

# SR-MPLS ポリシーのプロビジョニング



- (注)
- SRv6 ポリシーは Crosswork 最適化エンジンを使用してプロビジョニングできません。
  - この項では、ナビゲーションを[トラフィックエンジニアリング (Traffic Engineering)] > [トラフィックエンジニアリング (Traffic Engineering)] と記載しています。ただし、Crosswork Network Controller ソリューション内で Crosswork 最適化エンジンを使用する場合、ナビゲーションは[トラフィックエンジニアリング & サービス (Traffic Engineering & Services)] > [トラフィックエンジニアリング (Traffic Engineering)] > [トラフィックエンジニアリング (Traffic Engineering)] になります。

ここでは、次の内容について説明します。

- [SR-MPLS ポリシーのサポート \(71 ページ\)](#)
- [SR-TE ポリシー設定のソース \(74 ページ\)](#)
- [明示的 SR-MPLS ポリシーの作成 \(75 ページ\)](#)
- [リンクアフィニティの設定 \(75 ページ\)](#)
- [最適化インテントベースのダイナミック SR-MPLS ポリシーの作成 \(76 ページ\)](#)
- [SR-MPLS ポリシーの変更 \(78 ページ\)](#)

## SR-MPLS ポリシーのサポート

表 1: サポートされる機能

機能	注記
PCE によって開始されたポリシー (Crosswork によってプロビジョニングまたは検出)	—
PCC によって開始されたポリシー (Crosswork によって検出)	—

機能	注記
Crosswork によって検出された SR-MPLS オンデマンドネクストホップ (ODN) ポリシー	—
Crosswork の対象となるドメイン全体のルータで設定された単一の一貫性のあるセグメント ルーティング グローバル ブロック (SRGB)	インデックス SID が使用され、ポリシーのパスに沿って異なる SRGB ベースがある場合、ラベルはパスに沿って変更できます。
プレフィックス SID	—
隣接 SID	—
EPE 隣接 SID	—
保護された隣接 SID と保護されていない隣接 SID	—
通常のプレフィックス SID とストリクトプレフィックス SID	—
SR-MPLS ポリシー最適化目標の最小メトリック (IGP、TE、および遅延)	—
SR-MPLS ポリシーパスの制約 (アフィニティと分離)	分離グループまたはサブ ID ごとに 2 つの SR-MPLS ポリシーのみをサポート
明示的ポリシーまたはダイナミックポリシーのバインド SID	—
プロファイル ID	—

表 2: サポートされていない機能と制限事項

説明	注記
Crosswork を使用した複数の候補パスのプロビジョニング	これらのパスは、PCC 上に設定されている場合は検出されません。Crosswork は、これらのパスの設定をサポートしていません。
重み付け等コストマルチパス (WECMP)	—
候補パスごとに複数のセグメントリスト	<ul style="list-style-type: none"> <li>この設定はサポートされていません。</li> <li>これらのセグメントリストは、PCC 上に設定されている場合は検出されません。</li> </ul>

説明	注記
複数の候補パスの可視化	現在アクティブなパスのみがUIに表示されます。
セグメントリストホップとしての SID のバインド	—
SR IGP フレキシブルアルゴリズム (Flex Algo)	—
エニーキャスト SID	—
ポリシーのホップ カウント メトリックタイプ	Cisco Crosswork は、このメトリックタイプによるプロビジョニングをサポートせず、PCC 上に設定されている場合は、このメトリックタイプを検出しません。
SR 対応でないルータ	Cisco Crosswork によって検出されたすべてのルータが SR 対応であることを前提としています。
セグメントリストのヘッドエンド/エンドポイントとプレフィックス SID に TE ルータ ID 以外のループバック IP を使用する SR-MPLS ポリシー	詳細については、 <a href="#">Cisco Crosswork Infrastructure およびアプリケーション アドミニストレーションガイド</a> の「Onboard and Manage Devices」の章を参照してください。
IPv6 エンドポイント/ホップを使用してプロビジョニングされた SR-MPLS ポリシー	—
SRv6	分離グループ/サブ ID ごとに 2 つの SR-TE ポリシーのみ
SR-MPLS ポリシー最適化目標の最小メトリック (マージンあり)	Cisco Crosswork によってプロビジョニングされたポリシーではサポートされていません。PCC によって開始されたポリシーではマージンは検出されません。
SR-MPLS ポリシーの制約 (リソース除外またはメトリックバウンド)	Cisco Crosswork によってプロビジョニングされたポリシーではサポートされていません。PCC によって開始されたポリシーでは制約は検出されません。

## SR-TE ポリシー設定のソース

Crosswork 最適化エンジンによって検出および報告された SR-TE ポリシーは、次のソースから設定されている可能性があります。

- PCCによって開始：PCCに設定されたポリシー（[PCCによって開始されたSR-TEポリシーの例（74ページ）](#)を参照）。このポリシータイプは、UIに [Unknown] と表示されます。
- PCEによって開始：PCE上に設定されたか、またはCrosswork最適化エンジンによって動的に作成されたポリシー。UIを使用して設定されたSR-MPLSの明示的ポリシーまたは動的なポリシーは、Crosswork最適化エンジンで変更または削除できる唯一のSR-TEポリシータイプです。PCEによって開始されたポリシータイプは、次のいずれかになります。
  - **Dynamic**
  - **Explicit**
  - **Bandwidth on Demand**
  - **Bandwidth Optimization**
  - ローカル輻輳の緩和

## PCCによって開始されたSR-TEポリシーの例

次に、ヘッドエンドルータでのSR-TEポリシーの設定例を示します。このポリシーには、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。特定のデバイスのSR設定のマニュアルを参照して、説明とサポートされている設定コマンドを確認してください（『[Segment Routing Configuration Guide for Cisco ASR 9000 Series Routers](#)』など）。

```
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
!
!
!
!
```

## 明示的 SR-MPLS ポリシーの作成

このタスクでは、プレフィックスまたは隣接関係セグメント ID (SID リスト) のリストで構成される明示的な (固定) パスを使用して SR-MPLS ポリシーを作成します。各リストは、パス上のノードまたはリンクを表します。

**ステップ 1** メインメニューから、[Traffic Engineering] > [Traffic Engineering] > [SR-MPLS] タブを選択します。

**ステップ 2** [SRポリシー (SR Policies)] テーブルで、[+ 作成 (+ Create)] をクリックします。

**ステップ 3** 必要な SR-MPLS ポリシー値を入力します。各フィールドの説明を表示するには、 の上にマウスポインタを合わせます。

**ヒント** デバイスグループをセットアップしている場合は、[デバイスグループ (Device Groups)] ドロップダウンメニューからデバイスグループを選択できます。次に、トポロジマップを移動してズームインし、デバイスをクリックしてヘッドエンドまたはエンドポイントを選択します。

**ステップ 4** [ポリシーパス (Policy Path)] で、[明示的パス (Explicit Path)] をクリックし、パス名を入力します。

**ステップ 5** SR-MPLS ポリシーパスに含まれるセグメントを追加します。

**ステップ 6** [プレビュー (Preview)] をクリックします。

**ステップ 7** ポリシーパスをコミットする場合は、[プロビジョニング (Provision)] をクリックします。

**ステップ 8** SR-MPLS ポリシーの作成を検証します。

1. 新しい SR-MPLS ポリシーが [SR Policy] テーブルに表示されることを確認します。ポリシーの横にあるチェックボックスをクリックして、マップに強調表示されていることを確認することもできます。

(注) 新しくプロビジョニングされた SR-TE ポリシーは、ネットワークのサイズとパフォーマンスによっては [SRポリシー (SR Policy)] テーブルに表示されるまでに時間がかかることがあります。[SR Policy] テーブルは 30 秒ごとに更新されます。

2. 新しい SR-MPLS ポリシーの詳細を表示して確認します。[SRポリシー (SR Policy)] テーブルで、 をクリックして [表示 (View)] を選択します。

(注) ノード数、ポリシー数、またはインターフェイス数が多い拡張セットアップでは、ポリシーの展開中にタイムアウトが発生することがあります。タイムアウトオプションを設定するには、[Cisco Crosswork Infrastructure](#) および [アプリケーションアドミニストレーションガイド](#) を参照してください。

## リンクアフィニティの設定

デバイスで定義されたアフィニティは Crosswork 最適化エンジンによって収集されません。アフィニティマッピング名は、Crosswork 最適化エンジンでの可視化にのみ使用されます。この

ため、デバイスインターフェイスでアフィニティを手動で収集してから、デバイスインターフェイスで使用されているものと同じ名前とビットを使用して Crosswork 最適化エンジン内でアフィニティマッピングを定義する必要があります。Crosswork 最適化エンジンは、プロビジョニング時にビット情報のみを SR-PCE に送信します。

SR-TE ポリシーまたは RSVP-TE トンネルのアフィニティは、SR-TE ポリシーまたは RSVP-TE トンネルがアフィニティを持つリンク属性を指定するために使用されます。SR-TE ポリシーまたは RSVP-TE トンネルのパスを形成するのに適したリンクを決定します。これは 32 ビット値で、各ビット位置 (0-31) はリンク属性を表します。アフィニティマッピングは、各ビット位置または属性を色にマッピングするために使用されます。これにより、リンク属性の参照が容易になります。

特定のデバイスの SR 設定マニュアルを参照して、説明とサポートされている設定コマンドを確認してください (『[Asr9000 Configuration](#)』など)。



(注) アフィニティマッピングを編集または削除するには、関連するメニューオプションをクリックします。

**ステップ 1** メインメニューから、[トラフィックエンジニアリング (Traffic Engineering)] > [アフィニティ (Affinities)] を選択します。[マッピングの管理 (Manage Mapping)] をクリックして、SR-TE ポリシーまたは RSVP-TE トンネルの作成時にアフィニティを定義することもできます。

**ステップ 2** 新しいアフィニティマッピングを追加するには、[+作成 (+ Create)] をクリックします。

**ステップ 3** 割り当てる名前 (色) とビットを入力します。

**ステップ 4** [保存 (Save)] をクリックしてマッピングを保存します。

(注) 孤立した TE トンネルを回避するには、アフィニティを削除する前に TE トンネルを削除する必要があります。TE トンネルに関連付けられたアフィニティを削除した場合、アフィニティは [SR ポリシー/RSVP-TE トンネルの詳細 (SR Policy/RSVP-TE Tunnel Details)] ウィンドウに [不明 (UNKNOWN)] として表示されます。

## 最適化インテントベースのダイナミック SR-MPLS ポリシーの作成

このタスクでは、ダイナミックパスを使用して SR-MPLS ポリシーを作成します。SR-PCE は、ユーザーが定義したメトリックとパスの制約 (アフィニティまたは分離) に基づいてポリシーのパスを計算します。ユーザーは、IGP、TE、または遅延の 3 つの使用可能なメトリックから選択してパス計算を最小限にすることができます。また、SR-PCE は、トポロジの変更に基づいて、必要に応じてパスを自動的に再度最適化します。リンクまたはインターフェイスに障害

が発生した場合、ネットワークは、ポリシーで指定されたすべての基準を満たす代替パスを見つけます。パスが見つからない場合、パケットはドロップされます。



**ヒント** アフィニティを使用する場合は、デバイスからアフィニティ情報を収集し、Cisco Crosswork にマッピングしてからダイナミック SR-MPLS ポリシーを作成します。詳細については、[リンク アフィニティの設定 \(75 ページ\)](#) を参照してください。

- ステップ 1** メインメニューから、[Traffic Engineering] > [Traffic Engineering] > [SR-MPLS] タブを選択します。
- ステップ 2** [SR Policy] テーブルで、[+ Create] をクリックします。
- ステップ 3** [Policy Details] で、必要な SR-MPLS ポリシー値を入力します。各フィールドの説明を表示するには、 の上にマウスポインタを合わせます。
- ヒント** デバイスグループをセットアップしている場合は、[デバイスグループ (Device Groups)] ドロップダウンメニューからデバイスグループを選択できます。次に、トポロジマップを移動してズームインし、デバイスをクリックしてヘッドエンドまたはエンドポイントを選択します。
- ステップ 4** [ポリシーパス (Policy Path)] で、[ダイナミックパス (Dynamic Path)] をクリックし、パス名を入力します。
- ステップ 5** [最適化の目的 (Optimization Objective)] で、最小化するメトリックを選択します。
- ステップ 6** 該当する制約と分離を定義します。
- (注)
- アフィニティの制約と分離は、同じ SR-MPLS ポリシーでは設定できません。また、同じ分離グループまたはサブグループ内に 3 つ以上の SR-MPLS ポリシーを含めることはできません。設定はプレビュー中に許可されません。
  - ここで定義した分離グループに属する既存の SR-MPLS ポリシーがある場合は、プレビュー時に、同じ分離グループに属するすべての SR-MPLS ポリシーが表示されます。
- ステップ 7** [セグメント (Segments)] で、使用可能な場合にパブリックセグメントを使用するかどうかを選択します。
- ステップ 8** [プレビュー (Preview)] をクリックします。パスがマップに強調表示されます。
- ステップ 9** ポリシーパスをコミットする場合は、[プロビジョニング (Provision)] をクリックします。
- ステップ 10** SR-MPLS ポリシーの作成を検証します。
1. 新しい SR-MPLS ポリシーが [SR Policy] テーブルに表示されることを確認します。ポリシーの横にあるチェックボックスをクリックして、マップに強調表示されていることを確認することもできます。
- (注) 新たにプロビジョニングされた SR-MPLS ポリシーは、ネットワークのサイズとパフォーマンスによっては、[SR Policy] テーブルに表示されるまでに時間がかかることがあります。[SR Policy] テーブルは 30 秒ごとに更新されます。
2. 新しい SR-MPLS ポリシーの詳細を表示して確認します。[SR ポリシー (SR Policy)] テーブルで、 をクリックして [表示 (View)] を選択します。

