Cisco Crosswork Network Controller 7.1 トラフィック エンジニアリングおよび最適化

最終更新：2026 年 1 月 14 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/

© 2025 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章 **Cisco Crosswork ネットワークコントローラでのトラフィック エンジニアリング 1**

サポート対象の SR-TE ポリシーと RSVP トンネル 1

セグメントルーティング（SR） 3

セグメントルーティングパス計算要素（SR-PCE） 5

SR-TE ポリシー PCC および PCE 設定のソース 6

リソース予約プロトコル（RSVP） 6

RSVP-TE トンネル PCC および PCE 設定のソース 8

サンプルポリシーおよびデバイスの設定 8

PCC によって開始された SR-TE ポリシーの例 9

複数のループバック IP アドレスをサポートするポリシーの送信元アドレス設定 9

PCC によって開始された RSVP-TE トンネルの例 10

アフィニティマップの設定 10

トラフィック エンジニアリング ダッシュボード 11

TE イベントと使用率履歴の表示 13

TE デバイスの詳細の表示 15

TE 設定の構成 16

TE タイムアウト設定の構成 16

TE 用のデバイスグループの表示方法の設定 17

TE データ保持設定の構成 17

SR-TE ポリシーと RSVP-TE トンネルの解決 18

第 2 章 **SR-MPLS および SRv6 19**

トポロジマップでの SR-MPLS および SRv6 ポリシーの表示 19

SR-MPLS および SRv6 ポリシーの詳細の表示 22

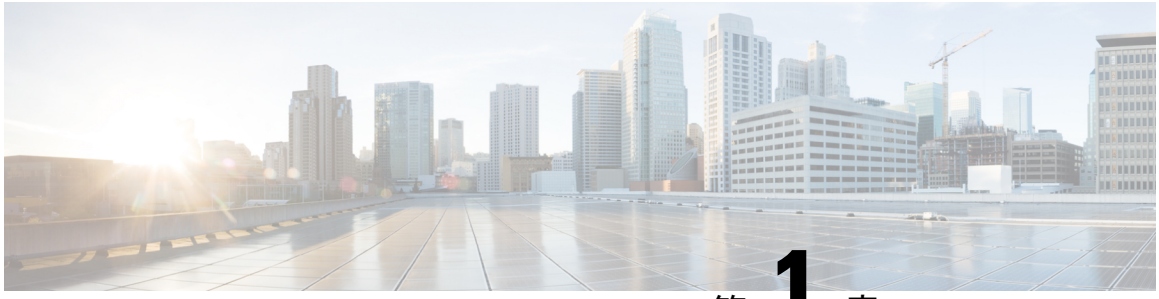
IGP パスとメトリックの可視化 24
複数の候補パス（MCP）の検索 25
定義済みのバインディングセグメント ID（B-SID）ラベルに関連付けられた基盤となるパスの可視化 28
ネイティブ SR パスの可視化 31
デバイスの前提条件 31
ネイティブパスの可視化 33
Crosswork Network Controller での TE リンクアフィニティの設定 34
ポリシー展開の考慮事項 36
明示的 SR-MPLS ポリシーの作成 36
最適化インテントに基づくダイナミック SR-MPLS ポリシーの作成 37
（PCC によって開始された）SR-TE ポリシーの作成 39
SR-MPLS ポリシーの変更 40

第 3 章 リソース予約プロトコル（RSVP） 43
トポロジマップでの RSVP-TE トンネルの表示 43
RSVP-TE トンネルの詳細の表示 46
明示的 RSVP-TE トンネルの作成 49
最適化インテントに基づくダイナミック RSVP-TE トンネルの作成 50
RSVP-TE トンネルの作成（PCC によって開始） 51
RSVP-TE トンネルの変更 52

第 4 章 フレキシブルアルゴリズム 53
サポートされるフレキシブルアルゴリズムのメトリックと制約 53
Crosswork Network Controller でのフレキシブルアルゴリズムのアフィニティの設定 54
フレキシブル アルゴリズム トポロジの可視化 55
フレキシブルアルゴリズムの詳細の表示 57

第 5 章 ツリーセグメント識別子（Tree-SID）マルチキャスト トラフィック エンジニアリング 61
Tree-SID ポリシーの可視化 62
トポロジマップでのポイントツーマルチポイント ツリーの表示 62

静的 Tree-SID ポリシーの作成 66
静的 Tree-SID ポリシーの設定例 68
Tree-SID ポリシーの変更 70
Tree-SID の重要な考慮事項 70



第 1 章

Cisco Crosswork ネットワークコントローラでのトラフィック エンジニアリング

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

Crosswork Network Controller を使用する最大の利点の 1 つは、トポロジマップで SR-TE ポリシーと RSVP-TE トンネルを可視化できることです。これにより、これらのポリシーのプロビジョニングと管理が簡素化されます。

具体的な内容は、次のとおりです。

- サポート対象の SR-TE ポリシーと RSVPトンネル （1 ページ）
- セグメントルーティング（SR） （3 ページ）
- セグメントルーティングパス計算要素（SR-PCE） （5 ページ）
- SR-TE ポリシー PCC および PCE 設定のソース （6 ページ）
- リソース予約プロトコル（RSVP） （6 ページ）
- RSVP-TE トンネル PCC および PCE 設定のソース （8 ページ）
- サンプルポリシーおよびデバイスの設定 （8 ページ）
- トラフィック エンジニアリング ダッシュボード （11 ページ）
- TE イベントと使用率履歴の表示 （13 ページ）
- TE デバイスの詳細の表示 （15 ページ）
- TE 設定の構成 （16 ページ）
- SR-TE ポリシーと RSVP-TE トンネルの解決 （18 ページ）

サポート対象の SR-TE ポリシーと RSVP トンネル

Crosswork Network Controller トラフィック エンジニアリングは、さまざまな SR-TE ポリシーと RSVP トンネルの可視化とプロビジョニングをサポートしています。UI で YANG モデルベースのフォームを公開し、外部システムと統合するための API を提供することで、サービスのプ

ロビジョニングを簡素化する一方で、Cisco NSO は基盤となるプロビジョニングエンジンとして機能します。

さらに、Crosswork Network Controller は、テレメトリと SR-PCE との対話を使用して、作成しなかった既存のサービス（ブラウンフィールドサービスの実装など）を検出して可視化できます。これらのサービスは、Crosswork Network Controller で管理対象外としてマークされます。これらのサービスを変更するために、管理者はデバイス CLI、NSO のサービスモデルまたは API、Crosswork Network Controller UI ツールセット、および場合によっては、既存のサービスを管理対象外から管理対象に移行するスクリプトを使用できます。

オペレータは、 Cisco CX Professional Services とコラボレーションしたり、 Cisco DevNet のリソースや項目を活用したりして、Crosswork Network Controller の機能をカスタマイズまたは拡張できます。これには、特定のユースケースに合わせて調整されたカスタム機能パックの開発を含めることができます。

表 *1*：サポート対象の *TE* テクノロジー

TE テクノロジー	Crosswork ネットワークコントローラ	
	視覚化	プロビジョニング（PCE によって開始）
SR-MPLS	✓	✓
SRv6	✓	✓
RSVP	✓	✓
フレキシブルアルゴリズム	✓	✗
Tree-SID	✓	✓ [1]
回線型	✓	✓

[1] 静的 Tree-SID ポリシーのみサポートされています。ダイナミック Tree-SID ポリシーは、デバイス上で手動でプロビジョニングするか、API を介してのみプロビジョニングできますが、Crosswork Network Controller UI で可視化できます。

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

セグメントルーティング（SR）

トラフィック エンジニアリング用のセグメント ルーティングは、送信元と宛先のペア間のトンネルを通じて行われます。トラフィック エンジニアリング用のセグメント ルーティングでは、送信元ルーティングの概念が使用されます。送信元はパスを計算し、パケットヘッダーでセグメントとしてエンコードします。セグメントは、任意のタイプの命令の識別子です。例えば、トポロジ セグメントは、宛先へのネクスト ホップを識別します。各セグメントを識別するセグメントID（SID）は、32ビットの符号なし整数で構成されます。各セグメントは、送信元から接続先までのエンドツーエンドのパスであり、プロバイダー コア ネットワークのルータに、IGPによって計算された指定されたパスに従うように指示します。宛先はトンネルの存在を認識しません。

セグメント

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

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

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

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

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

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

SR ポリシー

トラフィックエンジニアリングを実現するためのセグメントルーティングでは、ネットワークを介してトラフィックを誘導する「ポリシー」を使用します。SR ポリシーパスは、セグメント ID（SID）リストと呼ばれるパスを指定するセグメントのリストとして表されます。各セグメントは、送信元から接続先までのエンドツーエンドのパスであり、ネットワークルータに、IGP によって計算された最短パスではなく指定されたパスに従うように指示します。パケットが SR ポリシーへと誘導される場合、ヘッドエンドは SID リストをパケットにプッシュします。残りのネットワークは、SID リストに埋め込まれた命令を実行します。

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

- SR-MPLS および SRv6 （19 ページ）
- フレキシブルアルゴリズム （53 ページ）
- ツリーセグメント識別子（Tree-SID）マルチキャスト トラフィック エンジニアリング （61 ページ）
- SR 回線型

SR ポリシーにはダイナミックと明示的の 2 つのタイプがあります。

ダイナミック SR ポリシー

動的パスは、最適化の目的と一連の制約に基づいています。ヘッドエンドはソリューションを計算し、結果として SID リストまたは SID リストのセットを生成します。トポロジが変更されると、新しいパスが計算されます。ヘッドエンドにトポロジーに関する十分な情報がない場合、ヘッドエンドは計算をパス計算エンジン（PCE）に委任できます。

明示的 SR ポリシー

明示的なポリシーを設定する場合は、プレフィックスまたは隣接 SID のリストで構成される明示的なパスを指定します。各 SID はパス上のノードまたはリンクを表します。

分離

Crosswork Network Controller はディスジョイントポリシーを使用して、2 つの送信元ノードから 2 つの接続先ノードへのトラフィックをディスジョイントパスに沿って誘導する 2 つのセットのセグメントリストを計算します。これらのディスジョイントパスの起点は、同じヘッドエンドまたは異なるヘッドエンドです。

ディスジョイントレベルは、2 つの計算されたパスで共有すべきではないリソースのタイプを指定します。次の分離パスの計算がサポートされています。

- **リンク**：パスは同じインターフェイスまたは物理リンクを共有しません。
- **ノード**：パスは同じノードを共有せず、ルーティングデバイスの完全な独立性を確保します。
- **SRLG**：パスは共通リスクを共有するリンクを表す共有リスクリンクグループ（SRLG）を回避します。

- **SRLG ノード**：パスは共有 SRLG と共有ノードの両方を回避し、最高レベルの障害の切り分けを提供します。

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

（注）
- 分離は、同じ分離 ID を持つ 2 つのポリシーでサポートされています。
- アフィニティと分離を同時に設定することはできません。

セグメントルーティングパス計算要素（SR-PCE）

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

Cisco SR-PCE は、物理デバイスまたは仮想マシン内で実行されている仮想ルータのいずれかで実行されている Cisco IOS XR オペレーティングシステムによって提供されます。SR-PCE は、ネットワークを最適化するために TE トンネルを制御および再ルーティングするのに役立つステートフル PCE 機能を提供します。PCE では、パス計算クライアント（PCC）が PCC を起点とする PCE ピアへのヘッドエンドトンネルを報告し、制御を委任する一連の手順を記述します。PCC および PCE は、更新をネットワークにプッシュするために SR-PCE が使用するパス計算要素通信プロトコル（PCEP）の接続を確立します。

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

（注）互換性の問題を回避するには、SR-PCE バージョンのサポートと互換性について、『Cisco Crosswork Network Controller リリースノート』を参照してください。

SR-PCE および HA の設定については、『Cisco Crosswork Network Controller 7.1 アドミニストレーション ガイド』の「**Cisco SR-PCE プロバイダー**」を参照してください。

SR-TE ポリシー PCC および PCE 設定のソース

UI または API を使用して設定された SR-TE ポリシーは、Crosswork Network Controller で変更または削除できる唯一のポリシータイプです。ただし、Crosswork Network Controller によって検出および報告された SR-TE ポリシーは、次のソースから設定されている可能性があります。

- パス計算クライアント（PCC）によって開始：PCC で直接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 （9 ページ）を参照）。これらのポリシーは、Crosswork Network Controller によってプロビジョニングまたは管理されないため、UI に [不明（Unknown）] と表示されます。ただし、オンデマンド帯域幅（BWoD）ポリシーと回線型（CS）ポリシーは例外です。PCC によって開始された場合でも、Crosswork Network Controller はその属性と目的に基づいてそれらを認識して分類するため、これらは [不明（Unknown）] としてラベル付けされません。

（注） 回線型ポリシーは常に PCC によって開始されます。

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

リソース予約プロトコル（RSVP）

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

RSVP-TE プロセスには、次の機能が含まれています。

- エンドポイント制御。ヘッドエンドとテールエンドでの TE トンネルの確立と管理に関連付けられます。

- リンク管理。TE ラベルスイッチパス（LSP）のリソース認識型ルーティングを実行し、MPLS ラベルをプログラムするためにリンクリソースを管理します。
- 高速再ルーティング（FRR）。保護が必要な LSP を管理し、これらの LSP にバックアップトンネル情報を割り当てます。

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

RSVP-TE 明示的ルーティング（ストリクト、ルーズ）

RSVP-TE の明示的ルートは、明示的ルートオブジェクト（ERO）で抽象ノードとして指定可能なネットワークトポロジ内の特別なパスです。これらのノードは、一連の IP プレフィックスまたは一連の自律システムである可能性があります。明示的パスは管理上指定することも、制約付き最短パス優先（CSPF）などのアルゴリズムを使用して自動的に計算することもできます。

ERO で指定された明示的パスは、ストリクトパスまたはルーズパスです。

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

ルーズ ERO（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 を使用した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（高速再ルート）

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（高速再ルート）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。

RESV（予約）メッセージのレコードルートオブジェクト（RRO）は、LSP でのローカル保護（FRR など）の可用性または使用をレポートします。また、その LSP で帯域幅保護とノード保護を使用できるかどうかも示します。

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。パスに沿って、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いて FRR 要件を評価します。適切なバックアップトンネルが使用可能な場合、PLR はそれを選択し、バックアップトンネル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（例：リンクまたはノード障害）、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。このメカニズムにより、フェールオーバープロセス中に元の LSP が MP によって切断されなくなります。

さらに、PLR は PATH-ERROR メッセージを使用して TE トンネルヘッドエンドにシグナリングし、元の LSP に沿った障害と、影響を受けた LSP で FRR がアクティブに使用されていることを示します。この情報を使用して、ヘッドエンドは TE トンネルの新しい LSP を確立します。新しい LSP が（make-before-break 手法を使用して）設定されると、ヘッドエンドは失敗したパスを切断します。

RSVP-TE トンネル PCC および PCE 設定のソース

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

- パス計算クライアント（PCC）によって開始：PCC で直接設定された RSVP-TE トンネル（PCC によって開始された RSVP-TE トンネルの例 （10 ページ）を参照）。
- パス計算要素（PCE）または PCC によって動的に開始：RSVP-TE トンネルは、PCE によって動的に計算および確立されるか、PCC によって要求されます。

PCC で設定された RSVP-TE トンネルや、PCE や PCC によって動的に開始された RSVP-TE トンネルは、Crosswork Network Controller で可視化できます。

サンプルポリシーおよびデバイスの設定

このセクションでは、トラフィックエンジニアリングおよび最適化機能に関連するポリシーとデバイス設定の例を示します。

トラフィックエンジニアリングとテレメトリ機能が Crosswork Network Controller 内で正常に動作するようにするには、デバイスを適切に設定する必要があります。他の Crosswork Network Controller 機能と連携するようにデバイスを設定する方法の詳細については、『Cisco Crosswork Infrastructure とアプリケーションアドミニストレーションガイド』の「デバイスの導入準備」の章を参照してください。

Crosswork Network Controller は、作成しなかった既存のサービス（ブラウンフィールドサービスの実装など）を検出して可視化できます。テーブルからポリシーを選択すると、これらのサービス設定の詳細がトポロジ画面に表示されます。ただし、これらのポリシーは、Crosswork Network Controller で管理対象外としてマークされます。これらのサービスを変更するために、管理者はデバイス CLI、NSO のサービスモデルまたは API、Crosswork Network Controller UI ツールセット、および場合によっては、既存のサービスを管理対象外から管理対象に移行するスクリプトを使用できます。

PCC によって開始された SR-TE ポリシーの例

この例は、ヘッドエンドルータでの SR-TE ポリシーの設定を示します。このポリシーでは、特定のアフィニティ制約に基づいてヘッドエンドルータによって計算されるダイナミックパスを使用します。この例では、**SampleSRTE** という名前のポリシーが、次の属性で作成されます。色の値は 100、候補の優先度は 100、メトリックタイプは **TE**、そして色は **red** が割り当てられたリンクを除外するアフィニティ制約です。

