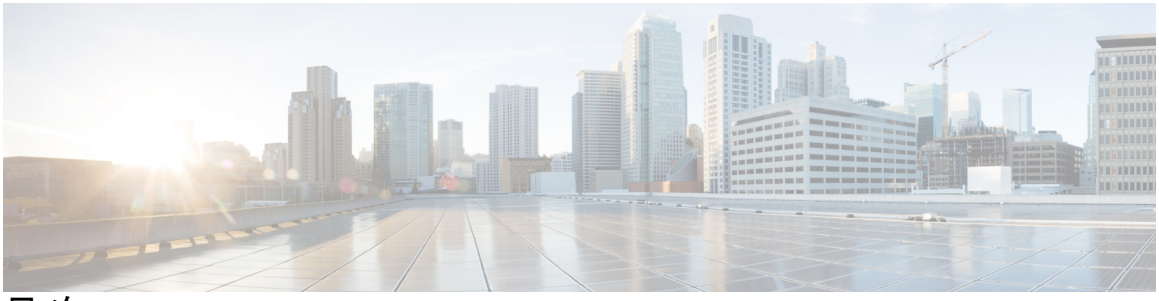
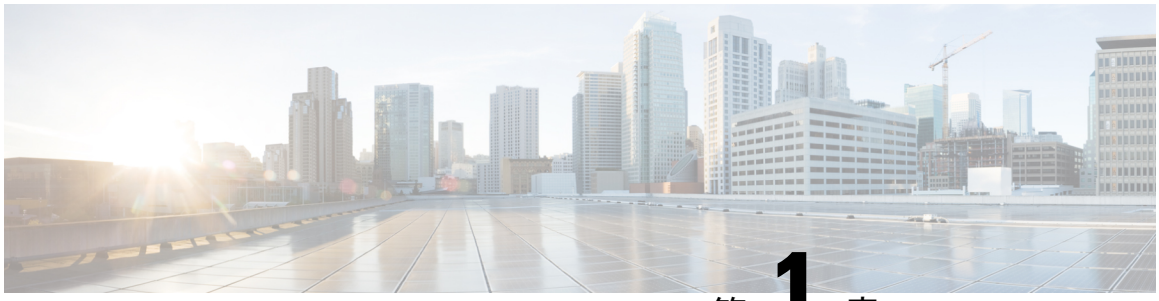
Cisco Crosswork Optimization Engine 4.1 ユーザーガイド

初版：2022 年 9 月 7 日

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



目 次



第 1 章

Cisco Crosswork Optimization Engine の概要

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

対象読者

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）
- トポロジマップのポイント 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

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

Crosswork 最適化エンジン は、次のとおりです。

- 次のような有益なリアルタイムのネットワーク可視化を実現するトポロジマップ
  - デバイス
  - リンクとリンク使用率
  - プロビジョニングされた SR-TE（SR-MPLS および SRv6）ポリシーと RSVP-TE トンネル

（注） 詳細については、「トポロジマップでのデバイスとリンクの表示（13 ページ）」を参照してください。

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

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

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

Crosswork Optimization Engine API

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

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

Crosswork 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、サービスの俊敏性、コスト効率、最適化の向上を実現し、お客様に届くまでの時間を短縮して運用コストを削減します。このソリューションは、インテントベースのネットワーク自動化を組み合わせて、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、および異常検出と自動修復のための重要な機能を提供します。詳細については、「Cisco Crosswork Network Controller」[英語] を参照してください。

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

セグメントルーティングパス計算要素（SR-PCE）

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

Cisco SR-PCE（以前の Cisco XR Traffic Controller（XTC））は、Cisco IOS XR オペレーティングシステムで実行します。SR-PCE は、ネットワークを最適化するために TE トンネルを制御

および再ルーティングするのに役立つステートフル 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 ドメインの一部であるすべてのデバイスを検出します。ただし、TE トンネルをデバイスに展開するには PCEP ピアリングが必要です。

（注） SR-PCE バージョンがサポートされていない場合、機能が期待どおりに動作しない場合があります。SR-PCE バージョンのサポートと互換性に関する『Crosswork Optimization Engine Release Notes』をご確認ください。

セグメント ルーティングについて

セグメントルーティングは、送信元のルーティングパラダイムに基づいてネットワーク上でパケットを転送する方法です。送信元がパスを選択し、セグメントの順序付きリストとしてパケットヘッダー内でエンコードします。セグメントは、任意のタイプの命令の識別子です。例えば、トポロジ セグメントは、宛先へのネクスト ホップを識別します。各セグメントは、32 ビットの符号なし整数で構成されるセグメント ID（SID）で識別されます。

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

セグメント

内部ゲートウェイ プロトコル（IGP）は、2 つのタイプのセグメント、プレフィックス セグメントと隣接関係セグメントを配布します。各ルータ（ノード）と各リンク（隣接関係）には、関連付けられたセグメント識別子（SID）があります。

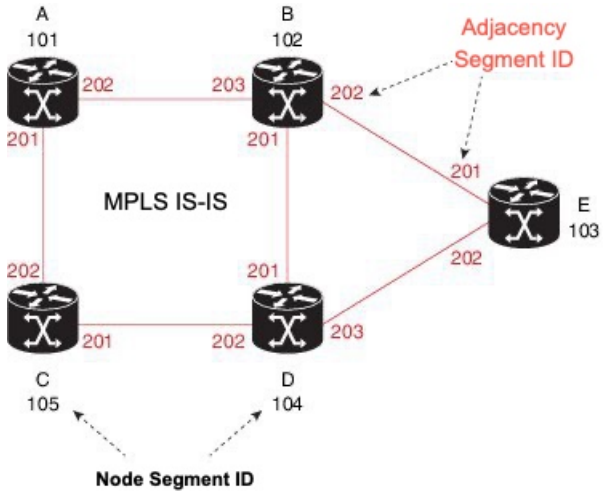
- プレフィックス SID は、IP プレフィックスに関連付けられます。プレフィックス SID は、ラベルのセグメント ルーティング グローバル ブロック（SRGB）の範囲から手動で設定され、IS-IS または OSPF によって配布されます。プレフィックス セグメントは、その宛先への最短パスに沿ってトラフィックを誘導します。ノード SID は、特定のノードを識別する特別なタイプのプレフィックス SID です。ノードのループバック アドレスをプレフィックスとして使用して、ループバック インターフェイスの下に設定されます。

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

- 隣接関係セグメントは、隣接ルータへの出力インターフェイスなどの特定の隣接関係を表す隣接関係 SID と呼ばれるラベルによって識別されます。隣接関係 SID は、IS-IS または OSPF によって配布されます。隣接関係セグメントは、トラフィックを特定の隣接関係に誘導します。

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

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



セグメント ルーティング ポリシー

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

SR ポリシーにはダイナミックと明示的の 2 つのタイプがあります。

ダイナミック SR ポリシー

動的パスは、最適化の目的と一連の制約に基づいています。ヘッドエンドはソリューションを計算し、結果として SID リストまたは SID リストのセットを生成します。トポロジが変更されると、新しいパスが計算されます。ヘッドエンドにトポロジに関する十分な情報がない場合、ヘッドエンドはパス計算エンジン（PCE）に計算させることがあります。パスが見つからない場合、ポリシーは動作上ダウン（動作ステータスダウン）になり、パケットはポリシーに基づいてルーティングされません。

明示的 SR ポリシー

明示的なポリシーを設定する場合は、プレフィックスまたは隣接 SID のリストで構成される明示的なパスを指定します。各 SID はパス上のノードまたはリンクを表します。各セグメントは、送信元から接続先までのエンドツーエンドのパスであり、ネットワーク内のルータに、IGP によって計算された最短パスではなく指定されたパスに従うように指示します。パケット

が SR ポリシーへと誘導される場合、SID リストはヘッドエンドによってパケットにプッシュされます。残りのネットワークは、SID リストに埋め込まれた命令を実行します。

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

Segment Routing over MPLS（SR-MPLS）

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

Segment Routing over IPv6（SRv6）

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

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

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

SRv6 の制限事項

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

トラフィック エンジニアリング用のセグメント ルーティング

SR-TE は、送信元と接続先のペア間のポリシーを介して実行されます。SR-TE では、送信元ルーティングの概念が使用されます。送信元はパスを計算し、パケットヘッダーでセグメントとしてエンコードします。

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

分離

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

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

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

Tree-SID ポリシー

ツリーセグメント識別子（Tree-SID）は、セグメントルーティングに基づく最新のコントローラ駆動型のマルチキャストテクノロジーです。これは、パス計算要素プロトコル（PCEP）を使用するセグメント ルーティング パス計算要素（SR-PCE）を使用して、SR ポリシーを使用してポイントツーマルチポイント（P2MP）ツリーを計算するツリー構築ソリューションです。Tree-SID は、SR ネットワークでマルチキャスト レプリケーション ツリーを構築するために、単一の MPLS ラベルを使用します。コントローラを使用する利点は、ツリーの計算にあらゆる種類の制約を適用できることです。

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 （68 ページ）を参照してください。

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、独自のニーズと制約（特定のメトリックとリンクプロパティ）に従って IGP 最短パスをカスタマイズおよび計算できます。ネッ

トワーク上のパスを計算するために、考えられる多くの制約が使用される可能性があります。たとえば、フレキシブルアルゴリズムでは、複数の論理プレーンを持つネットワークに対する特定のプレーンへのパスを制限できます。アルゴリズムの意味が標準規格によってではなく、ユーザーによって定義されるため、フレキシブルアルゴリズムと呼ばれます。

フレキシブルアルゴリズムの可視化 （61 ページ）を参照してください。

関連リンク

SR-MPLS ポリシーのプロビジョニング （89 ページ）
リンクアフィニティの設定 （91 ページ）

Resource Reservation Protocol（RSVP）について

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

RSVP-TE プロセスには、次の機能が含まれています。

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

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

RSVP-TE 明示的ルーティング（ストリクト、ルーズ）

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

ERO で指定された明示的パスは、ストリクトパスまたはルーズパスです。

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

ルーズホップとは、ERO で指定されたネットワーク ノードがパス内にある必要があるものの、その前のノードと直接接続されている必要がないことを意味します。ERO の処理中にルーズホップに遭遇した場合、ルーズホップを処理するノードは、パスに沿った、それ自身から ERO

内の次のノードまで、1 つ以上のノードを使用して ERO を更新できます。ルーズ パスの利点は、ERO の作成時にパス全体を指定したり、既知にする必要がないことです。ルーズ パスの欠点は、下位のルーティング プロトコルでの一時的な状態中に転送ループが発生する可能性があることです。

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

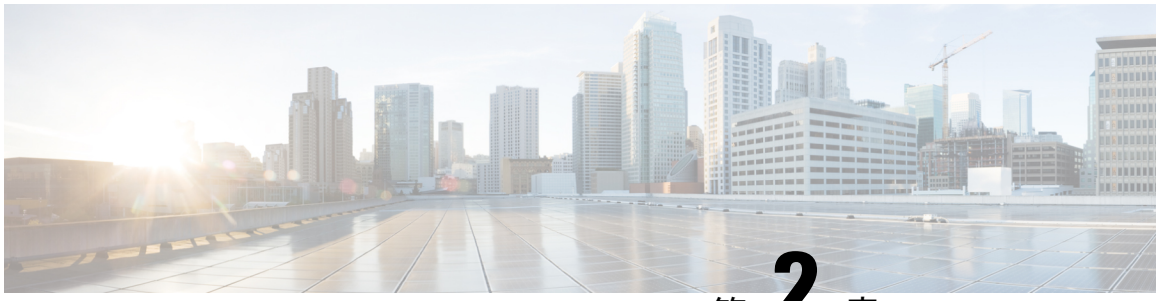
RSVP FRR

ルータのリンクまたは隣接デバイスに障害が発生すると、インターフェイス停止の通知を受信することでルータはこの障害を検出する場合が多くあります。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。この情報はヘッドエンドで使用され、TE トンネルの新しい LSP をシグナリングし、メ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。



第 2 章

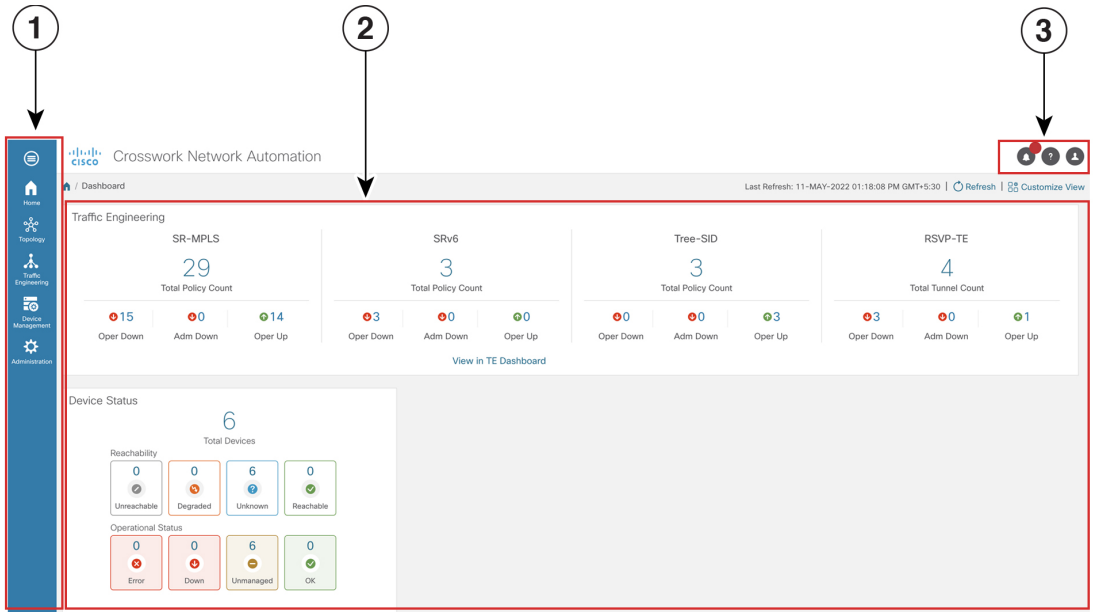
ネットワークビューのセットアップとモニター

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

ダッシュボードでのクイックビューの取得

ホームページにはカスタマイズ可能な一連のダッシュレットが表示され、デバイスの到達可能性や動作ステータスなど、管理対象ネットワークの運用の概要がひと目でわかります。ダッシュボードは一連のダッシュレットで構成され、各ダッシュレットは同じカテゴリに属するさまざまなタイプのデータを表します。

図 *1 : Crosswork* のホームページ



522573

引き出し線番号	説明
1	**メインメニュー**：メインメニューでは、インストールされている Cisco Crosswork アプリケーションと、デバイス管理および管理のタスクに移動できます。メニューオプションは、インストールされている Cisco Crosswork アプリケーションによって若干異なる場合があります。
2	**ダッシュレット**：情報は、インストールされている Cisco Crosswork アプリケーションによって異なります。 • ダッシュレット内の詳細情報をドリルダウンするには、値をクリックします。クリックしたフィルタ処理済みデータのみを表示するウィンドウが表示されます。 • ダッシュレットのレイアウトを追加または変更するには、[ビューのカスタマイズ（Customize View）] をクリックします。ダッシュレットを目的のレイアウトに移動し、[保存（Save）] をクリックします。

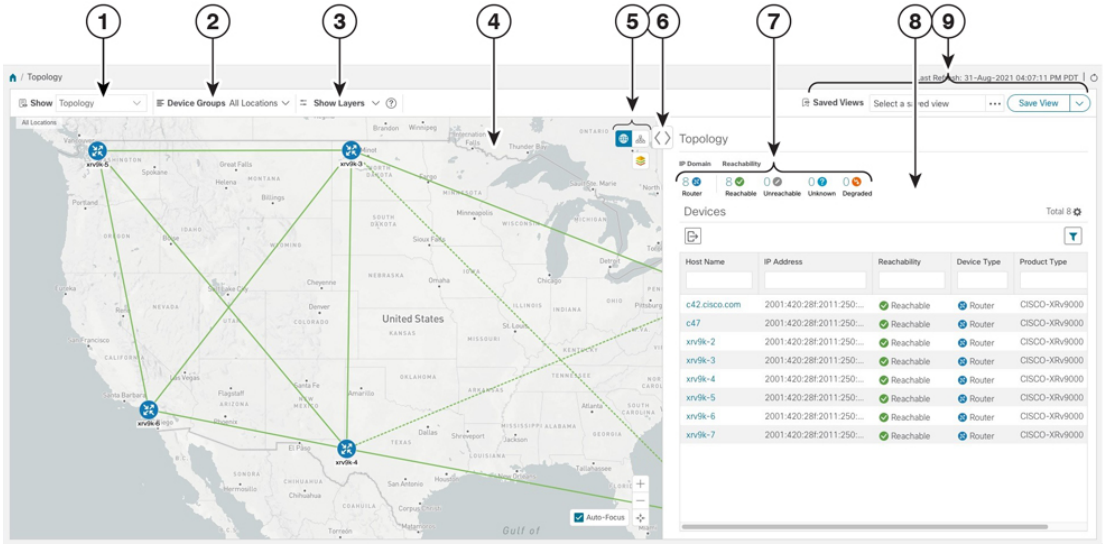
引き出し線番号	説明
3	設定のアイコン： [アラート（Alerts）] アイコンは、注意が必要なシステム操作に関連する現在のエラー状態を通知し、それらの状態に関する詳細情報へのリンクを提供します。 [イベント（Events）] アイコンは、システム操作に関連する新しいイベントを通知し、すべてのシステムイベントの履歴にアクセスできるようにします。 [バージョン情報（About）] アイコンには、Cisco Crosswork 製品の現在のバージョンが表示されます。 [ユーザーアカウント（User Account）] アイコンを使用すると、ユーザー名の表示、パスワードの変更、ログアウトを行えます。

トポロジマップでのデバイスとリンクの表示

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

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

図 *2 : Cisco Crosswork UI* とトポロジマップ



引き出し線番号	説明
1	[トポロジマップビュー（Topology Map View）]：[表示（Show）] ドロップダウンリストから、マップに表示するデータを表示するオプションをクリックします。 [トポロジ（Topology）] を選択すると、ネットワーク内のデバイスとリンクが表示されます。 [トラフィック エンジニアリング（Traffic Engineering）] を選択すると、TE トンネル情報が表示されます。トラフィック エンジニアリングのトポロジマップの詳細については、「トポロジマップでの SR-MPLS および SRv6 ポリシーの表示 （39 ページ）」および「トポロジマップでの RSVP-TE トンネルの表示 （81 ページ）」を参照してください。
2	[デバイスグループ（Device Groups）]：ドロップダウンリストから、マップに表示するデバイスのグループをクリックします。他のすべてのデバイスグループは非表示になります。
3	[表示/非表示（Show/Hide）]：ドロップダウンリストから、マップに表示するネットワークレイヤをクリックします。選択したレイヤに属するすべてのデバイスとリンクが表示されます。デフォルトでは、すべてのレイヤが表示されます。

引き出し線番号	説明
4	[トポロジマップ（Topology Map）]：ネットワークトポロジは、論理マップまたは地理的マップに表示できます。ここでは、デバイスとリンクが地理的コンテキストで表示されます。マップでドリルダウンすると、デバイスとリンクに関する詳細を確認できます。 [デバイス（Device）]： • デバイス設定の概要を表示するには、マウスカーソルをデバイスアイコンの上に合わせます。ホスト名、状態、ノードID、およびデバイスタイプを表示するポップアップウィンドウが表示されます。 • デバイスの詳細を表示するには、デバイスアイコンをクリックします。 • デバイスが物理的に近接している場合、地理的なマップはそれらをクラスタとして表示します。青色の円内の番号（4）は、クラスタ内のデバイスの数を示します。この方法でデバイスを表示すると、マップ上での重複や混乱を防ぐことができます。 [リンク（Link）]： • 実線は、2 つのデバイス間の単一リンクを示します。2 つのデバイス間、またはデバイスとデバイスのクラスタの間に複数のリンクがある場合は、代わりに線は点線で表示されます。破線は、複数のリンクを表す集約リンクか、または同じ物理リンクでの複数のプロトコル（IPv4 や IPv6 など）の使用を示します。 • A と Z はそれぞれヘッドエンドとエンドポイントを示します。 • リンク情報の詳細を表示するには、リンクをクリックします。 （注）　デュアルスタックリンクは、集約されていても 1 本の線で表示されます。
5	：論理マップは、自動レイアウトアルゴリズムに従って配置されたデバイスとそれらのリンクを示し、地理的な位置は無視されます。レイアウトアルゴリズムを変更できます。 ：地理的マップは、単一のデバイス、デバイスクラスタ、リンク、およびトンネルを世界地図に重ねて表示します。マップ上の各デバイスの位置は、デバイスインベントリで定義されているデバイスの GPS 座標（経度と緯度）を反映します。 ：[表示設定（Display Preferences）] ウィンドウでは、デバイス、リンク、使用率、フレキシブルアルゴリズム、および TE トンネルメトリックの表示設定を変更できます。

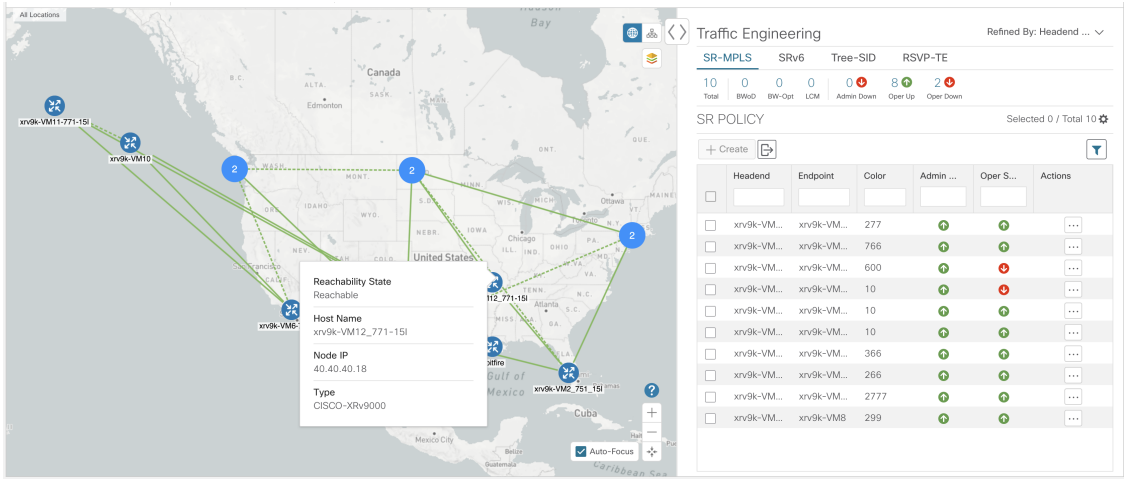
引き出し線番号	説明
6	[サイドパネルの展開/折りたたみ/非表示（Expand/Collapse/Hide Side Panel）]：サイドパネルの内容を展開するか、または折りたたみます。トポロジマップを拡大表示するには、サイドパネルを閉じます。
7	[ミニダッシュボード（Mini Dashboard）] には、IP ドメインとデバイスの到達可能性ステータスの概要が表示されます。フィルタが適用されると、[ミニダッシュボード（Mini Dashboard）] が更新され、[デバイス（Devices）] テーブルに表示される内容が反映されます。 （注） アラームステータス機能が有効になっている場合は、ここにアラーム情報も表示されます。アラームステータスを表示するには、Common EMS サービスアプリケーションをインストールし、アラームを表示するデバイスで Syslog および SNMP トラップのホスト情報を設定する必要があります。詳細については、『*Cisco Crosswork Infrastructure and Applications Installation Guide*』および『*Cisco Crosswork Infrastructure and Applications Administration Guide*』を参照してください。アラームステータス機能は、一部のライセンスパッケージで利用できます。
8	このウィンドウの内容は、トポロジマップの [表示（Show）] に設定されている内容と、デバイス、リンク、SR-MPLS ポリシー、SRv6 ポリシー、または RSVP-TE トンネル の詳細情報を表示することを選択しているかによって異なります。
9	[保存済みカスタムマップビュー（Saved Custom Map Views）]：現在のマップの設定とレイアウト、保存済みビューに保存されているテーブルの設定を使用して名前付きカスタムビューを作成したり、以前に作成したカスタムビューを表示できます。また、[デバイス（Devices）] テーブルと [トラフィック エンジニアリング（Traffic Engineering）] テーブルに適用されるフィルタもすべて保存されます。

デバイスとリンクの詳細の表示

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

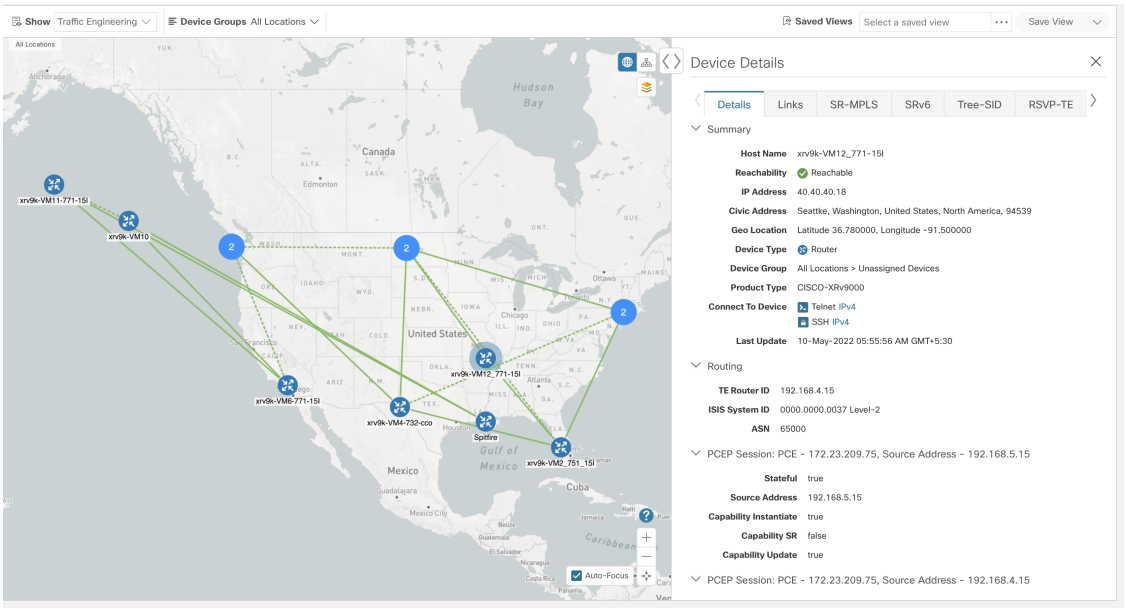
ステップ 1 メインメニューから、[トポロジ（Topology）] または **[トラフィックエンジニアリング（Traffic Engineering）] > [トラフィックエンジニアリング（Traffic Engineering）]** を選択します。

ステップ 2 デバイスのホスト名、到達可能性の状態、IP アドレス、およびタイプをすばやく表示するには、デバイスアイコン上にマウスを合わせます。



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

a) 次の例は、トポロジマップのデバイスの詳細を示しています。



（注） アラームステータス機能が有効になっている場合は、ここにアラーム情報も表示されます。アラームステータスを表示するには、Common EMS サービスアプリケーションをインストールし、アラームを表示するデバイスで Syslog および SNMP トラップのホスト情報を設定する必要があります。詳細については、『*Cisco Crosswork Infrastructure and Applications Installation Guide*』および『*Cisco Crosswork Infrastructure and Applications Administration Guide*』を参照してください。アラームステータス機能は、一部のライセンスパッケージで利用できます。

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

図 *3 :* 複数の *IGP* : *OSPF* プロセス

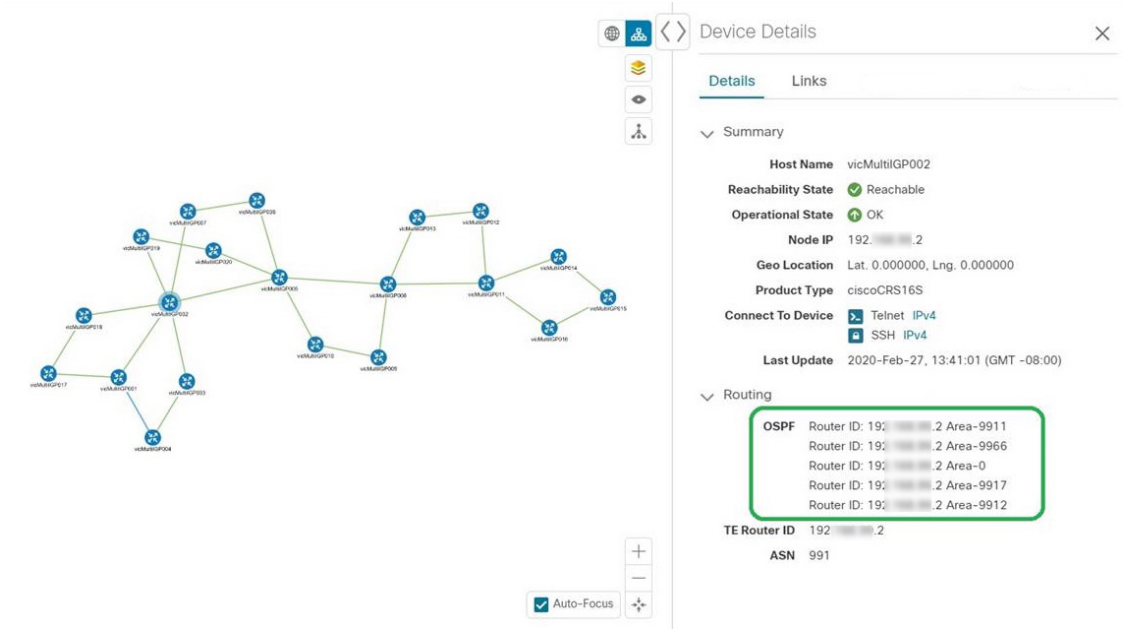


図 *4 :* 複数の *IGP* : *ISIS* プロセス

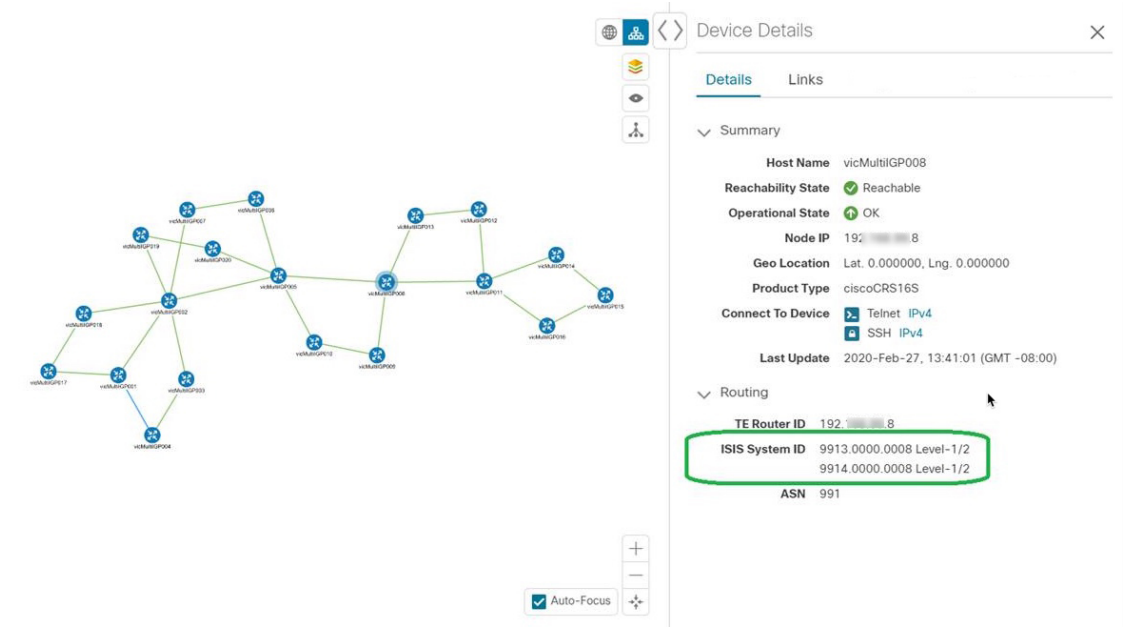
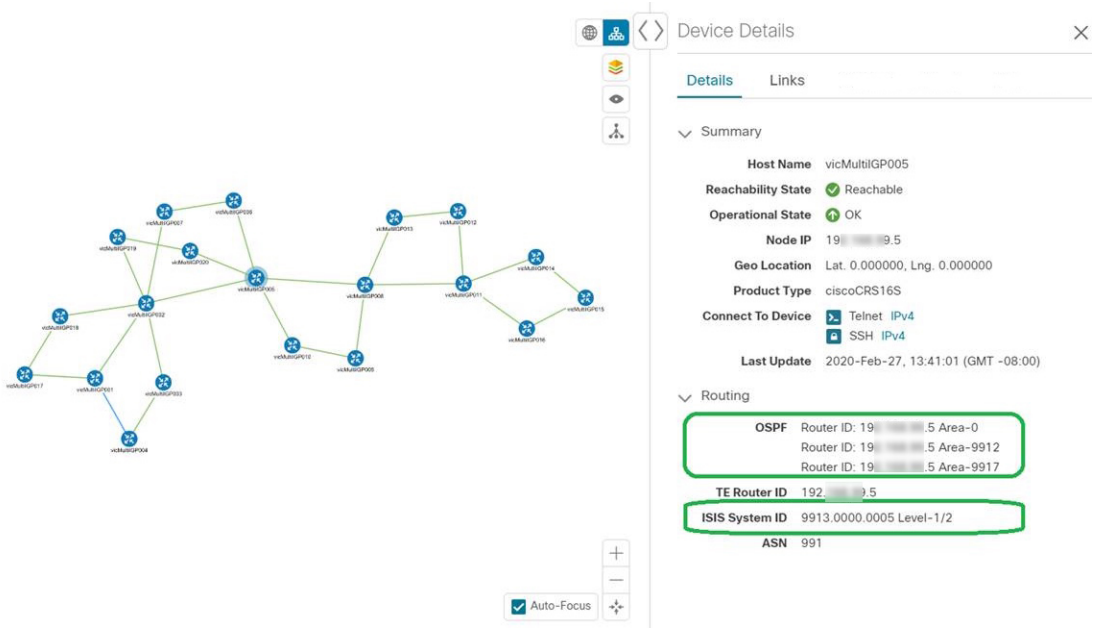
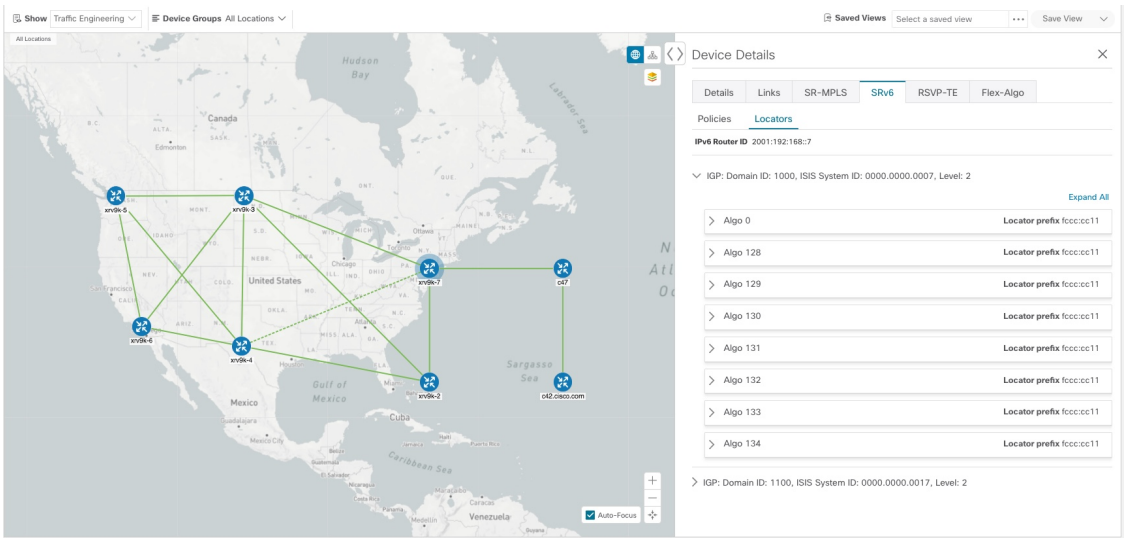