- (注) ノード数、ポリシー数、またはインターフェイス数が多い拡張セットアップでは、ポリシーの展開中にタイムアウトが発生することがあります。タイムアウトオプションを設定するには、[Cisco Crosswork Infrastructure](#) および [アプリケーションアドミニストレーションガイド](#) を参照してください。

---

## SR-MPLS ポリシーの変更

SR-MPLS ポリシーを表示、変更、または削除するには、次の手順を実行します。

---

**ステップ 1** メインメニューから、[Traffic Engineering] > [Traffic Engineering] > [SR-MPLS] タブを選択します。

**ステップ 2** [SR Policy] テーブルから、目的の SR-MPLS ポリシーを見つけて  をクリックします。

**ステップ 3** [View] または [Edit / Delete] を選択します。

- (注)
- UI を使用して作成した SR-MPLS ポリシーのみ変更または削除できます。
  - SR-MPLS ポリシーの詳細を更新した後は、変更を保存する前にマップでプレビューできます。
-



## 第 7 章

# RSVP-TE トンネルのプロビジョニング



(注) この項では、ナビゲーションを **[Traffic Engineering] > [Traffic Engineering]** と記載しています。ただし、Crosswork Network Controller ソリューションを使用する場合、ナビゲーションは **[Traffic Engineering & Services] > [Traffic Engineering]** です。

ここでは、次の内容について説明します。

- [RSVP-TE トンネルのサポート \(79 ページ\)](#)
- [RSVP-TE トンネル設定のソース \(81 ページ\)](#)
- [明示的 RSVP-TE トンネルの作成 \(81 ページ\)](#)
- [リンクアフィニティの設定 \(82 ページ\)](#)
- [最適化インテントベースのダイナミック RSVP-TE トンネルの作成 \(83 ページ\)](#)
- [RSVP-TE トンネルの変更 \(84 ページ\)](#)

## RSVP-TE トンネルのサポート

表 3: サポートされる機能

機能	注記
PCE によって開始されたトンネル (Crosswork 最適化エンジンによるプロビジョニングまたは検出)	—
PCC によって開始されたトンネル (Crosswork 最適化エンジンによる検出)	—
ERO のストリクトホップ	—
ERO のルーズホップ (PCC による開始のみ)	—
Crosswork 最適化エンジンによってプロビジョニングされたトンネルの FRR 保護	—

機能	注記
パス最適化の目標最小メトリック (IGP、TE、または遅延)	—
パスの制約 (アフィニティと分離)	分離されたグループまたはサブ ID ごとに 2 つの RSVP トンネルのみをサポート
明示的トンネルおよび動的トンネルのバインディングラベル	—
シグナル帯域幅	—
セットアップ/保留の優先順位	—

表 4: サポートされていない機能と制限事項

説明	注記
COE でのルーズホップ ERO の設定	ストリクトホップのみを設定できます。パス上のすべてのホップにストリクトホップが設定されておらず、それらのホップがリモートインターフェイス IP またはループバック IP ではない場合、予期しない動作が発生することがあります。たとえば、トンネルが動作上ダウンしたままになったり、ホップが変更されたりすることがあります。
PCC で設定された名前付きトンネル	これらのトンネルは Crosswork 最適化エンジンによって検出されません。
ヘッドエンドまたはエンドポイントとパスホップの TE ルータ ID 以外のループバック IP を持つトンネル	—
トポロジマップ内のアクティブな FRR 保護パスの表示	Crosswork 最適化エンジンはトポロジマップに表示される FRR トンネルを検出しますが、アクティブに保護されているトンネルを使用中の FRR トンネルには関連付けません。保護がアクティブな場合、トポロジマップのパスには FRR 保護パスは含まれません。
P2MP トンネル	—

## RSVP-TE トンネル設定のソース

Crosswork 最適化エンジンによって検出および報告される RSVP-TE トンネルは、次のソースから設定されている可能性があります。

- PCC によって開始 : PCC に設定された RSVP-TE トンネル ([PCC によって開始された RSVP-TE トンネルの例 \(81 ページ\)](#) を参照)。
- 動的に作成。

### PCC によって開始された RSVP-TE トンネルの例

次に、PCC によって開始された RSVP-TE トンネルのデバイス設定の例を示します。特定のデバイスの説明およびサポートされている RSVP-TE トンネルコンフィギュレーションコマンドを表示するには、該当するマニュアルを参照してください (たとえば、Cisco NCS 5500 シリーズ、Cisco NCS 540 シリーズ、および Cisco NCS 560 シリーズルータの MPLS コマンドリファレンス)。

```
interface tunnel-te777
  ipv4 unnumbered Loopback0
  destination 192.168.0.8
  path-option 10 dynamic
  pce
  delegation
!
```

## 明示的 RSVP-TE トンネルの作成

このタスクでは、プレフィックスまたは隣接セグメント ID (SID リスト) のリストで構成されるプレフィックスのリストの明示的な (固定) パスを使用して RSVP-TE トンネルを作成します。このそれぞれがパス上のノードまたはリンクを表します。

- 
- ステップ 1** メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [トラフィック エンジニアリング (Traffic Engineering)] を選択します。
  - ステップ 2** 右側のウィンドウで、[RSVP-TE] をクリックします。
  - ステップ 3** [RSVP-TE トンネル (RSVP-TE Tunnels)] で、[+ 作成 (+Create)] をクリックします。
  - ステップ 4** 必要な RSVP-TE トンネル 値を入力します。各フィールドの説明を表示するには、 の上にマウスポインタを合わせます。  
**ヒント** デバイスグループをセットアップしている場合は、[デバイスグループ (Device Groups)] ドロップダウンメニューからデバイスグループを選択できます。次に、トポロジマップを移動してズームインし、デバイスをクリックしてヘッドエンドまたはエンドポイントを選択します。
  - ステップ 5** [ポリシーパス (Policy Path)] で、[明示的パス (Explicit Path)] をクリックし、パス名を入力します。
  - ステップ 6** RSVP-TE パスの一部となるセグメントを追加します。

**ステップ7** [プレビュー (Preview)] をクリックします。パスがマップに強調表示されます。

**ステップ8** トンネルパスをコミットする場合は、[プロビジョニング (Provision)] をクリックします。

**ステップ9** RSVP-TE トンネルの作成を検証します。

1. 新しい RSVP-TE トンネルが [RSVP-TE トンネル (RSVP-TE Tunnels)] テーブルに表示されることを確認します。ポリシーの横にあるチェックボックスをクリックして、マップに強調表示されていることを確認することもできます。

(注) 新しくプロビジョニングされた RSVP-TE トンネルは、ネットワークのサイズやパフォーマンスによっては、[RSVP-TE トンネル (RSVP-TE Tunnels)] テーブルに表示されるまでに時間がかかる場合があります。[RSVP-TE トンネル (RSVP-TE Tunnels)] テーブルは 30 秒ごとに更新されます。

2. 新しい RSVP-TE トンネルの詳細を表示して確認します。[RSVP-TE] テーブルで、... (RSVP-TE トンネルと同じ行にある) をクリックし、[表示 (View)] を選択します。

(注) ノード数、ポリシー数、またはインターフェイス数が多い拡張セットアップでは、ポリシーの展開中にタイムアウトが発生することがあります。関連するタイマーを調整するには、シスコの担当者にお問い合わせください。

## リンクアフィニティの設定

デバイスで定義されたアフィニティは Crosswork 最適化エンジンによって収集されません。アフィニティマッピング名は、Crosswork 最適化エンジンでの可視化にのみ使用されます。このため、デバイスインターフェイスでアフィニティを手動で収集してから、デバイスインターフェイスで使用されているものと同じ名前とビットを使用して Crosswork 最適化エンジン内でアフィニティマッピングを定義する必要があります。Crosswork 最適化エンジンは、プロビジョニング時にビット情報のみを SR-PCE に送信します。

SR-TE ポリシーまたは RSVP-TE トンネルのアフィニティは、SR-TE ポリシーまたは RSVP-TE トンネルがアフィニティを持つリンク属性を指定するために使用されます。SR-TE ポリシーまたは RSVP-TE トンネルのパスを形成するのに適したリンクを決定します。これは 32 ビット値で、各ビット位置 (0-31) はリンク属性を表します。アフィニティマッピングは、各ビット位置または属性を色にマッピングするために使用されます。これにより、リンク属性の参照が容易になります。

特定のデバイスの SR 設定マニュアルを参照して、説明とサポートされている設定コマンドを確認してください (『[Asr9000 Configuration](#)』など)。



- (注) アフィニティマッピングを編集または削除するには、関連するメニューオプションをクリックします。

**ステップ1** メインメニューから、[トラフィックエンジニアリング (Traffic Engineering)] > [アフィニティ (Affinities)] を選択します。[マッピングの管理 (Manage Mapping)] をクリックして、SR-TE ポリシーまたは RSVP-TE トンネルの作成時にアフィニティを定義することもできます。

**ステップ2** 新しいアフィニティマッピングを追加するには、[+作成 (+ Create)] をクリックします。

**ステップ3** 割り当てる名前 (色) とビットを入力します。

**ステップ4** [保存 (Save)] をクリックしてマッピングを保存します。

(注) 孤立した TE トンネルを回避するには、アフィニティを削除する前に TE トンネルを削除する必要があります。TE トンネルに関連付けられたアフィニティを削除した場合、アフィニティは [SR ポリシー/RSVP-TE トンネルの詳細 (SR Policy/RSVP-TE Tunnel Details)] ウィンドウに [不明 (UNKNOWN)] として表示されます。

## 最適化intentベースのダイナミック RSVP-TE トンネルの作成

このタスクでは、ダイナミックパスを使用して RSVP-TE トンネルを作成します。SR-PCE は、ユーザーが定義したメトリックとパスの制約 (アフィニティまたは分離) に基づいてトンネルのパスを計算します。パス計算で最小化する使用可能な3つのメトリック (IGP、TE、または遅延) から選択できます。SR-PCE は、トポロジの変更に基づいて、必要に応じてパスを自動的に再度最適化します。



**ヒント** アフィニティを使用する場合は、デバイスからアフィニティ情報を収集し、ダイナミック RSVP-TE トンネルを作成する前に Cisco Crosswork にマッピングします。詳細については、「[リンクアフィニティの設定 \(75 ページ\)](#)」を参照してください。

**ステップ1** メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [トラフィック エンジニアリング (Traffic Engineering)] を選択します。

**ステップ2** 右側のウィンドウで、[RSVP-TE] をクリックします。

**ステップ3** [RSVP-TE トンネル (RSVP-TE Tunnels)] で、[+作成 (+Create)] をクリックします。

**ステップ4** 必要な RSVP-TE トンネル 値を入力します。各フィールドの説明を表示するには、② の上にマウスポインタを合わせます。

**ヒント** デバイスグループをセットアップしている場合は、[デバイスグループ (Device Groups)] ドロップダウンメニューからデバイスグループを選択できます。次に、トポロジマップを移動してズームインし、デバイスをクリックしてヘッドエンドまたはエンドポイントを選択します。

**ステップ 5** [トンネルパス (Tunnel Path)] の下にある [ダイナミックパス (Dynamic Path)] をクリックし、パス名を入力します。

**ステップ 6** [最適化の目的 (Optimization Objective)] で、最小化するメトリックを選択します。

**ステップ 7** 該当する制約と分離を定義します。

(注) アフィニティの制約と分離は、同じ RSVP-TE トンネルに設定できません。また、3 つ以上の RSVP-TE トンネルを同じ分離グループグループやサブグループに含めることはできません。ここで定義した分離グループに属する既存の RSVP-TE トンネルがある場合は、プレビュー時に同じ分離グループに属するすべての RSVP-TE トンネルが表示されます。

**ステップ 8** [プレビュー (Preview)] をクリックします。パスがマップに強調表示されます。

**ステップ 9** トンネルパスをコミットする場合は、[プロビジョニング (Provision)] をクリックします。

**ステップ 10** RSVP-TE トンネルの作成を検証します。

1. 新しい RSVP-TE トンネルが [RSVP-TE トンネル (RSVP-TE Tunnels)] テーブルに表示されることを確認します。ポリシーの横にあるチェックボックスをクリックして、マップに強調表示されていることを確認することもできます。

(注) 新しくプロビジョニングされた RSVP-TE トンネルは、ネットワークのサイズやパフォーマンスによっては、[RSVP-TE トンネル (RSVP-TE Tunnels)] テーブルに表示されるまでに時間がかかる場合があります。[RSVP-TE トンネル (RSVP-TE Tunnels)] テーブルは 30 秒ごとに更新されます。

2. 新しい RSVP-TE トンネルの詳細を表示して確認します。[RSVP-TE] テーブルで、 をクリックして [表示 (View)] を選択します。

(注) ノード数、ポリシー数、またはインターフェイス数が多い拡張セットアップでは、ポリシーの展開中にタイムアウトが発生することがあります。関連するタイマーを調整するには、シスコの担当者にお問い合わせください。

## RSVP-TE トンネルの変更

RSVP-TE トンネルを表示、編集、または削除するには、次の手順を実行します。

**ステップ 1** メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [トラフィック エンジニアリング (Traffic Engineering)] を選択します。

**ステップ 2** [トラフィック エンジニアリング (Traffic Engineering)] ウィンドウから [RSVP-TE] タブを選択します。

**ステップ 3** 対象とする RSVP-TE トンネルを見つけて  をクリックします。

**ステップ 4** [表示 (View)] または [編集/削除 (Edit / Delete)] を選択します。

- (注)
- UI を使用して作成した RSVP-TE トンネルのみ変更または削除できます。
  - RSVP-TE トンネルの詳細を更新した後は、変更を保存する前にマップ上でプレビューできます。
-