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

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

複数のループバック IP アドレスをサポートするポリシーの送信元アドレス設定

複数のループバック IP アドレスをサポートするには、これらのポリシー設定を、ポリシーのヘッドエンドまたは発信元として機能する PCC デバイスに含める必要があります。

すべてのポリシーのグローバル設定

```
Router# segment-routing traffic-eng candidate-paths all source-address ipv4 ip-address
```

特定のポリシーの設定

```
Router# segment-routing traffic-eng policy policy-name source-address ipv4 ip-address
```

PCC によって開始された RSVP-TE トンネルの例

次に、PCC によって開始された RSVP-TE トンネルのデバイス設定の例を示します。特定のデバイスの説明およびサポートされている RSVP-TE トンネル コンフィギュレーション コマンドを表示するには、該当するマニュアルを参照してください（たとえば、「*MPLS Command Reference for Cisco NCS 5500 Series, Cisco NCS 540 Series, and Cisco NCS 560 Series Routers*」）。

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

アフィニティマップの設定

アフィニティマップを使用すると、ネットワークオペレータは、人間が読める名前（「赤」、「低遅延」、「高帯域幅」など）をリンク属性を表す特定のビット位置に関連付けることができます。アフィニティマッピングが Crosswork Network Controller 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、Tree-SID、RSVP-TE トンネル、または Crosswork Network Controller でサポートされているその他のポリシーの一部として可視化を目的としてアフィニティ属性を設定するには、デバイスで設定されたアフィニティマップも Crosswork Network Controller で再作成する必要があります。デバイスで構成されているアフィニティマッピングの収集から始めて、一致する名前とビット位置を使用して Crosswork Network Controller UI で同じマッピングを定義します。

デバイスでの SR-TE アフィニティマップの設定

これは、デバイスでのSR-TEアフィニティマッピングの設定例です。詳細については、Crosswork Network Controller での TE リンクアフィニティの設定 （34 ページ） を参照してください。

```
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
  !
 !
!
```

デバイスでのフレキシブルアルゴリズムのアフィニティマップ設定

これは、デバイスでのフレキシブルアルゴリズムのアフィニティマッピングの設定例です。詳細については、「Crosswork Network Controller でのフレキシブルアルゴリズムのアフィニティの設定 （54 ページ）」を参照してください。

