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

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
- 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 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 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」を参照してください。

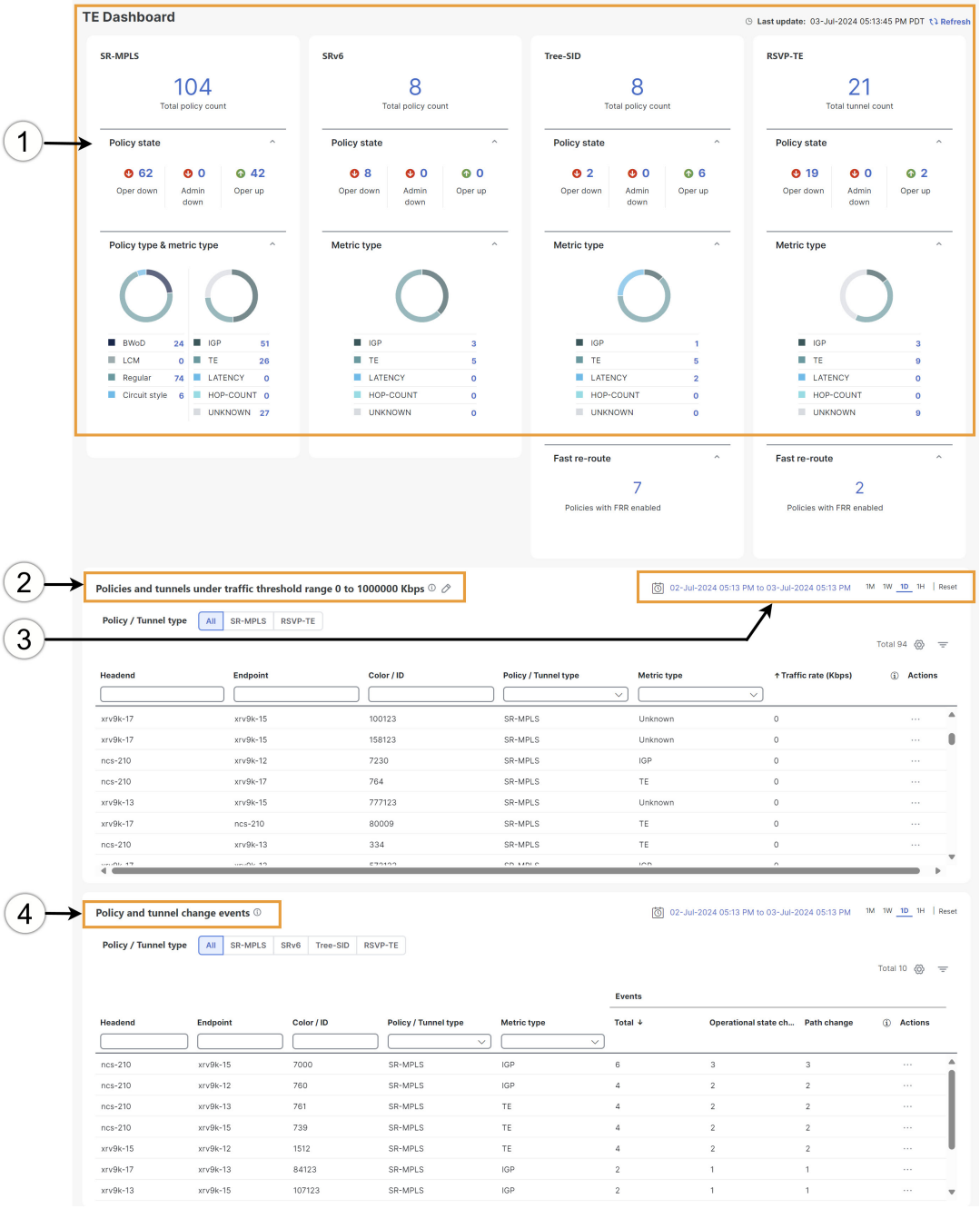
```
router isis CORE
 is-type level-2-only
 net 49.0001.0000.0000.0002.00
