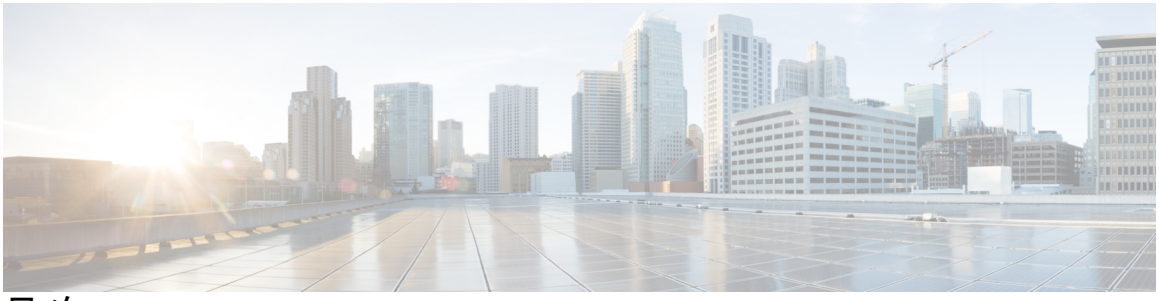
Cisco Crosswork Optimization Engine 7.0 ユーザーガイド

最終更新：2025 年 3 月 17 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 について 1

対象読者 1

Cisco Crosswork 最適化エンジン の概要 2

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

帯域幅機能パック 3

Crosswork Optimization Engine API 4

第 2 章

Cisco Crosswork 最適化エンジン でのトラフィック エンジニアリング 5

サポート対象の SR-TE ポリシーと RSVP トンネル 6

セグメントルーティングの概要 6

セグメントルーティングパス計算要素（SR-PCE） 9

SR-TE ポリシー PCC および PCE 設定のソース 9

PCC によって開始された SR-TE ポリシーの例 10

リソース予約プロトコル（RSVP）について 10

RSVP-TE トンネル PCC および PCE 設定のソース 12

PCC によって開始された RSVP-TE トンネルの例 12

トラフィック エンジニアリング サービスのクイックビューを取得する 13

TE イベントと使用率履歴の表示 15

トラフィック エンジニアリング デバイスの詳細の表示 17

トラフィック エンジニアリング設定の構成 18

TE タイムアウトの設定 18

トラフィック エンジニアリング用のデバイスグループの表示方法の構成 19

TE データ保持設定の構成 20

SR-TE ポリシーと RSVP-TE トンネルの解決 20

第 3 章 SR-MPLS および SRv6 21

トポロジマップでの SR-MPLS および SRv6 ポリシーの表示 21

SR-MPLS および SRv6 ポリシーの詳細の表示 24

IGP パスとメトリックの視覚化 26

複数の候補パス（MCP）の検索 27

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 30

ネイティブ SR パスの可視化 33

ネイティブパスデバイスの前提条件の可視化 35

TE リンクアフィニティの設定 36

明示的 SR-MPLS ポリシーの作成 38

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 39

SR-MPLS ポリシーの変更 41

第 4 章 リソース予約プロトコル（RSVP） 43

トポロジマップでの RSVP-TE トンネルの表示 43

RSVP-TE トンネルの詳細の表示 46

明示的 RSVP-TE トンネルの作成 49

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 50

RSVP-TE トンネルの変更 51

第 5 章 フレキシブルアルゴリズム 53

フレキシブルアルゴリズムのアフィニティの設定 53

フレキシブル アルゴリズム トポロジの可視化 54

フレキシブルアルゴリズムの詳細の表示 56

第 6 章 ツリーセグメント識別子（Tree-SID）マルチキャスト トラフィック エンジニアリング 59

Tree-SID ポリシーの可視化 60

トポロジマップでポイントツーマルチポイント ツリーを表示する 60

静的 Tree-SID ポリシーの作成 64
Crosswork UI による静的 Tree-SID ポリシーの設定例 66
ツリー SID ポリシーを変更する 68
Tree-SID の特記事項 68

第 I 部： 帯域幅機能パック 71

第 7 章 SR 回線型マネージャ（CSM） 73
回線型 SR-TE に関する特記事項 73
CS SR-TE ポリシーの可視化を設定するためのワークフロー 78
SR 回線型マネージャ を有効にする 80
回線型 SR ポリシーの設定 81
回線型 SR-TE ポリシーの帯域幅使用率の確認 83
回線型 SR-TE ポリシーの表示 85
回線型 SR-TE ポリシーを再計算するための CSM のトリガー 90
帯域幅予約の設定を超えた場合の動作 91
CSM のパス障害の処理方法 95

第 8 章 ローカル輻輳緩和（LCM） 99
ローカル輻輳緩和の概要 99
LCM の輻輳評価要件 100
LCM の使用に関する厳密な SID の有効化 100
LCM の輻輳緩和要件 102
LCM に関する特記事項 103
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 105
LCM 計算のワークフロー 106
ワークフローの例：ローカルインターフェイスでの輻輳の緩和 108
LCM の設定 114
個別のインターフェイスしきい値の追加 117
LCM 動作のモニター 119

LCM からのインターフェイスの一時的な除外 122

第 9 章 オンデマンド帯域幅（BWoD） 125

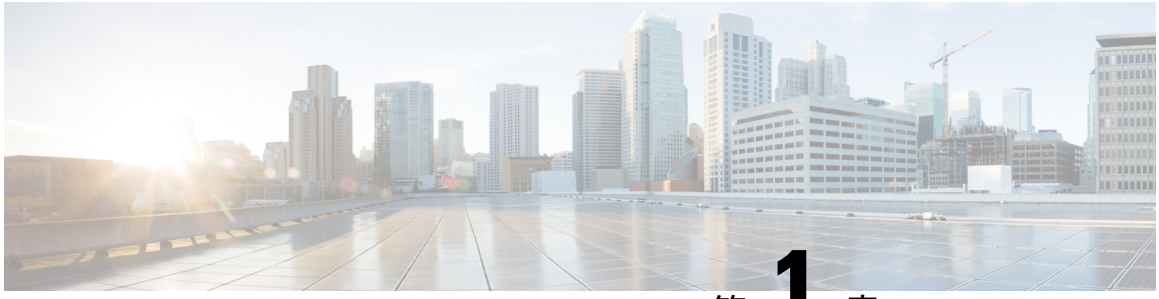
BWoD に関する特記事項 125

PCC によって開始された BWoD SR-TE のポリシー 126

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 128

オンデマンド帯域幅の設定 134

BWoD のトラブルシューティング 135



第 1 章

Cisco Crosswork Optimization Engine について

- 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 Network Controller ソリューションと Crosswork Optimization Engine （3 ページ）
- 帯域幅機能パック （3 ページ）
- Crosswork Optimization Engine API （4 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）
- ポイントツーマルチポイントのツリー（Tree-SID）
- フレキシブルアルゴリズム

Cisco Crosswork 最適化エンジン の概要

Cisco Crosswork 最適化エンジン は、一連の Cisco Crosswork Network Automation の製品の一部であり、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 Optimization Engine は、個別のアプリケーションとして、および Cisco Crosswork ネットワークコントローラ のトラフィック エンジニアリング コンポーネントとして提供されます（Crosswork Network Controller ソリューションと Crosswork Optimization Engine （3 ページ）を参照）。

Crosswork 最適化エンジン は、次のとおりです。

- 次のような有益な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
  - SR-TE ポリシー
    - SR-MPLS および SRv6
    - Tree-SID
    - フレキシブルアルゴリズム
    - 回線型セグメントルーティング（CS-SR）ポリシー
  - 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 ポリシーと RSVP-TE トンネルをプロビジョニングし、それらを変更または削除する
  - SR 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 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）
  - 静的ポイントツーマルチポイント（Tree-SID）ポリシーのプロビジョニング
  - 回線型 SR-TE ポリシーのプロビジョニング
- 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。

このガイドでは、Crosswork Optimization Engine のすべての機能を説明します。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（『Crosswork Network Controller Administration Guide』を参照してください）。ライセンスと注文に関する情報については、シスコパートナーまたはシスコのアカウント担当者にお問い合わせください。

Crosswork Network Controller ソリューションと Crosswork Optimization Engine

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す。サービスアジリティやコスト効率の向上、最適化を実現し、お客様に価値を提供するまでの時間を短縮し、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て、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、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 Optimization Engine は、単独でアクティブ化することも、他の Crosswork コンポーネントと組み合わせてアクティブ化することもできます（『Crosswork Network Controller Installation Guide』を参照）。このドキュメント全体で、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、一部のオプションは若干異なるか、または使用できません。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。

帯域幅機能パック

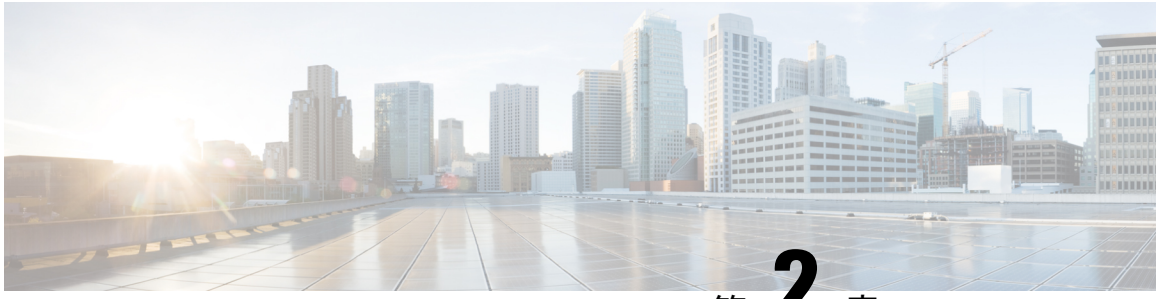
Crosswork 最適化エンジン 機能パック（特定のライセンスで利用可能）は、輻輳に対処し、SR-TE ポリシーを管理するように設計されたツールであり、帯域幅、遅延などに基づいて要件のメンテナンスと最適化を保証します。ユーザーが最適化の目的を指定し、ツールはその目的を実現しながら、継続的にモニター、追跡、対応して元の目的を維持できます。これらの機能パックの詳細については、次のトピックを参照してください。

- ローカル輻輳緩和（LCM） （99 ページ）
- SR 回線型マネージャ（CSM） （73 ページ）
- オンデマンド帯域幅（BWoD） （125 ページ）

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。



第 2 章

Cisco Crosswork 最適化エンジン でのトラフィック エンジニアリング

トラフィック エンジニアリング（TE）は、ネットワーク内のトラフィックを最適化およびステアリングして、優先順位付けされたトラフィックに保証された帯域幅ルートを使用するなど、運用目標を達成したり、カスタムサービスを提供したりする方法です。TE がネットワークパフォーマンスを向上させる方法の 1 つは、トラフィックに事前定義されたルートを強制し、使用可能なリソースを効果的に使用することです。

Crosswork を使用する最大の利点の 1 つは、トポロジマップで SR-TE ポリシーと RSVP-TE トンネルを可視化できることです。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。

ブラウンフィールド展開での既存の SR-TE ポリシーと RSVP-TE

Crosswork は、デバイスのインポート時に既存のポリシーとトンネルを検出しますが、それらを管理することはできません。Crosswork は、Crosswork でプロビジョニングされたポリシーのみを管理できます。

ここでは、次の内容について説明します。

- サポート対象の SR-TE ポリシーと RSVP トンネル （6 ページ）
- セグメントルーティングの概要 （6 ページ）
- セグメントルーティングパス計算要素（SR-PCE） （9 ページ）
- SR-TE ポリシー PCC および PCE 設定のソース （9 ページ）
- リソース予約プロトコル（RSVP）について （10 ページ）
- RSVP-TE トンネル PCC および PCE 設定のソース （12 ページ）
- トラフィック エンジニアリング サービスのクイックビューを取得する （13 ページ）
- TE イベントと使用率履歴の表示 （15 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 （17 ページ）
- トラフィック エンジニアリング設定の構成 （18 ページ）
- SR-TE ポリシーと RSVP-TE トンネルの解決 （20 ページ）

サポート対象の SR-TE ポリシーと RSVP トンネル

Crosswork Traffic Engineering は、ほとんどの SR-TE ポリシーと RSVP トンネルの可視化とプロビジョニングをサポートしています。Crosswork でプロビジョニングされていない既存のポリシーがあるネットワークでは、検出はされますが、管理することはできません。

表 *1*: サポート対象の *TE* テクノロジー

TE テクノロジー	Crosswork Optimization Engine	
	視覚化	プロビジョニング（PCE によって開始）
SR-MPLS	✓	✓
SRv6	✓	✗
RSVP	✓	✓
フレキシブルアルゴリズム	✓	✗[1]
Tree-SID	✓	✓[2]
回線型	✓	✓

[1] SR-TE ポリシーをプロビジョニングする場合、フレキシブルアルゴリズムの一部である SID が含まれるセグメントリストを使用できます。
[2] 静的 Tree-SID ポリシーのみサポートされています。動的 Tree-SID ポリシーは、デバイス上で手動でプロビジョニングすることも、API を介してプロビジョニングすることもできます。

（注） Crosswork は、ロールベース アクセス コントロール（RBAC）の使用をサポートしており、ユーザーが実行できる機能だけでなく、それらの機能を実行できるデバイスも制限します。『Cisco Crosswork Network Controller Administration Guide』を参照してください。

既知の制限事項、重要な注意事項、およびサポートされているネットワークテクノロジーのリストについては、『Cisco Crosswork Optimization Engine Release Notes』を参照してください。

セグメントルーティングの概要

トラフィック エンジニアリング用のセグメント ルーティングは、送信元と宛先のペア間のトンネルを通じて行われます。トラフィック エンジニアリング用のセグメント ルーティングでは、送信元ルーティングの概念が使用されます。送信元はパスを計算し、パケットヘッダーで

セグメントとしてエンコードします。セグメントは、任意のタイプの命令の識別子です。例えば、トポロジ セグメントは、宛先へのネクスト ホップを識別します。各セグメントを識別するセグメントID（SID）は、32ビットの符号なし整数で構成されます。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、プロバイダー コア ネットワークのルータに、IGPによって計算された最短パスではなく指定されたパスに従うように指示します。宛先はトンネルの存在を認識しません。

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。これは、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）範囲から手動で設定され、IS-IS（Intermediate System to Intermediate System）またはOSPF（Open Shortest Path First）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、隣接関係SIDと呼ばれるラベルによって識別されます。このラベルは、出力インターフェイスなど、隣接ルータへの特定の隣接関係を表します。隣接関係SIDは、IS-ISまたはOSPFによって配布されます。隣接関係セグメントは、トラフィックを特定の隣接関係に誘導します。

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

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

セグメント ルーティング ポリシー

トラフィック エンジニアリングを実現するためのセグメントルーティングでは、ネットワークを介してトラフィックを誘導する「ポリシー」を使用します。SR ポリシーパスは、セグメントID（SID）リストと呼ばれるパスを指定するセグメントのリストとして表されます。各セグメントは、送信元から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、ヘッドエンドは SID リストをパケットにプッシュします。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。

Crosswork は、次の SR 関連ポリシーの可視化（および一部のプロビジョニング）をサポートしています。

- SR-MPLS および SRv6 （21 ページ）
- フレキシブルアルゴリズム （53 ページ）
- ツリーセグメント識別子（Tree-SID）マルチキャスト トラフィック エンジニアリング （59 ページ）
- SR 回線型マネージャ（CSM）

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ーに関する十分な情報がない場合、ヘッドエンドは計算をパス計算エンジン（PCE）に委任できます。

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。

分離

Crosswork はディスジョイントポリシーを使用して、2 つの送信元ノードから 2 つの宛先ノードへのトラフィックをディスジョイントパスに沿って誘導する 2 つのセグメントのリストを計算します。ディスジョイント パスの起点は、同じヘッドエンドまたは異なるヘッドエンドです。ディスジョイント レベルとは、2 つの計算されたパスで共有すべきではないリソースのタイプを指します。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。

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

の送信元から2つ目の宛先へのパス）が計算されます。両方のパスが同時に計算されます。セグメントの最短リストは、計算されたパス上のトラフィックを誘導するために計算されます。

（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を同時に設定することはできません。

セグメントルーティングパス計算要素（SR-PCE）

Crosswork ネットワークコントローラ 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 は、物理デバイスまたは仮想マシン内で実行されている仮想ルータのいずれかで実行されている Cisco ISO XR オペレーティングシステムによって提供されます。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トフル 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 ドメインのすべてのデバイスを検出します。ただし、TE トンネルをこれらのデバイスに展開するには PCEP ピアリングが必要です。

（注）
SR-PCE バージョンがサポートされていない場合、特定の機能が期待どおりに動作しない場合があります。互換性の問題を回避するには、SR-PCE バージョンのサポートと互換性について、『Crosswork Optimization Engine Release Notes 』を参照してください。

SR-PCE および HA の設定については、『*Cisco Crosswork Network Controller Administration Guide*』の「Prepare Infrastructure for Device Management: Manage Providers」の項を参照してください。

SR-TE ポリシー PCC および PCE 設定のソース

Crosswork 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。

- パス計算クライアント（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 （10 ページ）を参照）。このタイプは、UI に [不明（Unknown）] と表示されます。

- パス計算要素（PCE）によって開始：PCE 上に設定されたか、または Crosswork によって動的に作成されたポリシー。PCE によって開始されたポリシータイプの例：
  - **Dynamic**
  - **Explicit**
  - **オンデマンド帯域幅**（PCC または PCE のいずれか）
  - **ローカル輻輳の緩和**

（注） UI を使用して設定された SR ポリシーは、Crosswork 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。