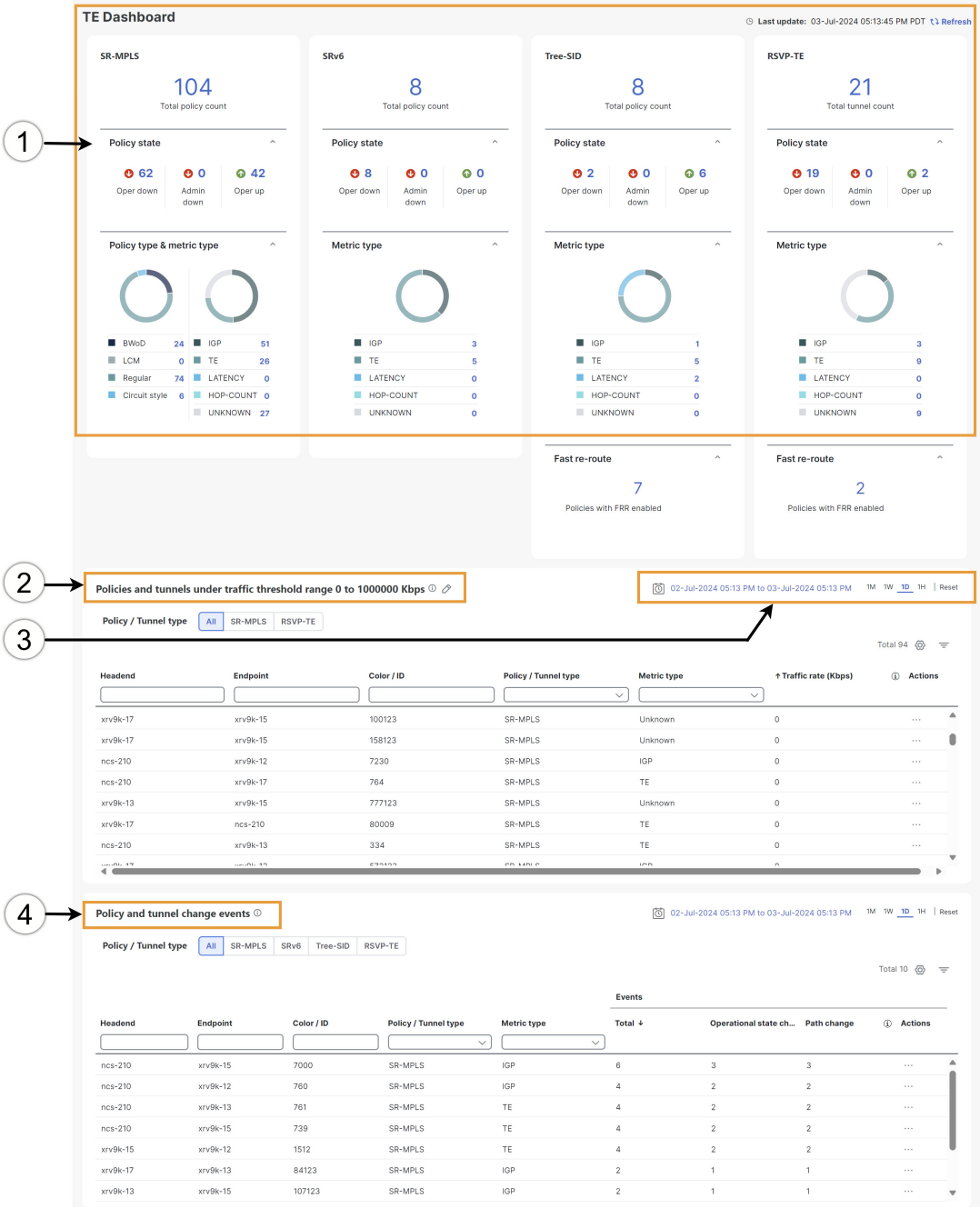
```
router isis CORE
 is-type level-2-only
 net 49.0001.0000.0000.0002.00
 log adjacency changes
 affinity-map b33 bit-position 33
 affinity-map red bit-position 1
 affinity-map blue bit-position 5
 flex-algo 128
  priority 228
  advertise-definition
  affinity exclude-any blue indigo violet black
 !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

トラフィック エンジニアリング ダッシュボード

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

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

図 *1:* トラフィック エンジニアリング ダッシュボード



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

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

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イベントの変更をキャプチャします。SRv6 または 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。トラフィックエンジニアリングイベントと使用率の履歴を表示するには、次の手順に従います。

始める前に

LSP 使用率の収集を有効にして、データを保持する期間を設定してください。
<c_configure-te-services.xml> を参照してください。

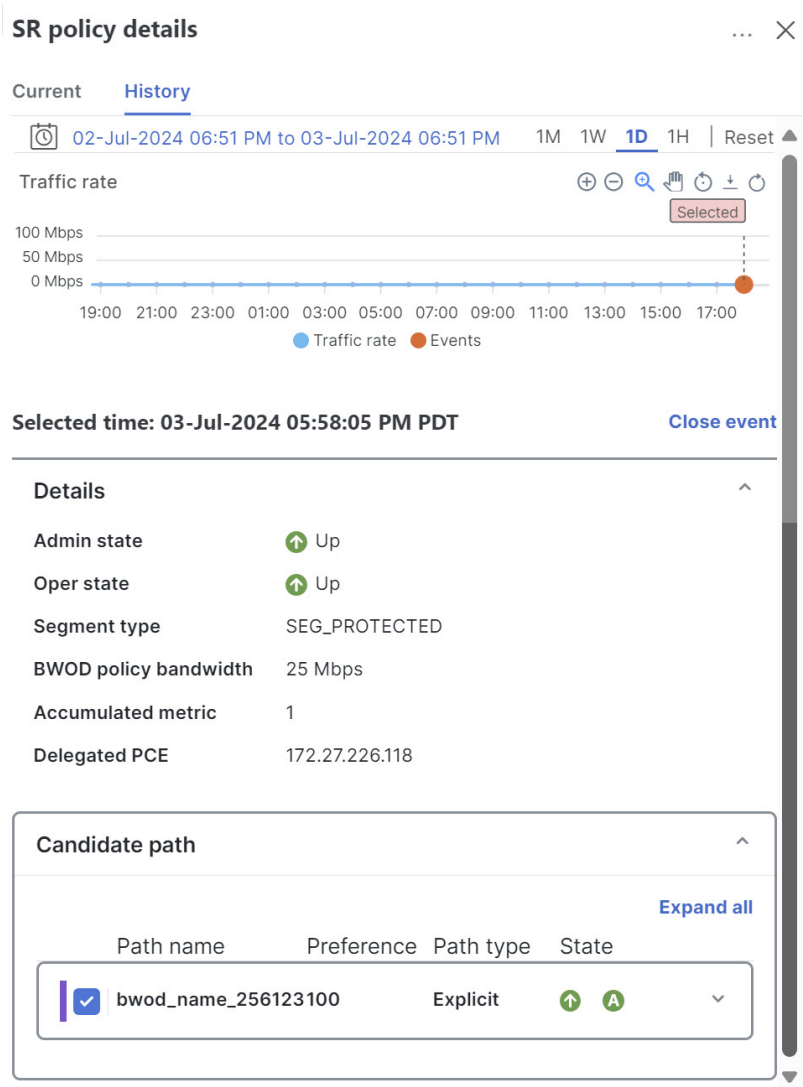
手順

ステップ 1 **[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）]** を選択します。

ステップ 2 **[アクション（Actions）]** 列から、ポリシーまたはトンネルの ··· > **[履歴の表示（View Details）] > [履歴（History）]** を選択します。[履歴（History）] ページには、そのデバイスの関連する履歴データが表示されます。

ステップ 3 イベントをクリックすると、パスまたは状態変更イベントの情報が表示されます。

図 *2 : TE* イベントと使用率履歴



追加遅延データ

Crosswork Service Health がインストールされている場合、遅延（平均）と遅延差異の情報を使用できます。詳細については、『Cisco Crosswork Network Controller Service Health Monitoring Guide』の「*Enable SR PM Monitoring for Links and TE Policies*」を参照してください。

拡張 TE リンク遅延メトリック（最小遅延値）は、最適化メトリックまたは累積遅延境界として SR ポリシーのパスの計算に使用できます。

これは、SR ポリシーを介して送信されるトラフィックで発生するエンドツーエンドの遅延をモニターし、遅延が要求された「上限」を超えず、SLA に違反していないことを確認するために使用できます。転送テーブル内の候補パスまたは SR ポリシーのセグメントリストをアクティブ化する前に、エンドツーエンドの遅延値を確認したり、転送テーブル内のアクティブな候補パスまたは SR ポリシーのセグメントリストを非アクティブ化したりできます。

図 *3*：モニタリングが有効な場合の *VPN* サービスの例

TE 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、次の手順に従います。

手順

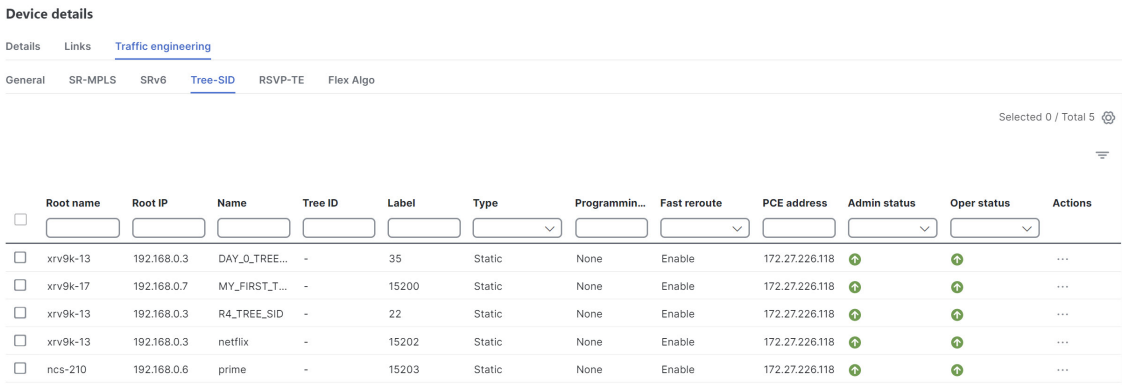
ステップ 1 **[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > > **[トラフィックエンジニアリング（Traffic Engineering）]** を選択します。

ステップ 2 トポロジマップで、デバイスを選択します。

ステップ 3 **[デバイスの詳細（Device details）]** で、**[トラフィックエンジニアリング（Traffic engineering）]** > ***[ポリシートンネルタイプ（policy-tunnel-type）]*** を選択します。各タブには、そのデバイスに関連付けられたポリシーまたはトンネルデータが表示されます。

この例では、選択したデバイスの Tree-SID 情報の詳細を示します。

図 *4:* トラフィック エンジニアリング デバイスの詳細



（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。

ステップ 4 （オプション）この情報を共有するには、URL をコピーしてリンクを他のユーザーに送信します。

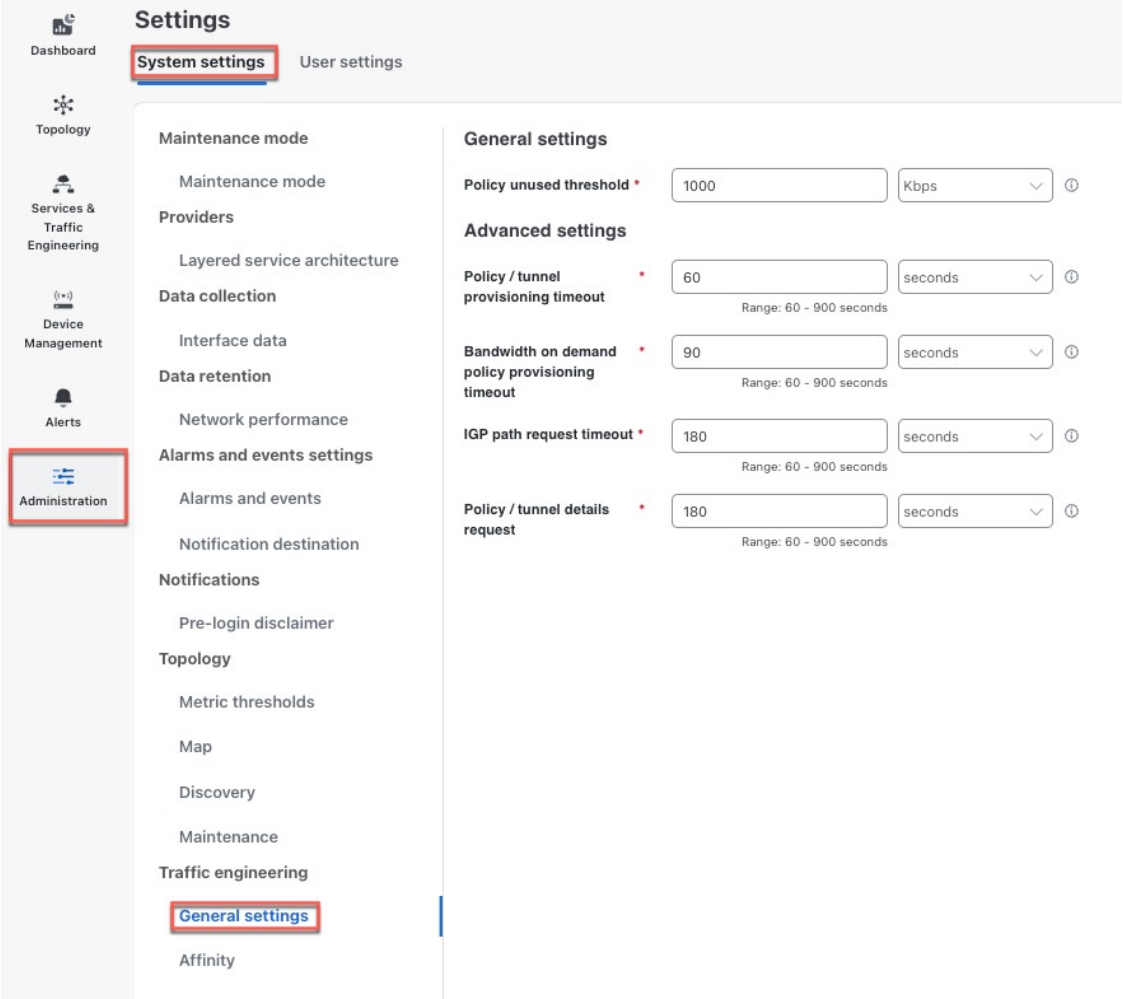
TE 設定の構成

TE タイムアウト設定の構成

SR-TE ポリシー、RSVP-TE トンネル、オンデマンド帯域幅、および IGP パスのデータのプロビジョニングと取得のタイムアウト設定を行うには、[管理（Administration）]>[設定（Settings）]>[システム設定（System settings）] タブ>[トラフィックエンジニアリング（Traffic engineering）]>[全般設定（General settings）] を選択します。タイムアウト期間のオプションを入力します。詳細については、ⓘをクリックしてください。

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

図 *5:* トラフィック エンジニアリング タイムアウトの設定



TE 用のデバイスグループの表示方法の設定

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

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

TE データ保持設定の構成

LSP 使用率の履歴ビュー（[履歴（Historical）] タブ）を表示するには、LSP 使用率の収集を有効にし、データを保持する期間を指定する必要があります。これを行うには、**[管理（Administration）] > [システム設定（System settings）] > [データ保持（Data retention）] >**

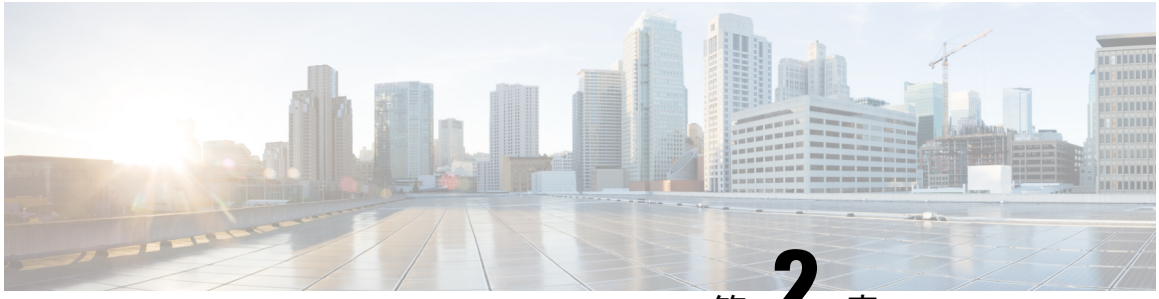
[ネットワークパフォーマンス（Network performance）] を選択し、**[LSP使用率（LSP utilization）]** チェックボックスをオンにします。必要に応じて、デフォルトのデータ保持期間を編集できます。

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

SR-TE ポリシーと RSVP-TE トンネルの解決

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

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



第 2 章

SR-MPLS および SRv6

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

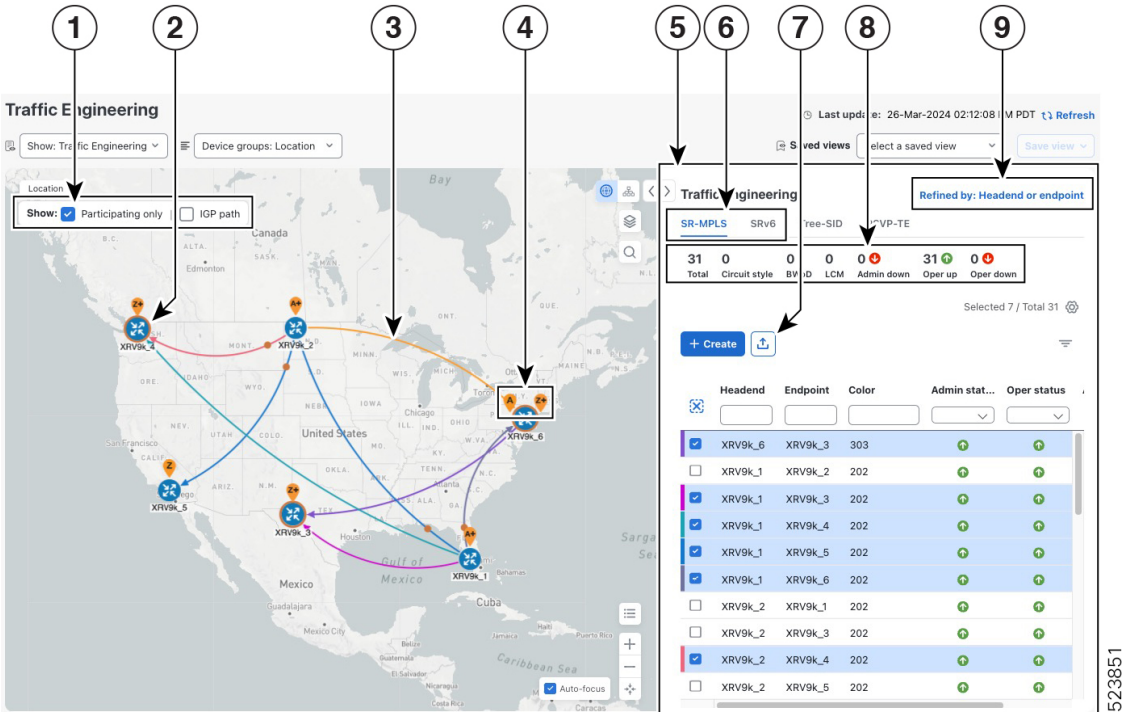
- トポロジマップでの SR-MPLS および SRv6 ポリシーの表示 （19 ページ）
- SR-MPLS および SRv6 ポリシーの詳細の表示 （22 ページ）
- IGP パスとメトリックの可視化 （24 ページ）
- 複数の候補パス（MCP）の検索 （25 ページ）
- 定義済みのバインディングセグメント ID（B-SID）ラベルに関連付けられた基盤となるパスの可視化 （28 ページ）
- ネイティブ SR パスの可視化 （31 ページ）
- Crosswork Network Controller での TE リンクアフィニティの設定 （34 ページ）
- ポリシー展開の考慮事項 （36 ページ）
- 明示的 SR-MPLS ポリシーの作成 （36 ページ）
- 最適化インテントに基づくダイナミック SR-MPLS ポリシーの作成 （37 ページ）
- （PCC によって開始された）SR-TE ポリシーの作成 （39 ページ）
- SR-MPLS ポリシーの変更 （40 ページ）

トポロジマップでの SR-MPLS および SRv6 ポリシーの表示

トラフィック エンジニアリングのトポロジマップを取得するには、**[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）]**を選択します。

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

図 *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	該当するチェックボックスをクリックして、次のオプションを有効にします。 • [表示：IGPパス（Show: IGP path）]：選択した SR-TE ポリシーの IGP パスを表示します。 • [表示：参加デバイスのみ（Show: Participating only）]：選択した SR-TE ポリシーに属するリンクのみを表示します。他のすべてのリンクとデバイスは表示されなくなります。
2	オレンジ色のアウトラインが付いたデバイス（）は、そのデバイスまたはクラスタ内のデバイスにノード SID が関連付けられていることを示します。
3	SR-TE ポリシーは [SR-MPLS] または [SRv6] テーブルで選択されると、送信元と宛先を示す色付きの矢印線としてマップに表示されます。 隣接関係セグメント ID（SID）は、パスに沿ったリンクにオレンジ色の円（）として表示されます。

引き出し線番号	説明
4	**[SR-MPLSおよびSRv6ポリシーの送信元と接続先（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、他のノードが接続先です。A+ は、1 つのノードから発信される複数の SR-TE ポリシーがあることを示します。Z+ は、ノードが複数の SR ポリシーの宛先であることを示します。
5	このウィンドウの内容は、選択またはフィルタ処理された内容によって異なります。この例では、[SR-MPLS] タブが選択され、[SRポリシー（SR Policy）] テーブルが表示されます。
6	[SR-MPLS] タブまたは [SRv6] タブをクリックして、SR-TE ポリシーの各リストを表示します。
7	CSV ファイルにすべてのデータをエクスポートします。選択またはフィルタ処理されたデータをエクスポートすることはできません。
