



Cisco Crosswork Optimization Engine 2.0 ユーザガイド

初版：2021年4月19日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスココンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



目次

第 1 章	使用する前に	1
	対象読者	1
	Cisco Crosswork Optimization Engine の概要	2
	Crosswork Optimization Engine API	3
	Crosswork Optimization Engine と Crosswork Network Controller ソリューション	3
	セグメントルーティングパス計算要素 (SR-PCE)	3
	セグメントルーティングについて	4
	Resource Reservation Protocol (RSVP) について	6

第 2 章	ネットワークビューのセットアップとモニタ	9
	ダッシュボードでのクイックビューの取得	9
	トポロジマップでのデバイスとリンクの表示	11
	デバイスとリンクの詳細の表示	13
	デバイスグループを使用したトポロジビューのフィルタ処理	17
	デバイスグループの作成と変更	21
	ダイナミック デバイス グループの有効化	22
	マップ表示設定のカスタマイズ	23
	リンクとデバイスの表示のカスタマイズ	23
	TE トンネルのデバイスグループの表示動作の設定	23
	簡易アクセスのトポロジビューの保存	23

第 3 章	SR-TE ポリシーと RSVP-TE トンネルのモニタ	25
	トポロジマップでの SR-TE ポリシーと RSVP-TE トンネルの表示	25

SR-TE ポリシーと RSVP-TE トンネルの可視化の例 28

タイムアウトの設定 38

第 4 章

SR-TE ポリシーのプロビジョニング 39

SR-TE ポリシーのサポート 39

SR ポリシー設定のソース 41

 PCC によって開始された SR ポリシーの例 42

明示的 SR-TE ポリシーの作成 42

リンクアフィニティの設定 43

最適化インテントに基づくダイナミック SR-TE ポリシーの作成 44

SR-TE ポリシーの変更 45

第 5 章

RSVP-TE トンネルのプロビジョニング 47

RSVP-TE トンネルのサポート 47

RSVP-TE トンネル設定のソース 49

 PCC によって開始された RSVP-TE トンネルの例 49

明示的 RSVP-TE トンネルの作成 49

リンクアフィニティの設定 50

最適化インテントベースのダイナミック RSVP-TE トンネルの作成 51

RSVP-TE トンネルの変更 52

第 6 章

ネットワーク輻輳の緩和 55

LCM を使用したローカルでの輻輳の緩和 56

 LCM に関する特記事項 56

 LCM 計算のワークフロー 57

 ローカルインターフェイスでの輻輳の緩和の例 59

 LCM の設定 64

 LCM 動作のモニタ 65

BWOpt を使用したネットワークの最適化 65

 BWOpt に関する特記事項 65

 自動化されたネットワーク輻輳の緩和の例 66

帯域幅最適化の設定	69
帯域幅最適化のトラブルシューティング	70
個別のインターフェイスしきい値の追加	71

第 7 章

インテントベースの帯域幅要件の定義と維持	73
BWoD に関する特記事項	74
インテントベースの帯域幅の要件を維持するための SR-TE ポリシーのプロビジョニングの例	74
PCC によって開始された BWoD SR-TE のポリシー	76
オンデマンド帯域幅の設定	78
BWoD のトラブルシューティング	79



第 1 章

使用する前に

これは、Cisco Crosswork Optimization Engine を起動して実行し、ユーザインターフェイス (UI) の使用を開始するために必要な手順を説明する、インストール後のドキュメントです。デバイスとユーザ管理を含む管理タスクについては、『Cisco Crosswork Administrator's Guide』を参照してください。

- [対象読者 \(1 ページ\)](#)
- [Cisco Crosswork Optimization Engine の概要 \(2 ページ\)](#)
- [Crosswork Optimization Engine API \(3 ページ\)](#)
- [Crosswork Optimization Engine と Crosswork Network Controller ソリューション \(3 ページ\)](#)
- [セグメントルーティングパス計算要素 \(SR-PCE\) \(3 ページ\)](#)
- [セグメントルーティングについて \(4 ページ\)](#)
- [Resource Reservation Protocol \(RSVP\) について \(6 ページ\)](#)

対象読者

このガイドは、ネットワークで Cisco Crosswork Optimization Engine を使用する経験豊富なネットワーク管理者を対象としています。このガイドは、次のテクノロジーの使用経験と知識があることを前提としています。

- ネットワーキングテクノロジーとプロトコル (BGP-LS、IGP (OSPF と IS-IS)、PCEP、モデル駆動型テレメトリなど)
- トラフィック エンジニアリング (TE) トンネル
 - RSVP-TE トンネルのプロビジョニング
 - セグメントルーティング トラフィック エンジニアリング (SR-TE) ポリシーのプロビジョニング
- Cisco セグメントルーティングパス計算要素 (SR-PCE)

Cisco Crosswork Optimization Engine の概要

Crosswork Optimization Engine は、一連の Cisco Crosswork ネットワークの自動化の製品の一部であり、プロアクティブなネットワークモニタリング、ネットワークの可視化、およびクローズドループの自動化により、ネットワークインテントを維持する機能を提供します。また、リアルタイムのネットワーク最適化を通じて、オペレータがネットワーク容量の使用率を効果的に最大化し、サービス速度を高められるようにします。

Crosswork Optimization Engine は、次のとおりです。

- 次のような有益なリアルタイムのネットワーク可視化を実現するトポロジマップ
 - デバイス
 - リンクとリンク使用率
 - プロビジョニングされた SR-TE ポリシーと RSVP-TE トンネル
- ネットワークオペレータが次のタスクを実行できる UI
 - 直感的なワークフローを使用して SR-TE ポリシーと RSVP-TE トンネルをプロビジョニングし、それらを変更または削除する
 - SR-TE ポリシーまたは RSVP-TE トンネルをネットワークに展開する前にプレビューする
 - SR-TE ポリシーのダイナミックパスの計算を継続的に追跡し、SLA の目的を維持する（正しいライセンスを使用）
 - ネットワークデバイス上で直接作成された SR-TE ポリシーと RSVP-TE トンネルを可視化し、アクティブなネットワーク設定の包括的なビューを提供する
- 他の Crosswork アプリケーションやサードパーティアプリケーションまで Crosswork Optimization Engine の機能を拡張する API
- Crosswork Optimization Engine の機能パック（正しいライセンスで使用可能）は、輻輳緩和とクローズドループの帯域幅最適化を提供します。ユーザは最適化の目的を定義し、ツールはその目的を実現し、継続的にモニタ、追跡、対応して元の目的を維持します。

このガイドでは、Crosswork Optimization Engine で許可されるすべての機能を説明します。ただし、ライセンスまたはユーザアカウントに関連付けられたロールの設定のいずれかにより、すべての機能にアクセスできない場合があります。

ライセンスおよび発注情報については、『[Cisco Crosswork Optimization Engine Ordering Guide](#)』（シスコパートナーが入手可能）を参照するか、シスコの営業担当者にお問い合わせください。

Crosswork Optimization Engine API

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

詳細については、[Cisco DevNet の Cisco Crosswork Network Automation API ドキュメント](#)を参照してください。ライセンスと発注情報については、『[Cisco Crosswork Optimization Engine Ordering Guide](#)』（シスコパートナーが入手可能）を参照するか、またはシスコのセールス担当者にお問い合わせください。

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

Cisco Crosswork Network Controller は、IP トランスポートネットワークを展開および運用するためのターンキーネットワーク自動化ソリューションで、サービスの俊敏性、コスト効率、最適化の向上を実現し、お客様に届くまでの時間の迅速化して運用コストを削減します。このソリューションは、インテントベースのネットワーク自動化を組み合わせ、サービスのオーケストレーションと実現、ネットワークの最適化、サービスパスの計算、デバイスの展開と管理、および異常検出と自動修復のための重要な機能を提供します。詳細については、「[Cisco Crosswork Network Controller](#)」を参照してください。

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

セグメントルーティングパス計算要素 (SR-PCE)

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

Cisco SR-PCE (以前の Cisco XR Traffic Controller (XTC)) は、Cisco IOS XR オペレーティングシステムで実行します。SR-PCE は、ネットワークを最適化するために TE トンネルを制御および再ルーティングするのに役立つステートフル PCE 機能を提供します。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、制御を委任できる一連の手順を記述します。PCC および PCE は、更新をネットワークにプッシュするために SR-PCE が使用するパス計算要素通信プロトコル (PCEP) の接続を確立します。

Crosswork は、SR-PCE との PCEP ピアリングを確立しないデバイスを含む、IGP ドメインの一部であるすべてのデバイスを検出します。ただし、TE トンネルをデバイスに展開するには PCEP ピアリングが必要です。

セグメントルーティングについて

セグメントルーティングは、送信元のルーティングパラダイムに基づいてネットワーク上でパケットを転送する方法です。送信元はパスを選択し、パケットヘッダーでセグメントの番号付きリス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、フラットな 32 ビットの符号なし整数で構成されます。

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

セグメント

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

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

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

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

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

セグメントルーティングポリシー

SR ポリシーパスはパス (SID リスト) を指定するセグメントのリストとして表されます。番号付きリストでプレフィックス (ノード) と隣接関係セグメント ID を組み合わせることにより、ネットワーク内で任意のパスを構築できます。各ホップにおいて、先頭のセグメントがネクストホップを識別するために使用されます。セグメントはパケットヘッダーの先頭に順番にスタックされます。先頭のセグメントに別のノードの ID が含まれている場合、受信ノード

は等コストマルチパス (ECMP) を使用してパケットをネクストホップに移動させます。ID が受信ノードの ID である場合、ノードは先頭のセグメントをポップし、次のセグメントに必要なタスクを実行します。

SR ポリシーにはダイナミックと明示的の 2 つのタイプがあります。

ダイナミック SR ポリシー

動的パスは、最適化の目的と一連の制約に基づいています。ヘッドエンドはソリューションを計算し、結果として SID リストまたは SID リストのセットを生成します。トポロジが変更されると、新しいパスが計算されます。ヘッドエンドにトポロジに関する十分な情報がない場合、ヘッドエンドは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。各セグメントは、送信元から接続先までのエンドツーエンドのパスであり、ネットワーク内のルータに、IGP によって計算された最短パスではなく指定されたパスに従うように指示します。パケットが SR ポリシーへと誘導される場合、SID リストはヘッドエンドによってパケットにプッシュされます。残りのネットワークは、SID リストに埋め込まれた命令を実行します。

トラフィックエンジニアリング用のセグメントルーティング

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

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

分離

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

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



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

関連リンク

[SR-TE ポリシーのプロビジョニング \(39 ページ\)](#)

[リンクアフィニティの設定 \(43 ページ\)](#)

Resource Reservation Protocol (RSVP) について

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

RSVP-TE プロセスには、次の機能が含まれています。

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

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

RSVP-TE 明示的ルーティング (ストリクト、ルーズ)

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

ERO で指定された明示的パスは、ストリクトパスまたはルーズパスです。

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

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

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



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

RSVP FRR

ルータのリンクまたは隣接デバイスに障害が発生すると、インターフェイス停止の通知を受信することでルータはこの障害を検出する場合があります。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LSPを、それぞれのバックアップトンネルに切り替えます（バックアップトンネルがある場合）。

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

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

FRR要件のシグナリングは、TEトンネルヘッドエンドで開始されます。パスに沿ったローカル修復ポイント (PLR) は、PLRでのバックアップトンネルの可用性に基づき、FRR要件に従って動作し、バックアップトンネル選択情報をヘッドエンドにシグナリングします。FRRイベントがトリガーされると、PLRはバックアップトンネルを介してPATHメッセージをバックアップトンネルが元のLSPに再参加するマージポイント (MP) に送信します。また、MPはPATHメッセージ内のPLRによって組み込まれたRSVP-Hopオブジェクトを使用してRESVメッセージをPLRに送信します。このプロセスにより、元のLSPがMPによって切断されることを防ぎます。また、PLRはPATH-ERRORメッセージを使用してトンネルヘッドエンドにシグナリングし、LSPに沿った障害と、そのLSPでFRRがアクティブに使用されていることを示します。この情報はヘッドエンドで使用され、TEトンネルの新しいLSPをシグナリングし、メイクビフォアブレイク技術によって新しいLSPがセットアップされた後に障害が発生した既存のパスを切断します。



第 2 章

ネットワークビューのセットアップとモニタ

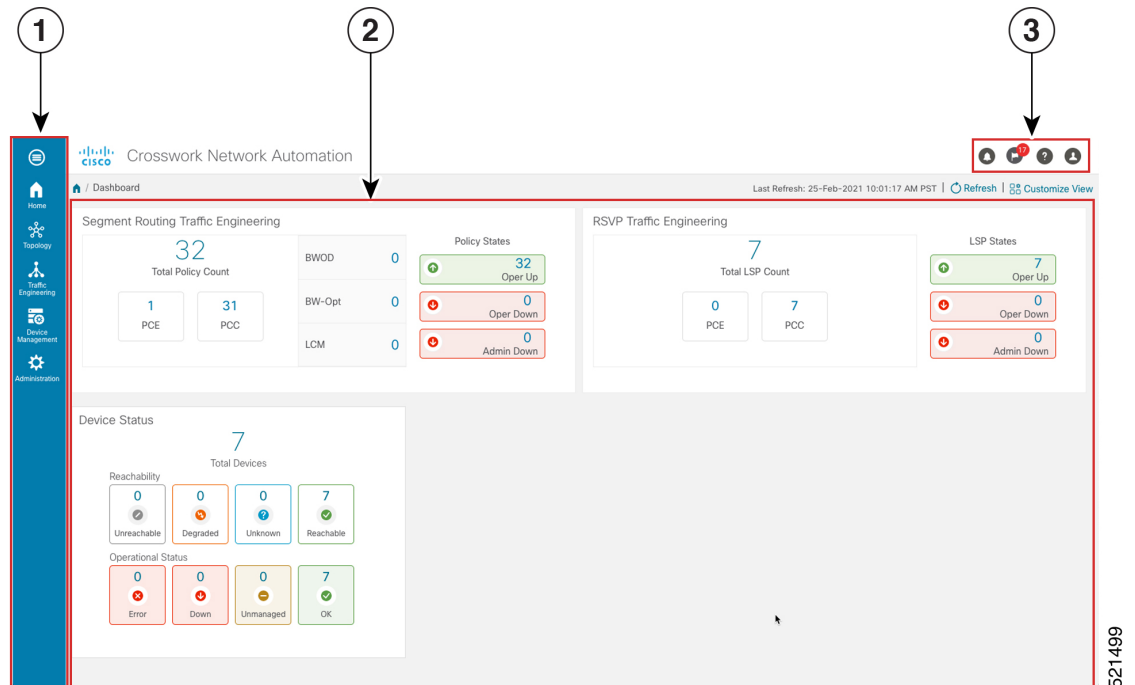
SR ポリシーと RSVP-TE トンネルを管理する前に、UI をよく理解して、ネットワークビューを設定します。ここでは、次の内容について説明します。

- [ダッシュボードでのクイックビューの取得 \(9 ページ\)](#)
- [トポロジマップでのデバイスとリンクの表示 \(11 ページ\)](#)
- [デバイスグループを使用したトポロジビューのフィルタ処理 \(17 ページ\)](#)
- [マップ表示設定のカスタマイズ \(23 ページ\)](#)
- [簡易アクセスのトポロジビューの保存 \(23 ページ\)](#)

ダッシュボードでのクイックビューの取得





[ホーム (Home)]ページにはダッシュボードが表示され、デバイスの到達可能性や動作ステータスなど、管理対象のネットワークの運用がひと目で分かる概要が表示されます。各ダッシュレットには、同じカテゴリに属しているさまざまなタイプのデータが表示されます。

図 1: Crosswork のホームページ



521499

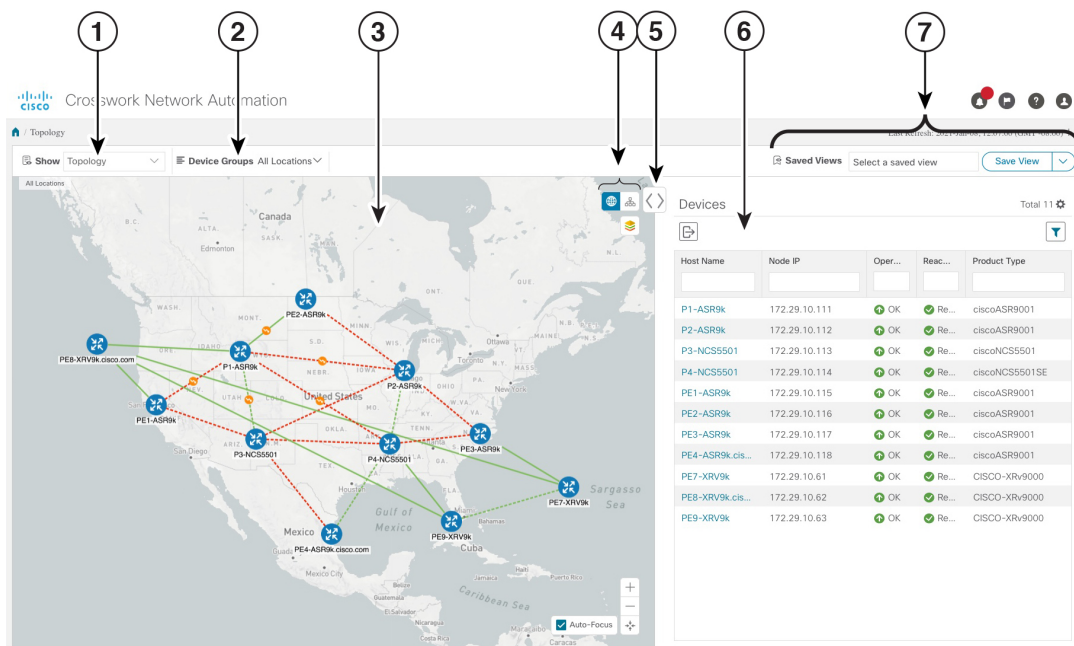
引き出し線番号	説明
1	<p>メインメニュー：メインメニューでは、インストールされている Cisco Crosswork アプリケーションと、デバイス管理および管理のタスクに移動できます。メニューオプションは、インストールされている Cisco Crosswork アプリケーションによって若干異なる場合があります。</p>
2	<p>ダッシュレット：情報は、インストールされている Cisco Crosswork アプリケーションによって異なります。</p> <ul style="list-style-type: none"> ダッシュレット内の詳細情報をドリルダウンするには、値をクリックします。クリックしたフィルタ処理済みデータのみを表示するウィンドウが表示されます。 ダッシュレットのレイアウトを追加または変更するには、[ビューのカスタマイズ (Customize View)] をクリックします。ダッシュレットを目的のレイアウトに移動し、[保存 (Save)] をクリックします。

引き出し線番号	説明
3	<p>設定のアイコン：</p> <ul style="list-style-type: none">  [アラート (Alerts)]アイコンは、注意が必要なシステム操作に関連する現在のエラー状態を通知し、それらの状態に関する詳細情報へのリンクを提供します。  [イベント (Events)]アイコンは、システム操作に関連する新しいイベントを通知し、すべてのシステムイベントの履歴にアクセスできるようにします。  [バージョン情報 (About)]アイコンには、Cisco Crosswork 製品の現在のバージョンが表示されます。  [ユーザアカウント (User Account)]アイコンを使用すると、ユーザ名の表示、パスワードの変更、ログアウトを行えます。

