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 がネットワークパフォーマンスを向上させる方法の 1 つは、トラフィックに事前定義されたルートを強制し、使用可能なリソースを効果的に使用することです。

Crosswork を使用する最大の利点の 1 つは、トポロジマップで SR-TE ポリシーと RSVP-TE トンネルを可視化できることです。ネットワークを視覚的に調べることで、SR-TE ポリシーのプロビジョニングと管理の複雑さが大幅に軽減されます。

ブラウンフィールド展開での既存の SR-TE ポリシーと RSVP-TE

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

ここでは、次の内容について説明します。

サポート対象の SR-TE ポリシーと RSVP トンネル

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

表 *1*: サポート対象の *TE* テクノロジー

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

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

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

セグメントルーティングの概要

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

セグメント

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

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

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

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

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

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

セグメント ルーティング ポリシー

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

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

- SR-MPLS および SRv6
- フレキシブルアルゴリズム

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

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

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

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

セグメントルーティングパス計算要素（SR-PCE）

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

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

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

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

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

SR-TE ポリシー PCC および PCE 設定のソース

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

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

（注） UI を使用して設定された SR ポリシーは、Crosswork で変更または削除できる唯一の SR-TE ポリシータイプです。

PCC によって開始された SR-TE ポリシーの例

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

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

リソース予約プロトコル（RSVP）について

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

RSVP-TE プロセスには、次の機能が含まれています。

- エンドポイント制御。ヘッドエンドとテールエンドでの TE トンネルの確立と管理に関連付けられます。
- リンク管理。TE ラベルスイッチパス（LSP）のリソース認識型ルーティングを実行し、MPLS ラベルをプログラムするためにリンクリソースを管理します。

- 高速再ルーティング（FRR）。保護が必要な LSP を管理し、これらの LSP にバックアップトンネル情報を割り当てます。

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

RSVP-TE 明示的ルーティング（ストリクト、ルーズ）

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

ERO で指定された明示的パスは、ストリクトパスまたはルーズパスです。

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

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

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

RSVP FRR

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

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

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

FRR 要件のシグナリングは、TE トンネルヘッドエンドで開始されます。パスに沿ったローカル修復ポイント（PLR）は、PLR でのバックアップトンネルの可用性に基づき、FRR 要件に従って動作し、バックアップトンネル選択情報をヘッドエンドにシグナリングします。FRR イ

ベントがトリガーされると、PLR はバックアップトンネルを介して PATH メッセージをバックアップトンネルが元の LSP に再参加するマージポイント（MP）に送信します。また、MP は PATH メッセージ内の PLR によって組み込まれた RSVP-Hop オブジェクトを使用して RESV メッセージを PLR に送信します。このプロセスにより、元の LSP が MP によって切断されることを防ぎます。また、PLR は PATH-ERROR メッセージを使用してトンネルヘッドエンドにシグナリングし、LSP に沿った障害と、その LSP で FRR がアクティブに使用されていることを示します。ヘッドエンドはこの情報を使用して、TE トンネルの新しい LSP をシグナリングし、メークビフォーブレーク技術によって新しい LSP がセットアップされた後に障害が発生した既存のパスを切断します。

RSVP-TE トンネル PCC および PCE 設定のソース

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

- パス計算クライアント（PCC）によって開始：PCC に設定された RSVP-TE トンネル（PCC によって開始された RSVP-TE トンネルの例 （8 ページ）を参照）。
- パス計算要素（PCE）または PCC が動的に開始。