8	**[ミニダッシュボード（Mini Dashboard）]** には、動作中の SR-MPLS または SRv6 ポリシーステータスの概要が表示されます。フィルタが適用されると、**[ミニダッシュボード（Mini Dashboard）]** が更新され、[SR ポリシー（SR Policy）] および [SRv6 ポリシー（SRv6 Policy）] テーブルに表示される内容が反映されます。**[SR-MPLS ミニダッシュボード（SR-MPLS Mini Dashboard）]** テーブルには、ポリシーステータスに加えて、現在 [SR ポリシー（SR Policy）] テーブルにリストされている PCC および PCE によって開始されたトンネルの数が表示されます。
9	このオプションでは、グループフィルタ（使用している場合）をテーブルデータに適用する方法を選択できます。たとえば、[ヘッドエンドのみ（Headend only）] を選択した場合、ポリシーのヘッドエンドデバイスが選択されたグループにあるポリシーのみが表示されます。このフィルタを使用すると、特定の設定を確認でき、大規模なネットワークがある場合に役立ちます。 フィルタオプション： • **[ヘッドエンドまたはエンドポイント（Headend or Endpoint）]**：選択したグループ内のヘッドエンドまたはエンドポイントデバイスを含むポリシーを表示します。 • **[ヘッドエンドおよびエンドポイント（Headend and Endpoint）]**：ヘッドエンドとエンドポイントの両方がグループ内にある場合にポリシーを表示します。 • [Headend only]：ポリシーのヘッドエンドデバイスが選択したグループにある場合にポリシーを表示します。 • [エンドポイントのみ（Endpoint only）]：ポリシーのエンドポイントデバイスが選択したグループ内にある場合にポリシーを表示します。

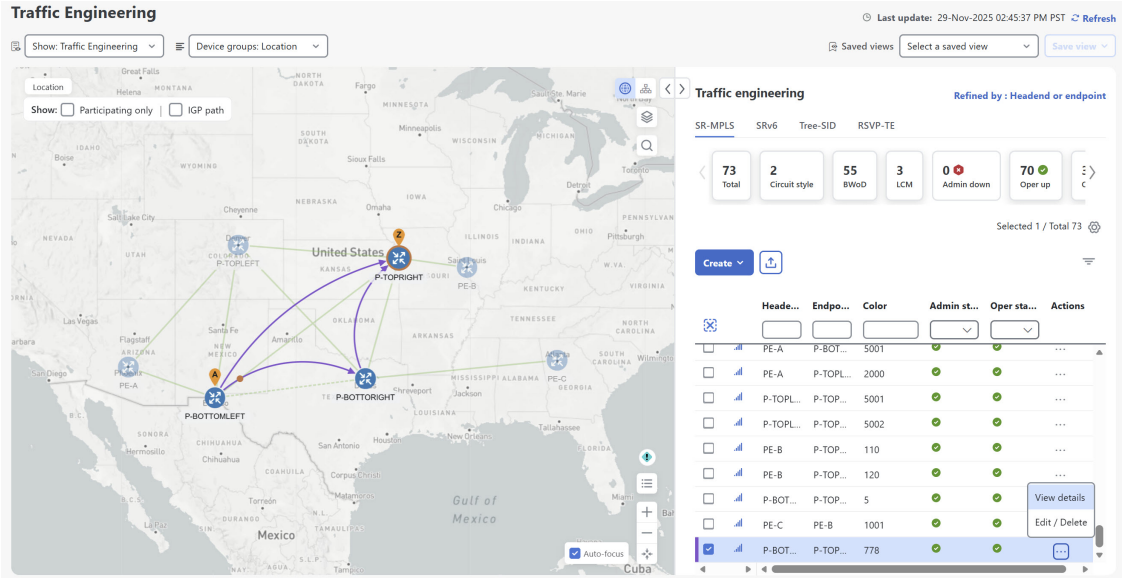
SR-MPLS および SRv6 ポリシーの詳細の表示

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

手順

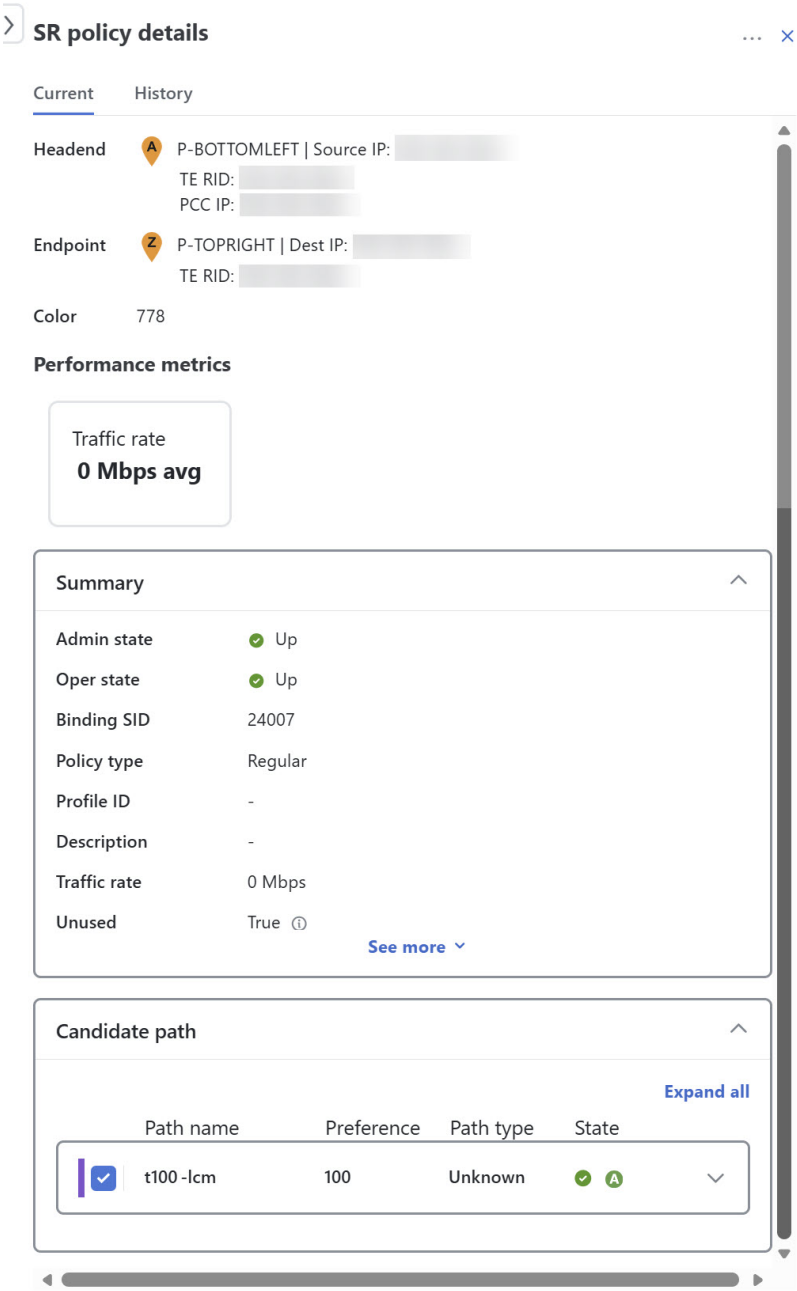
ステップ 1 **[アクション（Actions）]** 列で、いずれかの SR-MPLS または SRv6 ポリシーに対して ··· > **[詳細の表示（View details）]** をクリックします。

図 *7: SR* ポリシーの詳細の表示



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

図 *8 : SR* ポリシーの詳細：ヘッドエンド、エンドポイント、およびサマリー



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

IGP パスとメトリックの可視化

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

手順

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

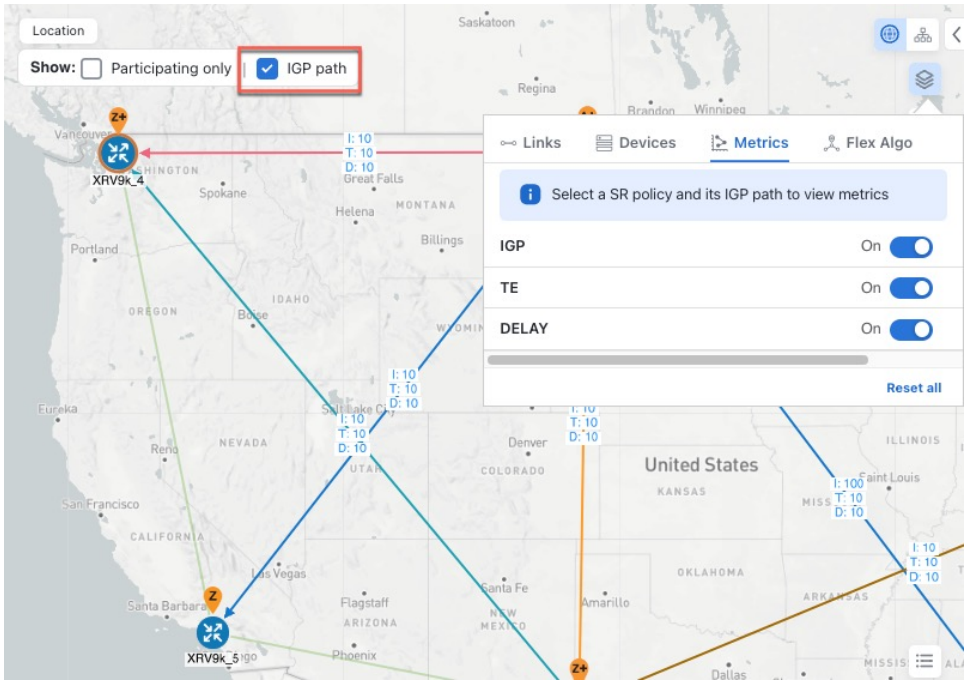
ステップ 2 [Show IGP Path] チェックボックスをオンにします。選択した SR-MPLS ポリシーの IGP パスが、セグメントホップの代わりに直線として表示されます。デュアルスタックトポロジでは、参加リンクのメトリックを表示するには、[参加のみ（Participating only）] チェックボックスもオンにする必要があります。

ステップ 3 > [メトリック（Metrics）] タブをクリックします。

ステップ 4 該当するメトリックを [オン（ON）] に切り替えます。

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

図 *9*: 物理パスとメトリックの表示



複数の候補パス（MCP）の検索

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

特記事項

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

始める前に

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

手順

ステップ 1 メインメニューから、**[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）] > [SR-MPLS]**または [SRv6] タブの順に選択します。

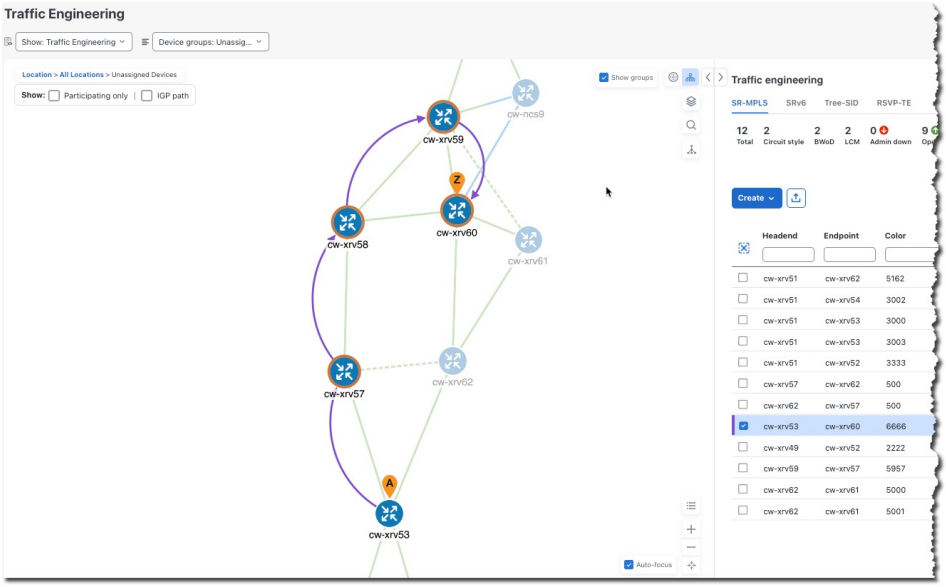
ステップ 2 MCP が設定されているアクティブな SR-TE ポリシーに移動し、トポロジマップで表示します。

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

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

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

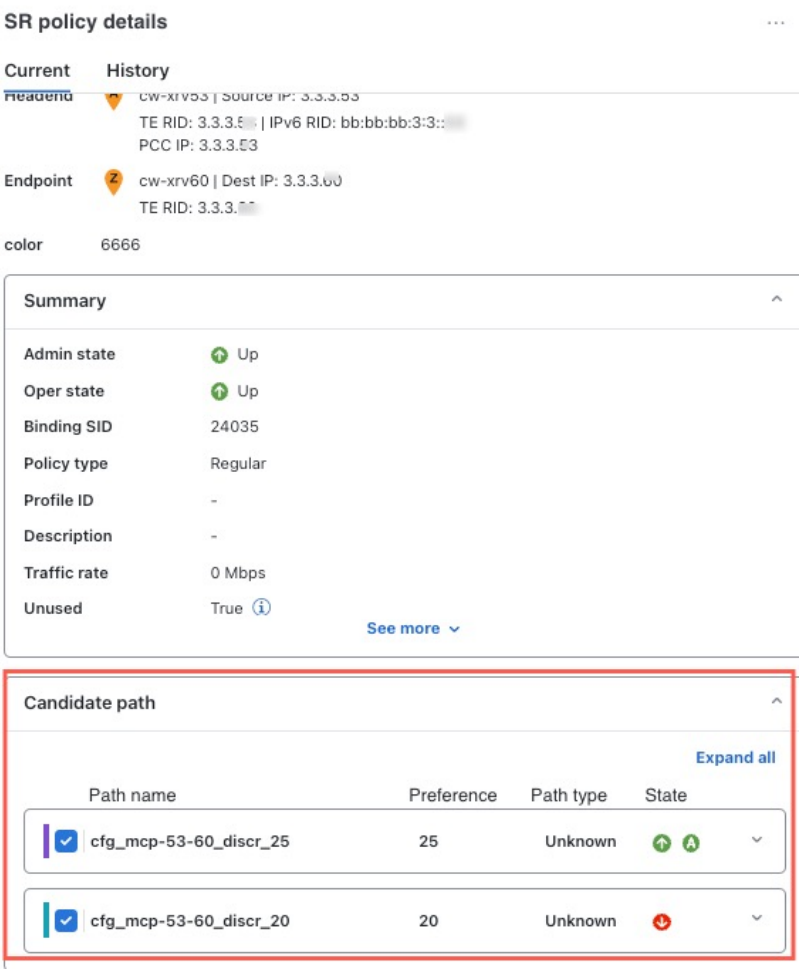
図 *10*：トポロジマップの *SR-TE* ポリシー



ステップ 3 候補パスのリストを表示します。

a) [SR-MPLS] または [SRv6ポリシー（SRv6 Policy）] テーブルの [アクション（Actions）] 列で、･･･ > **[詳細の表示（View details）]** をクリックします。[SRポリシーの詳細（SR policy details）] ウィンドウに、候補パスのリストがポリシーの詳細とともに表示されます。[状態（State）] 列の緑の A は、アクティブパスを示します。

図 *11 : SR* ポリシーの詳細の候補パス



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

ステップ 5 トポロジマップで候補パスを可視化します。

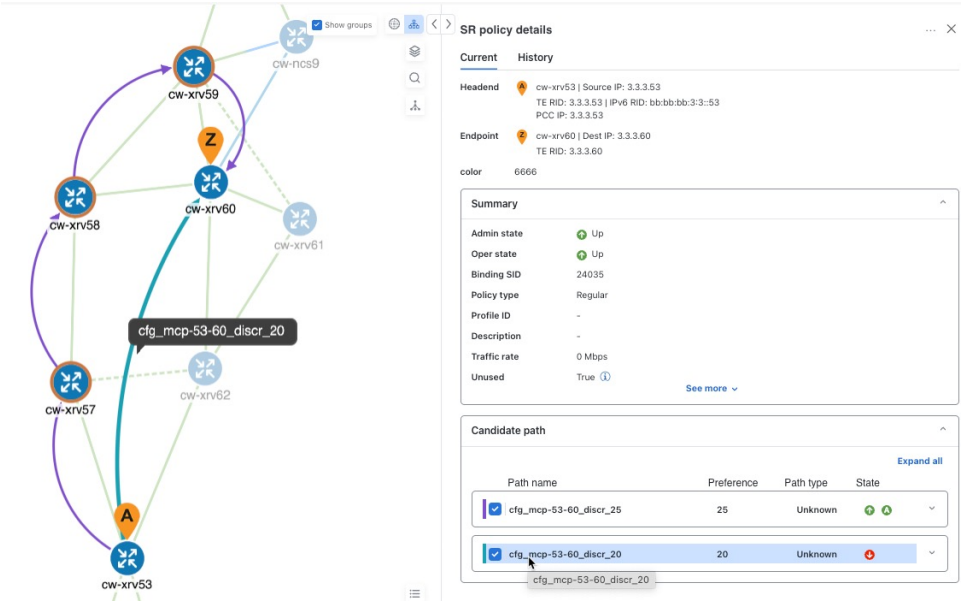
a) 候補パスの横にあるチェックボックスをオンにします。

（注）
明示的な候補パスを選択または表示することはできません。

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

この例では、代替パスが [cw-xrv53] から [cw-xrv60] に直接移動していることがわかります。

図 *12*：トポロジマップ上の候補パス



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

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

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

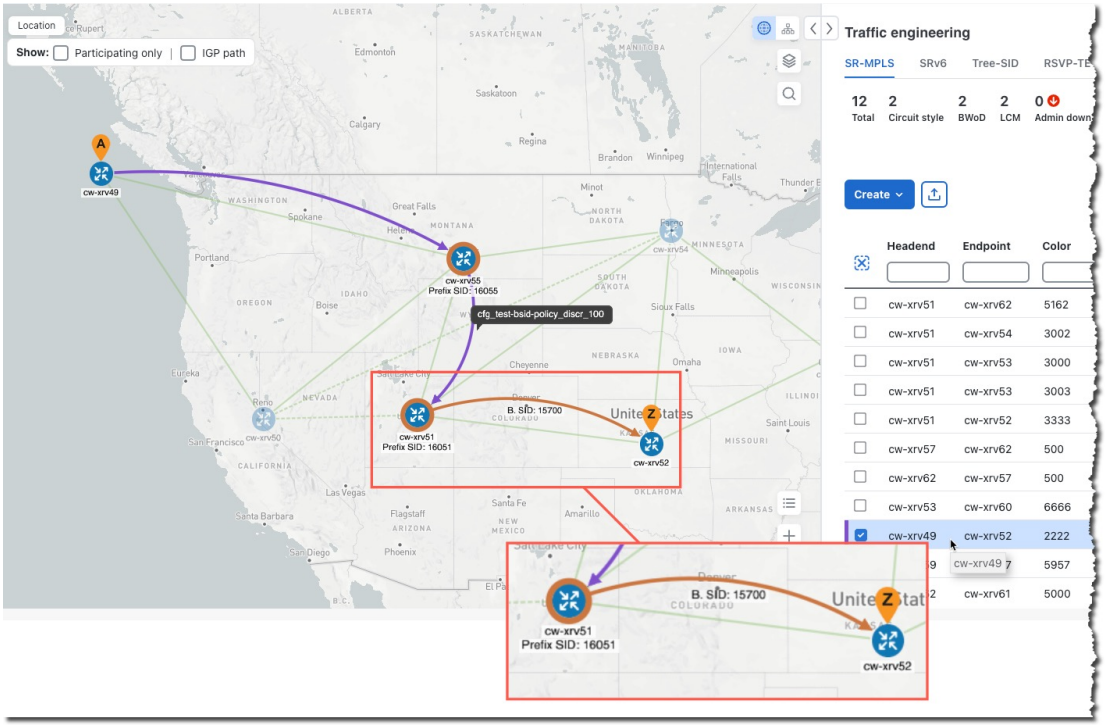
手順

ステップ 1 **[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）]** を選択します。

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

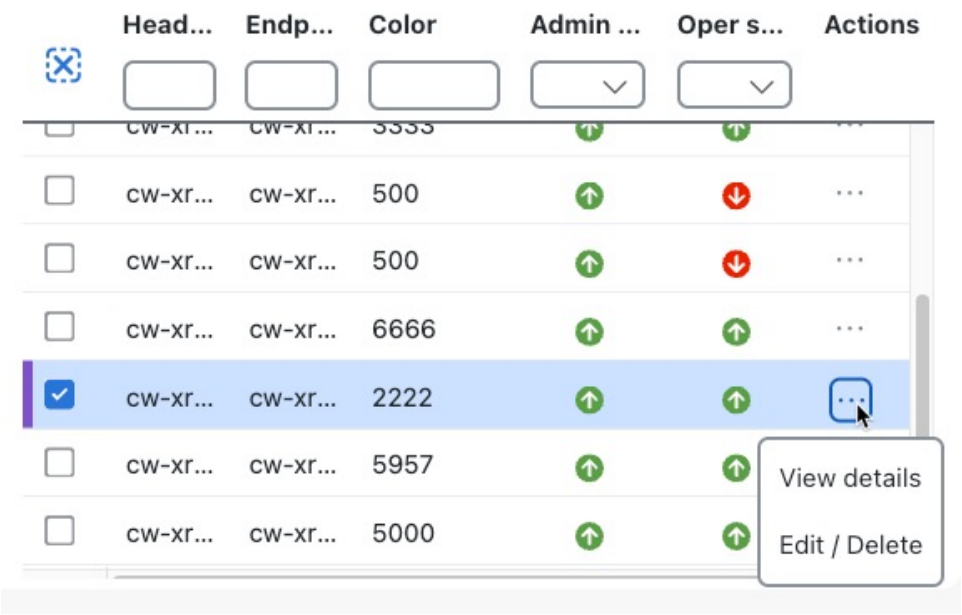
この例では、B-SID パスが [cw-xrv51] から [cw-xrv52] に移動していることがわかります。

図 *13 : B-SID* ラベル



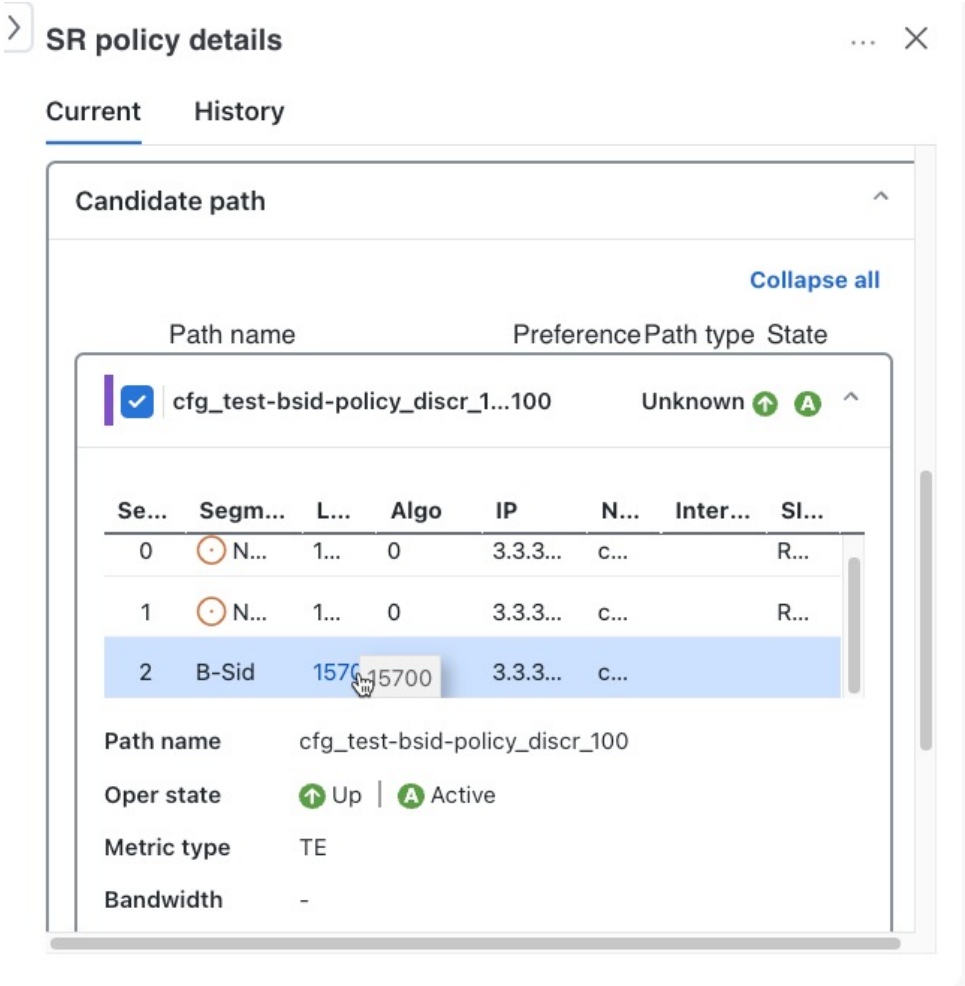
ステップ 3 **[SR ポリシーの詳細（SR policy details）]** ページで、[…] > **[詳細の表示（View details）]** をクリックします。

図 *14 : [*詳細の表示（*View Details*）*]*



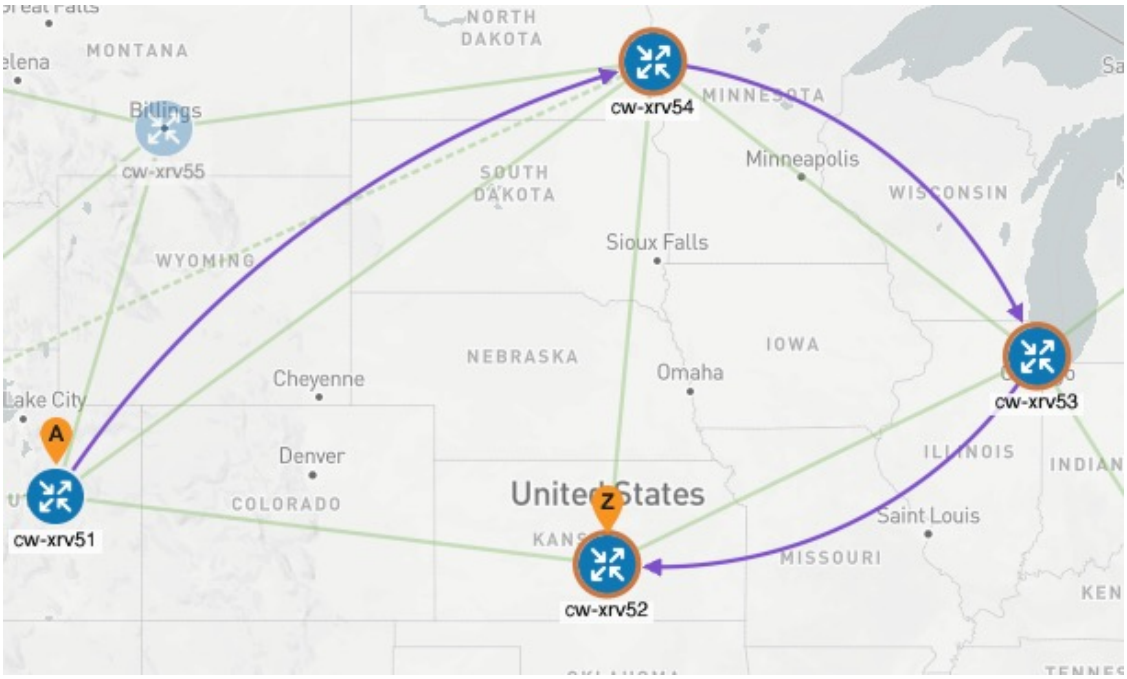
ステップ 4 アクティブパスを展開し、B-SID ラベル ID をクリックして、基礎となるパスを表示します。

図 *15 : B-SID* ラベル *ID*



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

図 *16 : B-SID* パス



ネイティブ SR パスの可視化

ネイティブパスを可視化すると、OAM（運用、管理、メンテナンス）アクティビティで、ラベルスイッチドパス（LSP）をモニターして転送の問題を迅速に隔離できるため、ネットワークの異常検出とトラブルシューティングに役立ちます。この機能ではマルチパスが使用されるため、すべての ECMP パスは送信元と接続先の間に表示されます。ネイティブ SR IGP パスのみを可視化できます。

デバイスの前提条件

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

1. デバイスは Cisco IOS XR 7.3.2 以上を実行している必要があります。`show version` コマンドを実行して確認します。
2. デバイスで GRPC を有効にする必要があります。PCE で gRPC を有効にする方法については、『Cisco Crosswork Network Controller 7.1 アドミニストレーション ガイド』の「Requirements for adding SR-PCE providers 」を参照してください。
    1. `show run grpc` を実行して GRPC の設定を確認します。以下のように表示されている必要があります。

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

or

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

（注）

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

3. デバイスでは、GNMI 機能を有効にして設定する必要があります。
   1. [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] で、目的のデバイスの IP アドレスをクリックします。
   2. [接続の詳細（Connectivity details）] の下に GNMI が一覧表示されていることを確認します。

      デバイスのタイプに基づいて、これらのデバイスのエンコーディングタイプを使用できます。適切なエンコーディングタイプは、デバイスの機能、サポートするデータモデル、およびデバイスと Crosswork Network Controller 間で予想されるデータの送信方法によって決まります。

      - **JSON**：人間が読めるため、ほとんどのデバイスで広くサポートされています。
      - **BYTES**：効率的な伝送のためにデータをバイナリ形式でエンコードします。
      - **PROTO**：gRPC で使用されるコンパクトで効率的なバイナリ形式。
      - **ASCII**：人間が読めるプレーンテキスト形式ですが、JSON と比較してあまり一般的に使用されていません。
      - **JSON IETF**：IETF YANG 仕様に準拠する JSON の標準化されたバリアント。

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。例：