トポロジマップでのデバイスとリンクの表示

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

図 2 : Cisco Crosswork UI とトポロジマップ



455223

引き出し線番号	説明
1	<p>[トポロジマップビュー (Topology Map View)] : [表示 (Show)] ドロップダウンリストから、マップに表示するデータを表示するオプションをクリックします。</p> <p>[トポロジ (Topology)] を選択すると、ネットワーク内のデバイスとリンクが表示されます。</p> <p>[トラフィック エンジニアリング (Traffic Engineering)] を選択すると、TE トンネル情報が表示されます。</p>
2	<p>[デバイスグループ (Device Groups)] : ドロップダウンリストから、トポロジマップに重点を置くデバイスのグループをクリックします。他のすべてのデバイスグループは非表示になります。</p>
3	<p>[トポロジマップ (Topology Map)] : ネットワークトポロジは、論理マップまたは地理的マップに表示できます。ここでは、デバイスとリンクが地理的コンテキストで表示されます。マップでドリルダウンすると、デバイスとリンクに関する詳細を確認できます。</p> <p>[デバイス (Device)] :</p> <ul style="list-style-type: none"> • デバイス設定の概要を表示するには、マウスカーソルをデバイスアイコンの上に合わせます。ホスト名、状態、ノードID、およびデバイスタイプを表示するポップアップウィンドウが表示されます。 • デバイスの詳細を表示するには、デバイスアイコンをクリックします。 • デバイスが物理的に近接している場合、地理的なマップはそれらをクラスタとして表示します。青色の円内の番号 (2) は、クラスタ内のデバイスの数を示します。この方法でデバイスを表示すると、マップ上での重複や混乱を防ぐことができます。 <p>[リンク (Link)] :</p> <ul style="list-style-type: none"> • 実線は、2つのデバイス間の単一リンクを示します。2つのデバイス間、またはデバイスとデバイスのクラスタの間に複数のリンクがある場合は、代わりに線は点線で表示されます。破線は、複数のリンクを表す集約リンクか、または同じ物理リンクでの複数のプロトコル (IPv4やIPv6など) の使用を示します。 • リンク情報の詳細を表示するには、リンクをクリックします。

引き出し線番号	説明
4	<p>⏏️ : 論理マップは、自動レイアウトアルゴリズムに従って配置されたデバイスとそれらのリンクを示し、地理的な位置は無視されます。レイアウトアルゴリズムを変更できます。</p> <p>🌐 : 地理的マップは、単一のデバイス、デバイスクラスタ、リンク、およびトンネルを世界地図に重ねて表示します。マップ上の各デバイスの位置は、デバイスインベントリで定義されているデバイスの GPS 座標（経度と緯度）を反映します。</p> <p>🎛️ : [表示設定 (Display Preferences)] ウィンドウでは、デバイス、リンク、使用率、および TE トンネルメトリックの表示設定を変更できます。</p>
5	[サイドパネルの展開/折りたたみ/非表示 (Expand/Collapse/Hide Side Panel)] : サイドパネルの内容を展開するか、または折りたたみます。トポロジマップを拡大表示するには、サイドパネルを閉じます。
6	このウィンドウの内容は、トポロジマップの [表示 (Show)] に設定されている内容と、デバイス、リンク、SR-TE ポリシー、または RSVP-TE トンネルの詳細情報を表示するように選択したかどうかによって異なります。
7	[保存済みカスタムマップビュー (Saved Custom Map Views)] : 現在のマップの設定とレイアウト、保存済みビューに保存されているテーブルの設定を使用して名前付きカスタムビューを作成したり、以前に作成したカスタムビューを表示できます。また、[デバイス (Devices)] テーブルと [トラフィック エンジニアリング (Traffic Engineering)] テーブルに適用されるフィルタもすべて保存されます。

デバイスとリンクの詳細の表示

次に、トポロジマップを使用してデバイスとリンクの詳細を表示する例を示します。

ステップ 1 メインメニューから、[トポロジ (Topology)] を選択します。

デバイスとリンクの詳細の表示

The screenshot displays a network topology map on the left and a 'Devices' table on the right. The map shows various nodes connected by lines, representing a network across North America. The 'Devices' table lists the following information:

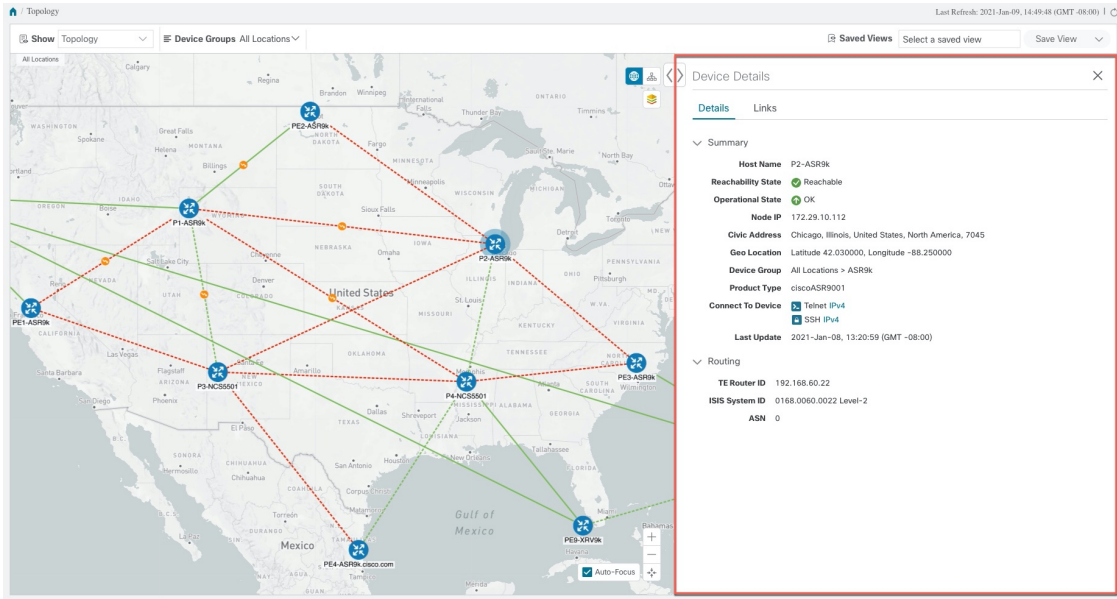
Host Name	Node IP	Oper...	Reac...	Product Type
P1-ASR9k	172.29.10.111	OK	Re...	ciscoASR9001
P2-ASR9k	172.29.10.112	OK	Re...	ciscoASR9001
P3-NCS5501	172.29.10.113	OK	Re...	ciscoNCS5501
P4-NCS5501	172.29.10.114	OK	Re...	ciscoNCS5501SE
PE1-ASR9k	172.29.10.115	OK	Re...	ciscoASR9001
PE2-ASR9k	172.29.10.116	OK	Re...	ciscoASR9001
PE3-ASR9k	172.29.10.117	OK	Re...	ciscoASR9001
PE4-ASR9k.cis...	172.29.10.118	OK	Re...	ciscoASR9001
PE7-XRV9k	172.29.10.61	OK	Re...	CISCO-XRV9000
PE8-XRV9k.cis...	172.29.10.62	OK	Re...	CISCO-XRV9000
PE9-XRV9k	172.29.10.63	OK	Re...	CISCO-XRV9000

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

The screenshot shows the same network topology map as in the previous image. A tooltip is displayed over the device icon for P2-ASR9k, providing the following details:

Reachability State	
Reachability State	Reachable
Host Name	P2-ASR9k
Node IP	172.29.10.112
Type	ciscoASR9001

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



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

図 3: 複数の IGP : OSPF プロセス

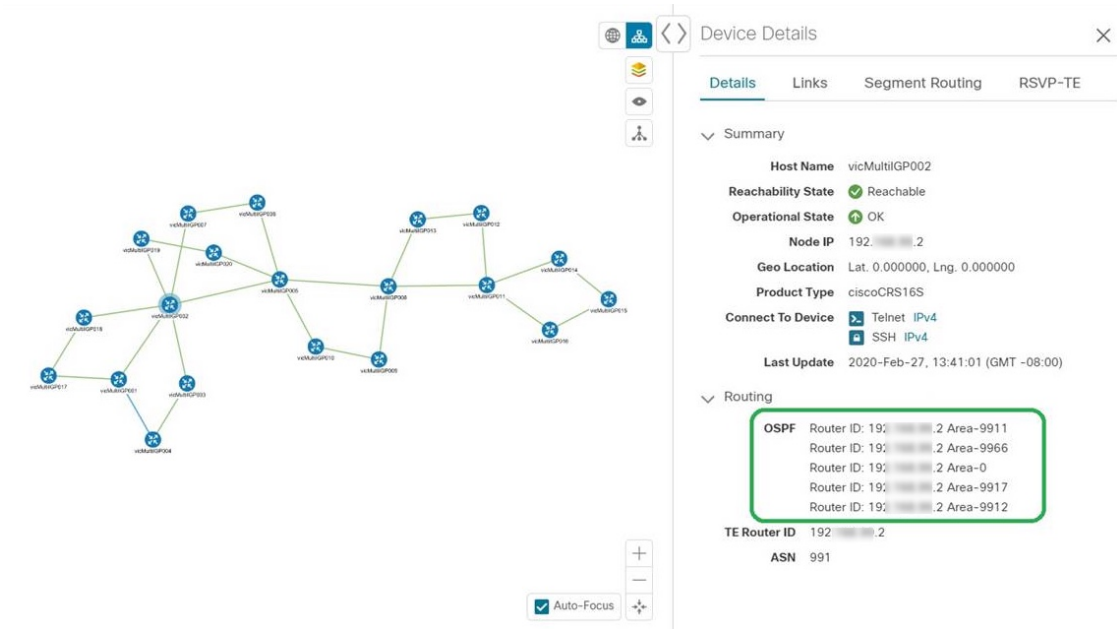


図 4: 複数の IGP : ISIS プロセス

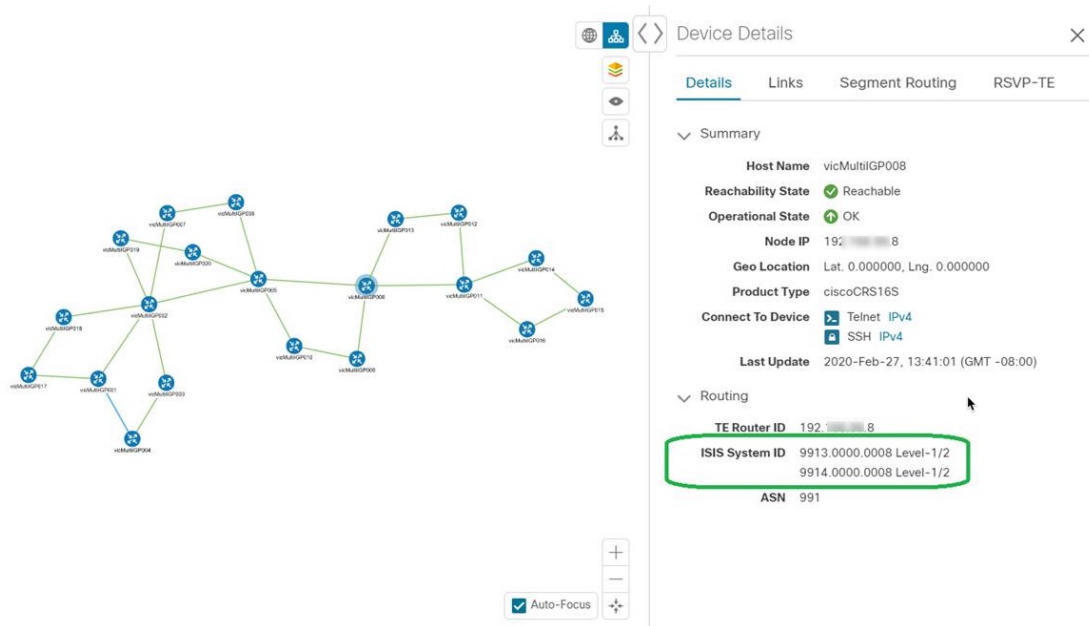


Figure 4 shows a network diagram with multiple devices (vMultiGP001 to vMultiGP019) connected in a mesh topology. The right panel displays the 'Device Details' for a specific device, with the 'Routing' section expanded to show the following configuration:

Category	Value
Host Name	vicMultiGP008
Reachability State	Reachable
Operational State	OK
Node IP	192.168.1.8
Geo Location	Lat. 0.000000, Lng. 0.000000
Product Type	ciscoCRS16S
Connect To Device	Telnet IPv4, SSH IPv4
Last Update	2020-Feb-27, 13:41:01 (GMT -08:00)
TE Router ID	192.168.1.8
ISIS System ID	9913.0000.0008 Level-1/2, 9914.0000.0008 Level-1/2
ASN	991

図 5: 複数の IGP : OSPF および ISIS プロセス

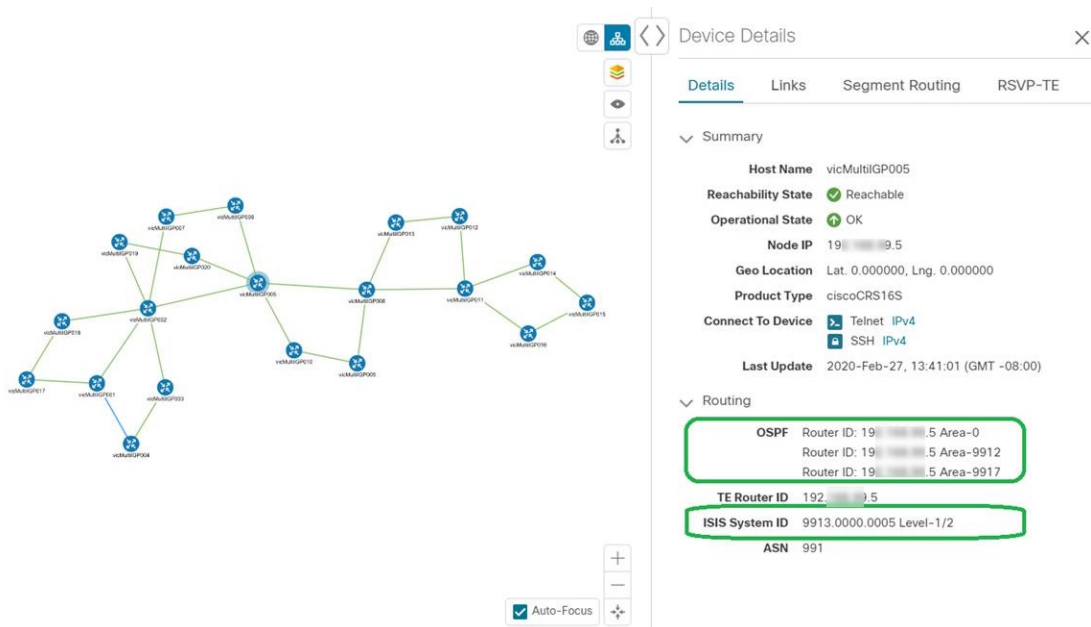


Figure 5 shows a network diagram with multiple devices (vMultiGP001 to vMultiGP019) connected in a mesh topology. The right panel displays the 'Device Details' for a specific device, with the 'Routing' section expanded to show the following configuration:

Category	Value
Host Name	vicMultiGP005
Reachability State	Reachable
Operational State	OK
Node IP	192.168.1.5
Geo Location	Lat. 0.000000, Lng. 0.000000
Product Type	ciscoCRS16S
Connect To Device	Telnet IPv4, SSH IPv4
Last Update	2020-Feb-27, 13:41:01 (GMT -08:00)
OSPF	Router ID: 192.168.1.5 Area-0, 192.168.1.5 Area-9912, 192.168.1.5 Area-9917
TE Router ID	192.168.1.5
ISIS System ID	9913.0000.0005 Level-1/2
ASN	991

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

Links on Device P2-ASR9k

Total 14

State	Link Type	A Side Interface	Z Side Interface	A Side Utilization	Z Side Utilization
🟢	L3 ISIS IPV4	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/3	0% (0Bps/1Gbps)	15.35% (153.5Mbps/1Gbps)
🟢	L2 LLDP	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/3	0% (0Bps/1Gbps)	15.35% (153.5Mbps/1Gbps)
🟢	L3 ISIS IPV4	GigabitEthernet0/0/0/4	GigabitEthernet0/0/0/2	20.34% (203.4Mbps/1Gbps)	0% (0Bps/1Gbps)
🟢	L2 LLDP	GigabitEthernet0/0/0/4	GigabitEthernet0/0/0/2	20.34% (203.4Mbps/1Gbps)	0% (0Bps/1Gbps)
🟢	L2 CDP	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/3	0% (0Bps/1Gbps)	22.39% (223.9Mbps/1Gbps)
🟢	L3 ISIS IPV4	GigabitEthernet0/0/0/3	GigabitEthernet0/0/0/7	8.14% (81.4Mbps/1Gbps)	0% (0Bps/1Gbps)
🟢	L2 LLDP	GigabitEthernet0/0/0/3	GigabitEthernet0/0/0/7	8.14% (81.4Mbps/1Gbps)	0% (0Bps/1Gbps)
🟡	L2 LLDP	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/3	0% (0Bps/1Gbps)	22.39% (223.9Mbps/1Gbps)
🟢	L3 ISIS IPV4	GigabitEthernet0/0/0/5	GigabitEthernet0/0/0/6	0% (0Bps/1Gbps)	0% (0Bps/1Gbps)
🟢	L2 CDP	GigabitEthernet0/0/0/5	GigabitEthernet0/0/0/6	0% (0Bps/1Gbps)	0% (0Bps/1Gbps)
🟢	L3 ISIS IPV4	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/4	0% (0Bps/1Gbps)	7.33% (73.3Mbps/1Gbps)
🟢	L2 LLDP	GigabitEthernet0/0/0/5	GigabitEthernet0/0/0/6	0% (0Bps/1Gbps)	0% (0Bps/1Gbps)
🟡	L2 LLDP	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/4	0% (0Bps/1Gbps)	7.33% (73.3Mbps/1Gbps)
🟢	L3 ISIS IPV4	Bundle-Ether9	Bundle-Ether9	0% (0Bps/1Gbps)	22.39% (223.9Mbps/1Gbps)

ステップ5 サイドパネルを折りたたんで、[デバイスの詳細 (Device Details)] ウィンドウを閉じます。

ステップ6 破線をクリックします。破線は、複数のリンクを表す集約リンクか、または同じ物理リンク上の複数のプロトコル (IPv4 や IPv6 など) の使用を示します。リンクが表示されます。

Links

Total 2

State	Link Type	A Side Interf...	Z Side Interf...	A Side Utiliz...	Z Side Utiliz...
🟢	L2 LLDP	GigabitEthem...	GigabitEthem...	8.14% (81.4...	0% (0Bps/1...
🟢	L3 ISIS IPV4	GigabitEthem...	GigabitEthem...	8.14% (81.4...	0% (0Bps/1...