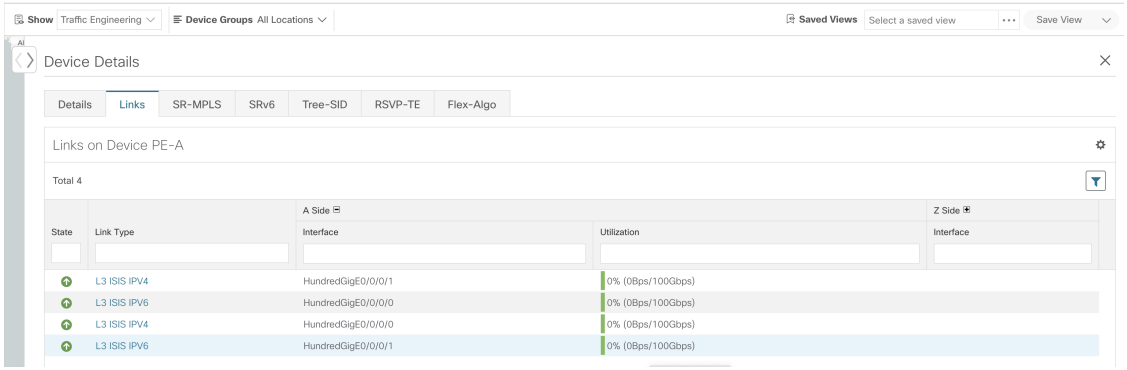
図 *5 :* 複数の *IGP* : *OSPF* および *ISIS* プロセス



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



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



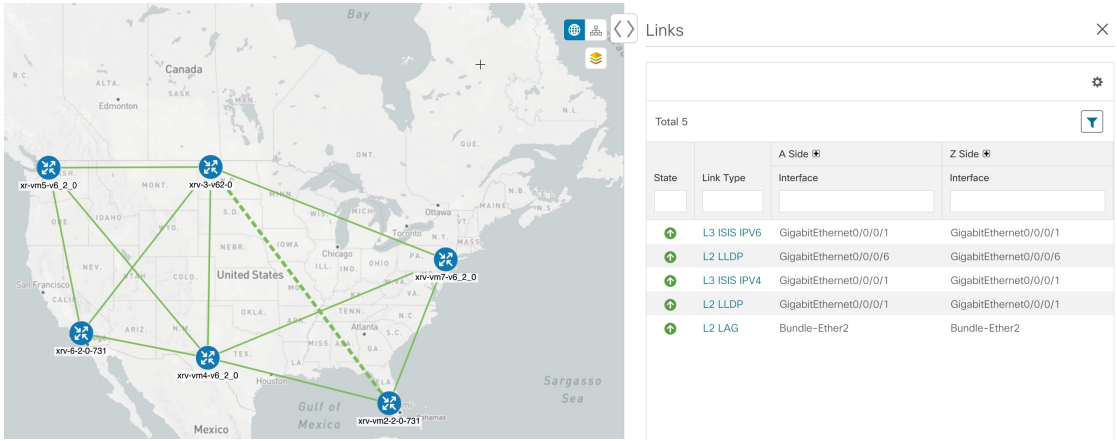
ステップ 5 使用率を表示するには、[A側（A side）] または [Z側（Z side）] を展開します。

ipv4 および ipv6 リンクに表示される使用率は、各アドレスファミリに固有ではなく、インターフェイスまたはサブインターフェイスの集約トラフィックを表します。サブインターフェイス リンクに表示される使用率は、サブインターフェイスのトラフィックのメインインターフェイスでの帯域幅使用率を表します。

ステップ 6 サイドパネルを折りたたんで、[デバイスの詳細（Device Details）] ウィンドウを閉じます。

ステップ 7 破線をクリックします。破線は、複数のリンクを表す集約リンクを示します。

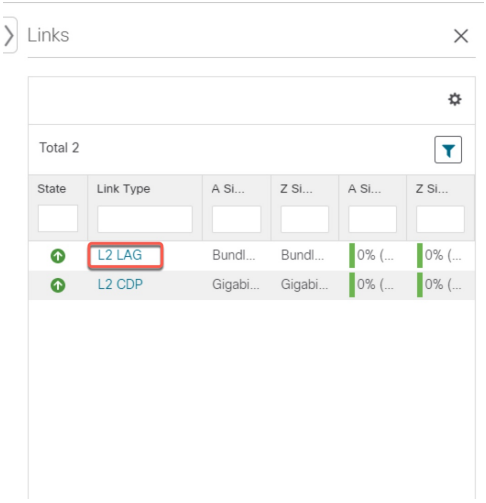
（注） デュアルスタックリンク（集約）は、1 本の線で表示されます。



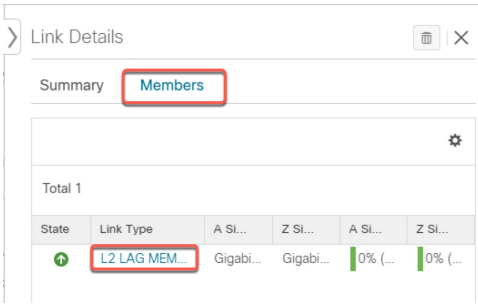
Link Aggregation Group（LAG）のさまざまなバンドルメンバーとメンバーの詳細を表示するには、LAG ディスカバリが有効になっていることを確認します（[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] タブ > [ディスカバリ（Discovery）] > [LAG] チェックボックス）。

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

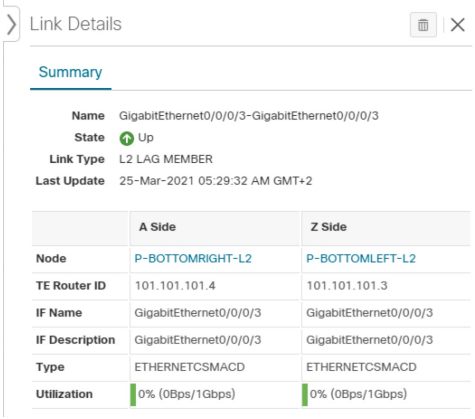
a) [LAG] リンクをクリックします。次に例を示します。



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



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



デバイスグループを使用したトポロジビューのフィルタ処理

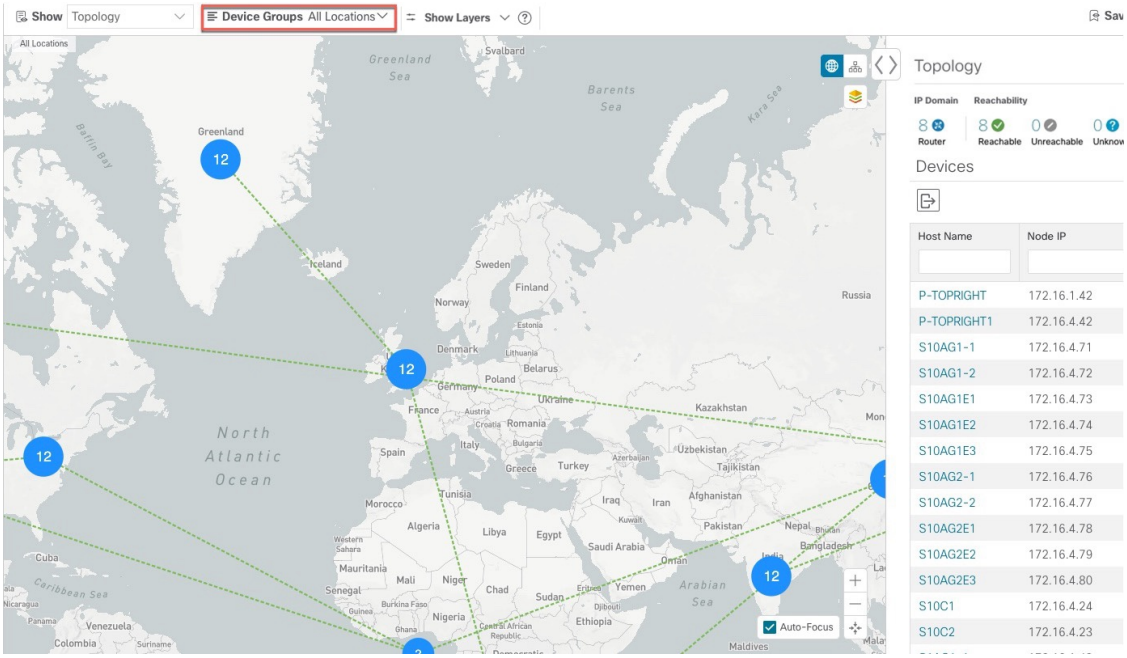
さまざまな目的でデバイスを識別、検索、およびグループ化するためにデバイスグループを作成できます。[Device Group] ウィンドウ（**[Device Management]** > **[Groups]**）には、すべてのデバイス、およびデバイスが属するデバイスグループが表示されます。デフォルトでは、すべてのデバイスが最初は [Unassigned Devices] グループに表示されます。

グループ化とフィルタリングの機能を示すために、グローバルに分散されたデバイスの環境が構築してあり、リージョンに基づいてデバイスをサブグループ化できます。この例には、US West というサブグループがあります。

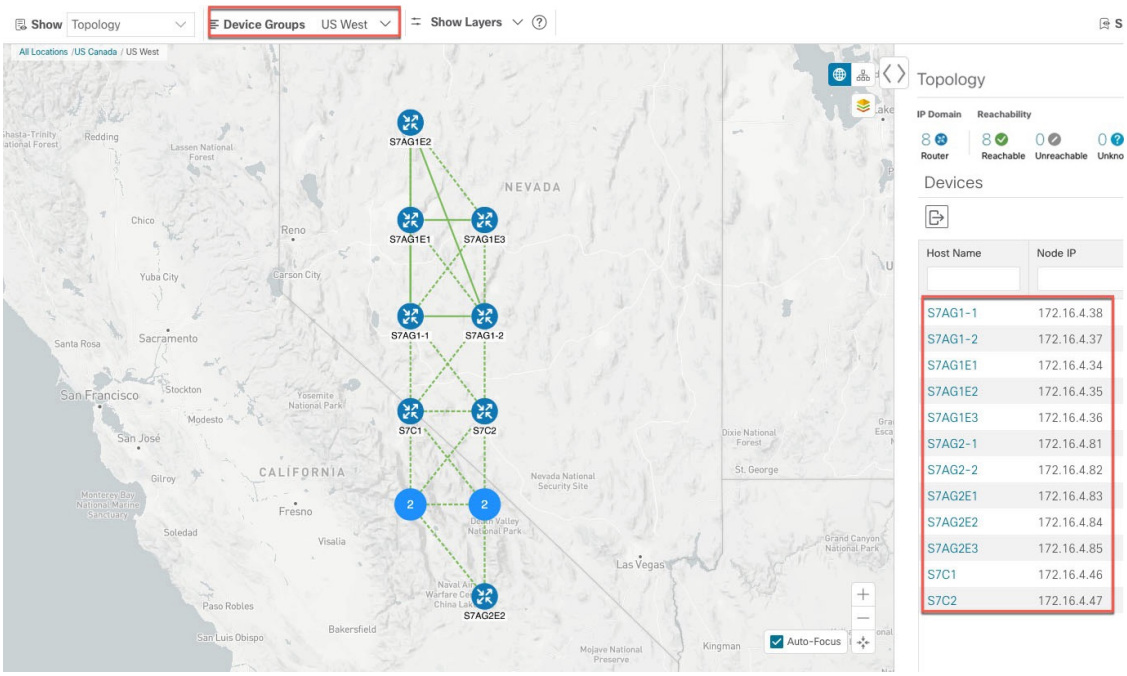
ステップ 1 地理的マップ上のデバイスを表示します。

a) メインメニューから、[Topology] を選択します。

（注） 位置情報のないデバイスは、[Devices] テーブルにのみ表示されます。位置情報のないデバイスをマップに表示するには、[Geo Location] 列にデバイスの地理座標を入力します。



b) [Device Group] ドロップダウンリストからグループ（US West）を選択します。そのグループ内のデバイスと関連リンクのみが地理的マップに表示されます。[Devices]テーブルもフィルタ処理され、グループ内のデバイスのみが表示されます。

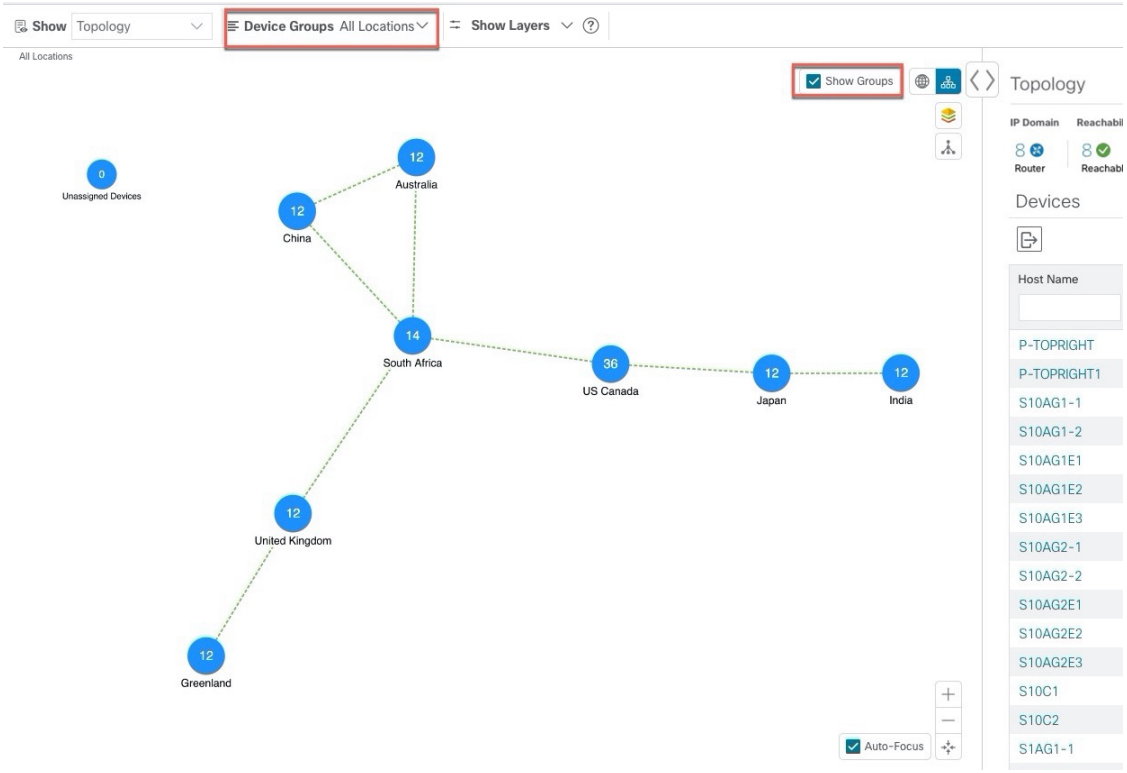


ステップ 2 論理マップ上のデバイスを表示します。

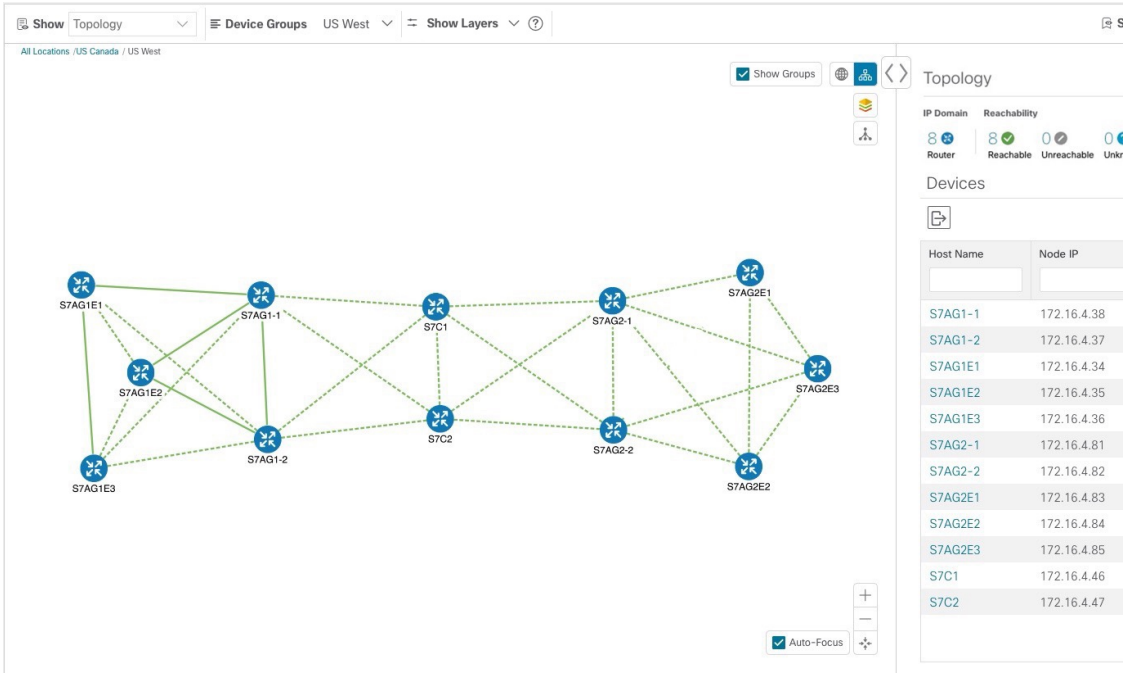
a) メインメニューから、[Topology] を選択します。

b) をクリックします。

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



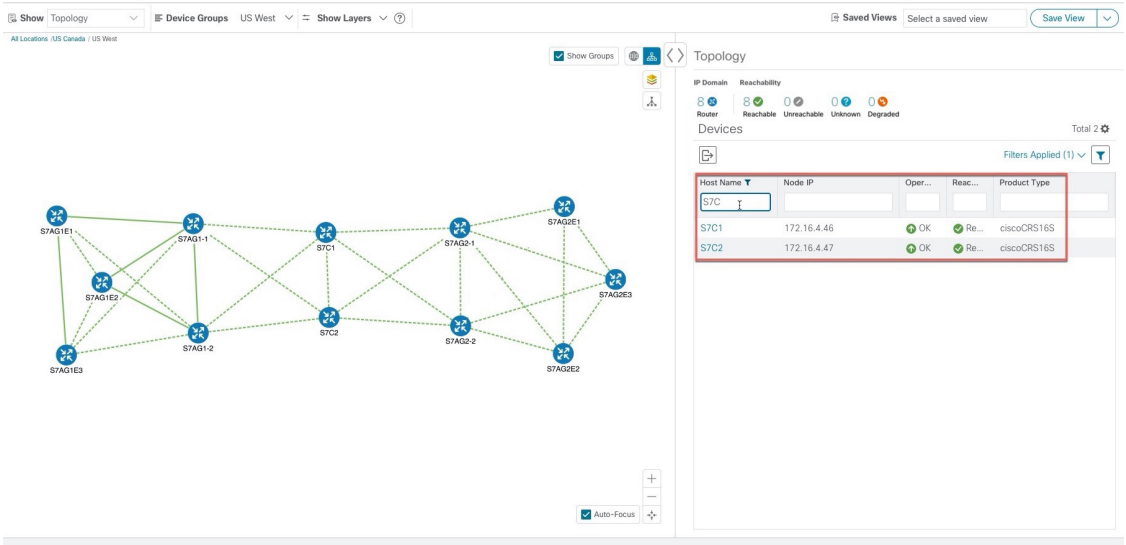
d) [Device Group] ドロップダウンリストからグループ（US West）を選択します。このグループに属するデバイスがトポロジマップと [Devices] テーブルに表示されます。



e) テキストボックスに部分的なホスト名または IP アドレスを入力して、[Device] テーブルのデバイスをフィルタ処理します（たとえば、現在の設定の [Host Name] テキストボックスに **S7C** と入力します）。[デバイス（Device）] テーブルには、フィルタ処理の基準に一致するデバイスのみが表示されます。た

だし、[デバイス（Device）]テーブルをフィルタ処理しても、トポロジマップ上のデバイスは視覚的にフィルタ処理されません。地理的マップまたは論理マップ上のデバイスを視覚的にフィルタ処理するには、デバイスグループを使用します。

（注）　リスト内のデバイスをダブルクリックして、選択したデバイスを地理的マップまたは論理マップ上で再センタリングすることもできます。



デバイスグループの作成と変更

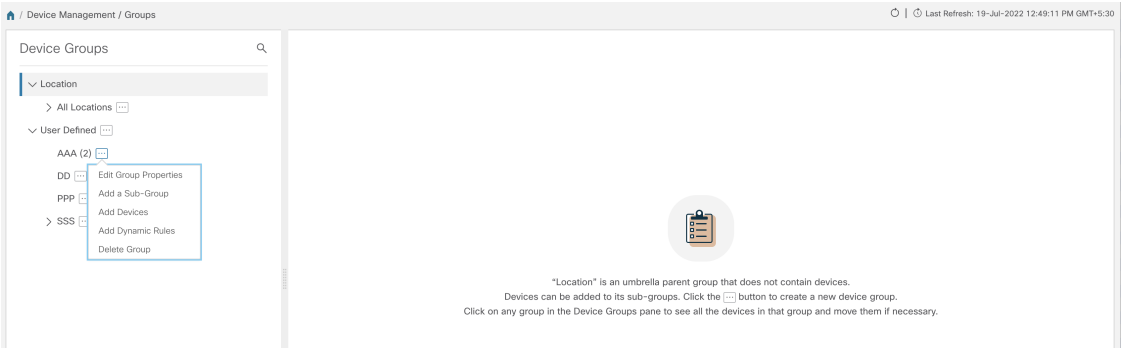
デバイスグループ、およびグループへのデバイスの割り当ては、手動（この項で説明）または自動（次の項で説明）で実行できます。

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

ステップ 2　新しいサブグループを追加するには、[すべての場所（All Locations）]の横にある をクリックします。[すべての場所（All Locations）] の下に新しいサブグループが追加されます。

ステップ 3　デバイスをグループに追加するには、右ペインの [未割り当てのデバイス（Unassigned Devices）] でデバイスを選択し、[グループに移動（Move to Group）] ドロップダウンから適切なグループを選択します。

ステップ 4　既存グループの下で、サブグループを編集、削除、または追加するには、[デバイスグループ（Device Groups）] ツリーでグループの横にある をクリックします。



ステップ 5 グループの追加、削除、または編集（名前の変更または移動）を選択します。グループを削除すると、そのグループに属しているすべてのデバイスが [未割り当てデバイス（Unassigned Devices）] グループに移動します。また、グループを削除すると、そのグループのサブグループがすべて削除されます。

（注） デバイスは、1 つのデバイスグループにのみ属することができます。

ステップ 6 [保存（Save）] をクリックします。

ダイナミック デバイス グループの有効化

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

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

始める前に

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

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

ステップ 2 [すべての場所（All Locations）] > [動的グループ化ルールの管理（Manage Dynamic Grouping Rule）] の横にある をクリックします。

ステップ 3 [他の詳細と例の表示（Show more details and examples）] をクリックして、必要な [ホスト名（Host Name）] フィールドと [グループ名（Group Name）] フィールドに入力します。

ステップ 4 [未割り当てデバイス（Unassigned Devices）] グループに既存のデバイスがある場合は、[ルールのテスト（Test Rule）] をクリックして、作成されるグループ名のタイプのサンプリングを表示します。

ステップ 5 [ルールの有効化（Enable Rule）] トグルをオンにして、ルールを有効にします。ルールが有効になると、システムは未割り当てのデバイスを 1 分おきに確認し、ルールに基づいてそれらを適切なグループに割り当てます。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 この方法で作成されたグループは、最初は [未割り当てグループ（Unassigned Groups）] の下に表示されます（ルールが初めて有効になったときに作成されます）。新たに作成したグループを必要なグループ階層に移動します。

ステップ 8 新しく作成した未割り当てグループを適切なグループに移動するには、次の手順を実行します。

a) すべてのロケーションの横にある をクリックし、[サブグループを追加（Add a Sub-Group）] をクリックします。
b) 新しいグループに詳細を入力して [作成（Create）] をクリックします。
c) 左ペインから未割り当てのデバイスをクリックします。
d) 右側のペインから、移動するデバイスを選択し、[グループに移動（Move to Group）] をクリックして適切なグループに移動します。

マップ表示設定のカスタマイズ

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

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

リンクとデバイスの表示のカスタマイズ

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

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

TE トンネルのデバイスグループの表示動作の設定

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

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

トラフィック エンジニアリングの表示のカスタマイズ

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

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

（注） デュアルスタックリンク（集約）は、1 本の線で表示されます。

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

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

- フレキシブルアルゴリズムのパスを表示するには、[Flex Algo] をクリックします。詳細については、フレキシブルアルゴリズムの可視化 （59 ページ）を参照してください。

簡易アクセスのトポロジビューの保存

マップ上のデバイスとリンクを再配置すると、通常、変更は保存されません。便利なマップレイアウトに簡単にアクセスするには、名前付きカスタムビューとして保存すると、毎回マップ

を再配置することなくすばやく取得できます。これは、多数のデバイスを含む大規模なネットワークを管理する場合に特に役立ちます。

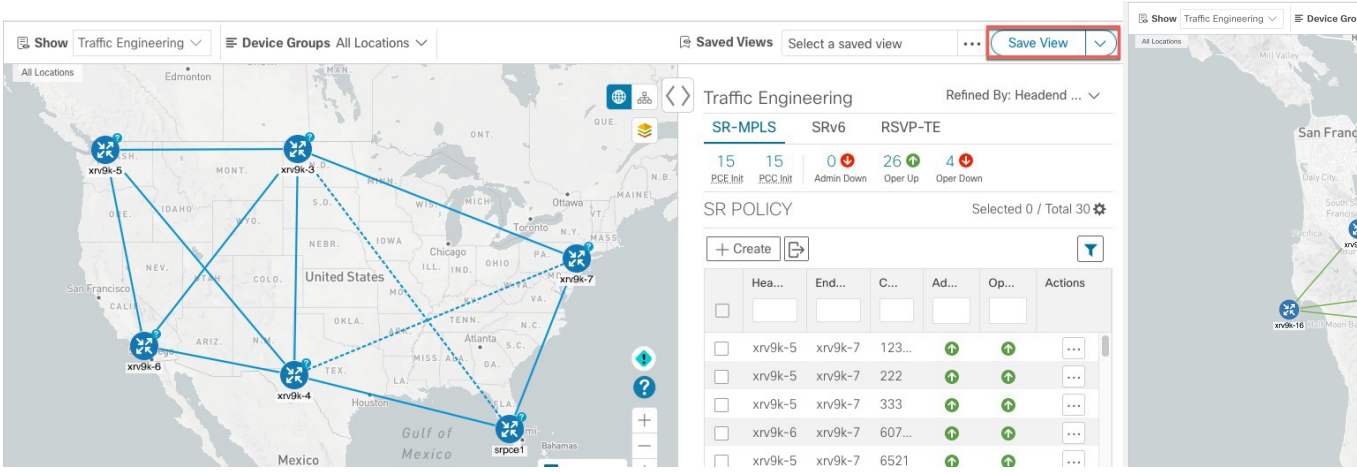
カスタムビューを保存すると、次の設定が保存されます。

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

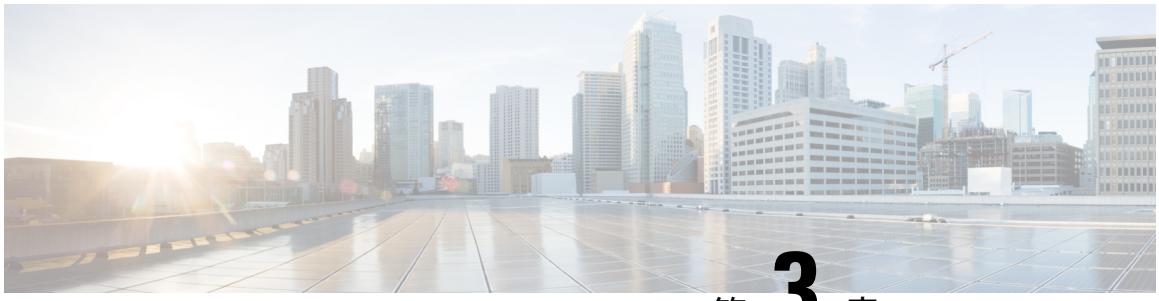
（注） すべてのカスタムビューは、すべてのユーザーに表示されます。ただし、ビューを変更できるのは管理者ロールを持つユーザーまたはカスタムビューを作成したユーザーのみです。

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

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



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



第 3 章

トラフィック エンジニアリング サービスの可視化

トラフィック エンジニアリングのトポロジマップから、ネットワーク内の次の TE サービスを可視化できます。

- SR-MPLS および SRv6 ポリシーの可視化
- フレキシブルアルゴリズムの可視化
- RSVP-TE トンネルの可視化
- 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 （68 ページ）

これらのサービスを可視化機能と Crosswork UI を使用することで、TE ポリシーとトンネルの、監視と管理のプロセスが簡素化されます。

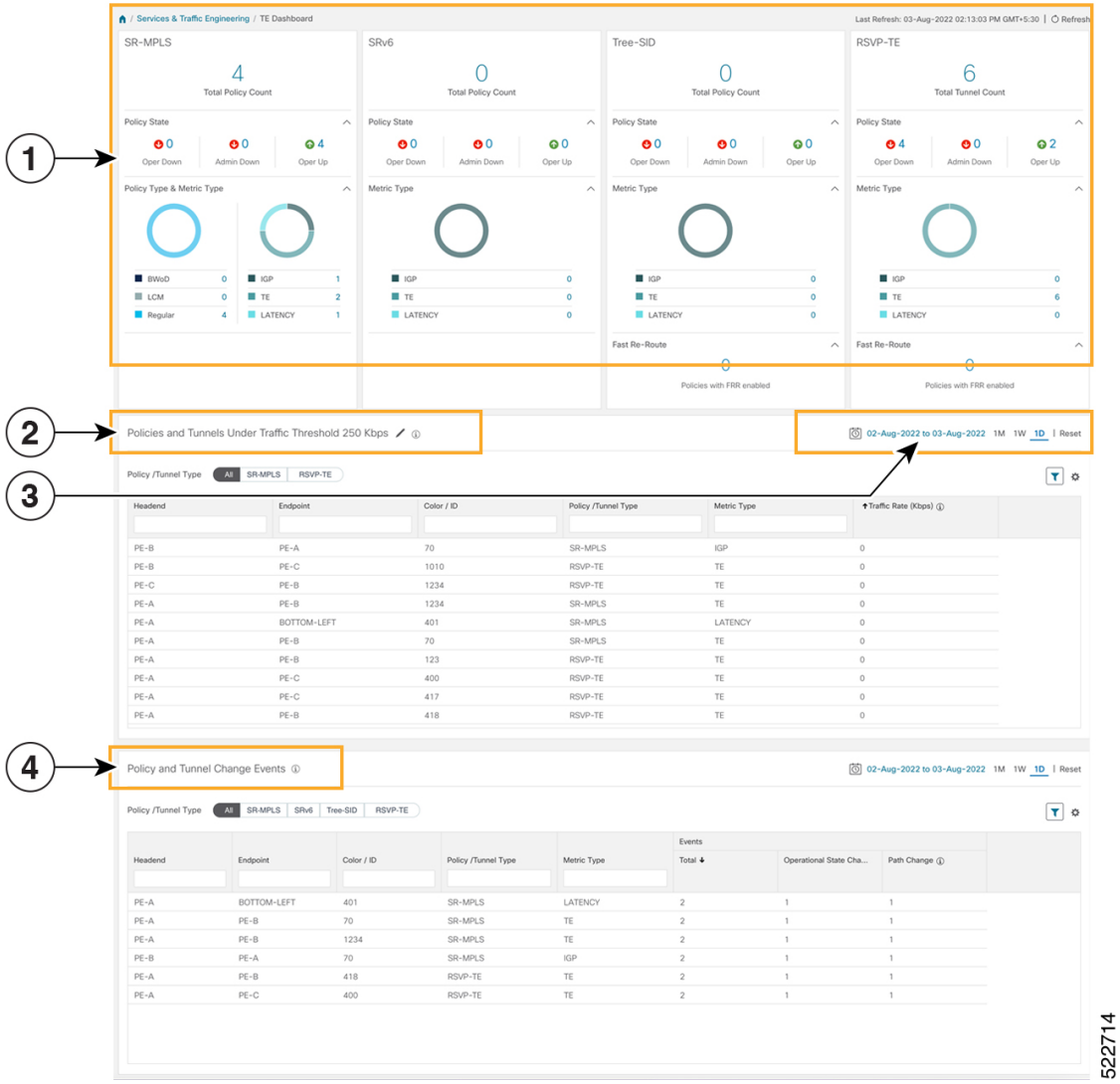
このセクションはすべての TE サービスに適用されます。説明する内容は以下のとおりです。

- 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 （31 ページ）
- TE イベントと使用率履歴の表示 （33 ページ）
- TE データのダッシュボード設定を構成する （35 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 （37 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

TE ダッシュボードにより、RSVP-TE トンネル、SR-MPLS、SRv6、およびツリー 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。



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、SR-MPLS、BWoD、および LCM 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や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。

引き出し線番号	説明
2	**履歴データの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、使用されていないポリシーまたは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、十分に活用されていない LSP しきい値を更新します。 （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 か月、1 週間、および 1 日）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。