## 第 8 章

# ローカル輻輳緩和（LCM）を使用したローカルでのネットワーク輻輳の緩和



- (注)
- この項で説明する機能は、Advanced RTM ライセンスパッケージの一部としてのみ使用できます。
  - この項では、ナビゲーションを[トラフィックエンジニアリング（Traffic Engineering）]>[トラフィックエンジニアリング（Traffic Engineering）]と記載しています。ただし、Crosswork Network Controller ソリューション内で Crosswork 最適化エンジンを使用する場合、ナビゲーションは[トラフィックエンジニアリング & サービス（Traffic Engineering & Services）]>[トラフィックエンジニアリング（Traffic Engineering）]になります。

- [ローカル輻輳緩和の概要（87 ページ）](#)
- [LCM に関する特記事項（88 ページ）](#)
- [LCM 計算のワークフロー（91 ページ）](#)
- [ローカルインターフェイスでの輻輳の緩和の例（93 ページ）](#)
- [LCM の設定（100 ページ）](#)
- [個別のインターフェイスしきい値の追加（102 ページ）](#)
- [LCM 動作のモニター（102 ページ）](#)

## ローカル輻輳緩和の概要

ローカル輻輳緩和（LCM）は、（トリガーされたイベントとは対照的に）設定可能な頻度で輻輳を検索し、ドメイン内の周囲のインターフェイスでローカライズされた緩和の推奨事項（ローカルインターフェイス レベルの最適化）を提供します。LCM は、1 つ以上の戦術的ポリシーの最短パスを計算して、輻輳したインターフェイス上の最小量のトラフィックを、十分な帯域幅を持つ代替パスに迂回させます。また、元の IGP パス上のトラフィックをできるだけ多く保持しようとしています。ユーザーが承認すると、LCM は戦術的トラフィック エンジニアリング（TTE）SR ポリシーの展開を通じて緩和を実行します。LCM は、輻輳を緩和するために SR

ポリシーの既存の展開のパスを変更しません。LCM を使用すると、次のことが可能になります。

- 戦術的トラフィック エンジニアリング (TTE) SR ポリシーの展開をコミットするかどうかを決定する前に、ネットワーク上で LCM の推奨事項を視覚的にプレビューできます。
- LCM ソリューションの設定に基づいて輻輳とネットワーク障害に対処するために、LCM がネットワークに変更を自動的に展開できるようにします。詳細については、[LCM の設定 \(100 ページ\)](#) の詳細な設定オプション ([Auto Repair Solution] および [Adjacency Hop Type]) を参照してください。

LCM を使用すると、パスの計算が簡素になり、特定のネットワーク要素に制限されるため、複数の IGP エリアを含むなど、さまざまなネットワークトポロジでソリューションをより幅広く適用できます。ドメイン内の問題にローカルに焦点を当てることにより、完全なトラフィックマトリックスを通じてネットワーク内のエッジツーエッジトラフィックフローをシミュレートする必要がなくなり、大規模ネットワークの拡張性が向上します。また、LCM では、SNMP を介して TTE SR ポリシーおよびインターフェイスカウンタの収集が実行されるため、SR-TM を使用する必要はありません。

TTE トンネルの推奨事項は、[LCM 運用ダッシュボード (LCM Operational Dashboard)] にリストされます。このダッシュボードから、TTE SR ポリシーを展開する前に推奨を視覚的にプレビューできます。輻輳を解決するための TTE SR ポリシーの展開は自動化されていません。LCM 推奨アクションを承認してコミットする必要があります。LCM では、以前の TTE SR ポリシー (LCM によってインスタンス化) が不要になった場合は削除することも推奨されます。

## LCM に関する特記事項

LCM を使用する場合は、次の情報を考慮してください。

- LCM を使用するには、Advanced RTM ライセンスパッケージが必要です。
- 帯域幅最適化が有効になっている場合は、LCM を有効にできません。
- LCM は、最大 2000 台のデバイスを持つドメインをサポートします。ドメインは、IGP プロセスに割り当てられる識別子です。ドメインはネットワークから学習されます。ドメイン ID は、BGP-LS で IGP をアドバタイズするために使用するルータ設定 (link-state instance-id) から取得されます。
- LCM 推奨ソリューションでは、単一ドメイン内のリソースのみ使用されます。
- LCM は、5 分以上の通常の設定可能な頻度でネットワーク使用率を評価します。頻度は通常、SNMP トラフィックのポーリング間隔以上に設定されます。デフォルトの頻度は 10 分です。
- LCM は、パラレル TTE SR ポリシー全体で ECMP を活用し、トラフィックのほぼ均等な分割を想定します。実際の ECMP 分割がこの想定に従う程度は、大規模なエレファントフローの存在とレベルトラフィックの集約によって異なります。
- 最適化できるトラフィックは、既存の SR-TE ポリシーで伝送しないでください。

- ドメインインターフェイスとリンクが（意図的または非意図的に）削除されると、次のようになります。
  - リンクがダウンする (LINK\_DOWN 状態になる) と、LCM 設定とドメイン UI カード (LCM の設定 (100 ページ) を参照) は、リンクがエージアウトする (4 時間後) まで使用できます。この動作は意図的なもので、誤って実行された場合にドメインインターフェイスとリンクを回復する時間が与えられます。
  - リンクがエージアウトする前にドメインを強制的に削除する場合は、UI から手動でリンクを削除できます。ドメインは、最後のリンクが削除されるまで「削除準備完了」ステータスのままになります。

## LCM プラットフォームの要件

次に、LCM を適切に動作させるための大まかな要件のリストを示します。

輻輳評価：

- LCM には、次のトラフィック統計情報が必要です。
  - SNMP インターフェイス トラフィック の測定値
  - SNMP ヘッドエンド SR-TE ポリシートラフィックの設定値
- SR にはストリクト SID ラベルを設定する必要があります。

輻輳緩和：

- ヘッドエンドデバイスは、複数のパラレル SR-TE ポリシー全体で等コストマルチパス (ECMP) をサポートする必要があります。
- ヘッドエンドデバイスは、`autoroute` のステアリングで PCE によって開始された SR-TE ポリシーをサポートする必要があります。

`autoroute` を使用して SR-TE ポリシーへのトラフィックステアリングを有効にするには、`force-sr-iinclude` を使用してデバイスを設定する必要があります。次に例を示します。

```
segment-routing traffic-eng pcc profile <id> autoroute force-sr-iinclude
```

特定のデバイスの SR 設定のマニュアルを参照して、説明とサポートされている設定コマンドを確認してください (『[Segment Routing Configuration Guide for Cisco ASR 9000 Series Routers](#)』など)。

プラットフォーム要件の完全なリストについては、シスコの営業担当者にお問い合わせください。

## ASBR 間の専用 IGP インスタンスでの複数 AS ネットワークに対する BGP-LS のスピーカー配置

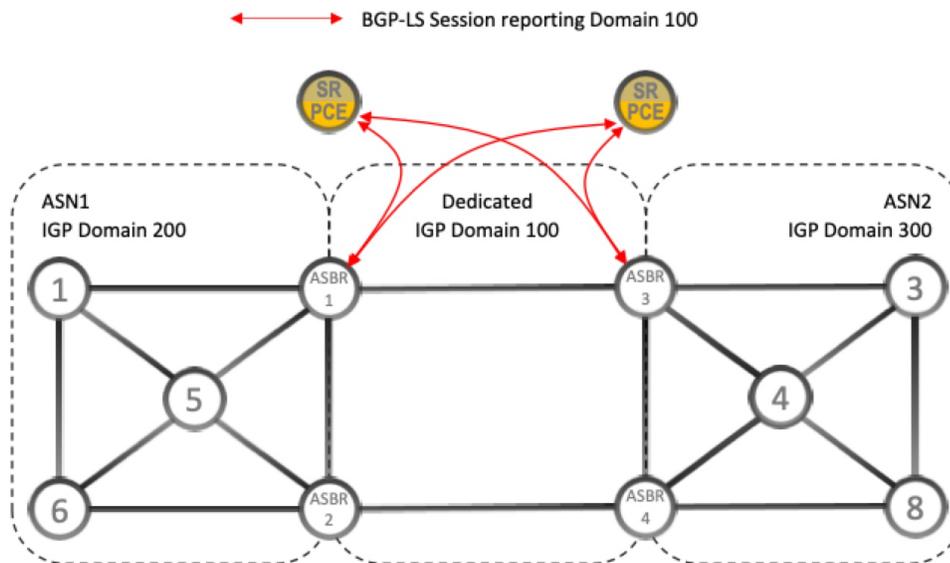
SR-PCE（または出力ピアエンジニアリング (EPE) がサポートされていないその他のユースケース）によるドメイン間遅延最適化 SR ポリシーパスの計算をサポートするために、異なる ASN の自律システム境界ルータ (ASBR) 間で専用 IGP インスタンスを設定できます。このような場合、適切なトポロジ検出のために、BGP-LS 経由でトポロジを報告する ASBR を特定することが重要です。

次の例では、専用 AS 間 IGP（ドメイン 100）に参加している各 AS の少なくとも 1 つの ASBR で、各 ASBR 間の IGP を報告する BGP-LS が有効になっている必要があります。各 ASBR は、同じ BGP-LS 識別子を持つドメインを報告する必要があります。



(注) BGP-LS トポロジを報告する AS ごとに複数の ASBR もサポートされます。

図 13: BGP-LS セッション報告ドメイン 100



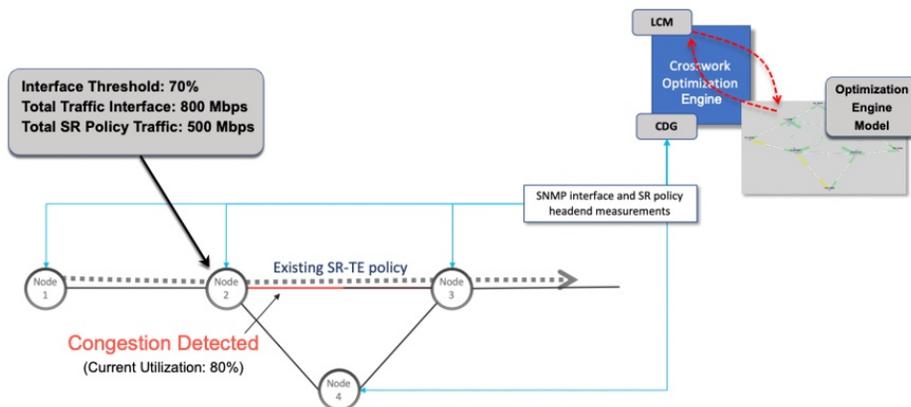
## アップグレード後における以前のモニター対象インターフェイスの欠落

Crosswork 最適化エンジン 2.0 でホスト名の変更が発生し、そのシステムのバックアップを使用して Crosswork 最適化エンジン 3.0 にアップグレードした場合、ホスト名が更新されたノードに属する、以前のモニター対象 LCM インターフェイスは移行されません。それらのインターフェイスは LCM モニター対象インターフェイスのリストからドロップされ、LCM ログに警告が表示されます。この問題を回避するために、移行が完了してシステムが安定した後、モニターする LCM のインターフェイスを手動で追加できます。

## LCM 計算のワークフロー

この例では、輻輳の検出から LCM が実行する計算を説明した後に、戦術的トンネル展開を推奨します。Crosswork Optimization Engine 3.0 のリリースでは、計算はドメイン単位で実行されるため、大規模なネットワークの拡張性が向上し、計算が高速になります。

図 14: LCM の設定ワークフローの例



**ステップ 1** LCM は、まず、Optimization Engine モデル（物理ネットワークのリアルタイムトポロジとトラフィックの表現）を定期的に分析します。

**ステップ 2** この例では、輻輳の確認間隔の後、ノード 2 の使用率が 70% の使用率しきい値を超えると、LCM が輻輳を検出します。

**ステップ 3** LCM は、転送に適したトラフィック量を計算します。

LCM は、既存の SR ポリシーでルーティングされていないトラフィックのみを転送します（ラベルなし、IGP ルーティング、または FlexAlgo-0 SID 経由で伝送など）。SR-TE ポリシート内のラフィックは、LCM 計算には含まれず、元のプログラムされたパスを通過し続けます。

対象トラフィックは、インターフェイス上のすべてのトラフィックを考慮したインターフェイストラフィック統計情報を取得し、インターフェイスを通過するすべての SR-TE ポリシーのトラフィック統計情報の合計を引いて計算されます。

合計インターフェイストラフィック - SR ポリシートラフィック = 最適化できる対象トラフィック

このプロセスでは、SR ポリシーの ECMP 分割を考慮して、SR ポリシートラフィックを適切にアカウントリングする必要があります。この例では、輻輳したノード 2 の合計トラフィックは 800 Mbps です。ノード 2 経由でルーティングされるすべての SR ポリシーの合計トラフィックは 500 Mbps です。