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。お使いのデバイスの 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
       !
      !
     !
    !
   !
```

リソース予約プロトコル（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 ラベルスイッチパス（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するためにリンクリソースを管理します。
- 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、明示的ルートオブジェクト（ERO）で抽象ノードとして指定可能なネットワークトポロジ内の特別なパスです。これらのノードは、一連の IP プレフィックスまたは一連の自律システムである可能性があります。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多くあります。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 LPS を、それぞれのバックアップトンネルに切り替えます（バックアップトンネルがある場合）。

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。ヘッドエンドはこの情報を使用して、TE トンネルの新しい LSP をシグナリングし、メークビフォーブレー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。

RSVP-TE トンネル PCC および PCE 設定のソース

Crosswork 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。

- パス計算クライアント（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 （12 ページ）を参照）。
- パス計算要素（PCE）または PCC が動的に開始。

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、「*MPLS Command Reference for Cisco NCS 5500 Series, Cisco NCS 540 Series, and Cisco NCS 560 Series Routers*」）。

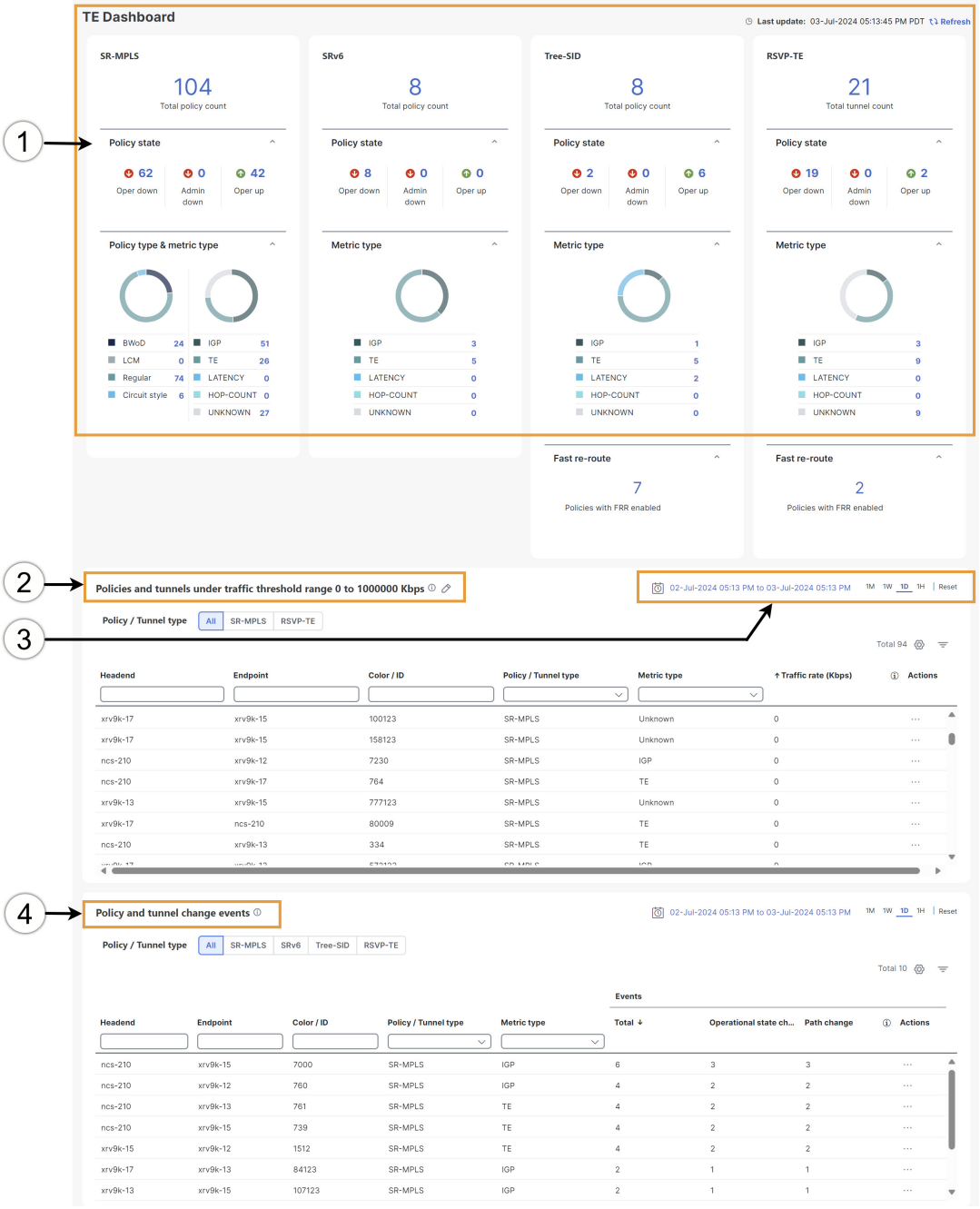
```
interface tunnel-te777
 ipv4 unnumbered Loopback0
 destination 192.168.0.8
 path-option 10 dynamic
 pce
  delegation
!
```

トラフィック エンジニアリング サービスのクイックビューを取得する

TE ダッシュボードにより、RSVP-TE トンネル、SR-MPLS、SRv6、および Tree-SID ポリシー情報の概要が提供されます。

TE ダッシュボードにアクセスするには、[トラフィックエンジニアリング（Traffic Engineering）] > [TEダッシュボード（TE Dashboard）] を選択します。

図 *1:* トラフィック エンジニアリング サービスのクイックビュー



（注） このガイドの HTML バージョンを表示している場合は、画像をクリックしてフルサイズで表示してください。

引き出し線番号	説明
1	**トラフィック エンジニアリング ダッシュレット**：ポリシーの状態に応じて、合計ポリシー数とポリシー数を表示します。 また、すべての TE ポリシーの数と、すべての TE サービスのメトリックタイプに応じたポリシーまたはトンネルの数も表示されます。 詳細情報をドリルダウンするには、値をクリックします。トポロジマップと TE テーブルが表示され、クリックしたフィルタリングされたデータのみが表示されます。
2	**トラフィックしきい値の下にあるポリシーとトンネル**： 選択した期間に定義されたしきい値を下回るトラフィックがある RSVP-TE トンネルおよびSR-MPLS ポリシーを表示します。この情報は、未使用のポリシーやトンネルを見つけてフィルタリングするために使用される場合があります。 をクリックして LSP しきい値の範囲を更新し、単位を Kbps から Mbps に変更します。 （注） SRv6 およびTree-SID ポリシーではトラフィック使用率はキャプチャされません。
3	表示する時間範囲（日付、1 ヵ月、1 週間、1 日、および 1 時間）に基づいて、ダッシュレット上のデータをフィルタリングできます。
4	**ポリシーおよびトンネル変更イベント**：選択した時間範囲内で、パスまたは状態変更イベントが発生したすべてのポリシーおよびトンネルをイベント数順に表示します。この情報は、不安定なポリシーとトンネルを特定するのに役立ちます。 （注） Tree-SID ポリシーのリーフノードの追加または削除は、イベントとしてキャプチャされます。

（注） 既知の制限事項のリストについては、『Cisco Crosswork Optimization Engine Release Notes』を参照してください。

TE イベントと使用率履歴の表示

履歴データは、ポリシーまたはトンネルのトラフィックレートと変更イベントをキャプチャします。履歴データを表示するには次の手順を実行します。

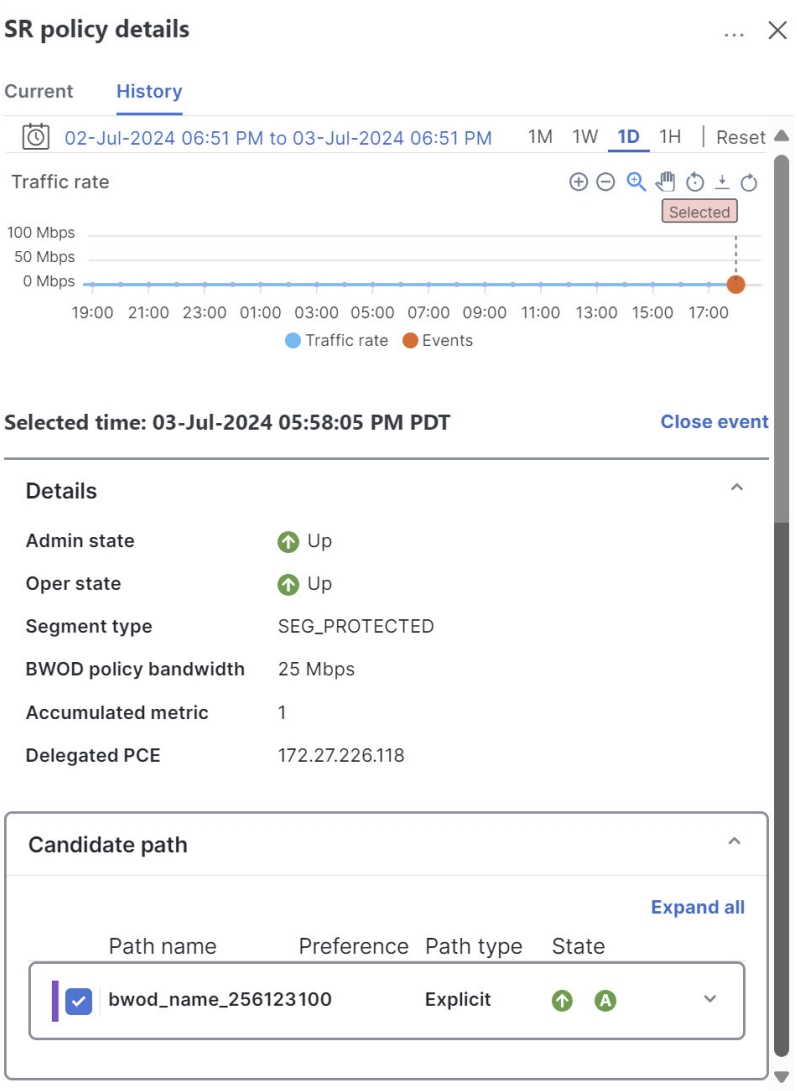
（注） SRv6 および Tree-SID ポリシーではトラフィックレートはキャプチャされません。

手順

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）] テーブルの [アクション（Actions）] 列で、ポリシーまたはトンネルの ··· > [詳細の表示（View Details）] > [履歴（History）] タブをクリックします。タブには、そのデバイスの関連する履歴データが表示されます。イベントをクリックすると、パスまたは状態変更イベントの情報が表示されます。

図 *2 : TE* イベントと使用率履歴



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。

手順

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。

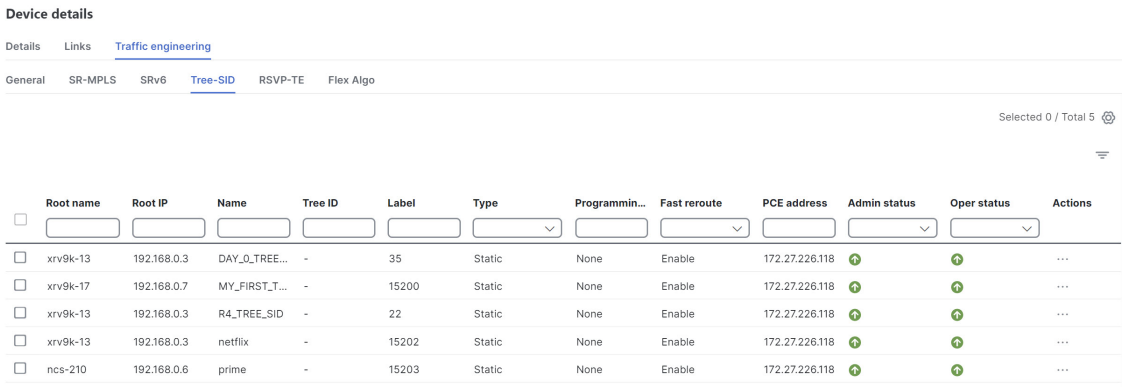
ステップ 2 トラフィック エンジニアリングのトポロジマップから、デバイスをクリックします。

ステップ 3 [トラフィックエンジニアリング（Traffic Engineering）]タブで、目的のポリシータイプをクリックします。各タブには、そのデバイスの関連データが表示されます。ブラウザから、URL をコピーして他のユーザーと共有できます。

次に、選択したデバイスの Tree-SID 情報の詳細を表示する例を示します。

（注）
このガイドの HTML バージョンを表示している場合は、画像をクリックしてフルサイズで表示してください。

図 *3:* トラフィック エンジニアリング デバイスの詳細



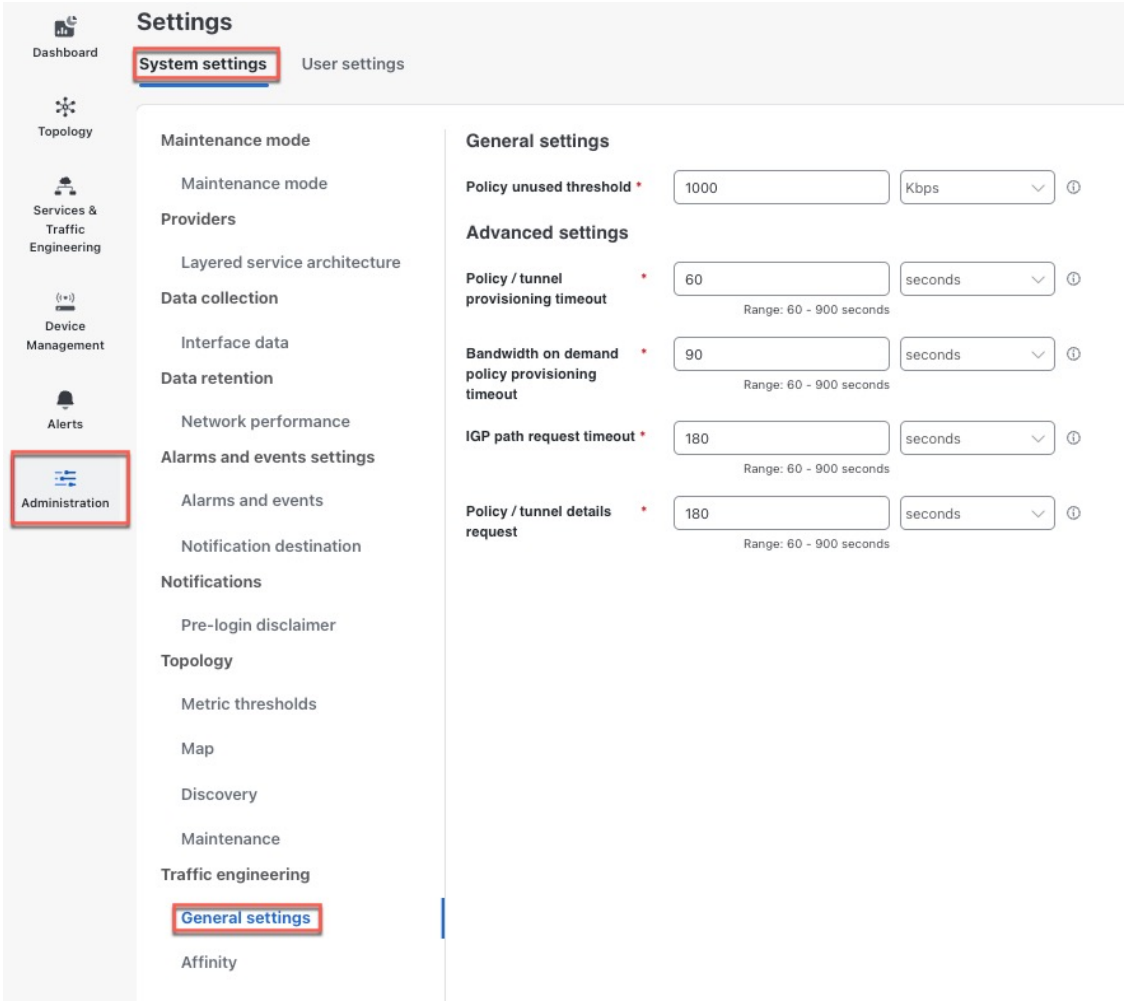
トラフィック エンジニアリング設定の構成

TE 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）]>[設定（Settings）]>[システム設定（System settings）] タブ>[トラフィックエンジニアリング（Traffic engineering）]>[全般設定（General settings）] 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。

図 *4:* トラフィック エンジニアリング タイムアウトの設定



トラフィックエンジニアリング用のデバイスグループの表示方法の構成

デバイスグループが選択されているものの、そのグループに選択したSRポリシー、サービス、またはRSVP-TEトンネル内のデバイスが属していない場合があります。こうした場合に、どのような情報をトポロジマップに表示するかを設定できます。動作を設定するには、[管理（Administration）] > [設定（Settings）] > [ユーザー設定（User settings）] タブ > [スイッチデバイスグループ（Switch device group）] を選択して、いずれかの動作オプションを選択します。

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。

TE データ保持設定の構成

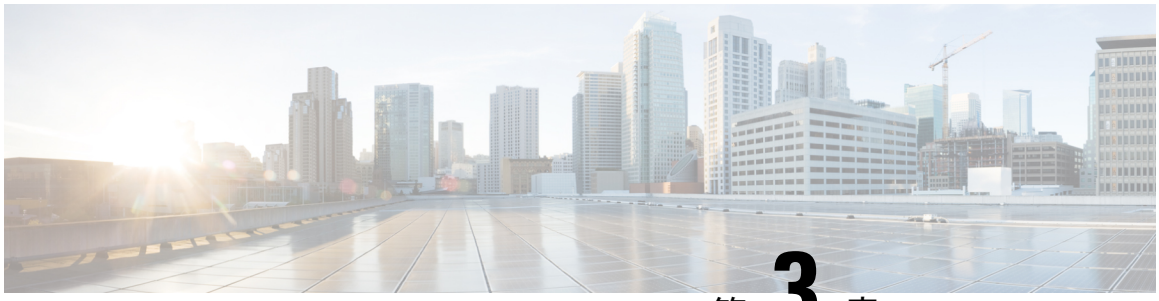
LSP 使用率の履歴ビュー（[履歴（Historical）] タブ）を表示するには、LSP 使用率の収集を有効にし、データを保持する期間を指定する必要があります。これを行うには、**[管理（Administration）] > [システム設定（System settings）] > [データ保持（Data retention）] > [ネットワークパフォーマンス（Network performance）]**の順にクリックし、[LSP使用率（LSP utilization）] チェックボックスをオンにします。必要に応じて、デフォルトのデータ保持期間を編集できます。

（注） 保持期間を短くすると、新しい保持期間より古いデータはすべて失われます。たとえば、毎日の保持間隔が 31 日に設定されていて、その後 7 日に短縮された場合、7 日より古いデータはすべて削除されます。

SR-TE ポリシーと RSVP-TE トンネルの解決

孤立した TE ポリシーとは、PCE で開始された SR-TE ポリシー（SRv6、SR-MPLS、および Tree-SID）または Crosswork 内で最後のクラスタデータ同期後に作成された RSVP-TE トンネルです。高可用性セットアップでのスイッチオーバー後、Crosswork は孤立した TE ポリシーがあるかどうかを自動的にチェックします。孤立したポリシー/トンネルは、バックアップ/復元操作の後にも発生する可能性があります。ポリシーの詳細は表示できますが、最後のデータ同期に含まれていないため、変更することはできません。Crosswork は、孤立した TE ポリシーを検出するとアラームを表示します（[アラート（Alerts）]>[アラームおよびイベント（Alarms and Events）]）。

Crosswork には、これらの孤立をクリアするための API が用意されています。孤立した SR-TE ポリシーまたは RSVP-TE トンネルのリストを取得するには、**cisco-crosswork-optimization-engine-sr-policy-operations:sr-datalist-oper** または **cisco-crosswork-optimization-engine-rsvp-te-tunnel-operations:rsvp-te-datalist-oper** を使用します。ここで、**is-orphan=True**で、デフォルトのアクションはGET です。孤立を再び管理可能にするには、ポリシータイプごとに対応する URL に対して SAVE アクションを使用します。詳細については、 Devnet の API ドキュメント （**「Crosswork Optimization Engine APIs」 > 「<リリース ID> Release APIs**」）を参照してください。



第 3 章

SR-MPLS および SRv6

このセクションでは、Crosswork がサポートする SR-MPLS および SRv6 ポリシー機能について説明します。既知の制限事項と重要な注意事項のリストについては、『Cisco Crosswork Optimization Engine Release Notes』を参照してください。

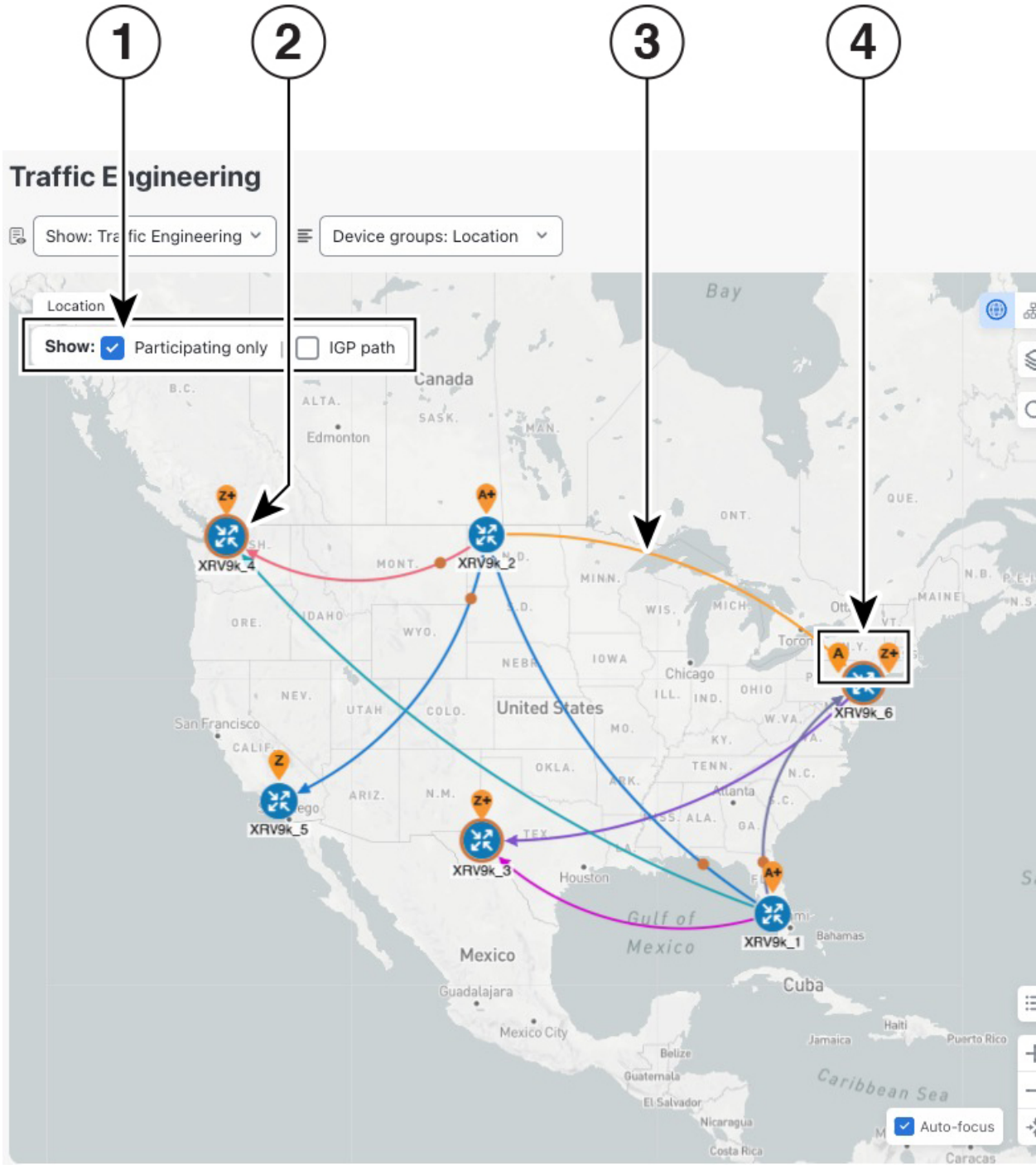
- トポロジマップでの SR-MPLS および SRv6 ポリシーの表示 （21 ページ）
- SR-MPLS および SRv6 ポリシーの詳細の表示 （24 ページ）
- IGP パスとメトリックの視覚化 （26 ページ）
- 複数の候補パス（MCP）の検索 （27 ページ）
- 定義済みのバインディングセグメント ID（B-SID）ラベルに関連付けられた基盤となるパスの可視化 （30 ページ）
- ネイティブ SR パスの可視化 （33 ページ）
- TE リンクアフィニティの設定 （36 ページ）
- 明示的 SR-MPLS ポリシーの作成 （38 ページ）
- 最適化インテントベースのダイナミック SR-MPLS ポリシーの作成 （39 ページ）
- SR-MPLS ポリシーの変更 （41 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

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）]**を選択します。

[トラフィックエンジニアリング（Traffic Engineering）] テーブルから、マップに表示する各 SR-MPLS または SRv6 ポリシーのチェックボックスをクリックします。個別の色付きリンクとして表示される最大 10 個のポリシーを選択できます。

図 *5*: 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



引き出し線番号	説明
1	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。 • [表示：IGPパス（Show: IGP path）]：選択した SR-TE ポリシーの IGP パスを表示します。 • [表示：参加デバイスのみ（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。
2	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。
3	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色付きの矢印線としてマップに表示されます。 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。
4	[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。
5	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。
6	[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。
7	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。
8	[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。

引き出し線番号	説明
9	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： • [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。 • [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。 • [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。 • [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。

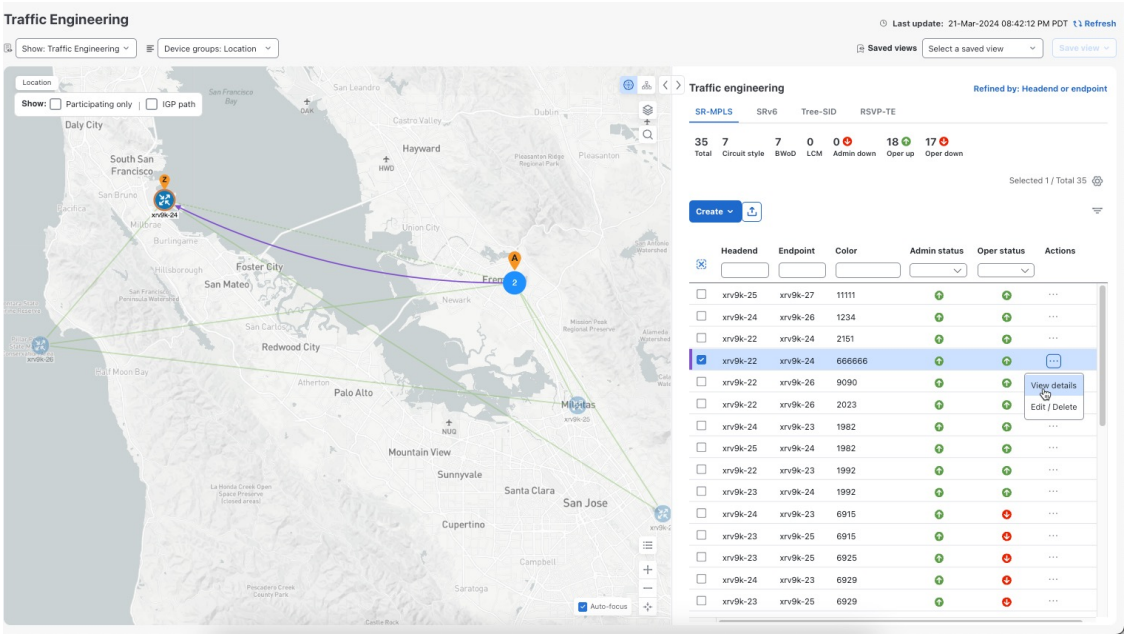
SR-MPLS および SRv6 ポリシーの詳細の表示

SR-MPLS または SRv6 TE ポリシーレベルの詳細、セグメントリスト、および候補パスごとに設定されたパス計算の制約を表示します。

手順

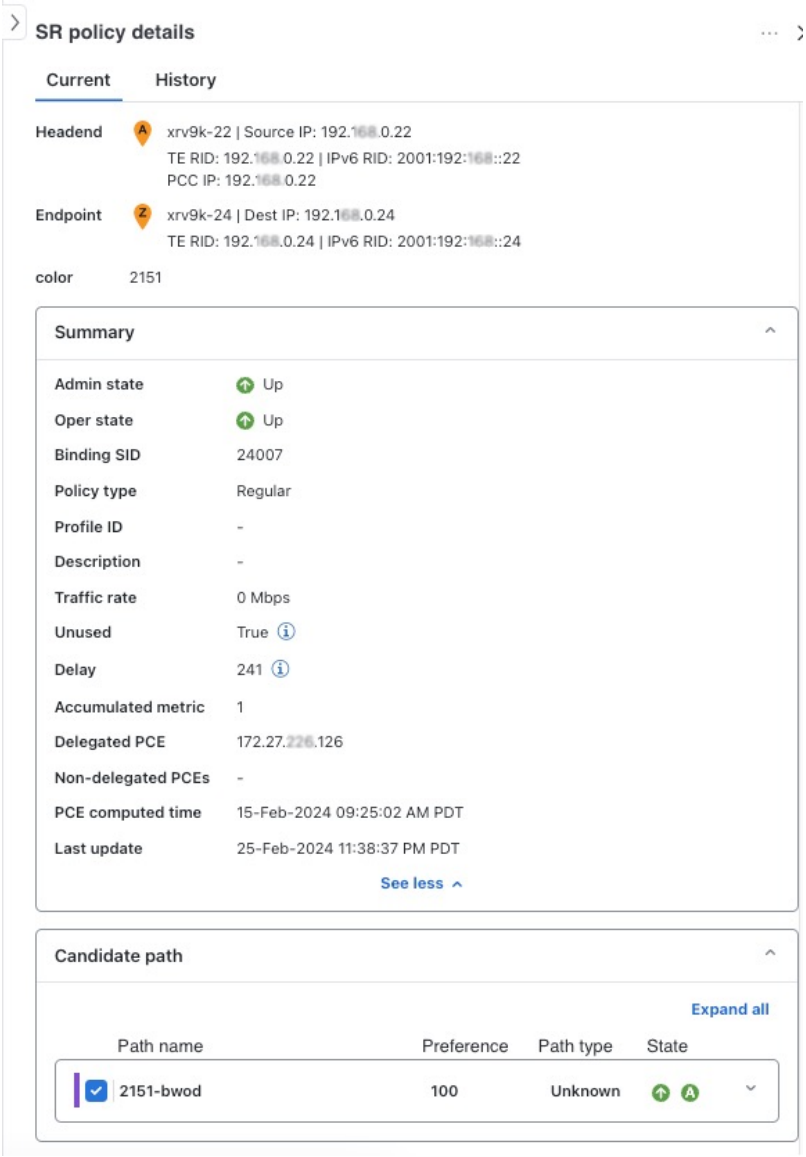
ステップ 1 [アクション（Actions）] 列で、いずれかの SR-MPLS または SRv6 ポリシーに対して … > [詳細の表示（View details）] をクリックします。

図 *6 : SR* ポリシーの詳細の表示



ステップ 2 SR-MPLS または SRv6 ポリシーの詳細を表示します。ブラウザから、URL をコピーして他のユーザーと共有できます。

図 *7: SR* ポリシーの詳細：ヘッドエンド、エンドポイント、およびサマリー



（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。

IGP パスとメトリックの視覚化

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。

手順

ステップ 1 [SRポリシー（SR Policy）]テーブルで、目的の SR-TE（SR-MPLS および SRv6）ポリシーの横にあるチェックボックスをオンにします。

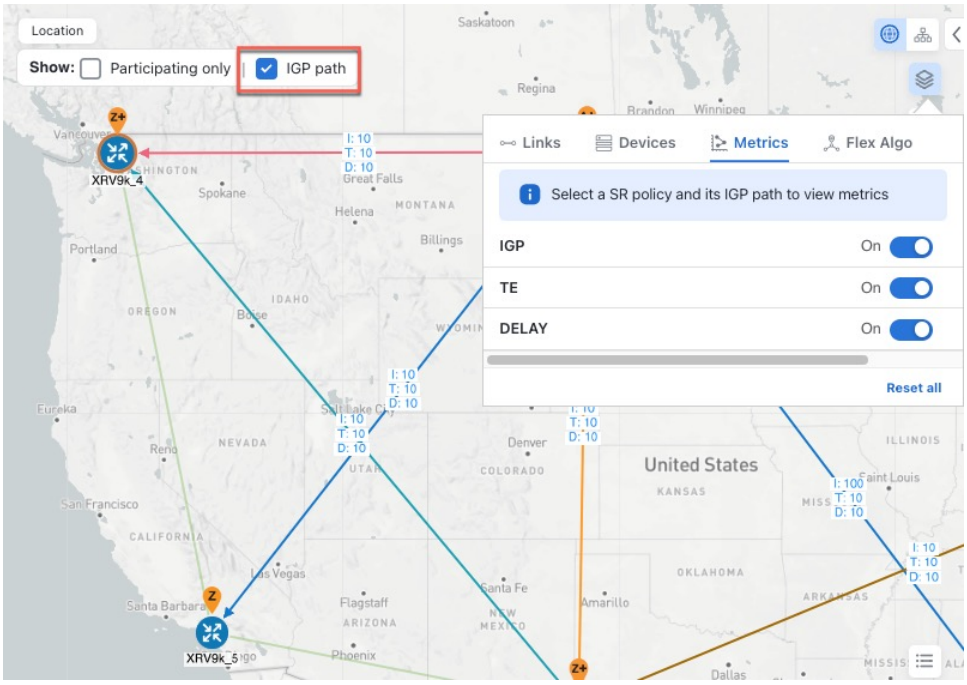
ステップ 2 [Show IGP Path] チェックボックスをオンにします。選択した SR-MPLS ポリシーの IGP パスが、セグメントホップの代わりに直線として表示されます。デュアルスタックトポロジでは、参加リンクのメトリックを表示するには、[参加のみ（Participating only）] チェックボックスもオンにする必要があります。

ステップ 3 > [メトリック（Metrics）] タブをクリックします。

ステップ 4 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、[IGPパスを表示（Show IGP Path）] チェックボックスをオンにする必要があります。

図 8 : 物理パスとメトリックの表示



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 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 内で行うことができます。

手順

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] タブの順に選択します。

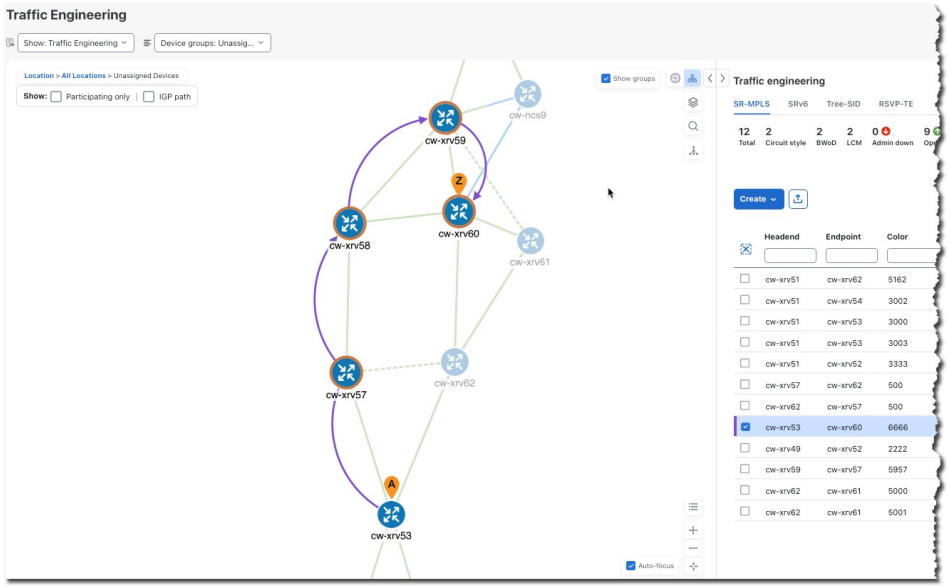
ステップ 2 MCP が設定されているアクティブな SR-TE ポリシーに移動し、トポロジマップで表示します。

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、アクティブパスが [cw-xrv53] > [cw-xrv57] > [cw-xrv58] > [cw-xrv59] > [cw-xrv60] の順に移動していることがわかります。

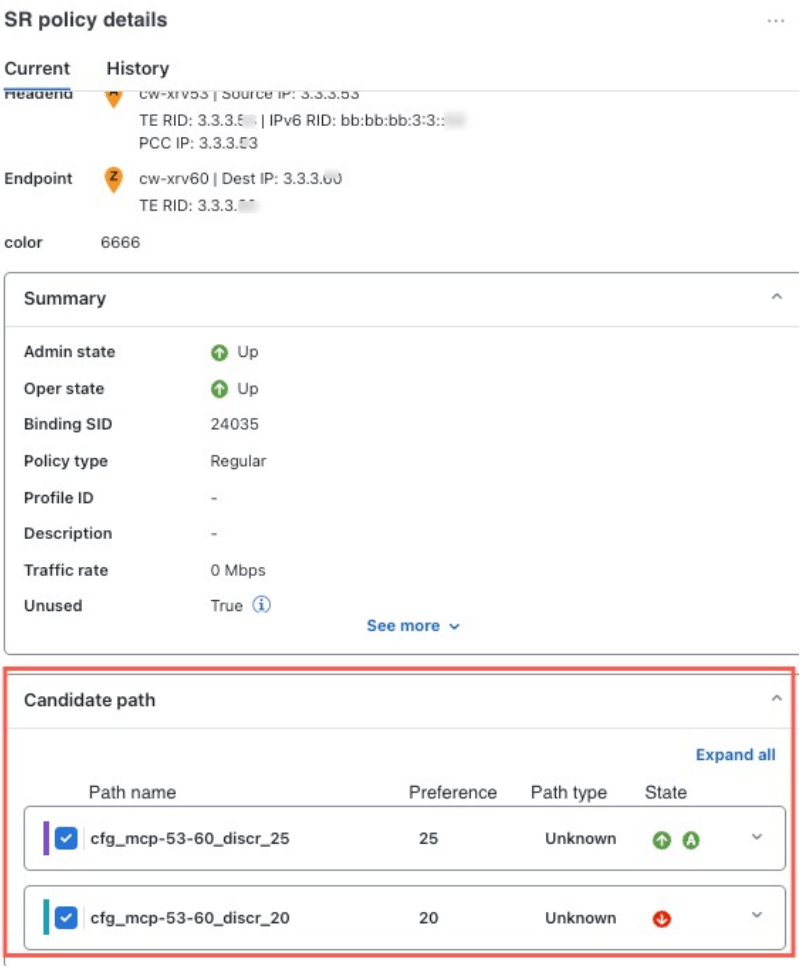
図 *9*: トポロジマップの *SR-TE* ポリシー



ステップ 3 候補パスのリストを表示します。

a) [SR-MPLS] または [SRv6ポリシー（SRv6 Policy）] テーブルの [アクション（Actions）] 列で、･･･ > **[詳細の表示（View details）]** をクリックします。[SRポリシーの詳細（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。[状態（State）] 列の緑の A は、アクティブパスを示します。

図 *10 : SR* ポリシーの詳細の候補パス



ステップ 4 個々のパスを展開するか、[すべて展開する（Expand all）] をクリックして各パスの詳細を表示できます。

ステップ 5 トポロジマップで候補パスを可視化します。

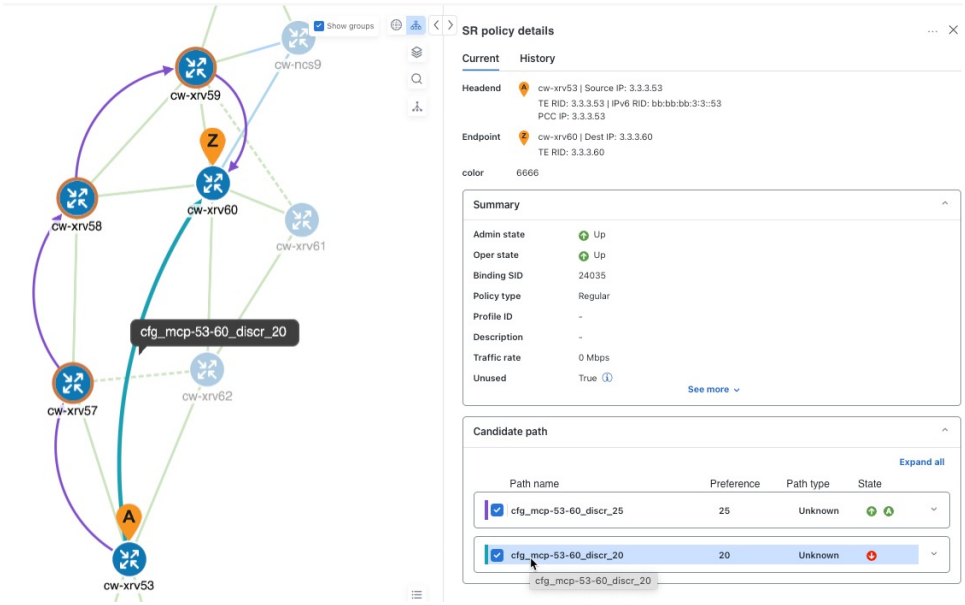
a) 候補パスの横にあるチェックボックスをオンにします。

（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。

b) [候補パス（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 [cw-xrv53] から [cw-xrv60] に直接移動していることがわかります。

図 *11* : トポロジマップ上の候補パス



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 ネットワークコントローラ 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 [15700] を割り当てています。

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。

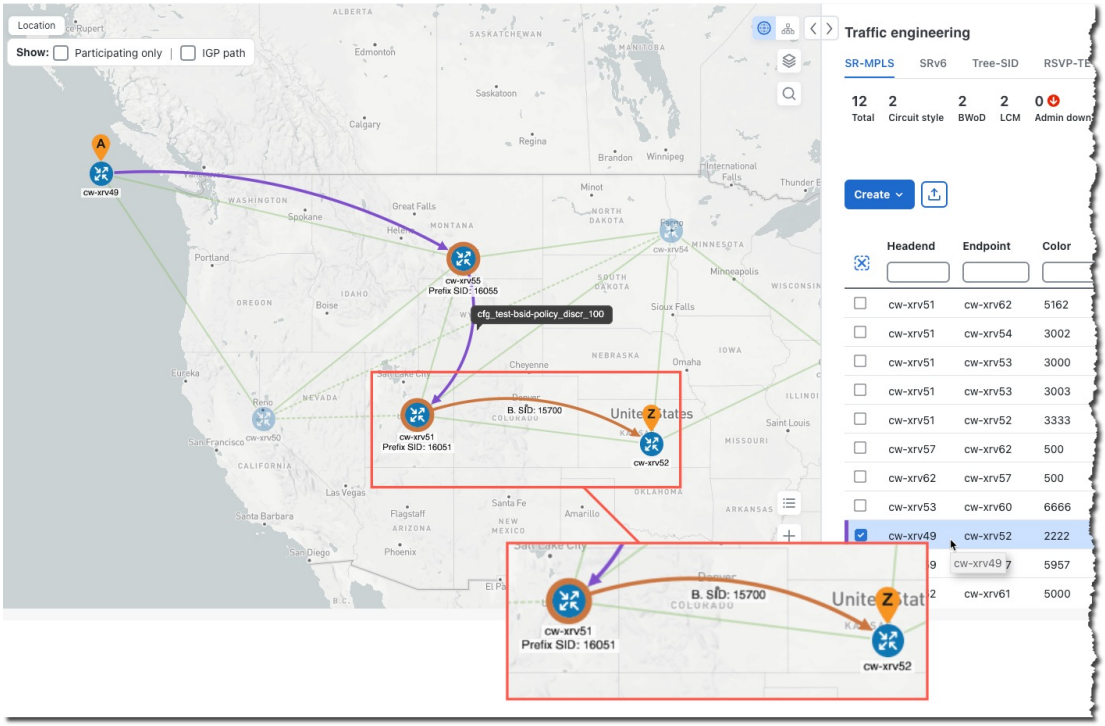
手順

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]**の順に選択します。

ステップ 2 [SRポリシー（SR Policy）] テーブルで、B-SID ラベルが割り当てられたホップを持つポリシーの横にあるチェックボックスをオンにします。SR-MPLS 行の任意の部分にマウスを合わせると、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。

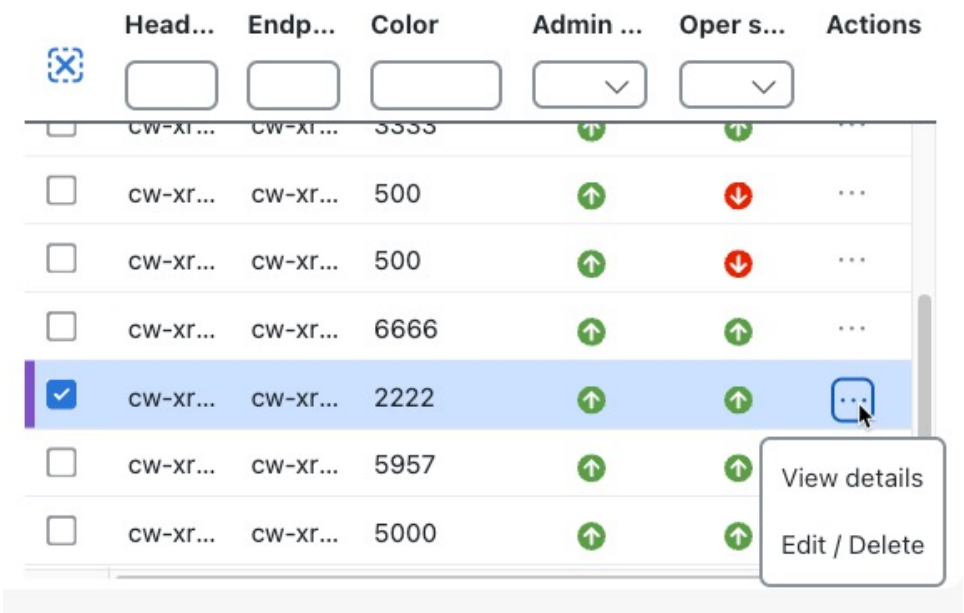
この例では、B-SID パスが [cw-xrv51] から [cw-xrv52] に移動していることがわかります。

図 *12 : B-SID* ラベル



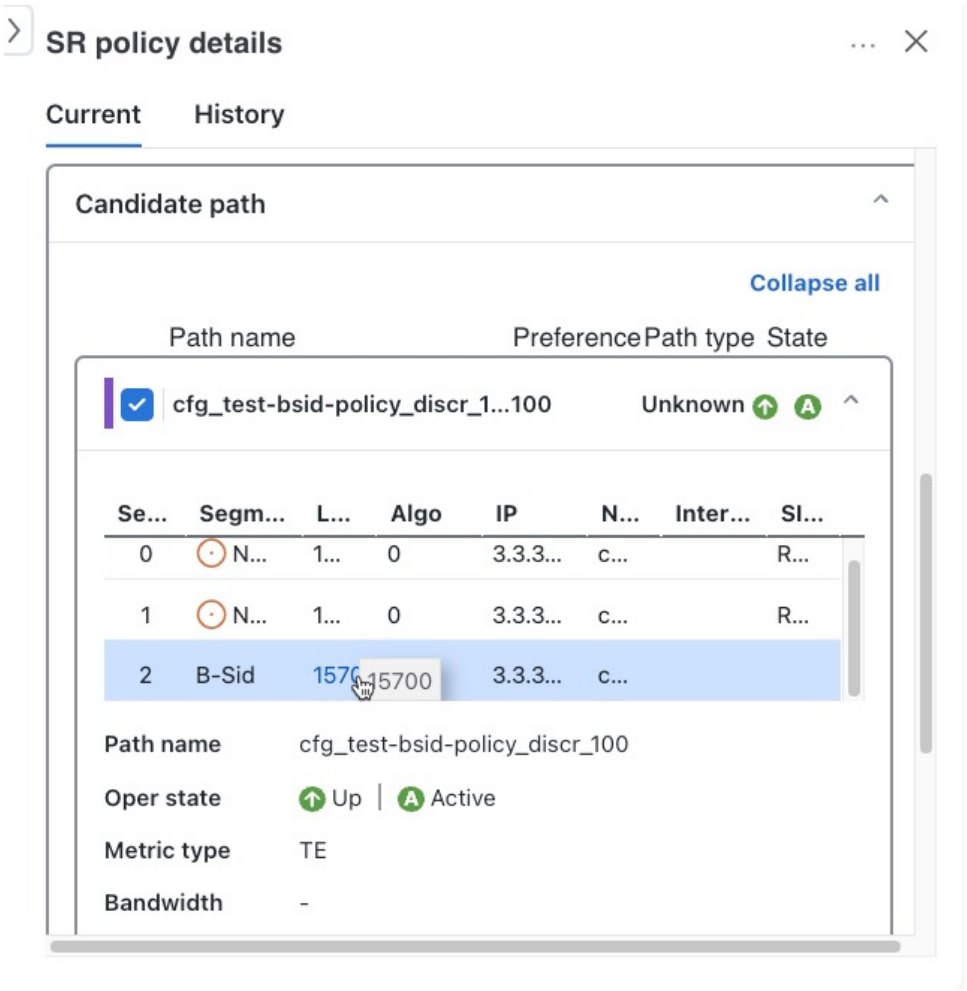
ステップ 3 [SRポリシーの詳細（SR policy details）] ウィンドウで、… > **[詳細の表示（View details）]**をクリックします。

図 *13 : [*詳細の表示（*View Details*）*]*



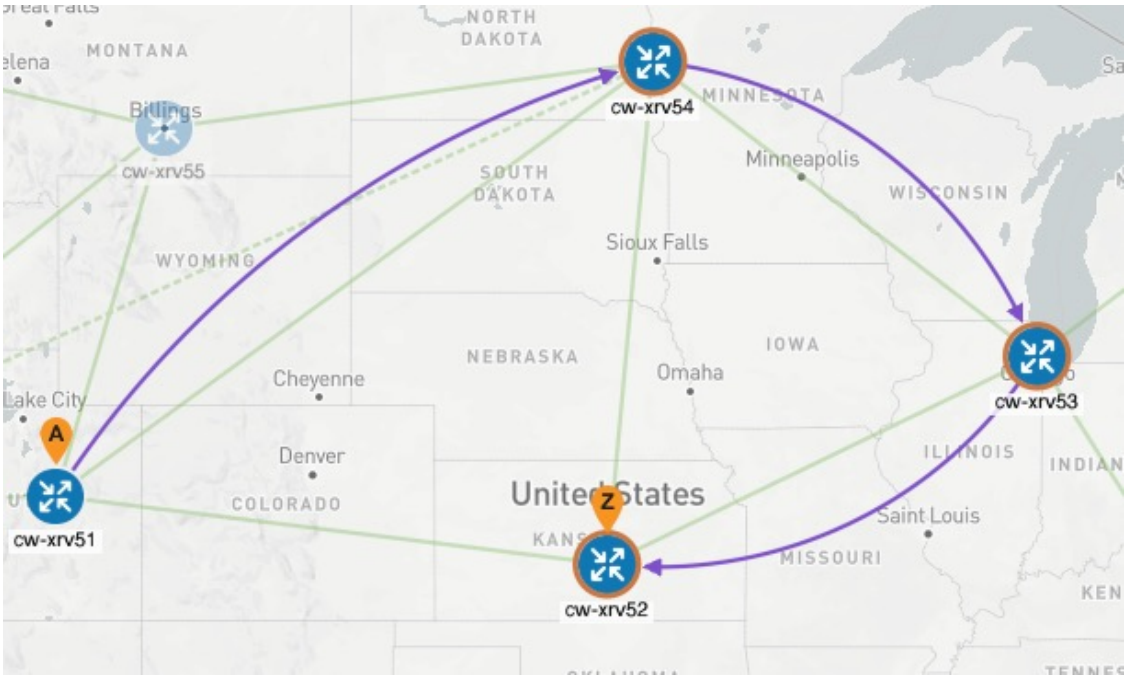
ステップ 4 アクティブパスを展開し、B-SID ラベル ID をクリックして、基礎となるパスを表示します。

図 *14 : B-SID* ラベル *ID*



この例では、基礎となるパスが実際に **[cw-xrv51]** > **[cw-xrv54]** > **[cw-xrv53]** > **[cw-xrv52]** と移動しています。

図 *15 : B-SID* パス



ネイティブ SR パスの可視化

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。この機能ではマルチパスが使用されるため、すべての ECMP パスは送信元と接続先の間に表示されます。ネイティブ SR IGP パスのみを可視化できます。

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 （35 ページ）」を参照してください。

パスクエリを作成するには、次の手順を実行します。

手順

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。を選択します。パスクエリのダッシュボードが表示されます。

ステップ 2 **[新規クエリ（New query）]**をクリックします。

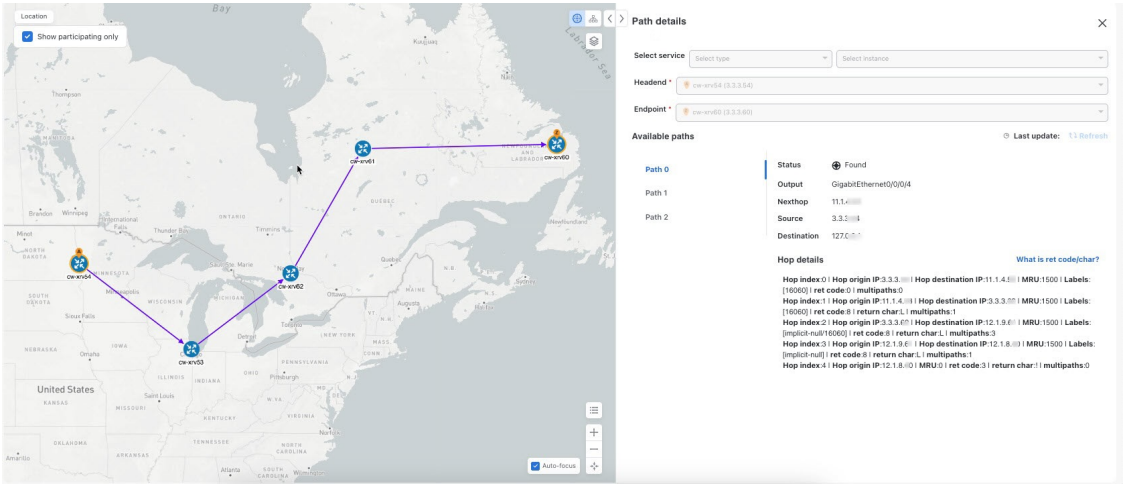
ステップ 3 必要なフィールドにデバイス情報を入力して、使用可能なネイティブ SR IGP パスを検索し、[パスの取得（Get paths）] をクリックします。

（注）
パスクエリが完了するまで時間がかかる場合があります。[実行中のクエリID（Running Query ID）] ポップアップが表示されたら、[過去のクエリを表示（View past queries）] を選択して、パスクエリダッシュボードに戻ることもできます。リストにすでにパスクエリが含まれている場合は、新しいクエリがバックグラウンドで実行され続けている間に既存のクエリの詳細を確認できます。これは、[Query State] 列の青色の実行アイコンで示されます。新しいクエリの状態が緑色に変わり、完了すると、そのクエリを確認できます。

図 *16*：新しいパスクエリ

ステップ 4 **[結果の表示（View results）]**が [実行中のクエリID（Running Query ID）] ポップアップで使用可能になったらクリックします。[パスの詳細（Path Details）] ウィンドウが表示され、対応する使用可能なパスの詳細が表示されます。左側には、使用可能なネイティブ SR IGP パスがトポロジマップに表示されます。

図 *17*：パスの詳細



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 以上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。