 log adjacency changes
 affinity-map b33 bit-position 33
 affinity-map red bit-position 1
 affinity-map blue bit-position 5
 flex-algo 128
  priority 228
  advertise-definition
  affinity exclude-any blue indigo violet black
 !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

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。

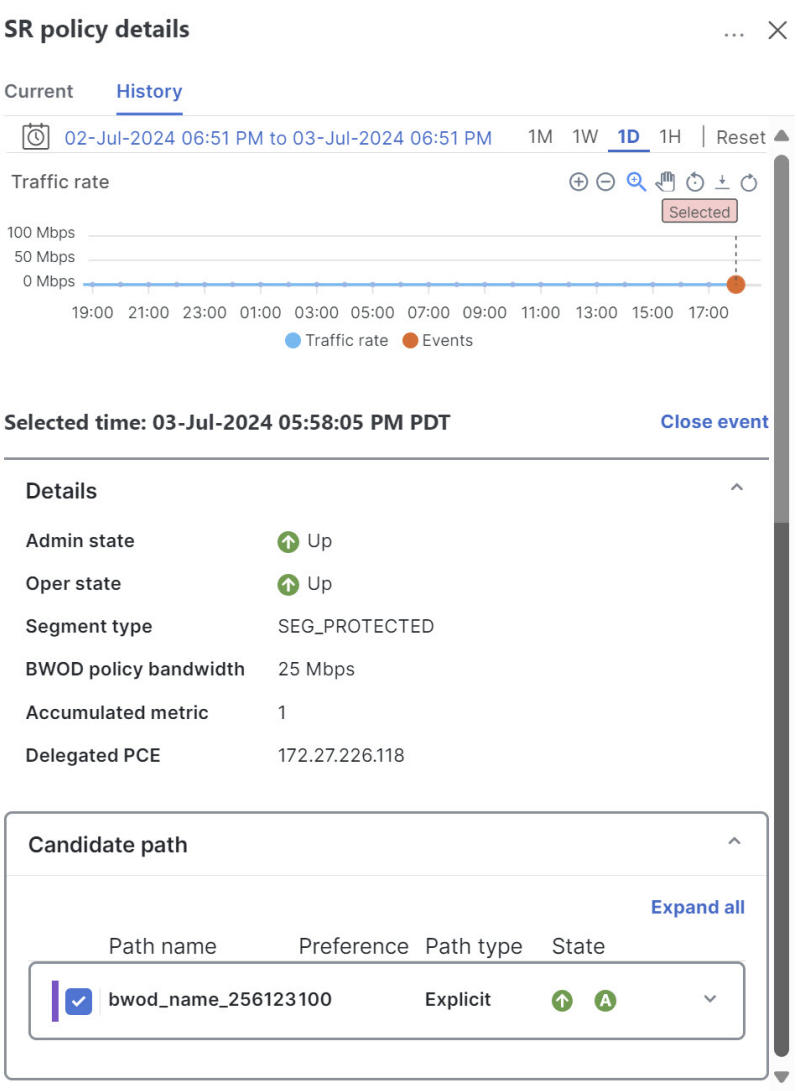
手順