この例で LCM が転送できる合計トラフィックは 300 Mbps (800 Mbps - 500 Mbps = 300 Mbps) です。

**ステップ 4** LCM は、インターフェイス上の合計トラフィックからしきい値相当のトラフィックを差し引くことにより、代替パスを介して送信する必要がある量を計算します。この例では、転送される量は 100 Mbps です。

800 Mbps - 700 Mbps (しきい値 70%) = 100 Mbps

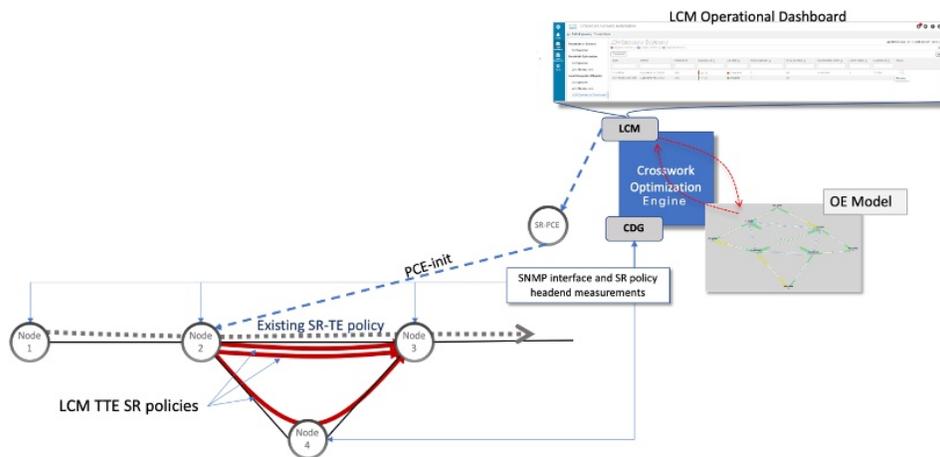
LCM は、300 Mbps のうちの 100 Mbps (対象トラフィック) を別のパスにルーティングする必要があります。オーバープロビジョニング係数 (OPF) のパーセンテージが 10 に設定されている場合、LCM は対象トラフィックの 110 (100 Mbps X 1.10) をルーティングする必要があることに注意してください。OPF は、[LCM Configuration] ウィンドウの [Advanced] タブで設定できます。詳細については、[LCM の設定 \(100 ページ\)](#) を参照してください。

**ステップ 5** LCM は、必要な TTE SR ポリシーの数とそのパスを決定します。迂回する必要がある量に対して最短パスに留まることができる LCM 対象トラフィックの割合によって、最短パスと代替パスでそれぞれ必要な TTE SR ポリシーの数が決まります。

この例では、LCM は輻輳したリンクから対象トラフィックの合計の 1/3 (300 Mbps のうち 100 Mbps) を転送する必要があります。LCM は完全な ECMP を想定し、このトラフィック分割には 3 つの戦術的 SR-TE ポリシーが必要だと予測します。1 つの戦術的 SR-TE ポリシーが転送パスをとり、2 つの戦術的 SR-TE ポリシーが元のパスをとります。ノード 2 とノード 4 の間のパスに十分な容量があります。したがって、LCM では、SR-PCE を介してノード 2 からノード 3 に展開する 3 つの TTE SR ポリシー (それぞれ約 100 Mbps をルーティングすると想定) を推奨しています。

- ノード 3 (200 Mbps) への直接パスを取る 2 つの TTE SR ポリシー
- TTE SR ポリシーの 1 つはノード 4 (100 Mbps) を介してホップします。

これらの推奨事項は、[LCM 運用ダッシュボード (LCM Operational Dashboard)] にリストされます。



**ステップ 6** LCM はこれらの TTE SR ポリシーを展開すると想定して、展開された TTE ポリシーを引き続きモニターし、[LCM Operational Dashboard] で必要に応じて変更または削除することを推奨します。TTE SR ポリシーの削除は、これらのポリシーが削除された (保留マージンを差し引く) 場合に、緩和されたインターフェイスが輻輳しない場合に推奨されます。これにより、LCM の操作全体で不必要な TTE SR ポリシーのチャーンを回避できます。

## ローカルインターフェイスでの輻輳の緩和の例

この例では、LCM を有効にし、定義された使用率のしきい値をデバイスのインターフェイスの使用率が超えた場合に TTE SR ポリシーを展開するための輻輳緩和の推奨事項を確認します。輻輳の緩和をコミットする前に、推奨される TTE SR ポリシーをプレビューします。この例では、次のワークフローを示します。

1. 輻輳していないトポロジを表示します。
2. LCM を有効にして設定します。
3. LCM が輻輳を検出した後、[Operational Dashboard] で LCM の推奨事項を表示します。
4. LCM TTE ポリシーをトポロジマップで視覚的にプレビューします。
5. すべての LCM TTE ポリシーの推奨事項をコミットして展開し、輻輳を緩和します。
6. LCM TTE ポリシーが展開されていることを確認します。



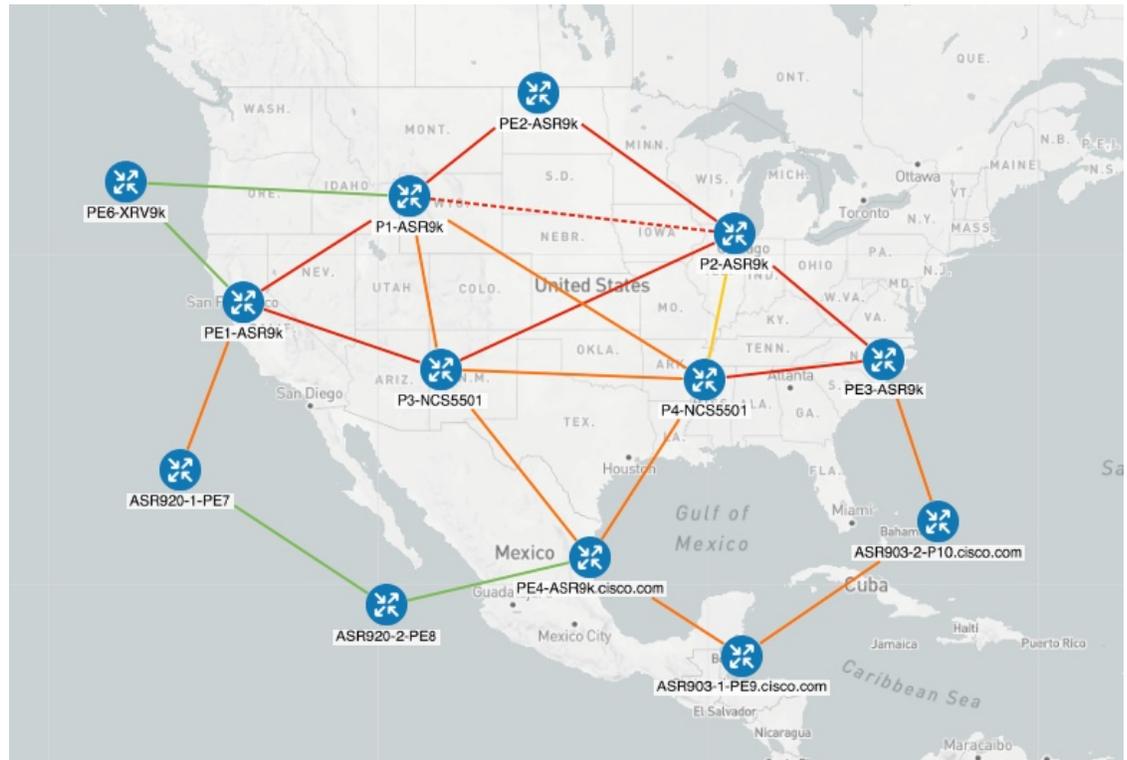
---

(注) この例で使用される使用率のしきい値は非常に低く (12%)、ラボ環境での使用に最適です。

---

次の図は、この例で使用されるトポロジを示しています。

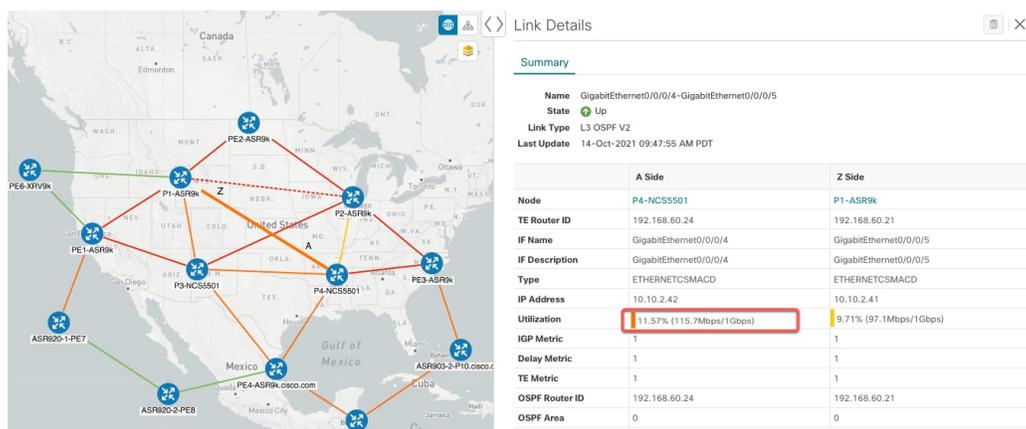
図 15: 初期トポロジ



ステップ 1 LCM 設定前の初期トポロジと使用率を表示します。

- リンクの詳細を表示するには、P4-NCS5501 と P1-ASR9k の間のリンクをクリックします。P4-NCS5501 の使用率は 11.57% です。

図 16: 初期使用率



ステップ 2 LCM を有効にし、グローバルおよびカスタムインターフェイスの使用率のしきい値を設定します。

- a) メインメニューから、[Traffic Engineering] > [Local Congestion Mitigation] > [Domain-ID] > ... > [Configuration] を選択します。この例では、しきい値を 12% に設定し、[Interfaces to Monitor] > [Selected Interfaces] オプションを選択します。詳細については、[LCM の設定 \(100 ページ\)](#) を参照してください。

図 17: LCM 設定ページ

### Configuration

Basic Advanced

<b>Enable</b> ⓘ False <input type="radio"/> True <input checked="" type="radio"/>	<b>Color</b> ⓘ 2000 <small>Range: 1 to 4294967295</small>	<b>Utilization Threshold</b> ⓘ 12 <small>Range: 0 to 100</small>
<b>Utilization Hold Margin</b> ⓘ 5 <small>Range: 0 to Utilization Threshold</small>	<b>Delete Tactical SR Policies when Disabled</b> ⓘ False <input type="radio"/> True <input type="radio"/>	<b>Profile ID</b> ⓘ 0 <small>Range: 0 to 65535</small>
<b>Congestion Check Interval</b> ⓘ 900 <small>Range: 600 to 86400 seconds</small>	<b>Max LCM Policies per Set</b> ⓘ 8 <small>Range: 1 to 8</small>	<b>Interfaces to Monitor</b> ⓘ <input checked="" type="radio"/> Selected Interfaces <input type="radio"/> All Interfaces
<b>Description</b> ⓘ LCM Startup Config		

Commit Changes Get Default Values Discard Changes

- b) [Commit Changes] をクリックして、設定を保存します。設定の変更をコミットすると、LCM はモニター対象インターフェイスで輻輳が発生した場合、[LCM Operational Dashboard] に推奨事項を表示します。LCM は新しい TTE ポリシーを自動的にコミットまたは展開しません。後で、推奨される TTE ポリシーをプレビューし、それらのポリシーをコミットしてネットワークに展開するかどうかを決定できます。
- c) [Interfaces to Monitor] > [Selected Interfaces] を選択した場合は、[Link Management] ページ ([Traffic Engineering] > [Local Congestion Mitigation] > [Domain-ID] > ... > [Link Management]) に移動し、カスタム使用率しきい値を持つインターフェイスのリストをアップロードします。このページにリストされているインターフェイスの輻輳のみモニターされます。次の例を参照してください。

(注) [Interfaces to Monitor] > [All Interfaces] を選択した場合、LCM はすべてのインターフェイスをモニターします。対象には、[Link Management] ページにインポートされた個々のしきい値が含まれます。残りのインターフェイスは、[Configuration] ページで定義されたグローバル [Utilization Threshold] を使用してモニターされます。

## Link Management

Total 4

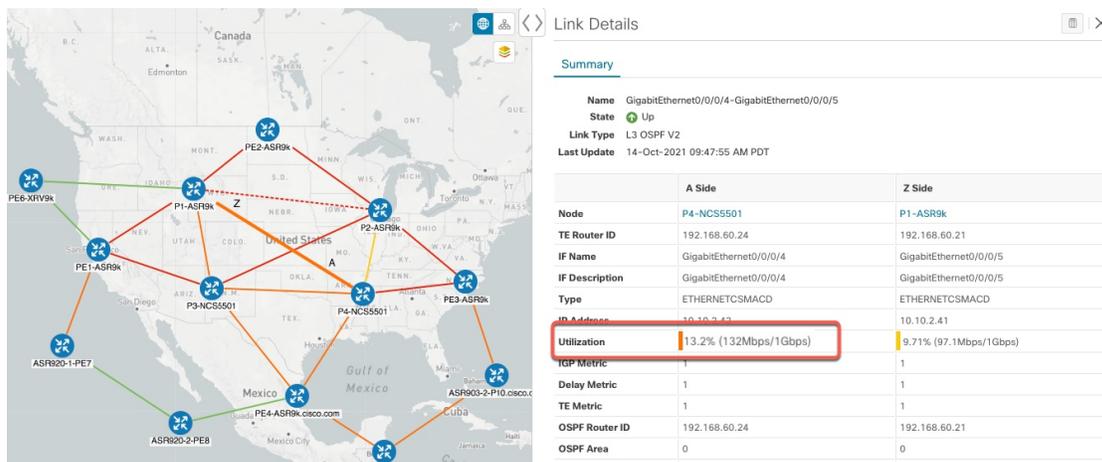
Interfaces with custom Thresholds should be uploaded to this page.