```
tpa
vrf default
address-family ipv4
default-route mgmt
!
address-family ipv6
default-route mgmt
!
!
!

or

linux networking
vrf default
address-family ipv4
default-route software-forwarding
!
address-family ipv6
default-route software-forwarding
!
!
!
```

（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. [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] で、目的のデバイスの IP アドレスをクリックします。
    2. [接続の詳細（Connectivity details）] の下に GNMI が一覧表示されていることを確認します。

（注） デバイスのタイプに基づいて、次のデバイスのエンコーディングタイプを使用できます。

- JSON
- BYTES
- PROTO
- ASCII
- JSON IETF

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-7.3.2#config

RP/0/RP0/CPU0:xrvr-7.3.2(config)#router static

RP/0/RP0/CPU0:xrvr-7.3.2(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-7.3.2(config-static)#commit
```

TE リンクアフィニティの設定

SR ポリシー、Tree-SID、または RSVP-TE トンネルをプロビジョニングするときに考慮したいアフィニティがある場合は、必要に応じて、デバイス設定のアフィニティ名との一貫性を保つために、Cisco Crosswork UI でアフィニティマッピングを定義できます。Cisco Crosswork は、プロビジョニング中にビット情報のみをSR-PCEに送信します。アフィニティマッピングがUIで定義されていない場合、アフィニティ名は「UNKNOWN」と表示されます。可視化のために Cisco Crosswork でアフィニティマッピングを設定する場合は、デバイスでアフィニティを収集し、デバ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 Cisco Crosswork UI でアフィニティマッピングを定義する必要があります。

インターフェイスのアフィニティ構成は、単にいくつかのビットをオンにします。これは 32 ビット値で、各ビット位置（0ー31）はリンク属性を表します。アフィニティマッピングは、特定のタイプのサービスプロファイルを表す色にすることができます（たとえば、低遅延、高帯域幅など）。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、Tree-SID、または RSVP-TE 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）。

次の例は、デバイスのアフィニティ構成（`affinity-map`）を示しています。

```
RP/0/RP0/CPU0:c12#sh running-config segment-routing traffic-eng affinity-map
Wed Jul 27 12:14:50.027 PDT
segment-routing
 traffic-eng
```

```
  affinity-map
   name red bit-position 1
   name blue bit-position 5
   name green bit-position 4
  !
 !
!
```

手順

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System settings）] タブ > [トラフィックエンジニアリング（Traffic engineering）] > [アフィニティ（Affinity）] > [TEリンクアフィニティ（TE link affinities）]**を選択します。[制約（Constraints）]>[アフィニティ（Affinity）] フィールドの [マッピングの管理（Manage Mapping）] をクリックして、SR-TE ポリシー、Tree-SID 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 割り当てる名前とビットを入力します。例（上記の構成を使用）：

図 *18 :* アフィニティのマッピング

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。別のマッピングを作成するには、[+作成（+ Create）] をクリックしてエントリを保存する必要があります。

（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。

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。

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明示的なSR-MPLSポリシーを作成します。詳細については、TEリンクアフィニティの設定 （36 ページ）を参照してください。

手順

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] タブを選択します。

ステップ 2　[+作成（+ Create）] をクリックします。

ステップ 3　[ポリシーの詳細（Policy details）] の下で、必要な SR-MPLS ポリシー値を入力または選択します。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）] ドロップダウンリスト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）] をクリックして、作成したポリシーが意図と一致していることを確認します。

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）] をクリックしてネットワーク上でポリシーをアクティブにするか、終了して設定プロセスを中止します。

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 [トラフィックエンジニアリング（Traffic engineering）] 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。[トラフィックエンジニアリング（Traffic engineering）] 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。[トラフィックエンジニアリング（Traffic engineering）] テーブルで、… をクリックし、[詳細表示（View details）] 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、TE タイムアウトの設定（18 ページ）を参照してください。

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アラームを起動します。パスが見つからない場合は、アラームを起動し、パケットがドロップされます。

ヒント　視覚化のために、必要に応じて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 ポリシーを作成することもできます。詳細については、TE リンクアフィニティの設定（36 ページ）またはフレキシブルアルゴリズムのアフィニティの設定（53 ページ）を参照してください。

手順

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]**タブの順に選択します。

ステップ 2　[+作成（+ Create）] をクリックします。

ステップ 3　[ポリシーの詳細（Policy details）] の下で、必要な SR-MPLS ポリシー値を入力または選択します。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、使用可能な場合に保護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 該当する場合は、[SIDアルゴリズム（SID Algorithm）] フィールドに SID の制約を入力します。Cisco Crosswork は、この SID を持つパスを見つけようとします。SID の制約のあるパスが見つからない場合、プロビジョニングされたポリシーは、条件が満たされるまで運用停止状態のままになります。

（注）
- フレキシブルアルゴリズム：値はデバイスで定義されているフレキシブルアルゴリズムに対応し、128 ～ 255 の範囲が Cisco IOS XR によって適用されます。
- アルゴリズム 0：これは、リンク メトリックに基づく最短パス優先（SPF）アルゴリズムです。この最短パス アルゴリズムは、内部ゲートウェイ プロトコル（IGP）によって計算されます。
- アルゴリズム 1：これは、リンク メトリックに基づく厳格な最短パス優先（SSPF）アルゴリズムです。アルゴリズム 1 はアルゴリズム 0 と同じですが、パスに沿ったすべてのノードが SPF ルーティングの決定を遵守することを必要とします。ローカル ポリシーは、転送の決定を変更しません。たとえば、パケットはローカルに設計されたパスを通じて転送されません。

ステップ 9 [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 10 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 11 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-MPLS ポリシーは、ネットワークのサイズやパフォーマンスによっては、[トラフィックエンジニアリング（Traffic engineering）] 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。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。[トラフィックエンジニアリング（Traffic engineering）] テーブルで、… をクリックし、[詳細表示（View details）] 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、TE タイムアウトの設定 （18 ページ）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。

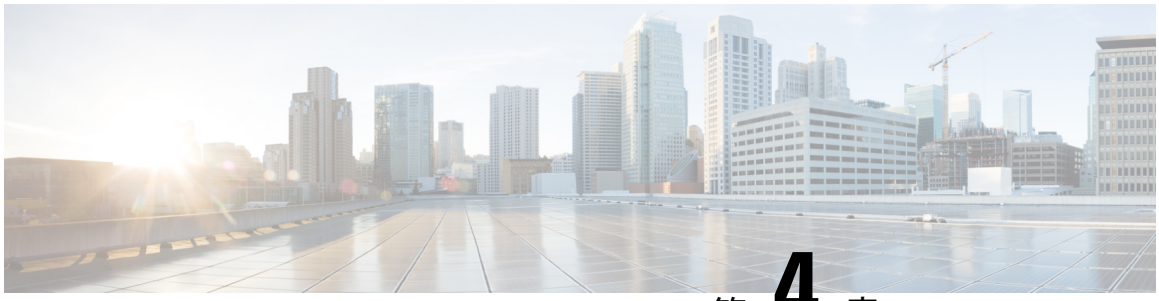
手順

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]**タブの順に選択します。

ステップ 2 [トラフィックエンジニアリング（Traffic engineering）] 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 [詳細表示（View details）] 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 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 4 章

リソース予約プロトコル（RSVP）

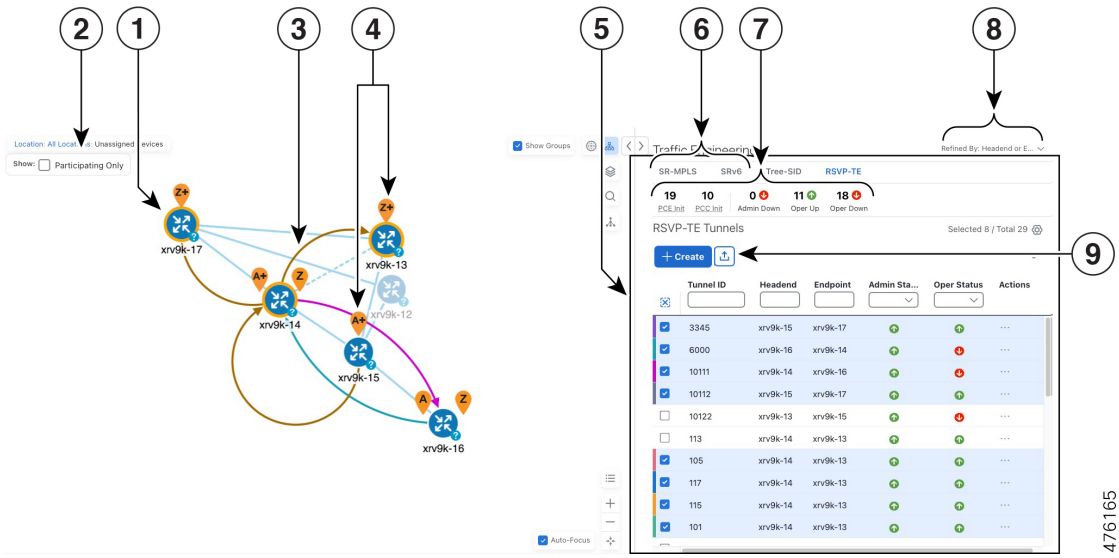
このセクションでは、Crosswork Optimization Engine がサポートする RSVP-TE トンネル機能について説明します。既知の制限事項と重要な注意事項のリストについては、『Cisco Crosswork Optimization Engine Release Notes』を参照してください。

- トポロジマップでの RSVP-TE トンネルの表示 （43 ページ）
- RSVP-TE トンネルの詳細の表示 （46 ページ）
- 明示的 RSVP-TE トンネルの作成 （49 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 （50 ページ）
- RSVP-TE トンネルの変更 （51 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]** タブを選択します。

図 *19 :* トラフィック エンジニアリング *UI* : *RSVP-TE* トンネル



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	RSVP-TE トンネルは [RSVP-TEトンネル（RSVP-TE Tunnels）] テーブルで選択されると、送信元と宛先を示す色付きの矢印線としてマップに表示されます。 • レコードルートオブジェクト（RRO）パスは直線で表示されます。 • 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。 （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。 • 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。 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。
4	[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。
5	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。 • 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 （50 ページ） • 明示的 RSVP-TE トンネルの作成 （49 ページ） • RSVP-TE トンネルの変更 （51 ページ） • RSVP-TE トンネルの詳細の表示 （46 ページ）
6	[RSVP-TE] タブをクリックします。
7	[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。

引き出し線番号	説明
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： • [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。 • [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。 • [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。 • [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。
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。

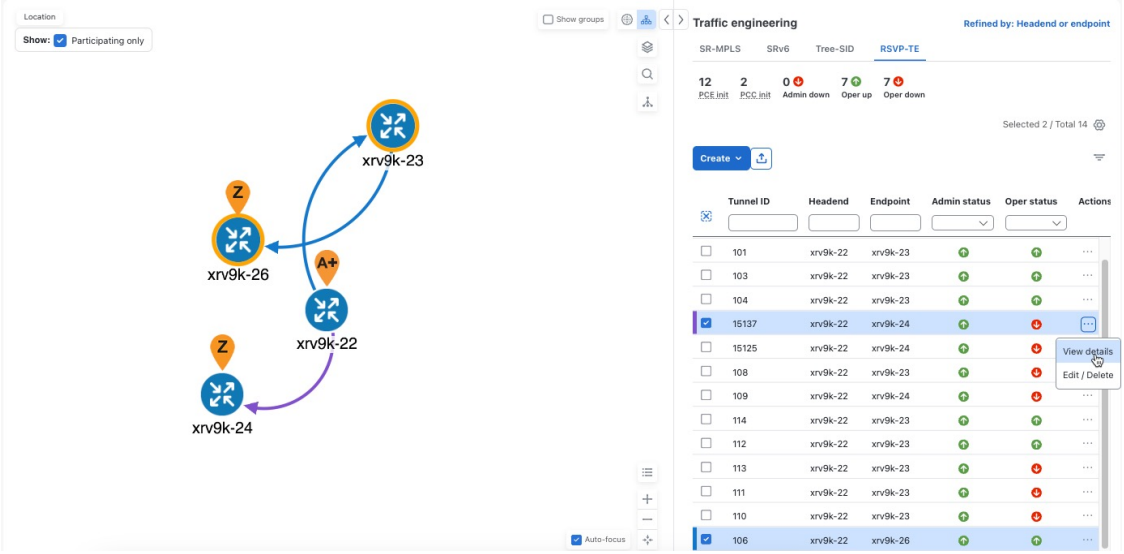
RSVP-TE トンネルの詳細の表示

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。

手順

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。

図 *20 : [RSVP-TE] > [*詳細の表示（*View details*）*]*



ステップ 2 RSVP-TE トンネルの詳細を表示します。ブラウザから、URL をコピーして他のユーザーと共有できます。

（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）。
- 該当する場合は、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] アイコンをクリックすると、値が最後に更新された時刻が表示されます。

図 *21 : RSVP-TE* トンネルの詳細

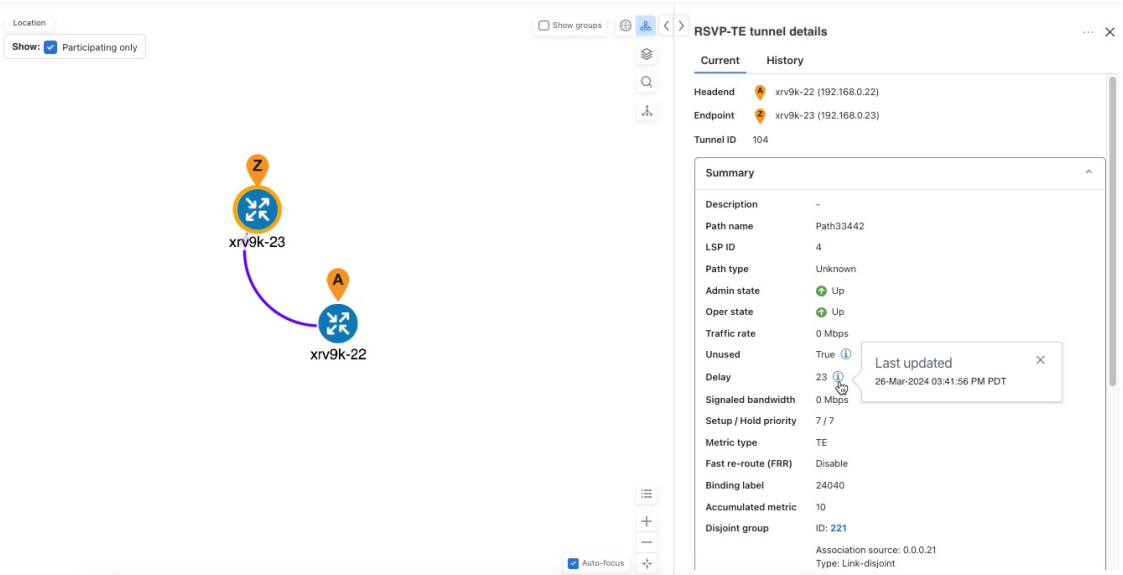


図 ***22 : RSVP-TE*** トンネルの詳細（クローズアップ）

明示的 RSVP-TE トンネルの作成

このタスクでは、プレフィックスのリストまたは隣接セグメント ID のリスト（SID リスト）で構成される明示的な（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に沿ったノードまたはリンクを表します。

手順

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）]**> [RSVP-TE] タブを選択します。

ステップ 2 [+作成（+ Create）] をクリックします。

ステップ 3 [トンネルの詳細（Tunnel details）] で、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：ロケーション（Device groups: Location）] 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 [トンネルパス（Tunnel 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 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 6 [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 7 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 8 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、[トラフィックエンジニアリング（Traffic engineering）]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。[トラフィックエンジニアリング（Traffic engineering）] 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。[トラフィックエンジニアリング（Traffic engineering）] テーブルで、⋯（RSVP-TE トンネルと同じ行にある）をクリックし、[詳細表示（View details）] 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。

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

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、TE リンクアフィニティの設定 （36 ページ）を参照してください。

手順

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）]**> [RSVP-TE] タブを選択します。

ステップ 2　[+作成（+ Create）] をクリックします。

ステップ 3　[トンネルの詳細（Tunnel details）] で、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：ロケーション（Device groups: Location）] 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　[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 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 RSVP-TE トンネルに設定できません。また、最大 2 つの 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ができます。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 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、[トラフィックエンジニアリング（Traffic engineering）]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。[トラフィックエンジニアリング（Traffic engineering）] 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。[トラフィックエンジニアリング（Traffic engineering）] テーブルで、… をクリックし、[詳細表示（View details）] 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。

手順

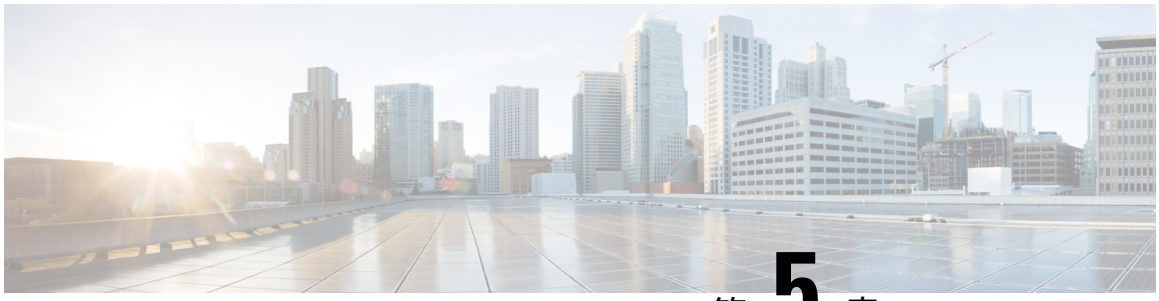
ステップ 1 メインメニューから、**[トラフィックエンジニアリング（Traffic Engineering）]**>**[トラフィックエンジニアリング（Traffic Engineering）]**> [RSVP-TE] タブを選択します。

ステップ 2 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 3 [詳細表示（View details）] または [編集/削除（Edit / Delete）] を選択します。

（注）
- UI または API 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 5 章

フレキシブルアルゴリズム

フレキシブルアルゴリズムを使用すると、オペレータは、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 トポロジの可視化は、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に重要なツールです。たとえば、フレキシブルアルゴリズムを使用して、サービスの可用性を向上させ、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。

ここでは、次の内容について説明します。

- フレキシブルアルゴリズムのアフィニティの設定 （53 ページ）
- フレキシブル アルゴリズム トポロジの可視化 （54 ページ）
- フレキシブルアルゴリズムの詳細の表示 （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

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によって収集されません。必要に応じて、デバイス設定のフレキシブルアルゴリズムのアフィニティ名との一貫性を保つために、Cisco Crosswork UIでアフィニティマッピングを定義することができます。Cisco Crossworkは、プロビジョニング中にビット情報のみをSR-PCEに送信します。アフィニティマッピングがUIで定義されていない場合、アフィニティ名は「UNKNOWN」と表示されます。可視化のためにCisco Crossworkでアフィニティマッピングを設定する場合は、デバイ

スでアフィニティを収集し、デバ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 Cisco Crosswork UI でアフィニティマッピングを定義する必要があります。

お使いのデバイスの 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）

次の例は、デバイスのフレキシブルアルゴリズムのアフィニティ設定（`affinity-map`）を示しています。

```
router isis CORE
 is-type level-2-only
 net 49.0001.0000.0000.0002.00
 log adjacency changes
 affinity-map b33 bit-position 33
 affinity-map red bit-position 1
 affinity-map blue bit-position 5
 flex-algo 128
  priority 228
  advertise-definition
  affinity exclude-any blue indigo violet black
 !
```

可視化のために、次の手順を使用して、アフィニティ名をビットにマップする必要があります。

手順

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [トラフィックエンジニアリング（Traffic Engineering）] > [アフィニティ（Affinity）] > [Flex-Algoアフィニティ（Flex-Algo Affinities）]**タブを選択します。

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。リンクのすべてのフレキシブル アルゴリズム アフィニティを表示するには、フレキシブルアルゴリズムの詳細の表示 （56ページ）を参照してください。

フレキシブル アルゴリズム トポロジの可視化

Crossworkを使用すると、ネットワーク内でUIを使用して手動で設定または動的にプロビジョニングされたトポロジマップ上の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。

（注） SR-MPLS ポリシーを動的にプロビジョニングするときにフレキシブルアルゴリズムの制約を適用するには、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 （39 ページ）を参照してください。

始める前に

ネットワークのフレキシブルアルゴリズムについて理解し、設定する必要があります。お使いのデバイスの SR フレキシブルアルゴリズムの設定について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 NCS 540 Series Routers』など）。

（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。

手順

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。

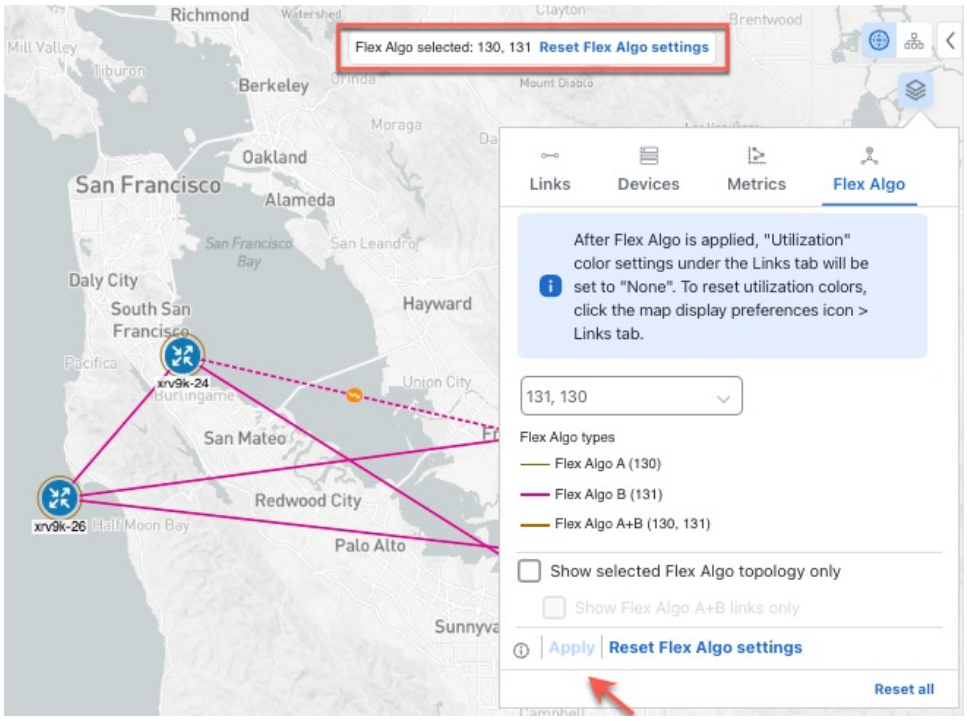
ステップ 5 [Flexible Algorithm Types] を表示し、選択内容が正しいことを確認します。各フレキシブルアルゴリズムの色の割り当てにも注意してください。