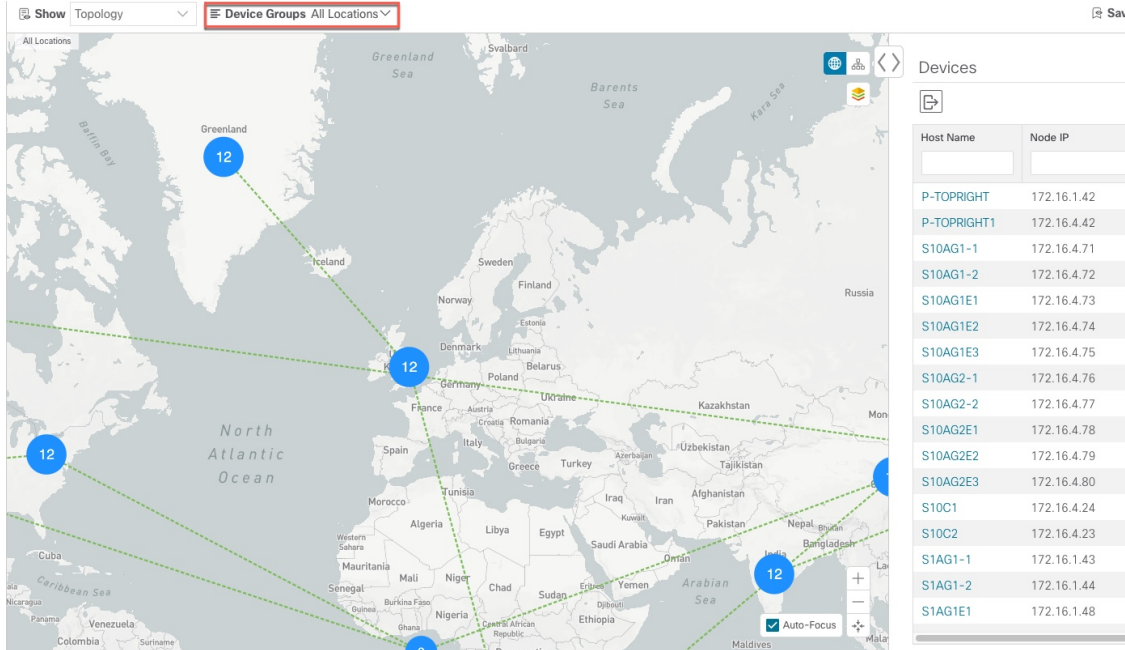
デバイスグループを使用したトポロジビューのフィルタ処理

さまざまな目的でデバイスを識別、検索、およびグループ化するためにデバイスグループを作成できます。[デバイスグループ (Device Group)] ウィンドウ ([デバイス管理 (Device

Management]>[**グループ (Groups)**]には、すべてのデバイスとそれらが属するデバイスグループが表示されます。デフォルトでは、すべてのデバイスが最初は [未割り当てデバイス (Unassigned Devices)]グループに表示されます。

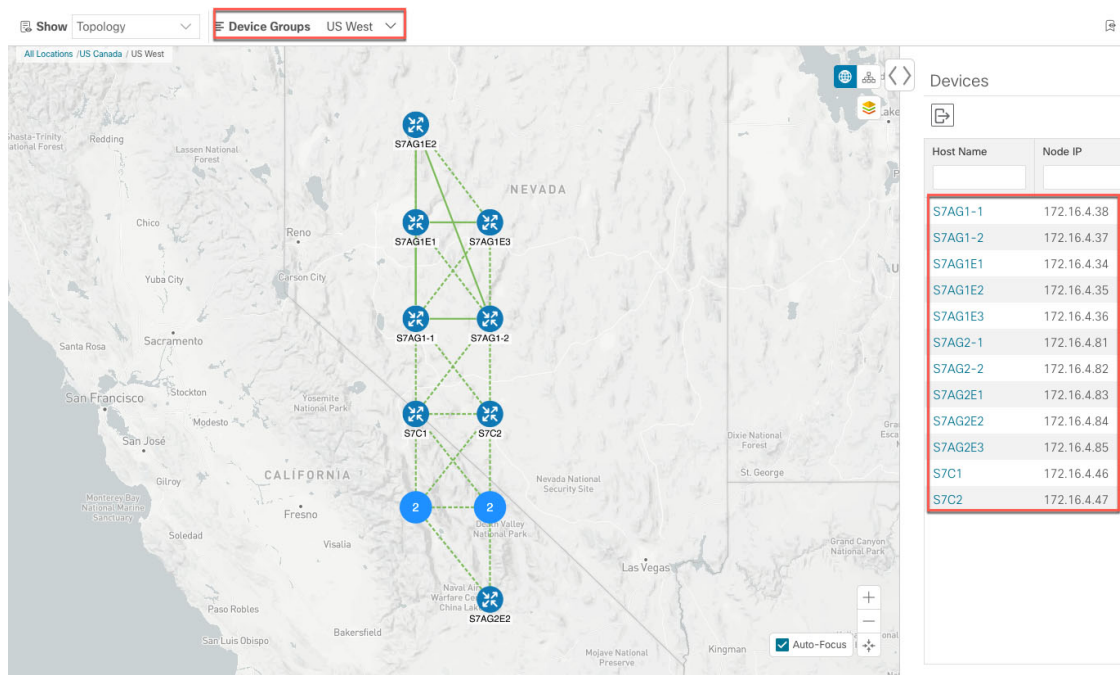
この例では、地理的マップと論理マップでのデバイスのグループ化の仕組みを説明します。

ステップ1 メインメニューから、[トポロジ (Topology)]を選択します。デフォルトでは、地理的な位置が設定されているデバイスのみが地理的マップに表示されます。




Host Name	Node IP
P-TOPRIGHT	172.16.1.42
P-TOPRIGHT1	172.16.4.42
S10AG1-1	172.16.4.71
S10AG1-2	172.16.4.72
S10AG1E1	172.16.4.73
S10AG1E2	172.16.4.74
S10AG1E3	172.16.4.75
S10AG2-1	172.16.4.76
S10AG2-2	172.16.4.77
S10AG2E1	172.16.4.78
S10AG2E2	172.16.4.79
S10AG2E3	172.16.4.80
S10C1	172.16.4.24
S10C2	172.16.4.23
SIAG1-1	172.16.1.43
SIAG1-2	172.16.1.44
SIAG1E1	172.16.1.48

ステップ2 [デバイスグループ (Device Group)]ドロップダウンリストからグループ (米国西部) を選択します。そのグループ内のデバイスと関連リンクのみが地理的マップに表示されます。[デバイス (Devices)]テーブルもフィルタ処理され、グループ内のデバイスのみが表示されることに注意してください。



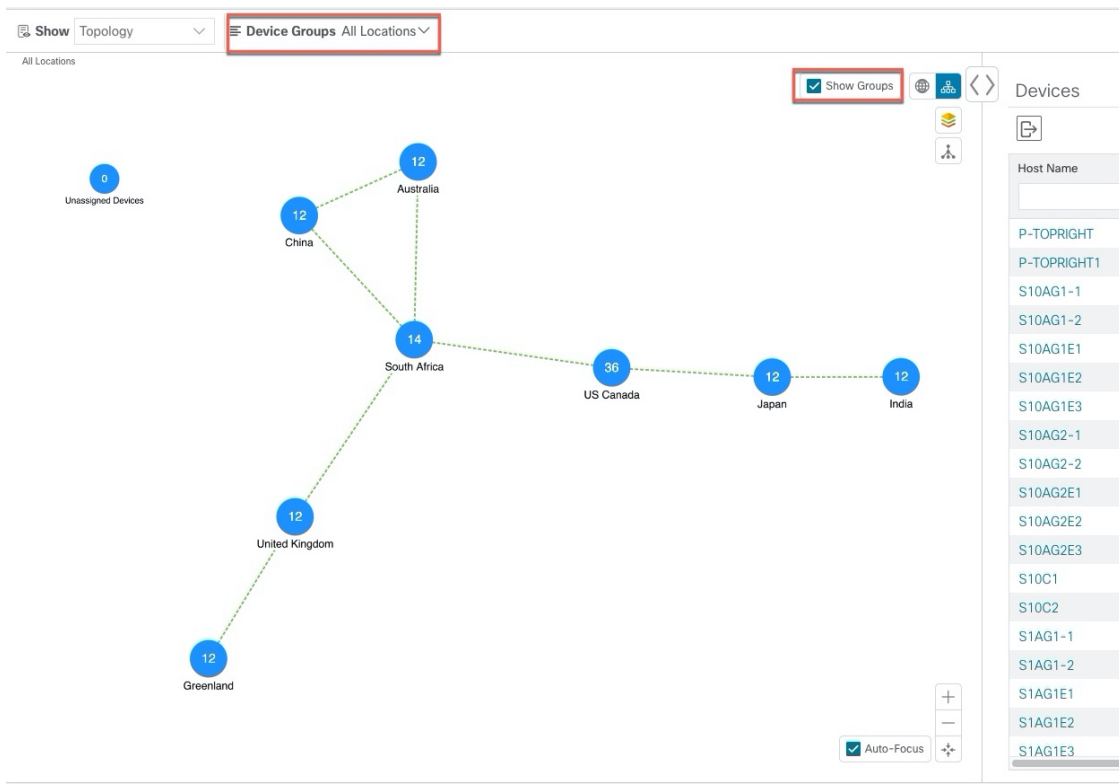
Host Name	Node IP
S7AG1-1	172.16.4.38
S7AG1-2	172.16.4.37
S7AG1E1	172.16.4.34
S7AG1E2	172.16.4.35
S7AG1E3	172.16.4.36
S7AG2-1	172.16.4.81
S7AG2-2	172.16.4.82
S7AG2E1	172.16.4.83
S7AG2E2	172.16.4.84
S7AG2E3	172.16.4.85
S7C1	172.16.4.46
S7C2	172.16.4.47

ステップ 3  をクリックします。

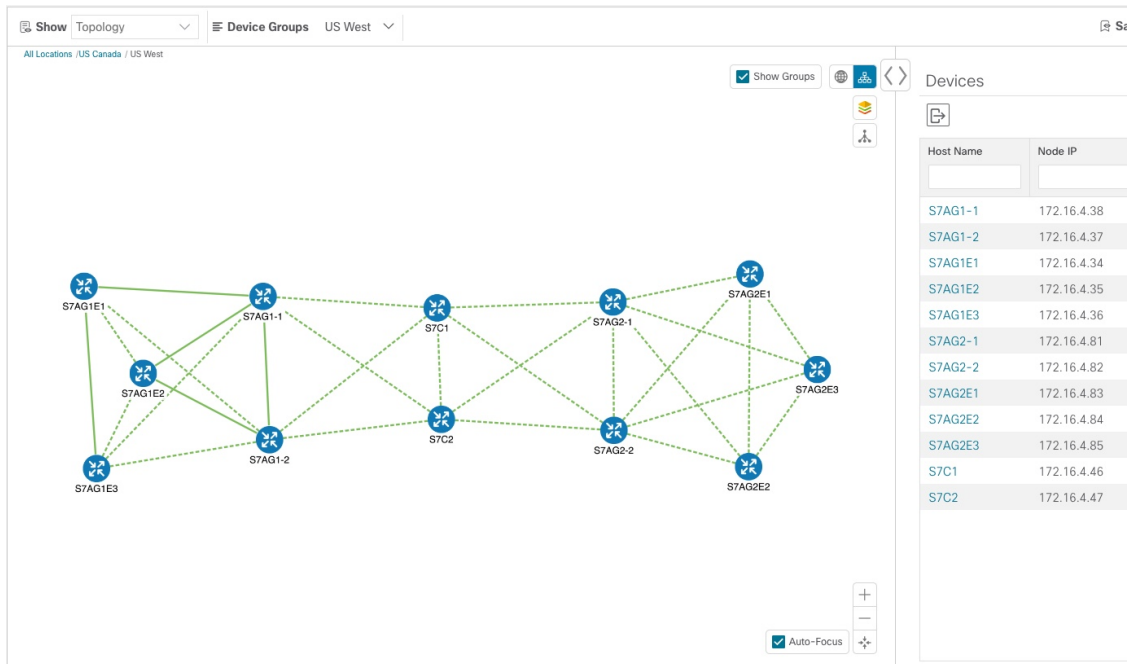
ステップ 4 [デバイスグループ (Device Group)] ドロップダウンリストから [すべての場所 (All Locations)] を選択し、[グループの表示 (Show Groups)] がオンになっていない場合はオンにします。このビューでは、すべてのデバイスグループを表示できます。デバイスグループは、論理マップ内でのみこの方法で表示できません。

(注) [グループの表示 (Show Groups)] チェックボックスをオフにすると、すべてのデバイスグループが展開され、マップが乱雑になる可能性があります。

デバイスグループを使用したトポロジビューのフィルタ処理

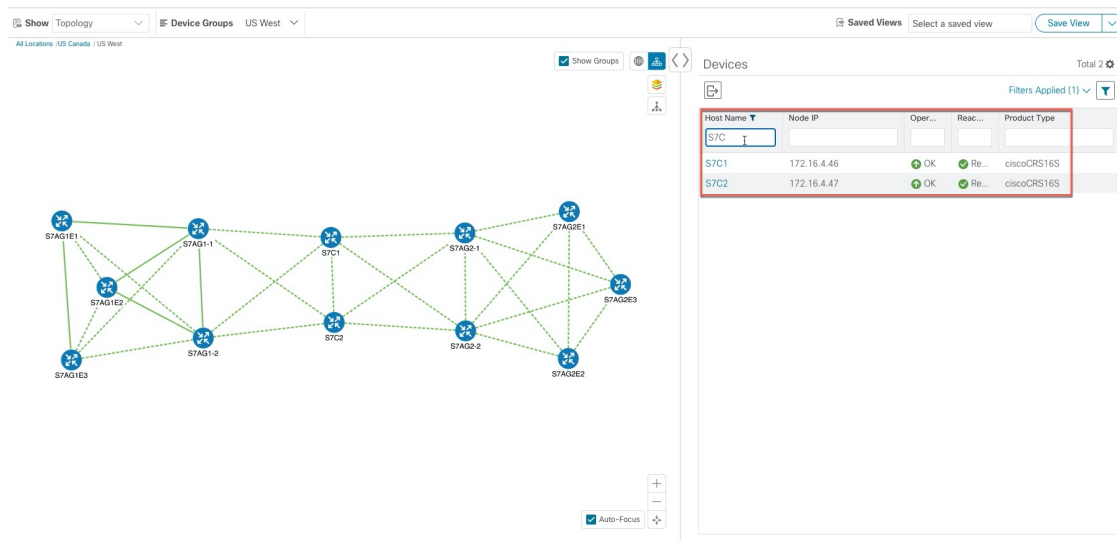


ステップ 5 [米国西部 (US West)] グループをクリックします。この場合も、このグループに属するデバイスのみがトポロジマップと [デバイス (Devices)] テーブルに表示されます。




ステップ 6 ホスト名に S7C と入力して、[デバイス (Device)] テーブルのデバイスをフィルタ処理します。[デバイス (Device)] テーブルには、フィルタ処理の基準に一致するデバイスのみが表示されます。ただし、[デバ

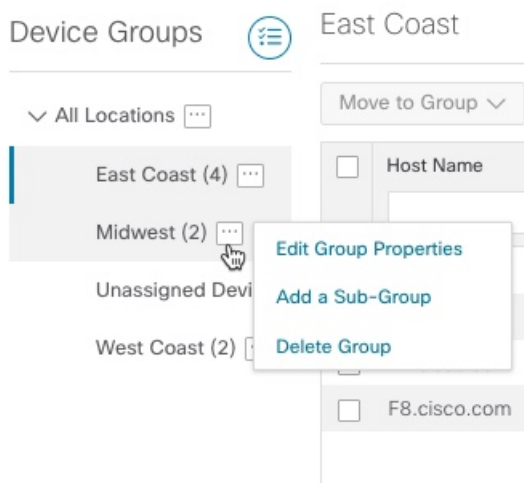
イス (Device)]テーブルをフィルタ処理しても、トポロジマップ上のデバイスは視覚的にフィルタ処理されません。地理的のマップまたは論理マップ上のデバイスを視覚的にフィルタ処理する唯一の方法は、デバイスグループを使用することです。



デバイスグループの作成と変更

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

ステップ 2 [デバイスグループ (Device Groups)]ツリーで、グループの横にある  をクリックします。



ステップ 3 グループの追加、削除、または編集 (名前の変更または移動) を選択します。グループを削除すると、そのグループに属しているすべてのデバイスが [未割り当てデバイス (Unassigned Devices)]グループに移動します。

(注) デバイスは、1つのデバイスグループにのみ属することができます。

ステップ4 [保存 (Save)]をクリックします。

ダイナミック デバイス グループの有効化


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



(注) ダイナミックルールは、すでにグループに属しているデバイスには適用されません。ダイナミックルールで考慮されるデバイスの一部としてそれらのデバイスを含める場合は、[未割り当てデバイス (Unassigned Devices)]に移動する必要があります。

始める前に

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

- ステップ1 メインメニューから [デバイス管理 (Device Management)] > [グループ (Groups)] を選択します。
- ステップ2  アイコンをクリックします。
- ステップ3 [他の詳細と例の表示 (Show more details and examples)] をクリックして、必要な [ホスト名 (Host Name)] フィールドと [グループ名 (Group Name)] フィールドに入力します。
- ステップ4 [未割り当てデバイス (Unassigned Devices)] グループに既存のデバイスがある場合は、[ルールのテスト (Test Rule)] をクリックして、作成されるグループ名のタイプのサンプリングを表示します。
- ステップ5 [ルールの有効化 (Enable Rule)] チェックボックスをオンにします。ルールが有効になると、システムはデバイスを1分おきに確認し、デバイスを作成するかグループに割り当てます。
- ステップ6 [保存 (Save)] をクリックします。
- ステップ7 この方法で作成されたグループは、最初は [未割り当てグループ (Unassigned Groups)] の下に表示されません (ルールが初めて有効になったときに作成されます)。新しく作成したグループを対応するグループ階層に移動します。
- ステップ8 新しく作成した未割り当てグループを適切なグループに移動するには、次の手順を実行します。
- [すべての場所 (All Locations)] の横にある [...] を選択し、[サブグループの追加 (Add a Sub-Group)] をクリックします。
 - [新しいグループ (New Group)] に詳細を入力して [保存 (Save)] をクリックします。
 - 未割り当ての作成済みダイナミックグループの横にある [...] を選択し、[グループプロパティの編集 (Edit Group Properties)] を選択します。


- d) [親グループの変更 (Change Parent Group)] をクリックし、適切なグループを選択します。

マップ表示設定のカスタマイズ

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

- [リンクとデバイスの表示のカスタマイズ](#) (23 ページ)
- [TE トンネルのデバイスグループの表示動作の設定](#) (23 ページ)

リンクとデバイスの表示のカスタマイズ

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

- デバイスの場合は、デバイスの状態とデバイスのラベル付けの方法を表示するかどうかを選択できます。デフォルトでは、デバイスの状態はマップに表示され、ホスト名はデバイスのラベル付けに使用されます。
- リンクの場合、集約リンクを表示するかどうかと、リンクの状態および使用状況を簡単に確認できるようにリンクを色付けする方法を選択できます。デフォルトでは、集約リンクはマップ上で単一リンクと区別され、リンクはリンク使用率のしきい値に基づいて色付けされます。管理者は、使用率のしきい値と対応する色を変更できます。
- TE トンネルの場合、IGP、TE、および遅延のメトリックを表示するかどうかを選択できます。デフォルトでは、これらのメトリックは有効になっていません。

TE トンネルのデバイスグループの表示動作の設定

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

デフォルトでは、ユーザ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。

簡易アクセスのトポロジビューの保存

マップ上のデバイスとリンクを再配置すると、通常、変更は保存されません。後でマップを開くと、マップ設定が失われます。

便利なマップレイアウトに簡単にアクセスするには、名前付きカスタムビューとして保存すると、毎回マップを再配置することなくすばやく取得できます。これは、多数のデバイスを含む大規模なネットワークを管理する場合に特に役立ちます。

カスタムビューを保存すると、次の設定が保存されます。

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




(注) すべてのカスタムビューは、すべてのユーザに表示されます。ただし、ビューを編集（変更、名前変更、または削除）できるのは管理者ロールを持つユーザまたはカスタムビューを作成したユーザのみです。

ステップ 1 カスタムビューを作成するには、次の手順を実行します。

- a) 必要な情報のみが含まれ、レイアウトがニーズを満たすまで、現在のマップビューをカスタマイズします。
- b) 思いどおりになったら、[ビューの保存 (Save View)] をクリックします。
- c) 新しいカスタムビューの一意の名前を入力し、[保存 (Save)] をクリックします。

ステップ 2 カスタムビューを削除するには、次の手順を実行します。

- a) [保存済みビュー (Saved Views)] フィールドをクリックします。
- b) 削除するカスタムビューを見つけて  をクリックします。

ステップ 3 カスタムビューを編集するには、次の手順を実行します。

- a) [保存済みビュー (Saved Views)] フィールドをクリックします。
- b) 編集するカスタムビューをクリックします。カスタムビューが表示されます。
- c) 現在のビューに変更を加え、[ビューの保存 (Save View)] をクリックします。これにより、以前に保存したビューが上書きされます。

ステップ 4 別の名前でビューの名前を変更するか、または保存するには、次の手順を実行します。

- a) [保存済みビュー (Saved Views)] ドロップダウンリストをクリックします。
- b) 適切なオプションを選択します。



第 3 章

SR-TE ポリシーと RSVP-TE トンネルのモニタ

ここでは、次の内容について説明します。

- [トポロジマップでの SR-TE ポリシーと RSVP-TE トンネルの表示 \(25 ページ\)](#)
- [SR-TE ポリシーと RSVP-TE トンネルの可視化の例 \(28 ページ\)](#)
- [タイムアウトの設定 \(38 ページ\)](#)