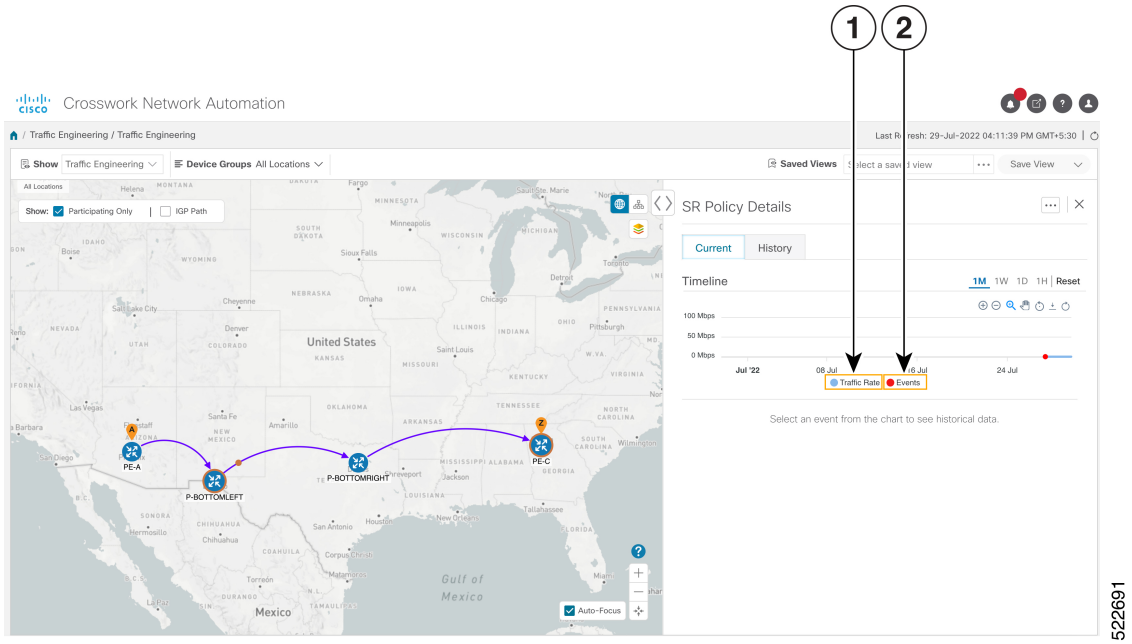
（注） 既知の制限事項のリストについては、『Cisco Crosswork Optimization Engine Release Notes』を参照してください。

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。

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。

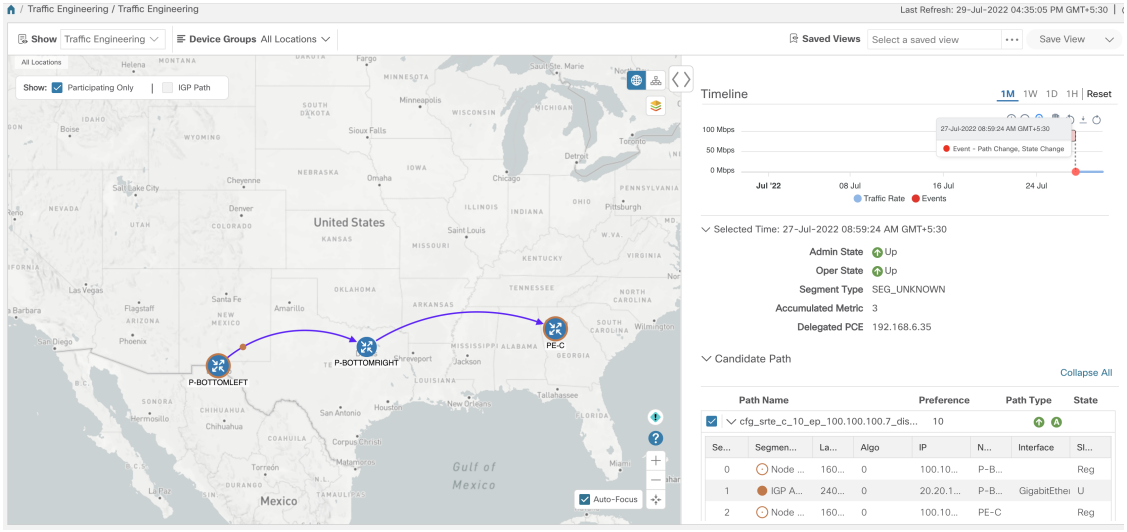
ステップ 2 [トラフィックエンジニアリング（Traffic Engineering）] テーブルの [アクション（Actions）] 列で、ポリシーまたはトンネルの … > [詳細の表示（View Details）] > [履歴データ（Historical Data）] タブをクリックします。タブには、そのデバイスの関連する履歴データが表示されます。次の例は、SR-MPLS ポリシーのトラフィックレートとイベント履歴を示しています。



引き出し線番号	説明
1	[トラフィックレート（Traffic Rate）]：ポリシーのトラフィックレートを表示します。 （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。
2	[イベント（Events）]： パスまたは状態の変更イベントを表示します。

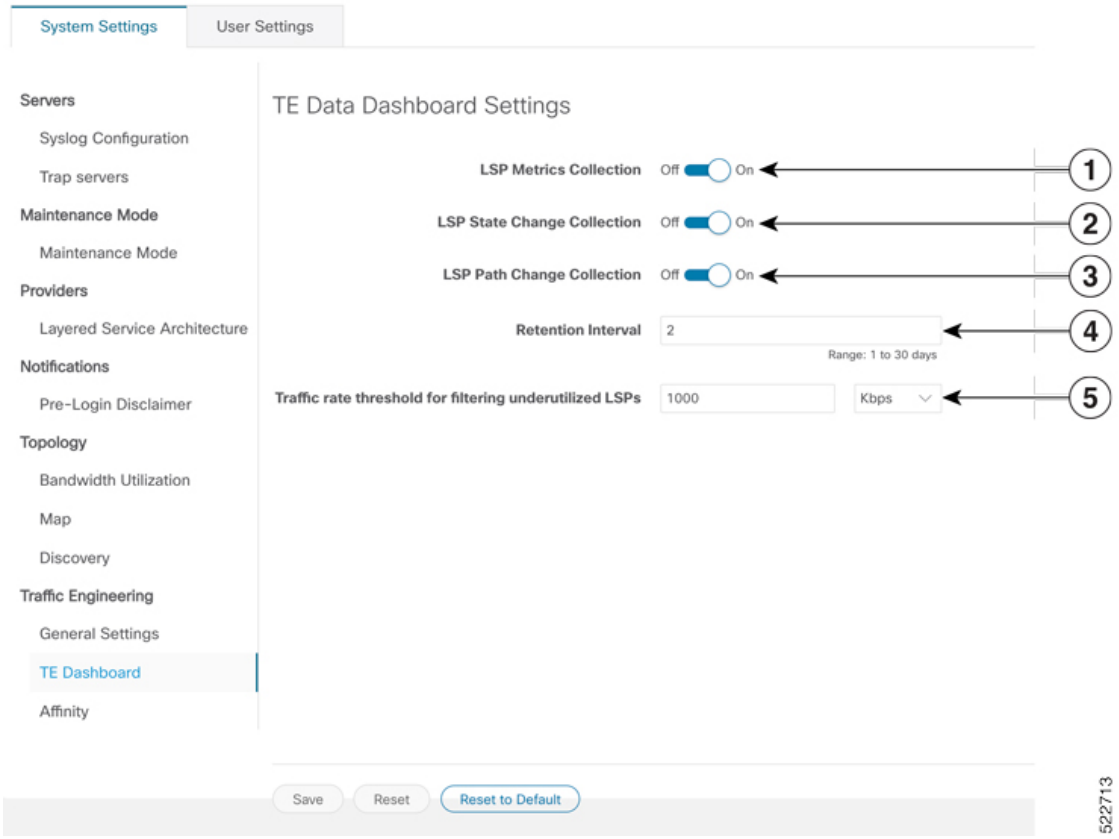
ステップ 3　次の図に示すように、その時点でのポリシーまたはトンネルの状態を表示するには、イベントをクリックします。

ポリシーのパスが左側のペインに表示されます。



TE データのダッシュボード設定を構成する

ポリシーとトンネルメトリック、状態の変更、パスの変更、データ保持間隔、および十分に活用されていない LSP の使用率のしきい値の収集に関する TE ダッシュボード（および履歴データ）設定を構成するには、**[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）] > [TEダッシュボード（TE Dashboard）] を選択します。



引き出し線番号	説明
1	[LSPメトリック収集（LSP Metric Collection）]：このフィールドをオンにして、TE ダッシュボードのメトリックデータをキャプチャします。
2	[LSP状態変更収集（LSP State Change Collection）]：このフィールドをオンにして、TE ダッシュボードで状態変更の詳細をキャプチャします。
3	[LSPパス変更収集（LSP Path Change Collecttion）]：このフィールドをオンにして、TE ダッシュボードでパス変更の詳細をキャプチャします。
	[保持間隔（Retention Interval）]：履歴データが収集され、削除される前に保持される間隔です。デフォルトの保持間隔は 2 日に設定されています。 （注）　保持間隔を短くすると、新しい保持間隔より古いデータはすべて失われます。たとえば、保持間隔が 30 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。
4	トラフィックがこのフィールドで指定されたしきい値を超えていない LSP は、TE ダッシュボードの活用されていない LSP のダッシュレットの下に表示されます。しきい値はダッシュレットでも設定できます。

トラフィック エンジニアリング デバイスの詳細の表示

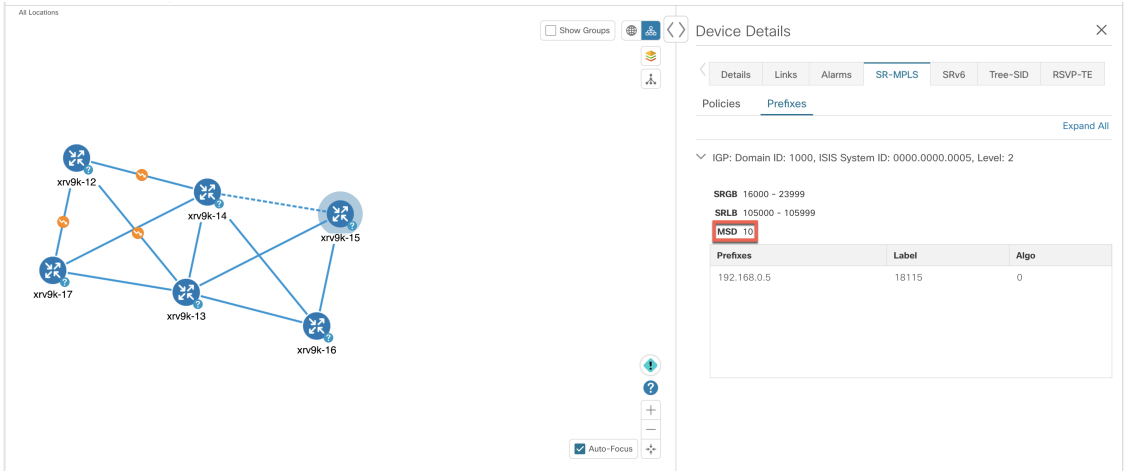
トラフィック エンジニアリング デバイスの詳細（SR-MPLS、SRv6、RSVP-TE、およびフレキシブルアルゴリズム情報）を表示するには、次の手順を実行します。

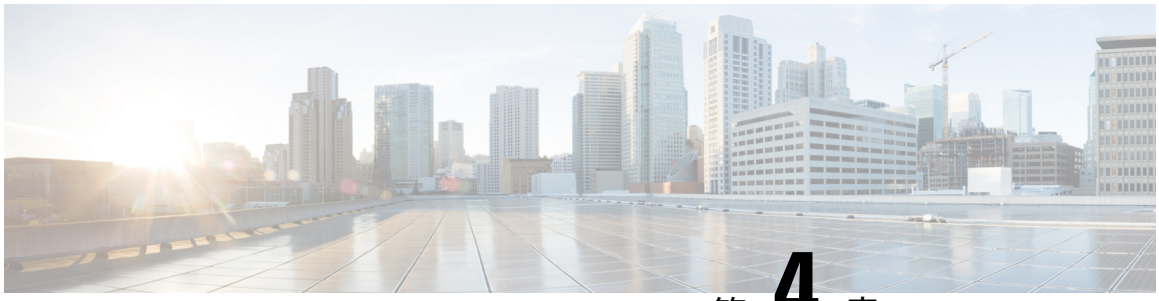
ステップ 1 メインメニューから、[トラフィックエンジニアリング（Traffic Engineering）] > [トラフィックエンジニアリング（Traffic Engineering）] を選択します。

ステップ 2 トラフィック エンジニアリング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 [デバイスの詳細（Device Details）] ページで、目的のトラフィック エンジニアリングのタブをクリックします。各タブには、そのデバイスの関連データが表示されます。

次の例は、デバイスの MSD 値を含む SR-MPLS プレフィックス情報を示しています。





第 4 章

SR-MPLS および SRv6 ポリシーの可視化

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

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。

ここでは、次の内容について説明します。

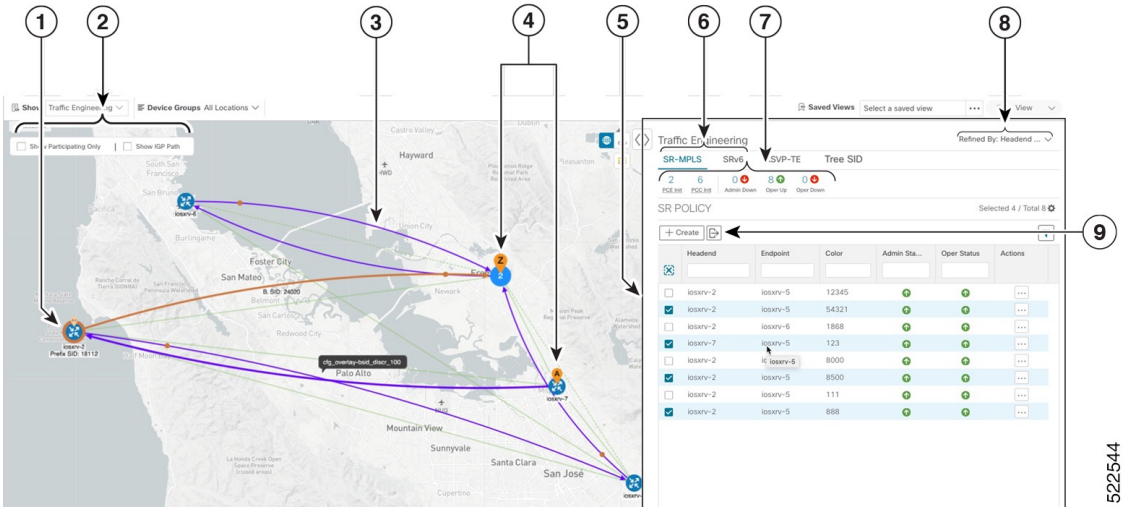
トポロジマップでの SR-MPLS および SRv6 ポリシーの表示

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

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

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

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



引き出し線番号	説明
1	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。
2	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。 • [IGPパスの表示（Show IGP Path）]：選択した SR-TE ポリシーの IGP パスを表示します。 • [参加デバイスのみ表示（Show Participating Only）]：選択した SR-TE ポリシーに属するリンクのみを表示します。他のすべてのリンクとデバイスは表示されなくなります。

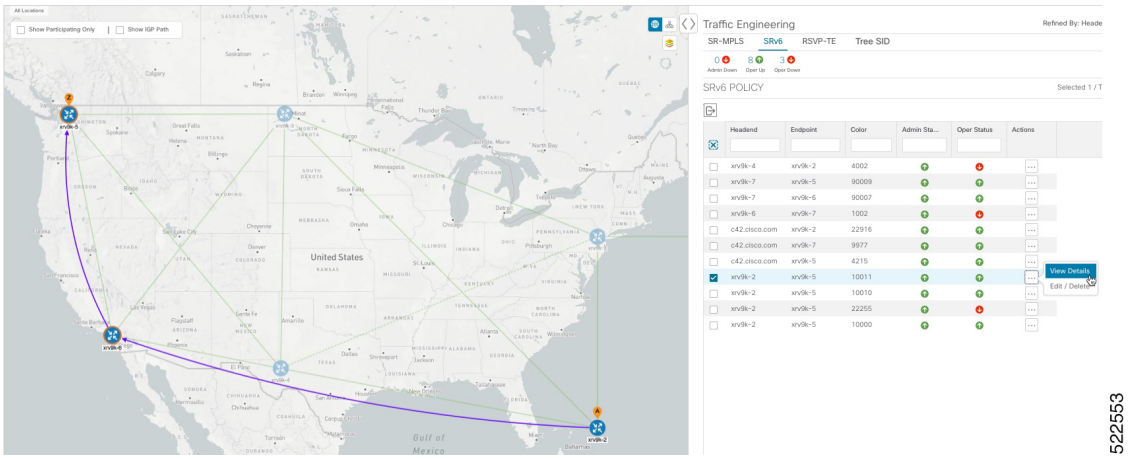
引き出し線番号	説明
3	SR-TE ポリシーは [SR-MPLS] または [SRv6] テーブルで選択されると、送信元と宛先を示す紫色の矢印線としてマップに表示されます。 隣接関係セグメント ID（SID）は、パスに沿ったリンクにオレンジ色の円（）として表示されます。
4	[SR-MPLS および SRv6 ポリシーの送信元と宛先（SR-MPLS and SRv6 Policy Origin and Destination）]：デバイスクラスタに A と Z の両方が表示される場合、クラスタ内の 1 つ以上のノードが送信元で、他のノードが宛先です。A+ は、1 つのノードから発信される複数の 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。トポロジマップで選択した内容、または SR-TE ポリシーを表示および管理しているプロセスに応じて、次の操作を実行できます。 • SR-MPLS または SRv6 ポリシーの可視化の例 （43 ページ） • SR-MPLS ポリシーのプロビジョニング （89 ページ） • デバイスとリンクの詳細の表示 （16 ページ）
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	[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
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。 • [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。

SR-MPLS および SRv6 ポリシーの詳細の表示

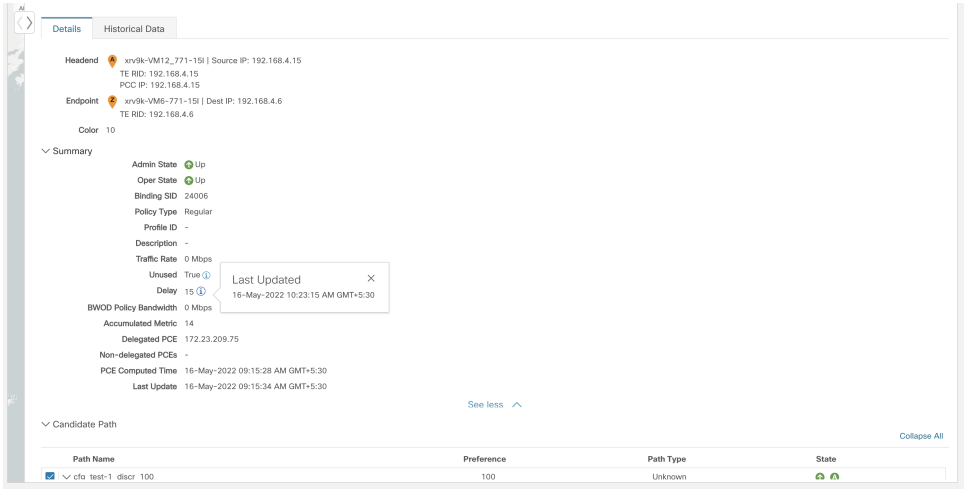
分離グループ、メトリックタイプ、候補パス、セグメントホップ情報など、SR-MPLS または SRv6 ポリシーの詳細を表示します。

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



ステップ 2 SR-MPLS または SRv6 ポリシーの詳細を表示します。

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



SR-MPLS または SRv6 ポリシーの可視化の例

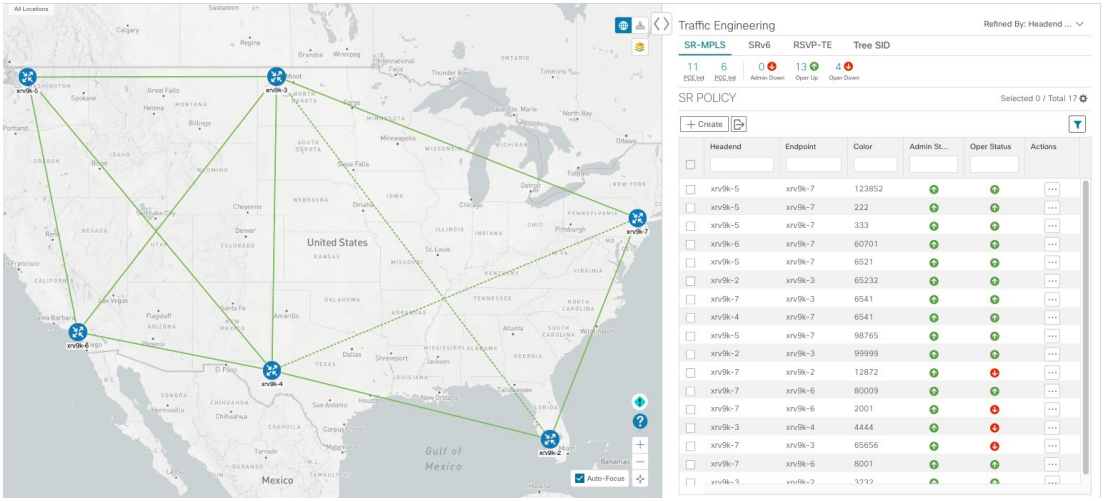
次の例では、トポロジマップから使用できる SR-TE（SR-MPLS および SRv6）ポリシー仮想化の一部の機能について説明します。トポロジマップには、UI を使用してプロビジョニングされた SR-TE ポリシーと、SR-PCE によってネットワークから検出されたポリシーが表示されます。トポロジマップから、参加している SR-TE ポリシーの詳細と可視化にドリルダウンできます。

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

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

拡大表示するには画像をクリックします。

図 7: トポロジマップの例



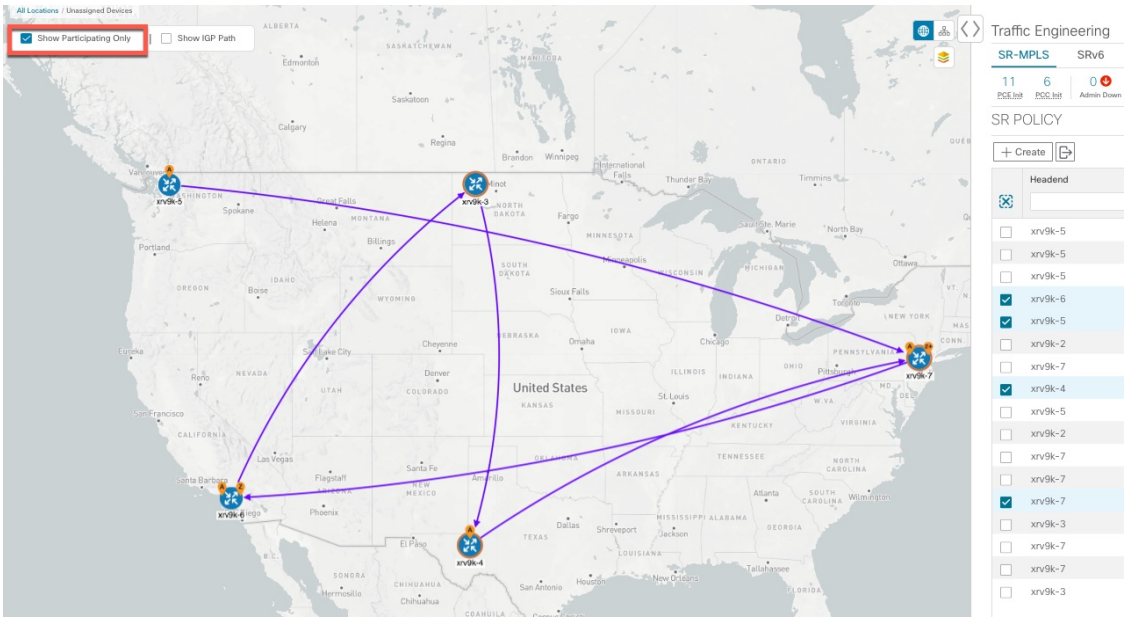
ステップ 1 可視化する SR-MPLS ポリシーを選択し、マップ上で分離します。

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）]** > **[トラフィック エンジニアリング（Traffic Engineering）]** を選択します。

b) [SR Policy] テーブルで、目的の SR-MPLS ポリシーの横にあるチェックボックスをオンにします。

c) [Show Participating Only] の横にあるチェックボックスをオンにして、選択した SR-TE ポリシーの一部ではない他のリンクとデバイスを非表示にします。
次の例では、トポロジマップに次のように表示されます。

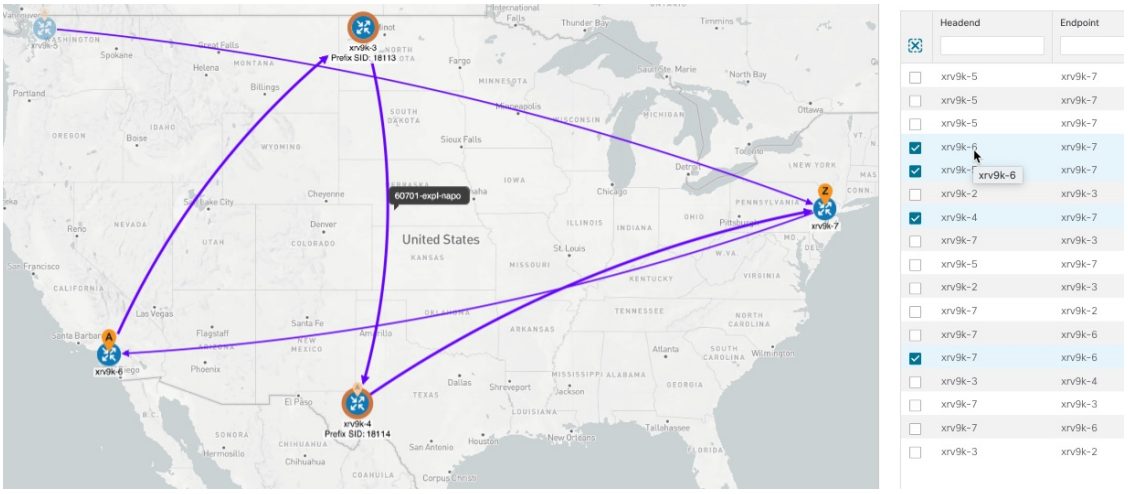
- 4つの SR-MPLS ポリシーが選択されています。
- SR-MPLS ポリシーは、パスの方向を示す矢印付きの紫色のリンクとして表示されます。
- xrv9k-7ノードは、選択した 2 つのポリシーの宛先です。xrv9k-3 と xrv9k-2 はどちらも、選択したポリシーの宛先です。SR-MPLS ポリシーの送信元と宛先は、それぞれ A と Z でマークされます。**A+** は、デバイスから発信される複数のポリシーがあることを示します。Z+は、デバイスが複数のポリシーの宛先であることを示します。
- オレンジ色のアウトライン（）は、**xrv9k-3**、**xrv9k-7**、およ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



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

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

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



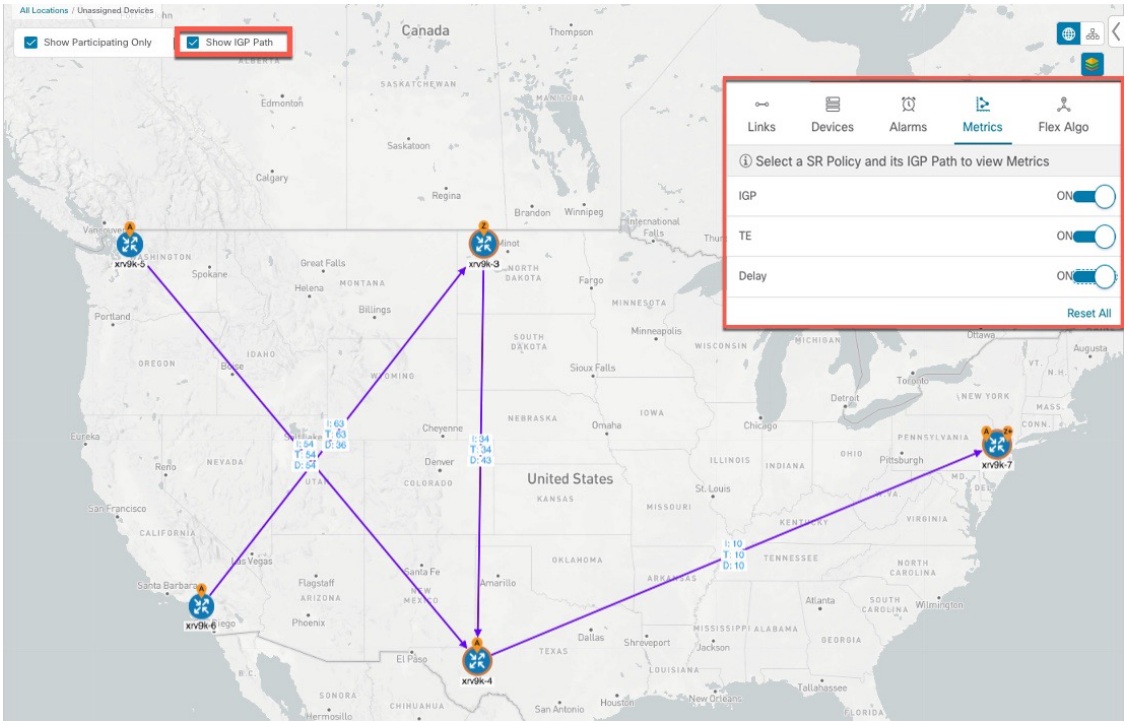
ステップ 3 選択した SR-MPLS ポリシーのエンドポイント間の物理パスとメトリックを表示します。

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

b) をクリックします。

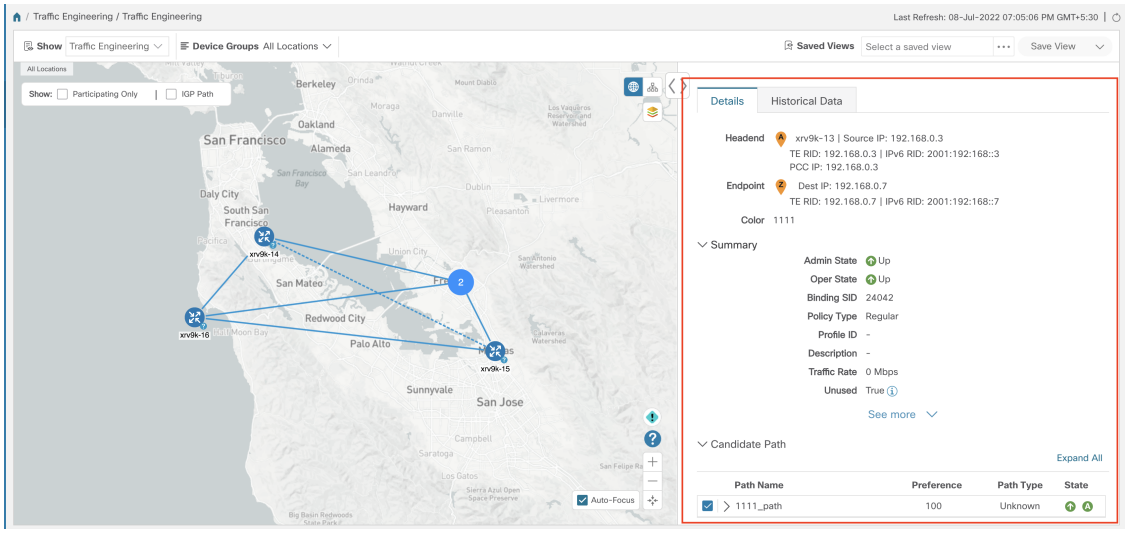
c) [メトリック（Metrics）] タブをクリックします。
d) 該当するメトリックを [オン（ON）] に切り替えます。

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



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

a) [Actions] 列で、いずれかの SR-MPLS ポリシーに対して [...] > [View Details] をクリックします。
サイドパネルに [SRポリシーの詳細（SR Policy Details）] ウィンドウが表示されます。選択したポリシーのみがトポロジマップに表示されていることに注意してください。