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を表示するには、[Flex-Algo A+B リンクのみを表示（Show Flex-Algo A+B links only）] をオンにします。

ステップ 7 [適用（Apply）] をクリックします。フレキシブルアルゴリズムの選択に対する追加の変更をトポロジマップに反映するには、[適用（Apply）] をクリックする必要があります。

図 *23 :* マップ上のフレキシブルアルゴリズム



（注）
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、トポロ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、トポロ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詳細の表示

デバイスまたはリンクのフレックスアルゴリズムの詳細を表示するには、次の手順を実行します。

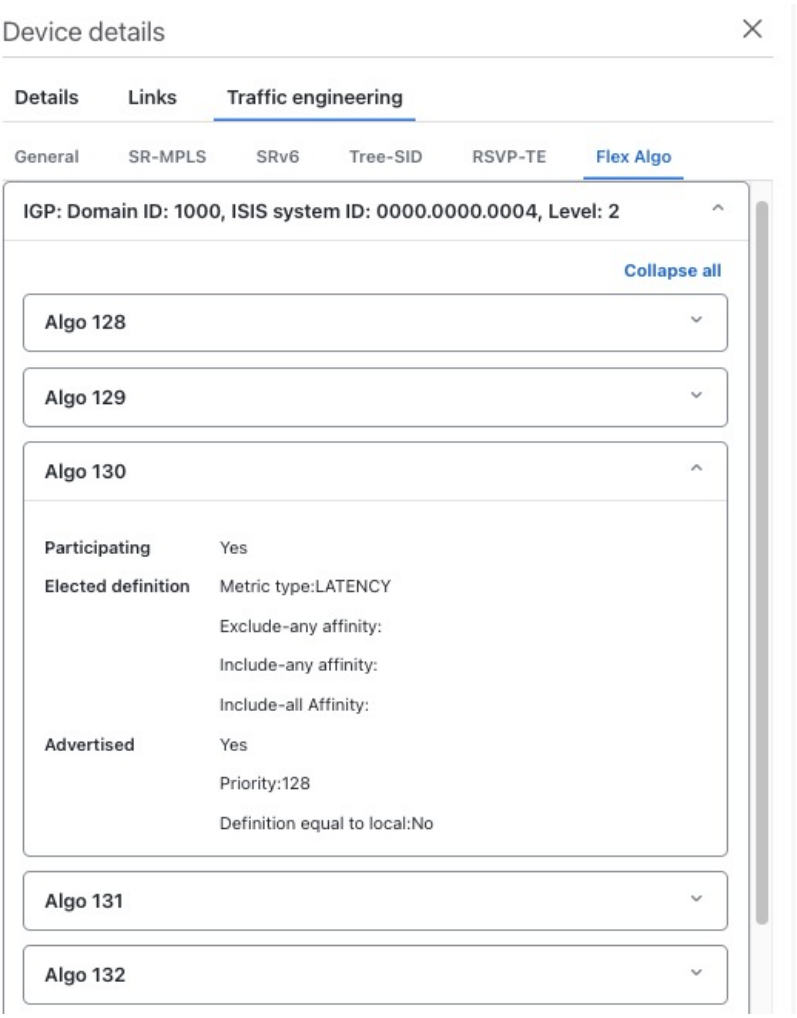
手順

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 デバイスのフレキシブルアルゴリズムの詳細を表示するには、次の手順を実行します。

a) トポロジマップから、デバイスをクリックします。
b) [デバイスの詳細（Device details）] ウィンドウで、**[トラフィックエンジニアリング（Traffic engineering）] > [フレキシブルアルゴリズム（Flex Algo）]**タブに移動します。次に例を示します。

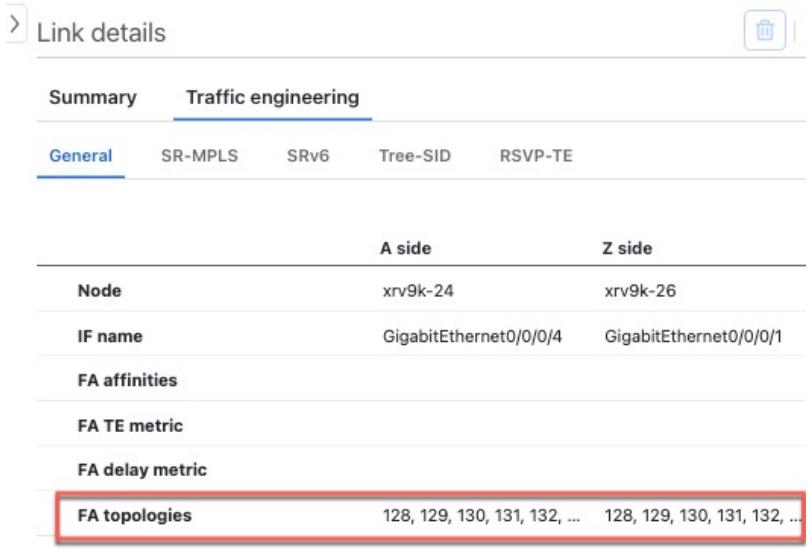
図 *24 : Flex Algo* デバイスの詳細



ステップ 3 リンクがフレキシブルアルゴリズム トポロジの一部であるかどうかを表示するには、次の手順を実行します。

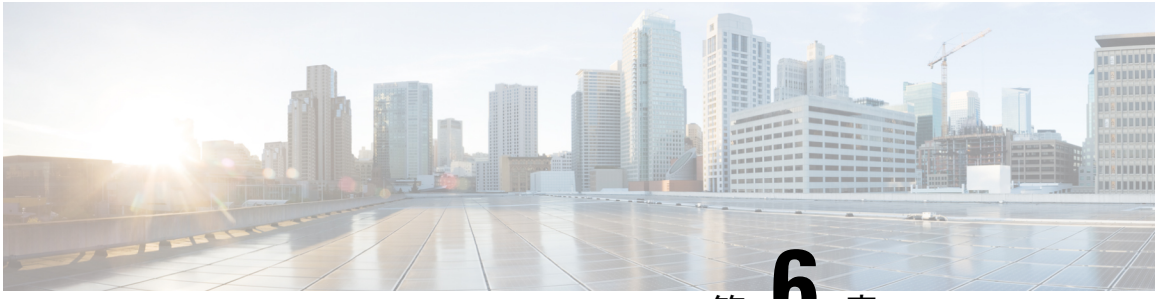
a) トポロジマップから、リンクをクリックします。リンクのリストが表示されたら、リンクタイプをクリックします。
b) [リンクの詳細（Link details）] ウィンドウで、[トラフィックエンジニアリング（Traffic Engineering）] タブをクリックします。リンクがメンバーの場合、[FAトポロジ（FA topologies）] の行には、各ソースおよび接続先デバイスが属するフレキシブルアルゴリズムが表示されます。

図 *25 : Flex Algo* リンクの詳細



（注）

- Application-Specific Link Attribute（ASLA）は、Cisco IOS XR 7.4.1 以降のバージョンである PCC およびコアルータでサポートされます。
- Crosswork ネットワークコントローラ は、フレキシブル アルゴリズム トポロジの厳密な ASLA 処理のみをサポートします。
- トラフィックエンジニアリング（TE）または遅延メトリックタイプで定義されたフレキシブルアルゴリズムの場合、OSPF または IS-IS ASLA TE および ASLA 遅延リンクメトリックをアドバタイズするノードのみが、対応するフレキシブル アルゴリズム トポロジに含まれます。



第 6 章

ツリーセグメント識別子（Tree-SID）マルチキャスト トラフィック エンジニアリング

Tree-SIDは、セグメント化されたルーティングネットワーク上でツリーのようなマルチキャストフローを導入する手法です。Tree-SID を使用して、SDN コントローラ（PCEP を使用して SR-PCE を実行するデバイス）がツリーを計算します。ツリー内の各ノード（デバイス）には、ツリーを介してマルチキャストデータをルーティングする際の特定のロールがあります。これらのロールには、ルートまたはヘッドエンドノードの Ingress、リーフノードではないミッドポイントノードの Transit または Bud、宛先リーフノードの Egress が含まれます。ツリー自体には、すべてのツリーセグメントとデバイスを表す単一の SID ラベルが割り当てられます。SDN コントローラは非常に柔軟で、セグメンテーションを把握しており、ネットワークアーキテクトが指定できる任意の制約を使用してルーティングパスを構築できます。

制約ベースの Tree-SID の最も興味深い使用例では、ルータが、異なるパスを介して同じコンテンツを含む 2 つの P2MP ストリームを配信するように設定されます。この場合、マルチキャストフローがネットワーク経由で 2 回転送され、各コピーは固有のパスをたどります。2 つのコピーが同じノードまたはリンクを使用して宛先に到達することはないため、いずれかのパスでのネットワーク障害によるパケット損失が減少します。

Tree-SID の詳細については、お使いのデバイスのセグメントルーティング Tree-SID 構成のマニュアルを参照してください（『Segment Routing Configuration Guide for Cisco NCS 540 Series Routers』など）

ここでは、次の内容について説明します。

- Tree-SID ポリシーの可視化 （60 ページ）
- トポロジマップでポイントツーマルチポイント ツリーを表示する （60 ページ）
- 静的 Tree-SID ポリシーの作成 （64 ページ）
- ツリー SID ポリシーを変更する （68 ページ）

Tree-SID ポリシーの可視化

Crosswork UI により、Tree-SID ルート、トランジットノード、リーフノード、バドノードの詳細を UI に表示できるようになり、Tree-SID がネットワークに正しく実装されていることを簡単に確認できます（トポロジマップでポイントツーマルチポイント ツリーを表示する （60 ページ）を参照してください）。

Tree-SID ポリシーには次のノードがあります。

- ルートノード：マルチキャストトラフィックをカプセル化して複製し、トランジットノードに転送します。
- トランジットノード：リーフ（出力）ノードおよび下流のサブツリーに向かう中間点（トランジット）ノードとして機能します。
- リーフノード：マルチキャストトラフィックのカプセル化を解除し、マルチキャスト受信者に転送します。
- バドノード：個別のリーフノードのパスがあり、トポロジマップに個別に表示されます。

次の Tree-SID ポリシーを可視化できます。

- **静的**：静的 Tree-SID ポリシーは、SR-PCE CLI を使用して直接、または Crosswork UI から、SR-PCE を介して設定されます。サポートされているコンフィギュレーション コマンドの詳細と例については、特定のデバイスの Tree-SID コンフィギュレーション ドキュメントを参照してください。（例：Cisco ASR 9000 シリーズ ルータのセグメント ルーティング コンフィギュレーション ガイド [英語]）
- **動的**：動的 Tree-SID ポリシーは明示的に設定されません。L3VPN/mVPN サービスの一部として設定されます。

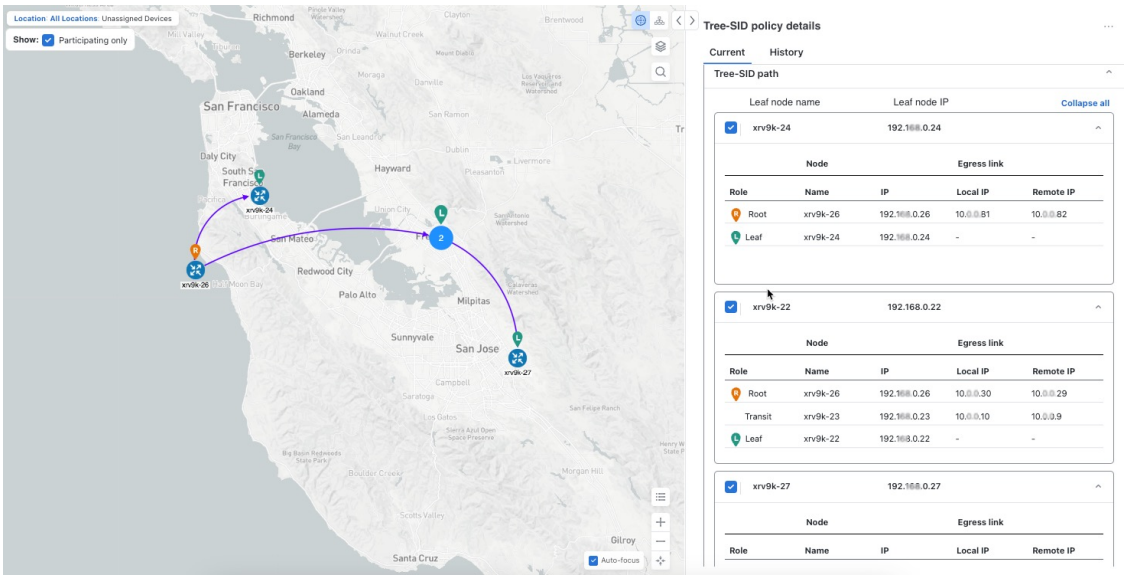
（注） 静的および動的 Tree-SID ポリシーは、高速再ルーティング（FRR）をサポートしています。

トポロジマップでポイントツーマルチポイントツリーを表示する

Crosswork を使用すると、ネットワークで設定されている Tree-SID ポリシーを可視化できます。

次の例は、トポロジマップの Tree-SID ポリシーの図を示しています。ルートノード（R）とリーフノード（L）がマークされ、矢印はルートからリーフノードまでのトランジットノードを通るパスを示しています。

図 *26* : 新しい *Tree-SID* ポリシーの作成（静的）



始める前に

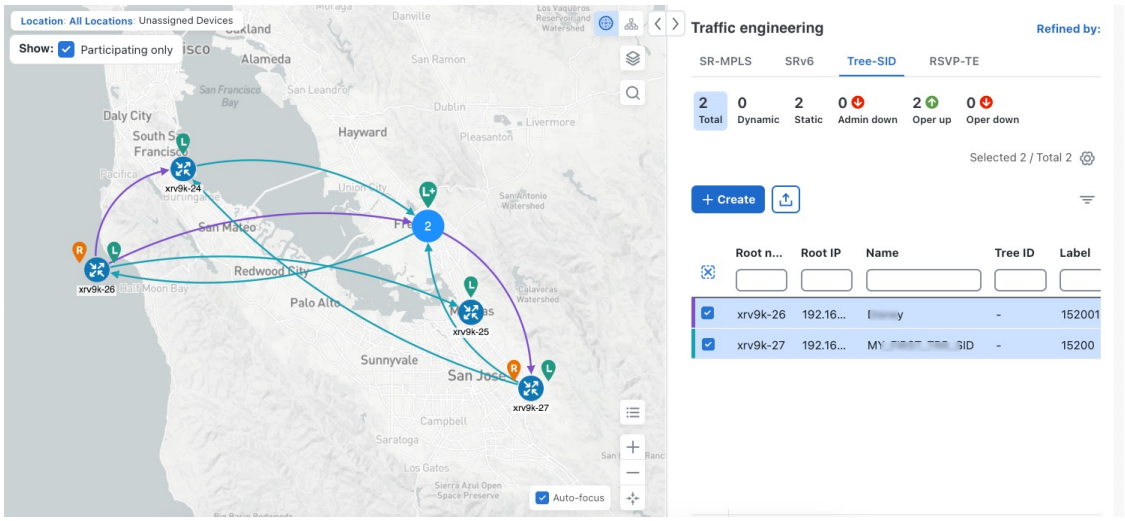
トポロジマップでマルチキャストツリーを可視化するには、ネットワークで Tree-SID ポリシーを設定する必要があります。詳細については、お使いのデバイスの SR Tree-SID 構成のマニュアルを参照してください（『Segment Routing Configuration Guide for Cisco NCS 540 Series Routers』など）

手順

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）]** > **[Tree-SID]** タブを選択します。

ステップ 2 トポロジマップに表示する Tree-SID ポリシーを選択します。トポロジマップには同時に最大 2 つのポリシーを表示できます。

図 *27*：トポロジマップの ***Tree-SID*** ポリシー（静的）



（注）
エンドポイントの変更は、履歴データのタブにイベントとしてキャプチャされます。Tree-SID の履歴データについては、TE イベントと使用率履歴の表示 （15 ページ）を参照してください

ステップ 3 Tree-SID の詳細を表示するには、[アクション（Actions）] 列から、いずれかの Tree-SID ポリシーで、… > [詳細の表示（View details）] をクリックします。サマリーと Tree-SID パス情報が表示されます。

例：

（注）
- SR-PCE フィールドの横にある（コンピューティング）ラベルには、ポリシーの作成に使用された SR-PCE の詳細が表示されます。
- 送信元ノードが使用できない場合は、[Operステータス（Oper Status）] フィールドの横に警告アイコンとメッセージが表示され（警告アイコンの上にマウスを合わせると）、接続の問題が存在する場所の詳細が示されます。

図 ***28 : Tree-SID*** の詳細の概要

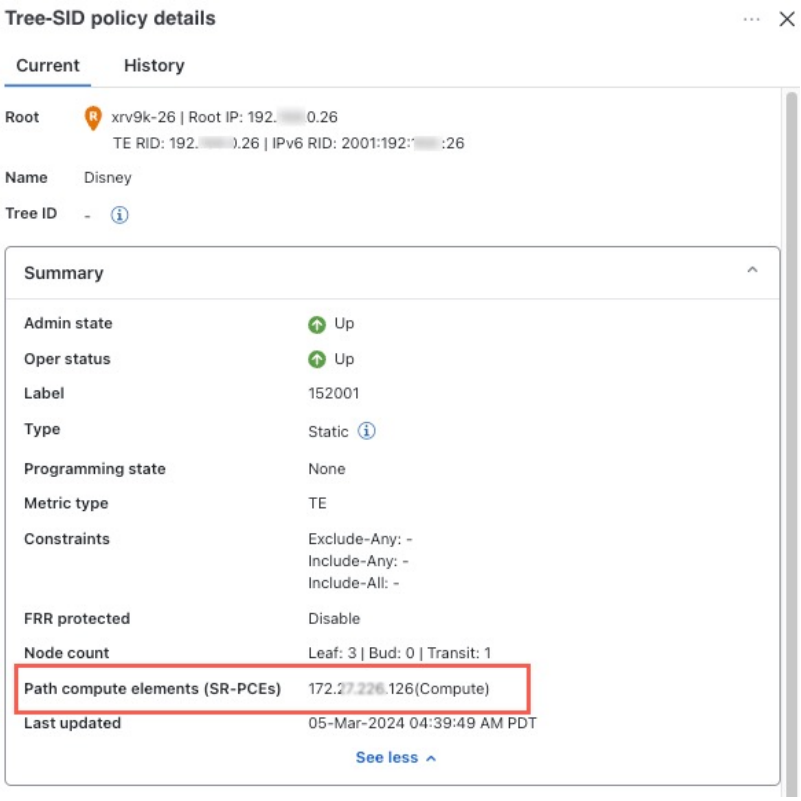
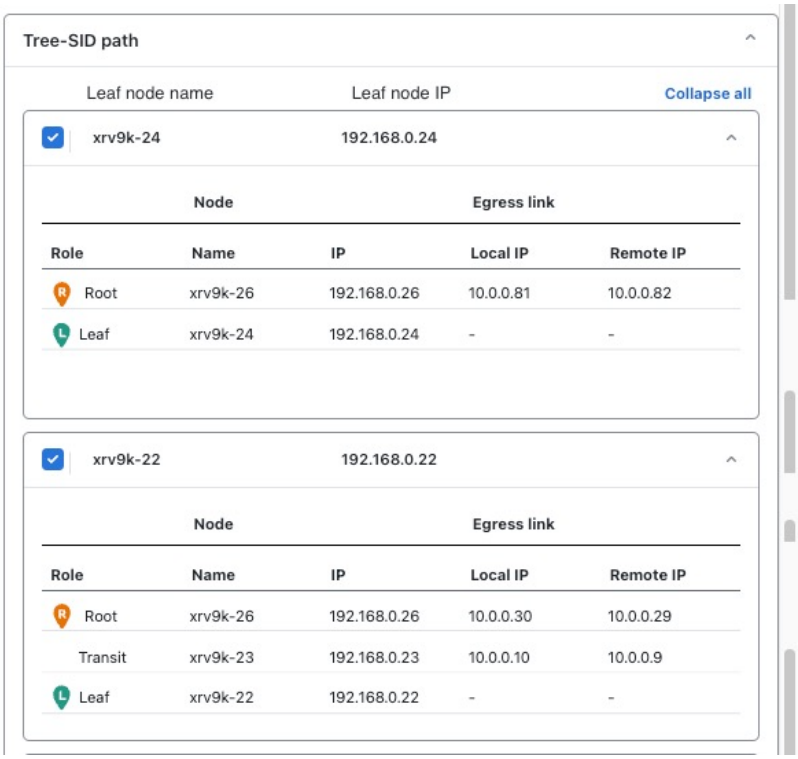


図 *29 : Tree-SID* パスの詳細



静的 Tree-SID ポリシーの作成

このタスクでは、それぞれがリーフまたはルートノードを表す静的な Tree-SID ポリシーを作成する方法について説明します。

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、それらを Cisco Crosswork にマッピングしてから静的 Tree-SID ポリシーを作成します。詳細については、TE リンクアフィニティの設定 （36 ページ）を参照してください。

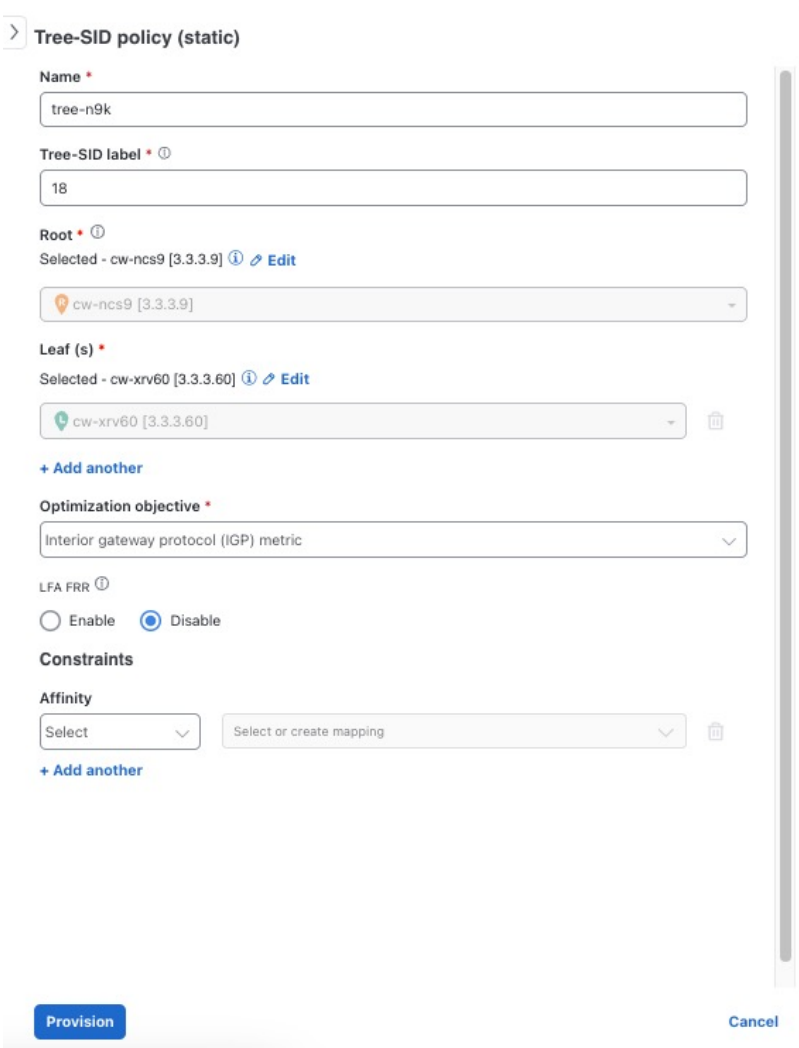
手順

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）]**>[ツリーSID（Tree-SID）] タブを選択し、[作成（Create）] をクリックします。

ステップ 2 必要なTree-SIDポリシー値を入力または選択します。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。

（注）
PCEP セッションを持つ PCC ノードのみをルートノードとして PCE に追加できます。

図 *30* : 静的 *Tree-SID* ポリシーの作成



ステップ 3 ポリシーをコミットするには、[プロビジョニング（Provision）] をクリックします。

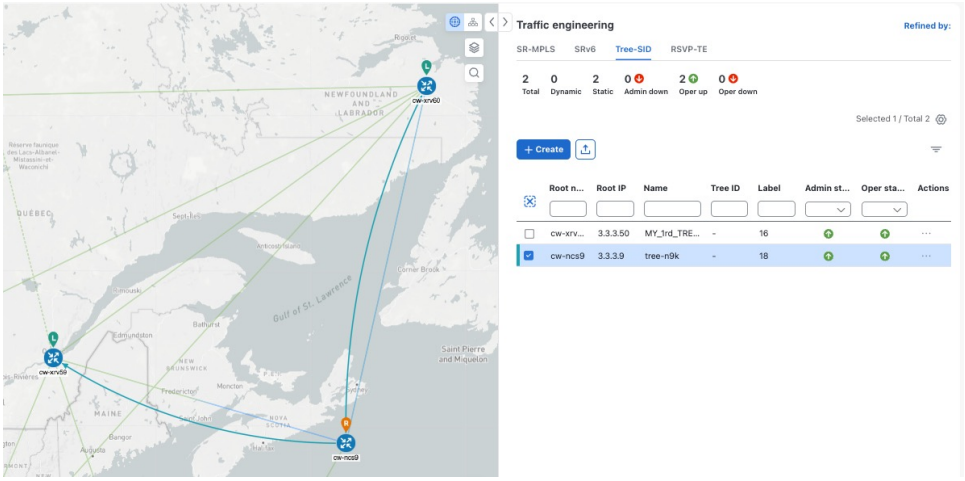
ステップ 4 Tree-SID ポリシーの作成を検証します。

1. 新しい Tree-SID ポリシーが [トラフィックエンジニアリング（Traffic engineering）] 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）

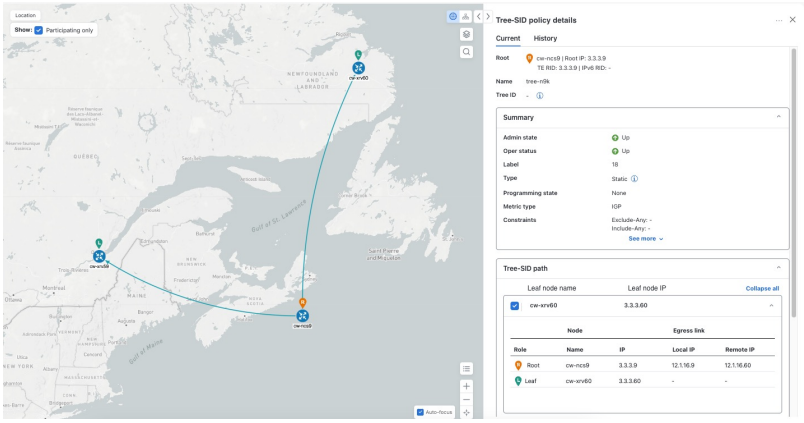
新しくプロビジョニングされた Tree-SID ポリシーは、ネットワークのサイズやパフォーマンスによっては、[トラフィックエンジニアリング（Traffic engineering）]テーブルに表示されるまでに時間がかかる場合があります。[トラフィックエンジニアリング（Traffic engineering）] テーブルは 30 秒ごとに更新されます。

図 *31 :* トポロジマップに新たに追加された *Tree-SID* ポリシー



2. 新しい Tree-SID ポリシーの詳細を表示して確認します。[アクション（Actions）]列で、[...] をクリックして [詳細の表示（View details）] を選択します。

図 *32 : Tree-SID* ポリシーの詳細



Crosswork UI による静的 Tree-SID ポリシーの設定例

次の出力は、コンピューティング SR-PCE で Crosswork UI から設定された静的 Tree-SID ポリシーを示しています。

```
RP/0/RP0/CPU0:cw-xrv56#sh pce lsp p2mp
```

```
Tree: 50-52-54, Root: 3.3.3.50
 PCC: 3.3.3.50
 Label:   505254
 Operational: up  Admin: up  Compute: Yes
 Local LFA FRR: Disabled
 Metric Type: IGP
 Transition count: 1
 Uptime: 00:01:45 (since Thu Apr 27 10:54:49 PDT 2023)
 Destinations: 3.3.3.52, 3.3.3.54
 Nodes:
  Node[0]: 3.3.3.50 (cw-xrv50)
   Delegation: PCC
   PLSP-ID: 205
   Role: Ingress
   Hops:
    Incoming: 505254 CC-ID: 1
    Outgoing: 505254 CC-ID: 1 (11.1.28.54) [cw-xrv54]
    Outgoing: 505254 CC-ID: 1 (11.1.1.51) [cw-xrv51]
  Node[1]: 3.3.3.54 (cw-xrv54)
   Delegation: PCC
   PLSP-ID: 148
   Role: Egress
   Hops:
    Incoming: 505254 CC-ID: 2
  Node[2]: 3.3.3.51 (cw-xrv51)
   Delegation: PCC
   PLSP-ID: 187
   Role: Transit
   Hops:
    Incoming: 505254 CC-ID: 3
    Outgoing: 505254 CC-ID: 3 (11.1.2.52) [cw-xrv52]
  Node[3]: 3.3.3.52 (cw-xrv52)
   Delegation: PCC
   PLSP-ID: 247
   Role: Egress
   Hops:
    Incoming: 505254 CC-ID: 4
```

次の出力は、高可用性（HA）ピア SR-PCE での同じ静的 Tree-SID ポリシーを示しています。

```
RP/0/RP0/CPU0:cw-xrv63#sh pce lsp p2mp

Tree: 50-52-54, Root: 3.3.3.50
 PCC: 3.3.3.50
 Label:   505254
 Operational: standby  Admin: up  Compute: No
 Local LFA FRR: Disabled
 Metric Type: IGP
 Transition count: 0
 Destinations: 3.3.3.52, 3.3.3.54
 Nodes:
  Node[0]: 3.3.3.54 (cw-xrv54)
   Delegation: PCE (3.3.3.56)
   PLSP-ID: 148
   Role: Egress
   Hops:
    Incoming: 505254 CC-ID: 2
  Node[1]: 3.3.3.52 (cw-xrv52)
   Delegation: PCE (3.3.3.56)
   PLSP-ID: 247
   Role: Egress
   Hops:
    Incoming: 505254 CC-ID: 4
```

```
Node[2]: 3.3.3.51 (cw-xrv51)
 Delegation: PCE (3.3.3.56)
 PLSP-ID: 187
 Role: Transit
 Hops:
  Incoming: 505254 CC-ID: 3
  Outgoing: 505254 CC-ID: 3 (11.1.2.52)
Node[3]: 3.3.3.50 (cw-xrv50)
 Delegation: PCE (3.3.3.56)
 PLSP-ID: 205
 Role: Ingress
 Hops:
  Incoming: 505254 CC-ID: 1
  Outgoing: 505254 CC-ID: 1 (11.1.28.54)
  Outgoing: 505254 CC-ID: 1 (11.1.1.51)
```

ツリー SID ポリシーを変更する

Tree-SID ポリシーを変更するには、次の手順を実行します。

（注） Tree-SID ポリシーの名前、ラベル、およびルートは変更できません。

手順

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）]**> [ツリーSID（Tree-SID）] タブを選択します。

ステップ 2 目的のツリー SID ポリシーを見つけて … をクリックします。

ステップ 3 [編集/削除（Edit / Delete）] を選択します。

（注）

- SR-PCE CLI を使用して作成されたポリシーではなく、Crosswork UI または API を使用して作成された静的 Tree-SID ポリシーのみを変更または削除できます。
- ツリー SID ポリシーの詳細を更新した後、変更を保存する前にマップでプレビューできます。