トポロジマップでの SR-TE ポリシーと RSVP-TE トンネルの表示

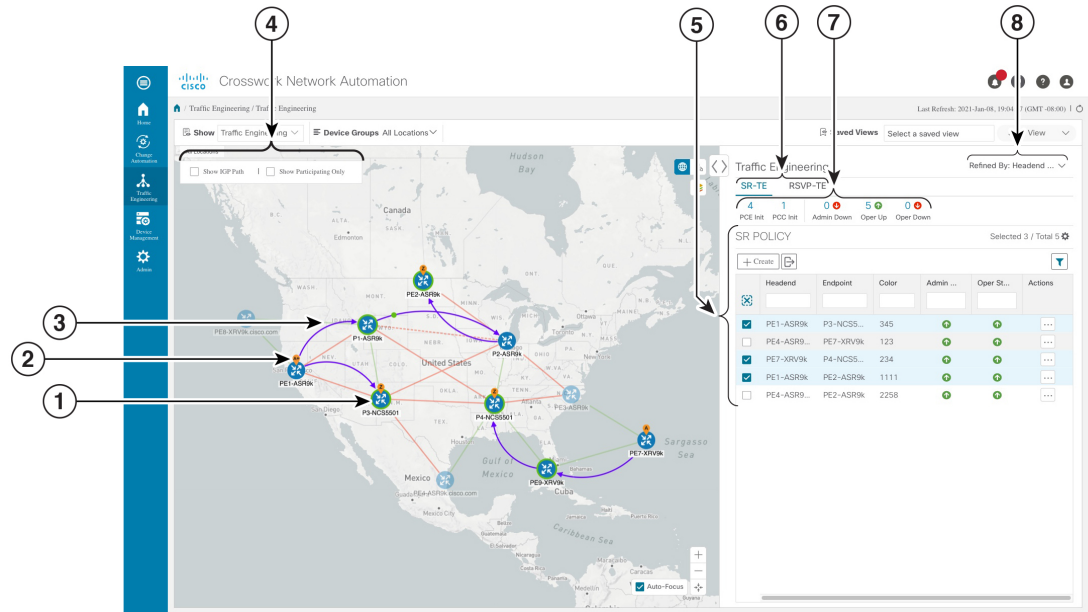
Crosswork Optimization Engine 可視化は、SR-TE ポリシーと RSVP-TE トンネルを簡単に表示および管理できるようにして、最も大きな価値をもたらします。ネットワークを視覚的に調べることで、これらの TE トンネルのプロビジョニングと維持の複雑さが大幅に緩和されます。

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



- (注) このドキュメントでは、ナビゲーションを [トラフィック エンジニアリング (Traffic Engineering)] > [トラフィック エンジニアリング (Traffic Engineering)] と記載しています。ただし、Crosswork Network Controller ソリューション内で Crosswork Optimization Engine を使用する場合、ナビゲーションは [トラフィック エンジニアリングとサービス (Traffic Engineering & Services)] > [トラフィック エンジニアリング (Traffic Engineering)] になります。

図 6: トラフィック エンジニアリングの UI

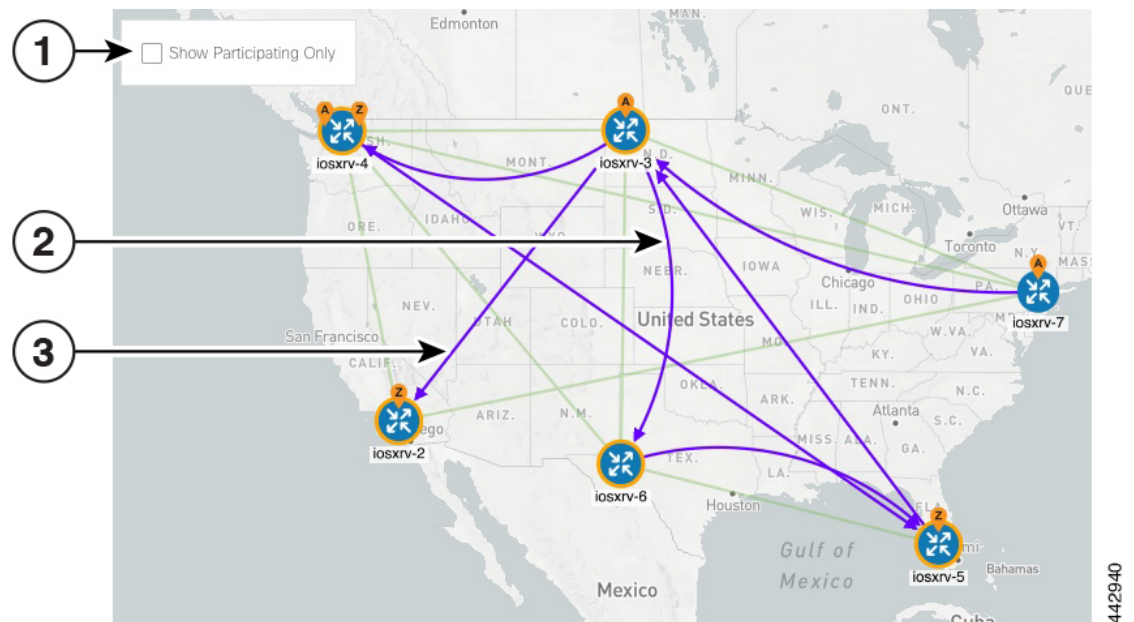


455226

引き出し線番号	説明
1	<p>SR-TEポリシー：緑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。</p> <p>RSVP-TE トンネル：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。</p> <p>(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。</p>
2	<p>SR-TE ポリシーと RSVP-TE トンネルの発信元と接続先：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、もう一方のノードが接続先です。A+ は、ノードから発信される複数の SR-TE ポリシーまたは 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 TE トンネルの接続先であることを示します。</p>

引き出し線番号	説明
3	<p>SR-TE ポリシーと RSVP-TE トンネル：</p> <p>SR-TE ポリシーまたは RSVP-TE トンネルが SR-TE ポリシーまたは RSVP-TE トンネルテーブルで選択されると、送信元と接続先を示す紫色の方向線としてマップに表示されます。</p> <p>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。</p>
4	<p>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。</p> <ul style="list-style-type: none"> • [IGPパスの表示 (Show IGP Path)]：選択した SR-TE ポリシーの IGP パスを表示します。このオプションは、RSVP-TE トンネルを表示する場合は使用できません。 • [参加の表示のみ (Show Participating Only)]：選択した TE トンネルに属するリンクのみを表示します。他のすべてのリンクとデバイスは表示されなくなります。
5	<p>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-TE] タブが選択され、[SRポリシー (SR Policy)] テーブルが表示されます。トポロジマップで選択した内容、または 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、次の操作を実行できます。</p> <ul style="list-style-type: none"> • SR-TE ポリシーと RSVP-TE トンネルの可視化の例 (28 ページ) • SR-TE ポリシーのプロビジョニング (39 ページ) • RSVP-TE トンネルのプロビジョニング (47 ページ)
6	<p>[SR-TE] タブまたは [RSVP-TE] タブをクリックして、TE トンネルのそれぞれのリストを表示します。</p>
7	<p>ミニダッシュボードには、動作中の TE トンネルのステータスと、[SRポリシー (SR Policy)] テーブルまたは [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、ミニダッシュボードが更新され、SR ポリシーまたは RSVP-TE テーブルに表示される内容が反映されます。</p>
8	<p>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。</p>

図 7: RSVP-TE トンネル



RSVP-TE トンネルの表示は、次の点を除いて類似しています。

引き出し線番号	説明
1	[IGPパスの表示 (Show IGP Path)] オプションは使用できません。
2	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。
3	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。

SR-TE ポリシーと RSVP-TE トンネルの可視化の例

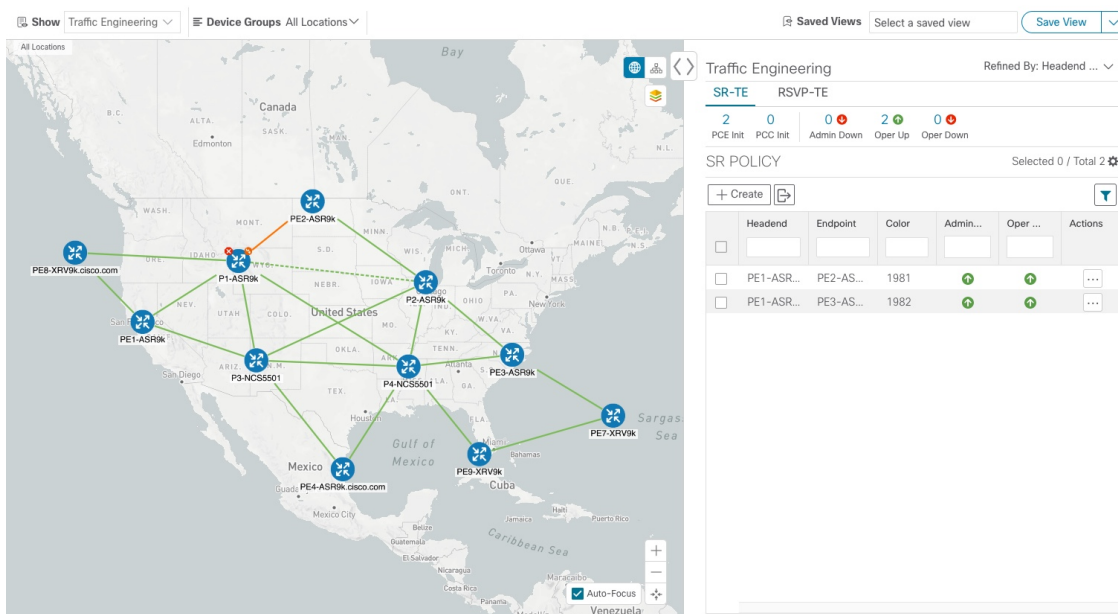
次の例では、トポロジマップから使用できる TE トンネル仮想化の多くの機能について説明します。トポロジマップには、UI を使用してプロビジョニングされた TE トンネルと、SR-PCE によってネットワークから検出されたトンネルが表示されます。そこから、参加している TE トンネルの詳細と可視化にドリルダウンできます。

この例では、デバイスと SR-TE ポリシーが追加され、デバイスグループが作成されていることを前提としています。SR-TE ポリシーはまだマップで強調表示されていません。



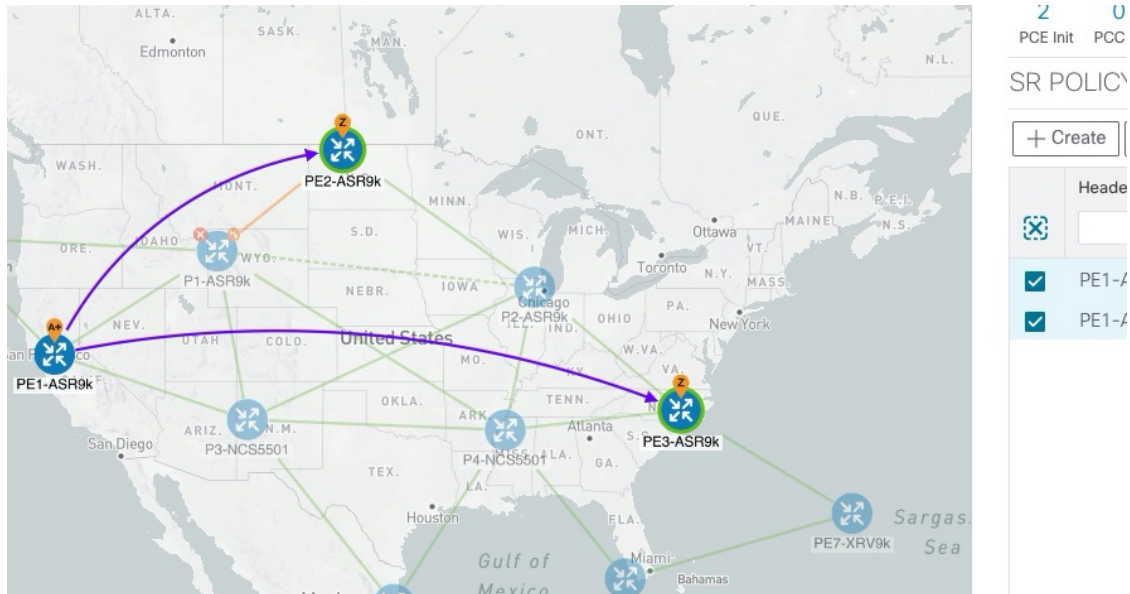
(注) この例では SR-TE ポリシーを使用していますが、SR-TE ポリシーと RSVP TE トンネルの両方のマップの基本機能は同じです。

図 8: トポロジマップの例



ステップ 1 [SRポリシー (SR Policy)]テーブルで、対象の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。この例では、2つのSRポリシーが選択されています。


図 9: SR-TE ポリシーの選択



SR-TE ポリシーを選択すると、マップには次が表示されます。

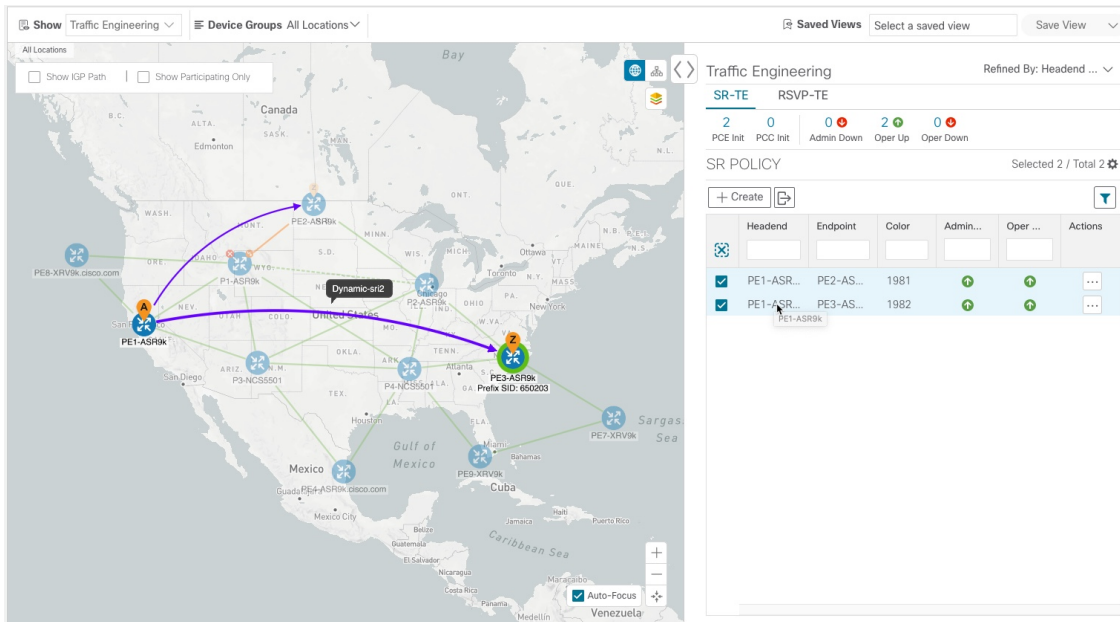
- SR-TE ポリシーは、パスの方向を示す矢印付きの紫色のリンクとして表示されます。
- PE1-ASR9k ノードは、選択した両方のポリシーの発信元です。PE2-ASR9k と PE3-ASR9k は、選択したポリシーの接続先です。SR-TE ポリシーの送信元と接続先は、それぞれ **A** と **Z** でマークされます。**A+** は、デバイスから発信される複数のポリシーがあることを示します。**Z+** は、デバイスが複数のポリシーの接続先であることを示します。

(注) **A** と **Z** の両方が 1 つのデバイスクラスタ内に表示される場合、クラスタ内の 1 つ以上のデバイスが送信元で、別のデバイスが接続先です。

-  は PE2-ASR9k と PE3-ASR9k にノード SID があることを示します。

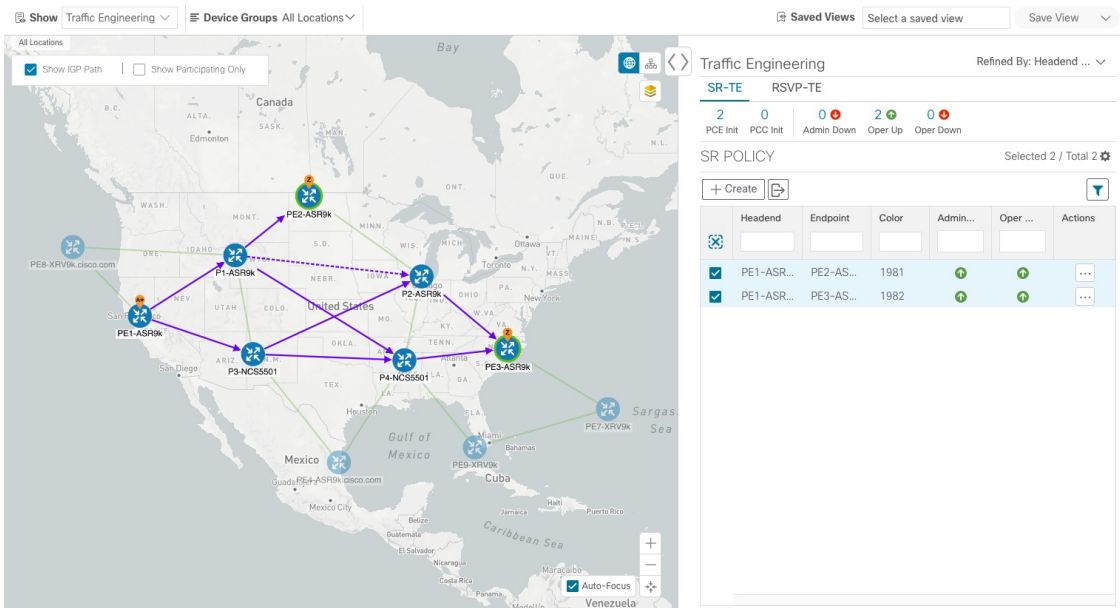
ステップ 2 [SRポリシー (SR Policy)] テーブルで、選択したポリシーにカーソルを合わせます。そのポリシーのパス名がトポロジビューに強調表示されます。プレフィックス SID 情報も表示されます。

図 10: SR-TE ポリシーにカーソルを合わせて詳細を表示



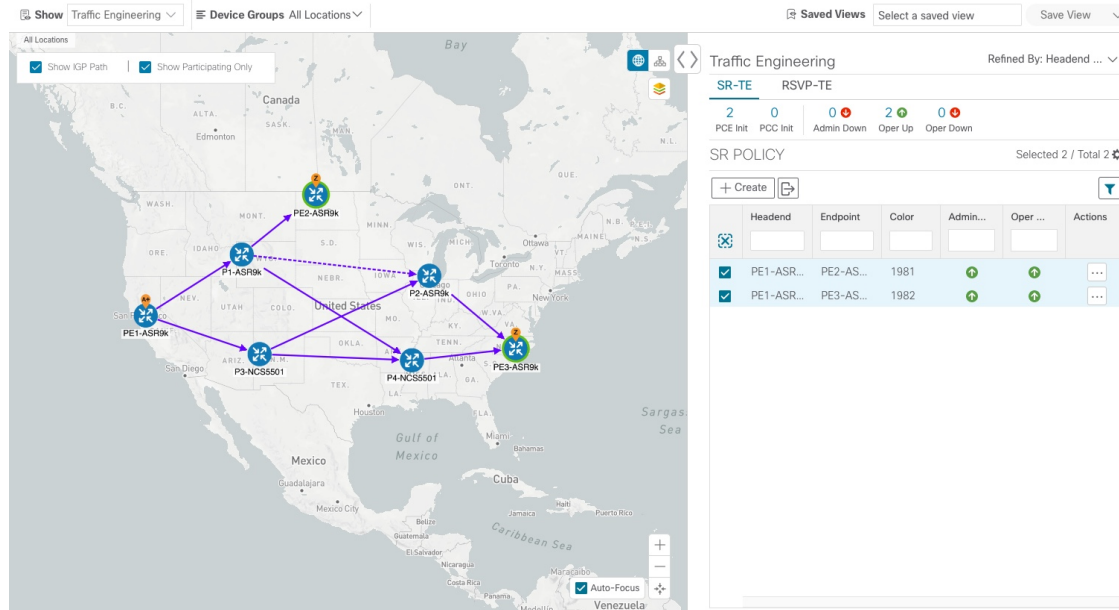
ステップ 3 エンドポイント間の物理パスを表示するには、[IGPパスを表示 (Show IGP Path)] チェックボックスをオンにします (SR-TE ポリシーでのみ使用可能)。選択した SR-TE ポリシーの IGP パスが、セグメントホップの代わりに直線で表示されます。

図 11: IGP パス




ステップ 4 [参加中のみ表示 (Show Participating Only)] チェックボックスをオンにします。参加していないリンクとデバイスはすべて表示されなくなります。参加中のポリシーのみが表示されます。