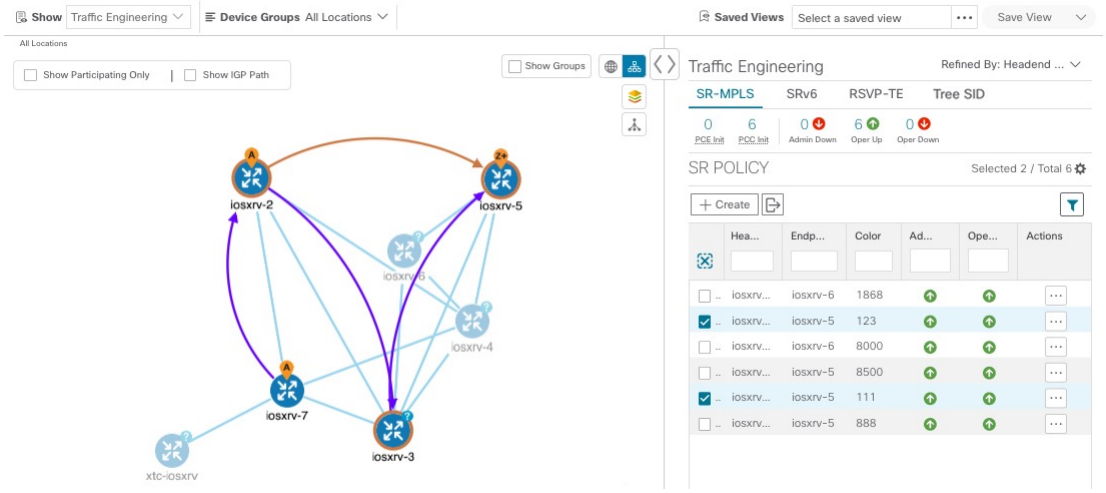


ステップ 5 トポロジの論理ビューをカスタマイズして保存します。

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

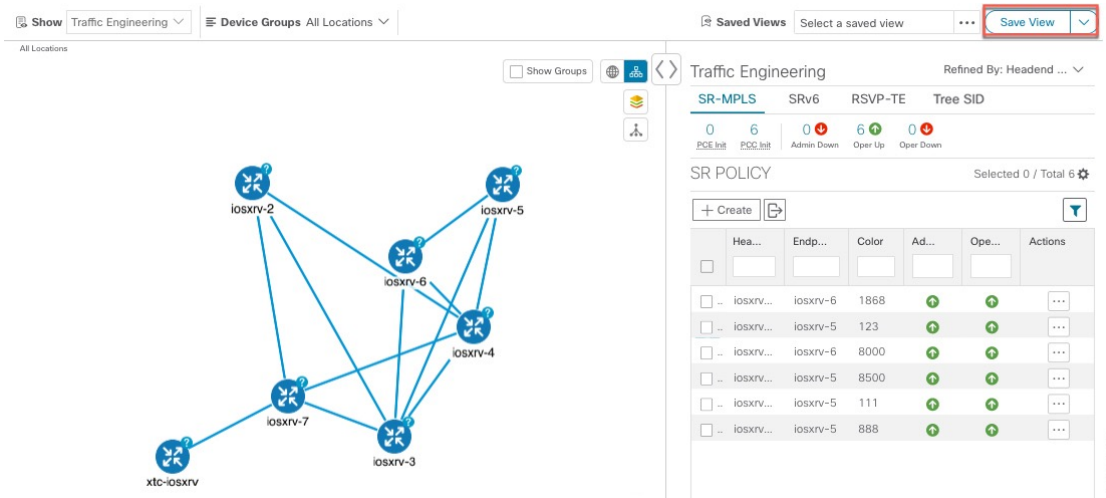
例：

図 *8 :* 論理マップ（*SR-MPLS* ポリシーを選択済み）



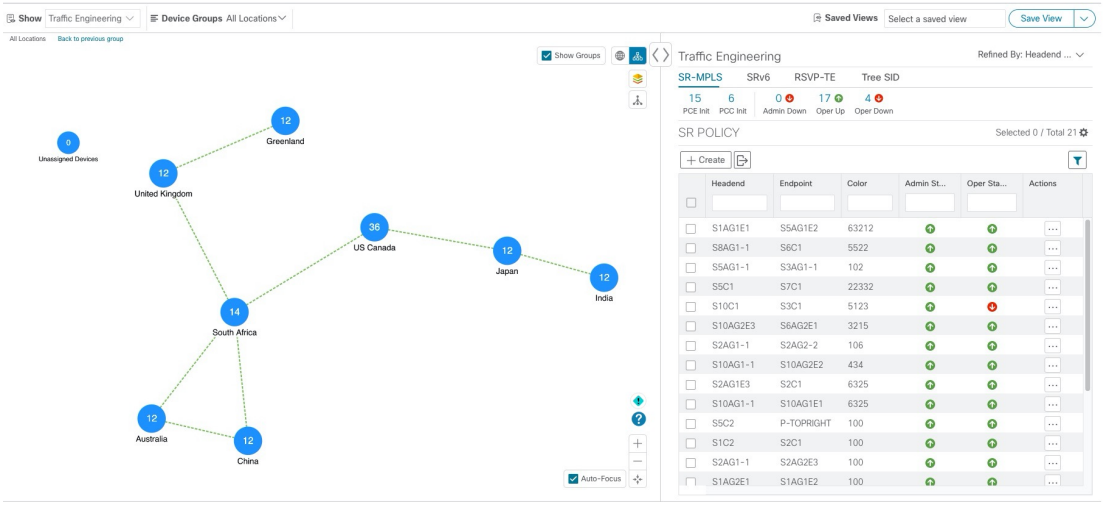
例：

図 *9 :* 論理マップ（*SR-MPLS* ポリシーを選択せずに保存）

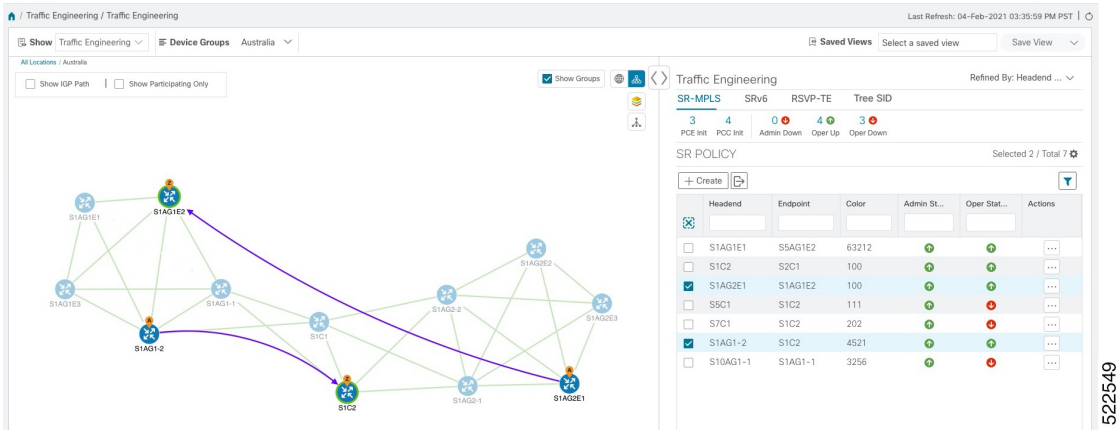


ステップ 6 現在のビュー（✕）を閉じて、[SRポリシー（SR Policy）] テーブルに戻ります。

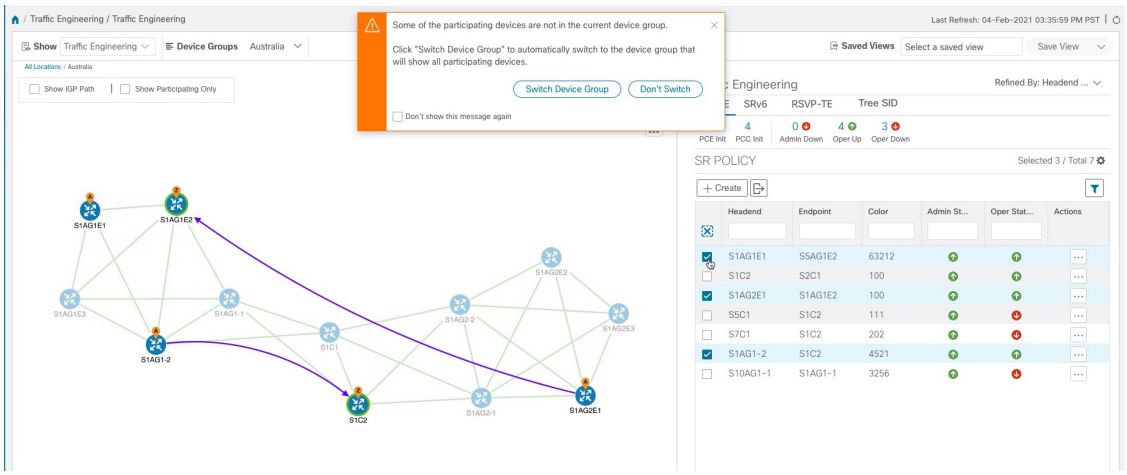
ステップ 7 SR-MPLS ポリシーを選択した場合のデバイスグループの表示方法を理解するには、選択されている可能性のある SR-MPLS ポリシーをオフにし、[Show Groups] をオンにします。



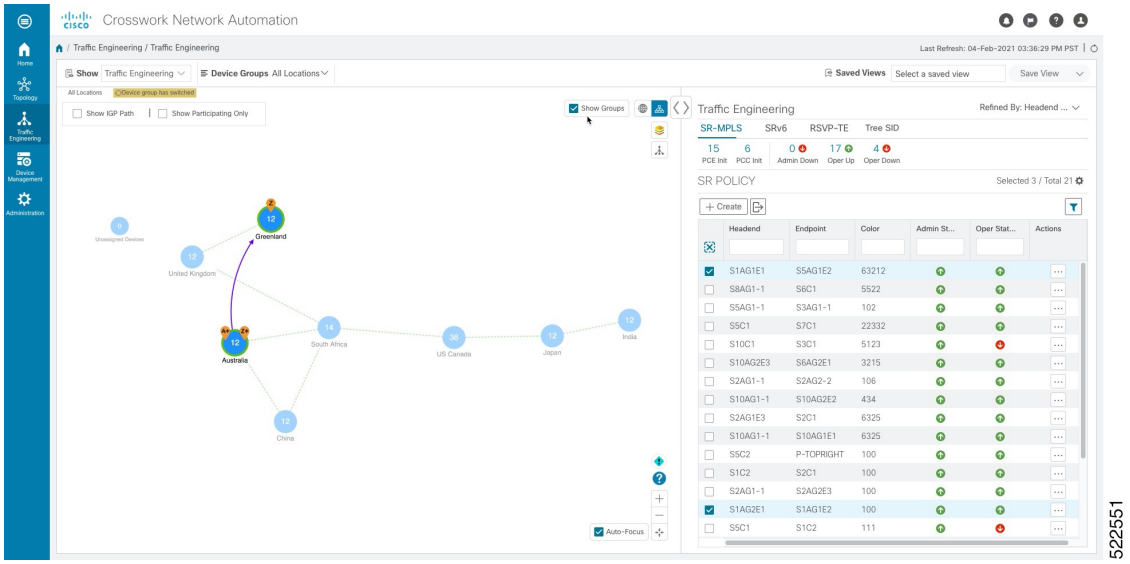
ステップ 8 [デバイスグループ（Device Groups）] ドロップダウンリストから特定のグループを選択すると、マップのグループが表示されます。この例では、[Australia] が選択され、関連する SR-MPLS ポリシーが選択されて表示されます。



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

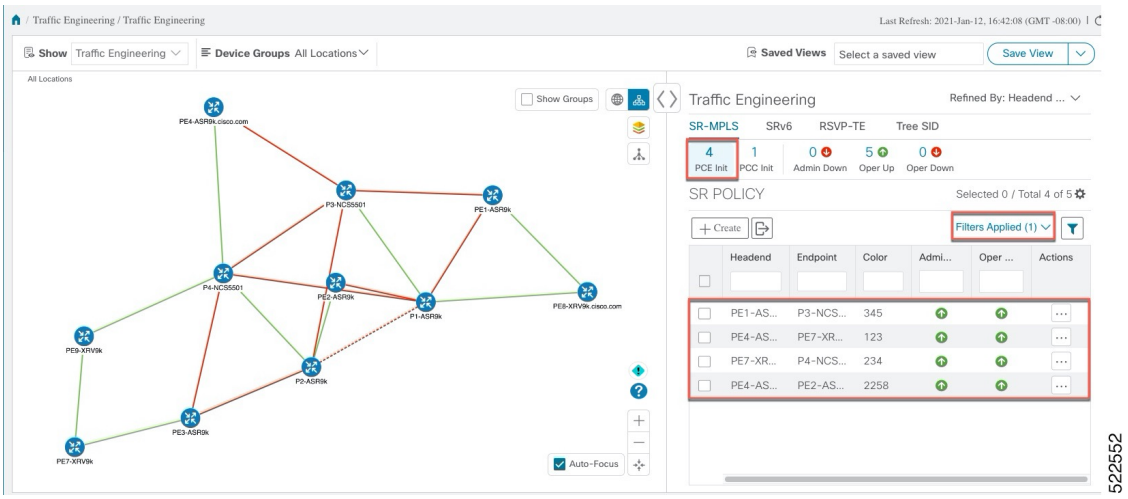


ステップ 10 [Switch Device Group] を選択すると、グループが変更され、選択した SR-MPLS ポリシーに参加中のデバイスがすべて表示されます。
前のグループビューに戻るには、[戻る（Back）] をクリックします（このリンクは、次の図に示す黄色のテキスト領域に後で表示されます）。



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

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



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

複数の候補パス（MCP）の検索

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

特記事項

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

始める前に

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

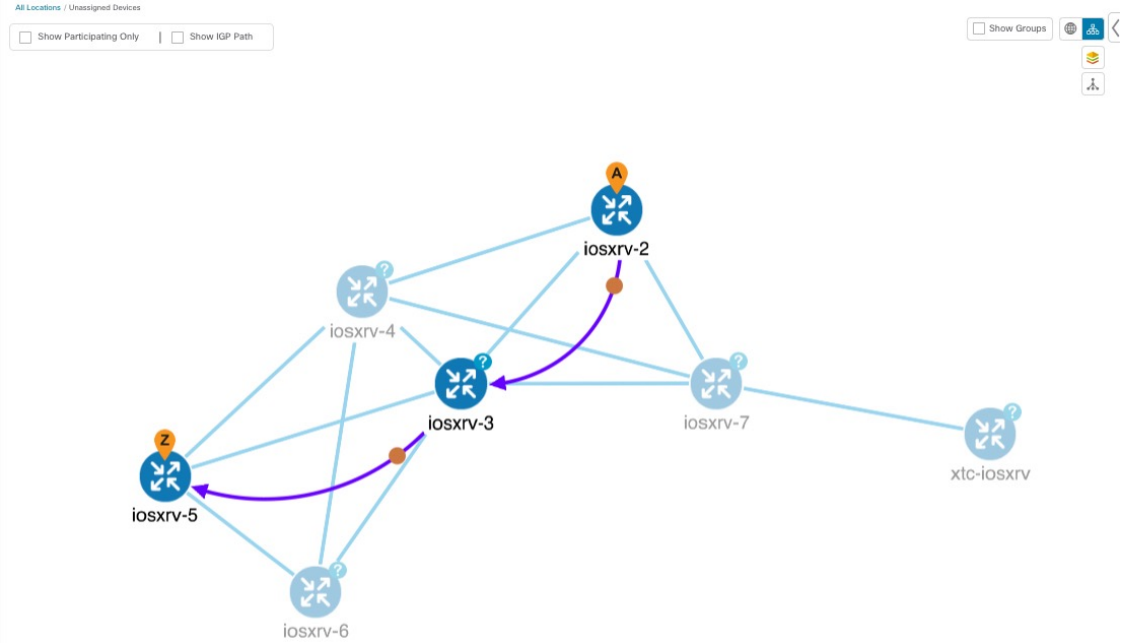
ステップ 1 メインメニューから、**[Traffic Engineering]** > **[Traffic Engineering]** > **[SR-MPLS]** または [SRv6] タブを選択します。

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

a) MCP が設定されている SR-TE ポリシーの横にあるチェックボックスをオンにします。

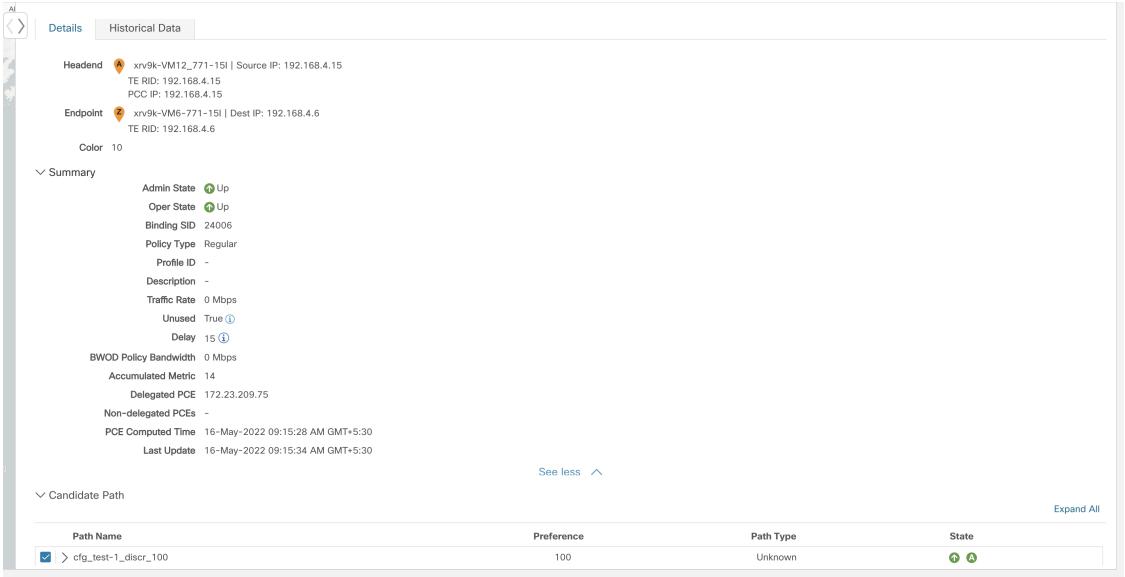
b) トポロジマップに強調表示されている SR-TE ポリシーを表示します。

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



ステップ 3 候補パスのリストを表示します。

a) [SR-TE Policy] テーブルの [Actions] 列で、[...] > **[View Details]** をクリックします。[SR Policy Details] ウィンドウに、候補パスのリストがポリシーの詳細とともに表示されます。ステータス列の緑の A は、アクティブパスを示します。

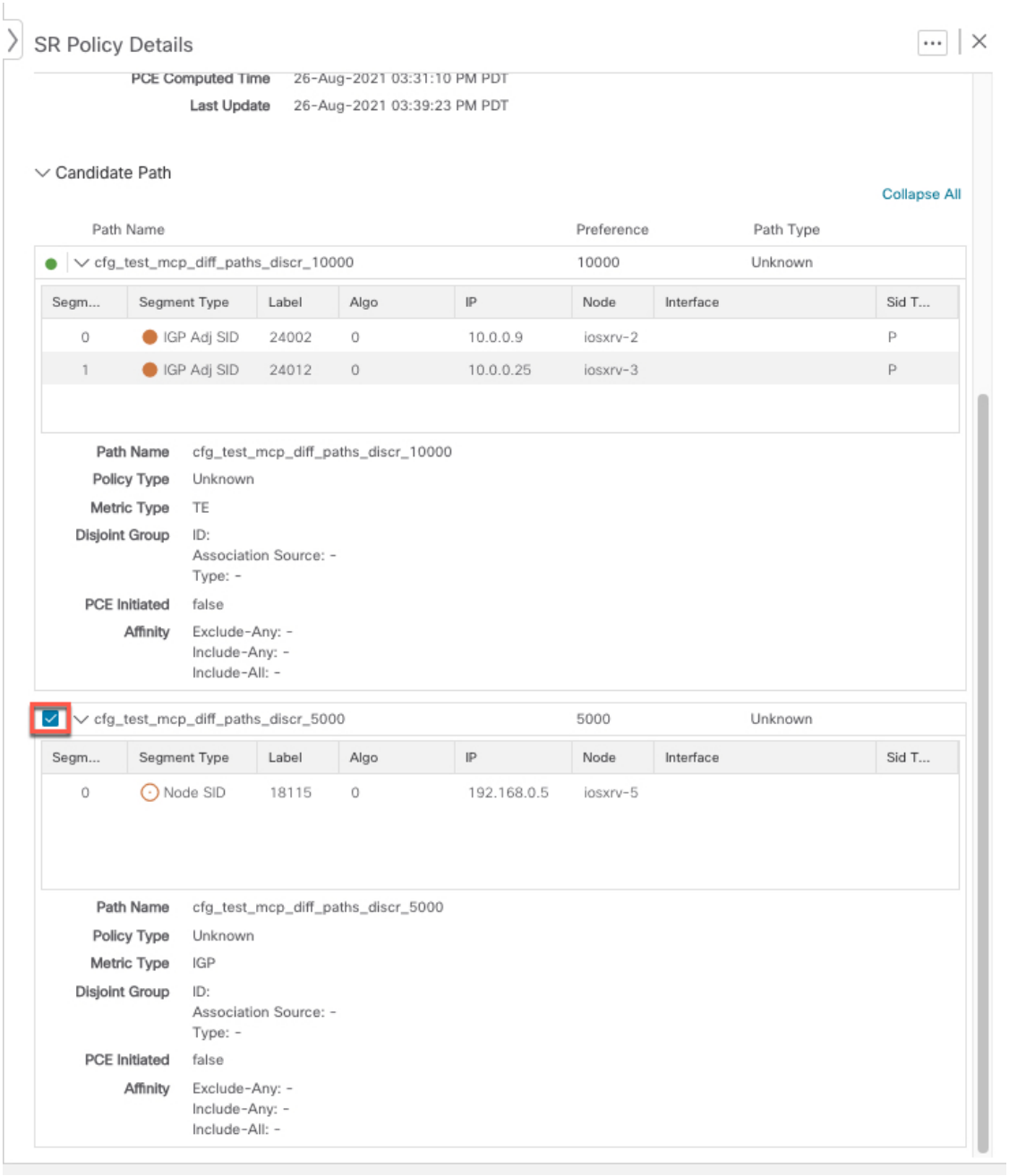


ステップ 4 個々のパスを展開するか、[Expand All] をクリックして各パスの詳細を表示できます。各セグメントにカーソルを合わせると、そのセグメントがマップ上で強調表示されます。

ステップ 5 トポロジマップで候補パスを可視化します。

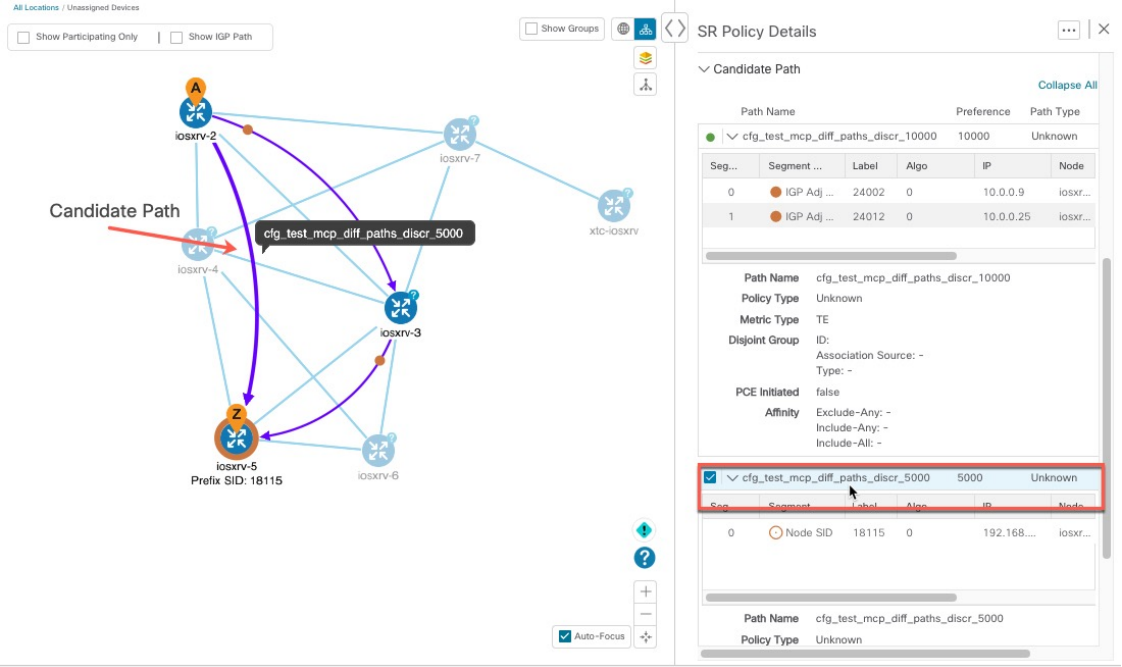
a) 候補パスの横にあるチェックボックスをオンにします。

（注） 明示的な候補パスを選択または表示することはできません。



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

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



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

Crosswork 最適化エンジン を使用すると、デバイスで手動で設定した、または Crosswork ネットワークコントローラを使用して設定した B-SID ホップの基盤となるパスを可視化できます。この例では、SR-MPLS ポリシーホップの B-SID ラベルとして [15700] を割り当てています。

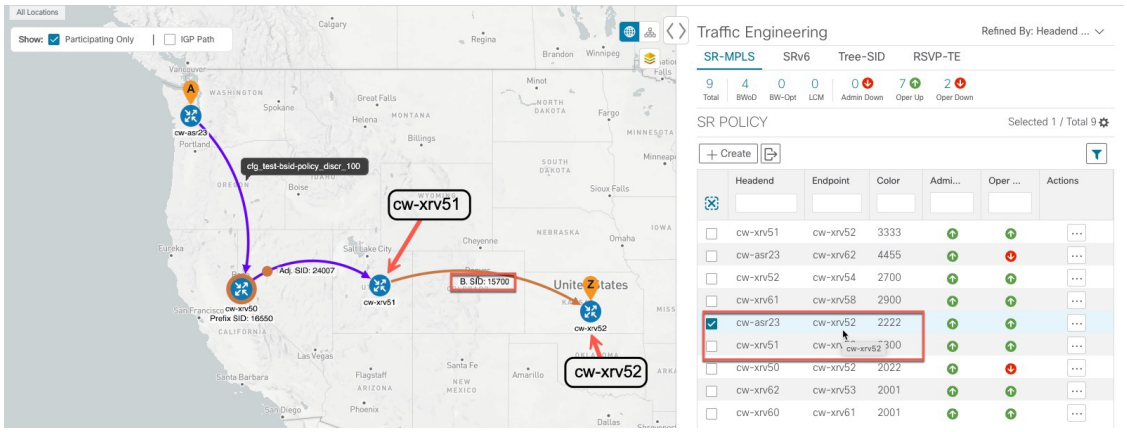
SR-MPLS または SRv6 ポリシーに関する B-SID の基盤となるパスを表示するには、次の手順を実行します。

ステップ 1 メインメニューから、**[トラフィックエンジニアリング（Traffic Engineering）]** > **[トラフィックエンジニアリング（Traffic Engineering）]** > **[SR-MPLS]** または [SRv6] タブを選択します。

ステップ 2 B-SID ラベルが割り当てられたホップを含む SR-MPLS ポリシーの横にあるチェックボックスをオンにし、SR-MPLS 行の任意の部分にマウスポインタを合わせると B-SID 名が表示されます。B-SID パスは、トポロジマップ上で**オレンジ色**で強調表示されます。

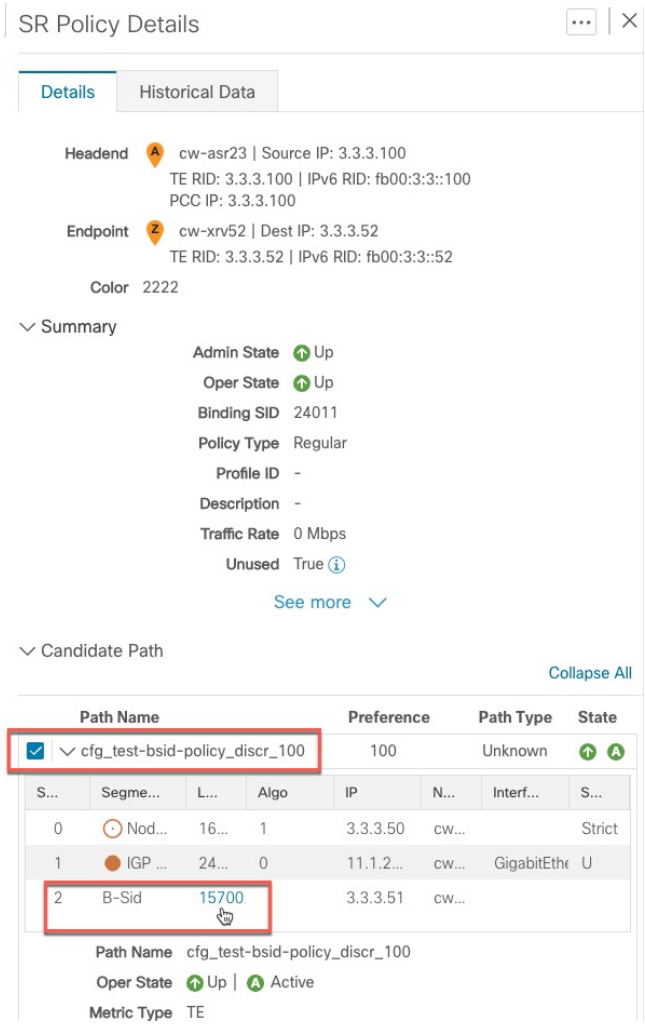
この例では、B-SID パスが [cw-xrv51] から [cw-xrv52] に移動していることがわかります。

（注） 拡大表示するには、画像の例をクリックします。

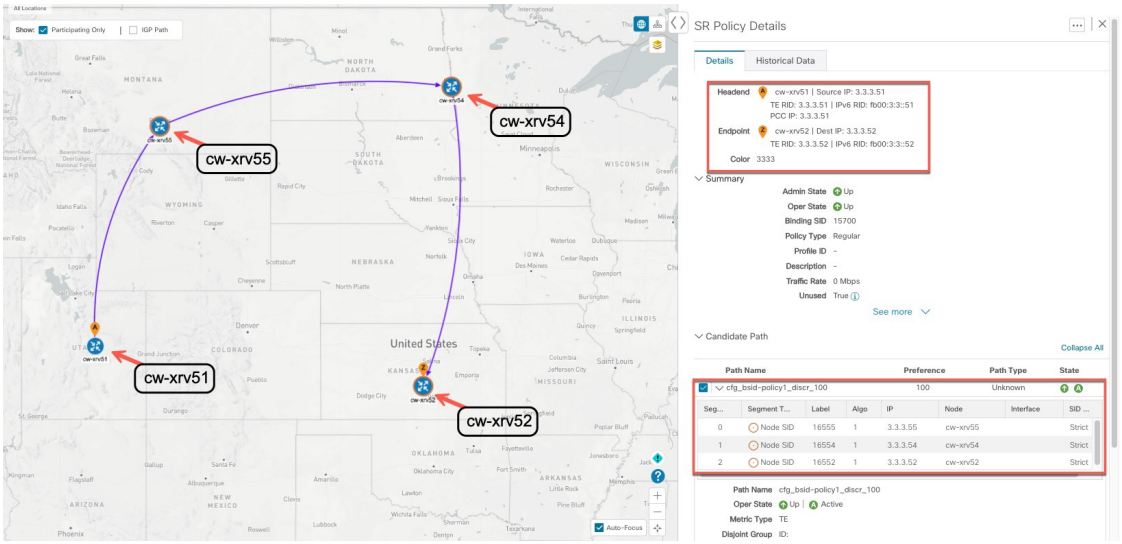


ステップ 3 [アクション（Actions）] 列で、[...] > **[詳細の表示（View Details）]** をクリックします。

ステップ 4 [SRポリシーの詳細（SR Policy Details）] ウィンドウで、アクティブパス名を展開し、**B-SID** ラベルをクリックします。この例では、B-SID ラベルは **[15700]** です。



ステップ 5 基盤となるパスの [SR ポリシーの詳細（SR Policy Details）] ウィンドウで、アクティブなパス名を展開して詳細を表示します。この例では、基礎となるパスが実際に **[cw-xrv51] > [cw-xrv55] > [cw-xrv54] > [cw-xrv52]** と移動していることが確認できます。



ネイティブ SR パスの可視化

Crosswork 最適化エンジン ではネイティブ SR パスを可視化できます。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。ネイティブパスを可視化すると、OAM（運用、管理、メンテナンス）アクティビティで、ラベルスイッチドパス（LSP）をモニターして転送の問題を迅速に隔離できるため、ネットワークの異常検出とトラブルシューティングに役立ちます。

（注） これは、SR-MPLS ポリシーにのみ適用されます。

パスクエリを作成するには、次の手順を実行します。

始める前に

デバイスの要件を満たしていることを確認します。「ネイティブパスデバイスの前提条件の可視化 （57 ページ）」を参照してください。

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

ステップ 2 [クエリパスダッシュボード（Query Path Dashboard）] で、[新しいクエリ（New Query）] をクリックします。

ステップ 3 [新しいパスクエリ（New Path Query）] で必要な値を選択し、**[パスを取得（Get Paths）] をクリックします。**

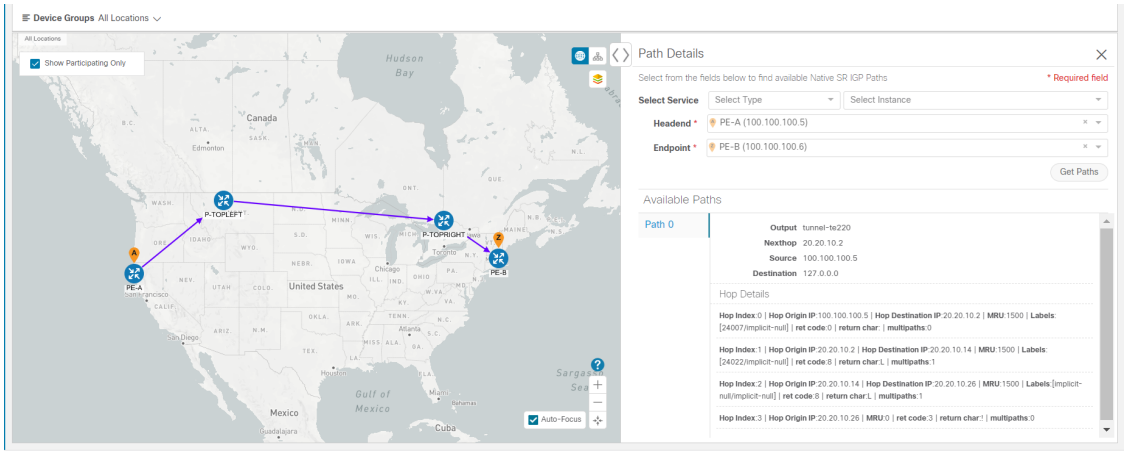
ステップ 4 [結果の表示（View Result）] をクリックして、クエリ結果を表示します。

ステップ 5 （オプション）[結果（Result）] ポップアップで、[以前の結果の表示（View Past Result）] をクリックします。クエリ ID を確認して、利用可能な結果を表示します。

例：

次の例では、使用可能なパス（Path 0）を表示できます。

図 *10* : パスの詳細



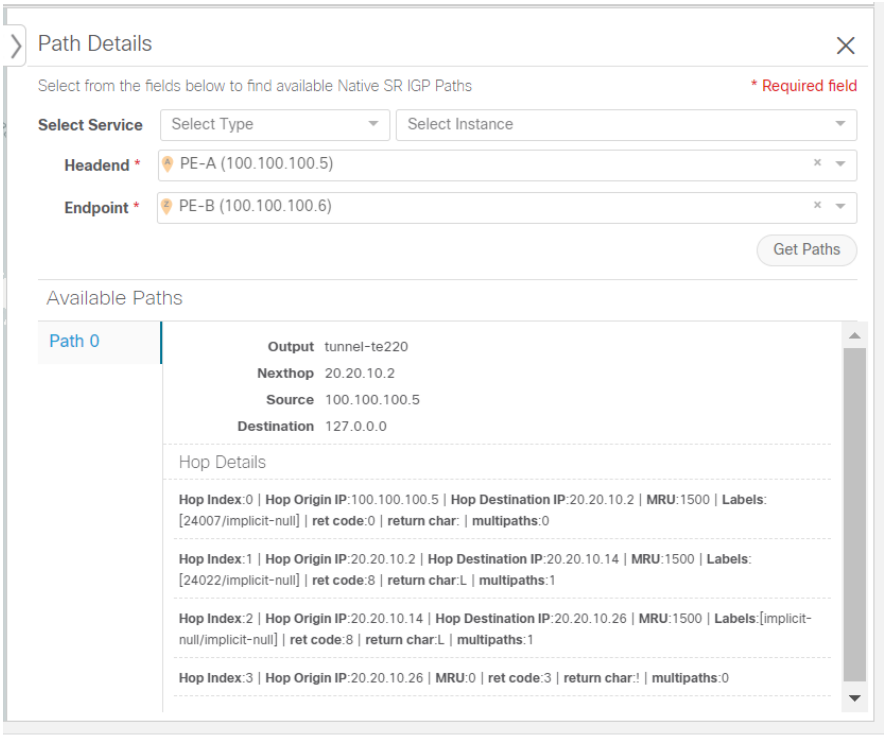
ステップ 6 [アクション（Actions）] 列で、[詳細の表示（View Details）] をクリックします。