```
RP/0/RP0/CPU0:xrvr-7.3.2#config

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

RP/0/RP0/CPU0:xrvr-7.3.2(config-static)#address-family ipv4 unicast <CDG Southbound
 interface IP: eg. 172.24.97.110> <Device Gateway eg: 172.29.105.1>

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

ネイティブパスの可視化

パスクエリを作成するには、次の手順に従います。

手順

ステップ 1 メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > **[パスクエリ（Path Query）]** を選択します。パスクエリのダッシュボードが表示されます。

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

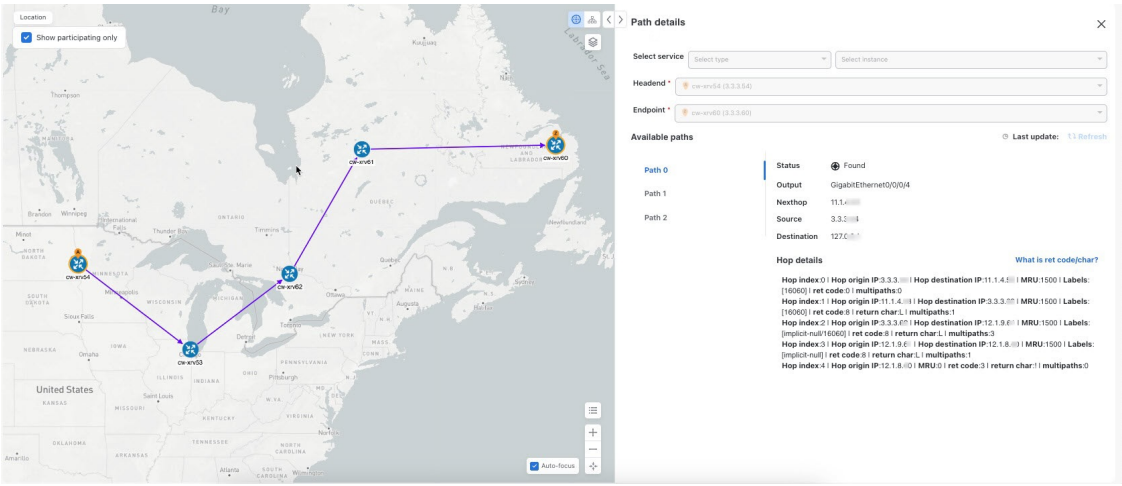
ステップ 3 必要なフィールドにデバイス情報を入力して、使用可能なネイティブ SR IGP パスを検索し、[パスの取得（Get paths）] をクリックします。

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

図 *17*：新しいパスクエリ

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

図 *18 :* パスの詳細



Crosswork Network Controller での TE リンクアフィニティの設定

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

インターフェイスのアフィニティ設定は、単にいくつかのビットをオンにします。これは 32 ビット値で、各ビット位置（0ー31）はリンク属性を表します。アフィニティマッピングは、特定のタイプのサービスプロファイルを表す色にすることができます（たとえば、低遅延、高帯域幅など）。これにより、リンク属性の参照が容易になります。

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

次の例は、デバイスの SR-TE アフィニティ設定（`affinity-map`）を示しています。

```
RP/0/RP0/CPU0:c12#sh running-config segment-routing traffic-eng affinity-map
Wed Jul 27 12:14:50.027 PDT
segment-routing
 traffic-eng
  affinity-map
   name red bit-position 1
   name blue bit-position 5
   name green bit-position 4
  !
 !
!
```

手順

ステップ 1 **[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。または、**[制約（Constraints）] > [アフィニティ（Affinity）]** フィールドの **[マッピングの管理（Manage Mapping）]** をクリックして、SR-TE ポリシー、Tree-SID または RSVP-TE トンネルのプロビジョニング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（上記の設定を使用）：

図 *19*：アフィニティのマッピング

ステップ 4 [保存（Save）] をクリックしてマッピングを保存します。別のマッピングを作成するには、[+作成（+ Create）] をクリックしてエントリを保存する必要があります。

アフィニティの削除と孤立したTEトンネル

（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。

ポリシー展開の考慮事項

ポリシーをプロビジョニングする前に、次のオプションを検討してください。

- ノード数、ポリシー数、またはインターフェイス数が多い拡張セットアップでは、ポリシーの展開中にタイムアウトが発生することがあります。タイムアウトオプションを設定するには、TE タイムアウト設定の構成 （16 ページ）を参照してください。
- 可視化のために、必要に応じてデバイスからアフィニティ情報を収集し、Cisco Crosswork にマッピングしてから SR ポリシー、Tree-SID、または RSVP-TE トンネルをプロビジョニングすることもできます。設定例については、アフィニティマップの設定 （10 ページ）を参照してください。

明示的 SR-MPLS ポリシーの作成

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

ヒント アフィニティを使用する場合は、デバイスからアフィニティ情報を収集し、Cisco Crosswork にマッピングしてから明示的な SR-MPLS ポリシーを作成します。詳細については、Crosswork Network Controller での TE リンクアフィニティの設定 （34 ページ）を参照してください。

手順

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

ステップ 2 [作成（Create）] > [PCEによって開始（PCE Init）] をクリックします。

（注）
Crosswork UI を介して Cisco Network Services Orchestrator（NSO）を使用して PCC によって開始されたポリシーをプロビジョニングする場合は、「（PCC によって開始された）SR-TE ポリシーの作成 （39 ページ）」を参照してください。

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

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

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

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

ステップ 6 [プレビュー（Preview）] をクリックして、作成したポリシーが意図と一致していることを確認します。

ステップ 7 ポリシーパスをコミットする場合は、[プロビジョニング（Provision）] をクリックしてネットワーク上でポリシーをアクティブにするか、終了して設定プロセスを中止します。

ステップ 8 SR-MPLS ポリシーの作成を検証します。

1. 新しい SR-MPLS ポリシーが [トラフィックエンジニアリング（Traffic engineering）] テーブルに表示されることを確認します。ポリシーの横にあるチェックボックスをクリックして、マップに強調表示されていることを確認することもできます。

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

2. 新しい SR-MPLS ポリシーの詳細を表示して確認します。[トラフィックエンジニアリング（Traffic engineering）] テーブルで、[…] をクリックし、[詳細表示（View details）] を選択します。

（注）
ノード数、ポリシー数、またはインターフェイス数が多いセットアップでは、ポリシーの展開中にタイムアウトが発生することがあります。タイムアウトオプションを設定するには、TE タイムアウト設定の構成（16 ページ）を参照してください。

最適化インテントに基づくダイナミック SR-MPLS ポリシーの作成

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

ダイナミックパスを使用して SR- MPLS ポリシーを作成するには、次の手順に従います。

手順

ステップ 1 **[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）]** > **[SR-MPLS]** を選択します。

ステップ 2 [作成（Create）]>[PCEによって開始（PCE Init）] をクリックします。Crosswork UI を介して Cisco Network Services Orchestrator（NSO）を使用して PCC によって開始されたポリシーをプロビジョニングする場合は、「（PCC によって開始された）SR-TE ポリシーの作成 （39 ページ）」を参照してください。

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。

アフィニティに関する考慮事項

- アフィニティの制約と分離は、同じ SR-MPLS ポリシーでは設定できません。また、同じ分離グループまたはサブグループ内に 3 つ以上の SR-MPLS ポリシーを含めることはできません。設定はプレビュー中に許可されません。
- ここで定義した分離グループに属する既存の SR-MPLS ポリシーがある場合は、プレビュー時に、同じ分離グループに属するすべての SR-MPLS ポリシーが表示されます。

ステップ 7 [セグメント（Segments）] で、使用可能な場合に保護セグメントを使用するかどうかを選択します。

ステップ 8 該当する SID 制約を入力します。Crosswork Network Controller 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。

SID 情報

- 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には、**[プロビジョニング（Provision）]** をクリックします。

ステップ 11 SR-MPLS ポリシーの作成を検証します。

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

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

2. 新しい SR-MPLS ポリシーの詳細を表示して確認します。[トラフィックエンジニアリング（Traffic engineering）] テーブルで、⋯ をクリックし、[詳細表示（View details）] を選択します。

（PCC によって開始された）SR-TE ポリシーの作成

このタスクでは、Crosswork UI を介して Cisco Network Services Orchestrator（NSO）を使用して、明示的または動的な SR-MPLS または SRv6 ポリシーを作成します。

始める前に

明示的に PCC によって開始された SR-MPLS または SRv6 ポリシーを作成する場合は、セグメント ID リストを作成する必要があります（[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [プロビジョニング（NSO）（Provisioning (NSO)）] > [SR-TE] > [SID リスト（SID-List）]）。プレフィックスまたは隣接セグメント ID のリストで構成される明示的な（固定）パスで、各リストはパス上のノードまたはリンクを表します。

手順

ステップ 1 メインメニューから、**[サービスとトラフィックエンジニアリング（Services and Traffic Engineering）] > [プロビジョニング（NSO）（Provisioning (NSO)）]**を選択します。

ステップ 2 [SR-TE] > [ポリシー（Policy）] の順に選択し、＋ をクリックします。Crosswork に [SR-TEの作成（Create SR-TE）] > [ポリシー（Policy）] ウィンドウが表示されます。

（注）
⬇ をクリックして、既存の SR-TE ポリシーをインポートすることもできます。

ステップ 3 ポリシー制約と必要な値を入力します。

次のオプションを入力する必要があります。

表 *2 : SR-TE* ポリシーの設定

これを展開します。	これを指定するには、次の手順を実行します。
name	この SR-TE ポリシーの名前を入力します。

これを展開します。	これを指定するには、次の手順を実行します。
head-end	• ＋ をクリックしてノードを選択するか、ノード名を手動で入力できます。
tail-end	ノード名を手動で入力します。
color	色を入力します。例：200。
path	**1.** ＋ をクリックし、プリファレンス値を入力します。例：123 **2.** 次のいずれかを選択し、スイッチを切り替えて有効にします。 • [明示的なパス（explicit-path）]：＋ をクリックして、以前に設定した SID リストを追加します。 • [動的パス（dynamic-path）]：最小化するメトリックを選択し、適用可能な制約と分離を定義します。
srv6	SRv6 ポリシーを作成する場合は、[srv6を有効にする（Enable srv6）] に切り替えます。

ステップ 4 完了したら、[ドライラン（Dry Run）] をクリックして変更を検証し、保存します。Crosswork でポップアップウィンドウに変更が表示されます。

この例で説明している要件と一致しない要件を持つサービスを設定する場合は、シスコのカスタマーエクスペリエンスにお問い合わせください。

ステップ 5 ポリシーをアクティブ化する準備ができたら、[変更を確定（Commit Changes）] をクリックします。

SR-MPLS ポリシーの変更

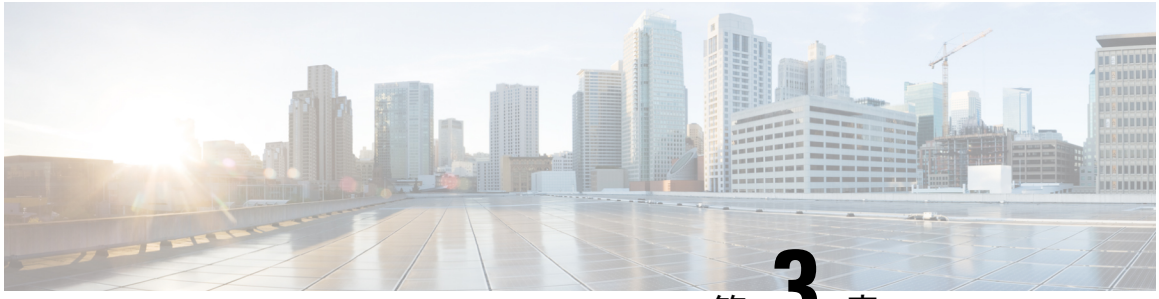
Crosswork Network Controller API または UI を使用して作成した SR-MPLS ポリシーのみ変更または削除できます。SR-MPLS ポリシーを表示、変更、または削除するには、次の手順に従います。

手順

ステップ 1 **[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）] > [SR-MPLS]** タブを選択します。

ステップ 2 [トラフィックエンジニアリング（Traffic engineering）] テーブルから、目的の SR-MPLS ポリシーを見つけて ⋯ をクリックします。