- If the **All Interfaces** option has been configured, interfaces and its Utilization Threshold defined and uploaded to this page will be monitored for congestion. All other interfaces will be monitored using the global Utilization Threshold defined in the Configuration page.
- If the **Selected Interfaces** option has been configured, only the interfaces and its Utilization Threshold defined and uploaded to this page will be monitored for congestion.

Node	Interface	Threshold (%)
F3.cisco.com	GigabitEthernet0/0/0/1	30.0
F4.cisco.com	GigabitEthernet0/0/0/2	45.0
F5.cisco.com	GigabitEthernet0/0/0/0	20.0
F6.cisco.com	GigabitEthernet0/0/0/1	35.0

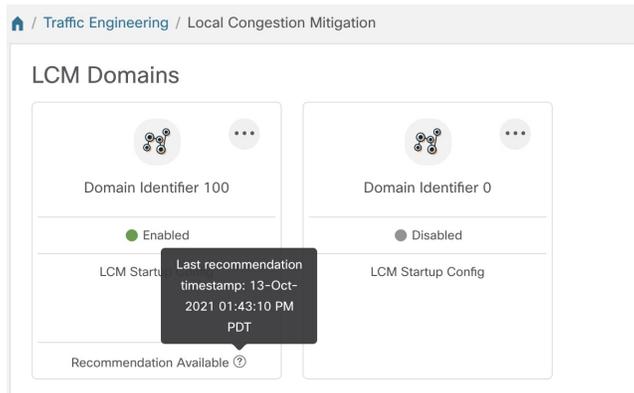
**ステップ 3** しばらくすると、設定された LCM しきい値を超えて輻輳が発生します。この例では、使用率が 12% を超えています。

図 18: 輻輳



**ステップ 4** [LCM Operational Dashboard] で TTE SR ポリシーの推奨事項を表示します。

- a) [Traffic Engineering] > [Local Congestion Mitigation] に移動します。輻輳が検出されると、ドメインに推奨アクションのタイムスタンプが表示されます。



- b) (オプション)  > [Events] タブをクリックして、新しいイベントを表示します。このウィンドウをモニターして、発生した LCM イベントを表示することもできます。LCM の推奨事項、コミットアクション、および例外のイベントを確認する必要があります。LCM イベントの例を次に示します。

Alarms & Events

All System Network

Alarms Events

Selected / Total 929 

Filters Applied (1) 

Source	Severity	Description	Creation Time	Category	Correlated Alarm
LCM					
LCM for domain 100	Info	A new recommendation has been created: 2 creates, 0 updates, 0 delete...	30-AUG-2021 04:56:33 P...	System	NO
LCM for domain 100	Info	Recommendation committed.	30-AUG-2021 04:45:31 P...	System	NO
LCM for domain 100	Info	A new recommendation has been created: 0 creates, 0 updates, 6 delete...	30-AUG-2021 04:44:51 P...	System	NO
LCM for domain 100	Major	Mitigated interface F2.cisco.com GigabitEthernet0/0/0/5 is down.	30-AUG-2021 04:44:50 P...	System	NO
LCM for domain 100	Info	A new recommendation has been created: 0 creates, 2 updates, 4 delete...	30-AUG-2021 04:25:46 P...	System	NO
LCM for domain 100	Info	Recommendation committed.	30-AUG-2021 04:00:46 P...	System	NO
LCM for domain 100	Info	A new recommendation has been created: 1 creates, 5 updates, 0 delete...	30-AUG-2021 03:52:29 P...	System	NO
LCM for domain 100	Info	LCM is enabled	30-AUG-2021 03:52:11 P...	System	NO
LCM for domain 101	Info	LCM Worker with domain_id: '101' has started.	30-AUG-2021 03:52:04 P...	System	NO
LCM for domain 100	Info	LCM Worker with domain_id: '100' has started.	30-AUG-2021 03:52:04 P...	System	NO
LCM for domain 101	Info	LCM is disabled	30-AUG-2021 03:52:03 P...	System	NO

- c) [Operational Dashboard] を開きます ([Traffic Engineering] > [Local Congestion Mitigation] > [Domain-ID] >  > [Operational Dashboard])。

ダッシュボードには、使用率が 12% を超えていて、13.01% であることが示されます。[Recommended Action] 列には、インターフェイスの輻輳に対処するために TTE ポリシーソリューションセット ([Create Set]) を展開することが推奨されています。[Expected Util] 列には、推奨アクションがコミットされた場合の各インターフェイスの予想使用率が表示されます。詳細については、[LCM 動作のモニター \(102 ページ\)](#) を参照してください。

図 19: [LCM Operational Dashboard]

Operational Dashboard

Last Refresh: 12-Oct-2021 09:14:03 AM PDT 

 Congested Interfaces (1) |  Mitigating Interfaces (0) |  Mitigated Interfaces (0)

Commit All Last Recommendation: 12-Oct-2021 09:02:23 AM PDT Urgency: MEDIUM 

Node	Interface	Threshold Util	Evaluatio...	LCM State	Pol...	Pol...	Recomm...	Com...	Expected Util	Solution Up...	Actions
P4-NCS55	GigabitEthernet0/0/0/1	12%	13.01%	 Congested	0	-	Create Set	None	11.97%	12-Oct-202...	

- d) TTE ポリシーをコミットする前に、各 TTE ポリシーソリューションセットの展開をプレビューできます。[Actions] 列で  をクリックし、[Preview] を選択します。各 TTE ポリシーのノード、インターフェイス、および推奨アクションがウィンドウに表示されます。[Preview] ウィンドウから、個々の TTE ポリシーを選択し、トポロジマップで通常行っているように、さまざまな側面と情報を表示できます。次の図に、インターフェイス GigabitEthernet0/0/0/4 の推奨 TTE ポリシーを示します。後で TTE ポリシーの展開を確認するために、[Color ID] をメモします。

図 20: LCM TTE 展開のプレビュー

Headend	Endpoint	Color	Recommended Action	
<input type="checkbox"/>	P4-NCS5501	P1-ASR9k	1910	CREATE
<input checked="" type="checkbox"/>	P4-NCS5501	P1-ASR9k	1911	CREATE

- e) マップ上で推奨される TTE ポリシーを確認したら、[Operational Dashboard] に戻り、[Commit All] をクリックします。LCM の [Status] 列が [Mitigating] に変化します。

(注) [Operational Dashboard] に示されているとおりに輻輳を緩和し、予想使用率を達成するには、ドメインごとに LCM のすべての推奨事項をコミットする必要があります。緩和ソリューションは、ソリューションセット間の依存関係により、コミットされているすべての LCM 推奨事項に基づいています。

Operational Dashboard Last Refresh: 12-Oct-2021 09:14:03 AM PDT | O

● Congested Interfaces (0) | ● Mitigating Interfaces (1) | ● Mitigated Interfaces (0)

Commit All Last Recommendation: 12-Oct-2021 09:02:23 AM PDT Urgency: MEDIUM

Node	Interface	Threshold Util	Evaluation...	LCM State	Pol...	Pol...	Recomm...	Com...	Expected Util	Solution Up...	Actions
P4-NCS55	GigabitEthernet0/0/0/1	12%	13.01%	Mitigating	2	-	Create Set	None	11.97%	12-Oct-202...	...

## ステップ 5 TTE SR ポリシーの展開を検証します。

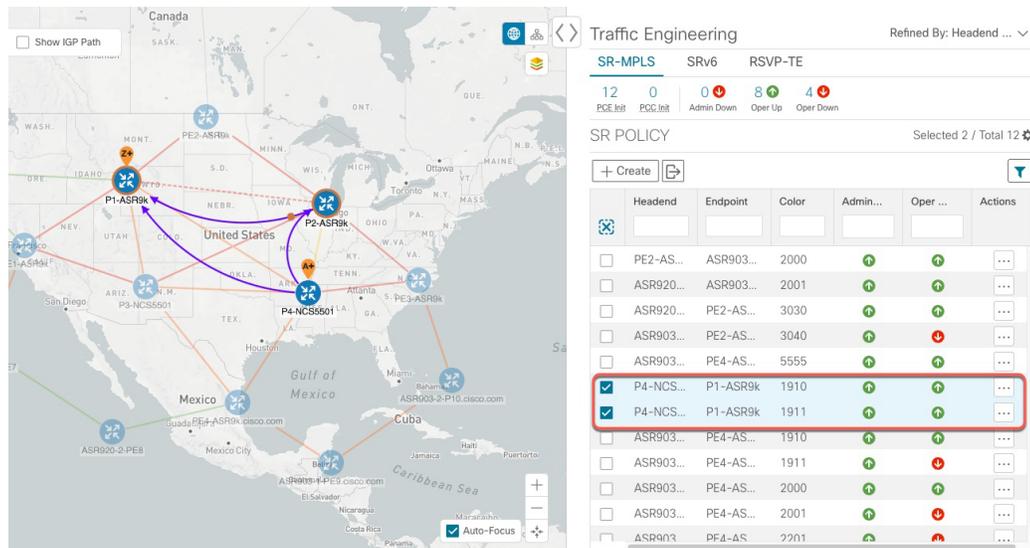
- a) > [Events] タブをクリックします。[Events] ウィンドウに表示される LCM イベントを確認します。

(注) Crosswork Optimization Engine は、有効にしたポリシーと機能に基づいて検出されたネットワークイベントを報告します。たとえば、リンクドロップによって SR-TE ポリシーがダウンした場合や、LCM が輻輳を検出した場合に報告されます。これらのアラートは UI で報告され、必要に応じてサードパーティのアラート/モニタリングツールに転送できます。

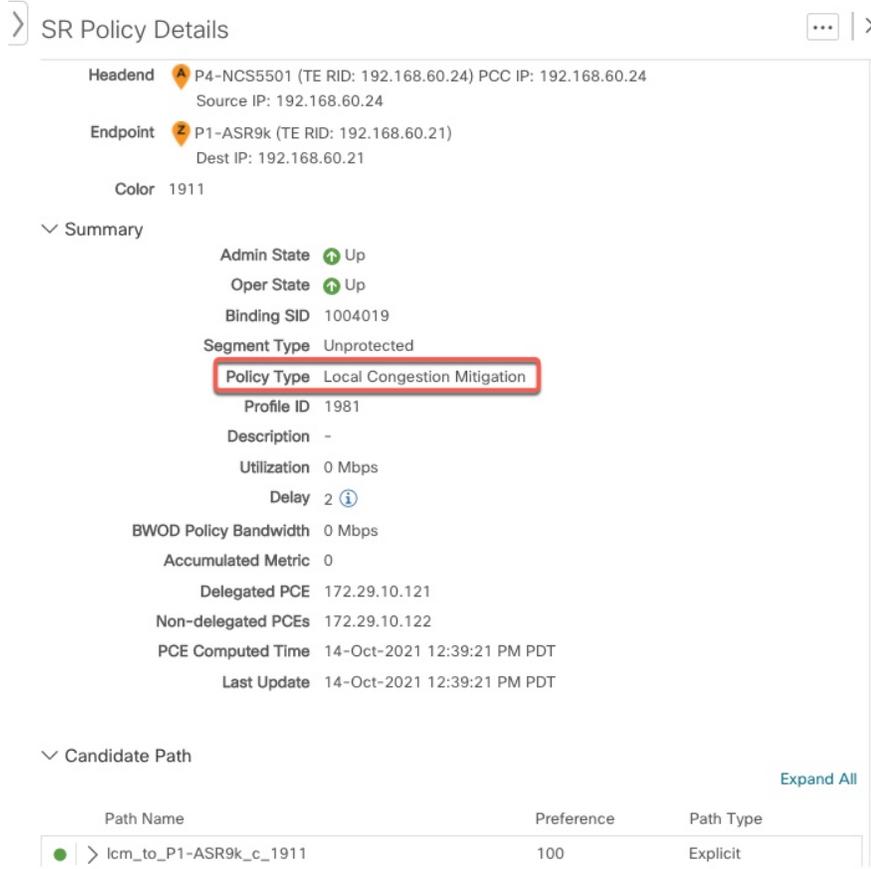
- b) [Operational Dashboard] に戻り、すべての TTE ポリシーソリューションセットの LCM の状態が [Mitigated] に変化したことを確認します。

LCM の状態が変化するには、SNMP 頻度の 2 倍の時間がかかることに注意してください。

- c) トポロジマップと [SR Policy] テーブルを表示して、TTE ポリシーの展開を確認します ([Traffic Engineering] > [Traffic Engineering] > [SR-MPLS] タブ)。



- d) 新しい SR-TE ポリシーのいずれかを選択し、SR ポリシーの詳細を表示します (... をクリックして [View Details] を選択)。



ステップ 6 LCM の推奨に従って TTE SR ポリシーを削除します。

- しばらくすると、展開された TTE SR ポリシーが不要になる場合があります。これは、LCM によって開始された TTE トンネルがなくても、使用率がしきい値を下回らない場合に発生します。この場合、LCM は TTE SR ポリシーセットを削除するための新しい推奨アクションを生成します。展開された TTE SR ポリシーを削除するには、[すべてコミット (Commit All)] をクリックします。
- SR ポリシーを削除するには、[すべてコミット (Commit All)] をクリックします。
- トポロジマップと [SRポリシー (SR Policy)] テーブルを表示して、削除を確認します。