Tree-SID の特記事項

制限事項

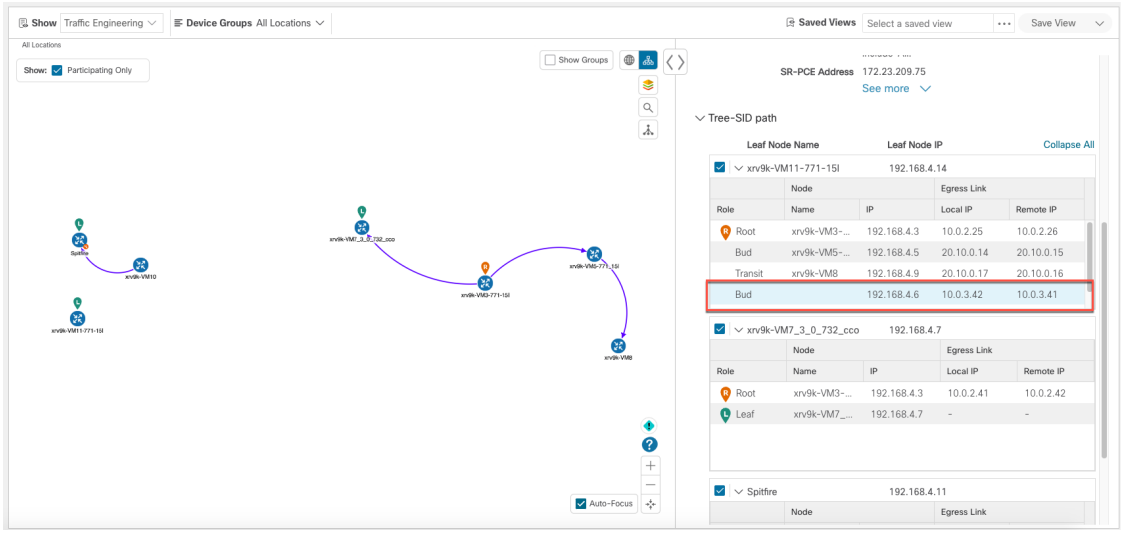
- Tree-SID ポリシーは、Cisco IOS XR ソフトウェアを実行しているデバイスでのみサポートされます。

- PCE 高可用性（HA）は、Cisco Crosswork UI を介して設定された静的 Tree-SID ポリシーでサポートされますが、SR-PCE CLI で直接設定されている場合はサポートされません。
- SRv6 に基づく Tree-SID ポリシーの詳細はサポートされていません。
- SR-PCE の単一のインスタンスが使用されている場合、SR-PCE が再起動すると、Crosswork UI から設定されたすべての静的 Tree-SID ポリシーが削除されます。
- IPv4 アンナンバード インターフェイスはサポートされていません。

ノードが欠落している Tree-SID パスの可視化

Tree-SID ノードがない場合、次の問題が発生する可能性があります。

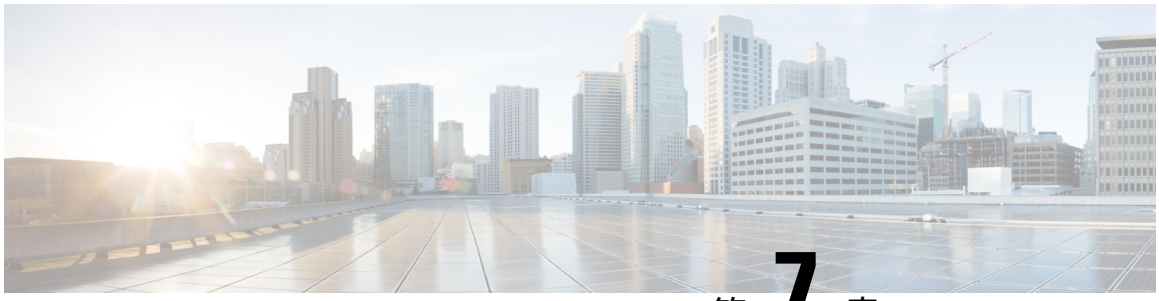
Tree-SID ポリシーパス上のノードが Crosswork トポロジ情報で使用できない場合があります。これは、ノードが Crosswork デバイスインベントリに追加されていない場合に発生する可能性があります。これは、トポロジマップ上の Tree-SID ポリシーパスの表示に影響し、1 つ以上のルートからリーフへのパスが破損しているように見えます。ただし、右側のパネルのパスの詳細には引き続きフルパスが表示されます。



第 部

帯域幅機能パック

- SR 回線型マネージャ（CSM） （73 ページ）
- ローカル輻輳緩和（LCM） （99 ページ）
- オンデマンド帯域幅（BWoD） （125 ページ）



第 7 章

SR 回線型マネージャ（CSM）

- 回線型 SR-TE に関する特記事項 （73 ページ）
- CS SR-TE ポリシーの可視化を設定するためのワークフロー （78 ページ）
- SR 回線型マネージャ を有効にする （80 ページ）
- 回線型 SR ポリシーの設定 （81 ページ）
- 回線型 SR-TE ポリシーの帯域幅使用率の確認 （83 ページ）
- 回線型 SR-TE ポリシーの表示 （85 ページ）
- 回線型 SR-TE ポリシーを再計算するための CSM のトリガー （90 ページ）
- 帯域幅予約の設定を超えた場合の動作 （91 ページ）
- **CSM のパス障害の処理方法** （95 ページ）

回線型 SR-TE に関する特記事項

このトピックでは、回線型 SR-TE ポリシーに対する Crosswork のサポートの範囲について説明します。内容には、各 回線型 SR-TE ポリシーで設定されたポリシー属性値の要件と制約、およびパスの復帰時に従う処理ロジックが含まれます。

（注） このリリースでは、ロールベース アクセス コントロール（RBAC）とタスクの権限が導入されました。回線型 SR-TE ポリシーをプロビジョニングするには、デバイス アクセス グループと割り当てられたロールに基づいた、ヘッドエンド デバイスへの書き込みアクセス権が必要です。回線型 SR-TE 管理ユーザーのみが 回線型 SR-TE 構成設定を変更できます。RBAC およびユーザー ロールの詳細については、Cisco Crosswork Network Controller アドミニストレーション ガイド [英語] を参照してください。

ポリシー属性の制約

回線型 SR-TE ポリシーを作成するときに、デバイスのコマンド ライン インターフェイスまたは Cisco Crosswork ネットワーク コントローラ を使用してポリシー属性値を設定します。属性値は後でも変更できます。

次の表に、各属性の要件と、変更が各属性に及ぼす影響を示します。次の表に記載されているすべての属性が制約として機能することを理解することが重要です。各属性が、回線型パスのホップの計算方法を制御するために Cisco Crosswork で使用される設定の要素に対応します。各値で、パスの必須プロパティを指定するか、そのパスの可能な選択肢を除外するため、各値は事実上パス計算や最適化の制約になります。

表 *2*：回線型 *SR-TE* ポリシー属性値と制約

属性	説明
ポリシーのパス保護	パス保護の制約は、回線型SR-TEポリシーの両側に必要です。
帯域幅の制約	帯域幅の制約は必須であり、回線型SR-TEポリシーの両側で同じである必要があります。帯域幅の変更は、既存のポリシーに対して実行でき、次のような効果があります。 • 両側で新しい帯域幅を設定すると、Crosswork によりパスが評価されますが、パスは再計算されません。 • 新しい帯域幅の方が高い場合、Crosswork が既存のパスをチェックして十分なリソースを確保します。現在委任されているすべてのパスが新しい帯域幅に対応できる場合、Crosswork から新しい帯域幅値を持つ同じパスが返され、パス計算クライアント（PCC）が成功したことが示されます。現在のパスのいずれかが新しい帯域幅に対応できない場合、パスが失敗したことを示す古い帯域幅値が返されます。この評価は、帯域幅が再度変更された場合にのみ再試行されます。 • 帯域幅の方が低い場合、Crosswork が新しい帯域幅値を使用して同じパスを返し、成功したことが PCC に示されます。 ポリシーの詳細を表示すると、ユーザーインターフェイスの各候補パスの下に要求された帯域幅と予約済みの帯域幅の両方が表示されます。各値は、要求された帯域幅が増加し、1 つ以上のパスで使用可能な CS プール帯域幅が不足している場合は異なる可能性があります。
候補パスとロール	現用パスは、優先順位が最も高い候補（CP）パスとして定義されます。 保護パスは、優先順位が2番目に高いCPとして定義されます。 復元パスは、優先順位が最も低いCPとして定義されます。ヘッドエンドには`backup-inligible`が設定されている必要があります。 各方向で同じロールの CP については、CP の優先順位が同じである必要があります。

属性	説明
双方向	すべてのパスを相互ルーティングとして設定する必要があります。 両側にある同じロールのパスには、グローバルに一意の同じ双方向アソシエーション ID が必要です。
分離	同じPCC上の現用パスと保護パスは、同じ分離アソシエーション ID と分離タイプを使用する分離制約で設定する必要があります。 ある方向の現用パスと保護パスのペアの分離アソシエーション IDは、反対方向の対応するペアと比較して一意である必要があります。 ノードおよびリンク分離タイプのみがサポートされています。使用される分離タイプは、同じポリシーの両方向で同じである必要があります。 復元パスには分離制約を設定できません。 Crosswork では厳密なフォールバック動作に従い、すべての現用パスと保護パスの分離が計算されます。つまり、ノードタイプの分離が設定されていて、使用可能なパスがない場合、Crosswork では制限の緩いリンクタイプの分離パスは自動的に計算されません。
メトリック タイプ	TE、IGP、ホップカウント、および遅延メトリックタイプのみがサポートされています。メトリックタイプは、両方向の現用パス、保護パス、および復元パスと一致する必要があります。
セグメントの制約	すべての現用パス、保護パス、および復元パスには、次のセグメントの制約が必要です。 • protection unprotected-only • adjacency-sid-only リンク障害が発生しても永続性を確保するには、回線型ポリシーで使用可能なすべてのインターフェイスで静的隣接関係 SID を設定します。

属性	説明
サポートされていない設定	次の設定はサポートされていません。 • メトリックバウンド • SID-Algo の制約 • 部分的なリカバリは 7.8.x ではサポートされていません。 • 高可用性ペアの PCE 間の状態同期設定。これらは 回線型 SR-TE ポリシーでは必要ありません。この機能を使用すると、パフォーマンスが低下する可能性があります。 • 色は同じでエンドポイントIPが異なる同じノード間の複数の 回線型 SR-TE ポリシー。
サポートされているポリシーの変更	以前に委任された運用上「アップ」の 回線型 SR-TE ポリシーでは、次の制約が変更される可能性があります。 • メトリックタイプ • 分離タイプ • MSD • アフィニティ 設定の変更がすべての CP と両方の PCC で一貫すると（たとえば、すべての CP と両側の新しいメトリックタイプを同じにする）と、Crosswork が再計算を開始し、現用パス、保護パス、および復元パスが新しくなります。 同じ PCC 上のパス間または PCC 間で設定が同期されていない過渡期には、パス更新は PCC に送信されません。
サポートされていないポリシーの変更	以前に委任され、運用上「アップ」の 回線型 SR-TE ポリシーに対する次の設定変更はサポートされていません。 • CP 優先順位 • 分離アソシエーション ID • 双方向アソシエーション ID 既存のポリシーに関するこれらの設定を変更するには、まず両側でポリシーをシャットダウンしてから変更を加え（整合性の観点から前述の制限に準拠）、ポリシーを「no shut」にする必要があります。

属性	説明
パス計算	Crosswork は、完全な双方向のパス保護された一連の候補パス（両側の現用パスと保護パスを含む）が委任されて初めて、回線型ポリシーのパスを計算します。帯域幅が不十分でパスが見つからない場合、SR 回線型マネージャ はソリューションが見つかるまで、または回線型SR-TEが無効になっている場合、30分後に再試行します。 Crosswork は、現用パスと保護パスがダウンして初めて復元パスを計算します。SR回線型マネージャ機能パック設定インターフェイスには、復元パスが両側から委任されてから、パスが計算されるまで待機する時間を制御する設定可能な遅延タイマーがあります。この遅延により、トポロジと SR ポリシーの状態変更によって復元パスの委任がトリガーされた場合、それらの変更が Crosswork に完全に伝達されます。 自動再最適化は、トポロジ、LSP の状態、または定期的なイベントの変更に基づくパスではサポートされません。パス計算は、エリア内/エリア間、レベル内/レベル間および IGP ドメイン内/IGP ドメイン間（同じ AS）でサポートされています。AS 間のパス計算はサポートされていません。
復帰動作	復帰動作は、保護パスと復元パスの WTR ロックタイマーオプションの設定によって制御されます（現用パスには関係ありません）。 • ロックなし設定：デフォルトの 5 分間のロック後に復帰 • 期間の指定がないロック：復帰なし • ロック期間 <value>：指定した秒数後に復帰

復帰ロジック

パスの復帰は、現用パス、保護パス、復元パスの初期状態と、各パスに影響するイベントによって異なります。次の表のシナリオに、一般的な復帰動作の例を示します。

表 *3:* パス復帰のシナリオ

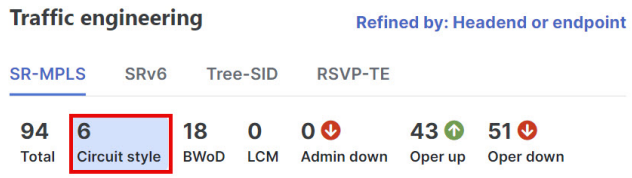
初期状態	イベント	動作
現用パスがダウン、保護パスがアップ/アクティブ	現用パスが復旧する	**1.** 現用パスがアップ/スタンバイ状態に回復します。 **2.** WTR タイマーが切れた後、各 PCC によって現用パスがアクティブに移行します。 **3.** 保護パスがアップ/スタンバイに移行します。

初期状態	イベント	動作
現用パスがダウン、保護パスがダウン、復元パスがアップ/アクティブ	現用パスが復旧し、保護パスが復旧する	1. 現用パスが回復し、アップ/アクティブになります。 2. 復元パスが削除されます。 3. 保護パスが回復し、アップ/スタンバイになります。
現用パスがダウン、保護パスがダウン、復元パスがアップ/アクティブ	保護パスが復旧し、現用パスが復旧する	サイド A：現用パス障害はローカル障害です（SegList の最初の Adj SID が**無効**です）。 1. 保護パスが回復し、アップ/アクティブになります。 2. 復元パスが削除されます。 3. 現用パスが回復し、アップ/スタンバイになります。 4. WTR タイマーが切れた後、各 PCC によって現用パスがアクティブに移行し、保護パスがアップ/スタンバイに移行します。 サイド Z：現用パス障害はリモート詳細です（SegList の最初の Adj SID が**有効**）。 1. 保護パスは回復しますが、起動せず、復元パスはアップ/アクティブのままです。 2. 現用パスが回復し、アップ/アクティブになります。 3. 復元パスが削除されます。 4. 保護パスがアップ/スタンバイになります。

CS SR-TE ポリシーの可視化を設定するためのワークフロー

トポロジマップで 回線型 SR-TE ポリシーの可視化を開始するには、次のタスクを実行する必要があります。

表 *4 :* 回線型 *SR-TE* ポリシーの可視化を開始するために完了するタスク

手順	操作
1.SR 回線型マネージャ（CSM）機能パックを有効にします。	メインメニューから、**[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）] > [回線型SR-TE（Circuit Style SR-TE）] > [設定（Configuration）]** の順に選択します。 SR 回線型マネージャ を有効にする （80 ページ） の手順を実行します。
2. デバイスで CS SR ポリシーを設定します。 （注） 回線型 SR-TE 機能パックを有効にする前にこのステップを実行すると、CS SR ポリシーは運用上ダウン状態に見えます。	次のいずれかの方法を使用して、CS SR ポリシーを設定できます。 • CLI を使用して、デバイスで CS SR ポリシーを手動で設定します。詳細については、「回線型 SR ポリシーの設定 （81 ページ）」を参照してください。 • Crosswork Network Controller 内で Crosswork 最適化エンジンを使用している場合は、UI を使用して CS SR ポリシーを設定できます。詳細については、Cisco Crosswork Network Controller ソリューション ワークフロー ガイド [英語] を参照してください。
3. CS SR ポリシーが [SRポリシー（SR Policy）] テーブルに表示されていることを確認します。	メインメニューから、[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）] > [トラフィックエンジニアリング（Traffic Engineering）] > [SR-MPLS] > [回線型（Circuit style）] の順に選択します。  [SRポリシー（SR Policy）] テーブルに、CS SR ポリシーのみを含むフィルタ処理されたリストが表示されます。

手順	操作
4. ステップ 1 で定義した予約済み帯域幅プール設定が正しく設定されていることを確認します。	CS SR ノードまたはポリシーをクリックし、[リンクの詳細（Link Details）]>[トラフィック エンジニアリング（Traffic Engineering）] ページに移動します（回線型 SR-TE ポリシーの帯域幅使用率の確認 （83 ページ）を参照）。[回線型（Circuit style）] セクションで、予約済み帯域幅プールサイズを確認します。また、現在の回線型 SR-TE 帯域幅使用率と、まだ使用可能な量を確認できます。

SR 回線型マネージャ を有効にする

トポロジマップで回線型 SR-TE ポリシーを管理および可視化するには、まず SR 回線型マネージャ（CSM）を有効にし、帯域幅予約設定を行う必要があります。

CSM が有効になっている場合、要求された帯域幅と、2 つのノード間の回線型 SR ポリシーの設定で定義されているその他の制約を使用して、最適なフェールオーバーの双方向パスが計算されます。

手順

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）] > [回線型SR-TE（Circuit Style SR-TE）] > [設定（Configuration）]** の順に選択します。

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 必要な帯域幅プールサイズとしきい値情報を入力します。次のリストに、追加のフィールド情報を示します。帯域幅予約の設定を超えた場合の動作 （91 ページ）も参照してください。

フィールド	説明
基本	
リンク CS BW プールサイズ（Link CS BW Pool Size）	回線型 SR-TE ポリシー用に予約可能な各リンクの帯域幅の割合。
リンク CS BW 最小しきい値（Link CS BW Min Threshold）	しきい値超過イベント通知が生成されるリンク CS BW プール使用率の割合。
詳細設定	

フィールド	説明
検証間隔（Validation Interval）	これは、委任されていないポリシー用に予約されている帯域幅が回線型 SR-TE ポリシー帯域幅プールに返される前に、CSM ポリシーが待機する間隔です。
タイムアウト	通知を生成するために、CSM が委任要求を待機する期間。
委任の復元の遅延（Restore Delegation Delay）	CSM が復元パスの委任を処理する前に一時停止する期間。

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。CSM を有効にしたら、デバイスで手動で（回線型 SR ポリシーの設定 （81 ページ）を参照）、または Cisco Crosswork Network Controller を介して回線型 SR ポリシーの設定を作成する必要があります。

回線型 SR ポリシーの設定

回線型 SR ポリシーの設定には、接続先エンドポイント、要求された帯域幅の量、および双方向属性を含める必要があります（追加の要件や注目すべき制約については、回線型 SR-TE に関する特記事項 （73 ページ）を参照してください）。設定には、Performance Measurement Liveness（PM）プロファイルも含める必要があります。PM プロファイルを使用すると、候補パスの活性状態が適切に検出され、パス保護が効果的に実行されます。PCC では最初の SID を過ぎると検証されないため、回線型SRポリシー候補パス障害がセグメントリストの最初のホップでない場合、PM がないとパス保護は実行されません。詳細については、「Configuring SR Policy Liveness Monitoring」を参照してください。

ここでは、デバイスで回線型 SR ポリシーと Performance Measurement Liveness（PM）プロファイルを手動で設定する方法について説明します。

手順

ステップ 1 該当する場合は、PM 設定用にデバイスのハードウェアモジュールを有効にします。

例：

```
hw-module profile offload 4

reload location all
```

ステップ 2 PM プロファイルを設定します。

例：

```
performance-measurement
 liveness-profile sr-policy name CS-active-path
```

```
  probe
   tx-interval 3300
  !
npu-offload enable   !! Required for hardware Offload only
  !
 !
 liveness-profile sr-policy name CS-protect-path
  probe
   tx-interval 3300
  !

npu-offload enable   !! Required for hardware Offload only
  !
 !
!
```

ステップ 3 PM プロファイルを使用して回線型 SR ポリシーを設定します。CSM で 回線型 SR-TE ポリシーを管理するには、例に示されているすべての設定が必要です。ユーザーが定義したエントリは斜体で表示されます。追加の要件や注目すべき制約については、回線型 SR-TE に関する特記事項 （73 ページ）を参照してください。

例：

```
segment-routing
 traffic-eng
  policy cs1-cs4

   performance-measurement
    liveness-detection
     liveness-profile backup name CS-protect      !! Name must match liveness profile defined for
Protect path
     liveness-profile name CS-active               !! Name must match liveness profile defined for
 Active path
    !
   !
   bandwidth 10000
   color 1000 end-point ipv4 192.168.20.4
   path-protection
   !
   candidate-paths
    preference 10
     dynamic
      pcep
      !
      metric
       type igp
      !
     !
     backup-ineligible
     !

     constraints
      segments
       protection unprotected-only
       adjacency-sid-only
      !
     !
     bidirectional
      co-routed
      association-id 1010
     !
    !
```

```
    preference 50
     dynamic
      pcep
      !
      metric
       type igp
      !
     !
     constraints
      segments
       protection unprotected-only
       adjacency-sid-only
      !
      disjoint-path group-id 3 type node
     !
     bidirectional
      co-routed
      association-id 1050
     !
    !
    preference 100
     dynamic
      pcep
      !
      metric
       type igp
      !
     !
     constraints
      segments
       protection unprotected-only
       adjacency-sid-only
      !
      disjoint-path group-id 3 type node
     !
     bidirectional
      co-routed
      association-id 1100
     !
    !

   !
  !

 !
!
```

回線型 SR-TE ポリシーの帯域幅使用率の確認

予約済み帯域幅プールの設定（CSMを有効にすると定義されます。SR 回線型マネージャ を有効にする （80 ページ）を参照）が正しく設定されていることを確認できます。また、現在の回線型 SR-TE 帯域幅使用率と、まだ使用可能な量を確認できます。

（注） [リンクの詳細（Link Details）] > [トラフィック エンジニアリング（Traffic Engineering）] ページには、参加している 回線型 SR-TE ノードやリンクからさまざまな方法で移動できます。次の手順は、[SRポリシー（SR Policy）] テーブルで 回線型 SR-TE ポリシーがチェックされていることを前提としています。

手順

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]** の順に選択し、[回線型（Circuit style）] をクリックします。[SRポリシー（SR Policy）] テーブルには、すべての 回線型 SR-TE ポリシーが一覧表示されます。

ステップ 2 目的の 回線型 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。

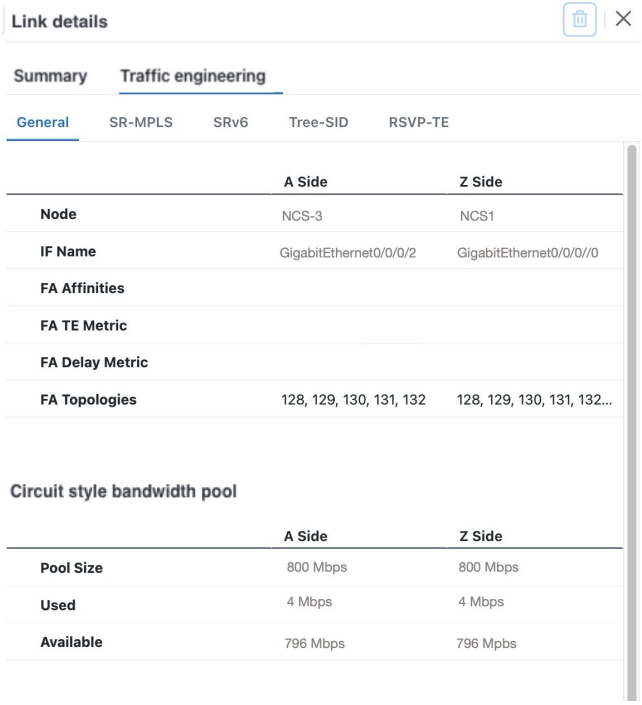
ステップ 3 トポロジマップから、参加している 回線型 SR-TE ポリシーノードをクリックします。

ステップ 4 [デバイスの詳細（Device details）] ページで、[リンク（Links）] タブ > [Link_Type _entry] > [トラフィック エンジニアリング（Traffic Engineering）] タブ > [全般（General）] の順にクリックします。

回線型の帯域幅プールでは、予約済み帯域幅プールサイズ、現在使用されている帯域幅の量、および（回線型 SR-TE ポリシーに割り当てられている）まだ使用可能な帯域幅を確認できます。

この例では、予約済み帯域幅プールサイズを、NCS-3 および NCS1 に対して 800 Mbps と表示します。構成済みの設定は、帯域幅プールサイズの 80% として事前に定義されています。インターフェイスは 1 Gbps であるため、これらのインターフェイスの 回線型 SR-TE ポリシーの帯域幅の 80% が CSM によって正しく割り当てられていることを確認できます。

図 *33 : CS SR* ポリシー帯域幅プール



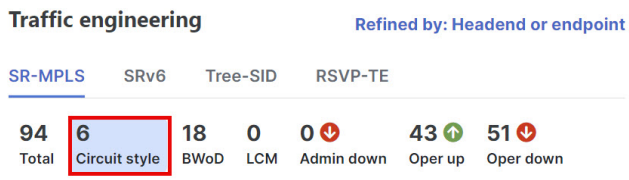
回線型 SR-TE ポリシーの表示

回線型 SR-TE ポリシーの詳細（エンドポイント、帯域幅の制約、 IGP メトリック、候補（現用および保護）パスなど）を表示します。

手順

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]** の順に選択し、[回線型（Circuit style）] をクリックします。

図 *34 : [*回線型の選択（*Select Circuit Style*）*]* タブ

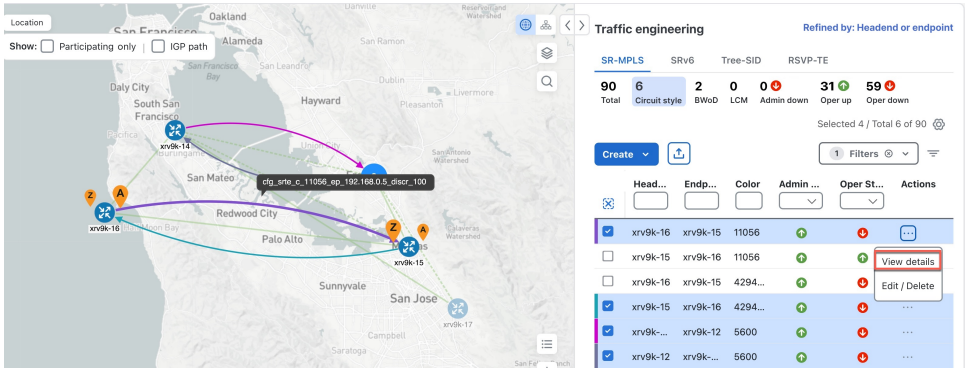


[SRポリシー（SR Policy）] テーブルには、すべての 回線型 SR-TE ポリシーが一覧表示されます。

ステップ 2 [アクション（Actions）]列で、いずれかの回線型SR-TEポリシーに対して…>[詳細の表示（View Details）]の順にクリックします。

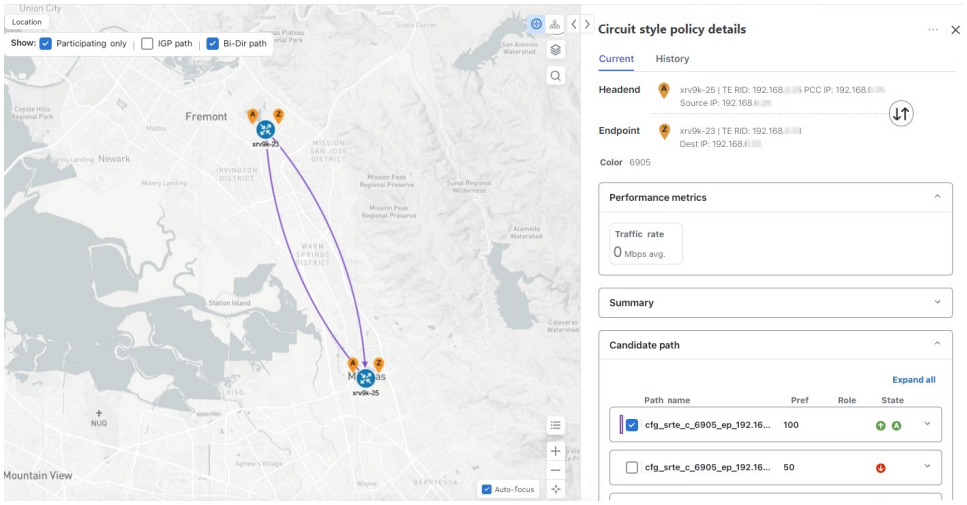
（注）
デバイスで直接作成された 回線型 SR-TE ポリシーの設定は、編集または削除できません。

図 *35 :* 回線型 *SR-TE* ポリシーの詳細の表示



サイドパネルに [回線型ポリシーの詳細（Circuit style policy details）] ウィンドウが表示されます。デフォルトでは、「アクティブ」状態の候補パスがトポロジマップに表示されます。アクティブな状態は、[状態（State）]の下に緑色の「A」アイコン付きで示され、現在動作中のアクティブなパスであることが示されています。また、このマップでは、[双方向パス（Bi-Dir path）] チェックボックスがデフォルトでオンになっており、双方向パスが表示されます。[候補パス（Candidate path）] リストには、ステータスがアクティブな候補パス（トラフィックを受け取るパス）とその他の候補パスが表示されます。

図 *36 : CS-SR* ポリシーの詳細の概要



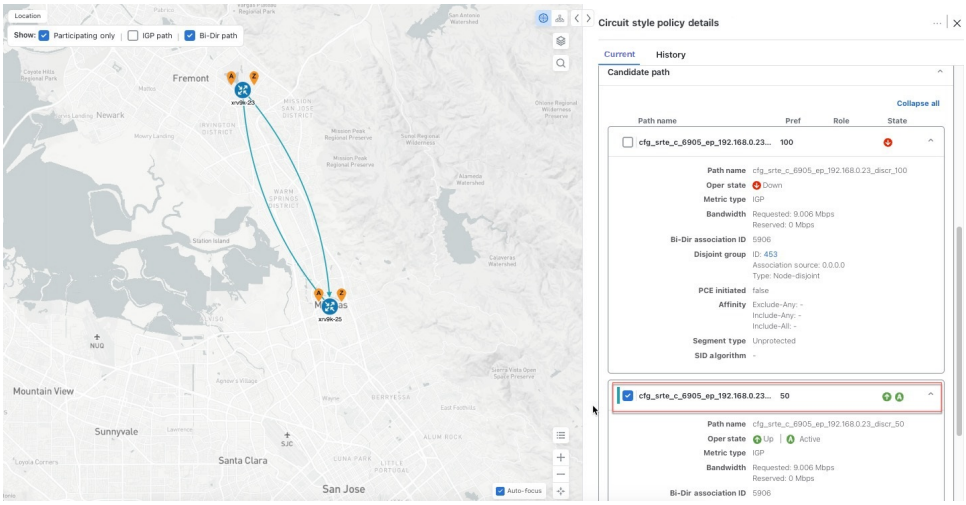
（注）
帯域幅の制約値は、値が増え、すべての現用および保護候補パスの要求を満たせる十分なリソースが存在しない場合、要求した帯域幅と異なる場合があります。

ステップ 3 候補パス設定の詳細を表示します。

a) [回線型ポリシーの詳細（Circuit style policy details）] ウィンドウでは、ドリルダウンして候補パスに関する詳細情報を表示できます。また、URL をコピーして、詳細情報を他のユーザーと共有できます。