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

リソース予約プロトコル（RSVP）

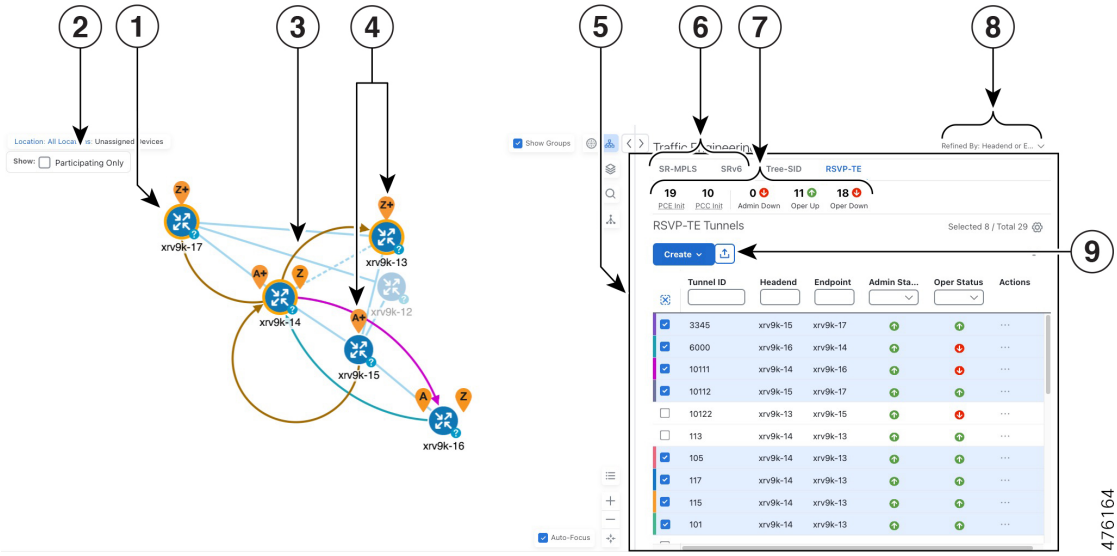
このセクションでは、Crosswork Optimization Engine がサポートする RSVP-TE トンネル機能について説明します。既知の制限事項と重要な注意事項のリストについては、『Cisco Crosswork Network Controller Release Notes』を参照してください。

- トポロジマップでの RSVP-TE トンネルの表示 （43 ページ）
- RSVP-TE トンネルの詳細の表示 （46 ページ）
- 明示的 RSVP-TE トンネルの作成 （49 ページ）
- 最適化インテントに基づくダイナミック RSVP-TE トンネルの作成 （50 ページ）
- RSVP-TE トンネルの作成（PCC によって開始） （51 ページ）
- RSVP-TE トンネルの変更 （52 ページ）

トポロジマップでの RSVP-TE トンネルの表示

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

図 *20 :* トラフィック エンジニアリング *UI* : *RSVP-TE* トンネル



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

引き出し線番号	説明
3	RSVP-TE トンネルは [RSVP-TEトンネル（RSVP-TE Tunnels）] テーブルで選択されると、送信元と宛先を示す色付きの矢印線としてマップに表示されます。 • レコードルートオブジェクト（RRO）パスは直線で表示されます。 • 明示的ルートオブジェクト（ERO）パスは曲線として表示されます。 （注） RRO と ERO の両方のパスが使用可能な場合、デフォルトで RRO パスが表示されます。 • 隣接セグメント ID（SID）は、パスに沿ったリンクに緑色のドット（）として表示されます。 A と Z の両方が 1 つのデバイスクラスタに表示される場合、クラスタ内の 1 つ以上のノードが送信元で、別のノードが宛先です。A+ は、1 つのノードから発信される複数の RSVP-TE トンネルがあることを示します。Z+ は、ノードが複数の RSVP-TE トンネルの宛先であることを示します。
4	**[SR-MPLSおよびSRv6ポリシーの送信元と接続先（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、他のノードが接続先です。A+ は、1 つのノードから発信される複数の SR-TE ポリシーがあることを示します。Z+ は、ノードが複数の SR ポリシーの宛先であることを示します。
5	このウィンドウの内容は、選択またはフィルタ処理された内容によって異なります。この例では、[RSVP-TE] タブが選択され、[RSVP-TE Tunnels] テーブルが表示されます。トポロジマップで選択した内容、または RSVP-TE トンネルを表示および管理しているプロセスに応じて、次の手順を実行できます。 • 最適化インテントに基づくダイナミック RSVP-TE トンネルの作成 （50 ページ） • 明示的 RSVP-TE トンネルの作成 （49 ページ） • RSVP-TE トンネルの変更 （52 ページ） • RSVP-TE トンネルの詳細の表示 （46 ページ）
6	[RSVP-TE] タブをクリックします。
7	[Mini Dashboard] には、動作中の RSVP-TE トンネルの概要と、[RSVP-TE] テーブルに現在リストされている PCC および PCE によって開始されたトンネルの数が表示されます。フィルタが適用されると、[Mini Dashboard] が更新され、[RSVP-TE] テーブルに表示される内容が反映されます。

引き出し線番号	説明
8	このオプションでは、グループフィルタ（使用している場合）をテーブルデータに適用する方法を選択できます。たとえば、[ヘッドエンドのみ（Headend only）] を選択した場合、ポリシーのヘッドエンドデバイスが選択されたグループにあるポリシーのみが表示されます。このフィルタを使用すると、特定の設定を確認でき、大規模なネットワークがある場合に役立ちます。 フィルタオプション： • **[ヘッドエンドまたはエンドポイント（Headend or Endpoint）]**：選択したグループ内のヘッドエンドまたはエンドポイントデバイスを含むポリシーを表示します。 • **[ヘッドエンドおよびエンドポイント（Headend and Endpoint）]**：ヘッドエンドとエンドポイントの両方がグループ内にある場合にポリシーを表示します。 • [Headend only]：ポリシーのヘッドエンドデバイスが選択したグループにある場合にポリシーを表示します。 • [エンドポイントのみ（Endpoint only）]：ポリシーのエンドポイントデバイスが選択したグループ内にある場合にポリシーを表示します。
9	CSV ファイルにすべてのデータをエクスポートします。選択またはフィルタ処理されたデータをエクスポートすることはできません。

RSVP-TE トンネルの詳細の表示

バインディングラベル、委任 PCE、メトリックタイプ、ERO/RRO、遅延など、RSVP-TE トンネルの詳細を表示します。RSVP-TE トンネルの詳細を表示するには、次の手順に従います。

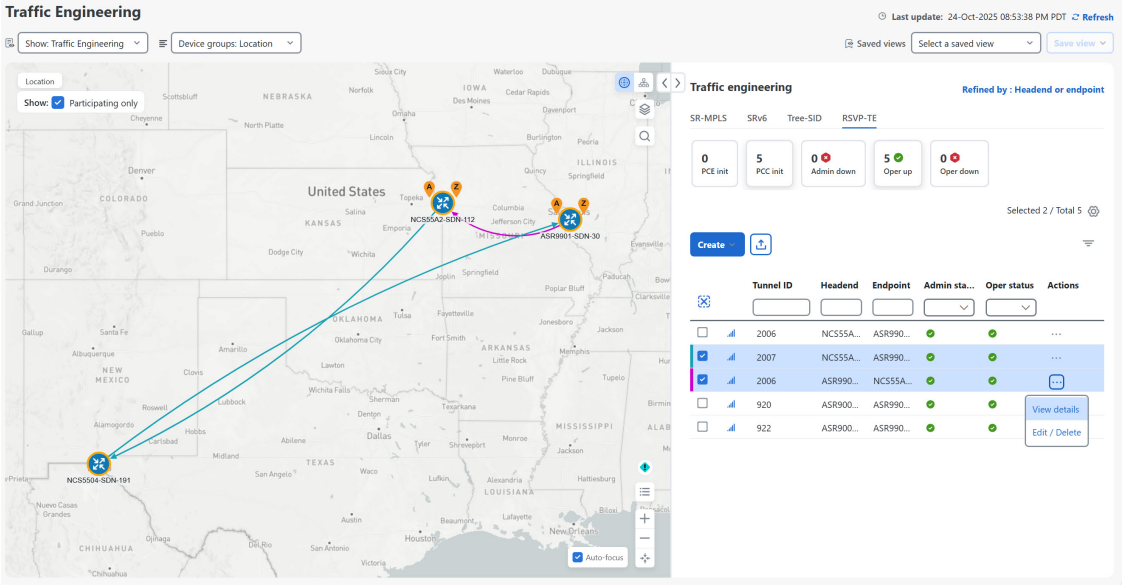
始める前に

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）。

手順

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

図 *21 : [RSVP-TE] > [*詳細の表示（*View details*）*]*



ステップ 2 RSVP-TE トンネルの詳細を表示します。ブラウザから、URL をコピーして他のユーザーと共有できます。該当する場合は、すべてのポリシーの [遅延（Delay）] 値は 10 分ごとに計算されます。[遅延（Delay）] 値の横にある [i] アイコンをクリックすると、値が最後に更新された時刻が表示されます。

図 *22 : RSVP-TE* トンネルの詳細

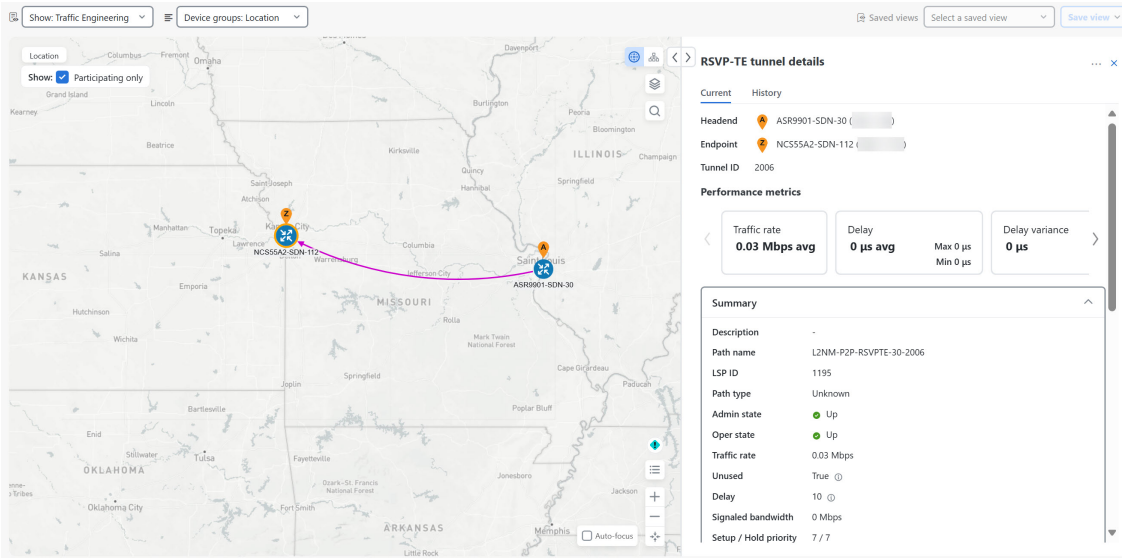


図 ***23 : RSVP-TE*** トンネルの詳細（クローズアップ）

明示的 RSVP-TE トンネルの作成

このタスクでは、プレフィックスのリストまたは隣接セグメント ID のリスト（SID リスト）で構成される明示的な（固定）パスを使用して RSVP-TE トンネルを作成します。このそれぞれがパスに沿ったノードまたはリンクを表します。明示的RSVP-TE トンネルを作成するには、次の手順に従います。

始める前に

ノード数、ポリシー数、またはインターフェイス数が多い拡張セットアップでは、ポリシーの展開中にタイムアウトが発生することがあります。タイムアウトオプションを設定するには、TE タイムアウト設定の構成 （16 ページ）を参照してください。

手順

ステップ 1 **[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）] > [RSVP-TE]** を選択します。

ステップ 2 [作成（Create）] > [PCEによって開始（PCE Init）] をクリックします。Crosswork UI を介して NSO を使用してPCCによって開始されたトンネルをプロビジョニングする場合は、「RSVP-TE トンネルの作成（PCC によって開始） （51 ページ）」を参照してください。

ステップ 3 [トンネルの詳細（Tunnel details）] で、必要な RSVP-TE トンネル値を入力します。各フィールドの説明を表示するには、ⓘ の上にマウスポインタを合わせます。

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

ステップ 4 [トンネルパス（Tunnel path）] で、[明示的パス（Explicit path）] をクリックし、パス名を入力します。

ステップ 5 RSVP-TE パスの一部となるセグメントを追加します。

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

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

ステップ 8 RSVP-TE トンネルの作成を検証します。

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

   （注）
   新しくプロビジョニングされた RSVP-TE トンネルは、ネットワークのサイズやパフォーマンスによっては、[トラフィックエンジニアリング（Traffic engineering）]テーブルに表示されるまでに時間がかか

る場合があります。[トラフィックエンジニアリング（Traffic engineering）] テーブルは 30 秒ごとに更新されます。

2. 新しい RSVP-TE トンネルの詳細を表示して確認します。[トラフィックエンジニアリング（Traffic engineering）] テーブルで、⋯（RSVP-TE トンネルと同じ行にある）をクリックし、[詳細表示（View details）] を選択します。

最適化インテントに基づくダイナミック RSVP-TE トンネルの作成

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

始める前に

ポリシー展開の考慮事項

- ノード数、ポリシー数、またはインターフェイス数が多い拡張セットアップでは、ポリシーの展開中にタイムアウトが発生することがあります。タイムアウトオプションを設定するには、TE タイムアウト設定の構成 （16 ページ）を参照してください。
- 視覚化のために、必要に応じてデバイスからアフィニティ情報を収集し、Cisco Crosswork にマッピングしてからダイナミック SR-MPLS ポリシーを作成することもできます。Crosswork Network Controller での TE リンクアフィニティの設定 （34 ページ） を参照してください。

手順

ステップ 1 **[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）] [RSVP-TE]** を選択します。

ステップ 2 [作成（Create）] > [PCEによって開始（PCE Init）] をクリックします。Crosswork Network Controller UI を介して NSO を使用して PCC によって開始されたトンネルをプロビジョニングする場合は、RSVP-TE トンネルの作成（PCC によって開始） （51 ページ）を参照してください。

ステップ 3 [トンネルの詳細（Tunnel details）] で、必要な RSVP-TE トンネル値を入力します。各フィールドの説明を表示するには、ⓘ の上にマウスポインタを合わせます。

ヒント

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

ステップ 4 **[トンネルパス（Tunnel path）]** の下にある **[ダイナミックパス（Dynamic path）]** をクリックし、パス名を入力します。

ステップ 5 [最適化の目的（Optimization objective）] で、最小化するメトリックを選択します。

ステップ 6 該当する制約と分離を定義します。

アフィニティに関する考慮事項

- 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。
- 最大 2 つの RSVP-TE トンネルを同じ分離グループグループやサブグループに含めることができます。ここで定義した分離グループに属する既存の RSVP-TE トンネルがある場合は、プレビュー時に同じ分離グループに属するすべての RSVP-TE トンネルが表示されます。

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

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

ステップ 9 RSVP-TE トンネルの作成を検証します。

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

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

2. 新しい RSVP-TE トンネルの詳細を表示して確認します。[トラフィックエンジニアリング（Traffic engineering）] テーブルで、[…] をクリックし、[詳細表示（View details）] を選択します。

RSVP-TE トンネルの作成（PCC によって開始）

このタスクでは、Crosswork UI を介して Cisco Network Services Orchestrator（NSO）を使用して、明示的または動的な RSVP-TE トンネルを作成します。

始める前に

明示的に PCC によって開始された RSVP-TE トンネルを作成する場合は、セグメント ID リストを作成する必要があります（[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [プロビジョニング（NSO）（Provisioning (NSO)）] > [SR-TE] > [SIDリスト

（SID-List）]）。プレフィックスまたは隣接セグメントIDのリストで構成される明示的な（固定）パスで、各リストはパス上のノードまたはリンクを表します。

手順

ステップ 1 メインメニューから、**[サービスとトラフィックエンジニアリング（Services and Traffic Engineering）] > [プロビジョニング（NSO）（Provisioning (NSO)）]**を選択します。

ステップ 2 [RSVP-TE] > [トンネル（Tunnel）] の順に選択し、＋ をクリックします。Crosswork に [RSVP-TEの作成（Create RSVP-TE）] > [トンネル（Tunnel）] ウィンドウが表示されます。

（注）
をクリックして、既存の RSVP-TE トンネルをインポートすることもできます。

ステップ 3 ポリシー制約と必要な値を入力します。

ステップ 4 完了したら、[ドライラン（Dry run）] をクリックして変更を検証し、保存します。Crosswork でポップアップウィンドウに変更が表示されます。