PCC によって開始された RSVP-TE トンネルの例

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

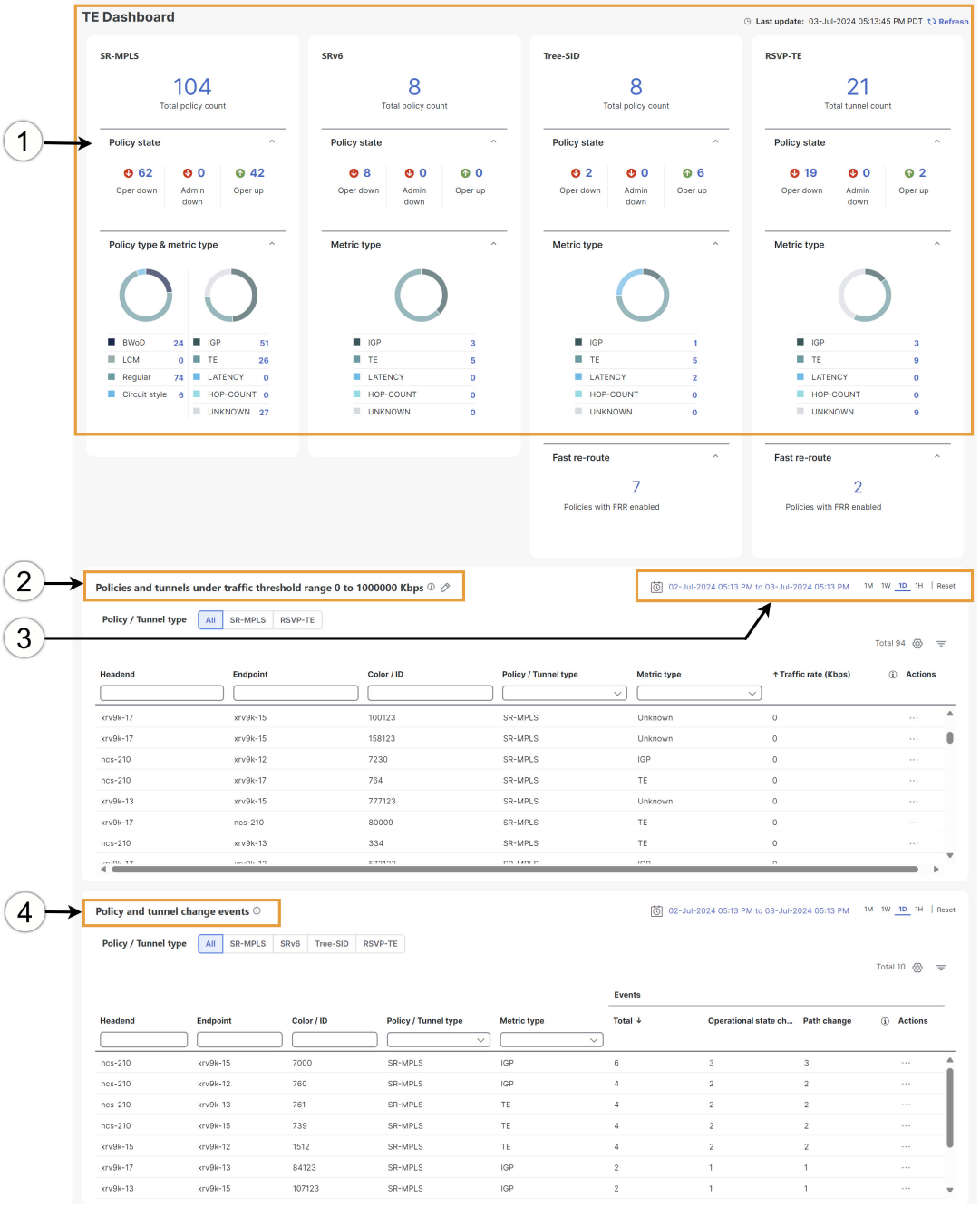
```
interface tunnel-te777
 ipv4 unnumbered Loopback0
 destination 192.168.0.8
 path-option 10 dynamic
 pce
  delegation
!
```

トラフィック エンジニアリング サービスのクイック ビューを取得する

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

TE ダッシュボードにアクセスするには、[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 サービスのクイックビュー