このシナリオでは、LCM を活用してネットワークのトラフィックの輻輳を軽減する方法を確認しました。LCM では、手動による追跡と計算は不要であり、同時に輻輳緩和の推奨事項を実装するかどうかを制御できます。推奨事項をプレビューして、展開する前にネットワークでの展開の有効性を確認できます。トラフィックが変化すると、LCM は展開された TTE SR-TE ポリシーを追跡し、それらのポリシーがまだ必要かどうかを判断します。必要でない場合、LCM は削除を推奨します。

#### 関連トピック

[個別のインターフェイスしきい値の追加 \(102 ページ\)](#)

## LCM の設定

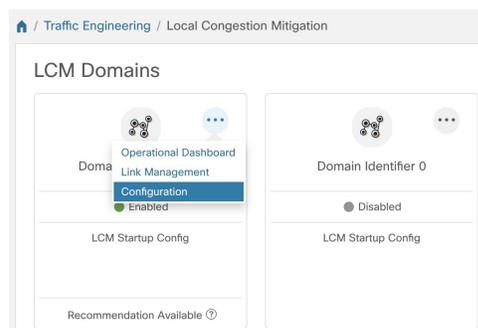
LCM を有効にして設定するには、次の手順を実行します。

#### 始める前に

[LCM に関する特記事項 \(88 ページ\)](#) を確認してください。

**ステップ 1** メインメニューから、[Traffic Engineering] > [Local Congestion Mitigation] > [Domain-ID-card] > ... > [Configuration] > [Basic] タブを選択します。

例：



**ステップ 2** [有効化 (Enable)] スイッチを [True] に切り替えます。

**ステップ 3** 必要な情報を入力します。各フィールドの説明を表示するには、(?) の上にマウスポインタを合わせます。

次のリストに、追加のフィールド情報を示します。

- [Utilization Threshold] : インターフェイスが輻輳していると LCM が判断する使用率を設定します。この値は、[Link Management] ページで個々のインターフェイスにしきい値を指定しない限り、すべてのインターフェイスに適用されます。
- [Profile ID] : LCM ポリシーへのトラフィックステアリングを有効にするために必要な設定です。autoroute (LCM が作成する戦術的な SR-TE ポリシーへのトラフィックのステアリング) は、(プロファイル ID を autoroute 機能に関連付ける PCC 上の設定と一致させるために) ここで設定した適切な [Profile ID] オプションを介して SR-TE ポリシーに適用されます。
- [輻輳確認間隔 (Congestion Check Interval) ] (秒単位) : この値は、LCM がネットワークの輻輳を評価する間隔を決定します。安定状態では、推奨のコミットがない場合、この間隔を使用してネットワークを再評価し、推奨事項を変更する必要があるかどうかを判断します。たとえば、間隔が 600 秒 (10 分) に設定されている場合、LCM は 10 分ごとにネットワークを評価して新しい輻輳を確認し、新しい推奨事項、または既存の推奨事項に対する変更が必要かどうかを判断します。変更の例としては、以前に推奨された個々のポリシーの削除や更新などがあります。ネットワークを変更すると、情報が安定して LCM に伝達されるまでに時間がかかる場合があるため、間隔を SNMP 収集パターンの 2 倍以上に設定します。
- [Interfaces to Monitor] : デフォルトでは、[Selected Interfaces] に設定されており、[Link Management] ページ ([Traffic Engineering] > [Local Congestion Mitigation] > [Domain-ID] > ... > [Link Management]) で CSV ファイルをインポートして、しきい値を個々のインターフェイスに追加する必要があります。[Link Management] ページで定義されたインターフェイスのみがモニターされます。[All Interfaces] に設定すると、LCM は、[Link Management] ページでアップロードされたカスタムしきい値を持つインターフェイスと、このページで設定された [Utilization Threshold] 値を使用して残りのインターフェイスをモニターします。
- [詳細設定 (Advanced) ] > [輻輳チェック抑制間隔 (秒) (Congestion Check Suspension Interval (seconds)) ] : この間隔によって、輻輳の検出と緩和を再開する前に ([すべてコミット (Commit All) ] が実行された後) 待機する時間が決まります。ネットワークモデルのコンバージェンスの時間を考慮するため、この間隔は SNMP 収集パターンの 2 倍以上に設定します。
- [Advanced] > [Auto Repair Solution] : [True] に設定すると、LCM はダウン、失敗、またはコミットされていない LCM TTE ポリシーを自動的に削除します。これは、主にポリシーの障害に対処するためのオプションです。

このオプションが無効で、[LCM Operational Dashboard] に表示される推奨の [Urgency] ステータスが [High] の場合、推奨されるソリューションは [Auto Repair Solution] の候補です。これは、ソリューションが展開されていない場合にネットワーク障害が発生する可能性が高いことを意味します。
- [Advanced] > [Adjacency Hop Type] : [Protected] に設定すると、LCM は保護された隣接関係 SID を使用して SR ポリシーを作成します。これにより、トポロジに依存しないループフリー代替 (TI-LFA) で隣接関係の障害のパスを計算できます。

(注) このオプションは、LCM が動作している同じ IGP エリア内のすべてのノードが厳密な SPF SID 対応である場合にのみ、[Protected] に設定する必要があります。
- [Advanced] > [Over-provisioning Factor (OPF)] : このオプションは、不均等な ECMP トラフィック分散 (エレファントフロー) に対処するのに役立ちます。この値により、バイパスポリシーのパスを計算するときに考慮する必要がある追加トラフィックの割合が決まります。LCM は、輻輳が原因でトラ

フィック量  $x$  を転送させる必要がある場合、 $x * (1 + OPF)$  トラフィックをサポートできるパスを検索します。詳細については、[LCM 計算のワークフロー \(91 ページ\)](#) を参照してください。デフォルト値は 0 です

**ステップ 4** 設定を保存するには、[Commit Changes] をクリックします。モニター対象インターフェイスで輻輳が発生すると、LCM は [LCM Operational Dashboard] に推奨事項を表示します (LCM は新しい TTE ポリシーを自動的にコミットしたり、展開したりしません)。その後、推奨される TTE ポリシーをプレビューし、コミットしてネットワークに展開するかどうかを決定できます。

## 個別のインターフェイスしきい値の追加

ネットワークにはさまざまなリンク (10G、40G、100G) があり、異なるしきい値を設定する必要があります。LCM または帯域幅最適化を使用する場合に、個々のインターフェイスに特定のしきい値を割り当てるには、次の手順を実行します。

**ステップ 1** メインメニューから、次のいずれかを選択します。

- [ローカルでの輻輳緩和 (Local Congestion Mitigation)] > [リンク管理 (Link Management)]
- [帯域幅最適化 (Bandwidth Optimization)] > [リンク管理 (Link Management)]

**ステップ 2**  をクリックします。

**ステップ 3** [サンプル設定ファイルのダウンロード (Download sample configuration file)] リンクをクリックします。

**ステップ 4** [キャンセル (Cancel)] をクリックします。

**ステップ 5** ダウンロードした設定ファイル (sampleLcmLinkManagement.csv) を開き、編集します。サンプルテキストを特定のノード、インターフェイス、およびしきい値情報に置き換えます。

**ステップ 6** ファイルの名前を変更して保存します。

**ステップ 7** [リンク管理 (Link Management)] ウィンドウに戻ります。

**ステップ 8**  をクリックして、編集した CSV ファイルに移動します。

**ステップ 9** [インポート (Import)] をクリックします。

**ステップ 10** [リンク管理 (Link Management)] ウィンドウに情報が正しく表示されることを確認します。

## LCM 動作のモニター

[LCM Operational Dashboard] ([Traffic Engineering] > [Local Congestion Mitigation] > [Domain-ID] > ... > [Operational Dashboard]) には、設定された使用率しきい値で定義された輻輳インターフェイスが表示されます。各インターフェイスについて、現在の使用率、推奨アクション、ステータス、推奨をコミットした後に予想される使用率などの詳細がリストされます。推奨事項

はセットの一部としてリストされ、展開されている場合はすべての変更がコミットされます。[Urgency] は、推奨事項の展開またはアクションの重要性を示します。[Urgency] の値は次のいずれかになります。

- [Low] : LCM インスタンス化ポリシーが不要になったために削除できること、または変更が不要であることを示します。
- [Medium] : 新規または変更された推奨事項を示します。
- [High] : ネットワーク障害と推奨事項を展開する必要があることを示します。これは、[Auto Repair Solution] の詳細オプションが有効になっている場合に自動的に対処できる候補です。「[LCM の設定 \(100 ページ\)](#)」を参照してください。

各列に表示される情報のタイプの説明を表示するには、マウスポインタを  に合わせます。このダッシュボードから、TTE ポリシーの推奨事項をプレビュー ( > [Preview]) して展開することもできます。

[LCM Operational Dashboard] に加えて、 > [Events] タブをクリックできます。[Events] ウィンドウに表示される LCM イベントを確認します。





## 第 9 章

# 帯域幅最適化（BWOpt）を使用したネットワークの最適化



- (注)
- この項で説明する機能は、Advanced RTM ライセンスパッケージの一部としてのみ使用できます。
  - この項では、ナビゲーションを[トラフィックエンジニアリング（Traffic Engineering）]>[トラフィックエンジニアリング（Traffic Engineering）]と記載しています。ただし、Crosswork Network Controller ソリューション内で Crosswork 最適化エンジンを使用する場合、ナビゲーションは[トラフィックエンジニアリング & サービス（Traffic Engineering & Services）]>[トラフィックエンジニアリング（Traffic Engineering）]になります。

- [帯域幅最適化の概要（105 ページ）](#)
- [BWOpt に関する特記事項（106 ページ）](#)
- [自動化されたネットワーク輻輳の緩和の例（107 ページ）](#)
- [帯域幅最適化の設定（110 ページ）](#)
- [個別のインターフェイスしきい値の追加（111 ページ）](#)
- [帯域幅最適化のトラブルシューティング（111 ページ）](#)

## 帯域幅最適化の概要

帯域幅最適化（BWOpt）は、ネットワーク内の輻輳を自動的に検出して緩和することで、セグメントルーテッドポリシーのクローズドループの戦術的トラフィックエンジニアリング（TTE）を提供します。テレメトリベースのセグメントルーティングトラフィックマトリックス（SRTM）を介して構築されたデマンドマトリックスでオーバーレイされたネットワークトポロジのリアルタイムビューによってこれを実現します。その目的は、リンクの使用率しきい値を設定することによって、帯域幅リソースの使用率を最適化することです。BWOpt は、ユーザーが要求したインターフェイス使用率のしきい値を使用し、ネットワークの実際の使用率と比較します。インターフェイスの輻輳が BWOpt によって検出されると、BWOpt は、SR-PCE

を介してネットワークに展開された TTE SR ポリシーを使用してインテントベースのトラフィックをホットスポットから再度ルーティングしようとしています。ネットワークの状態（トポロジまたはトラフィック、あるいはその両方）が時間の経過とともに変化する場合、BWOpt は引き続きインターフェイスの使用率をモニターし、展開された TTE SR ポリシーを管理します。これには、パスの変更や、不要になったと見なされた場合のネットワークからの削除が含まれます。

## BWOpt に関する特記事項

BWOpt を使用する場合は、次の情報を考慮してください。

- BWOpt を使用するには、Advanced RTM ライセンスパッケージが必要です。
- LCM が有効になっている場合は、帯域幅最適化を有効にできません。
- BWOpt は、作成しなかった既存の SR-TE ポリシー内のトラフィックを移動しません。これにより、輻輳したリンク上のトラフィックのほとんどが BWOpt 以外の SR-TE ポリシー内にある場合に、輻輳を緩和できなくなる場合があります。
- BWOpt は、PCC の autoroute 機能を使用して、作成する戦術的な SR-TE ポリシーにトラフィックを誘導します。autoroute は、BWOpt で設定された適切な [プロファイル ID (Profile ID)] のオプションを介してこれらのポリシーに適用されます（そのプロファイル ID を autoroute 機能に関連付ける PCC 上の設定と一致させるため）。これは、輻輳したリンクからトラフィックを移動させる戦術的な SR ポリシーにとって重要です。
- シングルレベル IGP ドメインでのみ BWOpt を有効にします。
- BWOpt は、セグメントルーティングトラフィックマトリックス (SR-TM) の使用を活用します。SR-TM には次の制限があります。
  - IPv6 はサポートされていません。
  - 管理、バンドル、サブインターフェイス、およびトンネルインターフェイスは、外部インターフェイスとしてサポートされていません。
  - デフォルト以外の仮想、ツーティング、および転送 (VRF) は外部インターフェイスとしてサポートされていません。
  - SR-TM は、SR ラベル付きトラフィックのみを考慮します。Label Distribution Protocol (LDP; ラベル配布プロトコル) トラフィックは考慮されません。



(注) SR-TM の詳細については、『[Segment Routing Traffic Matrix](#)』を参照してください。

- BWOpt は、測定された SR-TM データに基づいてシミュレートされたトラフィックを使用して、リンク使用率と輻輳を緩和するタイミングを決定します。BWOpt がモニターするシミュレートされたインターフェイス使用率は、UI に表示される SNMP ベースのインター

フェイス使用率と厳密に一致する必要があります。ただし、SNMPポーリング頻度やレート平均化手法などのさまざまな要因により、それらが異なる場合があります。これにより、UIでリンクが輻輳しているように見え、BWOptが反応していないという状況になることがあります。