ステップ 5 ポリシーをアクティブ化する準備ができたら、[変更を確定（Commit changes）] をクリックします。

RSVP-TE トンネルの変更

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

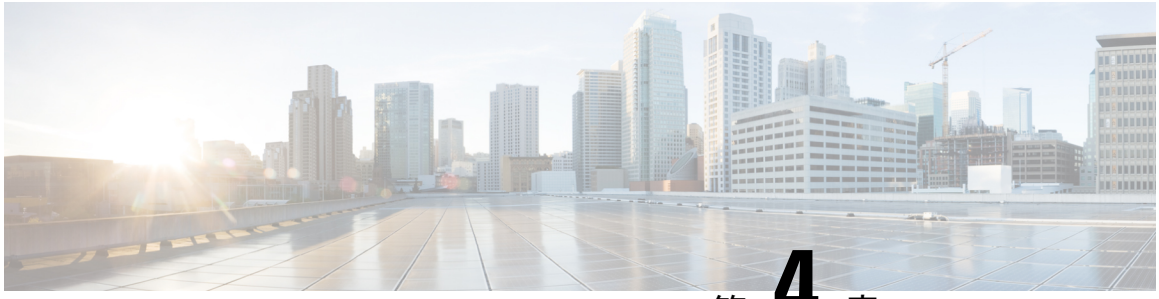
手順

ステップ 1 メインメニューから、**[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）]**> [RSVP-TE] タブを選択します。

ステップ 2 対象とする RSVP-TE トンネルを見つけて ··· をクリックします。

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

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



第 4 章

フレキシブルアルゴリズム

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

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

ここでは、次の内容について説明します。

- サポートされるフレキシブルアルゴリズムのメトリックと制約 （53 ページ）
- Crosswork Network Controller でのフレキシブルアルゴリズムのアフィニティの設定 （54 ページ）
- フレキシブル アルゴリズム トポロジの可視化 （55 ページ）
- フレキシブルアルゴリズムの詳細の表示 （57 ページ）

サポートされるフレキシブルアルゴリズムのメトリックと制約

Crosswork Network Controller は、Cisco IOS XR で使用可能なものと比較して、限定されたメトリックと制約のセットをサポートしています。Crosswork Network Controller でまだサポートされていないメトリックと制約を使用してフレキシブルアルゴリズムを設定する場合、この機能

は引き続きルータで機能します。ただし、Crosswork Network Controller UI での SR ポリシーのパスとトポロジの可視化は正確ではない場合があります。

以下は、Crosswork Network Controller でサポートされているメトリックと制約のリストです。

メトリック

- IGP メトリック
- [ASLA トラフィック エンジニアリング デフォルト（ASLA Traffic Engineering Default）]：このメトリックは必須です。設定されていない場合は、リンクがプルーニングされます。
- [ASLA 最小単方向リンク遅延（ASLA Min Unidirectional Link Delay）]：このメトリックは必須です。設定されていない場合は、リンクがプルーニングされます。

制約

アプリケーション固有のリンク属性（ASLA）では、Crosswork Network Controller は以下をサポートします。

- include-any
- include-all
- exclude

Crosswork Network Controller でのフレキシブルアルゴリズムのアフィニティの設定

デバイスで定義されたフレキシブルアルゴリズムのアフィニティは Crosswork によって収集されません。必要に応じて、デバイス設定のフレキシブルアルゴリズムのアフィニティ名との一貫性を保つために、Crosswork ネットワークコントローラ UI でアフィニティマッピングを定義することができます。Crosswork ネットワークコントローラ は、プロビジョニング中にビット情報のみを SR-PCE に送信します。アフィニティマッピングが UI で定義されていない場合、アフィニティ名は「UNKNOWN」と表示されます。可視化のために Crosswork ネットワークコントローラ でアフィニティマッピングを設定する場合は、デバイスでアフィニティを収集し、デバイスで使用されているものと同じ名前とビットを使用して Crosswork ネットワークコントローラ でアフィニティマッピングを定義する必要があります。

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

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

```
router isis CORE
 is-type level-2-only
 net 49.0001.0000.0000.0002.00
```

```
log adjacency changes
affinity-map b33 bit-position 33
affinity-map red bit-position 1
affinity-map blue bit-position 5
flex-algo 128
 priority 228
 advertise-definition
 affinity exclude-any blue indigo violet black
!
```

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

手順

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

ステップ 2 **[+作成（+ Create）]** をクリックします。

ステップ 3 割り当てる名前とビットを入力します。

ステップ 4 [保存（Save）] をクリックしてマッピングを保存します。リンクのすべてのフレキシブル アルゴリズム アフィニティを表示するには、フレキシブルアルゴリズムの詳細の表示 （57ページ）を参照してください。

フレキシブル アルゴリズム トポロジの可視化

Crosswork を使用すると、ネットワーク内で UI を使用して手動で設定または動的にプロビジョニングされたトポロジマップ上のフレキシブルアルゴリズムのノードやリンクを可視化できます。

（注） SR-MPLS ポリシーを動的にプロビジョニングするときにフレキシブルアルゴリズムの制約を適用するには、最適化インテントに基づくダイナミック SR-MPLS ポリシーの作成 （37 ページ）を参照してください。

始める前に

ネットワークのフレキシブルアルゴリズムについて理解し、設定する必要があります。お使いのデバイスの SR フレキシブルアルゴリズムの設定についてのマニュアルを参照して、説明とサポートされている設定コマンドを確認してください（『Segment Routing Configuration Guide for Cisco NCS 540 Series Routers』など）。

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

手順

ステップ 1 メインメニューから、**[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）]** を選択します。

ステップ 2 トポロジマップから、 をクリックします。

ステップ 3 [Flex Algo] タブをクリックします。

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

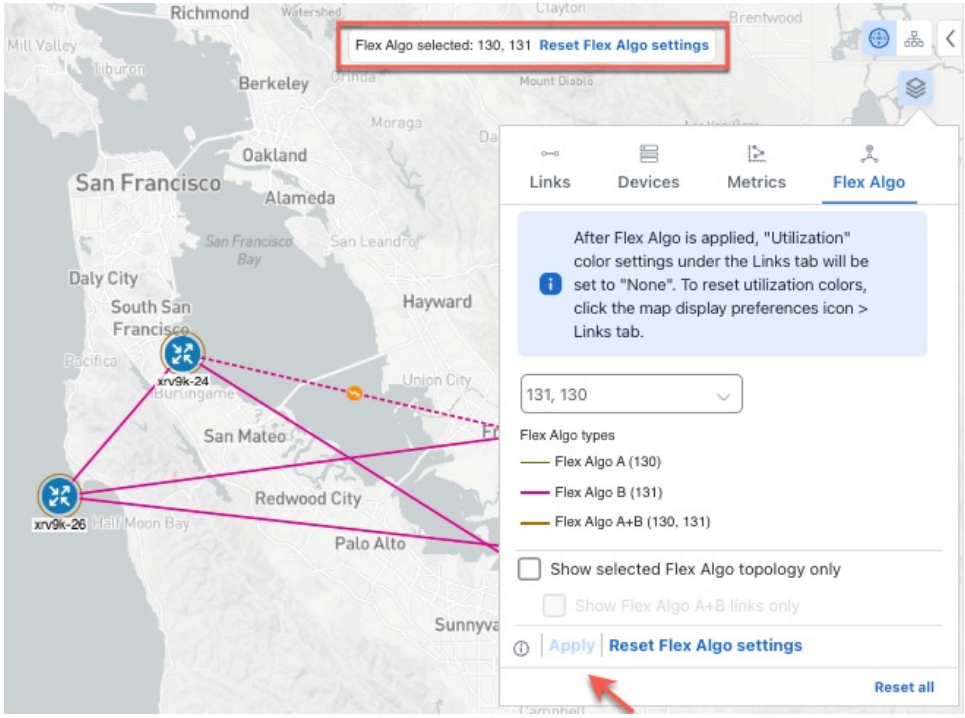
ステップ 5 [Flexible Algorithm Types] を表示し、選択内容が正しいことを確認します。各フレキシブルアルゴリズムの色の割り当てにも注意してください。

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

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

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

図 *24*：マップ上のフレキシブルアルゴリズム



（注）
選択したフレキシブルアルゴリズムが基準で定義されているが、（青色ですべてのノードやリンクを含むように定義されたアフィニティなど）一致するリンクとノードの組み合わせがない場合、トポロジマップ

は空白になります。選択したフレキシブルアルゴリズムがノードまたはリンクに設定されていない場合は、青色（デフォルト）のリンクまたはノードの色が表示されます。

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

フレキシブルアルゴリズムの詳細の表示

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

手順

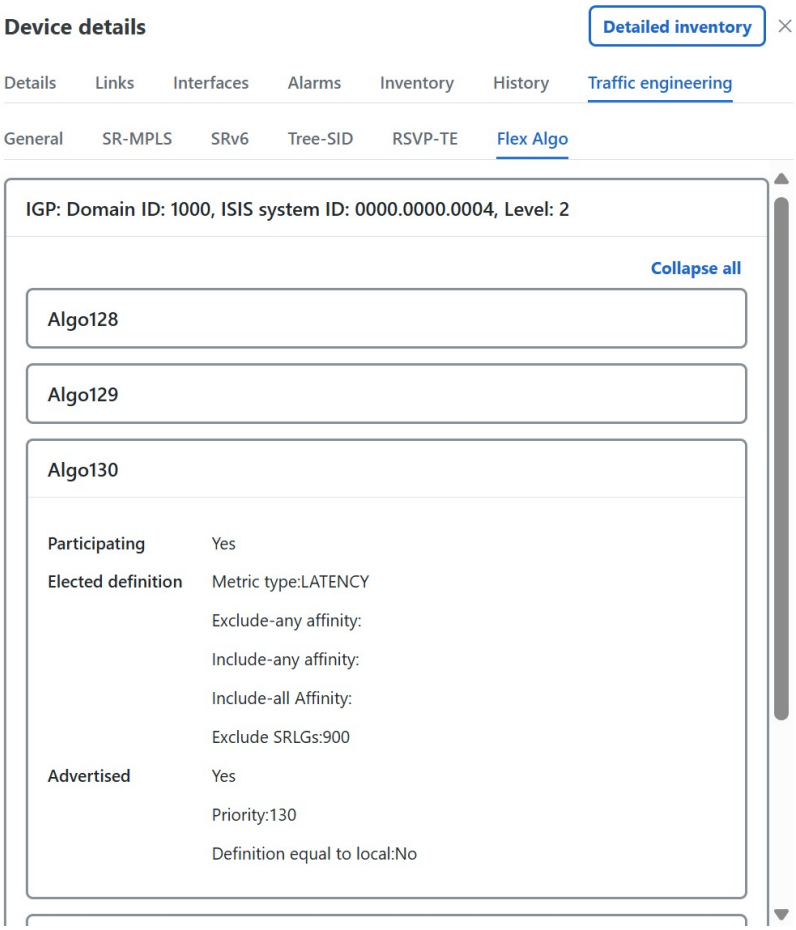
ステップ 1 メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > **[トラフィックエンジニアリング（Traffic Engineering）]** を選択します。

ステップ 2 デバイスのフレキシブルアルゴリズムの詳細を表示するには、次の手順を実行します。

a) トポロジマップから、デバイスをクリックします。

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

図 *25 : Flex Algo* デバイスの詳細

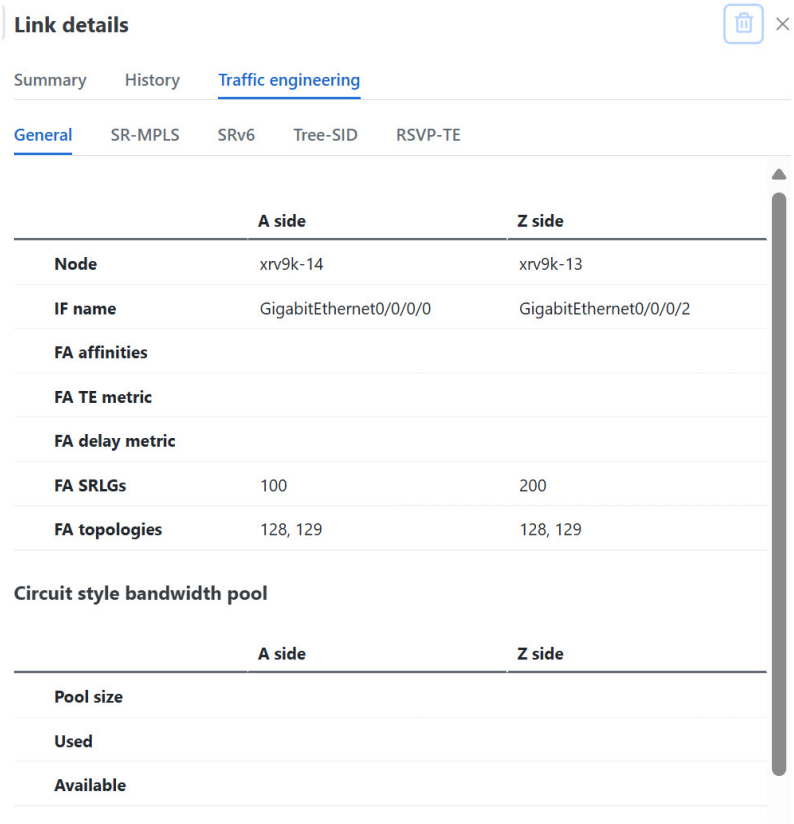


ステップ 3 リンクがフレキシブルアルゴリズム トポロジの一部であるかどうかを表示するには、次の手順を実行します。

a) トポロジマップから、リンクをクリックします。リンクのリストが表示されたら、リンクタイプをクリックします。

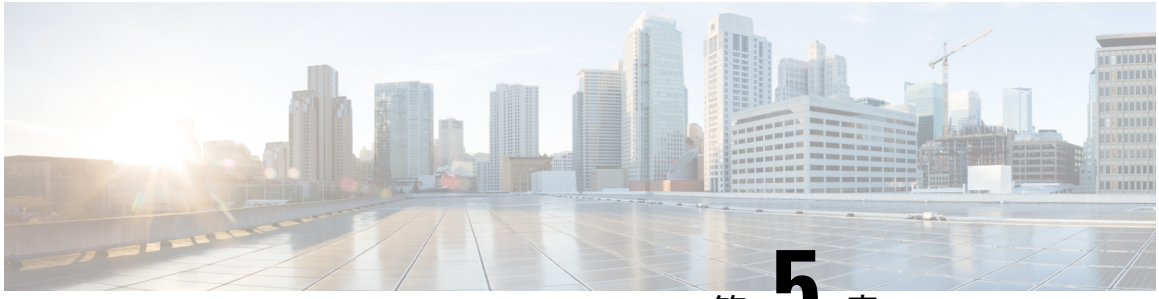
b) [リンクの詳細（Link details）] ウィンドウで、[トラフィックエンジニアリング（Traffic Engineering）] タブをクリックします。リンクがメンバーの場合、[FAトポロジ（FA topologies）] の行には、各ソースおよび接続先デバイスが属するフレキシブルアルゴリズムが表示されます。

図 *26 : Flex Algo* リンクの詳細



（注）

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



第 5 章

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

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

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

Tree-SID の詳細については、お使いのデバイスのセグメントルーティング Tree-SID 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）

ここでは、次の内容について説明します。

- Tree-SID ポリシーの可視化 （62 ページ）
- トポロジマップでのポイントツーマルチポイント ツリーの表示 （62 ページ）
- 静的 Tree-SID ポリシーの作成 （66 ページ）
- Tree-SID ポリシーの変更 （70 ページ）

Tree-SID ポリシーの可視化

Crosswork UI により、Tree-SID ルート、トランジットノード、リーフノード、バドノードの詳細を UI に表示できるようになり、Tree-SID がネットワークに正しく実装されていることを簡単に確認できます（トポロジマップでのポイントツーマルチポイント ツリーの表示 （62 ページ）を参照してください）。

Tree-SID ポリシーには次のノードがあります。

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

次の Tree-SID ポリシーを可視化できます。

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

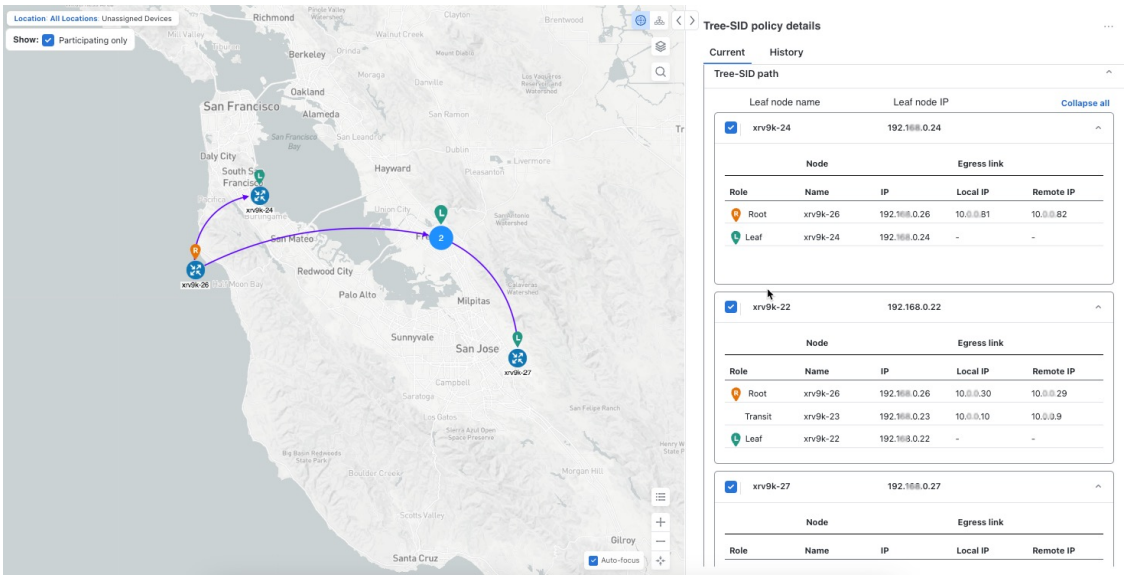
（注） 静的および動的 Tree-SID ポリシーは、高速再ルーティング（FRR）をサポートしています。