デバイスの経度と緯度の情報を提供していない場合、パスは論理ビューで可視化されます。

ステップ 7 使用可能なパスから [Path 0] をクリックして展開し、アクティブなパスを表示します。

例：

図 *11* : パスの詳細



ネイティブパスデバイスの前提条件の可視化

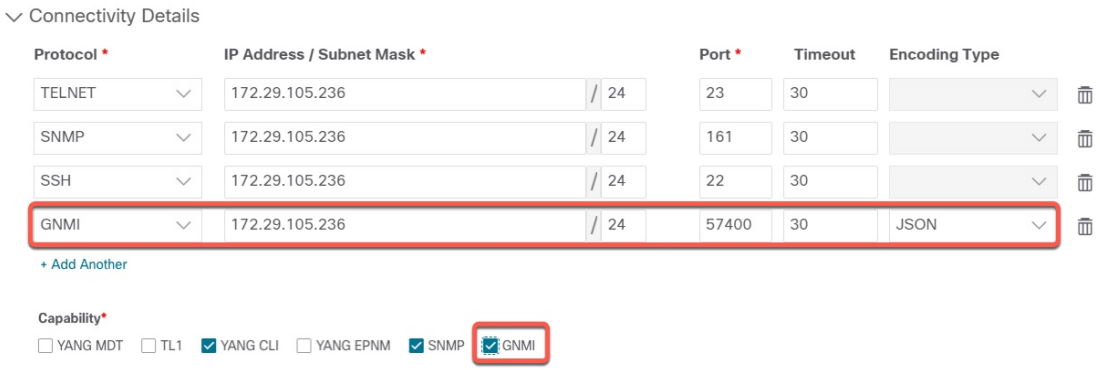
ネイティブパスを可視化する前に、次のデバイスソフトウェアと設定の要件を満たしていることを確認します。

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

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

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

3. デバイスでは、GNMI 機能を有効にして設定する必要があります。
   1. [Device Management] で、デバイスをクリックし、デバイスの詳細（ ）を表示します。
   2. GNMI 機能、および接続の詳細が設定されていることを確認します。



（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

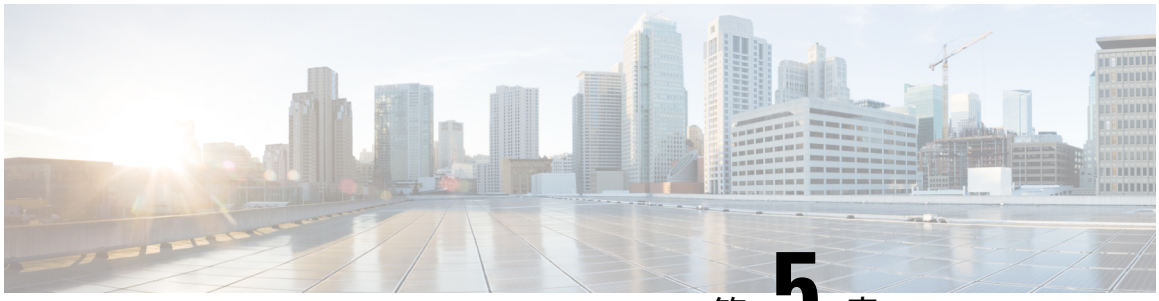
4. デバイスには、CDG ルータの静的アドレスが必要です。スタティックルートは、デバイスからサウスバウンド CDG IP アドレスに追加する必要があります。次に例を示します。

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

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

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

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



第 5 章

フレキシブルアルゴリズムの可視化

フレキシブルアルゴリズムを使用すると、オペレータは、独自のニーズと制約（特定のメトリックとリンクプロパティ）に従ってIGP最短パスをカスタマイズおよび計算できます。ネットワーク上のパスを計算するために、考えられる多くの制約が使用される可能性があります。たとえば、フレキシブルアルゴリズムでは、複数の論理プレーンを持つネットワークに対する特定のプレーンへのパスを制限できます。アルゴリズムの意味が標準規格によってではなく、ユーザーによって定義されるため、フレキシブルアルゴリズムと呼ばれます。

（注） 複数のドメインにあるフレキシブルアルゴリズムはフィルタ処理できません。

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

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

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。アフィニティマッピング名は視覚化に使用され、フレキシブルアルゴリズムを可視化する前に設定する必要があります。このため、デバイスでフレキシブルアルゴリズムのアフィニティを手動で設定、収集してから、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UI内でアフィニティマッピングを定義する必要があります。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。

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。

ステップ1 メインメニューから、**[管理（Administration）]**>**[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）]**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。例（上記の構成を使用）：

例：

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、リンクとデバイスのフレキシブルアルゴリズムの検索 （64 ページ）を参照してください。

フレキシブルアルゴリズムの可視化

Crossworkを使用すると、ネットワーク内で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 （93 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）。
- ネットワークで使用されているフレキシブルアルゴリズム ID を知っている必要があります。フレキシブル アルゴリズム メンバーシップを表示するには、リンクとデバイスのフレキシブルアルゴリズムの検索 （64 ページ）を参照してください。

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

フレキシブルアルゴリズムの可視化

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

ステップ 2 トポロジマップから、をクリックします。

ステップ 3 [Flex Algo] タブをクリックします。

ステップ 4 ドロップダウンリストから、最大 2 つのフレキシブルアルゴリズム ID を選択します。

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

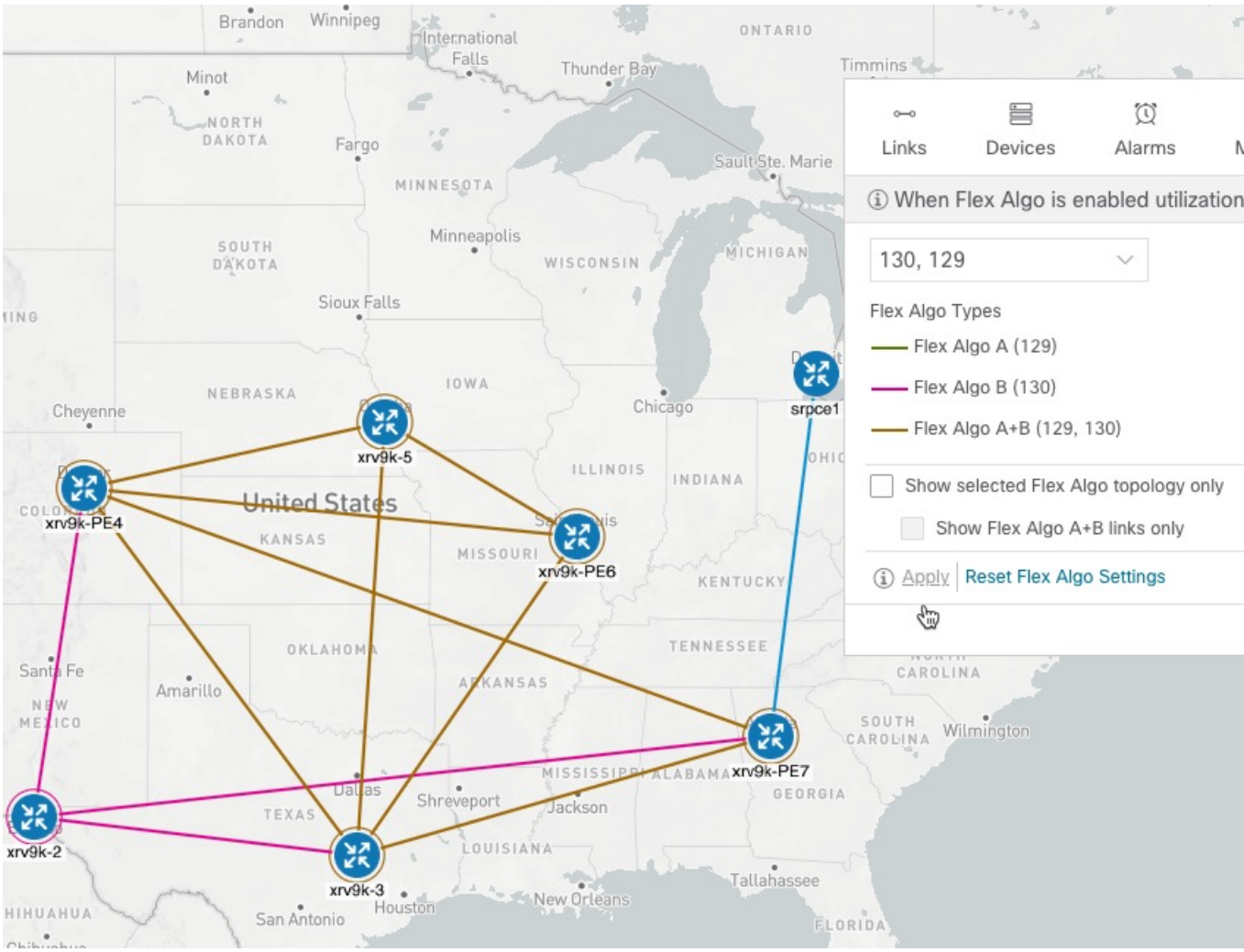
ステップ 6 （オプション）[Show selected Flex Algo topology only] チェックボックスをオンにして、トポロジマップでフレキシブルアルゴリズムを分離します。このオプションを有効にすると、SR ポリシーの選択が無効になります。

a) 両方のフレキシブルアルゴリズムに参加しているリンクとノードのみを表示するには、[Show Flex Algo A+B links only] をオンにします。

ステップ 7 [Apply] をクリックします。フレキシブルアルゴリズムの選択内容に追加の変更を加えるには、[Apply] をクリックして、トポロジマップの更新内容を確認する必要があります。

例：

フレキシブルアルゴリズムの可視化



（注）
- 複数のドメインにあるフレキシブルアルゴリズムIDはフィルタ処理できません。ドメインフィルタリングは、フレキシブルアルゴリズムに基づいてサポートされていません。
- 選択したフレキシブルアルゴリズムが基準で定義されているが、（青色ですべてのノードやリンクを含むように定義されたアフィニティなど）一致するリンクとノードの組み合わせがない場合、トポ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。

リンクとデバイスのフレキシブルアルゴリズムの検索

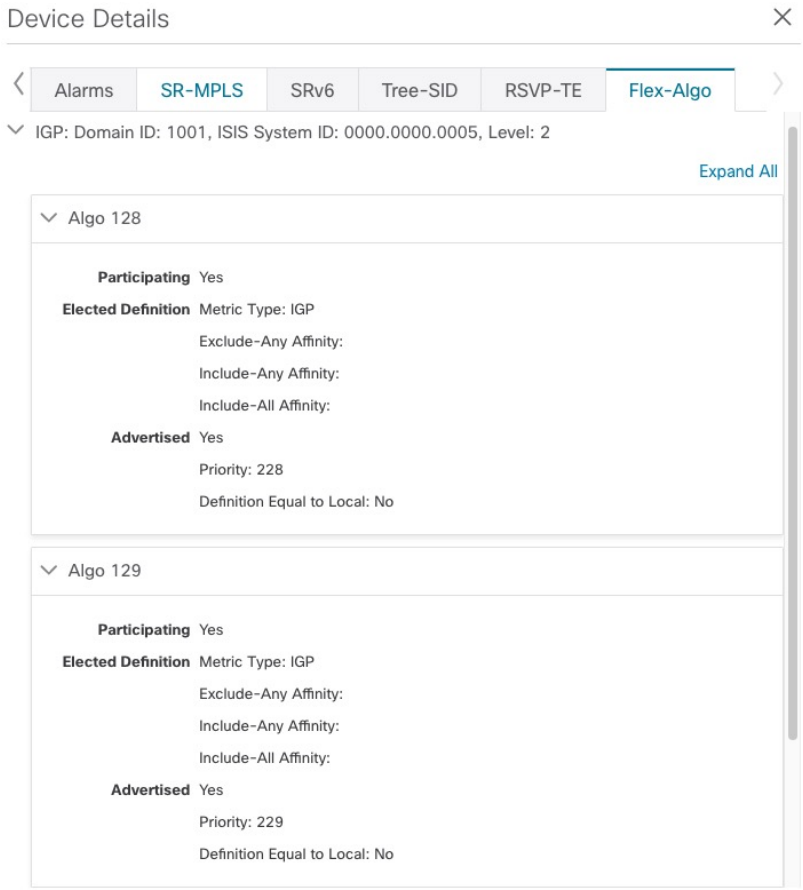
デバイスまたはリンクがフレキシブルアルゴリズムのメンバーであるかを確認するには、次の手順を実行します。

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

ステップ 2 デバイスがフレキシブルアルゴリズム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、デバイスをクリックします。

b) [Device Details] ウィンドウで、[Flex-Algo] タブをクリックします。デバイスがフレキシブルアルゴリズムの一部である場合、Algo ID と情報が表示されます。次に例を示します。



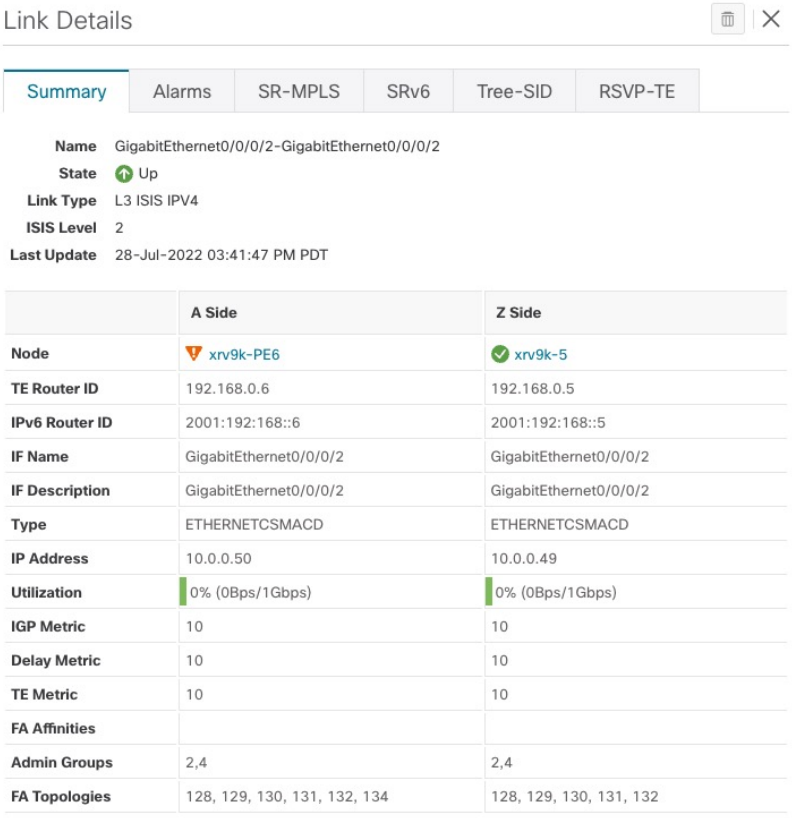
（注） デバイスがメンバーでない場合は、IGP ドメインと OSPF ID 情報のみが表示されます。

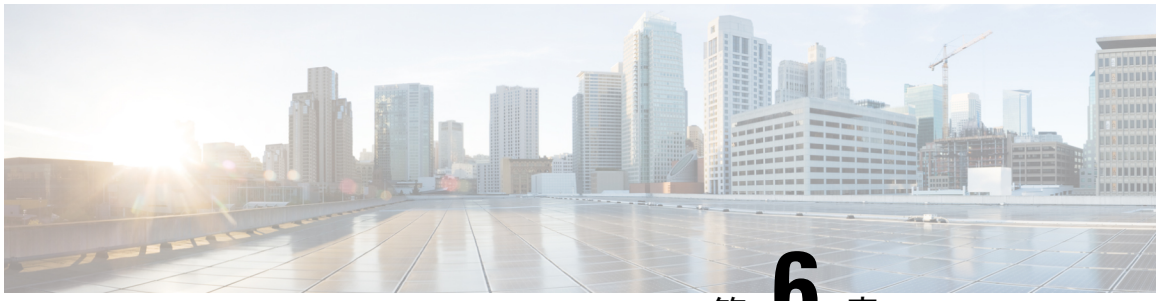
ステップ 3 リンクがフレキシブルアルゴリズムの一部であるかどうかを表示するには、次の手順を実行します。

a) トポロジマップから、リンクをクリックします。

b) [Links] ページで、いずれかのリンクタイプをクリックします。

c) デフォルトでは、[Summary] タブが [Link Details] ウィンドウ内に表示されます。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。[FAアフィニティ（FA Affinities）] の行でアフィニティを表示することもできます。





第 6 章

Tree-SID ポリシーの可視化

Crosswork Optimization Engine を使用すると、ネットワークに実装されている Tree-SID ポリシーを可視化できます。これにより、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。また、P2MP SR ポリシーは P2MP SR ポリシーのパスの更新時における一時的なループやパケット損失を防止します。

ルートノードは、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はマルチキャストトラフィックを複製し、リーフノードに転送します。バドノードは、下流のサブツリーに向かう中間点（トランジット）ノードだけでなく、リーフ（出力）ノードとしても機能するノードです。リーフノードは、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。

ネットワークで Tree-SID を設定するには、お使いのデバイスの SR Tree-SID 設定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）

COE は、次のタイプの Tree-SID ポリシーの可視化をサポートしています。

- **静的**：静的 Tree-SID ポリシーは、PCE を介して設定されます。すべてのパスは、静的 Tree-SID ポリシーで明示的に指定されています。Tree-SID 名は設定中に割り当てられ、ID はありません。
- **動的**：動的 Tree-SID ポリシーはサービスエンドポイントで設定され、PCE および SEP でデイゼロ設定が必要です。

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

（注） Crosswork Optimization Engine を使用して Tree-SID ポリシーを可視化する場合は、常に**[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。Crosswork Network Controller ソリューションを使用してこれらのポリシーを可視化する場合は、ナビゲーションパスは**[トラフィックエンジニアリングとサービス（Traffic Engineering & Services）]>[トラフィックエンジニアリング（Traffic Engineering）]**です。

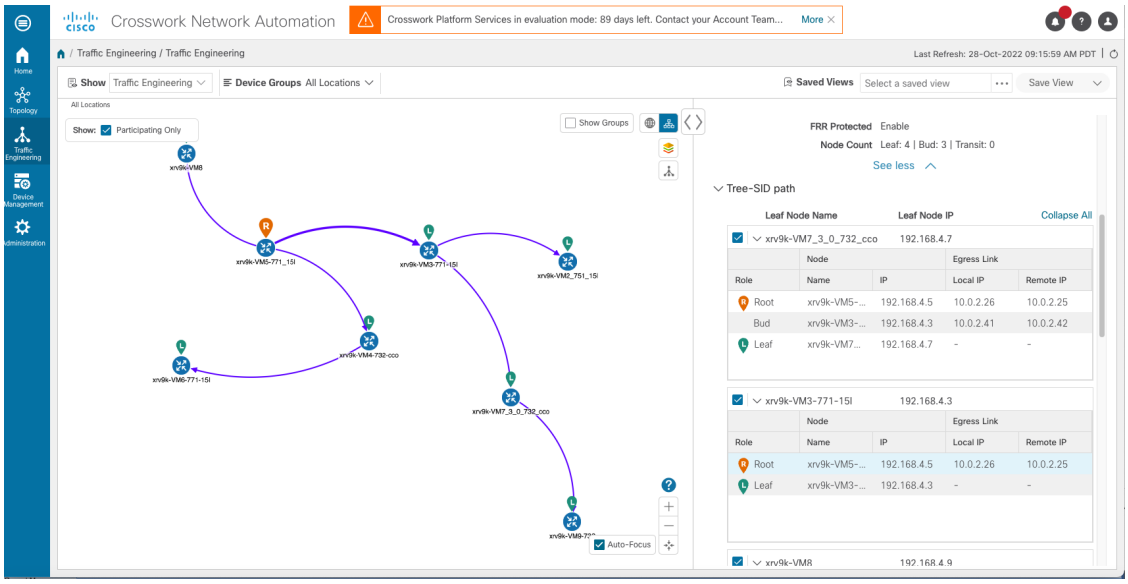
- トポロジマップでポイントツーマルチポイント ツリーを表示する （68 ページ）
- Tree-SID ポリシーの制限事項 （70 ページ）
- ツリー SID の設定例 （72 ページ）

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

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、Crosswork ネットワークマップの 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）が明確にマークされ、矢印はルートから 2 つのリーフまでのトランジットノードを通るパスを示しています。また、バドノードには別のリーフノードのパスがあり、トポロジマップに表示されます。

ノードとリンクをドリルダウンして、Tree-SID ポリシーの詳細を表示し、設定を検証できます。



始める前に

Tree-SID ポリシーとノードには、次の設定が必要です。

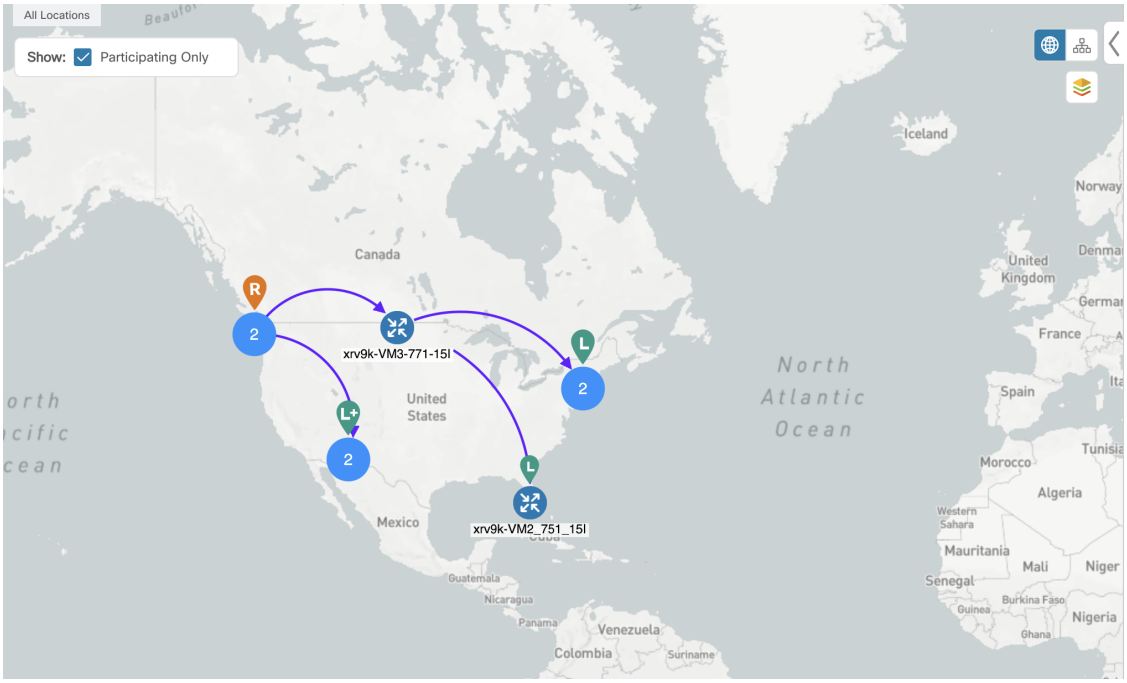
- トランジットノード：PCEP が必要です。
- バドノード、出力ノード、および入力ノード：PCEP、アクティブな BGP MVPN セッション、BGP 自動検出セグメントルーティング、および MDT デフォルト セグメントルーティング、MDT 分割セグメントルーティング

ネットワーク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）

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。

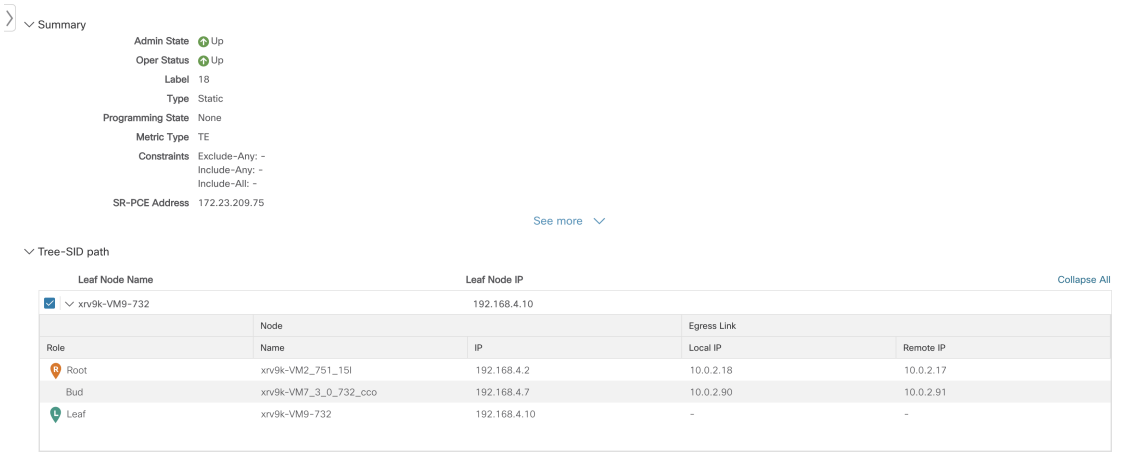
ステップ 2 トポロジマップに表示する Tree-SID ポリシーを選択します。

（注） 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。



（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 （33 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。



ステップ 4 Tree-SID の詳細を表示し、パスとノードの詳細を確認して、Tree-SID が正しく設定されていることを確認できます。

Tree-SID ポリシーの制限事項

制限事項

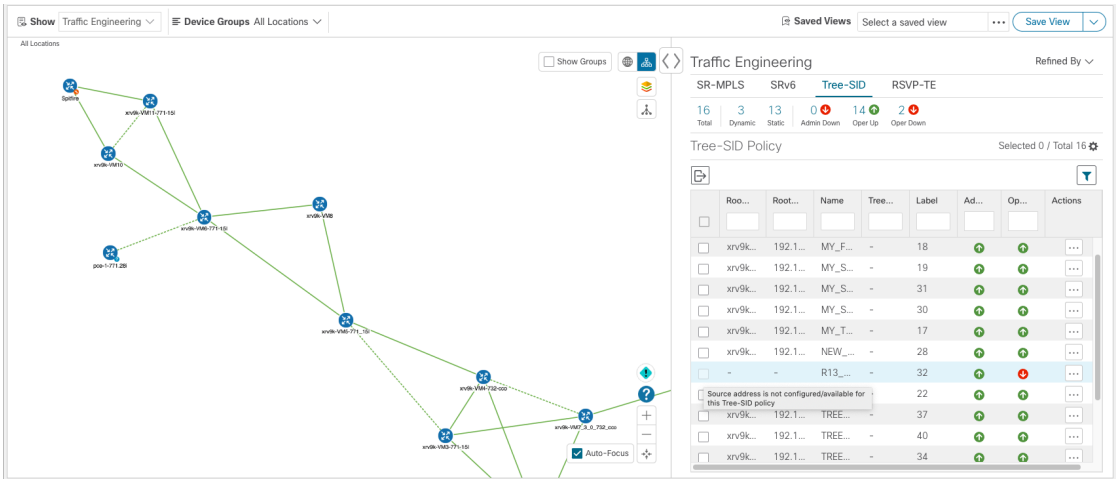
- Tree-SID ポリシーの可視化のみがサポートされています。UI から Tree-SID ポリシーを作成、編集、または削除することはできません。
- Tree-SID ポリシーは、Cisco IOS XR ソフトウェアを実行しているデバイスでのみサポートされます。
- HA モードの PCE がダウンしている場合、そして PCE が Crosswork UI から削除されている場合も、Tree-SID ポリシーは UI から削除されません。
- PCE HA はサポートされていません。
- Tree-SID ポリシーは、Label Switch Multicast（LSM）ルーティングではサポートされていません。LSM が有効になっている場合、IGP アップデートとトラフィック使用率データはサポートされません。
- pim の下の「no vrf」または PCC での「no multicast」の後に、PCE では Tree-SID ポリシーは作成されません。
- FRR=true の場合、local-hop-address は無視され、「next-hop-address」の値が表示されます。
- IGP 設定が更新されると、PE ルータでの FIB プラットフォームの更新が失敗します。
- LCM は、Tree-SID LSP を運ぶネットワークの一部では動作しません。

- RestConf API はサポートされていません。
- Tree-SID ポリシーの詳細には、IPv6 ルータ ID または Srv6 コア情報は表示されません。

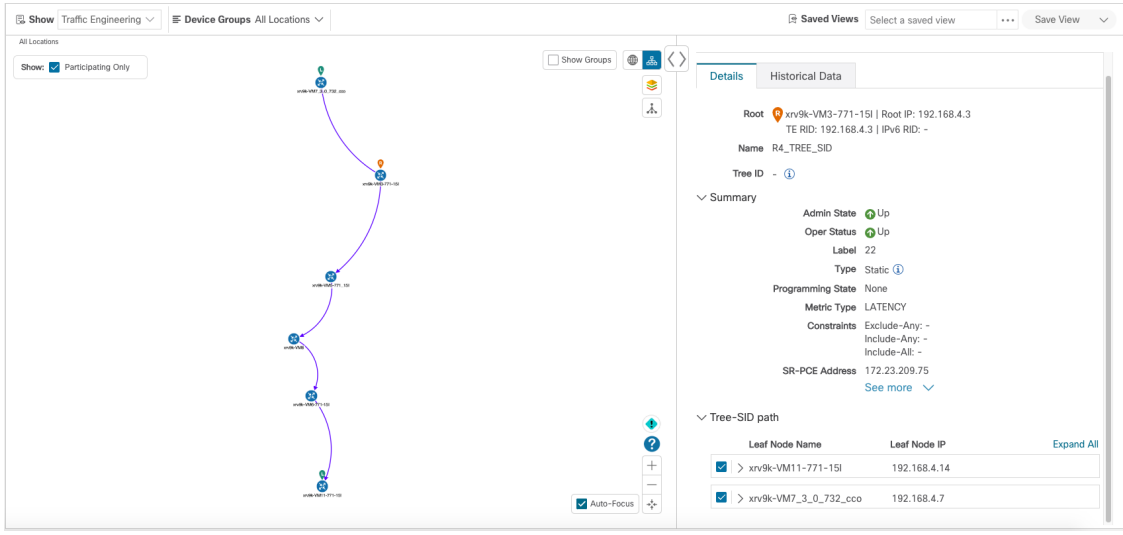
ノードが欠落している Tree-SID パスの可視化

トポロジで Tree-SID ノードが欠落しているシナリオは次のとおりです。

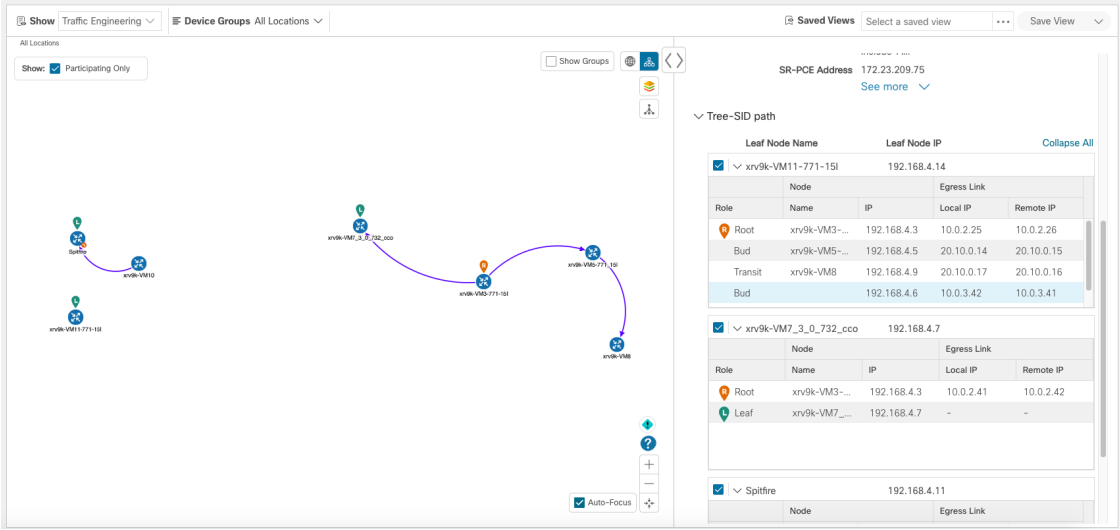
- 送信元ノードまたはルートノードが PCE で設定されていない場合、Tree-SID ポリシーを可視化することはできません。このような Tree-SID ポリシーの詳細は入力されず、ポリシーはオペレーションダウンとなります。



- 特定のリーフノードが欠落している Tree-SID ポリシーパスを可視化することはできません。このような Tree-SID ポリシーの詳細は、リーフノードのパスが欠落した状態で入力されます。ポリシー内の他の Tree-SID パスがある場合はネットワークに表示されます。



- トランジットノードまたはバドノードが欠落している Tree-SID ポリシーを、部分的なオーバーレイで可視化できます。Tree-SID ポリシーの詳細は、ホスト名なしで入力されます。



（注） トランジットノードまたはバッドノードが欠落している場合は、以下の警告が表示されます。

1. 履歴データタブ：一部のデバイスリンクは、現在のデバイスインベントリおよびトポロジのデータベースに存在しないため、ポリシーパスから欠落しています。
2. トポロジの UI：トポロジマップは、ネットワークの現在の状態を反映しています。現在のデバイスやリンクの状態は、必ずしもトラフィックエンジニアリングポリシー、トンネル、またはサービスに影響を与えるとは限りません。

- ルートまたは送信元ノードが UI から削除された場合、ルートホスト名は空になり、Tree-SID ポリシーはトポロジマップで使用可能なパスなしでオペレーションアップとなります。ルートルータ IP は、以前の Tree-SID ディスカバリから表示されます。

ツリー SID の設定例

セグメントルーティングの Tree-SID を可視化するには、SR-PCE および Tree-SID パスに含まれるデバイスでいくつかの設定が必要です。以下は、ネットワークで必要な各ステップの設定例です。

- 静的 Tree-SID ポリシーの設定例 （73 ページ）
- VRF を使用した動的 Tree-SID ポリシーの設定例 （74 ページ）
- VRF を使用しない動的 Tree-SID ポリシーの設定例 （79 ページ）

次のデイゼロ設定が必要です。

すべての SEP および PCE での MVPN アドレスファミリの有効化。

PCE での p2mp の有効化。

静的 Tree-SID ポリシーの設定例

（注） お使いのデバイスの Tree-SID 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）。

次の手順は、静的 Tree-SID デバイスの設定例を示しています。

ステップ 1 パス計算要素プロトコル（PCEP）とパス計算クライアント（PCC）を、Tree-SID パス（ルート、トランジットやバド、リーフ）に含まれるすべてのノードで設定します。

例：

```
pce
 address ipv4 <pce-loopback0-IP>
 api
  user admin
   password encrypted xxxx
  !
 !
 segment-routing
  traffic-eng
   p2mp
    endpoint-set MY_FIRST_TREE_SID_EPs
     ipv4 <leaf or pcc1-loopback0-IP>
     ipv4 <leaf or pcc2-loopback0-IP>
    !
```