図 12: 参加中の SR-TE ポリシー

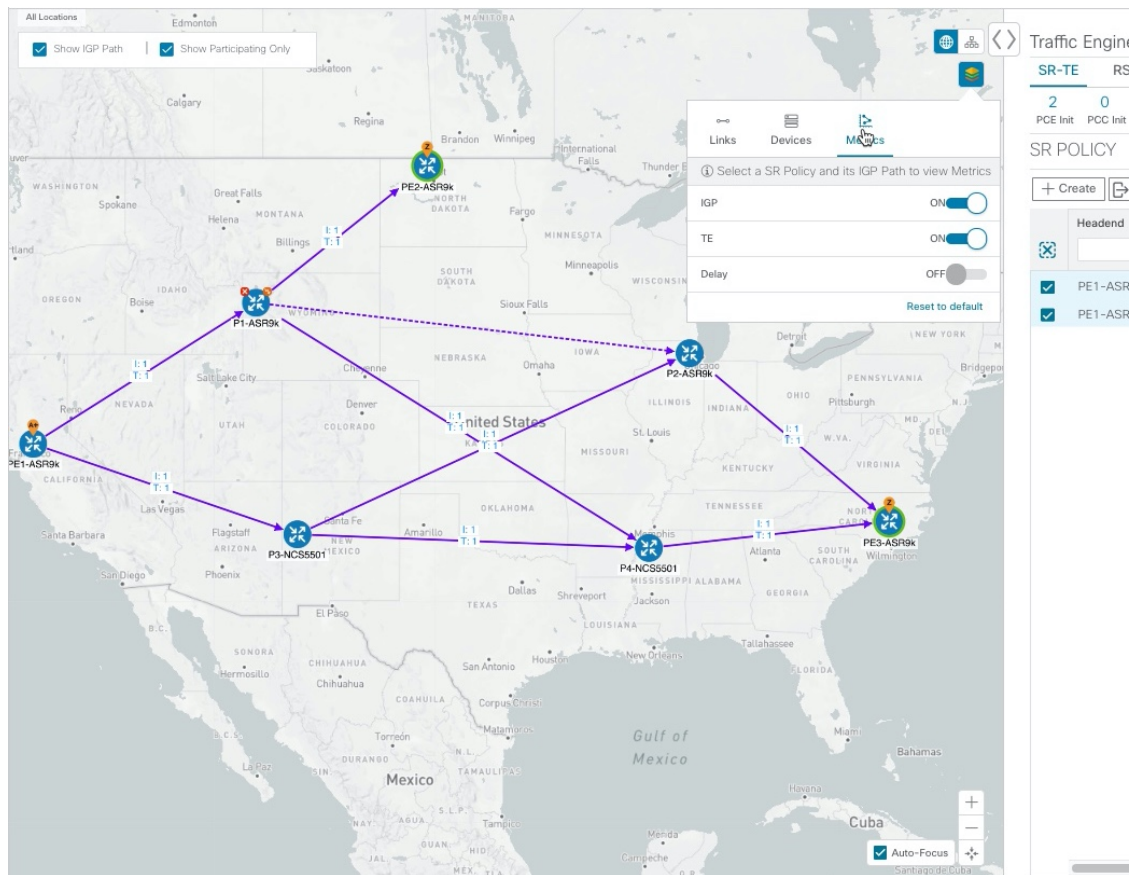


ステップ 5 ポリシーのパスに沿った各トンネルの IGP、TE、または遅延のメトリックを表示するには、次の手順を実行します。

- SR-TE ポリシーの場合にのみ、[IGPパスの表示 (Show IGP Path)] チェックボックスがオンになっていることを確認します。
-  をクリックします。
- [メトリック (Metrics)] タブをクリックします。
- 該当するメトリックを [オン (ON)] に切り替えます。

マップ上の各ポリシーのメトリックの詳細が表示されます。

図 13: IGP、遅延、および TE メトリック




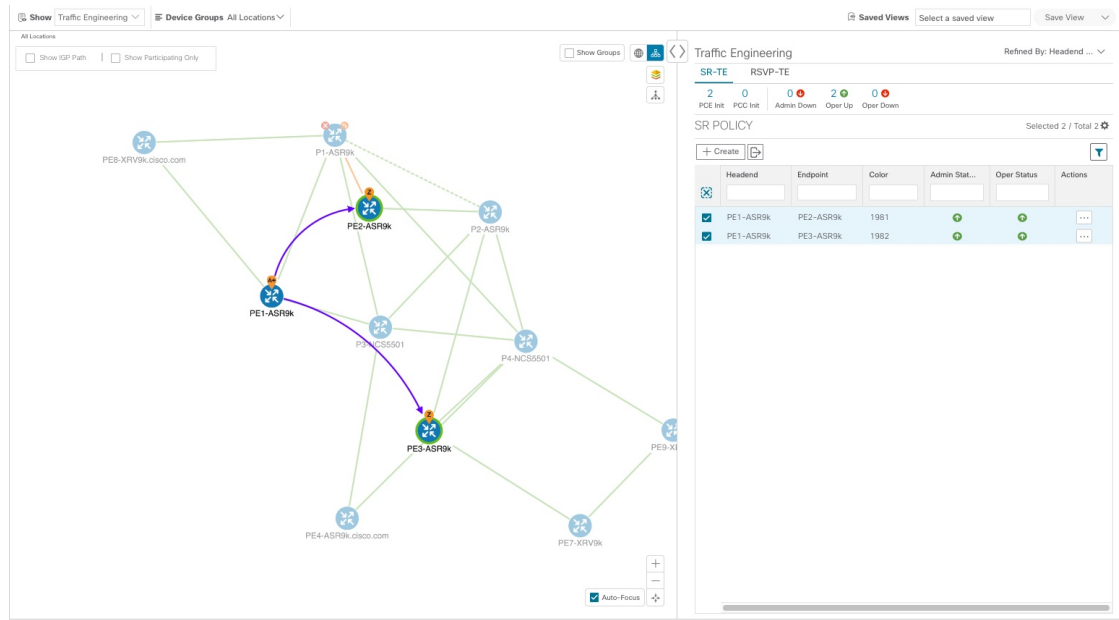
ステップ 6  をクリックすると、論理ビューが表示されます。

図 14: 論理マップ



地理的なトポロジマップで使用可能な同じ情報（地理的な場所を除く）を表示できます。また、マップ上でデバイスやリンクを移動して、見やすくすることもできます。[ビューの保存 (Save View)] をクリックして、現在のビューを保存し、後で取得します。

ステップ 7 分離グループ、メトリックタイプ、セグメントホップの情報などの SR-TE ポリシーの詳細を表示するには、テーブルの [アクション (Actions)] 列の下にある ... をクリックします。サイドパネルに [SRポリシーの詳細 (SR Policy Details)] ウィンドウが表示されます。選択したポリシーのみがトポロジマップに強調表示されていることに注意してください。

図 15: SR-TE ポリシーの詳細

SR Policy Details

Summary

- Headend: PE1-ASR9k (192.168.60.11)
- Endpoint: PE2-ASR9k (192.168.60.12) | 192.168.60.12
- Color: 1981
- Description: -
- Path Name: Dynamic-sri
- Policy Type: Dynamic
- Admin State: Up
- Oper State: Up
- Binding SID: 1005009
- Profile ID: 1981
- Utilization: 0 Mbps
- Delay: 2
- BWOD Policy Bandwidth: 0 Mbps
- Metric Type: IGP
- Accumulated Metric: 2
- Disjoint Group: ID: Association Source: - Type: -
- PCE Initiated: true
- Delegated PCE: 172.29.10.121
- Non-delegated PCEs: -
- Affinity: Exclude-Any: - Include-Any: - Include-All: -
- Segment: PCE Computed Time: 2020-Dec-16, 14:59:33 (GMT -08:00) Last Update: 2020-Dec-16, 14:59:43 (GMT -08:00)

Path

Segment	Segment Type	Label	IP	Node	Interface
0	Node SID	650202	192.168.60.12	PE2-ASR9k	

ステップ 8 現在のビュー (X) を閉じて、[SRポリシー (SR Policy)] テーブルに戻ります。

ステップ 9 SR-TE ポリシーまたは RSVP-TE トンネルを選択した場合のデバイスグループの表示方法を理解するには、選択されている可能性のある SR-TE ポリシーをオフにし、[グループの表示 (Show Groups)] をオンにします。

図 16: グループの表示

Show Groups

Traffic Engineering

SR-TE: 15 PCE Init, 6 PCC Init, 0 Admin Down, 17 Oper Up, 4 Oper Down

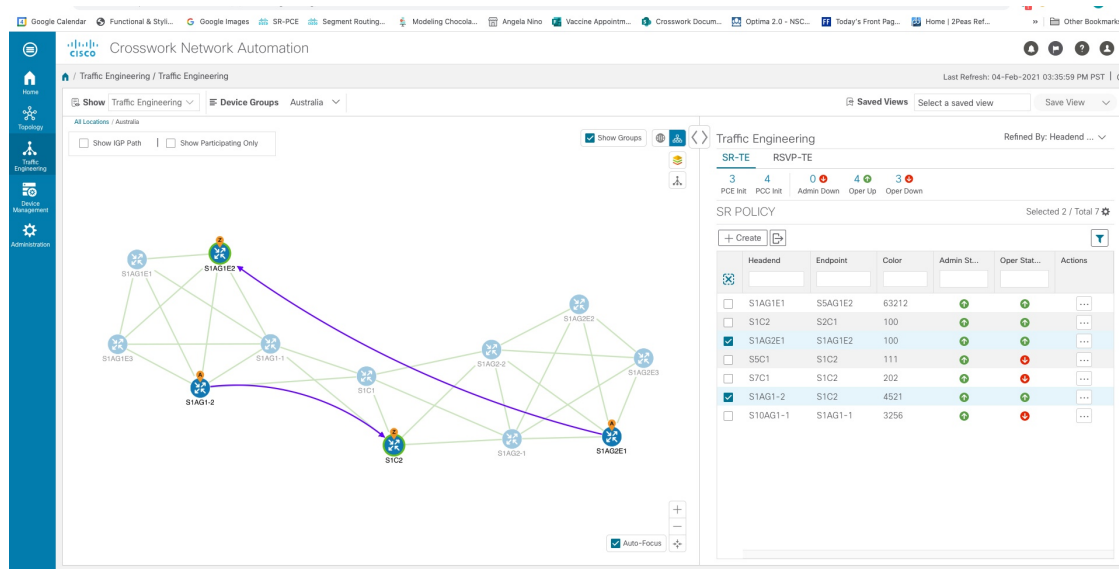
RSVP-TE: 0 Admin Down, 17 Oper Up, 4 Oper Down

SR POLICY

	Headend	Endpoint	Color	Admin St...	Oper Sta...	Actions
<input type="checkbox"/>	S1AG1E1	SSAG1E2	63212			...
<input type="checkbox"/>	S8AG1-1	S6C1	5522			...
<input type="checkbox"/>	S5AG1-1	S3AG1-1	102			...
<input type="checkbox"/>	S5C1	S7C1	22332			...
<input type="checkbox"/>	S10C1	S3C1	5123			...
<input type="checkbox"/>	S10AG2E3	S6AG2E1	3215			...
<input type="checkbox"/>	S2AG1-1	S2AG2-2	106			...
<input type="checkbox"/>	S10AG1-1	S10AG2E2	434			...
<input type="checkbox"/>	S2AG1E3	S2C1	6325			...
<input type="checkbox"/>	S10AG1-1	S10AG1E1	6325			...
<input type="checkbox"/>	S5C2	P-TOPRIGHT	100			...
<input type="checkbox"/>	S1C2	S2C1	100			...
<input type="checkbox"/>	S2AG1-1	S2AG2E3	100			...
<input type="checkbox"/>	S1AG2E1	S1AG1E2	100			...

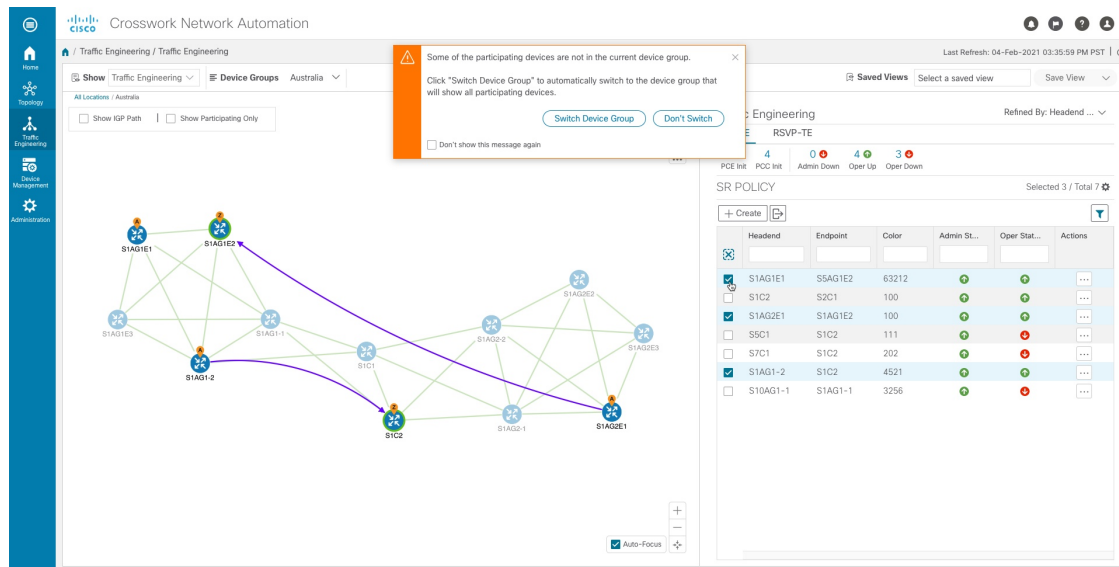
ステップ 10 [デバイスグループ (Device Groups)] ドロップダウンリストから特定のグループを選択すると、マップとにそのグループが表示されます。この例では、[オーストラリア (Australia)] が選択され、関連する SR-TE ポリシーが選択され、表示されます。

図 17: デバイスグループの選択



ステップ 11 参加中のデバイスが選択したグループの一部ではないポリシーを選択すると、グループビューを切り替えるオプションを示すダイアログが表示されます。これはデフォルトの動作です。このウィンドウが表示されない場合、自動的にビューを切り替えるか、または現在のビューにとどまるように管理者が表示を設定しています。詳細については、[TE トンネルのデバイスグループの表示動作の設定](#) (23 ページ) を参照してください。

図 18: [デバイスグループの切り替え (Switch Device Group)] ダイアログ



- ステップ 12** [デバイスグループの切り替え (Switch Device Group)] を選択すると、グループが変更され、選択した SR ポリシーに参加中のデバイスがすべて表示されます。前のグループビューに戻るには、[戻る (Back)] をクリックします (このリンクは、次の図に示す黄色のテキスト領域に後で表示されます)。

図 19: デバイスグループの切り替えの結果

The screenshot displays the Cisco Crosswork Network Automation interface. On the left, a network topology is shown with nodes representing different geographical locations: United Kingdom, Australia, China, South Africa, US Canada, Japan, and India. A specific device group is highlighted. On the right, the 'Traffic Engineering' dashboard is visible, showing a table of SR policies. The table has columns for Headend, Endpoint, Color, Admin Status, and Oper Status. Several policies are listed, including S1AG1E1, S8AG1-1, S5AG1-1, S5C1, S10C1, S10AG2E3, S2AG1-1, S10AG1-1, S2AG1E3, S10AG1-1, S5C2, S1C2, S2AG1-1, S1AG2E1, and S5C1. The 'S1AG2E1' policy is selected.

- ステップ 13** ミニダッシュボードを使用して、特定の SR-TE ポリシーにドリルダウンして焦点を当てることもできます。

The screenshot shows a detailed view of a specific SR-TE policy. The network topology on the left is more complex, showing connections between various ASes (Autonomous Systems) such as PE4-ASRtk, P3-NCS01, PE1-ASRtk, PE4-ASRtk, PE7-XRtk, PE2-ASRtk, and PE7-XRtk. The right-hand dashboard shows the 'Traffic Engineering' section with a table of SR policies. The table has columns for Headend, Endpoint, Color, Admin Status, and Oper Status. The 'PE1-AS...' policy is selected, and its details are shown in the table below.

Headend	Endpoint	Color	Admi...	Oper ...	Actions
<input type="checkbox"/>					
<input type="checkbox"/>	PE1-AS...	P3-NCS...	345	+	+
<input type="checkbox"/>	PE4-AS...	PE7-XR...	123	+	+
<input type="checkbox"/>	PE7-XR...	P4-NCS...	234	+	+
<input type="checkbox"/>	PE1-AS...	PE2-AS...	1111	+	+
<input type="checkbox"/>	PE4-AS...	PE2-AS...	2258	+	+

PCEによって開始されたポリシーのみを表示するように SR ポリシーテーブルをフィルタ処理するには、SR-TE ミニダッシュボードから [PCE で開始 (PCE Init)] の値をクリックします。[適用されたフィルタ (Filters Applied)] テキストが表示されます。

The screenshot shows the Cisco Traffic Engineering interface. On the left, there is a network topology diagram with nodes labeled PE4-ASRk, PE3-ASRk, PE2-ASRk, PE1-ASRk, PE7-XRk, PE6-XRk, PE5-XRk, PE4-AS, PE3-AS, PE2-AS, PE1-AS, P3-NCS, P4-NCS, and P5-NCS. On the right, the 'Traffic Engineering' section is visible, showing 'SR-TE' and 'RSVP-TE' status. Below this, there is a table of SR policies. The table has columns for 'Headend', 'Endpoint', 'Color', 'Admi...', 'Oper ...', and 'Actions'. The table contains four rows of data, each with a checkbox in the first column. The first row is highlighted with a red box.

	Headend	Endpoint	Color	Admi...	Oper ...	Actions
<input type="checkbox"/>	PE1-AS...	P3-NCS...	345			...
<input type="checkbox"/>	PE4-AS...	PE7-XR...	123			...
<input type="checkbox"/>	PE7-XR...	P4-NCS...	234			...
<input type="checkbox"/>	PE4-AS...	PE2-AS...	2258			...