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

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

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

TE イベントと使用率履歴の表示

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

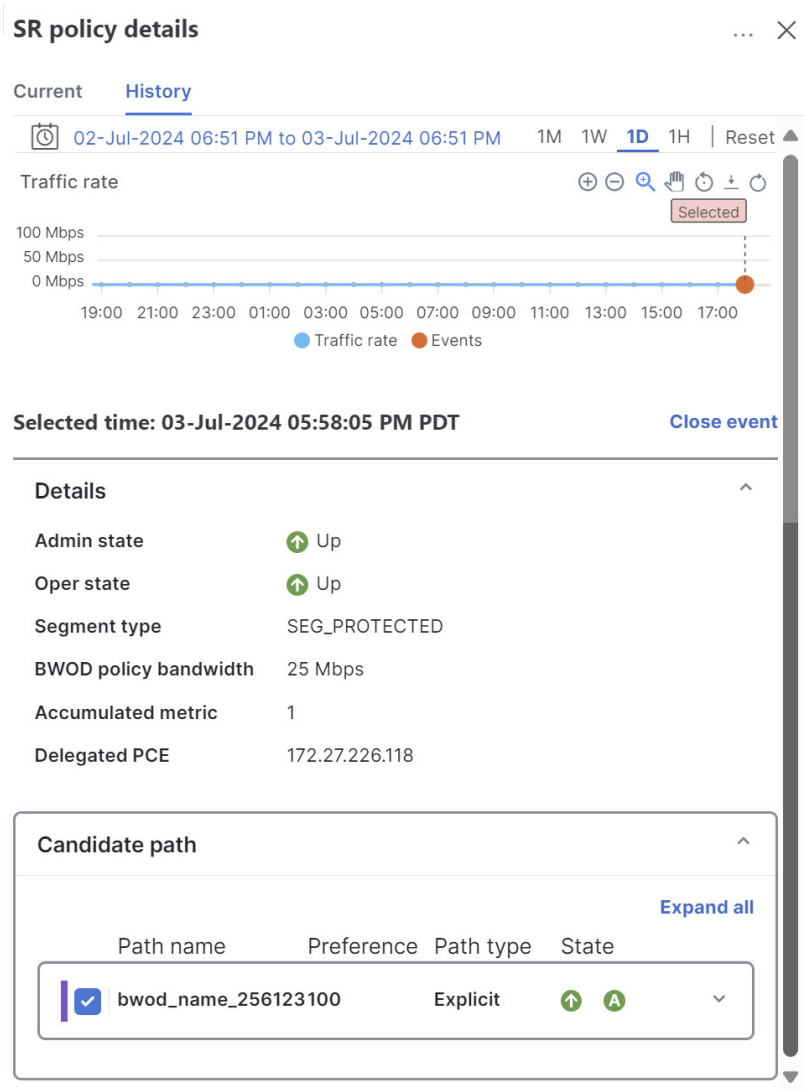
（注） SRv6 および Tree-SID ポリシーではトラフィックレートはキャプチャされません。

手順

ステップ 1 メインメニューから、**[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 [トラフィックエンジニアリング（Traffic Engineering）] テーブルの [アクション（Actions）] 列で、ポリシーまたはトンネルの … > [詳細の表示（View Details）] > [履歴（History）] タブをクリックします。タブには、そのデバイスの関連する履歴データが表示されます。イベントをクリックすると、パスまたは状態変更イベントの情報が表示されます。

図 *2 : TE* イベントと使用率履歴



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

トラフィック エンジニアリング デバイスの詳細の表示

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

手順

ステップ 1 メインメニューから、**[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。

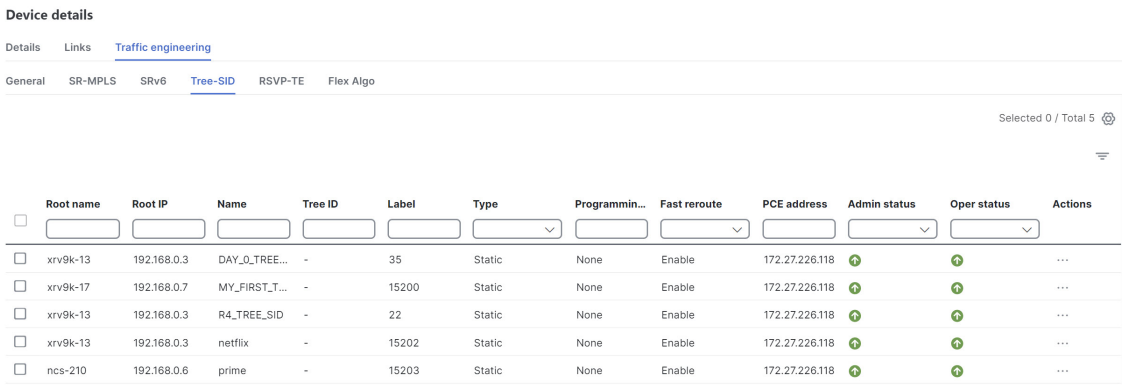
ステップ 2 トラフィック エンジニアリングのトポロジマップから、デバイスをクリックします。