ステップ 2 エンドポイントのある SR-PCE で P2MP SR 静的ポリシーを設定します。

例：

```
policy MY_FIRST_TREE_SID
             source ipv4 <root or pcc3-loopback0-IP>
             color 20 endpoint-set MY_FIRST_TREE_SID_EPs
```

```
  treesid mpls 18
  candidate-paths
    preference 100
     dynamic
      metric
       type te
 !
!
!
!
```

VRF を使用した動的 Tree-SID ポリシーの設定例

Tree-SIDポリシーに動的ポリシーを追加するには、ルートデバイスとリーフデバイスの両方でVRF を作成します。PCE、ルートデバイス、リーフデバイスの BGP ルータ設定の下で対応するVRF、ネイバーを指定します。以下の例で説明するように、マルチキャストルーティング、ルータ pim の下で VRF は異なる VRF ごとのルートポリシーを作成します。

動的 Tree-SID ポリシーの手順に従います。

前提条件のルートポリシー（PCE、ルートおよびリーフの両方で設定）デバイス

PCE の下

```
route-policy PASS
  pass
end-policy
!
```

ルートおよびリーフの下

```
route-policy bgp_in
  pass
end-policy
!
route-policy PIM-RPF
  set core-tree sr-p2mp
end-policy
```

```
!
route-policy bgp_out
  pass
end-policy
!
route-policy PASS_ALL
  pass
end-policy
!
route-policy TREESID-CORE
  set core-tree sr-p2mp
end-policy
!
```

ステップ 1 pce の下で segment-routing traffic engineering -> p2mp-> label range <>、multi-path disable と設定します。

例：

```
label-range min 15400 max 60000
              fast-reroute lfa
              multipath-disable
```

ステップ 2 ルータ bgp の下で、最上位に address family ipv4 mvpn を設定し、ネイバーノード IP <root> および <leaf> レベルでも同様に address family ipv4 mvpn を設定します。

例：

```
router bgp 1
                  ……..
                  address-family ipv4 mvpn
                  route-reflector-client
                !
                  neighbor <root or pcc3-loopback0-IP>
                  remote-as 1
                 update-source Loopback0
                 address-family ipv4 unicast
                 route-policy PASS in
                 route-policy PASS out
```

```
   !
     address-family ipv4 mvpn
 !
!

neighbor <leaf or pcc1-loopback0-IP>
      remote-as 1
     update-source Loopback0
     address-family ipv4 unicast
     route-policy PASS in
     route-policy PASS out
   !
     address-family ipv4 mvpn
 !
!
```

ステップ 3 ヘッドエンドとエンドポイントを設定します。

（注） PCEの下のルートBGP設定で、エンドポイントルータをネイバーとして追加できます。Router-IDは、トポロジ内の各 PCC ループバック IP で更新する必要があります。

a) interface Loopback<80> を作成

例：

```
interface Loopback80
 ipv4 address 80.80.10.1 255.255.255.252
 ipv6 address 2001:192:168:80::1/128
!
```

b) VRF <vrf-name-80> を作成

例：

```
vrf L3VPN_NM-MVPN-80
 address-family ipv4 unicast
  import route-target
   80:80
  !
  export route-target
```

```
   80:80
  !
 !
!
```

c) ルーティング BGP 設定の下で <vrf-name-80> を指定

例：

```
vrf L3VPN_NM-MVPN-80
  rd 80:80
  address-family ipv4 unicast
   redistribute connected
  !
  address-family ipv4 mvpn
  !
  neighbor 80.80.10.1 <leaf or pcc1-vrf-IP>
   remote-as 80
   address-family ipv4 unicast
    route-policy PASS_ALL in
    route-policy PASS_ALL out
   !
  !
 !
!
```

d) マルチキャストルーティング設定の下で <vrf-name-80> を指定

例：

```
multicast-routing
 address-family ipv4
  interface Loopback0
   enable
  !
  mdt source Loopback0
  mdt static segment-routing
 !
```

```
 vrf L3VPN_NM-MVPN-80
  address-family ipv4
   interface all enable
   bgp auto-discovery segment-routing
   !
   mdt default segment-routing mpls color 80
  !
 !
!
```

e) route-policy <vrf-name-80> を作成

例：

```
route-policy L3VPN_NM-MVPN-80
  if destination in (232.0.0.80) then
    set on-demand-color 80
    pass
  endif
end-policy
!
```

f) セグメント ルーティング トラフィック エンジニアリングの下で、ODN color <80> を設定

例：

```
on-demand color 80
   dynamic
    pcep
    !
    metric
     type te
    !
   !
  !
```

ステップ 4 リーフの設定

（注） 手順 a から d に従って、ルートノードのヘッドエンドとエンドポイントを設定します。

例：

```
router pim
 address-family ipv4
  rpf topology route-policy PIM-RPF
 !
 vrf L3VPN_NM-MVPN-80
  address-family ipv4
   rpf topology route-policy TREESID-CORE
   mdt c-multicast-routing bgp
   !
  !
 !
```

VRF を使用しない動的 Tree-SID ポリシーの設定例

ルートデバイスとリーフデバイスの両方で、VRF を使用せずに動的ポリシーを Tree-SID ポリシーに追加するには、次の手順に従います。

（注） PCE の設定は、VRF を使用した動的 Tree-SID の設定と同じです。VRF を使用した動的 Tree-SID ポリシーの設定例 （74 ページ）を参照してください。

ステップ 1 ルートの設定

a) ルータの BGP 設定の下で、ネイバーとして <**leaf-node-IP or pcc1-IP**> を指定します。

b) マルチキャストルーティング設定の下で一意の RT を指定します。

（注） RT は、ルートセットとリーフセットの間で一意である必要があります。

例：

```
multicast-routing
              address-family ipv4
                import-rt 12:12
                export-rt 12:12
                mdt source Loopback0
                interface all enable
                bgp auto-discovery segment-routing
```

```
        !
         mdt default segment-routing mpls color 12 fast-reroute lfa
        mdt data segment-routing mpls 5 threshold 0
    !
```

c) セグメント ルーティング トラフィック エンジニアリングの下で、ODN color <unique one> を設定します。

ステップ 2 リーフの設定

a) ルータの BGP 設定の下で、ネイバーとして <**root-node-IP or pcc3-IP**> を指定します。

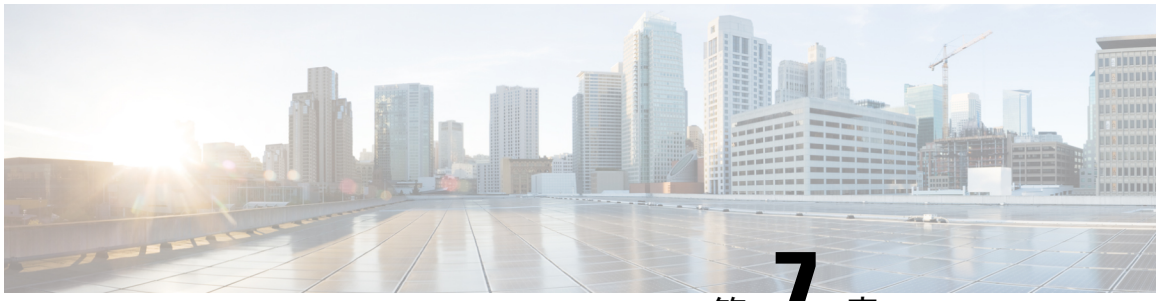
b) マルチキャストルーティング設定の下で一意の RT を指定します。

（注） RT は、ルートセットとリーフセットの間で一意である必要があります。

例：

```
multicast-routing
     address-family ipv4
        import-rt 12:12
        export-rt 12:12
        mdt source Loopback0
        interface all enable
        bgp auto-discovery segment-routing
    !
     mdt default segment-routing mpls color 12 fast-reroute lfa
    mdt data segment-routing mpls 5 threshold 0
!
```

c) ルータ PIM、route-policy TREESID_CORE を設定します。



第 7 章

RSVP-TE トンネルの可視化

（注） Crosswork Network Controller ソリューションを使用する場合、ナビゲーションは **[トラフィック エンジニアリングおよびサービス（Traffic Engineering & Services）] > [トラフィック エンジニアリング（Traffic Engineering）]** です。

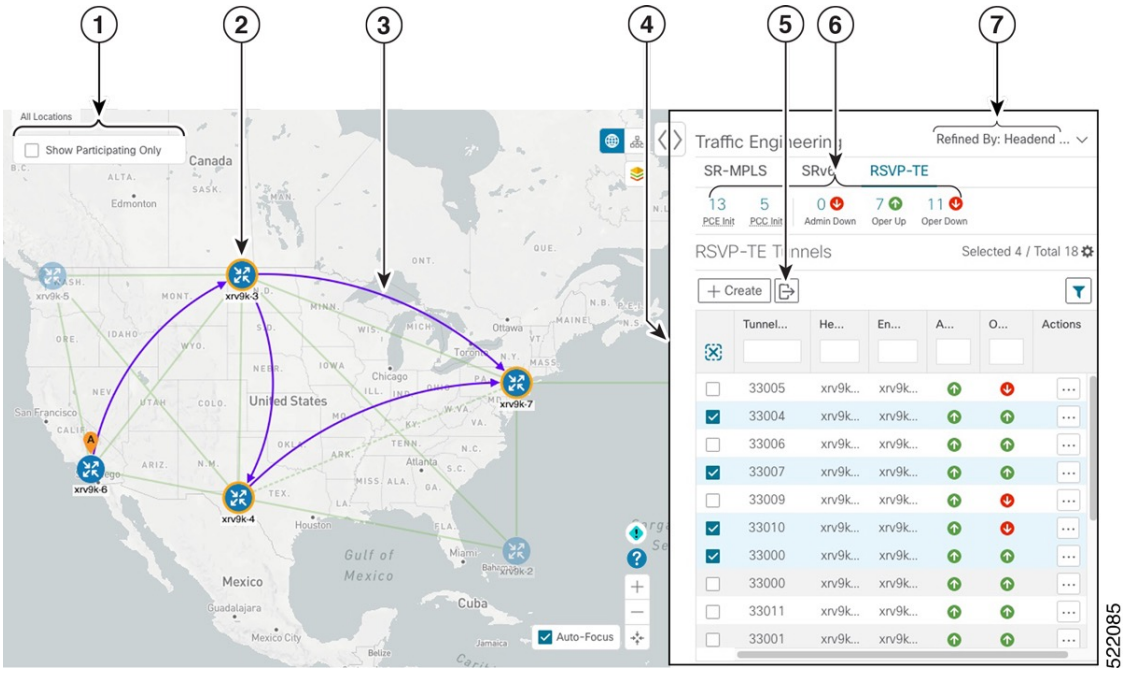
既知の制限事項、重要な注意事項、およびサポートされているネットワークテクノロジーのリストについては、『Cisco Crosswork Optimization Engine Release Notes』を参照してください。

ここでは、次の内容について説明します。

トポロジマップでの RSVP-TE トンネルの表示

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

図 *12 :* 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のみを表示します。他のすべてのリンクとデバイスは表示されなくなります。
2	オレンジ色のアウトラインが付いたデバイス（  ）は、ストリクトホップであることを示します。オレンジ色の点線のアウトラインは、ルーズホップが検出されたことを示します。 （注） RSVP-TE トンネルは、UI でのプロビジョニング時にルーズホップを使用して設定できません。

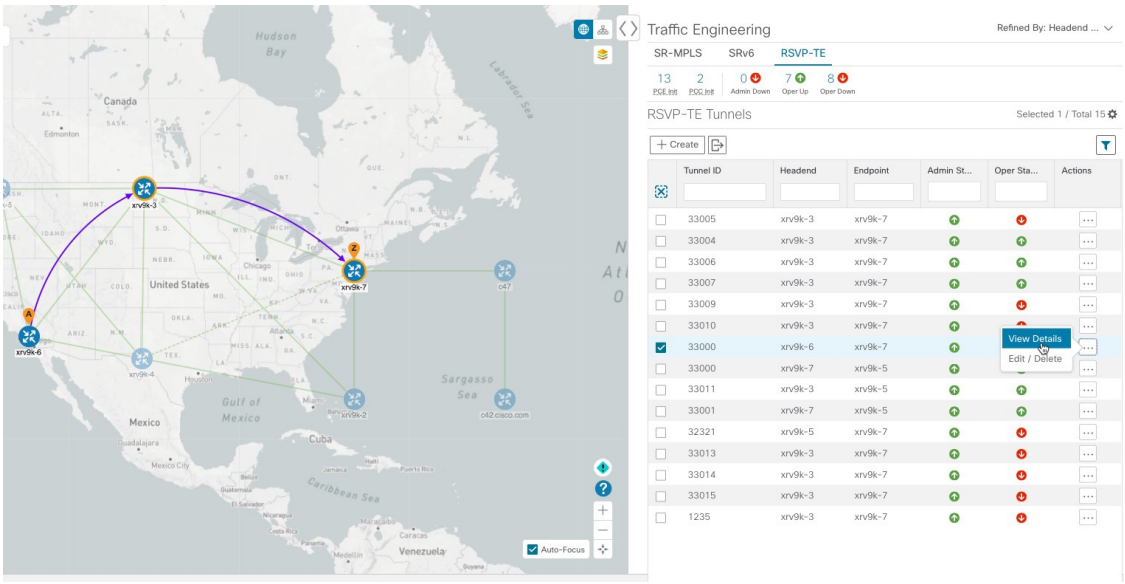
引き出し線番号	説明
3	RSVP-TE トンネルは [RSVP-TE Tunnels] テーブルで選択されると、送信元と宛先を示す紫色の矢印線としてマップに表示されます。 • レコードルートオブジェクト（RRO）パスは直線で表示されます。 • 明示的ルートオブジェクト（ERO）パスは曲線として表示されます。 （注） RRO と ERO の両方のパスが使用可能な場合、デフォルトで RRO パスが表示されます。 • 隣接セグメント ID（SID）は、パスに沿ったリンクに緑色のドット（）として表示されます。 A と Z の両方が 1 つのデバイスクラスタに表示される場合、クラスタ内の 1 つ以上のノードが送信元で、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	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 （100 ページ） • 明示的 RSVP-TE トンネルの作成 （98 ページ） • RSVP-TE トンネルの変更 （101 ページ） • RSVP-TE トンネルの詳細の表示 （84 ページ） • デバイスとリンクの詳細の表示 （16 ページ）
5	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。
6	[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
7	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。 • [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。

RSVP-TE トンネルの詳細の表示

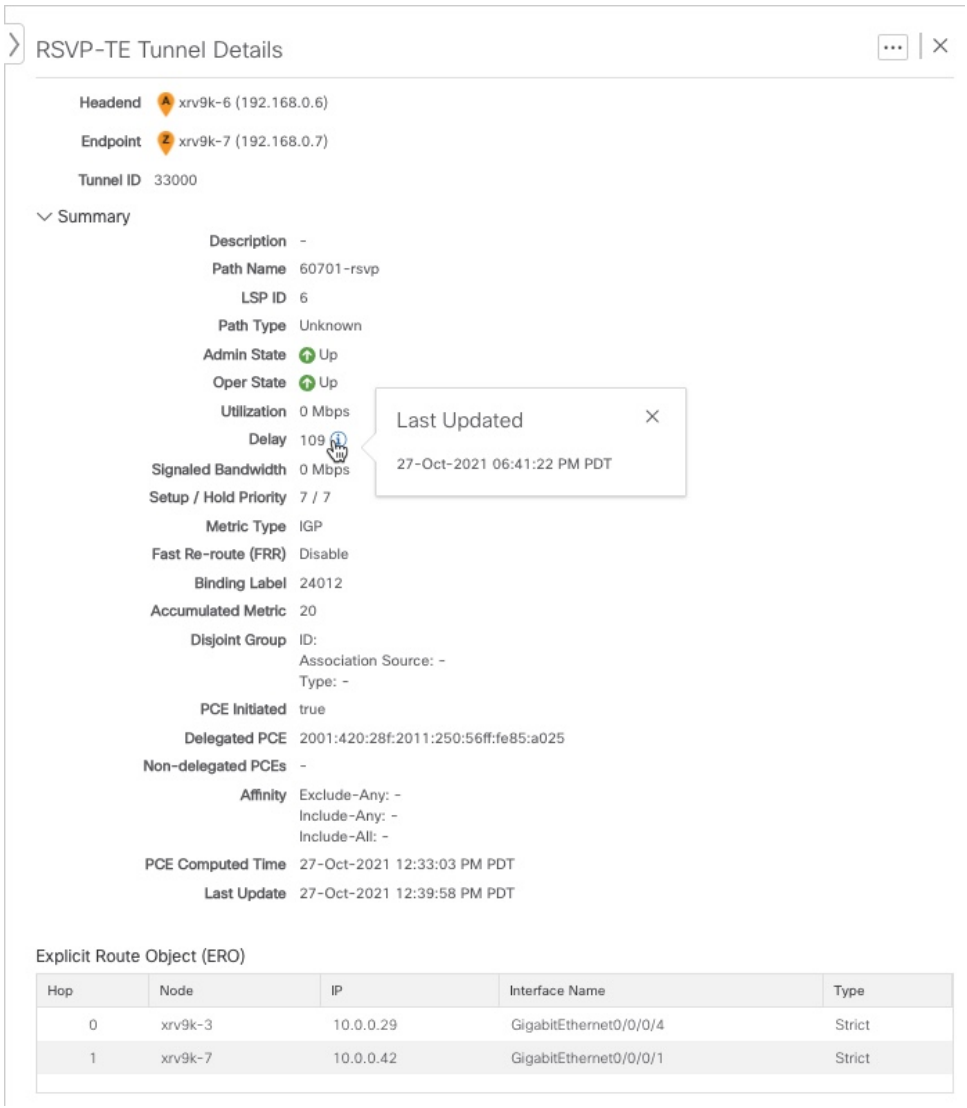
バインディングラベル、委任 PCE、メトリックタイプ、ERO/RRO、遅延など、RSVP-TE トンネルの詳細を表示します。

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



ステップ 2 RSVP-TE トンネルの詳細を表示します。

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



トラフィック エンジニアリング デバイスの詳細の表示

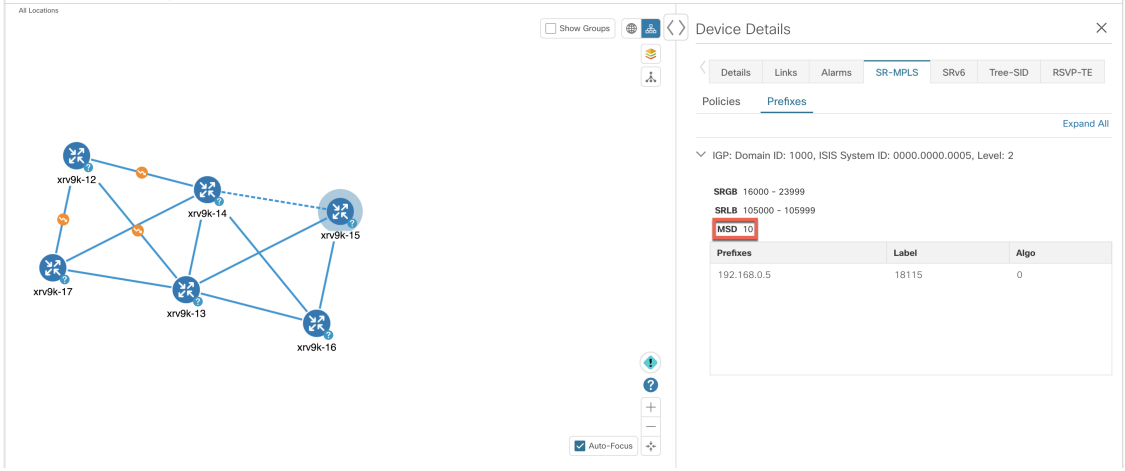
トラフィック エンジニアリング デバイスの詳細（SR-MPLS、SRv6、RSVP-TE、およびフレキシブルアルゴリズム情報）を表示するには、次の手順を実行します。

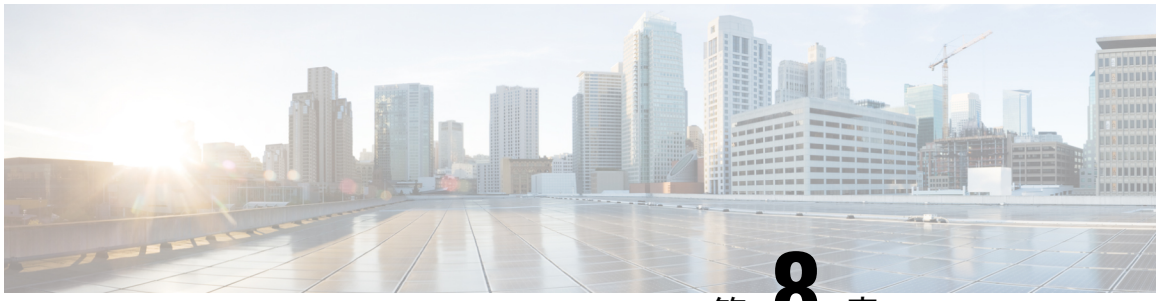
ステップ 1 メインメニューから、[トラフィックエンジニアリング（Traffic Engineering）] > [トラフィックエンジニアリング（Traffic Engineering）] を選択します。

ステップ 2 トラフィック エンジニアリング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 [デバイスの詳細（Device Details）] ページで、目的のトラフィック エンジニアリングのタブをクリックします。各タブには、そのデバイスの関連データが表示されます。

次の例は、デバイスの MSD 値を含む SR-MPLS プレフィックス情報を示しています。





第 8 章

SR-MPLS ポリシーのプロビジョニング

（注） Crosswork Network Controller ソリューション内で Crosswork 最適化エンジン を使用する場合：

- ナビゲーションは、**[トラフィック エンジニアリングおよびサービス（Traffic Engineering & Services）] > [トラフィック エンジニアリング（Traffic Engineering）] > [トラフィック エンジニアリング（Traffic Engineering）]** です。
- SRv6 ポリシーは、NSO メニューからのみプロビジョニングできます。

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。

ここでは、次の内容について説明します。

SR-TE ポリシー設定のソース

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

- PCC によって開始：PCC に設定されたポリシー（PCC によって開始された SR-TE ポリシーの例 （90 ページ）を参照）。このポリシータイプは、UI に [Unknown] と表示されます。
- PCE によって開始：PCE 上に設定されたか、または Crosswork 最適化エンジン によって動的に作成されたポリシー。UI を使用して設定された SR-MPLS の明示的ポリシーまたは動的なポリシーは、Crosswork 最適化エンジン で変更または削除できる唯一の SR-TE ポリシータイプです。PCE によって開始されたポリシータイプは、次のいずれかになります。
  - **Dynamic**

- **Explicit**
- **Bandwidth on Demand**
- **Bandwidth Optimization**
- **ローカル輻輳の緩和**

PCC によって開始された SR-TE ポリシーの例

次に、ヘッドエンドルータでの SR-TE ポリシーの設定例を示します。このポリシーには、ダイナミックパスと、ヘッドエンドルータによって計算されたアフィニティ制約があります。特定のデバイスの SR 設定のマニュアルを参照して、説明とサポートされている設定コマンドを確認してください（『*Segment Routing Configuration Guide for Cisco ASR 9000 Series Routers*』など）。

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

明示的 SR-MPLS ポリシーの作成

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

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

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

ステップ 3 必要な SR-MPLS ポリシー値を入力または選択します。フィールドの説明を表示するには、⑦ の上にマウスポインタを合わせます。

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

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

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

ステップ 6 [プレビュー（Preview）] をクリックして、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。プレビューが表示されない場合は、編集を続行するか、[キャンセル（Cancel）] をクリックします。

ステップ 7 ポリシーパスをコミットする場合は、[プロビジョニング（Provision）] をクリックし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 [SR Policy] テーブルに表示されることを確認します。ポリシーの横にあるチェックボックスをクリックして、マップに強調表示されていることを確認することもできます。

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

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

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

リンクアフィニティの設定

デバイスで定義されたアフィニティ名は Crosswork 最適化エンジンによって収集されません。アフィニティマッピングは、Crosswork 最適化エンジン での可視化にのみ使用されます。このため、デバイスでアフィニティを収集してから、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 Crosswork 最適化エンジン内でアフィニティマッピングを定義する必要があります。Crosswork 最適化エンジン は、プロビジョニング時にビット情報のみを SR-PCE に送信します。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。

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

特定のデバイスの SR 設定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
  !
 !
!
```

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）] > [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。[マッピングの管理（Manage Mapping）] をクリックして、SR-TE ポリシーまたは RSVP-TE トンネルの作成時にアフィニティを定義することもできます。

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

ステップ 3 割り当てる名前とビットを入力します。例（上記の構成を使用）：

例：

ステップ 4 [保存（Save）] をクリックしてマッピングを保存します。

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

最適化インテントベースのダイナミック SR-MPLS ポリシーの作成

このタスクでは、ダイナミックパスを使用してSR-MPLSポリシーを作成します。SR-PCEは、ユーザーが定義したメトリックとパスの制約（アフィニティまたは分離）に基づいてポリシーのパスを計算します。ユーザーは、IGP、TE、または遅延の3つの使用可能なメトリックから選択してパス計算を最小限にすることができます。また、SR-PCE は、トポロジの変更に基づいて、必要に応じてパスを自動的に再度最適化します。リンクまたはインターフェイスに障害が発生した場合、ネットワークは、ポリシーで指定されたすべての基準を満たす代替パスを見つけアラームを起動します。パスが見つからない場合にもアラームを起動し、パケットはドロップされます。

ヒント アフィニティを使用する場合は、デバイスからアフィニティ情報を収集し、Cisco Crossworkにマッピングしてからダイナミック SR-MPLS ポリシーを作成します。詳細については、リンクアフィニティの設定（91 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（60 ページ）を参照してください。

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

ステップ 2 [SR Policy] テーブルで、[+ Create] をクリックします。

ステップ 3 [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、使用可能な場合にパブリックセグメントを使用するかどうかを選択します。

ステップ 8 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） 新たにプロビジョニングされた SR-MPLS ポリシーは、ネットワークのサイズとパフォーマンスによっては、[SR Policy] テーブルに表示されるまでに時間がかかることがあります。[SR Policy] テーブルは 30 秒ごとに更新されます。

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

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

SR-MPLS ポリシーの変更

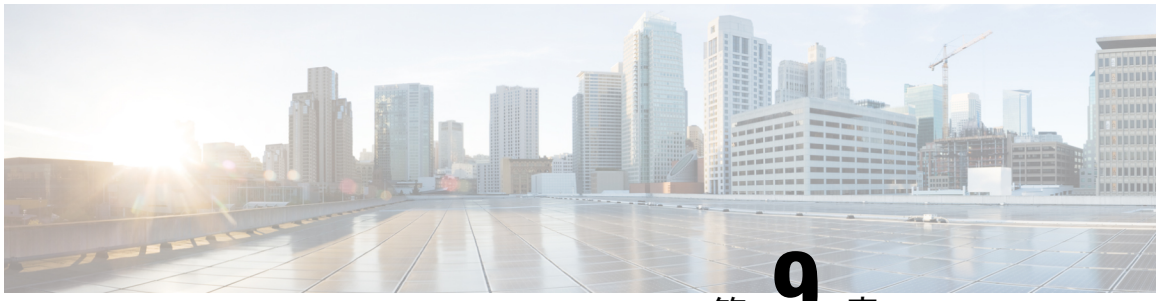
SR-MPLS ポリシーを表示、変更、または削除するには、次の手順を実行します。

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

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

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

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



第 9 章

RSVP-TE トンネルのプロビジョニング

（注） Crosswork Network Controller ソリューションを使用する場合、ナビゲーションは **[トラフィックエンジニアリングおよびサービス（Traffic Engineering & Services）] > [トラフィック エンジニアリング（Traffic Engineering）]** です。

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。

ここでは、次の内容について説明します。

RSVP-TE トンネル設定のソース

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

- PCC によって開始：PCC に設定された RSVP-TE トンネル（PCC によって開始された RSVP-TE トンネルの例 （97 ページ）を参照）。
- PCE または PCC によって動的に開始されました。

PCC によって開始された RSVP-TE トンネルの例

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

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

明示的 RSVP-TE トンネルの作成

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

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

ステップ 2 右側のウィンドウで、[RSVP-TE] をクリックします。

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

ステップ 4 Crosswork Network Controller 内で Crosswork Optimization Engine を使用している場合は、[PCE Init] または [PCC Init] を選択します。

ステップ 5 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、⑦ 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 6 [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 7 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 8 [プレビュー（Preview）] をクリックします。パスがマップに強調表示されます。

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

ステップ 10 RSVP-TE トンネルの作成を検証します。

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

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

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

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

リンクアフィニティの設定

デバイスで定義されたアフィニティ名はCrosswork最適化エンジンによって収集されません。アフィニティマッピングは、Crosswork 最適化エンジン での可視化にのみ使用されます。このため、デバイスでアフィニティを収集してから、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Crosswork最適化エンジン内でアフィニティマッピングを定義する必要があります。Crosswork 最適化エンジン は、プロビジョニング時にビット情報のみを SR-PCE に送信します。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。

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

特定のデバイスの SR 設定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
  !
 !
!
```

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）] > [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。[マッピングの管理（Manage Mapping）] をクリックして、SR-TE ポリシーまたは RSVP-TE トンネルの作成時にアフィニティを定義することもできます。

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

ステップ 3 割り当てる名前とビットを入力します。例（上記の構成を使用）：

例：

ステップ 4 [保存（Save）] をクリックしてマッピングを保存します。

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

最適化インテントベースのダイナミック RSVP-TE トンネルの作成

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

ヒント アフィニティを使用する場合は、デバイスからアフィニティ情報を収集し、ダイナミック RSVP-TE トンネルを作成する前に Cisco Crosswork にマッピングします。詳細については、「リンクアフィニティの設定 （91 ページ）」を参照してください。

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

ステップ 2 右側のウィンドウで、[RSVP-TE] をクリックします。

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

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

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

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

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

ステップ 7　該当する制約と分離を定義します。

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

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

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

ステップ 10　RSVP-TE トンネルの作成を検証します。

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

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

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

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

RSVP-TE トンネルの変更

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

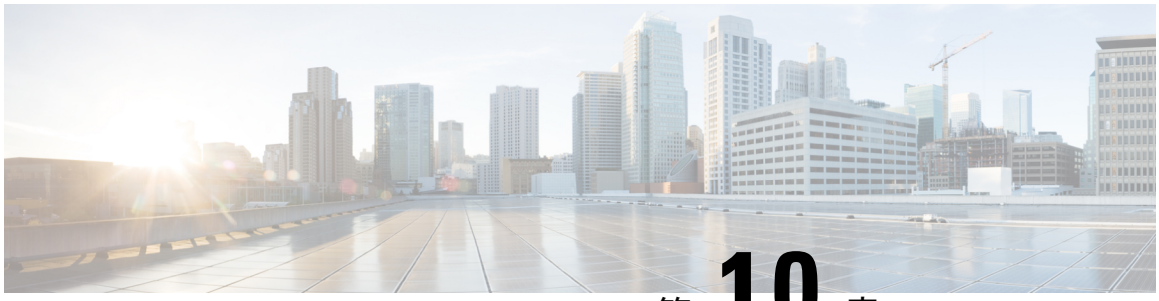
ステップ 1　メインメニューから、**[トラフィック エンジニアリング（Traffic Engineering）]** > **[トラフィック エンジニアリング（Traffic Engineering）]** を選択します。

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

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

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

（注）
- UI 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 10 章

ローカル輻輳緩和（LCM）を使用したローカルでのネットワーク輻輳の緩和

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

ローカル輻輳緩和の概要

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

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

- 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。
- LCM ソリューションの設定に基づいて輻輳とネットワーク障害に対処するために、LCM がネットワークに変更を自動的に展開できるようにします。詳細については、LCM の設定 （119 ページ）の詳細な設定オプション（[Auto Repair Solution] および [Adjacency Hop Type]）を参照してください。

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

（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 （109 ページ）を参照してください。

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 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。
  - リンクがダウンする（LINK_DOWN状態になる）と、LCM設定とドメインUIカード（LCMの設定（119ページ）を参照）は、リンクがエージアウトする（4時間後）まで使用できます。この動作は意図的なもので、誤って実行された場合にドメインインターフェイスとリンクを回復する時間が与えられます。
  - リンクがエージアウトする前にドメインを強制的に削除する場合は、UIから手動でリンクを削除できます。ドメインは、最後のリンクが削除されるまで「削除準備完了」ステータスのままになります。

LCM プラットフォームの要件

次に、LCMを適切に動作させるための大まかな要件のリストを示します。

輻輳評価：

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

輻輳緩和：

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

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

```
segment-routing traffic-eng pcc profile <id> autoroute include ipv4 all
segment-routing traffic-eng pcc profile <id> autoroute force-sr-include
```

  ここで <id> は、ユーザーが設定した ID（ルータごとに許可される任意の数）です。

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

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

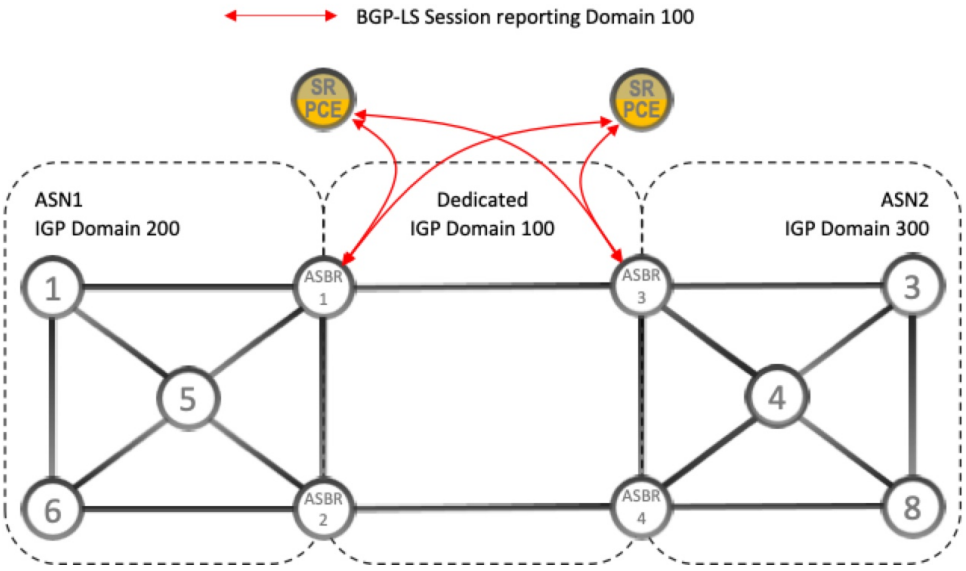
ASBR 間の専用 IGP インスタンスでの複数 AS ネットワークに対する BGP-LS のスピーカー配置