動作状態（Oper state）が「アップ（Up）」の現用パス（最も優先度の高いパス）は常に、トラフィックを受け取ることを示すアクティブな状態になります（CSM のパス障害の処理方法 （95 ページ）を参照）。現用パスがダウンすると、保護パスがアクティブになります。この例では、保護パス（優先順位 50）がアクティブであり、トポロジマップに表示されます。[すべて展開（Expand all）] をクリックして、両方のパスに関する詳細情報を表示します。

図 *37*: トポロジマップ上の候補パス

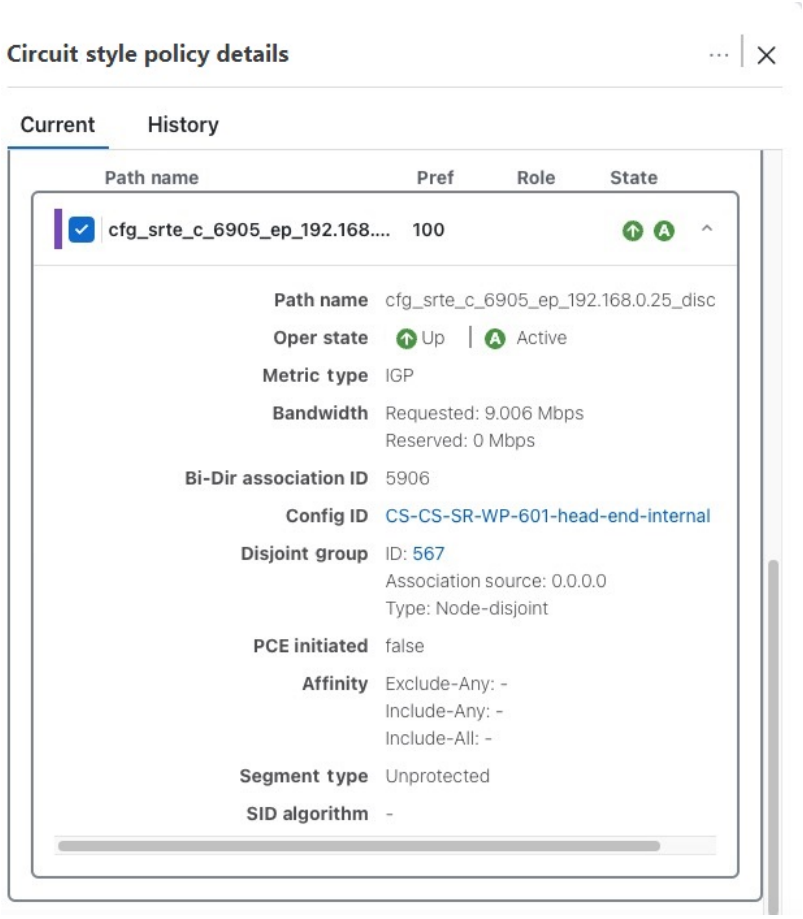


（注）

- 1 番目の優先パスは紫色のリンクで表示されます。
- 2 番目の優先パスは青色のリンクで表示されます。
- 3 番目の優先パスはピンク色のリンクで表示されます。

Cisco Crosswork ネットワークコントローラ を使用して 回線型 SR-TE ポリシーを設定した場合は、回線型 SR-TE ポリシーの設定を表示するオプションがあります。設定を表示するには、[設定ID（Config ID）] の横にあるリンクをクリックします。次に例を示します。

図 *38* : 候補パスの詳細の表示

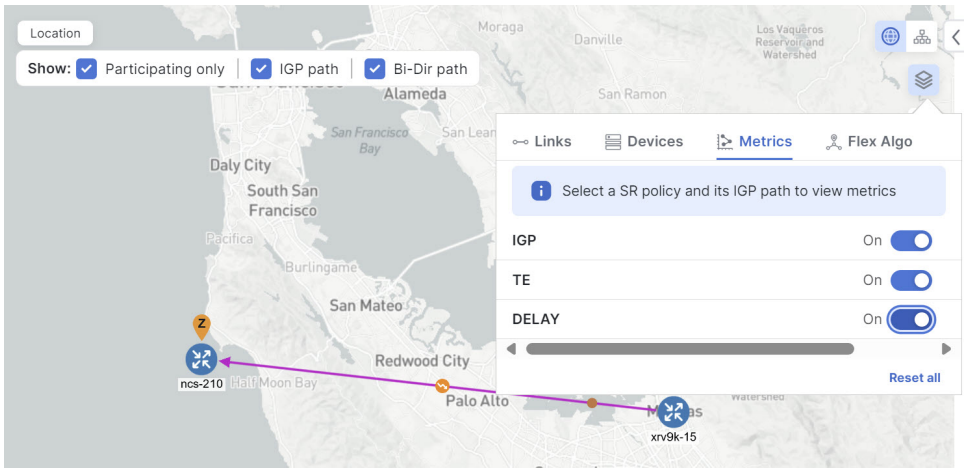


次に、回線型ポリシーの設定例を示します。詳細については、「回線型 SR ポリシーの設定 （81 ページ）」を参照してください。

図 *39 :* 回線型ポリシーの設定例

ステップ 4 選択した回線型SR-TE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するには、をクリックして該当するメトリックをオンにし、[IGPパス（IGP path）] チェックボックスをオンにします。

図 *40 : IGP* メトリック



回線型 SR-TE ポリシーを再計算するための CSM のトリガー

回線型 SR-TE ポリシーは本質的に静的です。つまり、パスが計算されると、パスに影響を与える可能性のあるトポロジまたは動作ステータスの変更に基づいて自動的に再最適化されません。ポリシーの動作ステータスがダウンからアップになった後、または帯域幅サイズと要件の変更が設定された場合は、CSM を手動でトリガーして CS-SR ポリシーを再計算できます。

（注） 再最適化できるのは、現用パスと保護パスのみで、復元パスでは機能しません。

手順

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]** の順に選択し、[回線型（Circuit style）] をクリックします。[SRポリシー（SR Policy）] テーブルには、すべての 回線型 SR-TE ポリシーが一覧表示されます。

ステップ 2 [アクション（Actions）] 列で、CSM がパスを再計算する 回線型 SR-TE ポリシーに対して … > [詳細の表示（View Details）] の順にクリックします。

ステップ 3 右上隅にある … > [再最適化（Reoptimize）] をクリックします。

帯域幅予約の設定を超えた場合の動作

CSMは、ネットワークで使用可能で予約可能な帯域幅を検出して更新します。また、CSMは、CS SR ポリシーに提供されるすべての帯域幅予約のアカウンティングを維持し、すべてのインターフェイスの予約済み帯域幅の合計がネットワーク全体のリソースプール（帯域幅プールサイズ）以下に保たれるようにします。

このトピックでは、CSM 設定ページで設定された帯域幅プールサイズまたは帯域幅アラームしきい値を超えるポリシーの CSM による処理方法の例を示します。

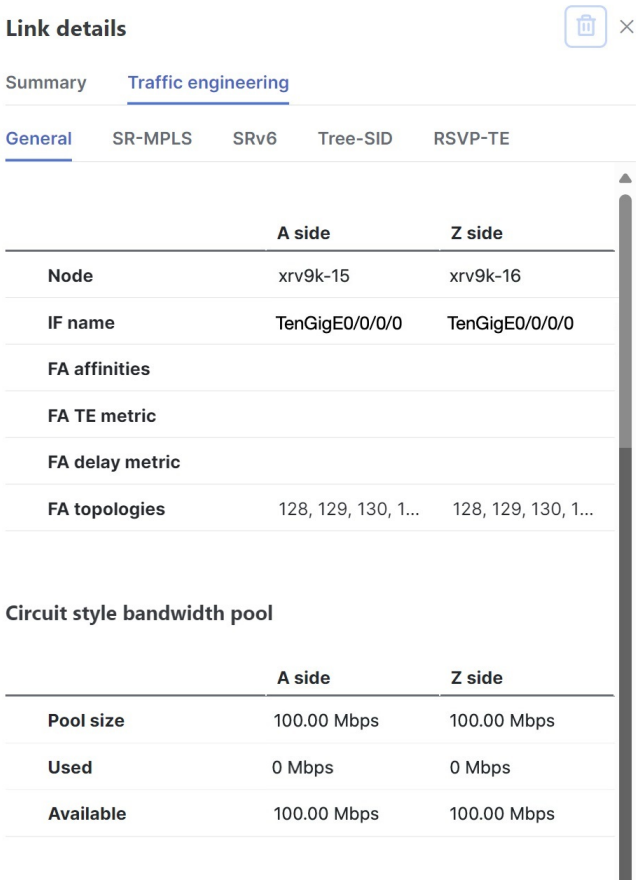
例：帯域幅使用率が定義されたしきい値を超えている場合

- リンク CS 帯域幅プールサイズ：10%
- リンク CS 帯域幅の最小しきい値：10%

この例では、10 Gbps イーサネット インターフェイスの帯域幅プールサイズは 1 Gbps で、アラームしきい値は 100 Mbps（プールサイズの 10%）に設定されています。

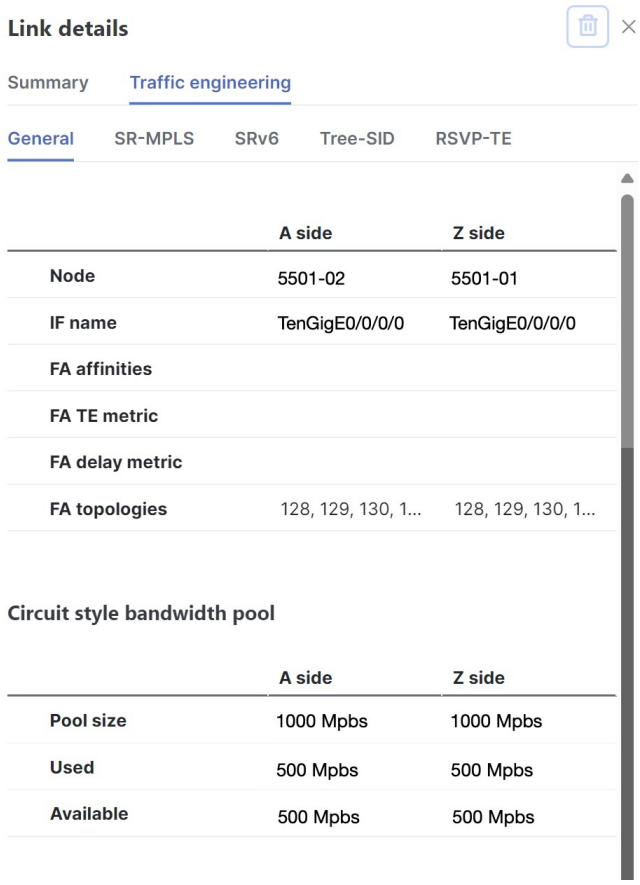
1. ノード 5501-02 からノード 5501-01（r02 - r01）への 回線型 SR-TE ポリシーは、100 Mbps の帯域幅で作成されます。

図 *41 : CS-SR* ポリシー *10 Mbps* アップ



2. その後、ポリシーに設定された要求帯域幅が 500 Mbps に増え、CSM は、既存のパスに沿った追加の帯域幅が使用可能であると判断し、帯域幅を予約します。

図 *42 : CS-SR* ポリシー *500 Mbps* アップ



3. 更新されたポリシーでの帯域幅使用率（500 Mbps）が、設定されたプール使用率のしきい値（100 Mbps）を超えているため、イベントがトリガーされます。

図 *43 :* しきい値アラート

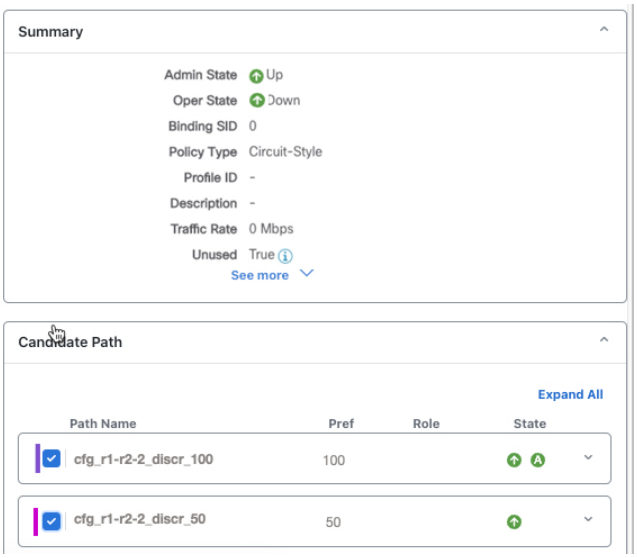
例：帯域幅プールサイズと使用率を超えた場合

- リンク CS 帯域幅プールサイズ：10%
- リンク CS 帯域幅の最小しきい値：90%

この例では、10 Gbps イーサネット インターフェイスの帯域幅プールサイズは 1 Gbps で、アラームしきい値は 900 Mbps に設定されています。

1. ノード 5501-02 からノード 5501-01（r02 - r01）への既存の 回線型 SR-TE ポリシーでは、500 Mbps の帯域幅が使用されます。
2. その後、ノード 5501-02 からノード 5501-01、5501-2（r02 - r01 - r2）へのパスで 750 Mbps の帯域幅を必要とする新しいポリシーが要求されます。これらの 2 つのノード間で使用可能な唯一のパスは、最初の CS ポリシーに対して計算されたパスです。
   - CSM は新しい 回線型 SR-TE ポリシー（r02 - r01 - r2）のパスを計算できず、運用上ダウン状態のままですが、CSM は、帯域幅要件を満たすパスを見つけるために 30 分ごとに再試行します。

   図 *44 : CS-SR* ポリシーが帯域幅プールサイズを超過

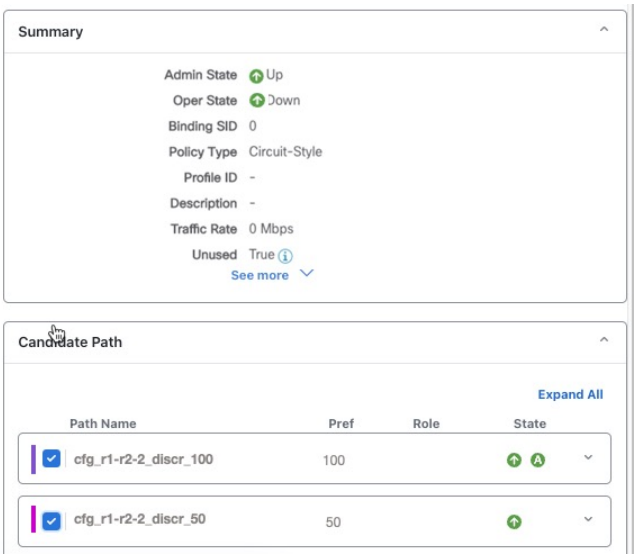


   - アラートがトリガーされます。

   図 *45 :* しきい値アラート

3. その後、回線型 SR-TE ポリシー（r02 - r01- r2）が更新され、10 Mbps のみ必要になり、次の動作が発生します。
   - 2 つのポリシーに必要な合計帯域幅（10 Mbps + 500 Mbps = 510 Mbps）は、帯域幅プールサイズ（1 Gbps）よりも少ないため、回線型 SR-TE ポリシー（r02 - r01 - r2）は、CSM によって計算されたパスを受け取り、運用上アップ状態になります。

図 *46 : 更新された CS-SR ポリシーの運用*



- 帯域幅が削減された 2 番目の 回線型 SR-TE ポリシーには CSM によってパスが提供されるため、アラートはクリアされます。

図 *47 : [Cleared Alerts]*

CSM のパス障害の処理方法

Cisco Crosswork は、完全な双方向のパス保護された一連の候補パスが委任されて初めて、回線型 SR-TE ポリシーのパスを計算します。パス障害時に使用される候補パスには、次の 3 タイプがあります。

- **現用**：優先順位値が最も高い候補パスです。
- **保護**：2 番目に優先順位値が高い候補パスです。現用パスがダウンすると、（優先順位値が低い）保護パスがアクティブになります。現用パスが回復しても、デフォルトのロック期間が経過するまで、保護パスはアクティブのままになります。
- **復元**：優先順位値が最も低い候補パスです。Crosswork は、現用パスと保護パスがダウンして初めて復元パスを計算します。復元パスが両側から委任された後、パスが計算されるまで待機する時間を制御できます（SR 回線型マネージャ を有効にする （80 ページ）を参照）。この遅延により、トポロジとポリシーの状態変更によって復元パスの委任がトリガーされた場合、それらの変更が Crosswork に完全に伝達されます。

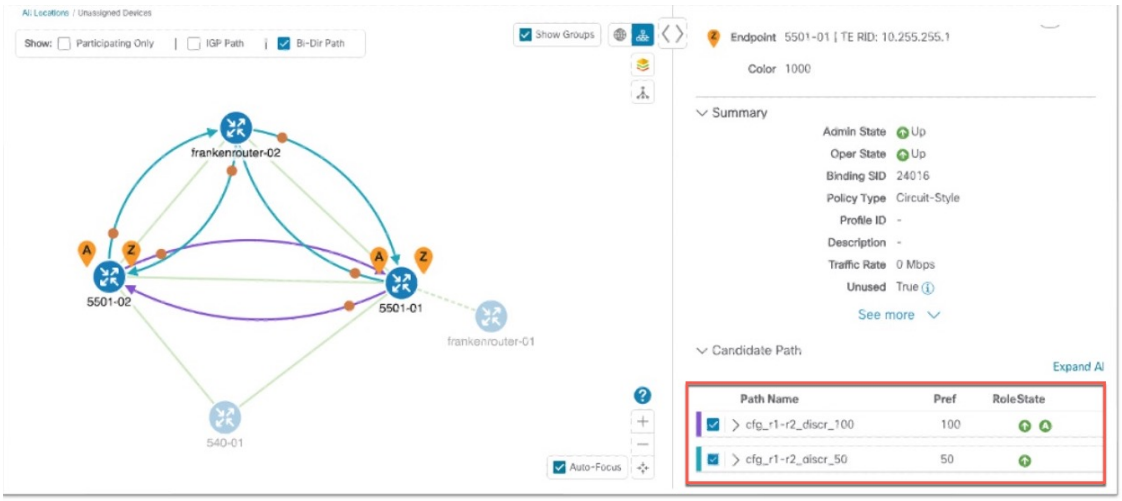
パス障害に効果的に対応し、現用パスから保護パスへの切り替えを実行するために、パフォーマンス測定（PM）を設定できます。詳細については、回線型 SR ポリシーの設定 （81 ページ）を参照してください。

例

（注） 以下の図はデモンストレーションのみを目的としており、ワークフローコンテンツ内で説明されている正確な UI やデータを常に反映しているとは限りません。このガイドの HTML バージョンを表示している場合は、画像をクリックしてフルサイズで表示してください。

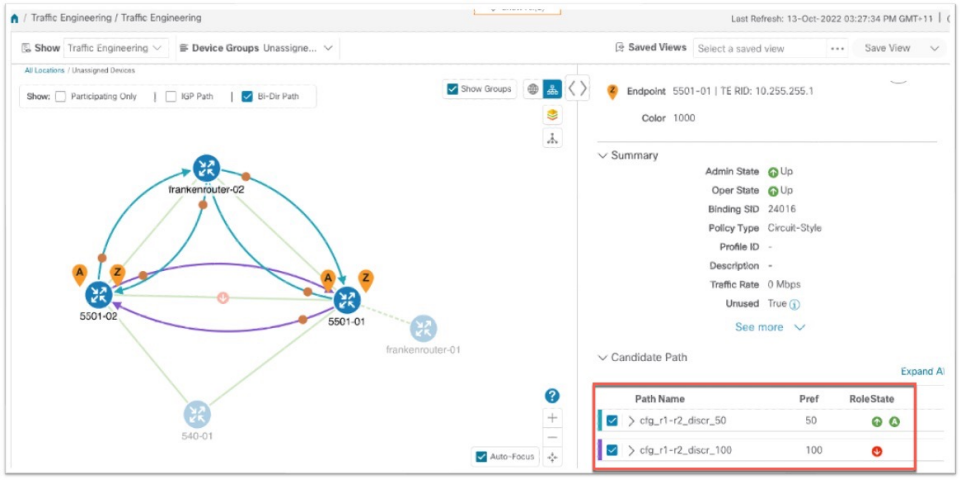
次の画像は、回線型 SR-TE ポリシーの現用パスと保護パスが動作していることを示しています。アクティブなパスは「A」アイコンで示されます。

図 *48 :* 初期候補パス



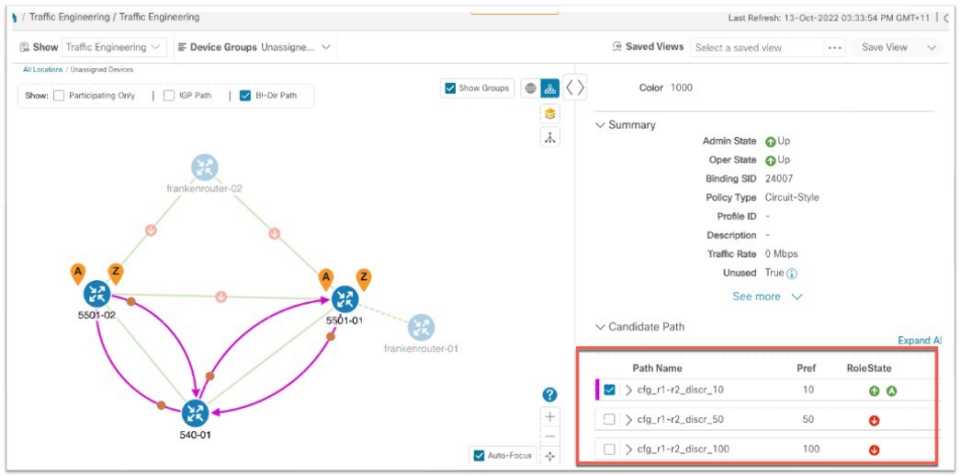
アクティブ状態の現用パスがダウンすると、保護パスはすぐに「アクティブ」になります。現用パスが回復すると、保護パスがアップ/スタンバイに移行し、現用パス（この例ではプリファレンスが 100）がアクティブになります。

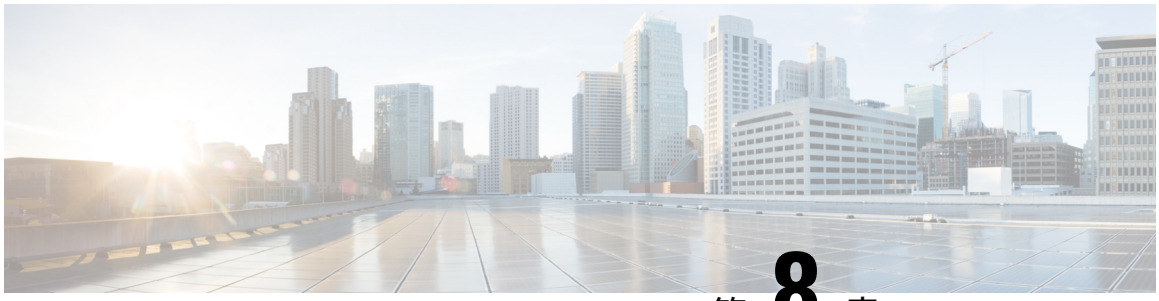
図 *49* : 保護パスがアクティブになる



現用パスと保護パスの両方がダウンした場合、CSM によって復元パスが計算されてアクティブになります。復元パスは、この特定のシナリオでのみ表示されます。この例では復元パスの最も低い優先順位値は 10 です。現用パスまたは保護パスが再び動作可能になると、復元パスはトポロジマップに表示されなくなり、**候補パス**リストから削除されます。

図 *50* : 復元パス





第 8 章

ローカル輻輳緩和（LCM）

- ローカル輻輳緩和の概要 （99 ページ）
- LCM の輻輳評価要件 （100 ページ）
- LCM の輻輳緩和要件 （102 ページ）
- LCM に関する特記事項 （103 ページ）
- LCM 計算のワークフロー （106 ページ）
- ワークフローの例：ローカルインターフェイスでの輻輳の緩和 （108 ページ）
- LCM の設定 （114 ページ）
- 個別のインターフェイスしきい値の追加 （117 ページ）
- LCM 動作のモニター （119 ページ）
- LCM からのインターフェイスの一時的な除外 （122 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ます。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ます。LCM を使用すると、次のことが可能になります。

- 指定したインターフェイスのしきい値によって定義された輻輳を監視できます。
- 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。
- 差し迫ったネットワーク障害のリスクがある場合、LCM ソリューション構成に基づいて、ダウン、機能不全、またはコミットされていない LCM TTE ポリシーを LCM が削除できるようにします。詳細については、LCM の設定 （114 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。問題にドメイン内で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ます。これにより、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が収集されるため、SR-TM は必要ありません。

（注） ネットワークで LCM を使用する方法についてはワークフローの例：ローカルインターフェイスでの輻輳の緩和 （108 ページ）を参照してください。

LCM の輻輳評価要件

LCM で輻輳を適切に評価するためには、インターフェイスおよびヘッドエンド SR-TE ポリシー トラフィック測定値のトラフィック統計が必要です。

LCM がこれらのトラフィック統計を受信していることを確認するには、次の手順を実行します。

- トラフィックをモニターするデバイス（ヘッドエンドデバイスを含む）で SNMP または gNMI を有効にします。各プロトコルの設定方法の詳細については、各デバイスのプラットフォーム コンフィギュレーション ガイド（例：「Configuring SNMP Support」）を参照してください。
- すべてのデバイスが Crosswork Data Gateway から到達可能であることを確認します。
- LCM ドメイン内のすべてのデバイスで厳密な SID ラベルを有効にします。

デバイスの設定と例については、次を参照してください。

LCM の使用に関する厳密な SID の有効化

LCM ドメイン内のすべてのデバイスで、厳密な SID が有効になっている必要があります。

手順

ステップ 1 LCM ドメイン内のすべてのデバイスに対して厳密な SID ラベルを有効にします。

例：

ISIS を使用した Cisco IOS XR：

```
router isis core
interface Loopback0
  address-family ipv4 unicast
   prefix-sid absolute 16003
   prefix-sid strict-spf absolute 16503
  !
```

```
  address-family ipv6 unicast
  !
!
```

例：

OSPF を使用した Cisco IOS XR：

```
router ospf 100
area 0
  mpls traffic-eng
  segment-routing mpls
  interface Loopback0
   passive enable
   prefix-sid absolute 16002
   prefix-sid strict-spf absolute 16502
  !
```

例：

Cisco IOS XE：

```
segment-routing mpls
!
connected-prefix-sid-map
  address-family ipv4
   <ipv4-address> absolute 16010 range 1
  exit-address-family
  address-family ipv4 strict-spf
   <ipv4-address> absolute 16510 range 1
  exit-address-family
!
!
```

ステップ 2 ヘッドエンドデバイスでセグメントルーティングを有効にし、すべてのデバイスが以下の状態であることを確認します。

- 同じデフォルトのセグメント ルーティング グローバル ブロック（SRGB）範囲または指定したカスタム範囲を使用している。
- ラベルスタックの深さに制限を課すデバイスがパスに沿って存在する場合 、最大 SID 深度が明示的に設定されている。

例：

```
segment-routing
global-block 16000 80000
  traffic-eng
    maximum-sid-depth 8
```

ステップ 3 既存の SR ポリシーがある場合は、厳密な SPF SID ラベルを使用するようにヘッドエンドデバイスを設定する必要があります。

例：

PCC によって開始または計算された SR ポリシーの場合：

```
segment-routing
traffic-eng
  policy srte_c_8000_ep
   color 8000 end-point ipv4 <ipv4-address>
   candidate-paths
    preference 100
```

```
     dynamic
      metric
       type igp
      !
     !
     constraints
      segments
       sid-algorithm 1
```

例：

PCE によって計算または委任された SR ポリシーの場合：

```
policy srte_c_8001_ep_198.19.1.4
   color 8001 end-point ipv4 198.19.1.4
   candidate-paths
    preference 100
     dynamic
      pcep
      !
      metric
       type igp
```

この SR-PCE 設定の場合、厳密な SID を持つパスのみ返されます。次に例を示します。

```
pce
segment-routing
  strict-sid-only
```

LCM の輻輳緩和要件

LCM が輻輳を正しく計算して緩和するには、ヘッドエンドデバイスで autoroute ステアリングと等コストマルチパス（ECMP）がサポートされている必要があります。

autoroute ステアリング

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。ただし、ヘッドエンドデバイスが Cisco NCS デバイスであり、ネットワークに L2VPN トラフィックがある場合、LCM は機能しません。