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

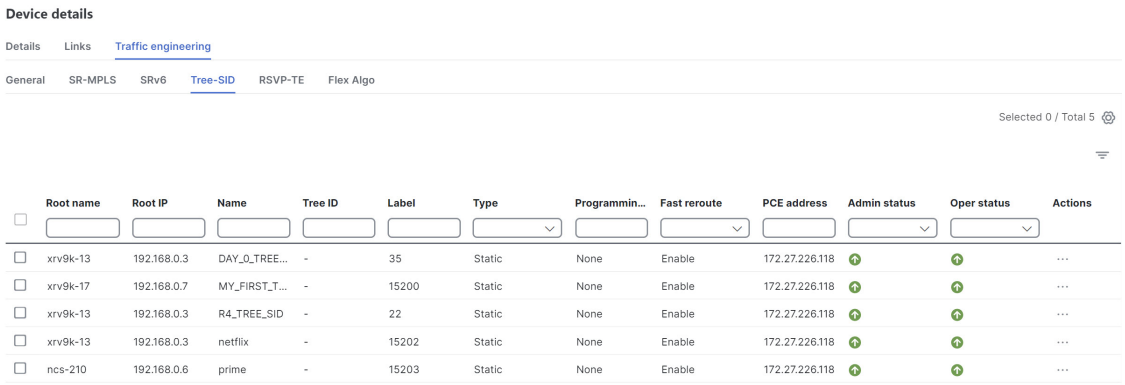
ステップ 1 **[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > > **[トラフィックエンジニアリング（Traffic Engineering）]** を選択します。

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。

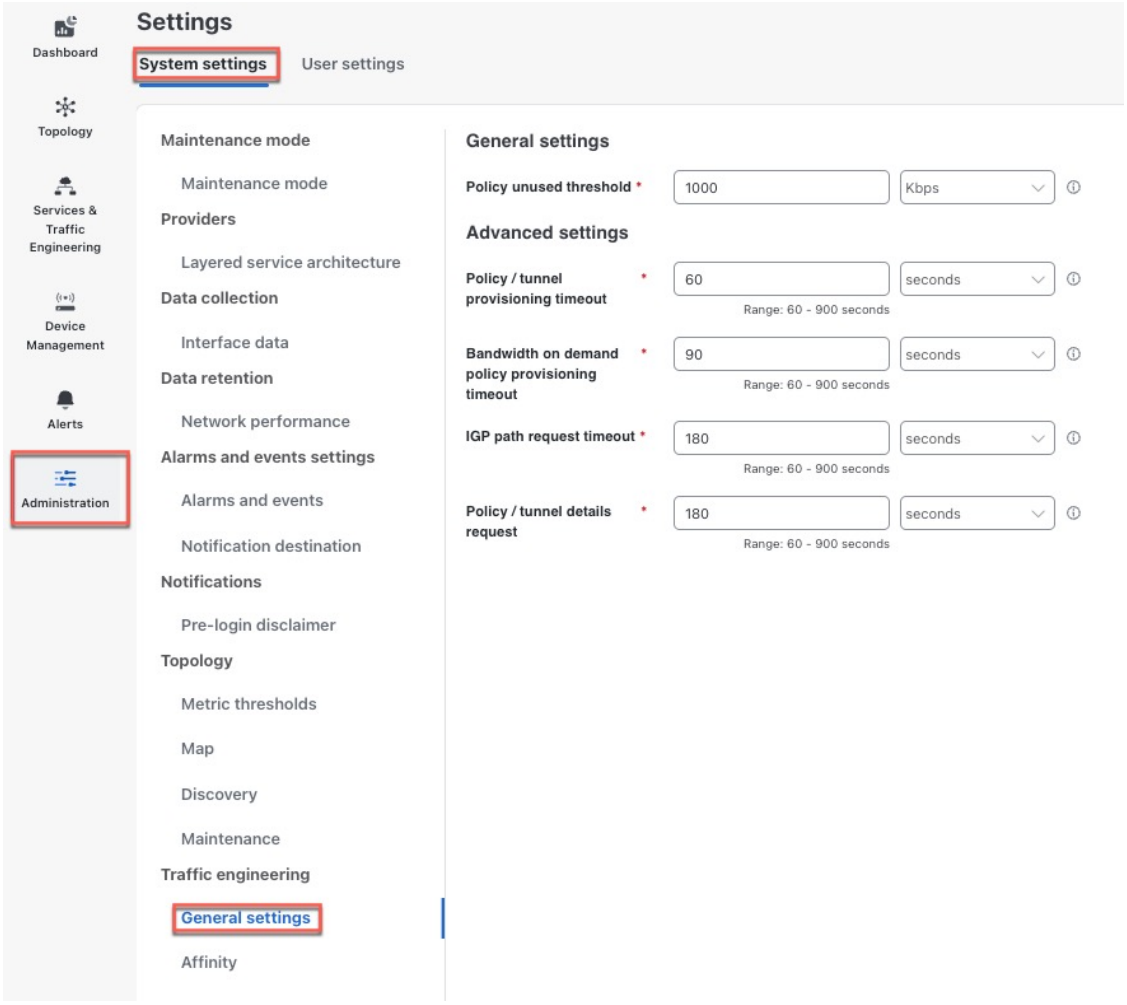
TE 設定の構成

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。

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。