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

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

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

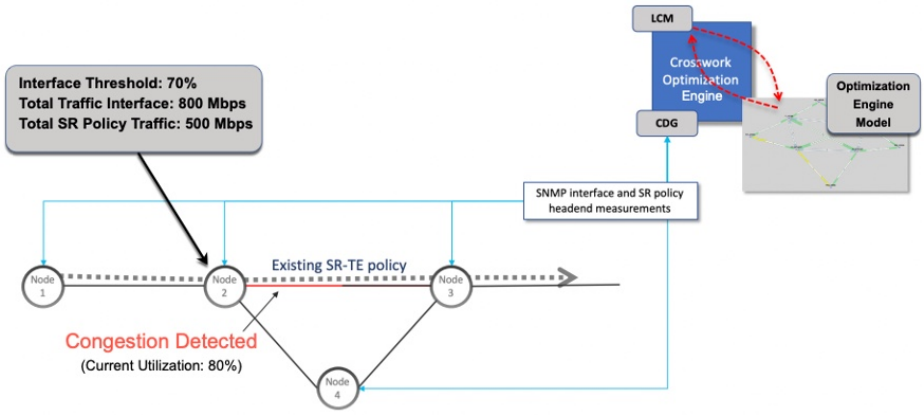
図 *13 : BGP-LS* セッション報告ドメイン *100*



LCM 計算のワークフロー

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

図 *14 : LCM* の設定ワークフローの例



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

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

ステップ 3 LCM は、転送に適したトラフィック量を計算ます。

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

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

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

このプロセスでは、SR ポリシーの ECMP 分割を考慮して、SR ポリシートラフィックを適切にアカウン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 です。ノード 2 経由でルーティングされるすべての SR ポリシーの合計トラフィックは 500 Mbps です。

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

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

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

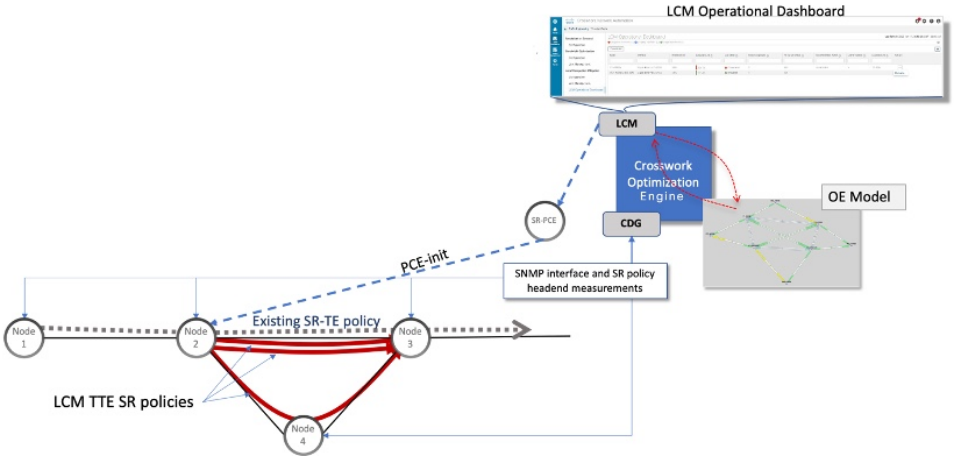
LCM は、300 Mbps のうちの 100 Mbps（対象トラフィック）を別のパスにルーティングする必要があります。オーバープロビジョニング係数（OPF）のパーセンテージが 10 に設定されている場合、LCM は対象トラフィックの 110（100 Mbps X 1.10）をルーティングする必要があることに注意してください。OPF は、[LCM Configuration] ウィンドウの [Advanced] タブで設定できます。詳細については、LCM の設定 （119 ページ）を参照してください。

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

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

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

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



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

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。

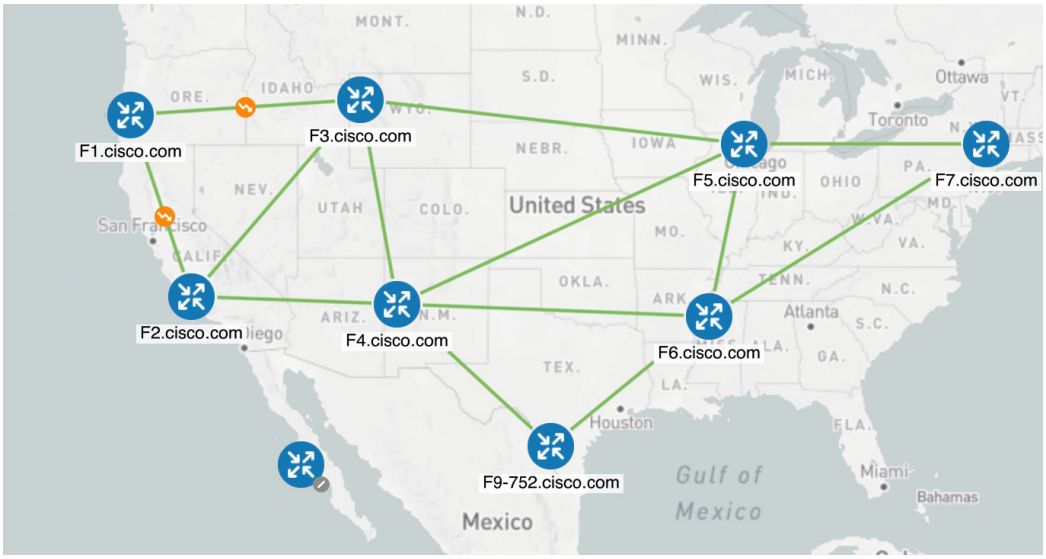
この例では、次のワークフローを示します。

1. 輻輳していないトポロジを表示します。
2. 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. LCM を有効にして設定します。
4. LCM が輻輳を検出した後、[Operational Dashboard] で LCM の推奨事項を表示します。
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。

次の図は、この例で使用されるトポロジを示しています。

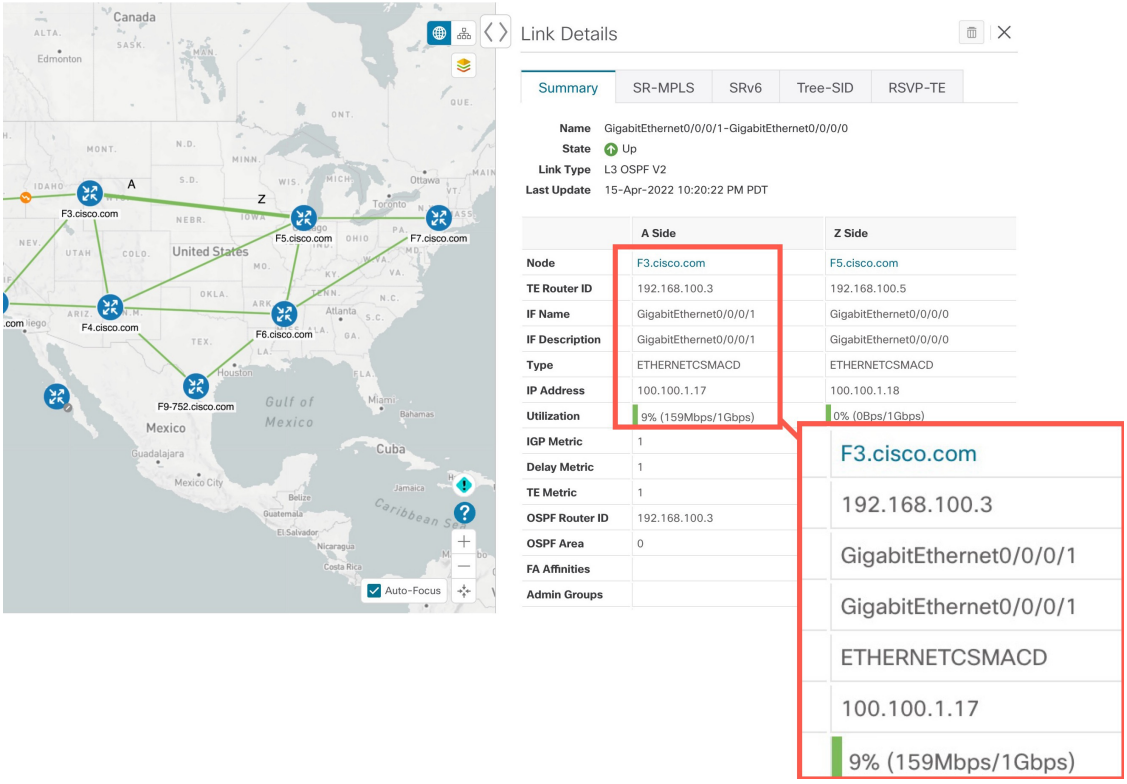
図 *15*：初期トポロジ



ステップ 1 LCM 設定前の初期トポロジと使用率を表示します。

a) F3.cisco.com と F5.cisco.com の間のリンクをクリックして、リンクの詳細を表示します。F3.cisco.com の使用率が 9% であることに注意してください。

図 *16 :* 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

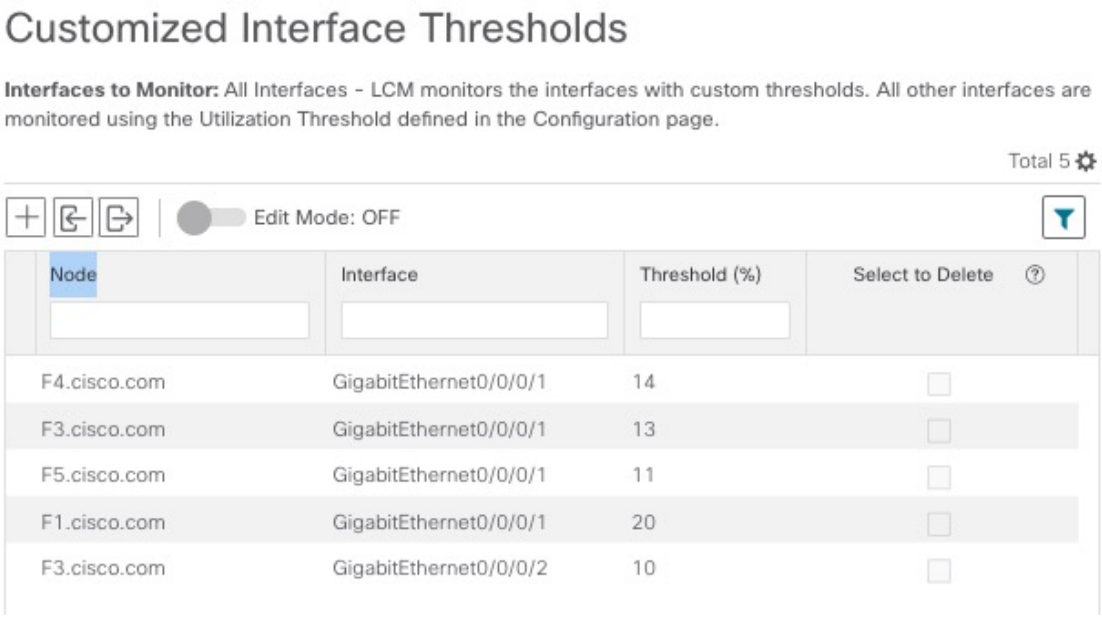
LCM では、すべてのインターフェイスに使用できるグローバル使用率のしきい値を設定できます。トラフィック使用率がしきい値を超えると、LCM は輻輳を修正するためにバイパスポリシーを見つけようとします。[LCMの設定（LCM Configuration）] ページでグローバル使用率のしきい値を設定します。ただし、個々のインターフェイスに異なるしきい値を定義する場合は、LCM を有効にする前に、[カスタマイズされたインターフェイスのしきい値（Customized Interface Threshold）] ページでそれらを定義することをお勧めします。

a) この例では、いくつかの個々のインターフェイスのしきい値を定義しています。[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）]** > [Domain-ID] > ··· > [インターフェイスのしきい値（Interface Thresholds）]）。インターフェイスを追加するか、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 （122ページ）を参照してください。

次の例を参照して、インターフェイスが GigabitEthernet0/0/0/1（13%）の F3.cisco.com およびインターフェイスが GigabitEthernet0/0/0/1（11%）の F5.cisco.com に定義されたしきい値に注意してください。

（注） この例で使用されている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 *17*：カスタマイズされたインターフェイスのしきい値



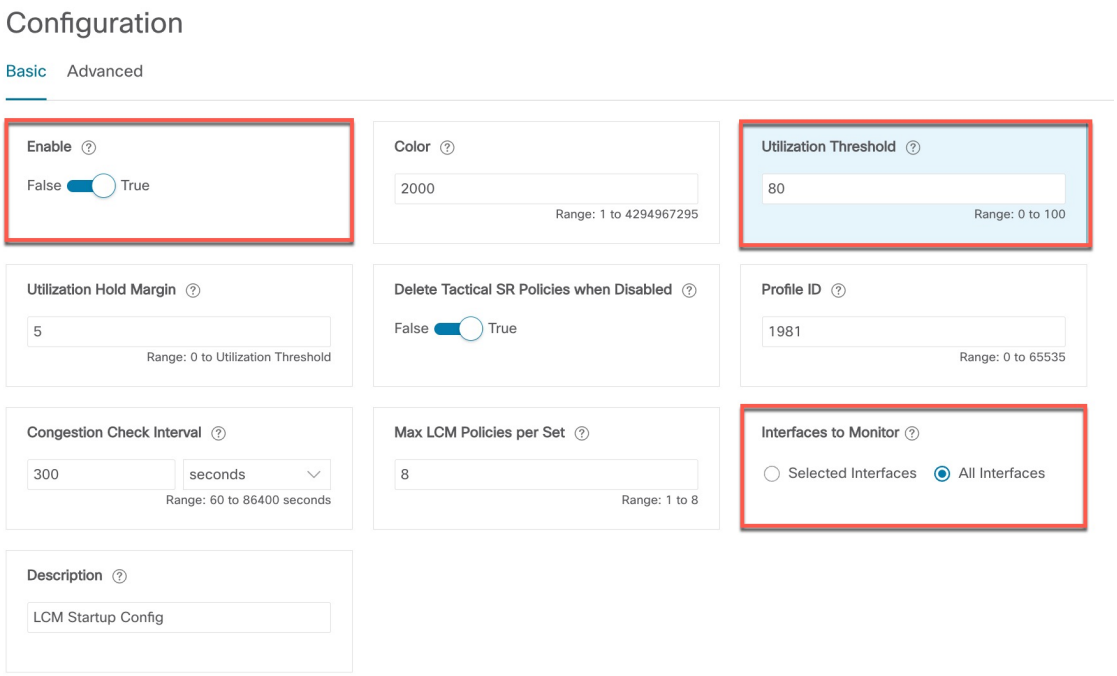
（注） デフォルトでは、LCM はすべてのインターフェイスを監視します。対象には、このページにインポートされた個々のしきい値が含まれます。残りのインターフェイスは、[LCMの設定（LCM Configuration）] ペーシ（**ステップ 3** を参照）で定義されたグローバルな [使用率のしきい値（Utilization Threshold）] を使用して監視されます。

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）]**> [Domain-ID] 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。すべての使用できるオプションの詳細については、LCM の設定 （119 ページ）を参照してください。

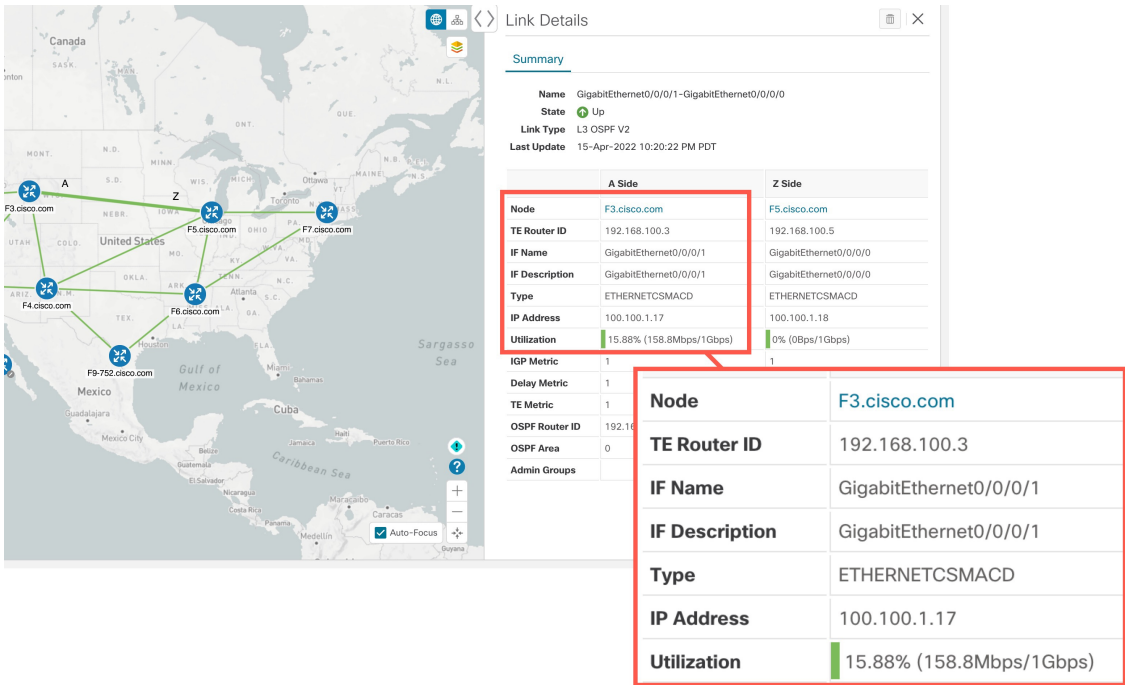
図 *18 : LCM* 設定ページ



b) [Commit Changes] をクリックして、設定を保存します。設定の変更をコミットすると、LCM はモニター対象インターフェイスで輻輳が発生した場合、[LCM Operational Dashboard] に推奨事項を表示します。LCM は新しい TTE ポリシーを自動的にコミットまたは展開しません。後で、推奨される TTE ポリシーをプレビューし、それらのポリシーをコミットしてネットワークに展開するかどうかを決定できます。

ステップ 4 しばらくすると、インターフェイスが GigabitEthernet0/0/0/1 のノード F3.cisco.com に 13% 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。

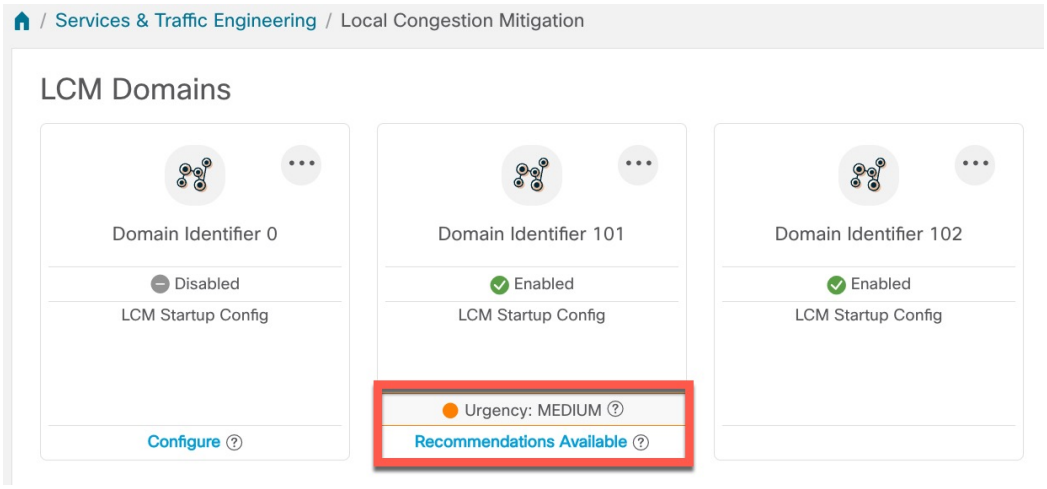
図 *19*：確認された輻輳



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 *20*：検出された輻輳と *LCM* の推奨事項



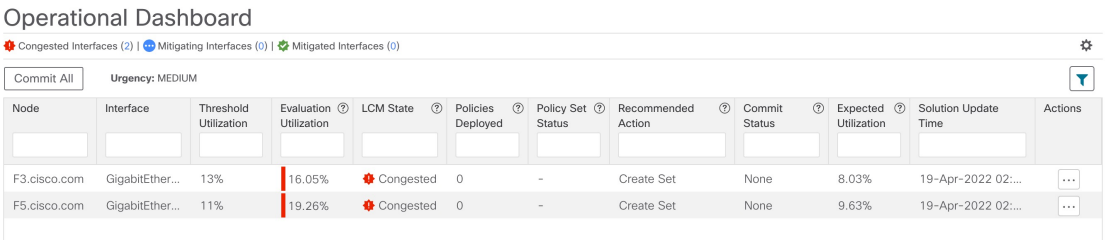
b) （オプション）LCM イベントを表示します。

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

ダッシュボードには、F3.cisco.com の使用率が 13% を超えており、16.05% であることが示されます。また、F5.cisco.com の使用率が 11% のしきい値を超えており、現在 19.26% であることも示されています。[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。[予想使用率（Expected Util）] 列には、推奨処置が実行された場合の各インターフェイスの予想使用率が表示されます。詳細については、LCM 動作のモニター （124 ページ）を参照してください。

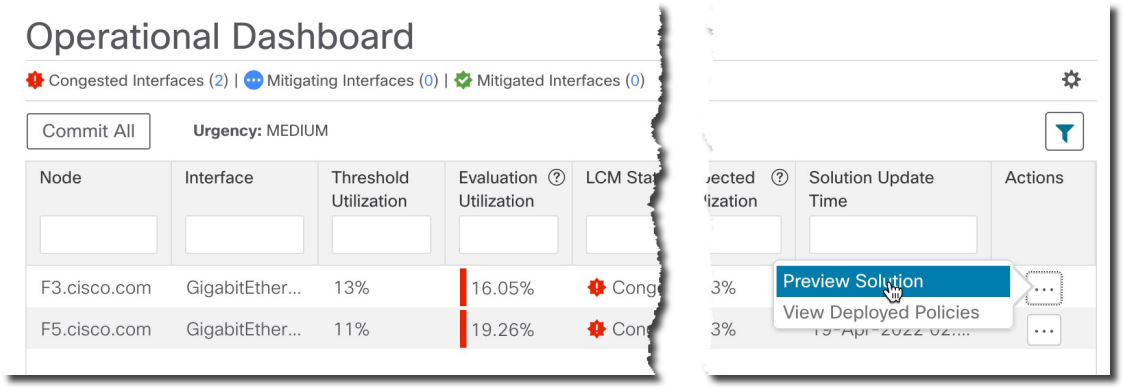
図 *21 : [LCM Operational Dashboard]*



（注） LCM で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。

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 *22 : [*解決策のプレビュー（*Preview Solution***）*]* を選択**

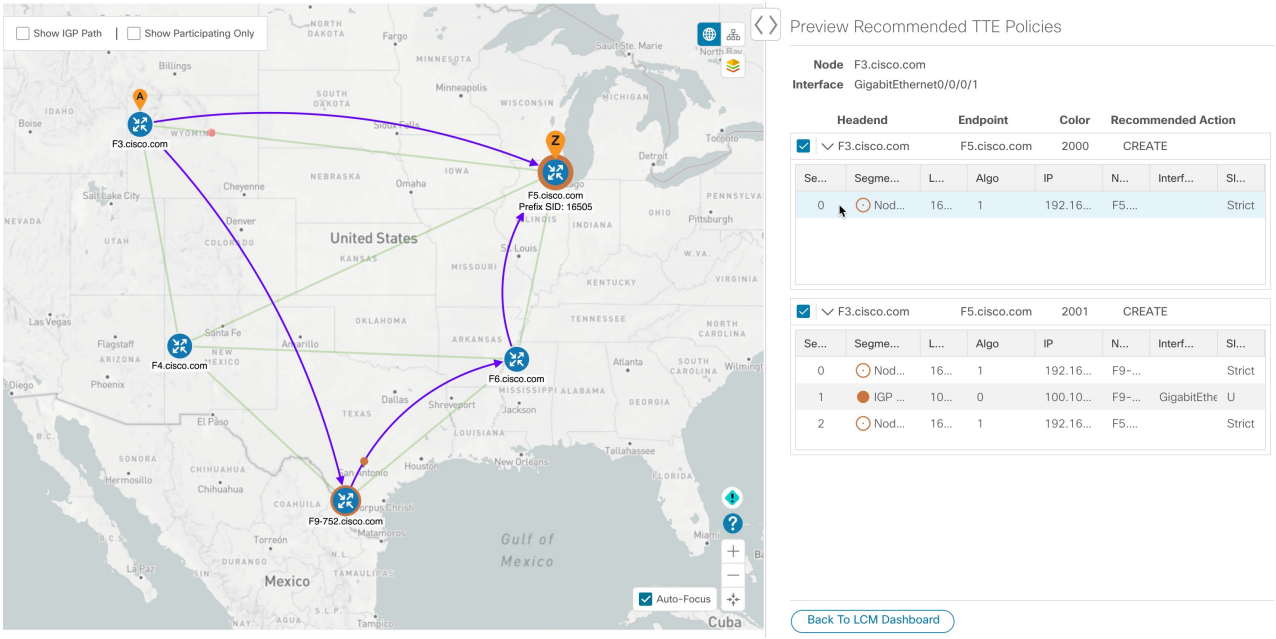


各 TTE ポリシーのノード、インターフェイス、および推奨アクションがウィンドウに表示されます。[Preview] ウィンドウから、個々の TTE ポリシーを選択し、トポロジマップで通常行っているように、さまざまな側面と情報を表示できます。各ポリシーを展開して、個々のセグメントを表示できます。

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。

次の図に、ノード F3.cisco.com とインターフェイス GigabitEthernet0/0/0/4 の推奨 TTE ポリシーを示します。上のパスには、ノード SID（オレンジ色のアウトライン）、ヘッドエンド、エンドポイント（A および Z）が表示されます。これはマウスポインタが該当するセグメントの上にあるためです。

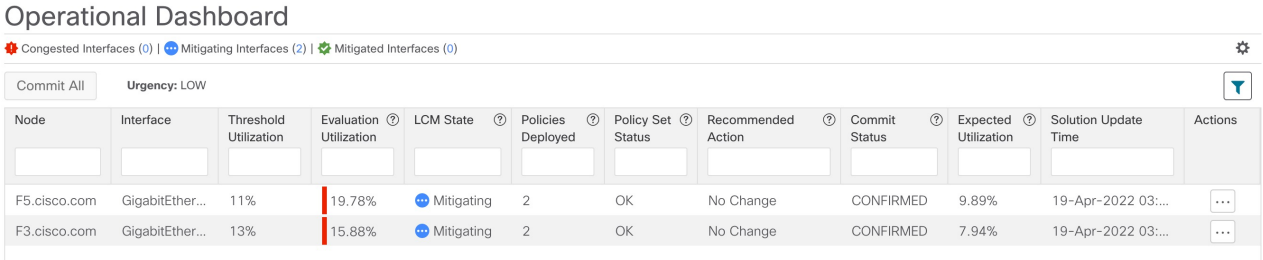
図 *23 : LCM TTE* 展開のプレビュー



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 [ステータス（Status）] 列が [緩和中（Mitigating）] に変化します。

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

図 *24 : LCM* 状態の緩和



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 Optimization Engine は、有効にしたポリシーと機能に基づいて検出されたネットワークイベントを報告します。たとえば、リンク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。

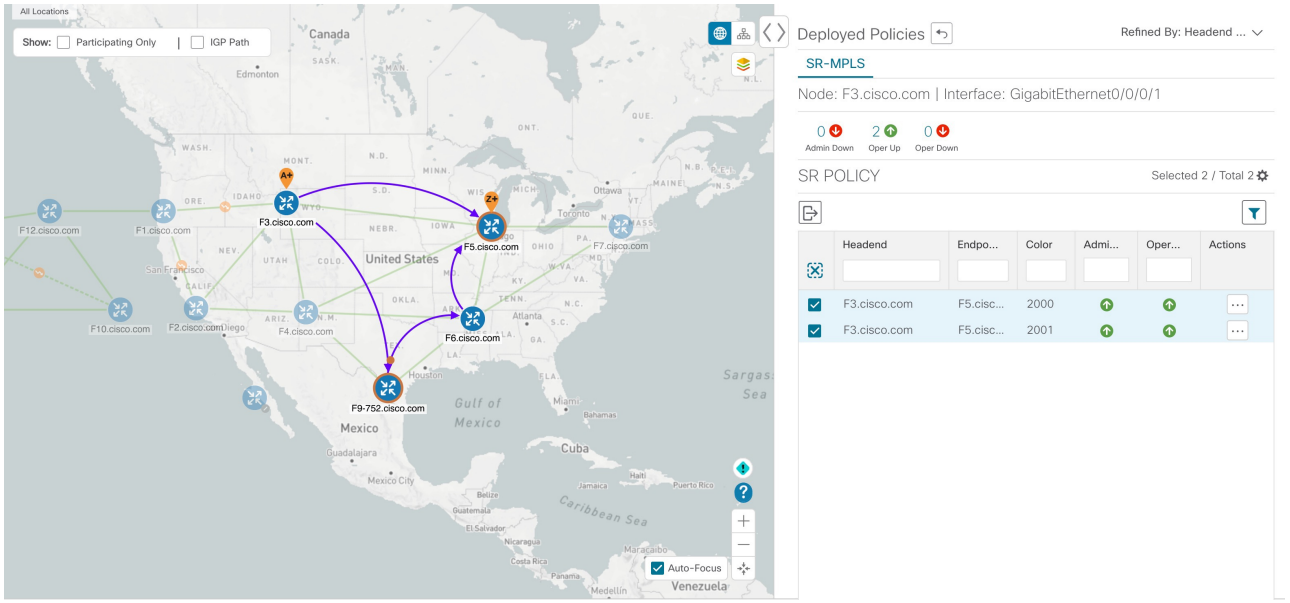
b) [Operational Dashboard] に戻り、すべての TTE ポリシー ソリューション セットの LCM の状態が [Mitigated] に変化したことを確認します。

（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。他のすべてのポリシーは淡色表示されます。

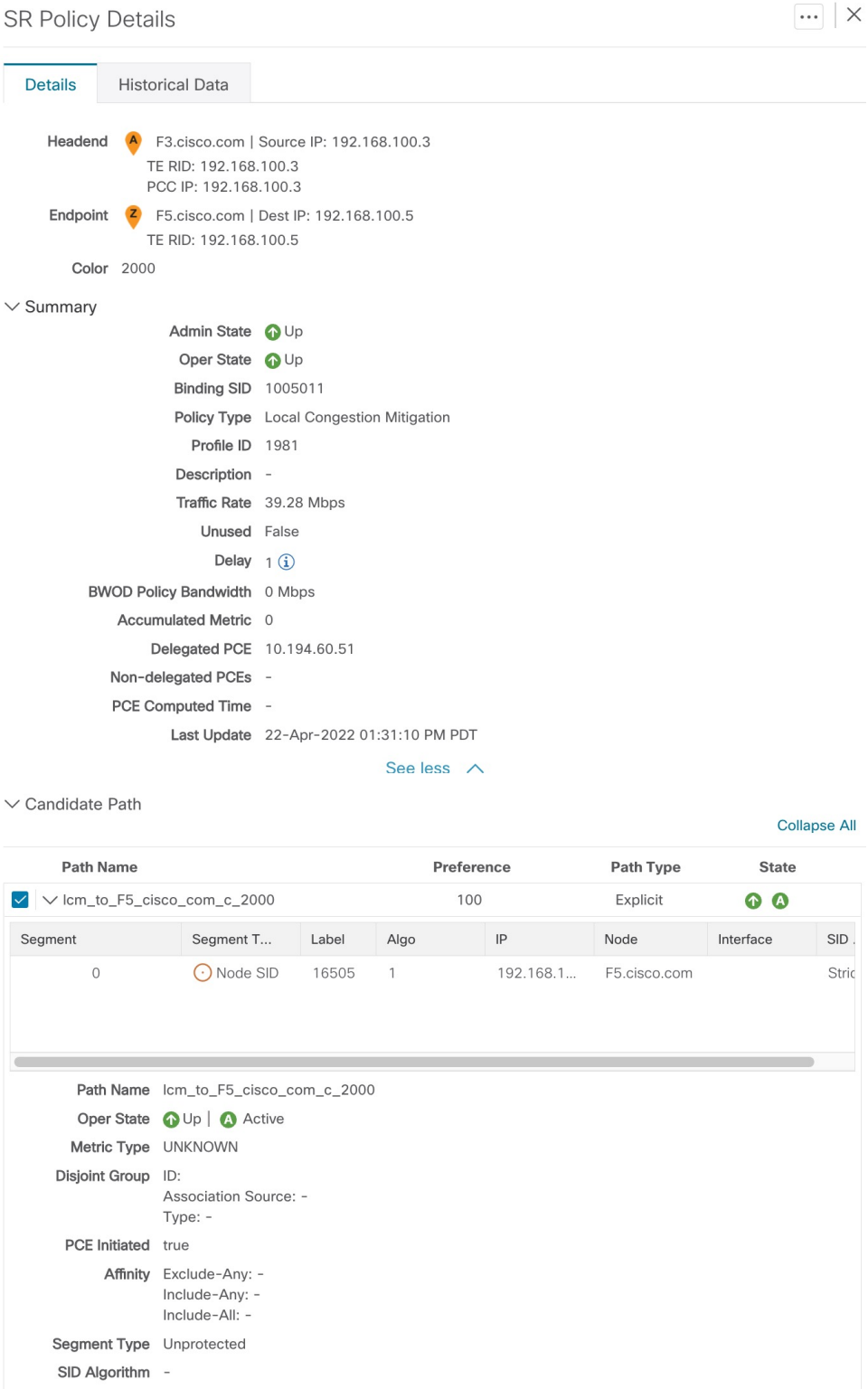
図 *25*：トポロジマップでの *TTE* 展開ポリシーの表示



d) SR ポリシーの詳細を表示します。

展開されたポリシーのいずれかの [アクション（Actions）] 列で、… をクリックし、[詳細の表示（View Details）] を選択します。[ポリシータイプ（Policy Type）] が [ローカル輻輳緩和（Local Congestion Mitigation）] であることに注意してください。

図 *26 : SR* ポリシーの詳細



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らない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。

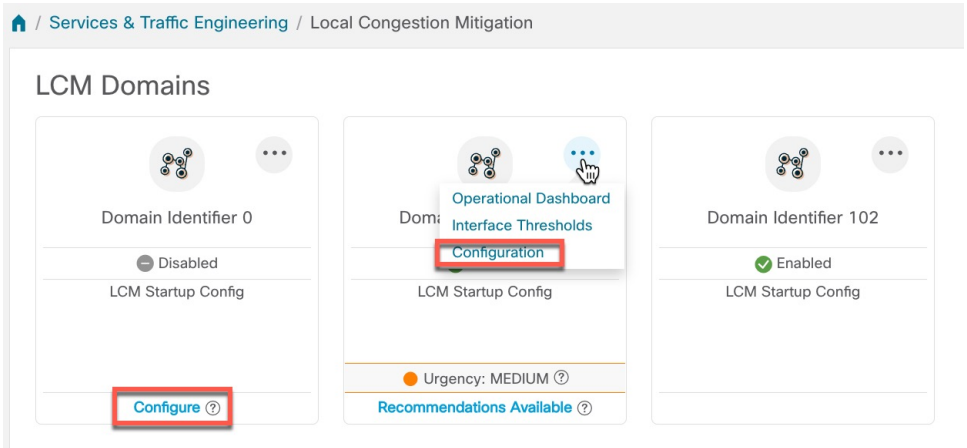
このシナリオでは、LCM を活用してネットワークのトラフィックの輻輳を軽減する方法を確認しました。LCM では、手動による追跡と計算は不要であり、同時に輻輳緩和の推奨事項を実装するかどうかを制御できます。推奨事項をプレビューして、展開する前にネットワークでの展開の有効性を確認できます。トラフィックが変化すると、LCM は展開された TTE SR-TE ポリシーを追跡し、それらのポリシーがまだ必要かどうかを判断します。必要でない場合、LCM は削除を推奨します。