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、**include ipv4 all** および **force-sr-include** 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 10      !!The profile ID must match the value in the UI LCM Configuration >
Basic > Profile ID
    autoroute
     include ipv4 all
     force-sr-include
```

このコマンドの *ID* パラメータは、PCE がプロビジョニングした SR-TE ポリシーに関連付けられた PCC プロファイルを識別します。ID 値には 1 ～ 65,535 の任意の整数を指定できますが、

PCE がポリシーをインスタンス化するために使用するプロファイル ID と一致させる必要があります。一致しない場合、ポリシーはアクティブ化されません。たとえば、PCE がプロファイル ID 10 のポリシーをプロビジョニングする場合、そのポリシーの autoroute アナウンスを有効にするには、ヘッドエンドルータで `segment-routing traffic-eng pcc profile 10 autoroute force-sr-include` を設定する必要があります。各デバイスのプラットフォーム コンフィギュレーション ガイド、たとえば、*Cisco IOS XE 17*（*Cisco ASR 920* シリーズ）セグメント ルーティング コンフィギュレーション ガイド [英語] の「COE-PCE Initiated SR Policy with OSPF and IS-IS SR-TE Autoroute Announce」を参照してください。

（注） PCC プロファイルで設定された ID は、[LCM設定（LCM Configuration）] ページで設定された [プロファイルID（Profile ID）] オプションと一致する必要があります。

等コストマルチパス（ECMP）

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。ECMP を使用して、デバイスが SR-TE ポリシーをサポートできることを確認するには、デバイスで以下の状態になっていることを確認します。

- SR-TE ポリシーのヘッドエンドルータとテールエンドルータのセグメント ルーティング グローバル ブロック（SRGB）と一致する SRGB を使用して、セグメントルーティングが有効化および設定されている。デバイスの SRGB 設定を確認するには、`show segment-routing mpls state` コマンドを使用します。
- BGP-LS が有効になっていて、SR-TE ポリシーのヘッドエンドルータとテールエンドルータからリンクステート情報をアドバタイズして受信するように設定されている。BGP-LS ステータスを確認するには `show bgp link-state link-state` コマンドを使用し、デバイスのリンクステート情報を確認するには `show bgp link-state link-state database` コマンドを使用します。
- ECMP が、フローに基づいて複数の等コストパス間でトラフィックをロードバランシングするように有効化および設定されている。ECMP ルートを確認するには `show ip route` コマンドを使用し、デバイスの ECMP ロードバランシング アルゴリズムを確認するには `show ip cef` コマンドを使用します。

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。
- LCM を設定し、LCM の推奨事項をコミットするには、ドメインに対する LCM タスク権限をユーザーロールに付与する必要があります。RBAC およびユーザーロールの詳細については、Cisco Crosswork Network Controller アドミニストレーション ガイド [英語] を参照してください。

- デバイスアクセスグループ（DAG）アクセスは、LCM ではサポートされていません。ドメインの LCM タスク権限が付与されたユーザーは、そのドメイン内のデバイスに対する DAG アクセス権の有無に関係なく、LCM の推奨事項を設定およびコミットできます。
- LCM は、LDP ラベル付きトラフィックをサポートしていません。LDP ラベル付きトラフィックは、LCM 自動ルート TTE SR ポリシーに誘導できません。
- Tree SID ポリシーを持つネットワークでは、LCM の使用は推奨されません。完全なトラフィック測定値が利用できないため、最初の計算には偏りがあります。
- 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 PCC 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、1 分以上の設定可能な頻度で定期的に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が、応答性を高めるために低く設定することもできます。デフォルトの頻度は 10 分です。
- トラフィック統計の収集間隔は、トポロジの変更や、インターフェイスと LSP トラフィックの測定値に影響を与える LSP 展開に対して LCM が応答する速さに影響します。これらの変更を完全に反映するには、LCM 推奨事項のトラフィック統計の収集間隔に LCM の評価間隔を加えた時間の、最大で 2 倍の時間がかかる場合があります。この間にトラフィック測定値が更新され、最終的に Crosswork で完全に収束するにつれて、LCM の推奨事項が改善される場合があります。
- 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。

  パラレル TTE SR ポリシー間で過度に不均一な ECMP 分割を検出し、通知するイベントを発行するように LCM を設定できます。不均一な ECMP の影響を軽減するために、LCM ではオーバープロビジョニング係数が使用されます。詳細については、「LCM の設定」を参照してください。
- LCM は、既存の SR-TE ポリシーのトラフィックは最適化の対象外であり、LCM TTE SR ポリシーに誘導されるべきではないと想定しています。この前提を適用するには、既存の非 LCM SR-TE ポリシーで通常の Algo-0 プレフィックス SID を使用しないでください。このトラフィックが LCM TTE SR ポリシーに誘導されないようにするために、Algo-1 Strict、Flexible Algorithm、または隣接関係 SID の任意の組み合わせが推奨されます。
- 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。
  - ドメインのすべてのリンクがダウンした場合（LINK_DOWN 状態）、LCM 設定とドメイン UI カード（LCM の設定 （114 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。

- HA スイッチオーバー後、システムが安定したら、以前にモニターされていた欠落しているインターフェイスを手動で追加したり、ドメイン構成オプションを更新したりできます。インターフェイスやその他の設定オプションの欠落は、最後のクラスタデータの同期後に追加された場合に発生します。

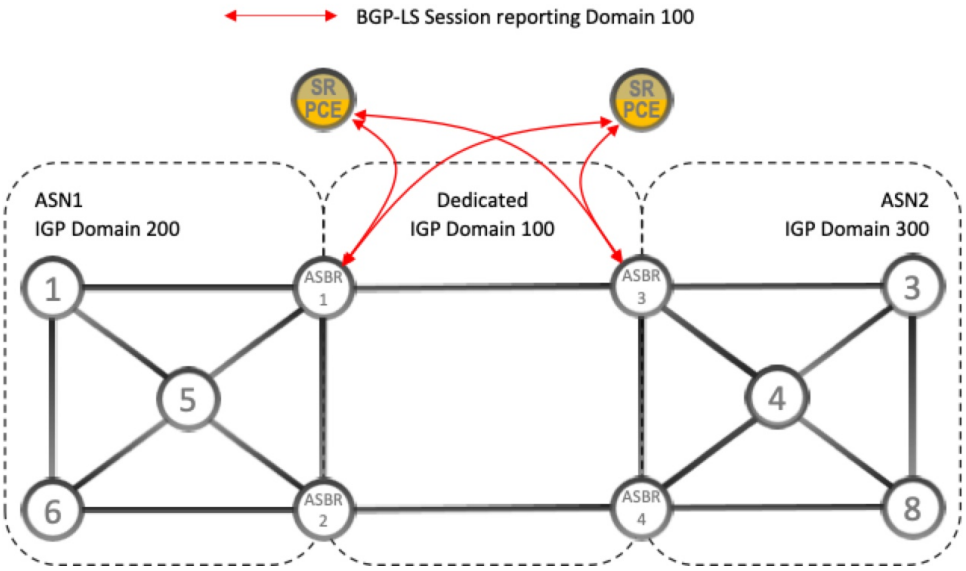
ASBR 間の専用 IGP インスタンスでの複数 AS ネットワークに対する BGP-LS のスピーカー配置

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。

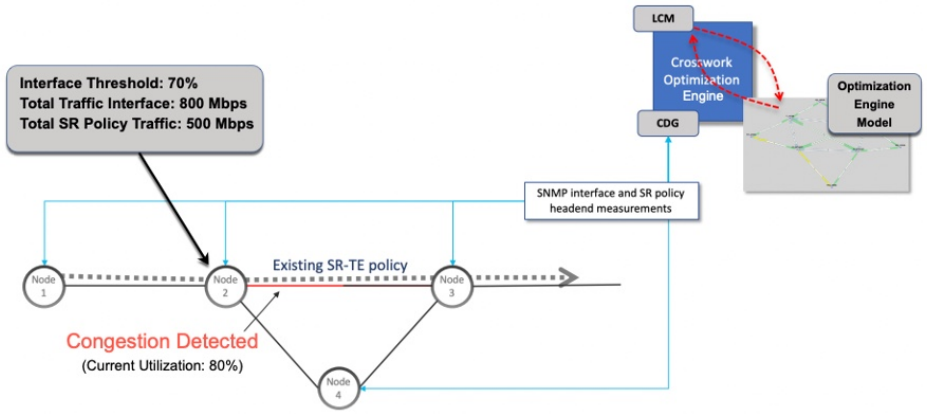
図 *51 : BGP-LS* セッション報告ドメイン *100*



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。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 *52 : LCM* の設定ワークフローの例



手順

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、ノード 2 の使用率が 70% の使用率しきい値を超えると、輻輳の確認間隔の後、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ます。

LCM は、既存の SR ポリシーや RSVP-TE トンネルでルーティングされていないトラフィック（ラベルなし、IGP ルーティング、または FlexAlgo-0 SID 経由で転送されていないトラフィックなど）のみを転送します。SR-TE ポリシー内のトラフィックは、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。

インターフェイス トラフィックの合計 - SR ポリシートラフィックおよび RSVP-TE トンネル = 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ティ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 であり、ノード 2 を介して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 （114 ページ）を参照してください。

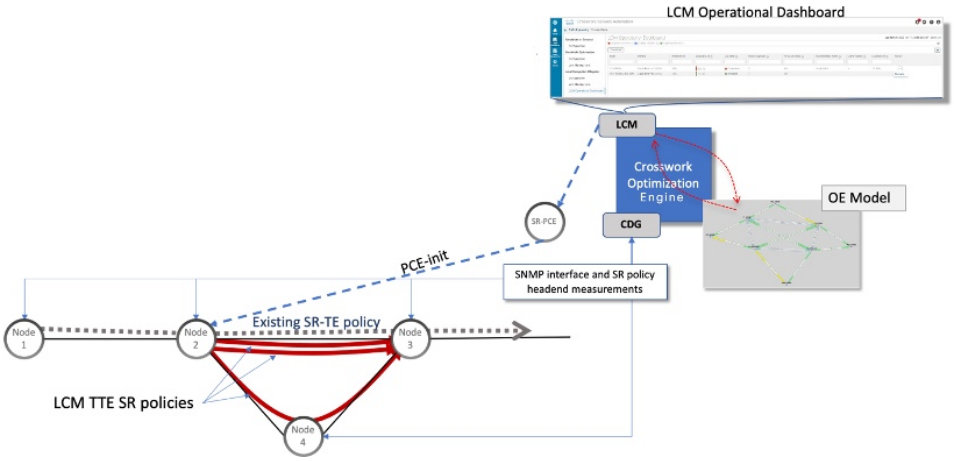
ステップ 5 LCM は、必要な TTE SR ポリシーの数とそのパスを決定します。迂回する必要がある量に対して最短パスに留まることができる LCM 対象トラフィックの割合によって、最短パスと代替パスでそれぞれ必要な TTE SR ポリシーの数が決まります。

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。

図 *53 : LCM* の推奨例



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。LCM は、緩和されたインターフェイスが削除された後も輻輳が発生しない場合（ホールドマージンを除く）、展開された

TTE SR ポリシーを削除することを推奨します。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。

ワークフローの例：ローカルインターフェイスでの輻輳の緩和

（注） このガイドの HTML バージョンを表示している場合は、画像をクリックしてフルサイズで表示してください。

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、次の手順を実行します。

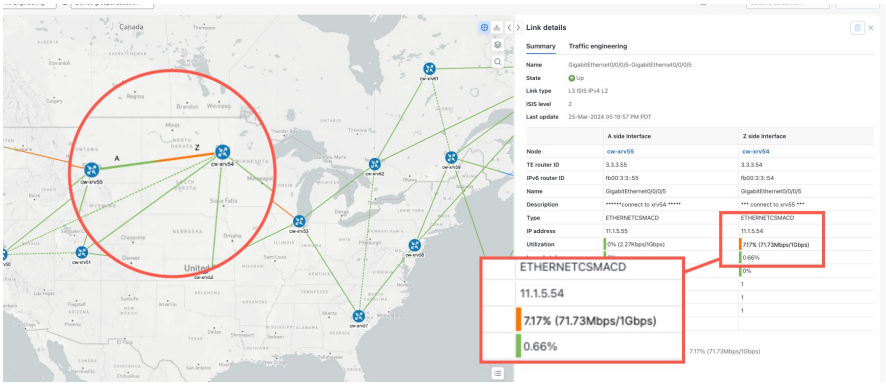
1. 輻輳していないトポロジを表示します。
2. 個々のインターフェイスの使用率のしきい値を設定します。
3. 手動モードで LCM を有効にして設定します。手動モードでは、推奨される TTE ポリシーを事前に表示して、展開するかどうかを決められます。
4. LCM が輻輳を検出した後、[操作（Operational）] ダッシュボードで LCM の推奨事項を表示します。
5. 展開する推奨される LCM TTE ポリシーをトポロジマップで視覚的にプレビューします。
6. すべての LCM TTE ポリシーの推奨事項をコミットして展開し、輻輳を緩和します。
7. LCM TTE ポリシーが展開されていることを確認します。

手順

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。

a) この例では、ノード cw-xrv54 の使用率が 7.17% であることに注意してください。

図 *54 :* 初期使用率



ステップ 2 個別のインターフェイスしきい値の定義

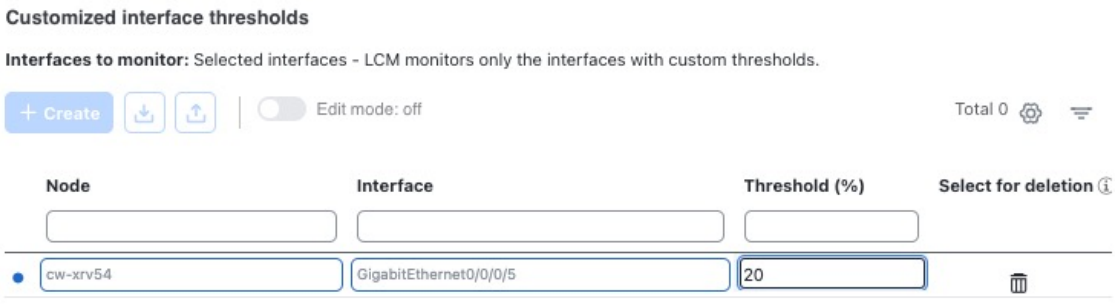
LCM では、すべてのインターフェイスに使用できるグローバル使用率のしきい値を設定できます。トラフィック使用率がしきい値を超えると、LCM は輻輳を修正するためにバイパスポリシーを見つけようとします。[LCMの設定（LCM Configuration）] ページでグローバル使用率のしきい値を設定します。ただし、個々のインターフェイスに異なるしきい値を定義する場合は、LCM を有効にする前に、[カスタマイズされたインターフェイスのしきい値（Customized interface threshold）] ページでそれらを定義することをお勧めします。

a) この例では、個々のインターフェイスのしきい値を定義します。[カスタマイズされたインターフェイスのしきい値（Customized interface threshold）] ページに移動します（**[トラフィックエンジニアリング（Traffic Engineering）] > [ローカル輻輳緩和（Local Congestion Mitigation）]** > [ドメイン識別子（Domain-Identifier）] > ⋯ > [インターフェイスのしきい値（Interface thresholds）]）。インターフェイスを個別に追加したり、カスタムの使用率しきい値を持つノードとインターフェイスのリストを含む CSV ファイルをアップロードしたりできます。詳細については、「個別のインターフェイスしきい値の追加 （117 ページ）」を参照してください。

次の例を参照してください。インターフェイス GigabitEthernet0/0/0/1 を使用する cw-xrv54 の定義済みしきい値は 20% です。

（注）
この例の使用率のしきい値は非常に低く、ラボ環境での使用に最適です。

図 *55*：カスタマイズされたインターフェイスのしきい値



（注）

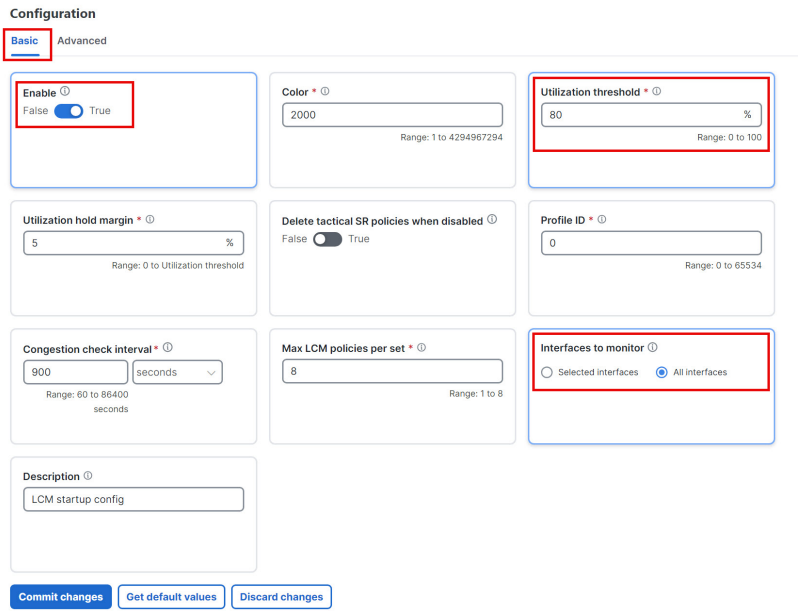
デフォルトでは、LCM はすべてのインターフェイスを監視します。対象には、このページにインポートされた個々のしきい値が含まれます。残りのインターフェイスは、[LCMの設定（LCM Configuration）] ページで定義されたグローバルな [使用率のしきい値（Utilization threshold）] を使用して監視されます。

b) インターフェイスを追加し、しきい値を定義したら、[保存（Save）] をクリックします。

ステップ 3 LCM を有効にし、グローバル使用率のしきい値を設定します。

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）] > [ローカル輻輳緩和（Local Congestion Mitigation）]**> [ドメイン識別子（Domain-Identifier）] を選択し、[設定（Configuration）] クリックします。[有効化（Enable）] スイッチを [True] に切り替え、他の LCM オプションを設定します。この例ではグローバルしきい値は80%に設定され、[監視するインターフェイス（Interfaces to monitor）] > [すべてのインターフェイス（All interfaces）] オプションが選択されています。

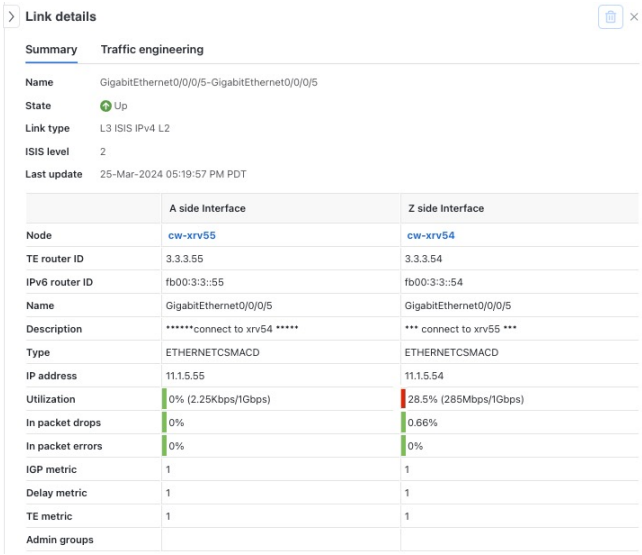
図 *56 : LCM* 設定ページ



b) [変更のコミット（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。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。

ステップ 4 しばらくすると、GigabitEthernet0/0/0/5 インターフェイスのノード cw-xrv54 に対して 20% で定義されたカスタム LCM しきい値を超える輻輳が発生します。

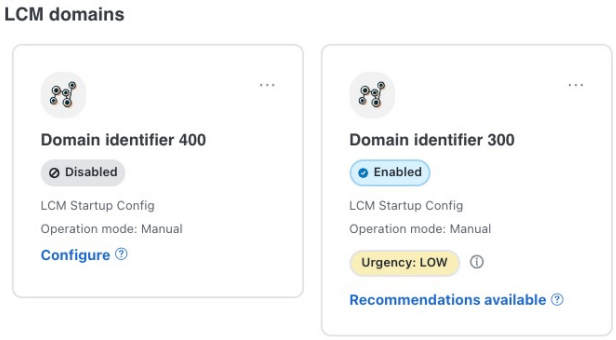
図 *57 :* 確認された輻輳



ステップ 5 [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、ドメインには緊急度のタイプと利用可能な推奨事項が表示されます。疑問符アイコンをクリックすると、緊急度のタイプと、最新の推奨事項が提示された時期に関する詳細が表示されます。

図 *58 :* 検出された輻輳と *LCM* の推奨事項



b) （オプション）LCM イベントを表示します。

Crosswork UI の右上隅から > [イベント（Events）] タブをクリックして、LCM 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。

c) [運用ダッシュボード（Operational Dashboard）] を開きます（**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [ローカルでの輻輳緩和（Local Congestion Mitigation）]**> [ドメイン識別子（Domain-Identifier）] > ··· > [運用ダッシュボード（Operational Dashboard）]）。

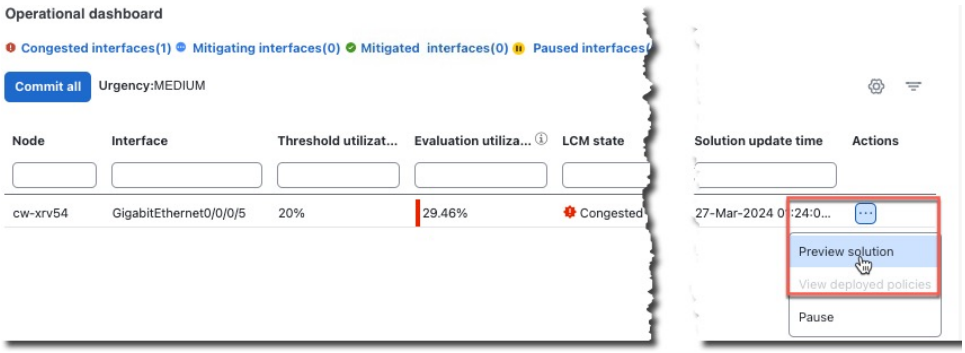
cw-xrv54 の使用率が 20% を超えていて、29.46% であることがダッシュボードに表示されます。[推奨処置（Recommended action）] 列では、LCM により、インターフェイスの輻輳に対処するために TTE

ポリシーのソリューションセット（[推奨処置（Recommended action）]：[セットの作成（Create set）]）を展開することが推奨されています。詳細については、LCM 動作のモニター （119 ページ）を参照してください。

（注）
LCM がソリューションを見つけられない場合（[推奨処置（Recommended action）]：[ソリューションなし（No solution）]）、LCM の設定（LCM の設定 （114 ページ））時に有効にした制約が原因の可能性があります。

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。[アクション（Actions）] 列で … をクリックし、[解決策のプレビュー（Preview solution）] を選択します。

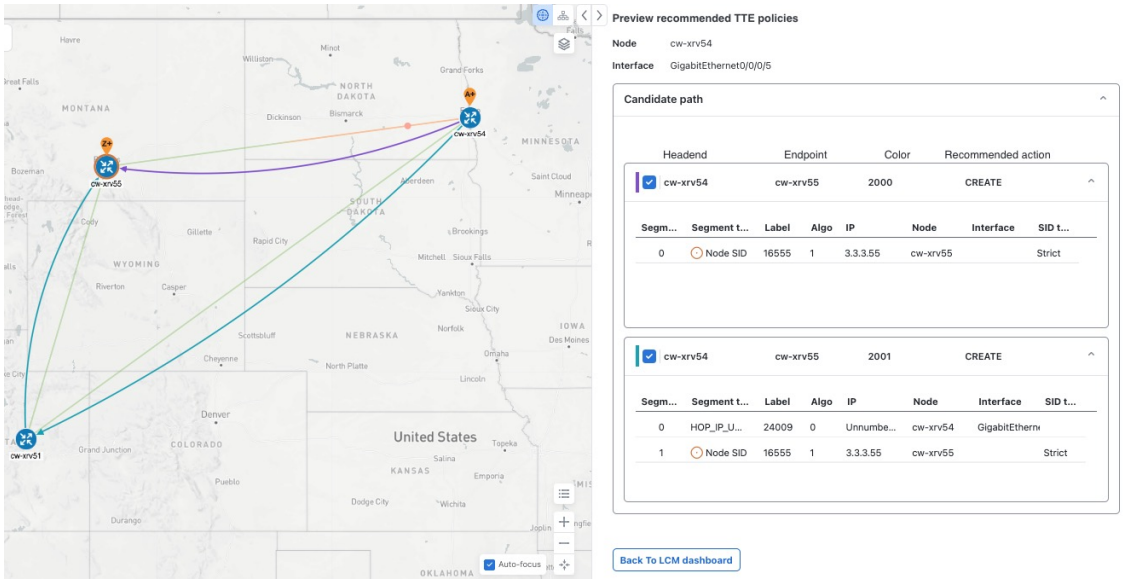
図 *59 : ソリューションのプレビュー*



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。[プレビュー（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。各ポリシーを展開して、個々のセグメントを表示できます。ネットワークへの潜在的な影響を検討してから、LCM が推奨するバイパスポリシーを展開するかどうかを決定できます。

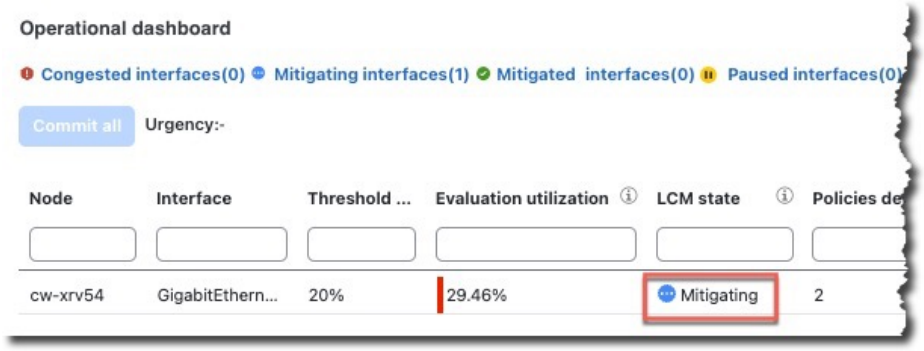
次の図は、ノード cw-xrv54 の推奨 TTE ポリシーを示しています。

図 *60 : LCM TTE* 展開のプレビュー



e) マップ上で推奨される TTE ポリシーを確認したら、[運用ダッシュボード（Operational dashboard）] に戻り、[すべて確定（Commit all）] をクリックします。[LCMの状態（LCM state）] 列が [緩和中（Mitigating）] に変化します。

図 *61* : 状態の緩和



（注）
[運用ダッシュボード（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。

ステップ 6 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は、ユーザーが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、リンクがドロップしたことでSR-TEポリシーがダウンした場合や、LCMが輻輳

を検出した場合は、イベントが表示されます。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) [運用ダッシュボード（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 [緩和済み（Mitigated）] に変化したことを確認します。

（注）
LCM の状態が変化するまでに、SNMP パターンの 2 倍の時間がかかります。

c) トポロジマップを表示して、TTE ポリシーの展開を確認します。

[アクション（Actions）] 列の … をクリックし、[展開されたポリシーを表示（View deployed policies）] を選択します。展開されたポリシーは、トポロジマップ内で強調表示されます。

ステップ 7 LCM の推奨に従って TTE SR ポリシーを削除します。

a) 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り続ける状況が続く場合に発生します。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処置を生成します。

b) 以前に展開された TTE SR ポリシーを削除するには、[すべて確定（Commit all）] をクリックします。

c) 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。

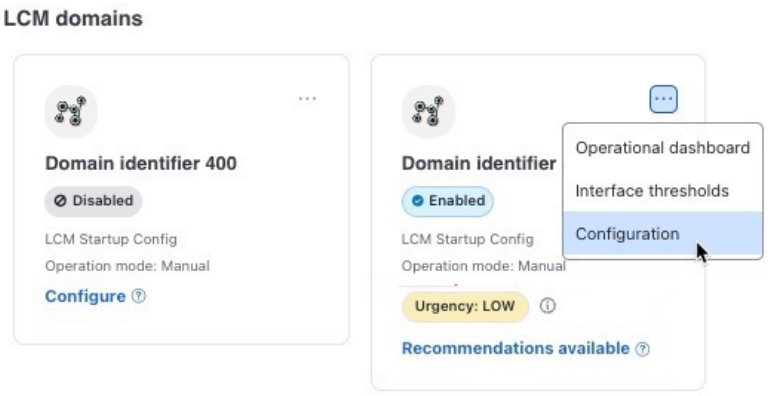
LCM の設定

LCM を有効にして設定するには、次の手順を実行します。

手順

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）]> [ローカル輻輳緩和（Local Congestion Mitigation）]> [Domain-ID-card]** > ⋯ > [設定（Configuration）] の順に選択します。

図 *62 : LCM* の設定



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。

（注）
LCM が有効になっているのに解決策が見つからない場合（[推奨処置（Recommended action）] : [解決策なし（No solution）]）、このページで有効になっている制約が原因である可能性があります。

以下に、ホバーテキストでは説明されていない追加の [基本（Basic）] フィールド情報を示します。

- [使用率のしきい値（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、[カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] 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、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。このオプションは通常、SNMP ポーリング頻度以上に設定されますが、トラフィック収集間隔によって課される範囲内で応答性を向上させるために、60 秒という低い値に設定することもできます。
- [監視するインターフェイス（Interfaces to monitor）] : デフォルトでは、[選択されたインターフェイス（Selected interfaces）] に設定され、[カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] ページ（**[トラフィックエンジニアリング（Traffic Engineering）] > [ローカル輻輳緩和（Local Congestion Mitigation）]** > [ドメイン識別子（Domain-identifier）] > ⋯ > [インターフェイスのしきい値（Interface thresholds）]）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。[カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] ページで定義されたインターフェイスのみが監視されます。[すべてのインターフェイス（All interfaces）] に設定すると、LCM は、[カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] 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 [使用率のしきい値（Utilization threshold）] 値を使用している残りのインターフェイスを監視します。

以下に、ホバーテキストでは説明されていない追加の [詳細設定（Advanced）] フィールド情報を示します。

- [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必要があるため、この間隔は SNMP 収集パターンの 2 倍以上に設定します。
- [詳細設定（Advanced）] > [自動修復ソリューション（Auto repair solution）] : [はい（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運用ダッシュボード（LCM Operational Dashboard）] に表示される推奨の [緊急（Urgency）] ステータスが [高（High）] の場合、推奨されるソリューションは [自動修復ソリューション（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。
- [詳細設定（Advanced）] > [隣接ホップタイプ（Adjacency hop type）] : [保護（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。
- [詳細設定（Advanced）] > [最適化の目的（Optimization objective）] : LCM は、最小化するために選択されたメトリックタイプに基づいて戦術的な SR ポリシーを計算します。
- [詳細設定（Advanced）] > [展開のタイムアウト（Deployment timeout）] : 戦術的な SR ポリシーの展開を確認するために許可される最大秒数を入力します。
- [詳細設定（Advanced）] > [オーバープロビジョニング係数（OPF）（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 （106 ページ）を参照してください。デフォルト値は 0 です
- [詳細設定（Advanced）] > [最大セグメントホップ（Maximum segment hops）] : バイパス TTE ポリシーを計算する場合、LCM は指定されたデバイスタグの有効な最大 SID 深度（MSD）値（ここで入力）を使用します。特定の MSD 値を持つデバイスタグを 5 つまで割り当てることができます。

  （注）

値が **0** の場合、解決にはなりません。**0** の値を設定した場合は LCM 監視と同等になり、推奨事項を提供せずにネットワークに輻輳があることを示します。

Crosswork は、SR-PCE から各プラットフォームの MSD を学習し、IGP および BGP-LS のハードウェア制限をアドバタイズします。これは、サービス/トランスポート/特殊ラベルを除いて適用できるハードウェア制限を表します。したがって、この新しいオプションを使用して、アドバタイズされた MSD 値よりも小さい値を割り当てることができ、LCM はバイパス TTE ポリシーの計算にその値を使用できます。デバイスの MSD 値を表示するには、[トラフィックエンジニアリング（Traffic Engineering）] トポロジマップに移動し、そのデバイスをクリックします。[デバイスの詳細（Device details）] ページで、[SR-MPLS] > [プレフィックス（Prefixes）] タブ > [すべて展開（Expand all）] をクリックします。