ステップ 14 ノードのレイアウトを変更します。SRポリシーのレイアウトとフィルタ処理されたリストを保存するには、[ビューの保存 (Save View)] をクリックします。

(注) SR-TE ポリシーが選択されたカスタムビューは保存できません。

ステップ 15 フィルタ条件を削除するには、[適用されたフィルタ (Filters Applied)] > [すべてのフィルタをクリア (Clear All Filters)] をクリックします。複数のフィルタが適用されている場合は、個々のフィルタを選択することもできます。

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)] > [システム設定 (System Settings)] > [タイムアウト設定 (Timeout Configuration)] タブを選択します。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。



第 4 章

SR-TE ポリシーのプロビジョニング

ここでは、次の内容について説明します。

- [SR-TE ポリシーのサポート](#) (39 ページ)
- [SR ポリシー設定のソース](#) (41 ページ)
- [明示的 SR-TE ポリシーの作成](#) (42 ページ)
- [リンクアフィニティの設定](#) (43 ページ)
- [最適化インテントに基づくダイナミック SR-TE ポリシーの作成](#) (44 ページ)
- [SR-TE ポリシーの変更](#) (45 ページ)

SR-TE ポリシーのサポート

表 1: サポートされる機能

機能	注記
PCE によって開始されたポリシー (Crosswork によってプロビジョニングまたは検出)	—
PCC によって開始されたポリシー (Crosswork によって検出)	—
Crosswork によって検出された SR-TE オンデマンドネクストホップ (ODN) ポリシー	—
Crosswork の対象となるドメイン全体のルータで設定された単一の一貫性のあるセグメントルーティンググローバルブロック (SRGB)	インデックス SID が使用され、ポリシーのパスに沿って異なる SRGB ベースがある場合、ラベルはパスに沿って変更できます。
プレフィックス SID	—
隣接 SID	—
EPE 隣接 SID	—

機能	注記
保護された隣接 SID と保護されていない隣接 SID	—
通常のプレフィックス SID とストリクトプレフィックス SID	—
SR-TE ポリシー最適化目標の最小メトリック (IGP、TE、および遅延)	—
SR-TE ポリシーパスの制約 (アフィニティと分離)	分離されたグループまたはサブ ID ごとに 2 つの SR-TE ポリシーのみをサポート
明示的ポリシーまたはダイナミックポリシーのバインド SID	—
プロファイル ID	—

表 2: サポートされていない機能と制限事項

説明	注記
Crosswork を使用した複数の候補パスのプロビジョニング	これらのパスは、PCC 上に設定されている場合は検出されません。Crosswork は、これらのパスの設定をサポートしていません。
重み付け等コストマルチパス (WECMP)	—
候補パスごとに複数のセグメントリスト	<ul style="list-style-type: none"> この設定はサポートされていません。 これらのセグメントリストは、PCC 上に設定されている場合は検出されません。
複数の候補パスの可視化	現在アクティブなパスのみが UI に表示されます。
セグメントリストホップとしての SID のバインド	—
SR IGP フレキシブルアルゴリズム (Flex Algo)	—
エニーキャスト SID	—

説明	注記
ポリシーのホップ カウント メトリックタイプ	Cisco Crosswork は、このメトリックタイプによるプロビジョニングをサポートせず、PCC 上に設定されている場合は、このメトリックタイプを検出しません。
SR 対応でないルータ	Cisco Crosswork によって検出されたすべてのルータが SR 対応であることを前提としています。
セグメントリストのヘッドエンド/エンドポイントとプレフィックス SID に TE ルータ ID 以外のループバック IP を使用する SR-TE ポリシー	
IPv6 エンドポイント/ホップを使用してプロビジョニングされた SR-TE ポリシー	—
SRv6	分離グループ/サブ ID ごとに 2 つの SR-TE ポリシーのみ
SR-TE ポリシー最適化目標の最小メトリック（マージンあり）	Cisco Crosswork によってプロビジョニングされたポリシーではサポートされていません。PCC によって開始されたポリシーではマージンは検出されません。
SR-TE ポリシーの制約（リソース除外またはメトリックバウンド）	Cisco Crosswork によってプロビジョニングされたポリシーではサポートされていません。PCC によって開始されたポリシーでは制約は検出されません。

SR ポリシー設定のソース

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

- PCC によって開始：PCC に設定されたポリシー（[PCC によって開始された SR ポリシーの例（42 ページ）](#) を参照）。
- PCE によって開始：PCE 上に設定されたか、または Crosswork Optimization Engine によって動的に作成されたポリシー。Crosswork Optimization Engine を使用して設定された SR-TE ポリシーは、Crosswork Optimization Engine が変更または削除できる唯一の SR-TE ポリシーのタイプです。


PCC によって開始された SR ポリシーの例

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

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


明示的 SR-TE 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-TEポリシーを作成します。各リストは、パス上のノードまたはリンクを表します。

-
- ステップ1** メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [トラフィック エンジニアリング (Traffic Engineering)] を選択します。
- ステップ2** [SRポリシー (SR Policies)] テーブルで、[+ 作成 (+ Create)] をクリックします。
- ステップ3** 必要なSR-TEポリシー値を入力します。各フィールドの説明を表示するには、 の上にマウスポインタを合わせます。
- ヒント** デバイスグループをセットアップしている場合は、[デバイスグループ (Device Groups)] ドロップダウンメニューからデバイスグループを選択できます。次に、トポロジマップを移動してズームインし、デバイスをクリックしてヘッドエンドまたはエンドポイントを選択します。
- ステップ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-TE 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)] をクリックします。

ステップ 8 SR-TE ポリシーの作成を検証します。

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

(注) 新しくプロビジョニングされたSR-TE ポリシーは、ネットワークのサイズとパフォーマンスによっては[SRポリシー (SR Policy)]テーブルに表示されるまでに時間がかかることがあります。[SRポリシー (SR Policy)]テーブルは30秒ごとに更新されます。
2. 新しいSR-TE ポリシーの詳細を表示して確認します。[SRポリシー (SR Policy)]テーブルで、 をクリックして[表示 (View)]を選択します。

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


リンクアフィニティの設定


デバイスで定義されたアフィニティはCrosswork Optimization Engineによって収集されません。アフィニティマッピング名は、Crosswork Optimization Engineでの可視化にのみ使用されます。このため、デバイスインターフェイスでアフィニティを手動で収集してから、デバイスインターフェ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 Optimization Engine内でアフィニティマッピングを定義する必要があります。Crosswork Optimization Engineは、プロビジョニング時にビット情報のみをSR-PCEに送信します。


SR-TE ポリシーまたはRSVP-TE トンネルのアフィニティは、SR-TE ポリシーまたはRSVP-TE トンネルがアフィニティを持つリンク属性を指定するために使用されます。SR-TE ポリシーまたはRSVP-TE トンネルのパスを形成するのに適したリンクを決定します。これは32ビット値で、各ビット位置(0-31)はリンク属性を表します。アフィニティマッピングは、各ビット位置または属性を色にマッピングするために使用されます。これにより、リンク属性の参照が容易になります。


ステップ 1 メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)]>[TE リンク属性 (TE Link Affinities)]を選択します。[マッピングの管理 (Manage Mapping)]をクリックして、SR-TE ポリシーまたはRSVP-TE トンネルの作成時にアフィニティを定義することもできます。

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

- a) 名前(色)と割り当て先のビットを入力します。
- b)  をクリックしてマッピングを保存します。

ステップ 3 アフィニティマッピングを編集するには、 をクリックします。

- a) 必要な変更を加えます。変更を取り消すには、✕をクリックします。
- b)  をクリックして変更を保存します。

ステップ 4 アフィニティマッピングを削除するには、 をクリックします。


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

最適化インテントに基づくダイナミック SR-TE ポリシーの作成

このタスクでは、ダイナミックパスを使用して SR-TE ポリシーを作成します。SR-PCE は、ユーザ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。



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ダイナミック SR-TE ポリシーを作成します。詳細については、[リンクアフィニティの設定 \(43 ページ\)](#) を参照してください。

- ステップ 1** メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [トラフィック エンジニアリング (Traffic Engineering)] を選択します。
- ステップ 2** [SR ポリシー (SR Policies)] テーブルで、[+ 作成 (+ Create)] をクリックします。
- ステップ 3** 必要な SR-TE ポリシー値を入力します。各フィールドの説明を表示するには、 の上にマウスポインタを合わせます。
ヒント デバイスグループをセットアップしている場合は、[デバイスグループ (Device Groups)] ドロップダウンメニューからデバイスグループを選択できます。次に、トポロジマップを移動してズームインし、デバイスをクリックしてヘッドエンドまたはエンドポイントを選択します。
- ステップ 4** [ポリシーパス (Policy Path)] で、[ダイナミックパス (Dynamic Path)] をクリックし、パス名を入力します。
- ステップ 5** [最適化の目的 (Optimization Objective)] で、最小化するメトリックを選択します。
- ステップ 6** 該当する制約と分離を定義します。

(注) アフィニティの制約と分離は、同じ SR-TE 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-TE ポリシーを含めることはできません。ここで定義した分離グループに属する既存の SR-TE 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-TE ポリシーが表示されます。

- ステップ 7** [セグメント (Segments)] で、使用可能な場合にパブリックセグメントを使用するかどうかを選択します。
- ステップ 8** [プレビュー (Preview)] をクリックします。パスがマップに強調表示されます。
- ステップ 9** ポリシーパスをコミットする場合は、[プロビジョニング (Provision)] をクリックします。
- ステップ 10** SR-TE ポリシーの作成を検証します。
1. 新しい SR ポリシーが [SR ポリシー (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 ポリシーは、ネットワークのサイズとパフォーマンスによっては [SR ポリシー (SR Policy)] テーブルに表示されるまでに時間がかかることがあります。[SR ポリシー (SR Policy)] テーブルは 30 秒ごとに更新されます。
 2. 新しい SR ポリシーの詳細を表示して確認します。[SR ポリシー (SR Policy)] テーブルで、 をクリックして [表示 (View)] を選択します。

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

SR-TE ポリシーの変更

ポリシーを表示、編集、または削除するには、次の手順を実行します。

- ステップ 1** メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [トラフィック エンジニアリング (Traffic Engineering)] を選択します。
- ステップ 2** [トラフィック エンジニアリング (Traffic Engineering)] ウィンドウから [SR-TE] タブを選択します。
- ステップ 3** 目的の SR ポリシーを見つけて をクリックします。
- ステップ 4** [表示 (View)] または [編集/削除 (Edit/Delete)] を選択します。
- (注)
- UI で作成された SR-TE ポリシーのみを削除できます。
 - SR-TE 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。



第 5 章

RSVP-TE トンネルのプロビジョニング

ここでは、次の内容について説明します。

- [RSVP-TE トンネルのサポート \(47 ページ\)](#)
- [RSVP-TE トンネル設定のソース \(49 ページ\)](#)
- [明示的 RSVP-TE トンネルの作成 \(49 ページ\)](#)
- [リンクアフィニティの設定 \(50 ページ\)](#)
- [最適化インテントベースのダイナミック RSVP-TE トンネルの作成 \(51 ページ\)](#)
- [RSVP-TE トンネルの変更 \(52 ページ\)](#)

RSVP-TE トンネルのサポート

表 3: サポートされる機能

機能	注記
PCE によって開始されたトンネル (Crosswork Optimization Engine によるプロビジョニングまたは検出)	—
PCC によって開始されたトンネル (Crosswork Optimization Engine による検出)	—
ERO のストリクトホップ	—
ERO のルーズホップ (PCC による開始のみ)	—
Crosswork Optimization Engine によってプロビジョニングされたトンネルの FRR 保護	—
パス最適化の目標最小メトリック (IGP、TE、または遅延)	—

機能	注記
パスの制約（アフィニティと分離）	分離されたグループまたはサブ ID ごとに2つの RSVP トンネルのみをサポート
明示的トンネルおよび動的トンネルのバインディングラベル	—
シグナル帯域幅	—
セットアップ/保留の優先順位	—

表 4: サポートされていない機能と制限事項

説明	注記
COE でのルーズホップ ERO の設定	ストリクトホップのみを設定できません。パス上のすべてのホップにストリクトホップが設定されておらず、それらのホップがリモートインターフェイス IP またはループバック IP ではない場合、予期しない動作が発生することがあります。たとえば、トンネルが動作上ダウンしたままになったり、ホップが変更されたりすることがあります。
PCC で設定された名前付きトンネル	これらのトンネルは Crosswork Optimization Engine によって検出されません。
ヘッドエンドまたはエンドポイントとパスホップの TE ルータ ID 以外のループバック IP を持つトンネル	—
トポロジマップ内のアクティブな FRR 保護パスの表示	Crosswork Optimization Engine はトポロジマップに表示される FRR トンネルを検出しますが、アクティブに保護されているトンネルを使用中の FRR トンネルには関連付けません。保護がアクティブな場合、トポロジマップのパスには FRR 保護パスは含まれません。
P2MP トンネル	—

RSVP-TE トンネル設定のソース

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

- PCC によって開始 : PCC に設定された RSVP-TE トンネル ([PCC によって開始された RSVP-TE トンネルの例 \(49 ページ\)](#) を参照)。
- 動的に作成。

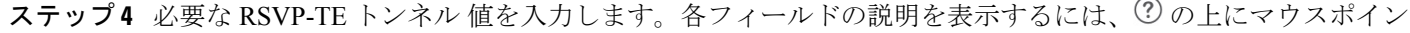
PCC によって開始された RSVP-TE トンネルの例

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

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

明示的 RSVP-TE トンネルの作成

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

-
- ステップ 1** メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [トラフィック エンジニアリング (Traffic Engineering)] を選択します。
 - ステップ 2** 右側のウィンドウで、[RSVP-TE] をクリックします。
 - ステップ 3** [RSVP-TE トンネル (RSVP-TE Tunnels)] で、[+ 作成 (+Create)] をクリックします。
 - ステップ 4** 必要な RSVP-TE トンネル 値を入力します。各フィールドの説明を表示するには、 の上にマウスポインタを合わせます。
ヒント デバイスグループをセットアップしている場合は、[デバイスグループ (Device Groups)] ドロップダウンメニューからデバイスグループを選択できます。次に、トポロジマップを移動してズームインし、デバイスをクリックしてヘッドエンドまたはエンドポイントを選択します。
 - ステップ 5** [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 6** 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、[RSVP-TE トンネル (RSVP-TE Tunnels)] テーブルに表示されるまでに時間がかかる場合があります。[RSVP-TE トンネル (RSVP-TE Tunnels)] テーブルは 30 秒ごとに更新されます。

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

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

リンクアフィニティの設定


デバイスで定義されたアフィニティは Crosswork Optimization Engine によって収集されません。アフィニティマッピング名は、Crosswork Optimization Engine での可視化にのみ使用されます。このため、デバイスインターフェイスでアフィニティを手動で収集してから、デバイスインターフェ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 Optimization Engine 内でアフィニティマッピングを定義する必要があります。Crosswork Optimization Engine は、プロビジョニング時にビット情報のみを SR-PCE に送信します。


SR-TE ポリシーまたは RSVP-TE トンネルのアフィニティは、SR-TE ポリシーまたは RSVP-TE トンネルがアフィニティを持つリンク属性を指定するために使用されます。SR-TE ポリシーまたは RSVP-TE トンネルのパスを形成するのに適したリンクを決定します。これは 32 ビット値で、各ビット位置 (0-31) はリンク属性を表します。アフィニティマッピングは、各ビット位置または属性を色にマッピングするために使用されます。これにより、リンク属性の参照が容易になります。


ステップ1 メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [TE リンク属性 (TE Link Affinities)] を選択します。[マッピングの管理 (Manage Mapping)] をクリックして、SR-TE ポリシーまたは RSVP-TE トンネルの作成時にアフィニティを定義することもできます。

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


- a) 名前 (色) と割り当て先のビットを入力します。

b)  をクリックしてマッピングを保存します。

ステップ3 アフィニティマッピングを編集するには、 をクリックします。

a) 必要な変更を加えます。変更を取り消すには、 をクリックします。

b)  をクリックして変更を保存します。

ステップ4 アフィニティマッピングを削除するには、 をクリックします。

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

最適化intentベースのダイナミック RSVP-TE トンネルの作成

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




ヒント アフィニティを使用する場合は、デバイスからアフィニティ情報を収集し、ダイナミック RSVP-TE トンネルを作成する前に Cisco Crosswork にマッピングします。詳細については、[リンクアフィニティの設定 \(43 ページ\)](#) を参照してください。

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

ステップ2 右側のウィンドウで、[RSVP-TE] をクリックします。

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

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

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

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

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

ステップ 7 該当する制約と分離を定義します。

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

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

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

ステップ 10 RSVP-TE トンネルの作成を検証します。

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

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

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

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

RSVP-TE トンネルの変更

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

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

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

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

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

- (注)
- UI を使用して作成した RSVP-TE トンネルのみを削除できます。
 - 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 6 章

ネットワーク輻輳の緩和



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

Cisco Crosswork は、ネットワーク帯域幅使用率をプロアクティブにモニタし、輻輳を緩和して、2つのツール（ローカルでの輻輳緩和と帯域幅最適化）のいずれかを使用して、指定されたしきい値を超えるトラフィック使用率の変化を追跡し、対応するという困難なタスクを緩和するのに役立ちます。

帯域幅最適化（BWOpt）は、輻輳に応じてネットワーク全体で動的にインテントベースのトラフィックを再ルーティングすることにより、クローズドループのトラフィックエンジニアリングを提供します。詳細については、[BWOpt を使用したネットワークの最適化（65 ページ）](#)を参照してください。

ローカルでの輻輳緩和（LCM）は、（トリガーされたイベントとは対照的に）設定可能な頻度で輻輳を検索し、周囲のインターフェイス内でローカライズされた緩和の推奨事項（ローカルインターフェイスレベルの最適化）を提供します。戦術的トラフィックエンジニアリング（TTE）SR ポリシーの展開をコミットするかどうかを決定する前に、ネットワーク上でこれらの推奨事項を視覚的にプレビューできます。LCM では、SNMP を介して TTE SR ポリシーとインターフェイスカウンタの収集を実行するため、SR-TM を使用する必要はありません。詳細については、[LCM を使用したローカルでの輻輳の緩和（56 ページ）](#)を参照してください。



(注) LCM を使用すると、パスの計算が簡素になり、特定のネットワーク要素に制限されるため、複数の IGP エリアを含むなど、さまざまなネットワークトポロジでソリューションをより幅広く適用できます。問題にローカルに焦点を当てることにより、完全なトラフィックマトリックスを通じてネットワーク内のエッジツーエッジトラフィックフローをシミュレートする必要がなくなります。

- [LCM を使用したローカルでの輻輳の緩和（56 ページ）](#)
- [BWOpt を使用したネットワークの最適化（65 ページ）](#)
- [個別のインターフェイスしきい値の追加（71 ページ）](#)

LCM を使用したローカルでの輻輳の緩和

ローカルでの輻輳緩和（LCM）は、インターフェイスレベルで、輻輳エリア内およびその周辺のキャパシティをローカルに確認します。LCMは、1つ以上の戦術的ポリシーの最短パスを計算して、輻輳したインターフェイス上の最小量のトラフィックを、十分な帯域幅を持つ代替パスに迂回させます。また、元のIGPパス上のトラフィックをできるだけ多く保持しようとします。ユーザが承認すると、LCMは戦術的トラフィックエンジニアリング（TTE）SRポリシーの展開を通じて緩和を実行します。LCMは、輻輳を緩和するためにSRポリシーの既存の展開のパスを変更しません。

TTE トンネルの推奨事項は、[LCM運用ダッシュボード（LCM Operational Dashboard）] にリストされます。このダッシュボードから、TTE SR ポリシーを展開する前に推奨を視覚的にプレビューできます。輻輳を解決するための TTE SR ポリシーの展開は自動化されていません。LCM 推奨アクションを承認してコミットする必要があります。LCM では、以前の TTE SR ポリシー（LCMによってインスタンス化）が不要になった場合は削除することも推奨されます。

LCM に関する特記事項

LCM を使用する場合は、次の情報を考慮してください。

- LCM は、10 分以上の通常の設定可能な頻度でネットワーク使用率を評価します。頻度は通常、SNMP トラフィックのポーリング間隔以上に設定されます。
- LCM は、パラレル TTE SR ポリシー全体で ECMP を活用し、トラフィックのほぼ均等な分割を想定します。実際の ECMP 分割がこの想定に従う程度は、大規模なエレファントフローの存在とレベルトラフィックの集約によって異なります。
- 最適化できるトラフィックは、既存の SR-TE ポリシーで伝送しないでください。

プラットフォーム要件

次に、LCM を適切に動作させるための大まかな要件のリストを示します。

輻輳評価：

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

輻輳緩和：

- ヘッドエンドデバイスは、複数のパラレル SR-TE ポリシーの全体にわたって等コストマルチパス（ECMP）をサポートする必要があります。

- ヘッドエンドデバイスは、autoroute のステアリングで PCE によって開始された SR-TE ポリシーをサポートする必要があります。

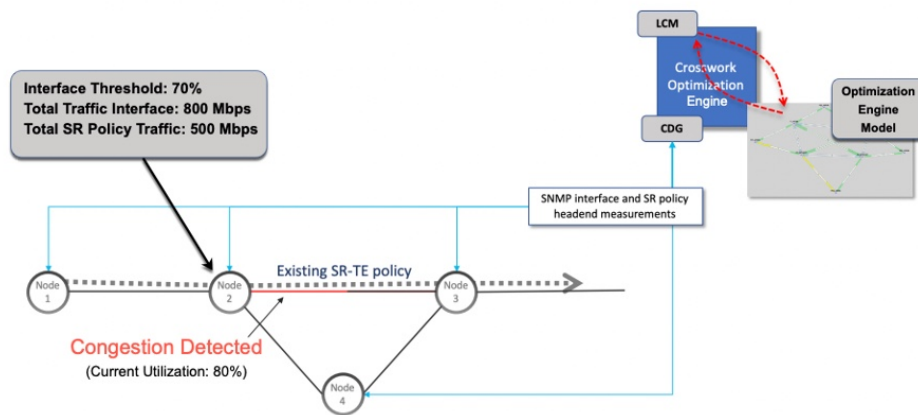
autoroute を使用して SR-TE ポリシーへのトラフィックステアリングを有効にするには、force-sr-include を使用してデバイスを設定する必要があります。次に例を示します。

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

LCM 計算のワークフロー

この例では、輻輳の検出から LCM が実行する計算を説明した後に、戦術的トンネル展開を推奨します。

図 20: LCM の設定ワークフローの例



- ステップ 1** LCM は、まず、Optimization Engine モデル（物理ネットワークのリアルタイムトポロジとトラフィックの表現）を定期的に分析します。
- ステップ 2** この例では、輻輳の確認間隔の後、ノード 2 の使用率が 70% の使用率しきい値を超えると、LCM が輻輳を検出します。
- ステップ 3** LCM は、転送に適したトラフィック量を見積もります。