- BWOptは、SRTMテレメトリデータの送信元であるPCCにのみ戦術的なSR-TEポリシーを作成します。これらのノード（通常はプロバイダーエッジルータ）のみが、そのノードからネットワーク内の他のPEノードへのトラフィックを表す内部モデル内のシミュレーションされたトラフィック要求を作成するために必要なテレメトリベースのデータを提供します。
- (すべてのインターフェイスに対して設定された) しきい値を下回るインターフェイス使用率になるソリューションのみが展開されます。BWOptがネットワーク全体の輻輳を緩和できない場合は、戦術的なSR-TEポリシーを展開し、「ネットワークが輻輳しています。BWOptで緩和できません。(Network Congested. BWOpt unable to mitigate.)」というアラームが発生します。このアラームは、輻輳が自然に軽減されるか、またはBWOptの戦術的SR-TEポリシーの展開によってうまく対処できた場合に解消されます。
- BWOptは、トポロジサービスからのトポロジの再起動または再構築が原因でシステムが使用できなくなった場合は常に、一時的に動作を停止します。これが発生すると、この状態を示すアラームがBWOptによって設定されます。この間、BWOptはネットワークの輻輳を評価しません。現在展開されているすべての戦術的SRポリシーは維持されますが、変更または削除されません。モデルが使用可能になるとすぐにアラームがクリアされ、BWOptは通常の動作を再開します。

## 自動化されたネットワーク輻輳の緩和の例

この例では、帯域幅最適化 (BWOpt) が、ユーザーの介入なしでインテントベースのトラフィックを再ルーティングすることで、ネットワークの輻輳を自動的に緩和する方法を示します。この例では、IGPメトリックを最小化するように最適化の目的が設定されています。

次のBWOptオプションが設定されます ([トラフィック エンジニアリング (Traffic Engineering)] > [帯域幅最適化 (Bandwidth Optimization)] > [設定 (Configuration)])。

図 21: 帯域幅最適化の設定

Bandwidth Optimization

Configuration

Basic Advanced

Enable  False  True

Optimization Objective

Color

Utilization Threshold

Utilization Hold Margin

Maximum Global Reoptimization Interval

Profile ID

Max Number of Parallel Tactical Policies

次に、米国に及ぶさまざまなデバイスとリンクのネットワークを示します。[SRポリシー (SR Policies)] テーブルに SR-TE ポリシーがリストされていないことに注意してください。

図 22: 例: 現在のネットワーク

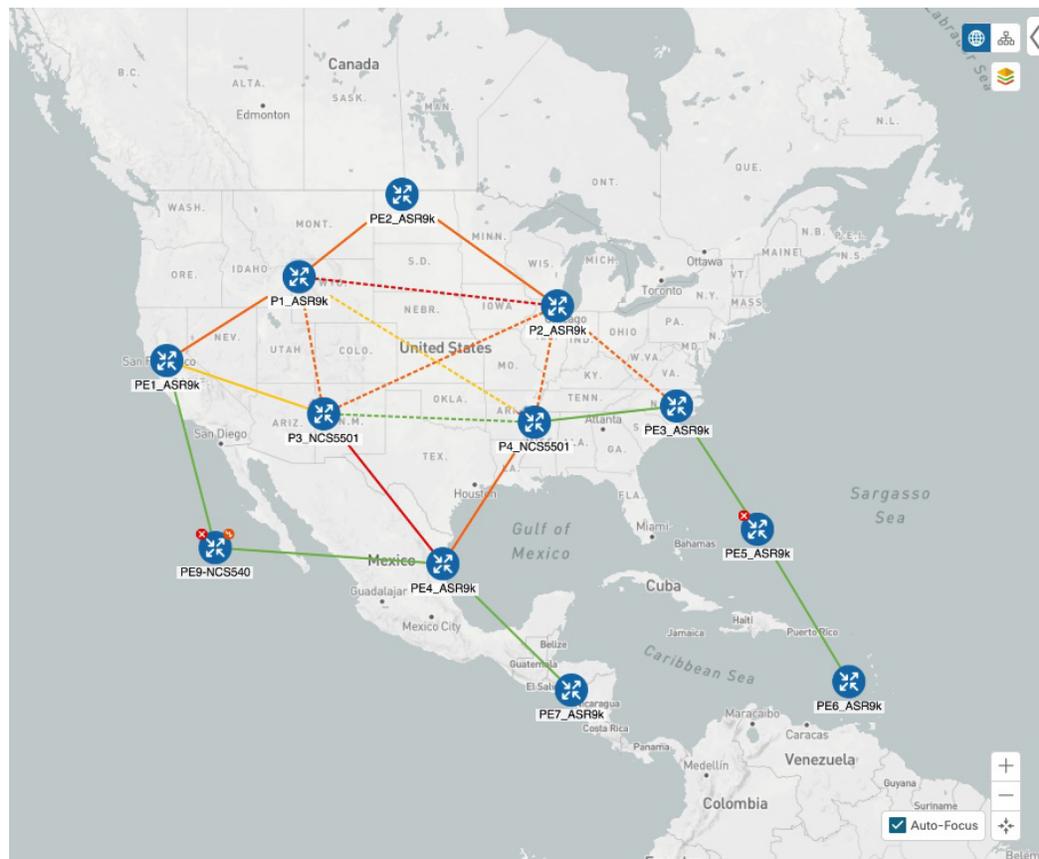
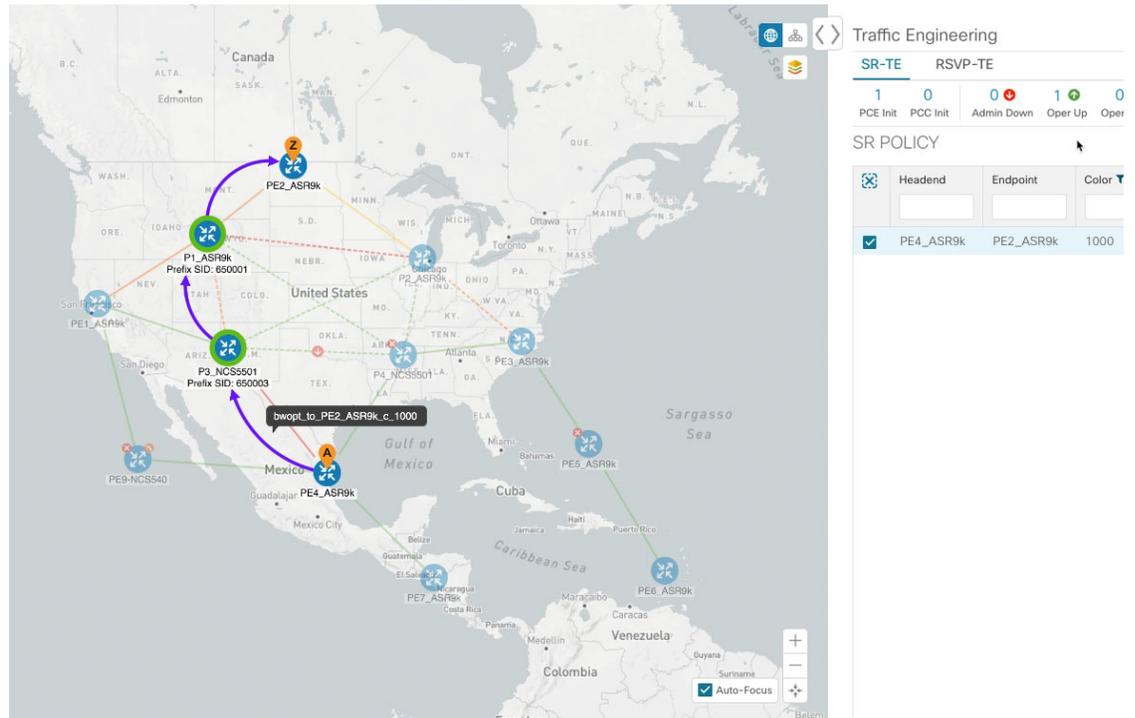




図 24: 例 : 展開された戦術的 SR ポリシー



BWOptは、ネットワークを継続的にモニターします。P3\_NCS5501とP4\_NCS5501間のリンクが復旧すると、BWOptは（定義された基準に基づいて）輻輳が緩和されたことを検出します。輻輳が、設定された使用率しきい値から使用率ホールドマージンを差し引いた値を下回ると、戦術的SR-TEポリシーは自動的にネットワークから削除されます。

BWOptによって作成された戦術的SR-TEポリシーのインスタンス化と削除に関連するイベントを表示するには、をクリックします。

## 帯域幅最適化の設定



(注) 帯域幅最適化 (BWOpt) は、Advance ライセンスパッケージの一部としてのみ使用できます。

BWOptを有効にすると、設定された使用率のしきい値に基づいて、ネットワーク内のすべてのインターフェイスの輻輳がモニターされます。使用率のしきい値を超えると、戦術的なポリシーが自動的に展開され、トラフィックが輻輳したリンクから移動されます。輻輳が緩和されると、BWOptは戦術的SRポリシーを自動的に削除します。

**ステップ 1** メインメニューから、[トラフィックエンジニアリング (Traffic Engineering)] > [帯域幅最適化 (Bandwidth Optimization)] を選択します。

ステップ2 [有効化 (Enable) ] スイッチを [True] に切り替えます。

(注) LCM と帯域幅の最適化を同時に有効にすることはできません。

ステップ3 必要な情報を入力します。各フィールドの説明を表示するには、 の上にマウスポインタを合わせます。

ステップ4 [変更を確定 (Commit Changes) ] をクリックします。BWOpt は、設定したしきい値と最適化の目的に基づいて、ネットワーク輻輳のモニターを開始します。

---

## 個別のインターフェイスしきい値の追加

ネットワークにはさまざまなリンク (10G、40G、100G) があり、異なるしきい値を設定する必要があります。LCM または帯域幅最適化を使用する場合に、個々のインターフェイスに特定のしきい値を割り当てるには、次の手順を実行します。

ステップ1 メインメニューから、次のいずれかを選択します。

- [ローカルでの輻輳緩和 (Local Congestion Mitigation) ] > [リンク管理 (Link Management) ]
- [帯域幅最適化 (Bandwidth Optimization) ] > [リンク管理 (Link Management) ]

ステップ2  をクリックします。

ステップ3 [サンプル設定ファイルのダウンロード (Download sample configuration file) ] リンクをクリックします。

ステップ4 [キャンセル (Cancel) ] をクリックします。

ステップ5 ダウンロードした設定ファイル (sampleLcmLinkManagement.csv) を開き、編集します。サンプルテキストを特定のノード、インターフェイス、およびしきい値情報に置き換えます。

ステップ6 ファイルの名前を変更して保存します。

ステップ7 [リンク管理 (Link Management) ] ウィンドウに戻ります。

ステップ8  をクリックして、編集した CSV ファイルに移動します。

ステップ9 [インポート (Import) ] をクリックします。

ステップ10 [リンク管理 (Link Management) ] ウィンドウに情報が正しく表示されることを確認します。

---

## 帯域幅最適化のトラブルシューティング

輻輳を適切に管理するその機能を妨げ、不安定な状態の要因となる特定のエラー状態が発生すると、BWOpt はそれ自体を無効にし、アラームを発行します。次の表に、これらの条件の一部と、調査の対象として考えられる原因を示します。BWOpt のログを参照すると、エラー状態ごとに追加の詳細情報を取得できます。



(注) [管理 (Administration)] > [収集ジョブ (Collection Jobs)] に移動し、[App ID] 列で Optimization Engine のアクティブな収集ジョブのリストをフィルタ処理できます。

表 5: エラー

エラーイベントメッセージ	考えられる原因と推奨される修正処置
Optima Engine モデルエラー	<p>Optimization Engine を通じて BWOpt で使用されるネットワークモデルが破損しているか、または BWOpt を適切にサポートするために必要なキーデータが欠落しています。考えられる原因には、Optimization Engine とトポロジサービス間のネットワーク検出の問題または同期の問題などがあります。Optimization Engine ポッドを再起動してモデルの再構築を試してください。</p> <p>このエラーは、SR-PCE を通じて戦術的ポリシーを展開し、それを検出し、モデルに追加するために必要な時間が BWOpt に設定された [展開のタイムアウト (Deployment Timeout)] オプションを超えた場合にも発生します。デフォルトは 30 秒で、小規模から中規模のネットワークの場合はこれで十分です。ただし、大規模なネットワークではそれ以上の時間が必要になる場合があります。</p>
PCE ディスパッチが到達不能	<p>ネットワークへの戦術ポリシーの展開は、[展開タイムアウト (Deployment Timeout)] を超える前は正常に確認されません。[展開のタイムアウト (Deployment Timeout)] オプションの値を引き上げて、大規模なネットワークでの展開にさらに時間をかけるようにします。</p>
戦術的 SR ポリシーを展開できない	<p>SR-PCE への戦術的な SR ポリシーの導入が失敗しています。これにはさまざまな理由が考えられます。BWOpt または PCE あるいはその両方のディスパッチログに障害の詳細に関するガイダンスが示されることがあります。SR-PCE プロバイダーのいずれかを介した PCC への基本的な SR ポリシーのプロビジョニング機能が動作していることを確認します。</p>



## 第 10 章

# インテントベースの帯域幅要件の定義と維持



(注) この項で説明する機能は、Advance RTM ライセンスパッケージの一部としてのみ使用できません。

オンデマンド帯域幅 (BWoD) は、帯域幅を認識するパス計算要素 (PCE) を提供し、使用可能な場合は要求された帯域幅を使用して SR ポリシーパスを取得します。計算されたパスは、SR-PCE を介してネットワークに展開されます。BWoD は継続的にリンク使用率をモニターし、パス上で輻輳が発生しないようにします。ネットワークの状態が変化してリンクの使用率がユーザーが設定した輻輳しきい値を超えると、BWoD は自動的にポリシーパスを再最適化します。BWoD は、PCE によって開始された SR-TE ポリシーと PCC によって開始された SR-TE ポリシーの両方の帯域幅制約をサポートしています。