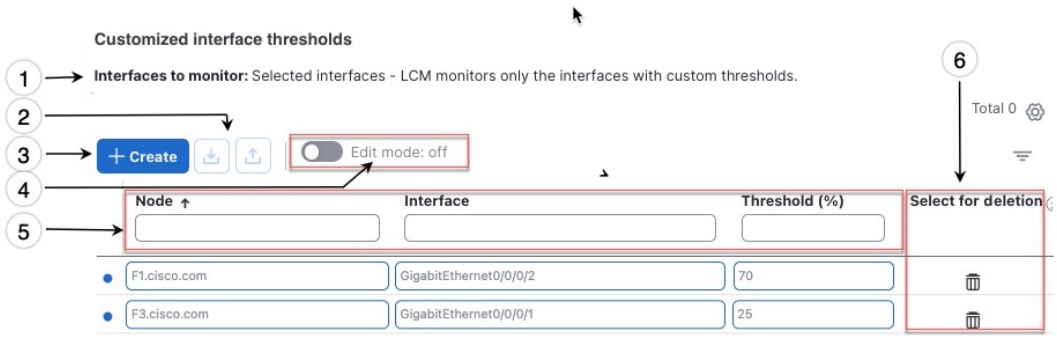
（注）
このオプションを使用する前に、特定の MSD 値を割り当てるデバイスタググループを作成する必要があります。タグの作成とデバイスへの割り当ての詳細については、*Cisco Crosswork Network Controller Administration Guide* を参照してください。

ステップ 4 設定を保存するには、[変更のコミット（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運用ダッシュボード（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。[カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] ページでは、個々のしきい値を管理し、ノードとインターフェイスに割り当てることができます。

図 *63*：カスタマイズされたインターフェイスのしきい値



引き出し線番号	説明
1	**監視するインターフェイス**：[LCMの設定（LCM Configuration）]LCM の設定 （114 ページ）ページで現在設定されているオプションを表示します。
2	**CSV ファイルのインポート**：現在テーブルにあるすべてのインターフェイスは、インポートする CSV ファイルのデータに置き換えられます。 **CSV ファイルのエクスポート**：すべてのインターフェイスが CSV ファイルにエクスポートされます。エクスポートするデータをフィルタリングすることはできません。
3	[+作成（+ Create）]：このボタンをクリックして、新しいインターフェイスのしきい値行を追加します。
4	[編集モード（Edit mode）]：[編集モード（Edit mode）] が [オン（ON）] の場合、1 つのセッションで複数のフィールドを編集して、[保存（Save）] をクリックできます。
5	**フィルタ**：デフォルトでは、この行はコンテンツをフィルタするテキストを入力するために使用できます。
6	[削除対象の選択（Select for deletion）]：行を削除するには、 をクリックします。[編集モード（Edit mode）] が [オン（ON）] の場合、削除する複数の行をチェックしてから、[保存（Save）] をクリックできます。

LCM 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。

手順

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）]>[ローカル輻輳緩和（Local Congestion Mitigation）]**> [ドメイン識別子（Domain-identifier）] > ··· > [インターフェイスのしきい値（Interface thresholds）] の順に選択し、次のいずれかをクリックします。

- [CSVファイルのインポート（Import CSV File）]：CSV ファイルを編集してインターフェイスとしきい値のリストを含め、後でファイルを LCM にインポートします。
- [新しいインターフェイスの追加（Add new interface）]：個々のインターフェイスとしきい値を手動で追加します。

ステップ 2 CSV ファイルをインポートする場合は次の手順を実行します。

a) [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。

b) [キャンセル（Cancel）] をクリックします。
c) ダウンロードした構成ファイル（LCMLinkManagementTemplate.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。
d) ファイルの名前を変更して保存します。
e) [カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] ページに戻ります。
f) [CSVファイルのインポート（Import CSV file）] をクリックして、編集した CSV ファイルに移動します。
g) [インポート（Import）] をクリックします。

ステップ 3 個々のインターフェイスを手動で追加する場合は次の手順を実行します。
a) 最初の空の行をクリックし、適切なノード、インターフェイス、およびしきい値を入力します。

図 *64 :* 最初のインターフェイスの追加

b) [+作成（+ Create）] をクリックして、インターフェイスを追加します。

ステップ 4 [カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] ページに情報が正しく表示されることを確認します。

（注）
テーブルを更新するには、編集モードをオンにするか、テーブル内の現在のすべてのデータを置き換える CSV ファイルをインポートします。

LCM 動作のモニター

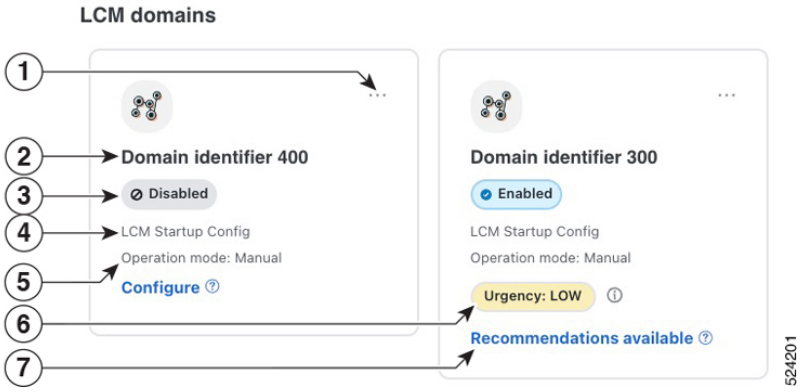
（注） このトピックでは、LCM の動作を監視するための LCM ドメインダッシュボードおよび LCM 運用ダッシュボードの使用方法と設定方法について説明します。ネットワークで LCM を使用する方法については、ワークフローの例：ローカルインターフェイスでの輻輳の緩和（108 ページ）のトピックを参照してください。

LCM ドメインダッシュボード

[LCMドメインダッシュボード（LCM Domain Dashboard）]（**[トラフィック エンジニアリング（Traffic Engineering）] > [ローカル輻輳緩和（Local Congestion Mitigation）]**）には、Crosswork

によって検出されたすべてのドメインが表示されます。ドメインは、IGP プロセスに割り当てられる識別子です。

図 *65 : LCM* ドメインダッシュボード



引き出し線番号	説明
1	**メインメニュー**：以下のページに移動できます。 • 運用ダッシュボード • 個別のインターフェイスしきい値の追加 • LCM の設定
2	**ドメイン識別子**：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。
3	**LCM ステータス**：ドメインで LCM が有効になっているか、または削除可能かどうかを示します。
4	**LCM 設定の説明**：説明は、LCM の設定ページで定義されます。デフォルトの説明は「LCM Startup Config」です。
5	[操作モード：手動（Operation mode: Manual）]：このオプションを使用する場合、ユーザーは [LCM運用ダッシュボード（LCM Operational Dashboard）] を確認し、TE トンネルの推奨事項をコミットするかどうか決める必要があります。

引き出し線番号	説明
6	[緊急性（Urgency）]：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 （114 ページ）」を参照してください。
7	**設定**：このリンクは、LCM がまだ設定されていない場合に表示されます。[設定（Configure）] をクリックして、LCM の設定 ページに移動します。 **使用可能な推奨事項**：このリンクは、LCM が輻輳を検出し、TTE ポリシーの推奨事項がある場合に表示されます。LCM の推奨事項を表示するには、リンクをクリックして **LCM 運用ダッシュボード**に移動します。 **削除**：ドメインカードを LCM モニタリング対象から削除できることを示します。

LCM 運用ダッシュボード

[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は、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。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。

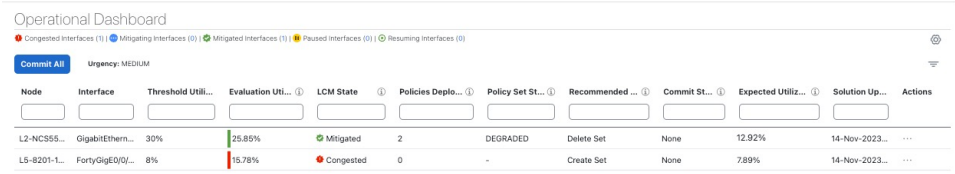
[アクション（Actions）] 列から次の操作を実行できます。

- 展開前の TTE ポリシーのプレビュー（··· > [ソリューションのプレビュー（Preview Solution）]）
- 展開の確認（··· > [展開されたポリシーを表示（View Deployed Policies）]）
- インターフェイスの一時停止または再開（··· > [再開（Resume）] / [一時停止（Pause）]）

LCM 運用ダッシュボードが提供する情報をよりよく理解するには、次の例を参照してください。

（注） このガイドの HTML バージョンを表示している場合は、画像をクリックしてフルサイズで表示してください。

図 *66 : LCM* 運用ダッシュボード



この例では、次の情報が伝えられます。

- 最初の行は、現在緩和状態にあるインターフェイスであり、以前の輻輳を緩和するために 2 つのポリシーが展開されていることを示しています（**Policies Deployed-2**）。ただし、現在の推奨事項（[推奨処置（Recommended Action）] : [セットの削除（Delete Set）]）では、ポリシーは不要になったため削除することになっています（以前に展開されたポリシーが削除されても、輻輳は発生しません）。現在の推奨事項はコミットされていないため、現在の [コミットステータス（Commit Status）] は [なし（None）] です。
- 2 番目の行は、現在輻輳状態にあるインターフェイスです。LCM が輻輳を検出し、輻輳を修正するためのポリシーの展開が推奨されています（[推奨処置（Recommended Action）] : [セットの作成（Create Set）]）。ソリューションのプレビューを選択できます（[…] > [ソリューションのプレビュー（Preview Solution）]）。

（注） LCM がソリューションを見つけられない場合（[推奨処置（Recommended Action）] : [ソリューションなし（No Solution）]）、[LCMの設定（LCM Configuration）] ページで有効になっている制約が原因の可能性があります。詳細については、「LCM の設定 （114 ページ）」を参照してください。

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。[すべてコミット（Commit All）] をクリックする必要があります。

LCM からのインターフェイスの一時的な除外

軽減のために LCM にインターフェイスを含めるのを一時的に停止できます。インターフェイスは一時停止されると、推奨項目の一部とは見なされなくなり、そのインターフェイスが参加している既存のソリューションはすべて削除されます。操作の一時停止は、次のような多くの使用例で必要になる場合があります。

- 展開されたソリューションで意図した解決につながらない場合

- ECMP トラフィックが不均一な場合
- トラフィックを伝送しないポリシーがある場合
- インターフェイスが異なるソリューション間で継続的にスロットリングしている場合

次のような特定の異常が検出されると、LCM 機能パックによってインターフェイスが自動的に一時停止されることがあります。

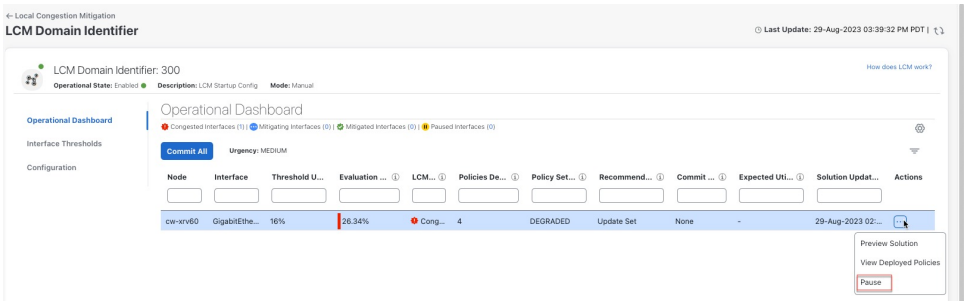
- LCM SR ポリシートラフィックがない
- 過剰な LCM ポリシー トラフィックの不均衡
- 1 時間あたりの過剰な LCM 振動や削除数

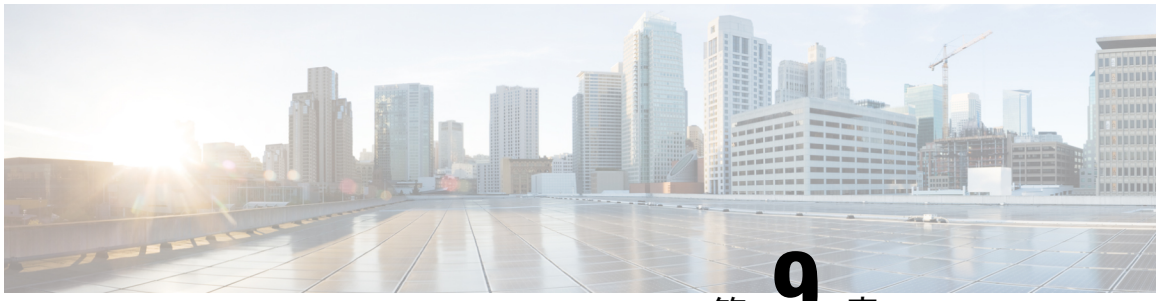
このような状況では、ユーザーは修正処置を実行し、手動でインターフェイスの一時停止を解除できます。

[LCM運用ダッシュボード（LCM Operational Dashboard）] の [アクション（Actions）] 列で、LCM 計算から除外するインターフェイスに対して ··· > [一時停止（Pause）] の順にクリックします。LCM 計算にインターフェイスを再度含めるには、··· > [再開（Resume）] の順にクリックします。

（注） 複数のインターフェイスを同時に一時停止すると、要求がタイムアウトする可能性がありますが、各要求はキューに入り、ダッシュボードに表示されます。

図 *67* : インターフェイスの一時停止





第 9 章

オンデマンド帯域幅（BWoD）

オンデマンド帯域幅（BWoD）は、セグメントルーティングポリシー（SRポリシー）のSR-PCEと組み合わせて帯域幅認識パス計算要素（PCE）を提供します。BWoD ポリシーは、PCC によって開始（PCE 委任）または PCE によって開始されたポリシーにできます。BWoD は、SR ポリシーを介してソフト帯域幅保証サービスを提供するように設計されています。BWoD はネットワークの状態をモニターし、BWoD パスを再最適化して、インターフェイス上の合計 BWoD トラフィックが設定されたしきい値の割合を超えないようにします。

BWoD はインターフェイスの総使用率を追跡しないため、BWoD トラフィックと非 BWoD トラフィックの合計がインターフェイス容量を超えた場合でも、インターフェイスが輻輳する可能性があります。さらに、BWoD では BWoD SR ポリシーに入るトラフィックの総量は強制されません。BWoD ポリシーでは、Equal Cost Multipath（ECMP; 等コストマルチパス）を通過する可能性があるトラフィックの均等なトラフィック分散が想定されます。ただし、特にフローが大きい場合は、実際の ECMP 分散が不均一になる可能性があります。

（注） ここで説明する機能は、特定のライセンスオプションでのみ使用できます。

ここでは、次の内容について説明します。

- BWoD に関する特記事項 （125 ページ）
- PCC によって開始された BWoD SR-TE のポリシー （126 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 （128 ページ）
- オンデマンド帯域幅の設定 （134 ページ）
- **BWoD のトラブルシューティング** （135 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。

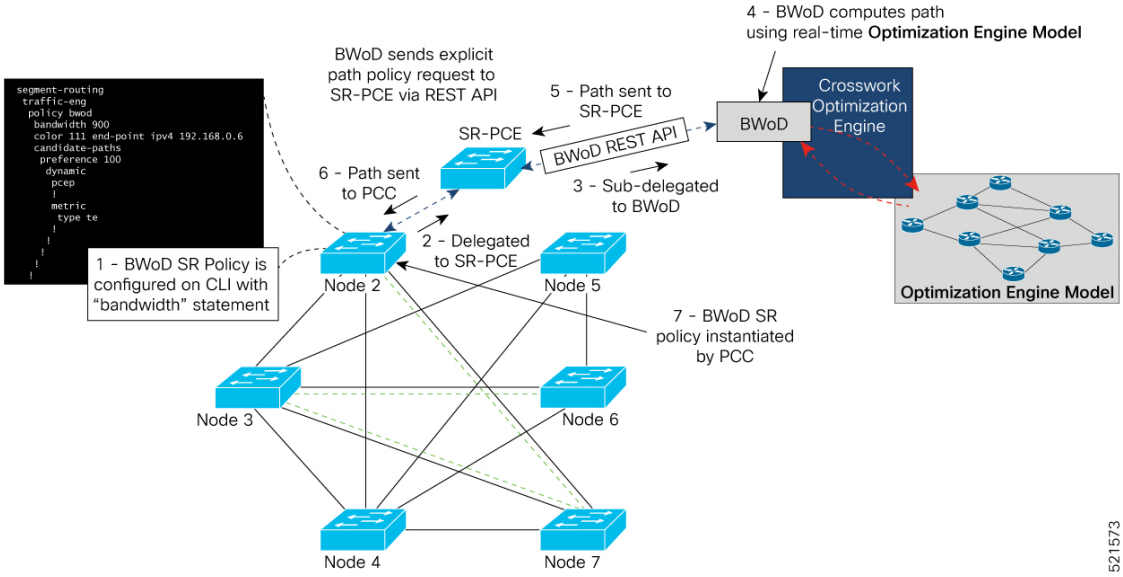
- このリリースでは、ロールベースアクセスコントロール（RBAC）とタスクの権限が導入されました。BWoDポリシーをプロビジョニングするには、デバイスアクセスグループと割り当てられたロールに基づいた、ヘッドエンドデバイスへの書き込みアクセス権が必要です。BWoD管理ユーザーのみがBWoD構成設定を変更できます。RBACおよびユーザーロールの詳細については、Cisco Crosswork Network Controller アドミニストレーション ガイド [英語] を参照してください。
- 要求された帯域幅を保証するポリシーのパスをBWoDが検出できない場合、このオプションが有効になっていると、BWoD は「ベストエフォート」パスの検出を試みます。
- BWoDは、予期しないエラーが発生した場合、ネットワークの中断を回避するためにBWoD自体を無効化します。
- Optimization Engine の再起動またはトポロジサービス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。
- [ポリシー違反（Policy Violation）] 詳細フィールドが [厳格（Strict）] に設定されている場合、SR ポリシートラフィックのオプションは [要求された最大測定値（Max Measured Requested）] に設定する必要があります。
- 高可用性セットアップでのスイッチオーバー後、最後のクラスタデータ同期後に作成されたBWoDポリシーは管理できなくなり、孤立したTEポリシーと見なされます。Crossworkは、孤立した TE ポリシーを検出するとアラームを表示します（[管理（Administration）] > [アラーム（Alarms）]）。API を使用して、孤立したポリシーをクリアして管理可能できるようにできます。詳細については、DevNet の API ドキュメントを参照してください。

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 で設定されているすべての 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。

図 *68 : PCC* によって開始された *BWoD SR-TE* のポリシー



引き出し線番号	説明

1	BWoDポリシーは、CLIを介してPCCで設定されます。次に例を示します。
	`segment-routing`
	` traffic-eng`
	`  policy bwod`
	`   bandwidth 900`
	`   color 100 end-point ipv4 1.1.1.2`
	`   candidate-paths`
	`    preference 100`
	`     dynamic`
	`      pcep`
	`      !`
	`      metric`
	`       type te`
	`      !`
	`     !`
	`     constraints`
	`      affinity`
	`       exclude-any`
	`        name RED`
	`       !`
	`      !`
	`     !`
	`    !`
	`   !`

2	帯域幅ステートメントが PCE 委任 SR ポリシーに追加され、BWoD ポリシーが作成されます。コミットされると、PCC はパスの計算を SR-PCE に委任します。
3、4	SR-PCE は、帯域幅の制約を満たすパスを計算しようとする BWoD にポリシーを委任します。

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。

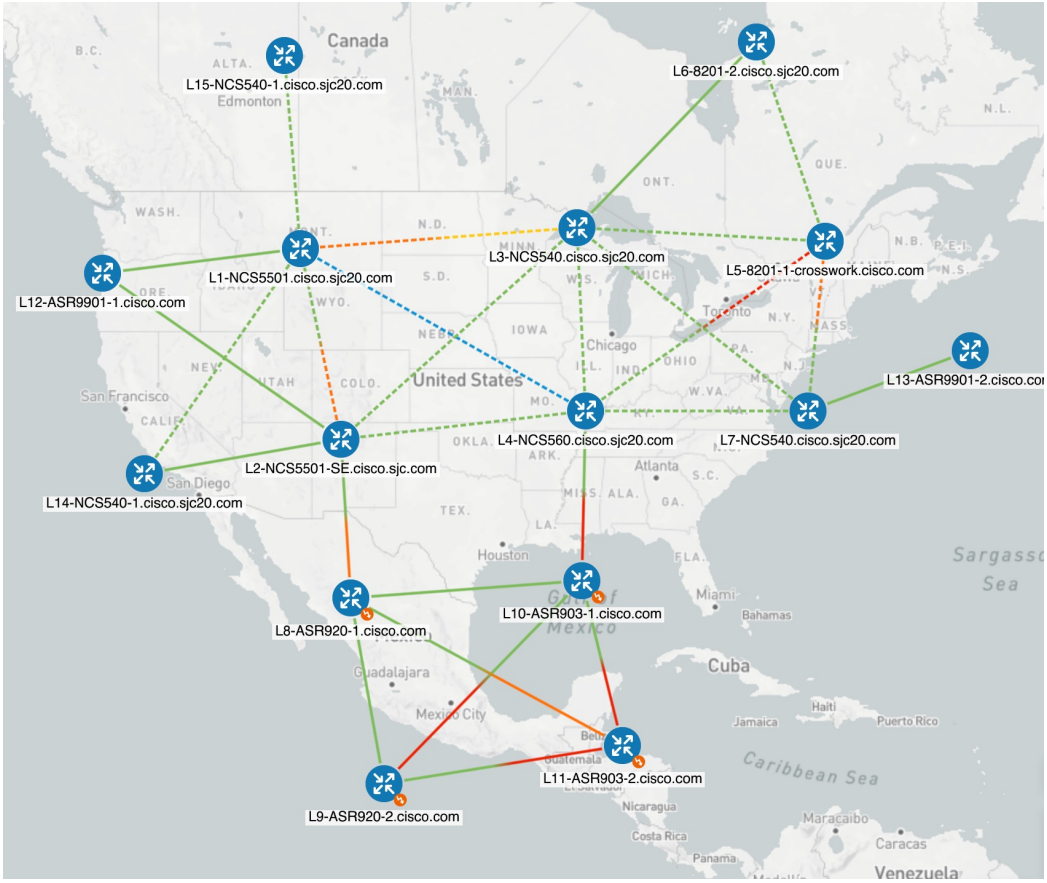
インテントベースの帯域幅の要件を維持するための SR-TE ポリシーのプロビジョニングの例

この例では、次のことを示します。

- オンデマンド帯域幅（BWoD）を有効にして設定する方法
- BWoD ポリシーの作成方法
- BWoD によるパスの計算方法
- ポリシー違反オプションが Loose または Strict に設定されている場合に、BWoD が新しいポリシーを計算する方法。

具体的には、使用率を 80% に維持しながら、**同じ**ヘッドエンド（L1-NCS5501.cisco.sjc20.com）とエンドポイント（L5-8201-1-crosswork.cisco.com）を使用して、帯域幅要件が 700 Mbps と 1000 Mbps の 3 つの BWoD ポリシーが作成されます。この例では、すべてのインターフェイスのキャパシティが **1 Gbps** です。

図 *69* : 初期 *BWoD* トポロジの例



手順

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）]** の順に選択します。

b) [有効化（Enable）] スイッチを [はい（True）] に切り替え、[リンク使用率（Link utilization）] フィールドに 80 と入力し、[詳細設定（Advance）] > [ポリシー違反（Policy Violations）] が [緩やか（Loose）] に設定されていることを確認します。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 最初の PCE 開始 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]** タブの順に選択し、**[+作成（+Create）]** をクリックします。

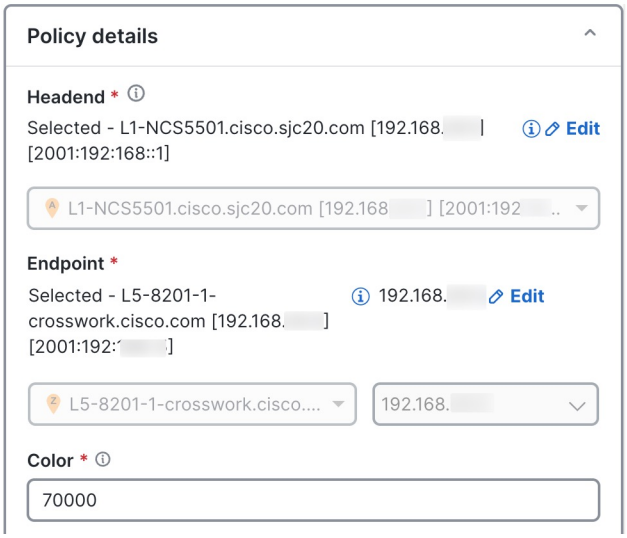
b) 必要なポリシーの詳細を入力します。この例では、次の値を使用してポリシーを作成します。

- ヘッドエンド：**L1-NCS5501.cisco.sjc20.com**

- エンドポイント：**L5-8201-1-crosswork.cisco.com**
- 色：**70000**

例：

図 *70 :* ポリシーの詳細

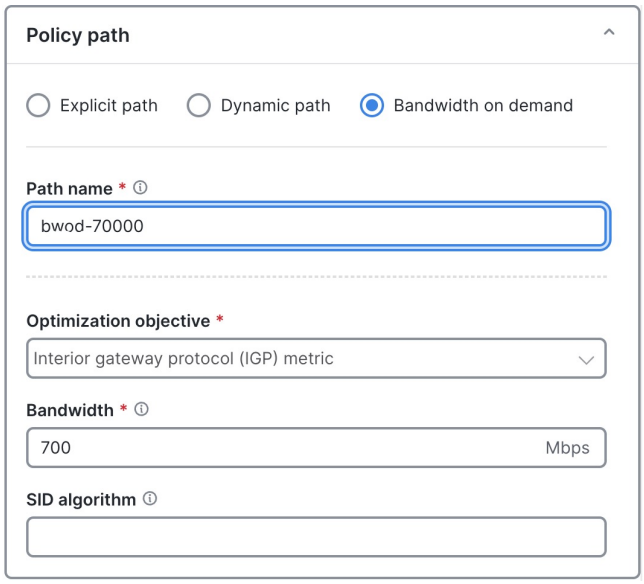


c) [ポリシーパス（Policy path）] 領域で、[オンデマンド帯域幅（Bandwidth on demand）] をクリックし、必要なポリシーパスの詳細を入力します。この例では、次の値を使用します。

- パス名：**bwod-70000**
- 最適化の目標：**内部ゲートウェイプロトコル（IGP）メトリック**
- 帯域幅：**7000 Mbps**

例：

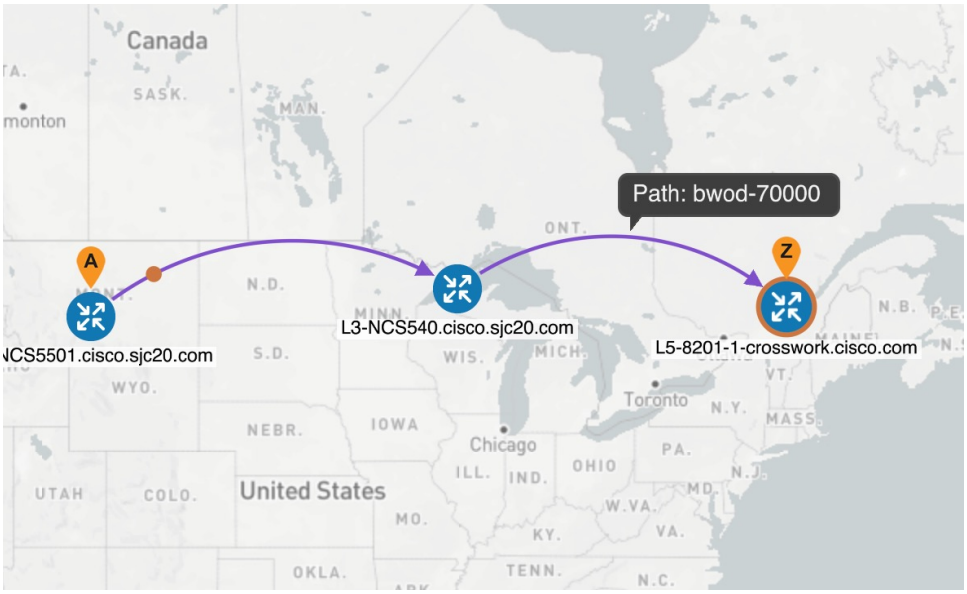
図 *71* : ポリシーパスの詳細



d) [プレビュー（Preview）] をクリックします。BWoD では、別の BWoD ポリシーによって予約されている現在のインターフェイス使用率のみが考慮されます。それ以外の場合、BWoD は計算でインターフェイスのキャパシティのみを考慮します。この例では、すべてのインターフェイスのキャパシティが 1 Gbps です。既存の BWoD ポリシーがないため、BWoD はすべてのノードのキャパシティを考慮し、最短ルートを選択します。

例：

図 *72* : 最初の *BWoD* ポリシー（*bwod-70000*）



e) 提案された BWoD 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。

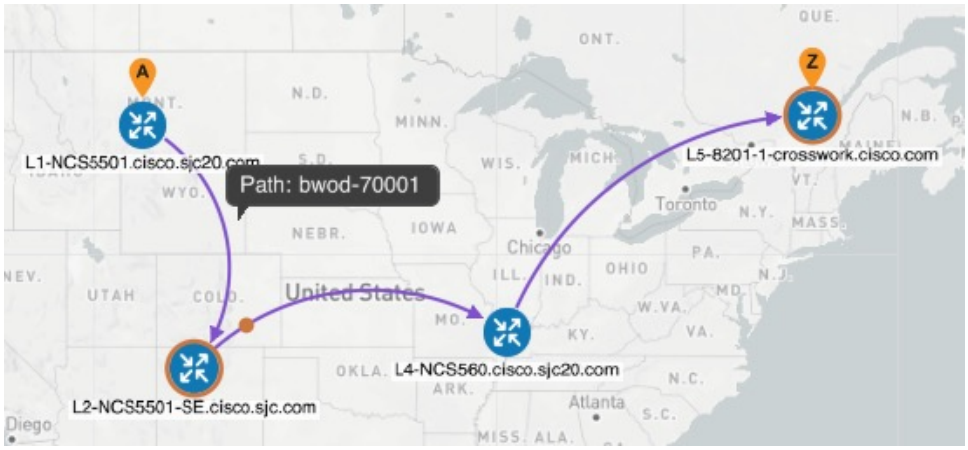
b) 新しい BWoD SR-TE ポリシーを選択し、SR ポリシーの詳細を表示します（[表示（View）] をクリックして選択します）。

ステップ 4 2 番目の BWoD ポリシーを作成します。この例では、次の値を使用します。

- ヘッドエンド：**L1-NCS5501.cisco.sjc20.com**
- エンドポイント：**L5-8201-1-crosswork.cisco.com**
- 色：**70001**
- パス名：**bwod-70001**
- 最適化の目標：**内部ゲートウェイプロトコル（IGP）メトリック**
- 帯域幅：**700 Mbps**

BWoD は、既存の BWoD ポリシー（bwod-70000）とその帯域幅要件をインターフェイス キャパシティの計算で考慮します。したがって、bwod-70001 ポリシー用の新しいパスが作成されます。

図 *73 :* 新しい *bwod-70001* ポリシー

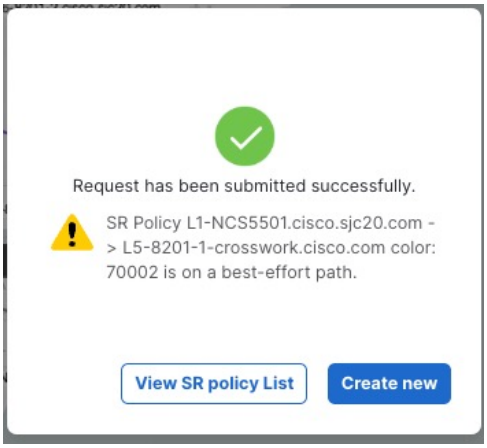


ステップ 5 3 番目の BWoD ポリシーを作成します。この例では、次の値を使用します。

- ヘッドエンド：**L1-NCS5501.cisco.sjc20.com**
- エンドポイント：**L5-8201-1-crosswork.cisco.com**
- 色：**70002**
- パス名：**bwod-70002**
- 最適化の目標：**内部ゲートウェイプロトコル（IGP）メトリック**
- 帯域幅：**1000 Mbps**

BWoD では以前のすべての BWoD ポリシー要件が考慮され、BWoD ポリシー違反オプションが**緩やか**（**Loose**）に設定されているため、BWoD は bwod-70002 ポリシーのベストエフォートパスを作成します。新しいポリシーをプロビジョニングすると、次のメッセージが表示されます。

図 *74 :* ベストエフォートメッセージ



bwod-7000 および bwod-70001 の既存のパスは、新しい bwod-70002 ポリシーに対応するために移動されることに注意してください。

例：

図 *75 : Loose* オプションを使用した *BWoD* ポリシー

ステップ 6 BWoDポリシー違反オプションを、**厳格（Strict）**に変更します（**[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）] > [詳細設定（Advanced）]**の順に選択）。

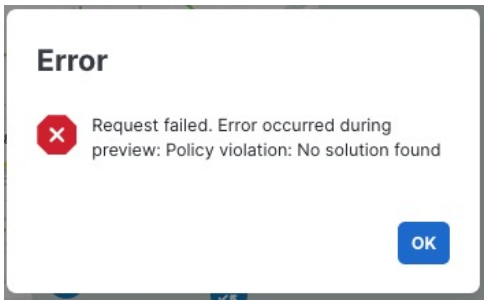
ステップ 7 4 番目の BWoD ポリシーを作成します。この例では、次の値を使用します。

- ヘッドエンド：**L1-NCS5501.cisco.sjc20.com**

- エンドポイント：**L5-8201-1-crosswork.cisco.com**
- 色：**70003**
- パス名：**bwod-70003**
- 最適化の目標：**内部ゲートウェイプロトコル（IGP）メトリック**
- 帯域幅：**1000 Mbps**

BWoD ポリシー違反オプションが**厳格（Strict）**に設定されているため、BWoD は既存の BWoD ポリシーを上書きできず、追加の 1000 Mbps ポリシーを要求すると、「ソリューションが見つかりません（No solution found）」というメッセージが表示されます。

図 *76 :* ソリューションが見つかりません



オンデマンド帯域幅の設定

オンデマンド帯域幅（BWoD）を使用するには、主に次の 2 つの手順があります。

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。

手順

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）]** の順に選択します。

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、**[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 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）]** を選択します。

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 該当する場合は、[SIDアルゴリズム（SID Algorithm）] フィールドにフレキシブルアルゴリズムの制約を入力します。値はデバイスで定義されているフレキシブルアルゴリズムに対応し、128 ～ 255 の範囲が Cisco IOS XR によって適用されます。Cisco Crosswork は、この SID を持つパスを見つけようとします。SID の制約のあるパスが見つからない場合、プロビジョニングされたポリシーは、条件が満たされるまで運用停止状態のままになります。

ステップ 9 [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 10 [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 *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
OptimaModelError	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。 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。

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
NATSTimedOutError	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。
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	シスコの営業担当者にお問い合わせください。

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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。