LCM は、既存の SR ポリシーにないトラフィック（ラベルなし、IGP ルーティング、または FlexAlgo-0 SID 経由で伝送など）のみを転送します。SR-TE ポリシートラフィックは、対象トラフィックとして LCM 計算に含まれず、元のプログラムされたパスを通過し続けます。

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

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

このプロセスでは、SR ポリシーの ECMP 分割を考慮して、SR ポリシートラフィックを適切にアカウントリングする必要があります。この例では、輻輳したノード 2 の合計トラフィックは 800 Mbps です。ノード 2 経由でルーティングされるすべての SR ポリシーの合計トラフィックは 500 Mbps です。

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

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

$$800 \text{ Mbps} - 700 \text{ Mbps} (\text{しきい値 } 70\%) = 100 \text{ Mbps}$$

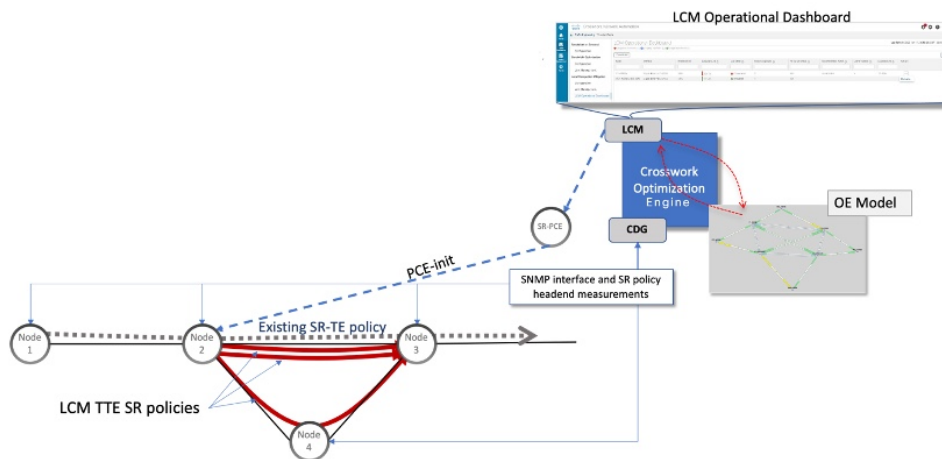
LCM は、300 Mbps のうちの 100 Mbps (対象トラフィック) を別のパスにルーティングする必要があると判断します。

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

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

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

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



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

ローカルインターフェイスでの輻輳の緩和の例

この例では、LCMを有効にし、使用率が定義されたしきい値を超えた場合にTTE SRポリシーを展開するための輻輳緩和の推奨事項を確認します。輻輳の緩和をコミットする前に、推奨されるTTE SRポリシーをプレビューします。次の図に、輻輳が発生する前の初期トポロジを示します。



ステップ1 LCM 設定前の初期トポロジと使用率を表示します。

- a) リンクの詳細を表示するには、PE1-ASR9k と P1-ASR9k 間のリンクをクリックします。現在、輻輳がない（使用率 0%）ことに注意してください。

The screenshot shows the 'Link Details' window for a link between PE1-ASR9k and P1-ASR9k. The link is labeled 'Z' on the map. The details are as follows:

Link Details		
	A Side	Z Side
Name	GigabitEthernet0/0/0/4-GigabitEthernet0/0/0/1	
State	Up	
Link Type	L3 ISIS IPV4	
ISIS Level	2	
Last Update	2020-Dec-19, 10:34:46 (GMT +08:00)	
Node	PE1-ASR9k	P1-ASR9k
TE Router ID	192.168.60.11	192.168.60.21
IF Name	GigabitEthernet0/0/0/4	GigabitEthernet0/0/0/1
IF Description	GigabitEthernet0/0/0/4	GigabitEthernet0/0/0/1
Type	ETHERNETCSMACD	ETHERNETCSMACD
IP Address	10.10.1.1	10.10.1.2
Utilization	0% (0Bps/1 Gbps)	0% (0Bps/1 Gbps)
IGP Metric	1	1
Delay Metric	1	1

ステップ2 LCM を有効にし、グローバル使用率のしきい値を設定します。

- a) メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [ローカルでの輻輳緩和の設定 (Local Congestion Mitigation Configuration)] を選択します。この場合、しきい値は25%に設定されます。

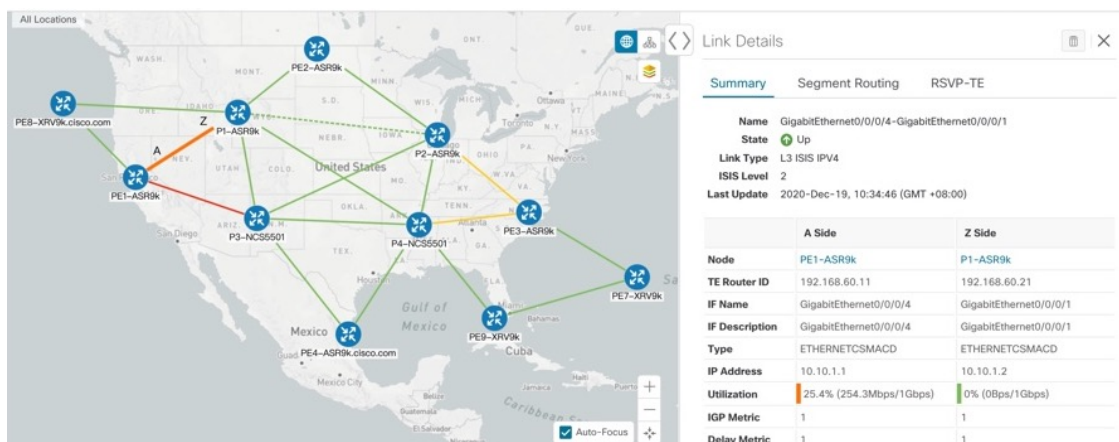
個々のインターフェイスに個別のしきい値を設定する場合は、[すべてのインターフェイスを含める (Include All Interfaces)] を [False] に切り替えます。

- b) (オプション) CSV ファイルをアップロードして、個々のリンクの特定のしきい値を定義します ([トラフィック エンジニアリング (Traffic Engineering)] > [ローカルでの輻輳緩和 (Local Congestion Mitigation)] > [リンク管理 (Link Management)])。

(注) CSV テンプレートの例をダウンロードできます。

ステップ3 LCM ダッシュボードで TTE SR ポリシーの推奨事項を表示します。

- a) しばらくすると、設定された LCM しきい値を超えて輻輳が発生します。リンクはオレンジ色で、使用率が高いことを示しています。



- b) [Refresh] をクリックして新しいイベントを表示します。このウィンドウをモニタして、発生した LCM イベントを表示することもできます。LCM の推奨事項、コミットアクション、および例外のイベントを確認する必要があります。

- c) [LCM運用ダッシュボード (LCMOperationalDashboard)] ([トラフィック エンジニアリング (Traffic Engineering)] > [ローカルでの輻輳緩和 (Local Congestion Mitigation)] > [LCM運用ダッシュボード (LCM Operational Dashboard)])。

ダッシュボードには、使用率が25%を超えていることが示されます。[推奨アクション (Recommended Action)] 列には、各インターフェイスの輻輳に対処するために2つの TTE ポリシー ソリューション セットの展開が推奨されています。[予測使用率 (Expected Util)] 列には、推奨アクションがコミットされた場合の各インターフェイスの予想使用率が表示されます。

LCM Operational Dashboard

Configuration

Link Management

LCM Operational Dashboard

Commit All

Node	Interface	Thresho...	Eval...	LCM State	Pol...	Pol...	Reco...	C...	Expected ...	Actions
PE1-ASR9k	GigabitEthernet0/0/0/5	25%	34.85%	Congested	0	-	Create Set	-	23.78%	...
PE1-ASR9k	GigabitEthernet0/0/0/4	25%	25.43%	Congested	0	-	Create Set	-	19.07%	...

- d) 各 TTE ポリシー ソリューション セットの TTE 展開をプレビューするには、 をクリックして [プレビュー (Preview)] を選択します。各 TTE ポリシーのノード、インターフェイス、および推奨アクションがウィンドウに表示されます。次の図に、インターフェイス GigabitEthernet0/0/0/4 の推奨 TTE ポリシーを示します。

[プレビュー (Preview)] ウィンドウから、個々の TTE ポリシーを選択し、トポロジマップで通常行っているように、さまざまな側面と情報を表示できます。

Recommended TTE Policies (Preview)

Node PE1-ASR9k

Interface GigabitEthernet0/0/0/4

Headend	Endpoint	Color	Recommended Action
<input checked="" type="checkbox"/>	PE1-ASR9k	P1-ASR9k	2000 CREATE
<input checked="" type="checkbox"/>	PE1-ASR9k	P1-ASR9k	2001 CREATE
<input checked="" type="checkbox"/>	PE1-ASR9k	P1-ASR9k	2002 CREATE
<input checked="" type="checkbox"/>	PE1-ASR9k	P1-ASR9k	2003 CREATE

Back To LCM Dashboard

- e) LCM の推奨事項に納得したら、[すべてコミット (Commit All)] をクリックします。LCM の [ステータス (Status)] 列が [緩和中 (Mitigating)] に変化します。

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

Node	Interface	Thresho...	Eval...	LCM State	Policies D...	Policy Set...	Reco...	Com...	Expected ...	Actions
PE1-AS...	GigabitEt...	25%	34.85%	Mitigating	2	-	-	-	23.78%	...
PE1-AS...	GigabitEt...	25%	25.43%	Mitigating	4	-	-	-	19.07%	...

ステップ 4 TTE SR ポリシーの展開を検証します。

- a) をクリックして [イベント (Events)] ウィンドウを開き、このウィンドウに表示される LCM イベントを確認します。

Description	Time	Severity	Source
Recommendation committed	2020-Dec-19, 10:43:52 (GMT +08:00)	INFO	Optima LCM
A new recommendation has been created: 6 creates, 0 updates, 0 delet...	2020-Dec-19, 10:40:17 (GMT +08:00)	INFO	Optima LCM
A new recommendation has been created: 2 creates, 0 updates, 0 delet...	2020-Dec-19, 10:18:48 (GMT +08:00)	INFO	Optima LCM
A new recommendation has been created: 7 creates, 0 updates, 0 delet...	2020-Dec-19, 10:08:48 (GMT +08:00)	INFO	Optima LCM
A new recommendation has been created: 5 creates, 0 updates, 0 delet...	2020-Dec-19, 09:58:47 (GMT +08:00)	INFO	Optima LCM
Recommendation committed	2020-Dec-17, 01:51:16 (GMT +08:00)	INFO	Optima LCM
A new recommendation has been created: 0 creates, 0 updates, 4 delet...	2020-Dec-17, 01:50:22 (GMT +08:00)	INFO	Optima LCM
Recommendation committed	2020-Dec-17, 01:44:49 (GMT +08:00)	INFO	Optima LCM
A new recommendation has been created: 4 creates, 0 updates, 0 delet...	2020-Dec-17, 01:36:29 (GMT +08:00)	INFO	Optima LCM
A new recommendation has been created: 4 creates, 0 updates, 0 delet...	2020-Dec-16, 22:03:10 (GMT +08:00)	INFO	Optima LCM
Recommendation committed	2020-Dec-16, 21:57:03 (GMT +08:00)	INFO	Optima LCM
Unable to fully deploy solution (delete Ips) to mitigate interface: PE1-A...	2020-Dec-16, 21:57:03 (GMT +08:00)	MAJOR	Optima LCM
Exception deleting LCM tactical policy: PE1-ASR9k : P1-ASR9k : 2002 ...	2020-Dec-16, 21:57:03 (GMT +08:00)	MAJOR	Optima LCM
A new recommendation has been created: 0 creates, 0 updates, 8 delet...	2020-Dec-16, 21:55:40 (GMT +08:00)	INFO	Optima LCM

- b) LCM ダッシュボードに戻り、すべての TTE ポリシー ソリューションセットの LCM の状態が [緩和済み (Mitigated)] に変化したことを確認します。

LCM の状態が変化するには、SNMP 頻度の 2 倍の時間がかかることに注意してください。

Node	Interface	Thresho...	Eval...	LCM State	Policies D...	Policy Set...	Reco...	Com...	Expected ...	Actions
PE1-AS...	GigabitEt...	25%	17.43%	Mitigated	2	OK	-	-	-	...
PE1-AS...	GigabitEt...	25%	15.81%	Mitigated	6	OK	-	-	-	...

- c) トポロジマップと [SRポリシー (SR Policy)] テーブルを表示して、TTE ポリシーの展開を確認します ([トラフィックエンジニアリング (Traffic Engineering)] > [トラフィックエンジニアリング (Traffic Engineering)] > [SR-TE] タブ)。

Headend	Endpoint	Color	Admin State	Oper State
<input type="checkbox"/>	PE1-ASR9k	P1-ASR9k	2000	Up
<input type="checkbox"/>	PE1-ASR9k	P1-ASR9k	2001	Up
<input type="checkbox"/>	PE1-ASR9k	P1-ASR9k	2002	Up
<input type="checkbox"/>	PE1-ASR9k	P1-ASR9k	2003	Up
<input type="checkbox"/>	PE1-ASR9k	P1-ASR9k	2004	Up
<input type="checkbox"/>	PE1-ASR9k	P1-ASR9k	2005	Up
<input type="checkbox"/>	PE1-ASR9k	P3-NCS5501	2000	Up
<input type="checkbox"/>	PE1-ASR9k	P3-NCS5501	2001	Up

ヒント 展開したばかりの SR-TE ポリシーの検索を絞り込むには、[SRポリシー (SR Policy)] テーブルで をクリックし、[ポリシータイプ (Policy Type)] を含めるチェックボックスをクリックします。次に、ポリシータイプを [ローカルでの輻輳緩和 (Local Congestion Mitigation)] としてフィルタ処理します。このタイプのすべての SR-TE ポリシーが表示されますが、SR-TE ポリシーリストではより簡単に並び替えることができます。

- d) 新しい SR-TE ポリシーのいずれかを選択し、SR ポリシーの詳細を表示します (をクリックして [表示 (View)] を選択します)。

Segment	Segment Type	Label	IP	Node	In
0	Node SID	650501	192.168.6...	P1...	

ステップ 5 LCM の推奨に従って TTE SR ポリシーを削除します。

- a) しばらくすると、展開された TTE SR ポリシーが不要になる場合があります。これは、LCM によって開始された TTE トンネルがなくても、使用率がしきい値を下回らない場合に発生します。この場合、LCM は TTE SR ポリシーセットを削除するための新しい推奨アクションを生成します。展開された TTE SR ポリシーを削除するには、[すべてコミット (Commit All)] をクリックします。

Node	Interface	Thresho...	Eval...	LCM State	Policies D...	Policy Set...	Reco...	Com...	Expected ...	Actions
PE1-AS...	GigabitE...	25%	17.43%	Mitigated	2	OK	Delete Set	-	17.43%	...
PE1-AS...	GigabitE...	25%	15.81%	Mitigated	6	OK	Delete Set	-	15.81%	...

- b) SR ポリシーを削除するには、[すべてコミット (Commit All)] をクリックします。
- c) トポロジマップと [SRポリシー (SR Policy)] テーブルを表示して、削除を確認します。

関連トピック

[個別のインターフェイスしきい値の追加 \(71 ページ\)](#)

LCM の設定


LCM を有効にして設定するには、次の手順を実行します。

- ステップ 1 メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [ローカルでの輻輳緩和 (Local Congestion Mitigation)] を選択します。
- ステップ 2 [有効化 (Enable)] スイッチを [True] に切り替えます。
- ステップ 3 必要な情報を入力します。各フィールドの説明を表示するには、(?) の上にマウスポインタを合わせます。
次のリストに、追加のフィールド情報を示します。

- [輻輳確認間隔 (Congestion Check Interval)] (秒単位) : この値は、LCM がネットワークの輻輳を評価する間隔を決定します。安定状態では、推奨のコミットがない場合、この間隔を使用してネットワークを再評価し、推奨事項を変更する必要があるかどうかを判断します。たとえば、間隔が 600 秒 (5 分) に設定されている場合、LCM は 5 分ごとにネットワークを評価して新しい輻輳がないかどうかを確認し、新しい推奨事項または既存の推奨事項に変更が必要かどうかを判断します。変更の例としては、以前に推奨された個々のポリシーの削除や更新などがあります。ネットワークを変更すると、情報が安定して LCM に伝達されるまでに時間がかかる場合があるため、間隔を SNMP 収集パターンの 2 倍以上に設定します。
- [詳細設定 (Advanced)] > [輻輳チェック抑制間隔 (秒) (Congestion Check Suspension Interval (seconds))] : この間隔によって、輻輳の検出と緩和を再開する前に ([すべてコミット (Commit All)] が実行された後) 待機する時間が決まります。ネットワークモデルのコンバージェンスの時間を考慮する必要があるため、この間隔は SNMP 収集パターンの 2 倍以上に設定します。

ステップ 4 [変更を確定 (Commit Changes)] をクリックします。

LCM 動作のモニタ

LCM の動作をモニタするには、LCM ダッシュボードを表示します ([トラフィック エンジニアリング (Traffic Engineering)] > [ローカルでの輻輳緩和 LCM 運用ダッシュボード (Local Congestion Mitigation LCM Operational Dashboard)])。[LCM運用ダッシュボード (LCM Operational Dashboard)] には、設定された使用率しきい値で定義された輻輳インターフェイスが表示されます。各インターフェイスについて、現在の使用率、推奨アクション、ステータス、推奨をコミットした後に予想される使用率などの詳細がリストされます。各列に表示される情報のタイプの説明を表示するには、マウスポインタを  に合わせます。このダッシュボードから、TTE ポリシーの推奨事項をプレビューして展開することもできます。

[LCM運用ダッシュボード (LCM Operational Dashboard)] に加えて、 をクリックして LCM イベントを表示できます。

BWOpt を使用したネットワークの最適化

帯域幅最適化 (BWOpt) は、ネットワーク内の輻輳を自動的に検出して緩和することで、セグメントルーテッドポリシーのクローズドループの戦術的トラフィックエンジニアリング (TTE) を提供します。テレメトリベースのセグメントルーティングトラフィックマトリックス (SRTM) を介して構築されたデマンドマトリックスでオーバーレイされたネットワークトポロジのリアルタイムビューによってこれを実現します。その目的は、リンクの使用率しきい値を設定することによって、帯域幅リソースの使用率を最適化することです。BWOpt は、ユーザが要求したインターフェイス使用率のしきい値を使用し、ネットワークの実際の使用率と比較します。インターフェイスの輻輳が BWOpt によって検出されると、BWOpt は、SR-PCE を介してネットワークに展開された TTE SR ポリシーを使用してインテントベースのトラフィックをホットスポットから再度ルーティングしようとしています。ネットワークの状態 (トポロジまたはトラフィック、あるいはその両方) が時間の経過とともに変化する場合、BWOpt は引き続きインターフェイスの使用率をモニタし、展開された TTE SR ポリシーを管理します。これには、パスの変更や、不要になったと見なされた場合のネットワークからの削除が含まれません。

BWOpt に関する特記事項

BWOpt を使用する場合は、次の情報を考慮してください。

- BWOpt は、作成しなかった既存の SR-TE ポリシー内のトラフィックを移動しません。これにより、輻輳したリンク上のトラフィックのほとんどが BWOpt 以外の SR-TE ポリシー内にある場合に、輻輳を緩和できなくなる場合があります。
- BWOpt は、PCC の autoroute 機能を使用して、作成する戦術的な SR-TE ポリシーにトラフィックを誘導します。autoroute は、BWOpt で設定された適切な [プロファイルID (Profile

ID)] のオプションを介してこれらのポリシーに適用されます（そのプロファイル ID を autoroute 機能に関連付ける PCC 上の設定と一致させるため）。これは、輻輳したリンクからトラフィックを移動させる戦術的な SR ポリシーにとって重要です。

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

自動化されたネットワーク輻輳の緩和の例

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

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

図 21: 帯域幅最適化の設定

Bandwidth Optimization

[Configuration](#)

[Link Management](#)

Configuration

Basic Advanced

Enable ?