BWoD は、ネットワークの準リアルタイムモデルと SNMP ベースの SR ポリシートラフィックの測定値を使用して、BWoD ポリシーが帯域幅の制約を満たすようにします。ユーザーは、ネット使用率のしきい値 (輻輳の定義) とパス最適化の目的など、選択したアプリケーションのオプションを使用して、BWoD の動作を微調整し、計算したパスに影響を与えることができます。BWoD は、UI を介して作成された SR ポリシーと、SR-PCE への委任を行うヘッドエンド上の CLI 設定を介して作成された SR ポリシーに対して、帯域幅を認識する PCE として機能します。後者の場合、SR-PCE は、帯域幅制限とともに SR ポリシーを BWoD にさらに委任してパスを計算し、BWoD によって戻された計算済みのパスをヘッドエンドに中継してインスタンス化します。

- [BWoD に関する特記事項 \(114 ページ\)](#)
- [インテントベースの帯域幅の要件を維持するための SR-TE ポリシーのプロビジョニングの例 \(114 ページ\)](#)
- [オンデマンド帯域幅の設定 \(118 ページ\)](#)
- [BWoD のトラブルシューティング \(119 ページ\)](#)

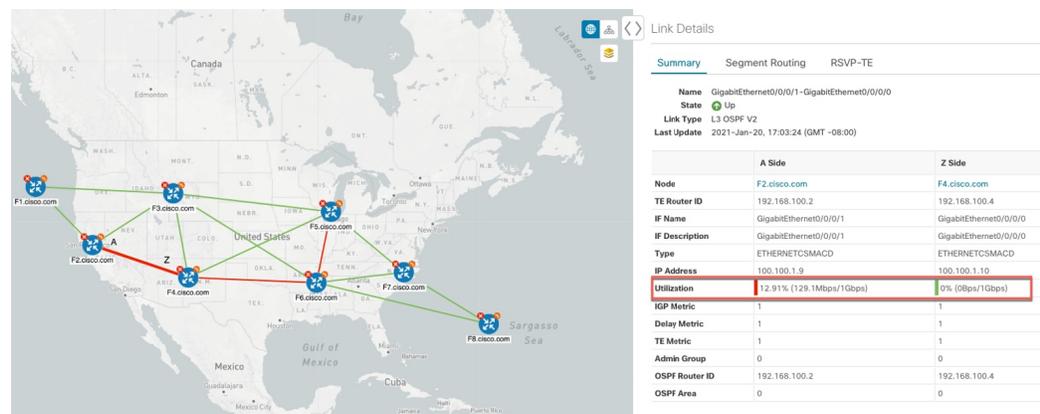
## BWoDに関する特記事項

BWoDを使用する場合は、次の情報を考慮してください。

- BWoDを使用するには、Advanced RTM ライセンスパッケージが必要です。
- 要求された帯域幅を保証するポリシーのパスをBWoDが検出できない場合、このオプションが有効になっていると、BWoDは「ベストエフォート」パスの検出を試みます。
- Optimization Engineの再起動またはトポロジサービスタからのトポロジの再構築が原因でOptimization Engineモデルが使用できなくなると、BWoDは一時的に動作を停止します。この期間中のBWoDへの要求は拒否されます。モデルが使用可能になり、BWoDがOptimization Engineから2つのトラフィック更新を受信すると、BWoDは通常の動作を再開します。

## インテントベースの帯域幅の要件を維持するためのSR-TEポリシーのプロビジョニングの例

図 25: 初期 BWoD トポロジの例



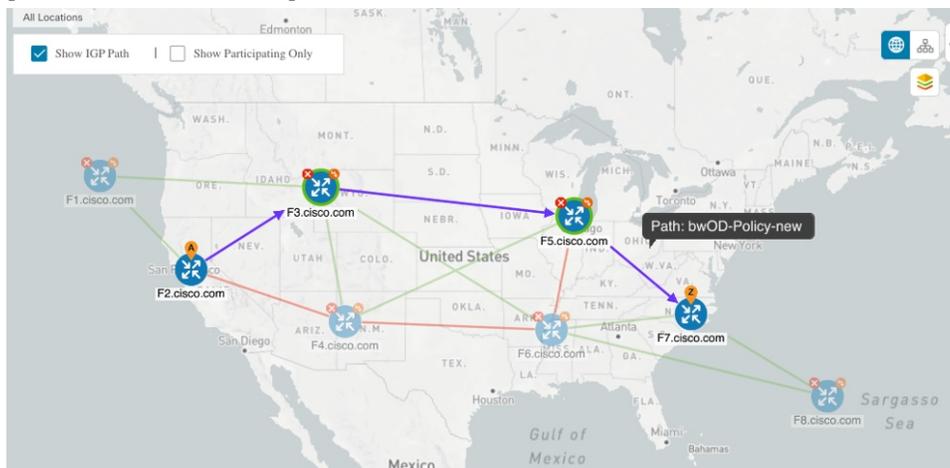
このシナリオでは、上記のトポロジを使用します。目標は、F2.cisco.com から F7.cisco.com へのパスを作成し、使用率を 80% に維持しながら 920 Mbps のトラフィックに対応できるようにすることです。上記の例では、ノード F2.cisco.com とノード F4.cisco.com の使用率が強調表示され、リンクが使用中であり、1 Gbps の容量があることが示されています。要求された帯域幅の追加が使用率のしきい値を超えるため、BWoDは最初にこのリンクを含まない単一のパスを見つけようとします。単一のパスが見つからない場合、BWoDはパスの分割を推奨する場合があります。

ステップ 1 BWoD を有効にして設定します。

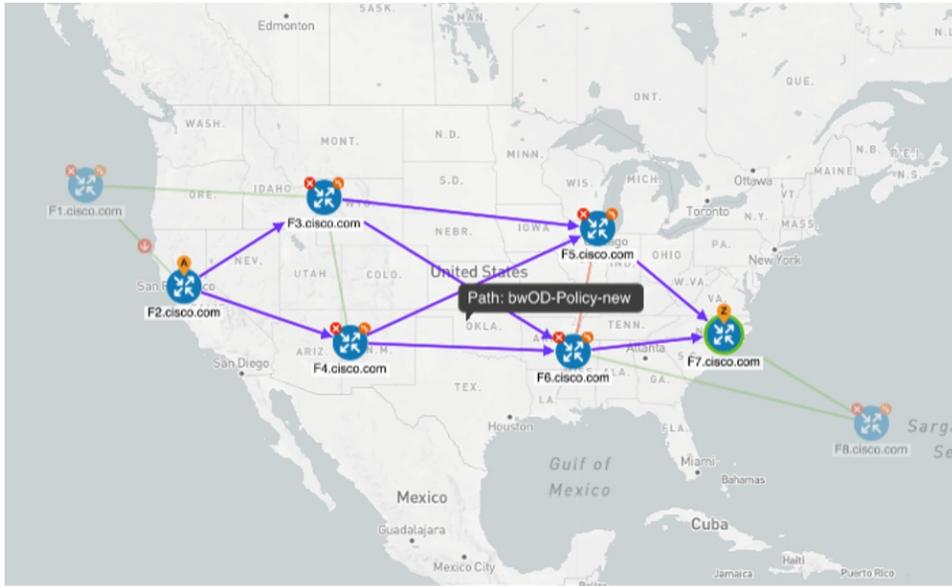
- a) メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [オンデマンド帯域幅 (Bandwidth on Demand)] > [設定 (Configuration)] を選択します。
- b) [有効化 (Enable)] スイッチを [True] に切り替え、**80** を入力して使用率のしきい値のパーセンテージを設定します。他のオプションの説明を表示するには、**?** の上にマウスを重ねます。
- c) [変更を確定 (Commit Changes)] をクリックします。

**ステップ 2** PCE によって開始された BWoD SR-TE ポリシーを作成します。

- a) メインメニューから [トラフィック エンジニアリング (Traffic Engineering)] > [SR-TE] タブを選択し、[+ 作成 (+Create)] をクリックします。
- b) 必要な SR-TE ポリシーの詳細を入力します。
- c) [ポリシーパス (Policy Path)] フィールドで、[オンデマンド帯域幅 (Bandwidth on Demand)] をクリックし、BWoD パスの一意の名前を入力します。この場合は、**bwOD-Policy-new** と入力します。
- d) [最適化の目的 (Optimization Objective)] ドロップダウンリストから、[トラフィック エンジニアリング (TE) メトリック (Traffic Engineering (TE) Metric)] を選択します。
- e) [帯域幅 (Bandwidth)] フィールドに、要求された帯域幅を入力します。この例では、**920 Mbps** を要求しています。
- f) [プレビュー (Preview)] をクリックします。



上記の例では、BWoD は使用率が低く、使用率のしきい値を超えずに要求された帯域幅に対応できる単一のパスを検出します。



上記の例では、BWoD は複数のリンクの使用率と容量の制限により、単一のパスを見つけることができません。この場合、BWoD はパスを分割して帯域幅と使用率の要件を取得します。

- g) 提案された SR-TE ポリシーの展開に問題がなければ、[プロビジョニング (Provision)] をクリックします。

**ステップ 3** 新しい BWoD SR-TE ポリシーが作成されたことを確認します。

- a) メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [SR-TE] を選択します。
- b) 新しい BWoD SR-TE ポリシーを選択し、SR ポリシーの詳細を表示します ([表示 (View)] をクリックして選択します)。[ポリシータイプ (Policy Type)] は [オンデマンド帯域幅 (Bandwidth on Demand)] であることを注意してください。

## PCCによって開始された BWoD SR-TE のポリシー

有効にすると、BWoD は Crosswork Optimization Engine で設定されたすべての SR-PCE プロバイダーに自動的に接続します。SR-PCE BWoD REST API に永続的に接続され、帯域幅が制約された SR-TE ポリシーの PCE として登録されます。

次の図に、BWoD の PCC によって開始されたワークフローを示します。



引き出し線番号	説明
5、6	帯域幅準拠のパスが見つかった場合、セグメントリストが SR-PCE に返され、PCEP を介して PCC に転送され、PCC によってインスタンス化されます。BWoD がポリシーの BW 準拠パスを計算できない場合か、または BWoD が既存の BWoD ポリシーに BW 準拠パスを持たないように強制する場合は、BWoD によってベストエフォートパスが計算され、違反が最小限に抑えられます。また、これが発生したことで、BWoD が COE イベント UI にイベントを発行し、現在ベストエフォートパスになっている BWoD ポリシーを示します。
7	BWoD SR-TE ポリシーがインスタンス化されます。

## オンデマンド帯域幅の設定

オンデマンド帯域幅 (BWoD) の設定は次の 2 つの部分から構成されています。

1. BWoD オプションを有効にし、設定します。
2. BWoD SR ポリシーを作成します。BWoD が有効になっている限り、複数の BWoD SR ポリシーを作成できます。

- 
- ステップ 1** メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [オンデマンド帯域幅 (Bandwidth on Demand)] > [設定 (Configuration)] を選択します。
- ステップ 2** [有効化 (Enable)] スイッチを [True] に切り替えます。
- ステップ 3** 追加のオプションを設定します。各フィールドの説明を表示するには、 の上にマウスポインタを合わせます。
- ステップ 4** [変更のコミット (Commit Changes)] をクリックして、設定を保存します。
- ステップ 5** BWoD SR ポリシーを作成するには、[Traffic Engineering (トラフィック エンジニアリング)] > [トラフィック エンジニアリング (Traffic Engineering)] に移動します。
- ステップ 6** [SR ポリシー (SR Policy)] テーブルで、[作成 (Create)] > [PCE によって開始 (PCE Init)] をクリックします。
- ステップ 7** 必要な SR ポリシーの詳細を入力する以外に、[オンデマンド帯域幅 (Bandwidth on Demand)] オプションをクリックし、必要な帯域幅を入力します。
- ステップ 8** [プレビュー (Preview)] をクリックして、提案された SR ポリシーを表示します。
- ステップ 9** [プロビジョニング (Provision)] をクリックして、SR ポリシーをコミットします。
-

# BWoD のトラブルシューティング

次に、BWODの最も一般的ないくつかのエラー状態と問題を解決する可能性のある修正処置を示します。

表 6: エラー

エラーイベントメッセージ	考えられる原因と推奨される修正処置
OptimaModelError	<p>Optimization Engine を通じて BWoD で使用されるネットワークモデルが破損しているか、または BWoD を適切にサポートするために必要なキーデータが欠落しています。考えられる原因には、Optimization Engine とトポロジサービス間のネットワーク検出の問題または同期の問題などがあります。Optimization Engine ポッドを再起動してモデルの再構築を試してください。</p> <p>このエラーは、展開された後にポリシーを検出してモデルに追加するために必要な時間が、BWOD に設定された [展開のタイムアウト (Deployment Timeout) ] オプションを超えた場合にも発生する可能性があります。デフォルトは 30 秒で、小規模から中規模のネットワークの場合はこれで十分です。ただし、大規模なネットワークではそれ以上の時間が必要になる場合があります。</p>
NATSTimedOutError	<p>SR-PCEによる帯域幅ポリシーの展開がBWODに設定された [展開のタイムアウト (Deployment Timeout) ] オプションを超えている。 [展開のタイムアウト (Deployment Timeout) ] オプションの値を引き上げて、大規模なネットワークでの展開にさらに時間をかけるようにします。</p>
トレースバックまたはログファイルで見つかったその他のエラー	<p>シスコの営業担当者にお問い合わせください。</p>



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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.