トポロジマップでのポイントツーマルチポイント ツリーの表示

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

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

図 *27*：新しい ***Tree-SID*** ポリシーの作成（静的）



始める前に

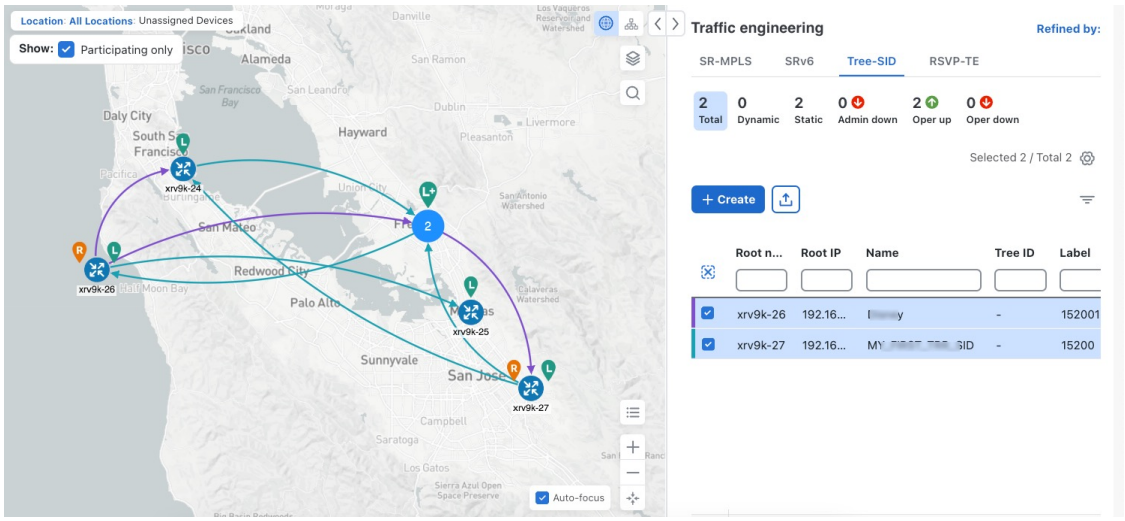
トポロジマップでマルチキャストツリーを可視化するには、ネットワークでTree-SIDポリシーを設定する必要があります。詳細については、お使いのデバイスの SR Tree-SID 設定のマニュアルを参照してください（『Segment Routing Configuration Guide for Cisco NCS 540 Series Routers』など）

手順

ステップ 1 メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [トラフィックエンジニアリング（Traffic Engineering）] > [Tree-SID]** を選択します。

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

図 *28 :* トポロジマップの *Tree-SID* ポリシー（静的）



（注）
エンドポイントの変更は、履歴データのタブにイベントとしてキャプチャされます。Tree-SID の履歴データについては、TE イベントと使用率履歴の表示 （13 ページ）を参照してください

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

例：

（注）

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

図 *29 : Tree-SID* の詳細の概要

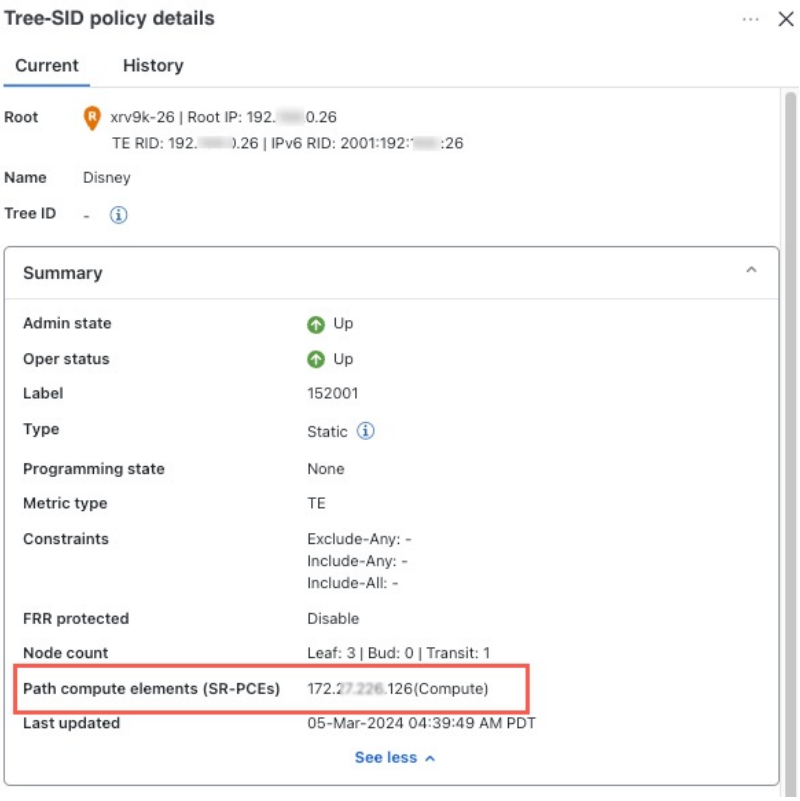
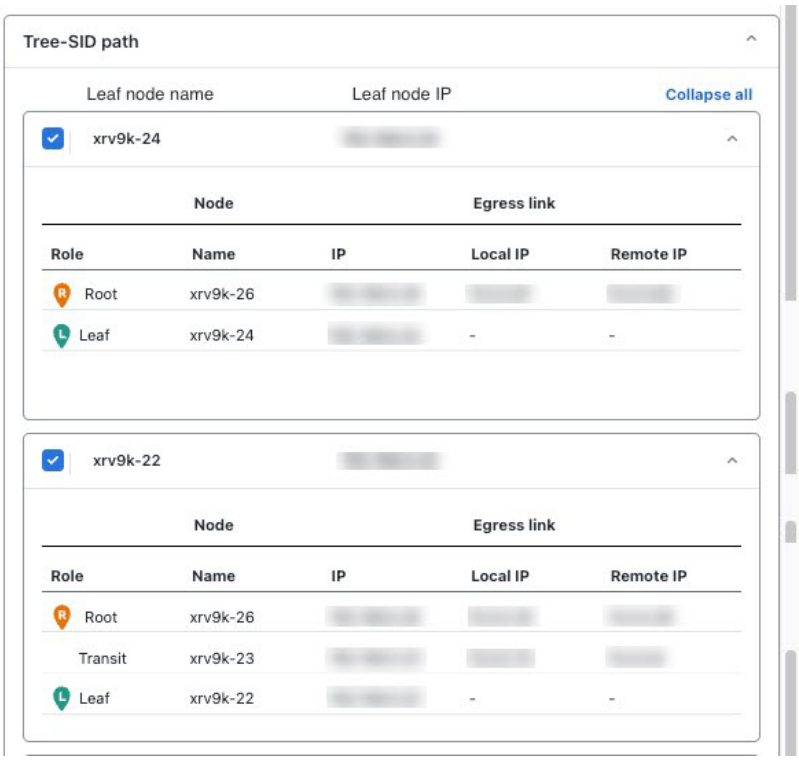


図 *30 : Tree-SID* パスの詳細



静的 Tree-SID ポリシーの作成

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

ヒント アフィニティを使用する場合は、デバイスからアフィニティ情報を収集し、それらを Cisco Crosswork にマッピングしてから静的 Tree-SID ポリシーを作成します。詳細については、Crosswork Network Controller での TE リンクアフィニティの設定 （34 ページ）を参照してください。

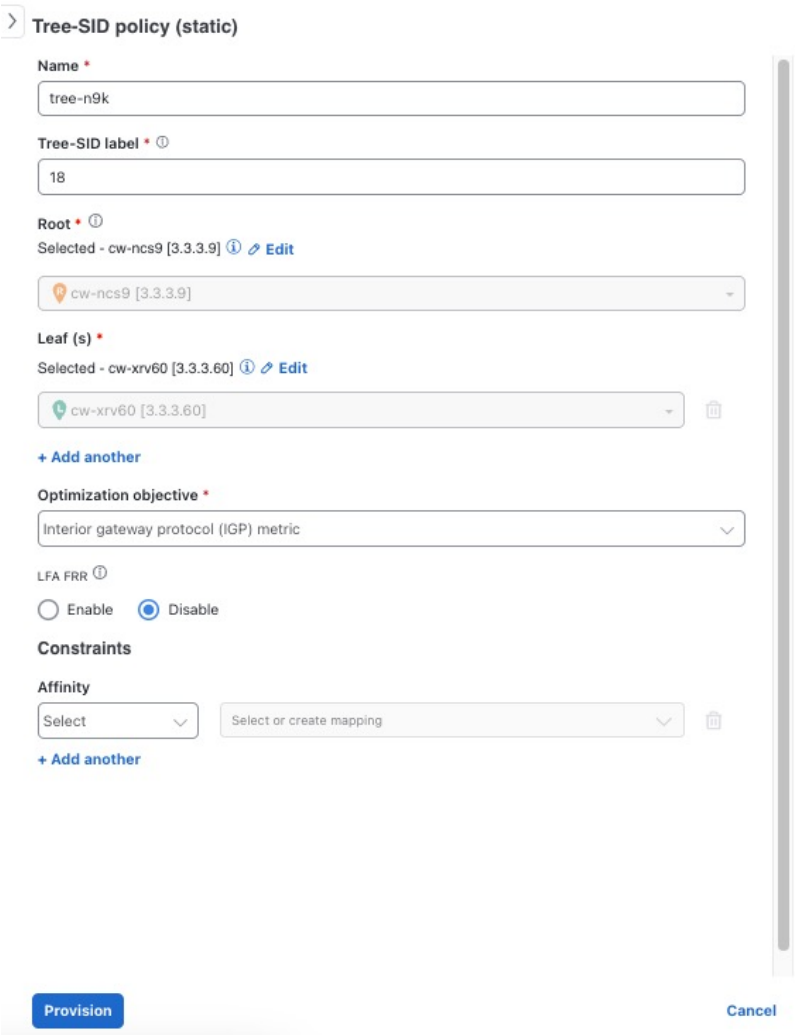
手順

ステップ 1 メインメニューから、**[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）]**> [ツリーSID（Tree-SID）] タブを選択し、[作成（Create）] をクリックします。

ステップ 2 必要なTree-SIDポリシー値を入力または選択します。フィールドの説明を表示するには、ⓘの上にマウスポインタを合わせます。

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

図 *31 :* 静的 *Tree-SID* ポリシーの作成



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

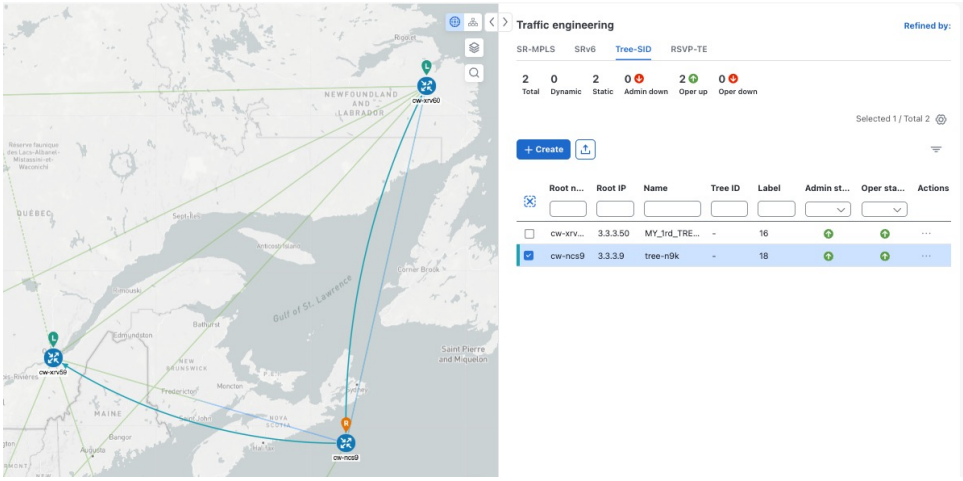
ステップ 4 Tree-SID ポリシーの作成を検証します。

1. 新しい Tree-SID ポリシーが [トラフィックエンジニアリング（Traffic engineering）] テーブルに表示されることを確認します。ポリシーの横にあるチェックボックスをクリックして、マップに強調表示されていることを確認することもできます。

   （注）

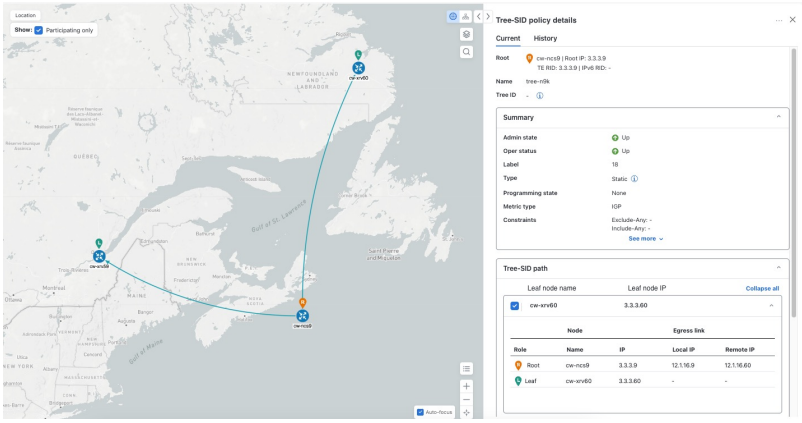
新しくプロビジョニングされた Tree-SID ポリシーは、ネットワークのサイズやパフォーマンスによっては、[トラフィックエンジニアリング（Traffic engineering）]テーブルに表示されるまでに時間がかかる場合があります。[トラフィックエンジニアリング（Traffic engineering）] テーブルは 30 秒ごとに更新されます。

図 *32 :* トポロジマップに新たに追加された *Tree-SID* ポリシー



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

図 *33 : Tree-SID* ポリシーの詳細



静的 Tree-SID ポリシーの設定例

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

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

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

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

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

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

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

Tree-SID ポリシーの変更

Tree-SID ポリシーを変更するには、次の手順を実行します。

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

手順

ステップ 1 メインメニューから、**[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）]**> [ツリーSID（Tree-SID）] タブを選択します。

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

ステップ 3 [編集/削除（Edit / Delete）] を選択します。

（注）

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

Tree-SID の重要な考慮事項

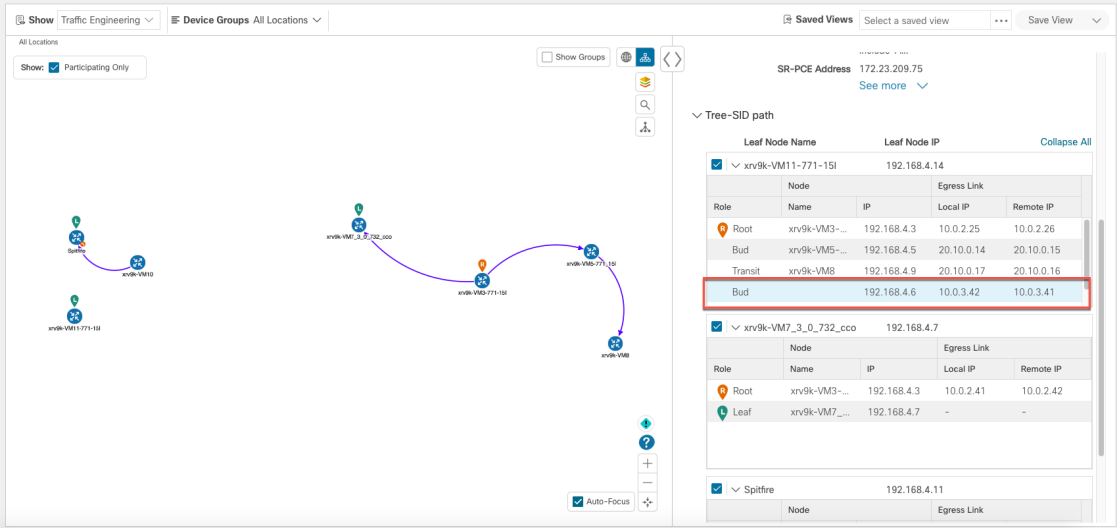
制限事項

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

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

ノードが欠落している Tree-SID パスの可視化

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



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。