False True

Optimization Objective ?

Minimize the IGP metric

Color ?

1000

Utilization Threshold ?

100

Utilization Hold Margin ?

5

Maximum Global Reoptimization Interval ?

0

Profile ID ?

0

Max Number of Parallel Tactical Policies ?

1

Commit Changes
Get Default Values
Discard Changes

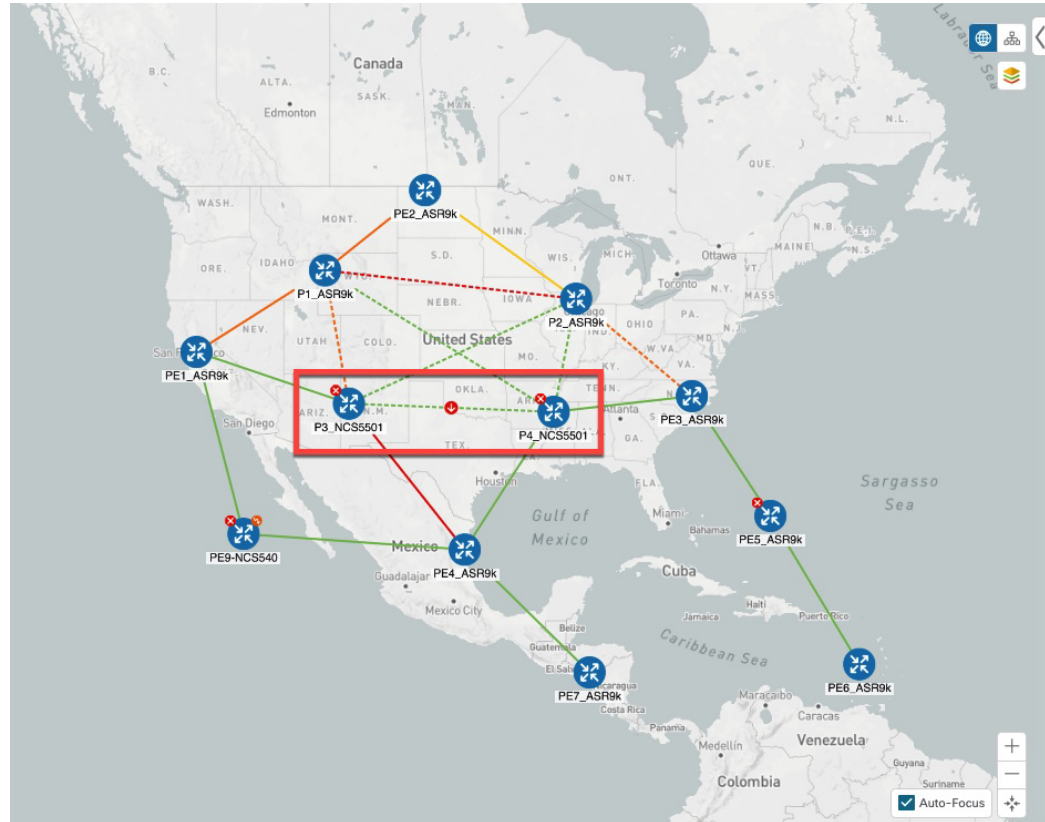
次に、米国に及ぶさまざまなデバイスとリンクのネットワークを示します。[SRポリシー (SR Policies)] テーブルに SR-TE ポリシーがリストされていないことに注意してください。

図 22: 例: 現在のネットワーク



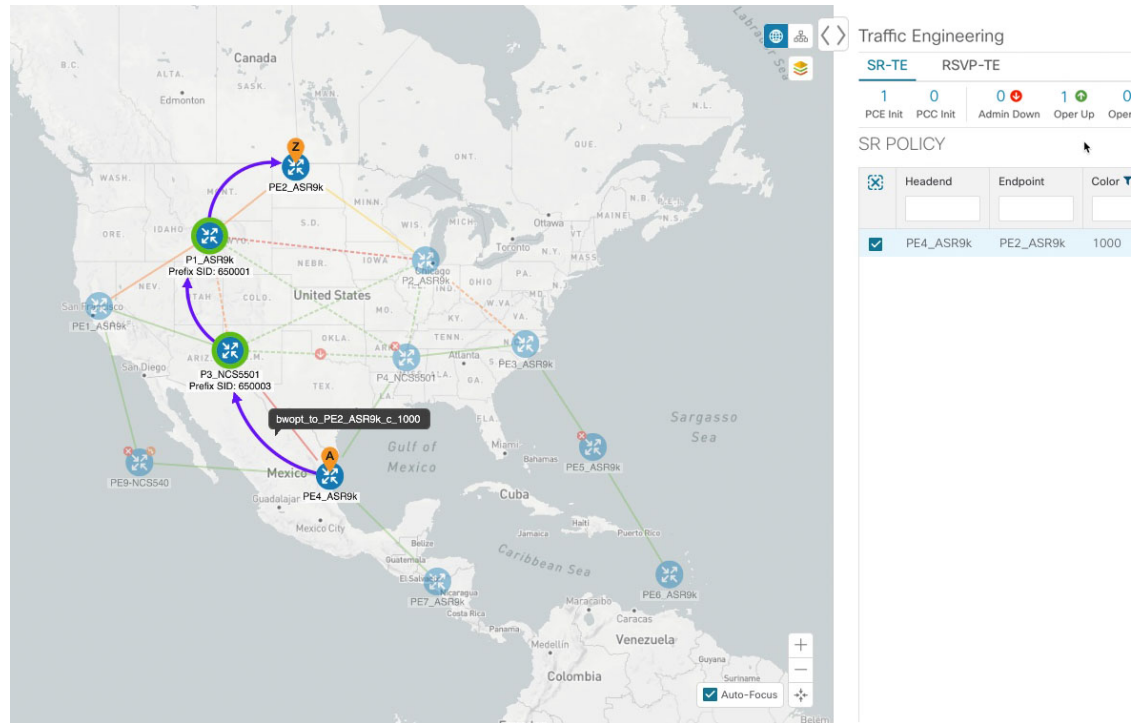
P3_NCS5501 と P4_NCS5501 間のリンクがダウンしたとします。トラフィックが他のリンクに移動し、それによって輻輳が発生して、設定された使用率のしきい値を超えます。

図 23: 例 : P3 ノードと P4 ノード間のリンクのダウン




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

図 24:例：展開された戦術的 SR ポリシー



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

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

帯域幅最適化の設定




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

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

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

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

(注) LCM と帯域幅の最適化を同時に有効にすることはできません。

- ステップ 3** 必要な情報を入力します。各フィールドの説明を表示するには、 の上にマウスポインタを合わせます。
- ステップ 4** [変更を確定 (Commit Changes)] をクリックします。BWOpt は、設定したしきい値と最適化の目的に基づいて、ネットワーク輻輳のモニタを開始します。

帯域幅最適化のトラブルシューティング

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



表 5: エラー

エラーイベントメッセージ	考えられる原因と推奨される修正処置
Optima Engine モデルエラー	<p>Optimization Engine を通じて BWOpt で使用されるネットワークモデルが破損しているか、または BWOpt を適切にサポートするために必要なキーデータが欠落しています。考えられる原因には、Optimization Engine とトポロジサービス間のネットワーク検出の問題または同期の問題などがあります。Optimization Engine ポッドを再起動してモデルの再構築を試してください。</p> <p>このエラーは、SR-PCE を通じて戦術的ポリシーを展開し、それを検出し、モデルに追加するために必要な時間が BWOpt に設定された [展開のタイムアウト (Deployment Timeout)] オプションを超えた場合にも発生します。デフォルトは 30 秒で、小規模から中規模のネットワークの場合はこれで十分です。ただし、大規模なネットワークではそれ以上の時間が必要になる場合があります。</p>
PCE ディスパッチが到達不能	<p>ネットワークへの戦術ポリシーの展開は、[展開タイムアウト (Deployment Timeout)] を超える前は正常に確認されません。[展開のタイムアウト (Deployment Timeout)] オプションの値を引き上げて、大規模なネットワークでの展開にさらに時間をかけるようにします。</p>

エラーイベントメッセージ	考えられる原因と推奨される修正処置
戦術的 SR ポリシーを展開できない	SR-PCE への戦術的な SR ポリシーの導入が失敗しています。これにはさまざまな理由が考えられます。BWOpt または PCE あるいはその両方のディスパッチログに障害の詳細に関するガイダンスが示されることがあります。SR-PCE プロバイダーのいずれかを介した PCC への基本的な SR ポリシーのプロビジョニング機能が動作していることを確認します。

個別のインターフェイスしきい値の追加

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

-
- ステップ 1** メインメニューから、次のいずれかを選択します。
- [ローカルでの輻輳緩和 (Local Congestion Mitigation)] > [リンク管理 (Link Management)]
 - [帯域幅最適化 (Bandwidth Optimization)] > [リンク管理 (Link Management)]
- ステップ 2**  をクリックします。
- ステップ 3** [サンプル設定ファイルのダウンロード (Download sample configuration file)] リンクをクリックします。
- ステップ 4** [キャンセル (Cancel)] をクリックします。
- ステップ 5** ダウンロードした設定ファイル (sampleLcmLinkManagement.csv) を開き、編集します。サンプルテキストを特定のノード、インターフェイス、およびしきい値情報に置き換えます。
- ステップ 6** ファイルの名前を変更して保存します。
- ステップ 7** [リンク管理 (Link Management)] ウィンドウに戻ります。
- ステップ 8**  をクリックして、編集した CSV ファイルに移動します。
- ステップ 9** [インポート (Import)] をクリックします。
- ステップ 10** [リンク管理 (Link Management)] ウィンドウに情報が正しく表示されることを確認します。
-



第 7 章

インテントベースの帯域幅要件の定義と維持



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

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

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

- [BWoD に関する特記事項 \(74 ページ\)](#)
- [インテントベースの帯域幅の要件を維持するための SR-TE ポリシーのプロビジョニングの例 \(74 ページ\)](#)
- [オンデマンド帯域幅の設定 \(78 ページ\)](#)
- [BWoD のトラブルシューティング \(79 ページ\)](#)

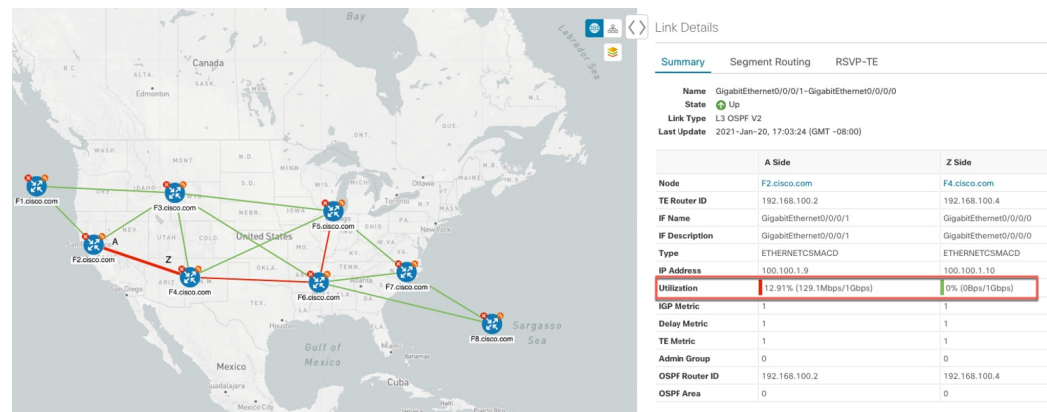
BWoDに関する特記事項

BWoDを使用する場合は、次の情報を考慮してください。

- 要求された帯域幅を保証するポリシーのパスをBWODが検出できない場合、このオプションが有効になっていると、BWODは「ベストエフォート」パスの検出を試みます。
- Optimization Engine の再起動またはトポロジサービスからのトポロジの再構築が原因で Optimization Engine モデルが使用できなくなると、BWODは一時的に動作を停止します。この期間中のBWODへの要求は拒否されます。モデルが使用可能になり、BWODが Optimization Engine から2つのトラフィック更新を受信すると、BWODは通常の動作を再開します。

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

図 25: 初期 BWoD トポロジの例



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

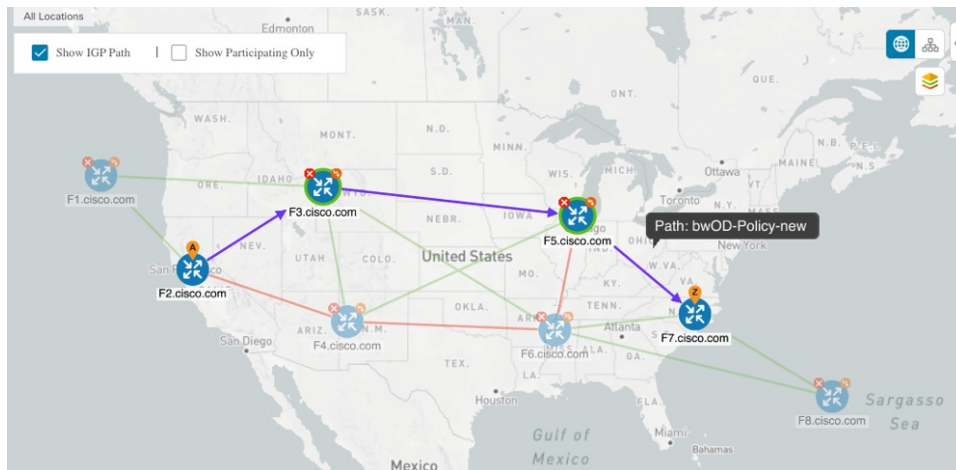
ステップ 1 BWoD を有効にして設定します。

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

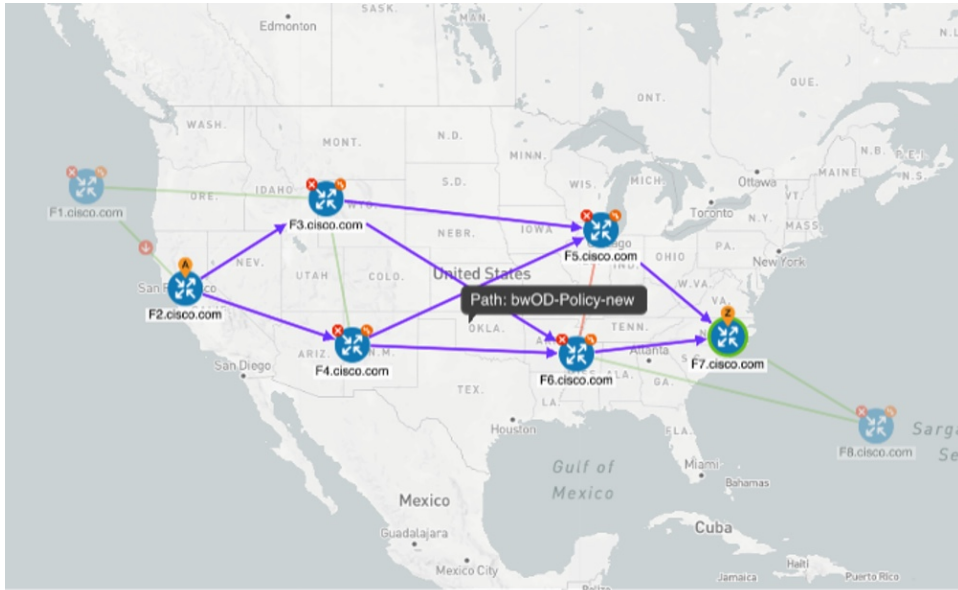
- b) [有効化 (Enable)] スイッチを [True] に切り替え、**80** を入力して使用率のしきい値のパーセンテージを設定します。他のオプションの説明を表示するには、**?** の上にマウスを重ねます。
- c) [変更を確定 (Commit Changes)] をクリックします。

ステップ 2 PCE-init BWoD SR-TE ポリシーを作成します。

- a) メインメニューから [トラフィック エンジニアリング (Traffic Engineering)] > [SR-TE] タブを選択し、[+ 作成 (+Create)] をクリックします。
- b) 必要な SR-TE ポリシーの詳細を入力します。
- c) [ポリシーパス (Policy Path)] フィールドで、[オンデマンド帯域幅 (Bandwidth on Demand)] をクリックし、BWoD パスの一意の名前を入力します。この場合は、**bwOD-Policy-new** と入力します。
- d) [最適化の目的 (Optimization Objective)] ドロップダウンリストから、[トラフィック エンジニアリング (TE) メトリック (Traffic Engineering (TE) Metric)] を選択します。
- e) [帯域幅 (Bandwidth)] フィールドに、要求された帯域幅を入力します。この例では、**920 Mbps** を要求しています。
- f) [プレビュー (Preview)] をクリックします。



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



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

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

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

- a) メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [SR-TE] を選択します。
- b) 新しい BWoD SR-TE ポリシーを選択し、SR ポリシーの詳細を表示します ([表示 (View)] をクリックして選択します)。[ポリシータイプ (Policy Type)] は [オンデマンド帯域幅 (Bandwidth on Demand)] であることを注意してください。

PCCによって開始された BWoD SR-TE のポリシー

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


次の図に、BWoD の PCC によって開始されたワークフローを示します。

引き出し線番号	説明
5、6	帯域幅準拠のパスが見つかった場合、セグメントリストが SR-PCE に返され、PCEP を介して PCC に転送され、PCC によってインスタンス化されます。BWoD がポリシーの BW 準拠パスを計算できない場合か、または BWoD が既存の BWoD ポリシーに BW 準拠パスを持たないように強制する場合は、BWoD によってベストエフォートパスが計算され、違反が最小限に抑えられます。また、これが発生したことで、BWoD が COE イベント UI にイベントを発行し、現在ベストエフォートパスになっている BWoD ポリシーを示します。
7	BWoD SR-TE ポリシーがインスタンス化されます。

オンデマンド帯域幅の設定

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

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

-
- ステップ 1** メインメニューから、[トラフィック エンジニアリング (Traffic Engineering)] > [オンデマンド帯域幅 (Bandwidth on Demand)] > [設定 (Configuration)] を選択します。
- ステップ 2** [有効化 (Enable)] スイッチを [True] に切り替えます。
- ステップ 3** 追加のオプションを設定します。各フィールドの説明を表示するには、 の上にマウスポインタを合わせます。
- ステップ 4** [変更のコミット (Commit Changes)] をクリックして、設定を保存します。
- ステップ 5** BWoD SR ポリシーを作成するには、[Traffic Engineering (トラフィック エンジニアリング)] > [トラフィック エンジニアリング (Traffic Engineering)] に移動します。
- ステップ 6** [SR ポリシー (SR Policy)] テーブルで、[作成 (Create)] > [PCE によって開始 (PCE Init)] をクリックします。
- ステップ 7** 必要な SR ポリシーの詳細を入力する以外に、[オンデマンド帯域幅 (Bandwidth on Demand)] オプションをクリックし、必要な帯域幅を入力します。
- ステップ 8** [プレビュー (Preview)] をクリックして、提案された SR ポリシーを表示します。
- ステップ 9** [プロビジョニング (Provision)] をクリックして、SR ポリシーをコミットします。
-

BWoD のトラブルシューティング

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

表 6: エラー

エラーイベントメッセージ	考えられる原因と推奨される修正処置
OptimaModelError	<p>Optimization Engine を通じて BWoD で使用されるネットワークモデルが破損しているか、または BWoD を適切にサポートするために必要なキーデータが欠落しています。考えられる原因には、Optimization Engine とトポロジサービス間のネットワーク検出の問題または同期の問題などがあります。Optimization Engine ポッドを再起動してモデルの再構築を試してください。</p> <p>このエラーは、展開された後にポリシーを検出してモデルに追加するために必要な時間が、BWoD に設定された [展開のタイムアウト (Deployment Timeout)] オプションを超えた場合にも発生する可能性があります。デフォルトは 30 秒で、小規模から中規模のネットワークの場合はこれで十分です。ただし、大規模なネットワークではそれ以上の時間が必要になる場合があります。</p>
NATSTimedOutError	<p>SR-PCEによる帯域幅ポリシーの展開がBWODに設定された[展開のタイムアウト (Deployment Timeout)]オプションを超えている。[展開のタイムアウト (Deployment Timeout)]オプションの値を引き上げて、大規模なネットワークでの展開にさらに時間をかけるようにします。</p>
トレースバックまたはログファイルで見つかったその他のエラー	<p>シスコの営業担当者にお問い合わせください。</p>

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.