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

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

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

図 *4:* トラフィック エンジニアリング デバイスの詳細



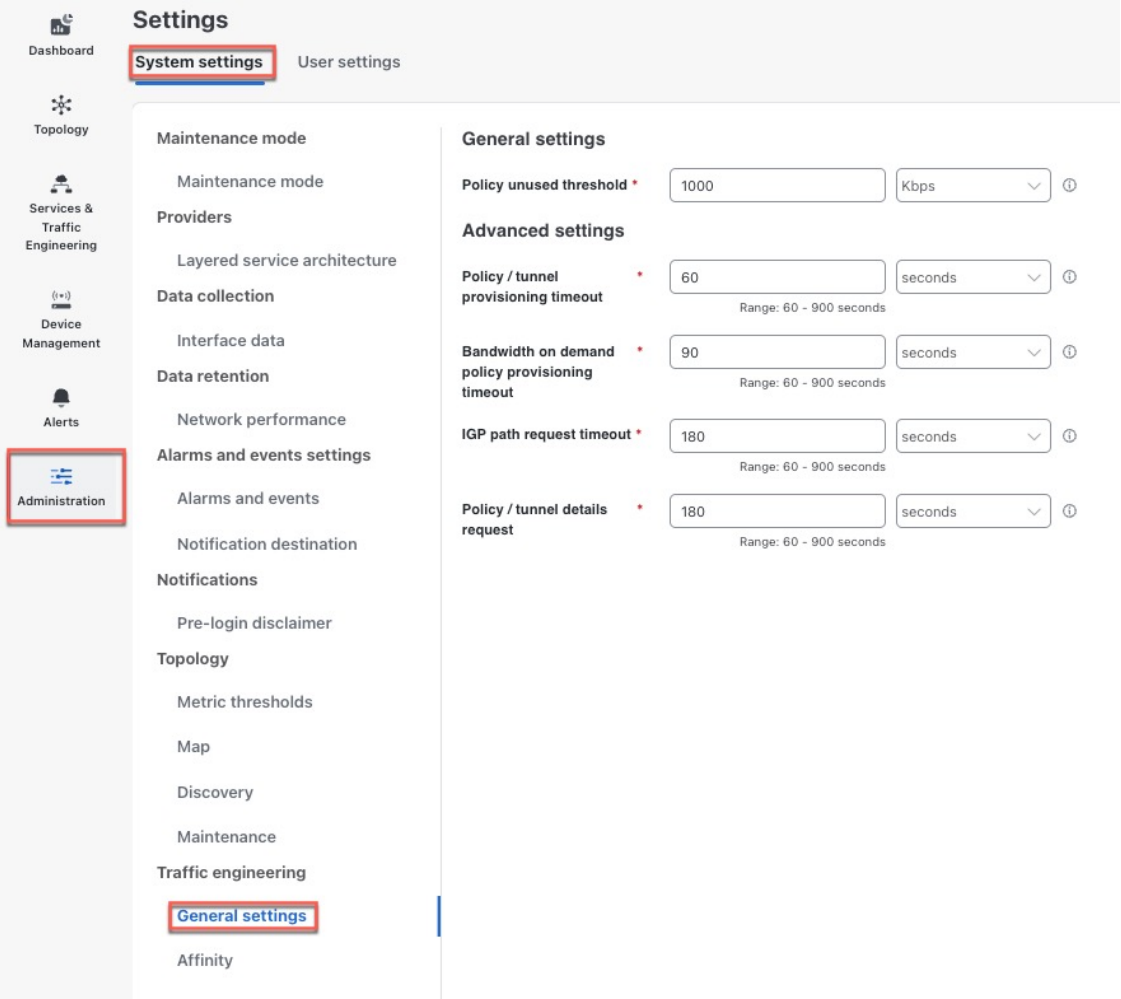
トラフィック エンジニアリング設定の構成

TE タイムアウトの設定

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

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

図 *5:* トラフィック エンジニアリング タイムアウトの設定



トラフィックエンジニアリング用のデバイスグループの表示方法の構成

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

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

TE データ保持設定の構成

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

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

SR-TE ポリシーと RSVP-TE トンネルの解決

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

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

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。