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。

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] を選択し、次のいずれかをクリックします。

- ··· > [設定（Configuration）]
- **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。

次のリストに、ホバーテキストでは説明されていない追加のフィールド情報を示します。

- [Utilization Threshold]：インターフェイスが輻輳していると LCM が判断する使用率を設定します。この値は、[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、推奨事項を変更する必要があるかどうかを判断します。たとえば、間隔が 600 秒（10 分）に設定されている場合、LCM は 10 分ごとにネットワークを評価して新しい輻輳を確認し、新しい推奨事項、または既存の推奨事項に対する変更が必要かどうかを判断します。変更の例としては、以前に推奨された個々のポリシーの削除や更新などがあります。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）]** > [Domain-ID] > ··· > [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）]）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。
- [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。
- [Advanced] > [Auto Repair Solution]：[True] に設定すると、LCM はダウン、失敗、またはコミットされていない LCM TTE ポリシーを自動的に削除します。これは、主にポリシーの障害に対処するためのオプションです。

  このオプションが無効で、[LCM Operational Dashboard] に表示される推奨の [Urgency] ステータスが [High] の場合、推奨されるソリューションは [Auto Repair Solution] の候補です。これは、ソリューションが展開されていない場合にネットワーク障害が発生する可能性が高いことを意味します。

- [Advanced] > [Adjacency Hop Type]：[Protected] に設定すると、LCM は保護された隣接関係 SID を使用して SR ポリシーを作成します。これにより、トポロジに依存しないループフリー代替（TI-LFA）で隣接関係の障害のパスを計算できます。

  （注） このオプションは、LCM が動作している同じ IGP エリア内のすべてのノードが厳密な SPF SID 対応である場合にのみ、[Protected] に設定する必要があります。

- [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。

- [Advanced] > [Over-provisioning Factor (OPF)]：このオプションは、不均等な ECMP トラフィック分散（エレファントフロー）に対処するのに役立ちます。この値により、バイパスポリシーのパスを計算するときに考慮する必要がある追加トラフィックの割合が決まります。LCM は、輻輳が原因でトラフィック量 x を転送させる必要がある場合、x *（1＋OPF）トラフィックをサポートできるパスを検索します。詳細については、LCM 計算のワークフロー （107 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。詳細については、トラフィック エンジニアリング デバイスの詳細の表示 （37 ページ）を参照してください。

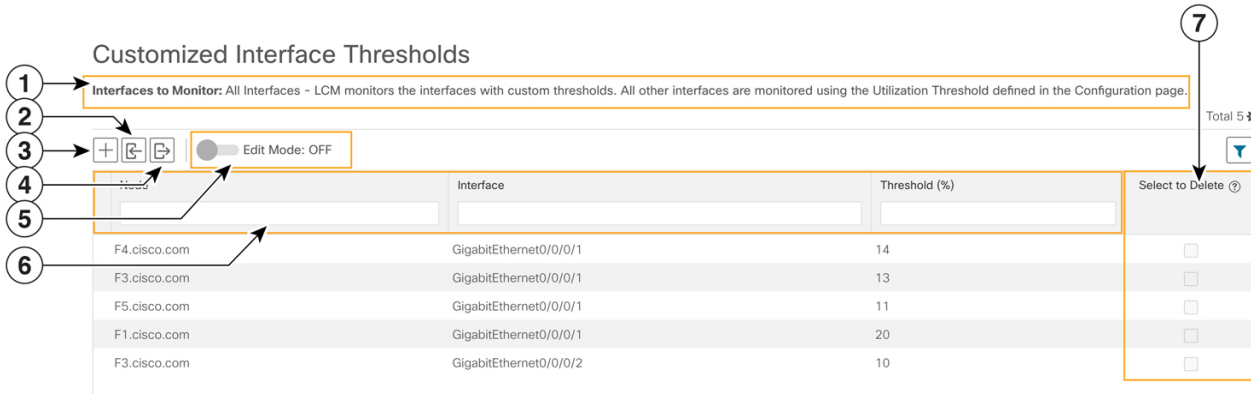
  （注） このオプションを使用する前に、特定の MSD 値を割り当てるデバイスタググループを作成する必要があります。タグの作成とデバイスへのタグの割り当てについては、『*Crosswork Infrastructure and Applications Administration Guide*』を参照してください。

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

個別のインターフェイスしきい値の追加

ネットワークにはさまざまなリンク（10G、40G、100G）があり、異なるしきい値を設定する必要があります。[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 *27*：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 （119 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。
3	**追加**：このアイコンをクリックして、新しいインターフェイスのしきい値行を追加します。
4	**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。
5	[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。
6	**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。フィルタリング機能を無効または有効にするには、 をクリックします。

引き出し線番号	説明
7	**選択して削除**：[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）] をクリックします。

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。

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] > ··· > [インターフェイスのしきい値（Interface Thresholds）] を選択し、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 *28*：最初のインターフェイスの追加

b) さらにインターフェイスを追加するには ⊞ をクリックします。

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。詳細については、図 15 を参照してください。

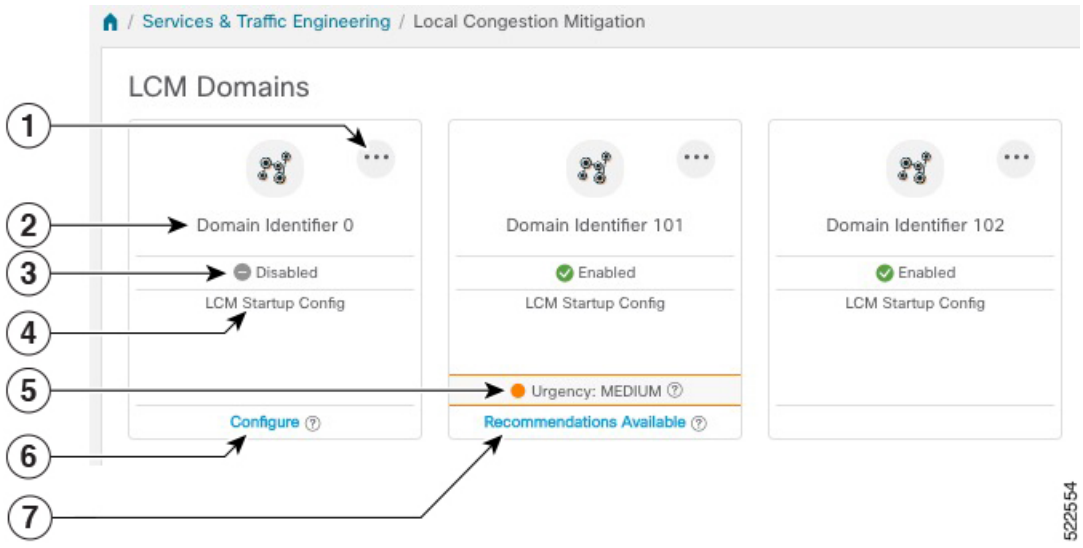
LCM 動作のモニター

（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（109 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（**[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 *29 : 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	[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 （119 ページ）」を参照してください。
6	**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。
7	**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。

[LCM Operational Dashboard]

[LCM Operational Dashboard]（**[Traffic Engineering] > [Local Congestion Mitigation] > *[Domain-ID]* > ⋯ > [Operational Dashboard]**）には、設定された使用率しきい値で定義された輻輳インターフェイスが表示されます。

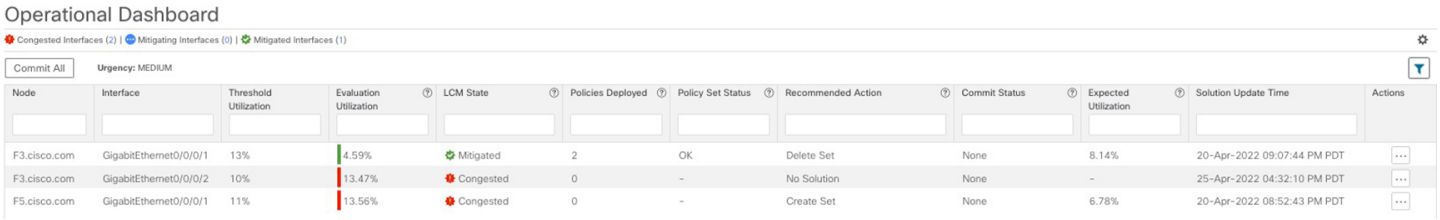
各インターフェイスについて、現在の使用率、推奨アクション、ステータス、推奨をコミットした後に予想される使用率などの詳細がリストされます。展開前に TTE ポリシーをプレビューしたり（⋯ > [ソリューションのプレビュー（Preview Solution）]）、トポロジマップ上で視覚

的に展開を確認したり（… > [展開されたポリシーを表示（View Deployed Policies）]）することもできます。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。

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 *30 : [LCM Operational Dashboard]*



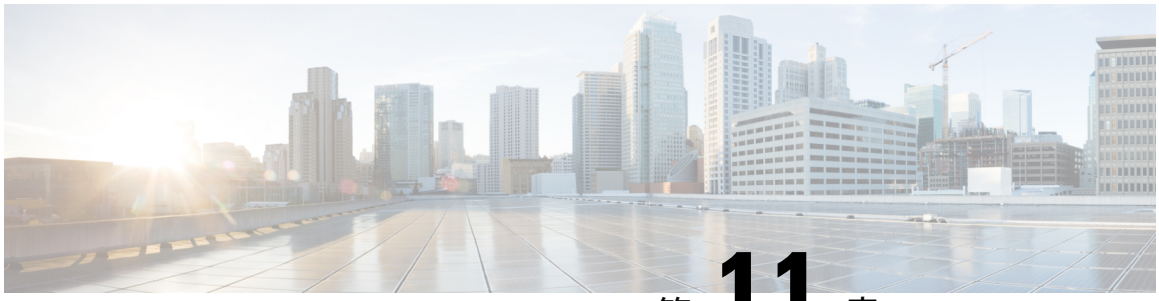
この例では、次の情報が伝えられます。

- インターフェイスが GigabitEthernet0/0/1 の f3.cisco.com：現在の LCM の状態は Mitigated であり、以前の輻輳を軽減するために 2 つのポリシーが展開されていること（[展開されたポリシー（Policies Deployed）] : 2）を示しています。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。
- インターフェイスが GigabitEthernet0/0/2 の f3.cisco.com：LCM は輻輳を検出しますが、輻輳を修正するためのバイパスポリシーを見つけることができません（[推奨処置（Recommended Action）] : [解決策なし（No Solution）]）。

（注） LCM が解決策を見つけられない（[解決策なし（No Solution）]）場合、[LCMの設定（LCM Configuration）] 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。詳細については、LCM の設定 （119 ページ）を参照してください。

- インターフェイスが GigabitEthernet0/0/1 の f5.cisco.com：LCM は輻輳を検出し、輻輳を修正するためのポリシーを展開することを推奨しています（[推奨処置（Recommended Action）] : [セットの作成（Create Set）]）。

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。インターフェイスが GogabitEthernet0/0/1 の F5.cisco.com で輻輳を修正する場合は、[すべてコミット（Commit All）] をクリックする必要があります。



第 11 章

帯域幅最適化（BWOpt）を使用したネットワークの最適化

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

帯域幅最適化の概要

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

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

BWOpt に関する特記事項

BWOpt を使用する場合は、次の情報を考慮してください。

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

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

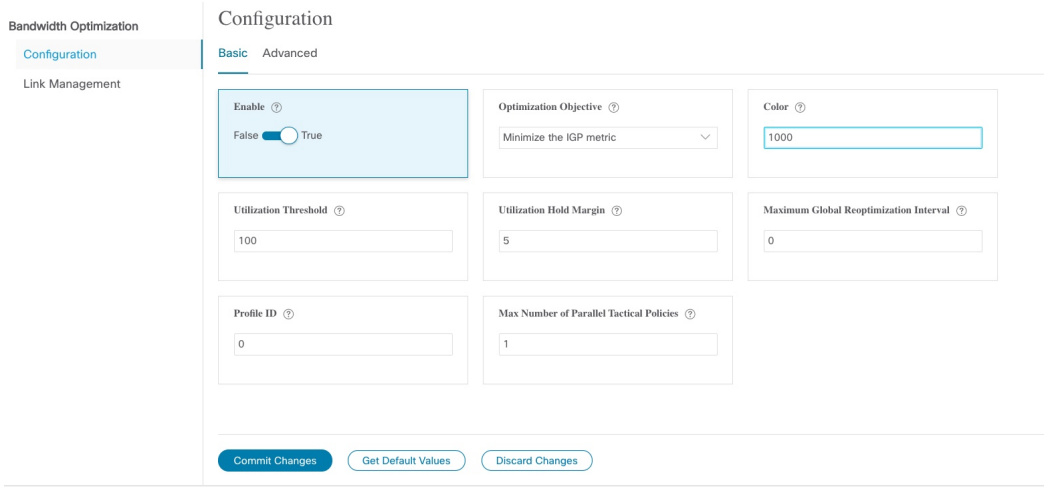
- BWOpt は、測定された SR-TM データに基づいてシミュレートされたトラフィックを使用して、リンク使用率と輻輳を緩和するタイミングを決定します。BWOpt がモニターするシミュレートされたインターフェイス使用率は、UI に表示される SNMP ベースのインターフェイス使用率と厳密に一致する必要があります。ただし、SNMP ポーリング頻度やレート平均化手法などのさまざまな要因により、それらが異なる場合があります。これにより、UI でリンクが輻輳しているように見え、BWOpt が反応していないという状況になることがあります。
- BWOpt は、SRTM テレメトリデータの送信元である PCC にのみ戦術的な SR-TE ポリシーを作成します。これらのノード（通常はプロバイダーエッジルータ）のみが、そのノードからネットワーク内の他の PE ノードへのトラフィックを表す内部モデル内のシミュレーションされたトラフィック要求を作成するために必要なテレメトリベースのデータを提供します。
- （すべてのインターフェイスに対して設定された）しきい値を下回るインターフェイス使用率になるソリューションのみが展開されます。BWOpt がネットワーク全体の輻輳を緩和できない場合は、戦術的な SR-TE ポリシーを展開し、「ネットワークが輻輳しています。BWOpt で緩和できません。（Network Congested. BWOpt unable to mitigate.）」というアラームが発生します。このアラームは、輻輳が自然に軽減されるか、または BWOpt の戦術的 SR-TE ポリシーの展開によってうまく対処できた場合に解消されます。
- BWOpt は、トポロジサービスからのトポロジの再起動または再構築が原因でシステムが使用できなくなった場合は常に、一時的に動作を停止します。これが発生すると、この状態を示すアラームが BWOpt によって設定されます。この間、BWOpt はネットワークの輻輳を評価しません。現在展開されているすべての 戦術的 SR ポリシーは維持されますが、変更または削除されません。モデルが使用可能になるとすぐにアラームがクリアされ、BWOpt は通常の動作を再開します。

自動化されたネットワーク輻輳の緩和の例

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

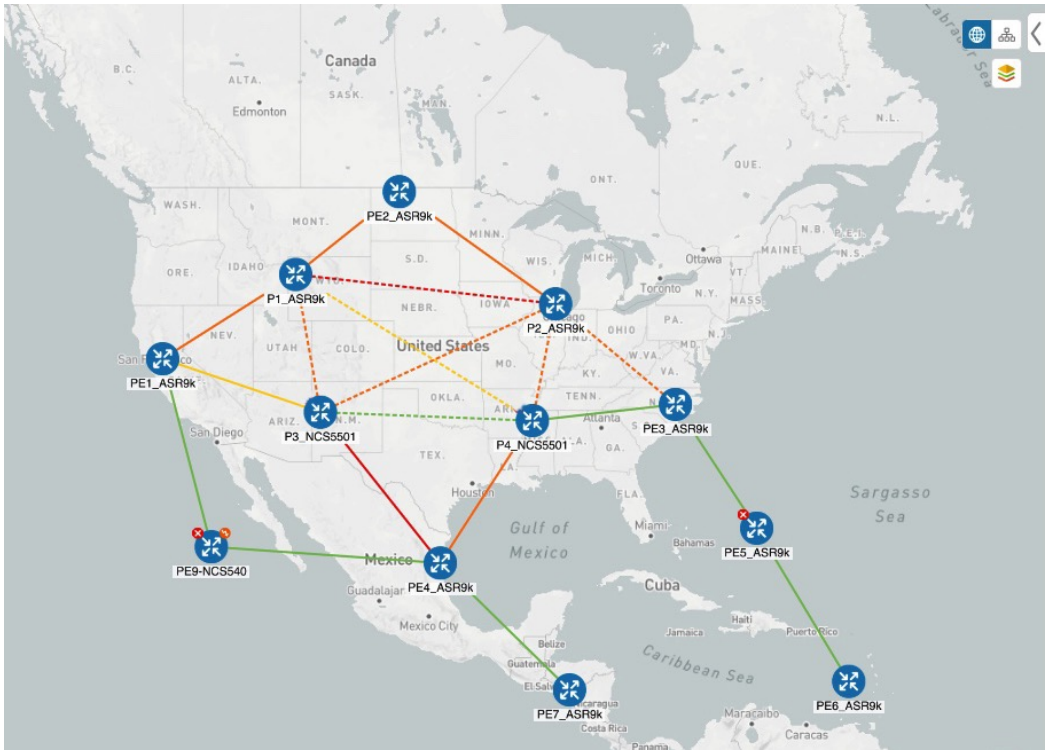
次の BWOpt オプションが設定されます（**[トラフィック エンジニアリング（Traffic Engineering）] > [帯域幅最適化（Bandwidth Optimization）] > [設定（Configuration）]**）。

図 *31 :* 帯域幅最適化の設定



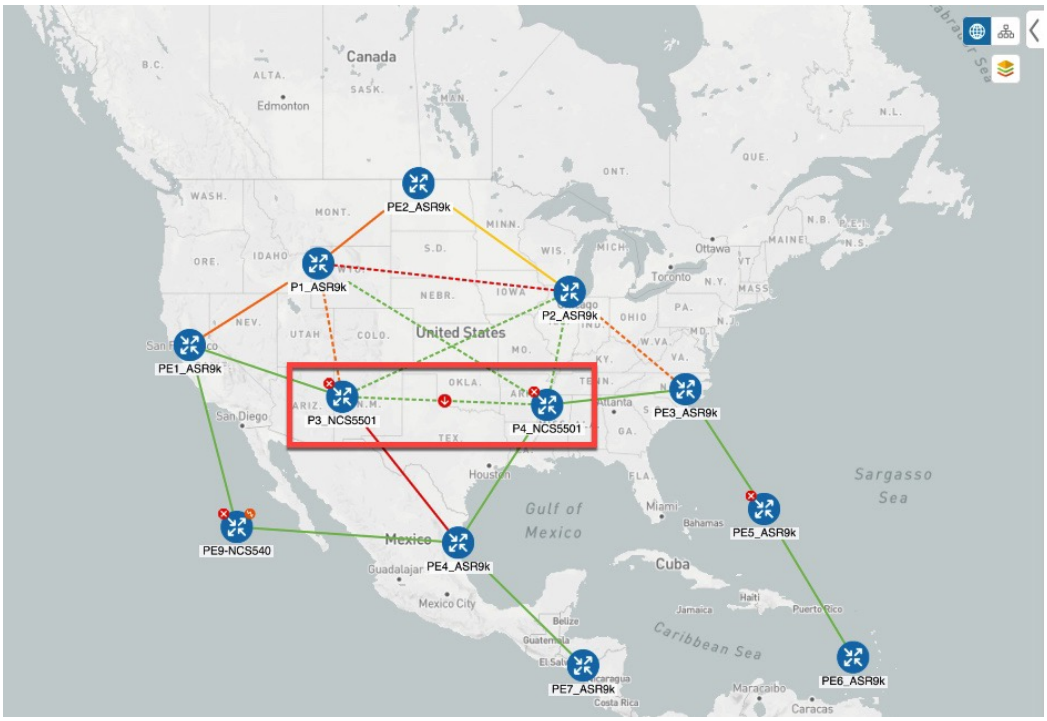
次に、米国に及ぶさまざまなデバイスとリンクのネットワークを示します。[SRポリシー（SR Policies）] テーブルに SR-TE ポリシーがリストされていないことに注意してください。

図 *32 :* 例：現在のネットワーク



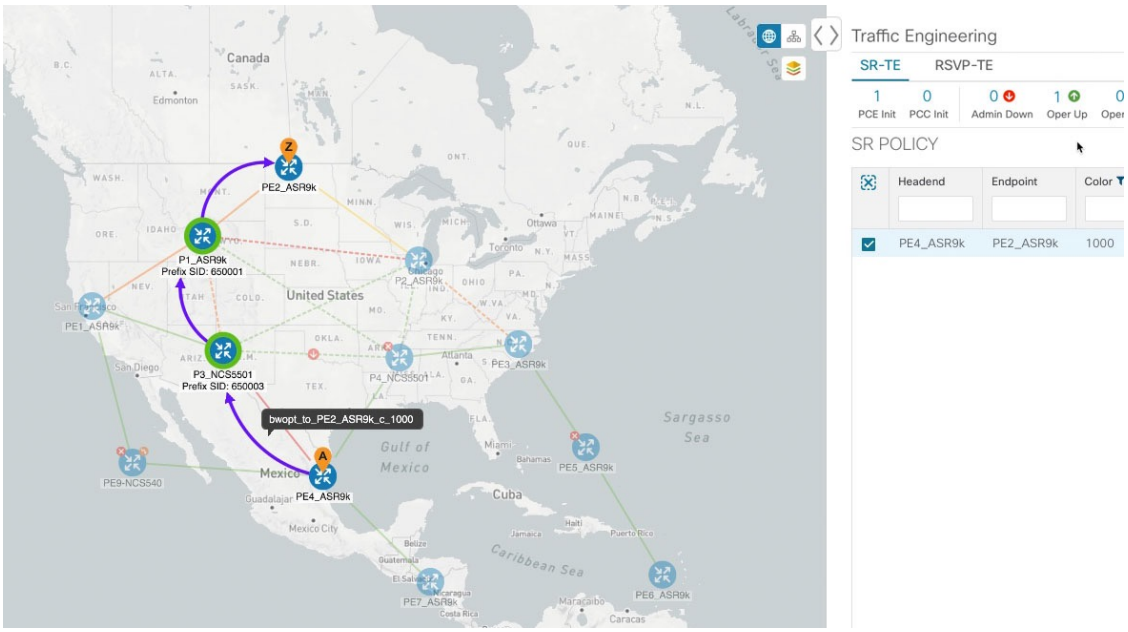
P3_NCS5501 と P4_NCS5501 間のリンクがダウンしたとします。トラフィックが他のリンクに移動し、それによって輻輳が発生して、設定された使用率のしきい値を超えます。

図 *33* : 例：*P3* ノードと *P4* ノード間のリンクのダウン



BWOpt は輻輳を認識し、すぐに戦術的な SR-TE ポリシーを計算して展開します。この新しい戦術的な SR-TE ポリシーは、[SRポリシー（SR Policies）] ウィンドウに表示されます。

図 *34* : 例：展開された戦術的 *SR* ポリシー



BWOptは、ネットワークを継続的にモニターします。P3_NCS5501とP4_NCS5501間のリンクが復旧すると、BWOptは（定義された基準に基づいて）輻輳が緩和されたことを検出します。輻輳が、設定された使用率しきい値から使用率ホールドマージンを差し引いた値を下回ると、戦術的SR-TEポリシーは自動的にネットワークから削除されます。

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

帯域幅最適化の設定

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

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

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

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

（注） LCMと帯域幅の最適化を同時に有効にすることはできません。

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

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

個別のインターフェイスしきい値の追加

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

ステップ1 メインメニューから、**[トラフィックエンジニアリング（Traffic Engineering）]>[帯域幅最適化（Bandwidth Optimization）]>[インターフェイスのしきい値（Interface Thresholds）]**を選択します。

ステップ2 [CSVファイルのインポート（Import .CSV File）]をクリックします。

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

ステップ 4 [キャンセル（Cancel）] をクリックします。

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

ステップ 6 ファイルの名前を変更して保存します。

ステップ 7 [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）] ウィンドウに戻ります。

ステップ 8 [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。

ステップ 9 [インポート（Import）] をクリックします。

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

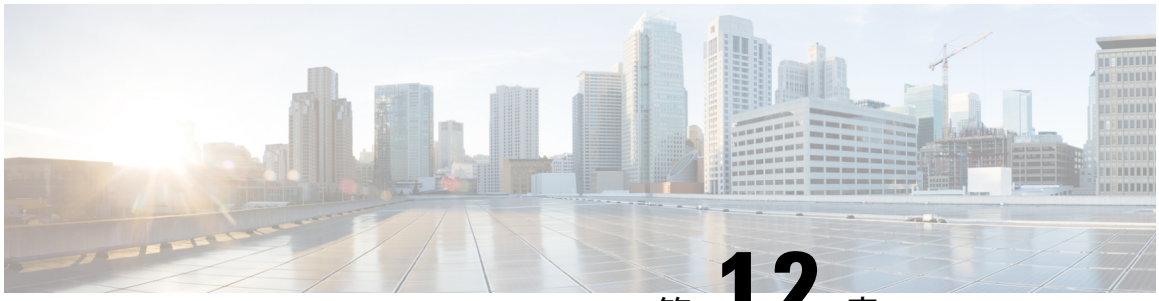
帯域幅最適化のトラブルシューティング

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

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

表 *1:* エラー

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



第 12 章

インテントベースの帯域幅要件の定義と維持

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

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

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

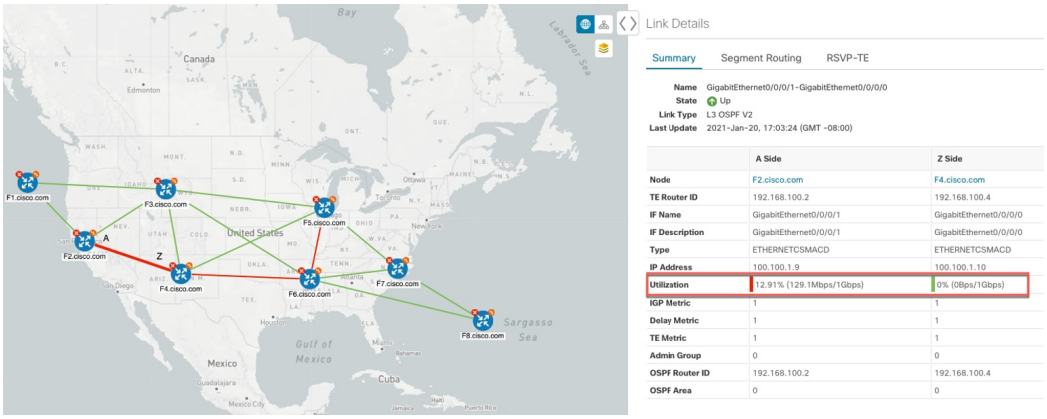
BWoD に関する特記事項

BWoD を使用する場合は、次の情報を考慮してください。

- BWoD を使用するには、Advanced RTM ライセンスパッケージが必要です。
- 要求された帯域幅を保証するポリシーのパスを BWoD が検出できない場合、このオプションが有効になっていると、BWoD は「ベストエフォート」パスの検出を試みます。
- Optimization Engine の再起動またはトポロジサービス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 [厳格なポリシー（Strict Policy）] または [厳格なネットワーク（Strict Network）] 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。

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

図 *35* : 初期 *BWoD* トポロジの例



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

見つけようとします。単一のパスが見つからない場合、BWoD はパスの分割を推奨する場合があります。

ステップ 1 BWoD を有効にして設定します。

a) メインメニューから、**[トラフィック エンジニアリング（Traffic Engineering）]** > **[オンデマンド帯域幅（Bandwidth on Demand）]** > **[設定（Configuration）]** を選択します。

b) [有効化（Enable）] スイッチを [True] に切り替え、**80** を入力して使用率のしきい値のパーセンテージを設定します。他のオプションの説明を表示するには、? の上にマウスを重ねます。

c) [変更を確定（Commit Changes）] をクリックします。

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

a) メインメニューから **[トラフィック エンジニアリング（Traffic Engineering）]** > **[SR-TE]** タブを選択し、[+ 作成（+Create）] をクリックします。

b) 必要な SR-TE ポリシーの詳細を入力します。

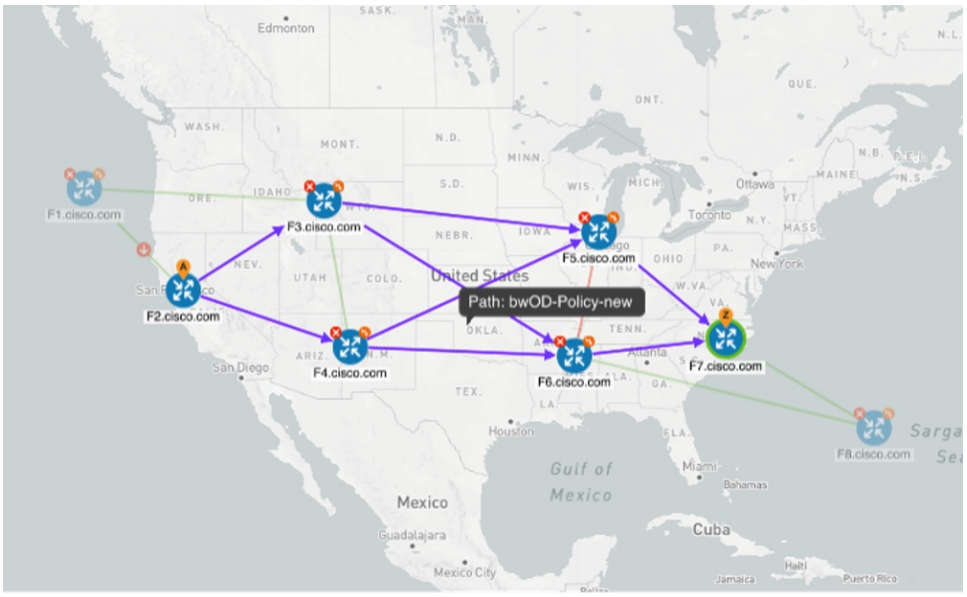
c) [ポリシーパス（Policy Path）] フィールドで、[オンデマンド帯域幅（Bandwidth on Demand）] をクリックし、BWoD パスの一意の名前を入力します。この場合は、**bwOD-Policy-new** と入力します。

d) [最適化の目的（Optimization Objective）] ドロップダウンリストから、[トラフィック エンジニアリング（TE）メトリック（Traffic Engineering (TE) Metric）] を選択します。

e) [帯域幅（Bandwidth）] フィールドに、要求された帯域幅を入力します。この例では、**920** Mbps を要求しています。

f) [プレビュー（Preview）] をクリックします。

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



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

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

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

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

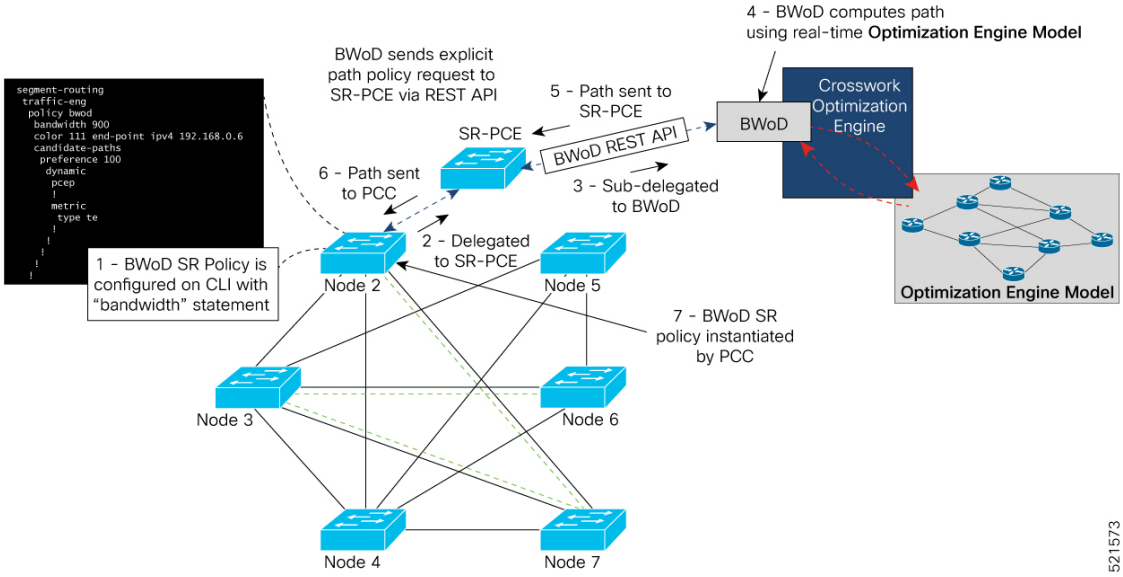
b) 新しい BWoD SR-TE ポリシーを選択し、SR ポリシーの詳細を表示します（[表示（View）] をクリックして選択します）。[ポリシータイプ（Policy Type）] は [オンデマンド帯域幅（Bandwidth on Demand）] であることに注意してください。

PCC によって開始された BWoD SR-TE のポリシー

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

次の図に、BWoD の PCC によって開始されたワークフローを示します。

図 *36 : 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。

オンデマンド帯域幅の設定

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

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

ステップ 1 メインメニューから、**[トラフィック エンジニアリング（Traffic Engineering）]** > **[オンデマンド帯域幅（Bandwidth on Demand）]** > **[設定（Configuration）]** を選択します。

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

ステップ 3 追加のオプションを設定します。各フィールドの説明を表示するには、の上にマウスポインタを合わせます。

ステップ 4 [変更のコミット（Commit Changes）] をクリックして、設定を保存します。

ステップ 5 BWoD SR ポリシーを作成するには、**[Traffic Engineering（トラフィック エンジニアリング）]**>**[トラフィック エンジニアリング（Traffic Engineering）]** に移動します。

ステップ 6 [SRポリシー（SR Policy）] テーブルで、**[作成（Create）]** > **[PCEによって開始（PCE Init）]** をクリックします。

ステップ 7 必要な SR ポリシーの詳細を入力する以外に、[オンデマンド帯域幅（Bandwidth on Demand）] オプションをクリックし、必要な帯域幅を入力します。

ステップ 8 [プレビュー（Preview）] をクリックして、提案された SR ポリシーを表示します。

ステップ 9 [プロビジョニング（Provision）] をクリックして、SR ポリシーをコミットします。

BWoD のトラブルシューティング

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

表 *2:* 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。
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。